Veeam Agent for Microsoft Windows

Version 6

User Guide

December, 2023

© 2023 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 9
ABOUT THIS DOCUMENT 10
OVERVIEW 11
Solution Architecture 12
Standalone and Managed Operation Modes 13
Data Backup 15
Backup Types 16
How Backup Works 24
Backup Job 26
Backup Job Schedule 27
Ad-Hoc Backup 34
Parallel Disk Processing 37
Backup Chain 38
Backup to Object Storage 54
Backup to Deduplicating Storage Appliances 59
Health Check for Backup Files 61
Changed Block Tracking 68
Data Compression 73
Guest Processing 75
Data Encryption 89
Backup Cache 101
Backup to Rotated Drives 105
Backup of External Drives 108
Data Restore 109
Volume-Level Restore 110
File-Level Restore 111
Volume Resize 112
Veeam Recovery Media 115
Drivers in Veeam Recovery Media 116
BitLocker Encrypted Volumes Support 117
Integration with Veeam Backup & Replication 122
Backup to Veeam Cloud Connect Repository 124
MANAGING VEEAM AGENT IN VEEAM BACKUP & REPLICATION 125
PLANNING AND PREPARATION 126
System Requirements 127
Permissions 131
Ports 134

INSTALLATION AND CONFIGURATION 140
Before You Begin 141
Installing Veeam Agent for Microsoft Windows 142
Installing Veeam Agent for Microsoft Windows in Unattended Mode 143
Using Sysprep and Veeam Agent for Microsoft Windows 145
Upgrading Veeam Agent for Microsoft Windows 146
Configuring Advanced Settings 148
Uninstalling Veeam Agent for Microsoft Windows 149
What You Do Next 150
GETTING STARTED 151
LICENSING 152
Product Editions 153
License Agreements 154
Installing License 155
Selecting Product Edition 157
Revoking License 158
PERFORMING BACKUP 159
Creating Veeam Recovery Media 160
Before You Begin 161
Step 1. Launch Create Recovery Media Wizard 163
Step 2. Specify Recovery Media Options 165
Step 3. Specify Path to ISO 167
Step 4. Review Recovery Image Settings 168
What You Do Next 170
Creating Veeam Recovery Media with Command Line Interface 171
Creating Backup Jobs 172
Before You Begin 173
Step 1. Launch New Backup Job Wizard 174
Step 2. Specify Job Name and Description 175
Step 3. Select Backup Mode 176
Step 4. Specify Backup Scope Settings 178
Step 5. Select Backup Destination 185
Step 6. Specify Backup Storage Settings 187
Step 7. Specify GFS Retention Policy 218
Step 8. Specify Advanced Backup Settings 220
Step 9. Specify Backup Cache Settings 226
Step 10. Specify Guest Processing Settings 227
Step 11. Specify Backup Schedule 236
Step 12. Review Backup Job Settings 241
What You Do Next 242

Managing Backup Jobs 243
Editing Backup Job Settings 244
Disabling and Enabling Scheduled Backups 245
Removing Backup Job 247
Controlling Backup Post-Job Action 248
Performing Ad-Hoc Backups 249
Creating Incremental Backups 250
Creating Active Full Backups 252
Creating Standalone Full Backups 254
Performing Backup to Another Location 256
Performing Backup with Command Line Interface 258
Deleting Backups 262
Managing Backup Cache 264
Monitoring Backup Cache Activity 265
Pausing Backup Cache Synchronization 268
Deleting Restore Points from Backup Cache 269
PERFORMING RESTORE 270
Restoring from Veeam Recovery Media 271
Before You Begin 272
Step 1. Boot from Veeam Recovery Media 273
Step 2. Select Network Adapter or Wireless Network 275
Step 3. Launch Veeam Recovery Media Wizard 277
Step 4. Specify Backup File Location 278
Step 5. Select Network Storage Type 280
Step 6. Specify Network Storage Settings 281
Step 7. Select Backup 295
Step 8. Select Restore Point 297
Step 9. Select Data Restore Mode 298
Step 10. Map Restored Disks 299
Step 11. Resize Restored Volumes 303
Step 12. Start Restore Process 304
Using Veeam Agent and Microsoft Windows Tools 305
Using Microsoft Windows Recovery Environment 307
Restoring Volumes 308
Before You Begin 309
Step 1. Launch Volume Level Restore Wizard 310
Step 2. Specify Backup File Location 311
Step 3. Select Network Storage Type 312
Step 4. Specify Network Storage Settings 313
Step 5. Select Backup 326

Step 6. Select Restore Point 328
Step 7. Map Restored Disks 329
Step 8. Resize Restored Volumes 333
Step 9. Complete Restore Process 334
Restoring Files and Folders 335
Before You Begin 336
Step 1. Launch File Level Restore Wizard 337
Step 2. Specify Backup File Location 338
Step 3. Select Remote Storage Type 339
Step 4. Specify Remote Storage Settings 340
Step 5. Select Backup 353
Step 6. Select Restore Point 355
Step 7. Complete Restore Process 356
Step 8. Save Restored Files 357
Restoring Data from Encrypted Backups 362
REPORTING 364
Viewing Statistics in Control Panel 365
Viewing Statistics for Separate Restore Points 368
Viewing Information About Job Retries 371
Viewing Status of Restore Points in Backup Cache 373
Monitoring Backup State with Tray Agent 374
Monitoring Backup Process in Taskbar Button 376
Viewing and Dismissing Veeam Agent Events 377
Viewing Events with Windows Notification Center 380
Viewing Job Session Results in Email Reports 382
SPECIFYING SETTINGS 383
Throttling Backup Activities 384
Restricting Network Connections Usage 385
Limiting Bandwidth Consumption 386
Disabling Backup over Metered Connections 387
Disabling Backup over VPN Connections 389
Selecting Wireless Networks for Backup 391
Managing Rotated Drives 393
Disabling Control Panel Notifications 394
Enabling Email Notifications 395
Custom SMTP Server Settings 396
Gmail Server Settings 398
Microsoft 365 Server Settings 401
Checking for New Product Versions and Updates 405
MANAGING VEEAM CBT DRIVER 406

Installing Veeam CBT Driver 407
Removing Veeam CBT Driver 409
Removing CBT Driver with Veeam Recovery Media 410
Resetting CBT 411
GETTING SUPPORT 412
Reporting Issues 413
USING WITH VEEAM BACKUP & REPLICATION 415
Setting Up User Permissions on Backup Repositories 417
Managing License 420
Managing Instance Consumption by Veeam Agents 421
Assigning License to Veeam Agent 422
Viewing Licensed Veeam Agents and Revoking License 423
Performing Data Protection Tasks 425
Backing Up to Backup Repositories 426
Backing Up to Cloud Repositories 427
Performing Backup Copy for Veeam Agent Backups 429
Archiving Veeam Agent Backups to Tape 431
Restoring Data from Veeam Agent Backups 432
Restoring Veeam Agent Backup to vSphere VM 433
Restoring Veeam Agent Backup to Hyper-V VM 435
Restoring Veeam Agent Backup to Nutanix VM 437
Restoring to Microsoft Azure 438
Restoring to Amazon EC2 439
Restoring to Google Compute Engine 440
Restoring Volumes 441
Restoring Files and Folders 452
Restoring Application Items 470
Exporting Disks 471
Publishing Disks 482
Exporting Restore Point to Full Backup File 492
Performing Administration Tasks 493
Importing Veeam Agent Backups 494
Enabling and Disabling Veeam Agent Backup Jobs 496
Viewing Veeam Agent Backup Job Statistics 497
Deleting Veeam Agent Backup Jobs 498
Viewing Veeam Agent Backup Properties 499
Creating Recovery Token 500
Copying Veeam Agent Backups 502
Removing Veeam Agent Backups 503
Deleting Agent Backups from Disk 504

Configuring Global Settings 505
Assigning Roles to Users 506
AUTOMATING VEEAM AGENT FOR WINDOWS OPERATIONS 507
APPENDIX A. VEEAM AGENT EVENTS 508
APPENDIX B. MOVING VEEAM AGENT BACKUPS 512
Moving Veeam Agent Backups to Veeam Backup Repository 513
Moving Veeam Agent Backups to Veeam Cloud Connect Repository 516

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 Veeam Agent for Microsoft Windows.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for Microsoft Windows 6.0 or later to protect their computer.

Overview

Veeam Agent for Microsoft Windows is a data protection and disaster recovery solution for physical and virtual machines. Veeam Agent for Microsoft Windows can be used to protect different types of computers and devices: desktops, laptops and tablets. The solution can be installed on Windows-based workstations, physical servers and virtual machines. To learn about supported OSes, see System Requirements.

> **NOTE**
>
> Veeam Agent for Microsoft Windows can operate in either standalone or managed mode. Depending on the mode, Veeam Agent provides different features and limitations. To learn more, see Standalone and Managed Operation Modes.

Veeam Agent for Microsoft Windows offers a variety of features to protect your data. You can:

- Create a Veeam Recovery Media on an external hard drive, USB flash drive, CD/DVD/BD, or create an ISO file with the Veeam Recovery Media on disk.
- Create an entire system image backup, back up specific computer volumes or individual folders with files. Backups can be stored on an external hard drive, in a network shared folder, in object storage, in a Veeam backup repository or Veeam Cloud Connect repository.

In case of a disaster, you can perform the following restore operations:

- Start the OS from the Veeam Recovery Media and use Veeam Agent for Microsoft Windows and standard Microsoft Windows tools to diagnose and fix problems.
- Perform bare metal restore.
- Restore necessary data from backups to its original location or a new location.

Veeam Agent for Microsoft Windows integrates with Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform advanced tasks with Veeam Agent backups: perform data restore tasks with Veeam Agent backups, manage Veeam Agent backup jobs or backups created with these jobs.

Solution Architecture

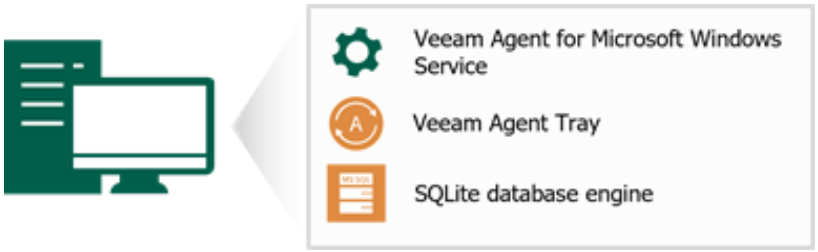
Veeam Agent for Microsoft Windows is set up on a computer whose data you want to protect.

Veeam Agent for Microsoft Windows has a one-service architecture. When you install the product, Veeam Agent deploys the following components on the computer:

- *Veeam Agent for Microsoft Windows Service* is a Microsoft Windows service responsible for performing all types of backup and restore tasks. The service is started automatically when you power on the computer, and runs in the background under the Local System account.
- *Veeam Agent Tray* is a tray agent that communicates with the Veeam Agent for Microsoft Windows Service to let you monitor the backup operation status and provide quick access to main functions of Veeam Agent for Microsoft Windows: starting backup and restore operations, viewing statistics for created backups and so on. The Veeam Agent Tray starts when you log on to the system and runs in the background.
- 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.

NOTE

The account under which Veeam Agent for Microsoft Windows Service runs should not be changed. Configurations with custom account are not supported.



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 object storage. 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 use the Veeam Agent management functionality in Veeam Backup & Replication, you must install Veeam Backup & Replication on the Veeam backup server.

  To use Veeam Agent operating in the managed mode, you must deploy the product in one of the following ways:

  - From Veeam Backup & Replication
  - Manually using external tools

  To learn more about managed Veeam Agent deployment, see the Protected Computers Discovery and Veeam Agent Deployment section in the Veeam Agent Management 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 Guides. Select the guide that suits your user role.

Data Backup

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

You can set up Veeam Agent for Microsoft Windows to perform automatic scheduled backups (triggered at specific time of the day or on specific events), or you can choose to back up data manually when needed. You can back up the entire computer image, specific computer volumes or individual folders with files.

Backups created with Veeam Agent for Microsoft Windows can be saved to one of the following locations:

- Removable storage device
- Local computer drive
- Network shared folder
- On-premises or cloud-based object storage
- Backup repository managed by a Veeam backup server
- Cloud repository managed by a Veeam Cloud Connect service provider

Backup Types

Veeam Agent for Microsoft Windows lets you create the following backup types:

- Volume-level backup
- File-level backup

  In the file-level backup, you can select what personal data to back up. To learn more, see Personal Data Backup.

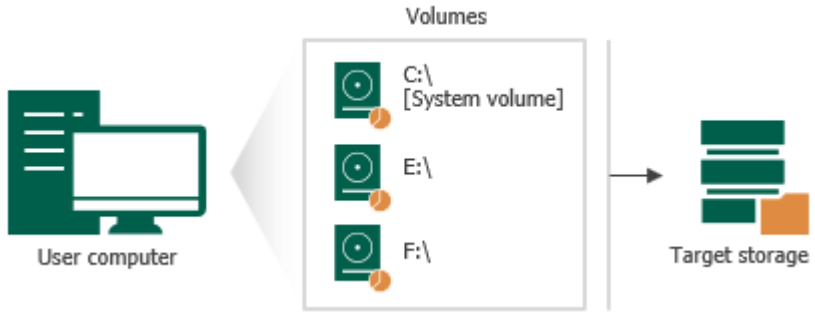
When backing up the operating system data, you can select the desired backup type. To learn more, see System State Data Backup.

Volume-Level Backup

You can set up Veeam Agent for Microsoft Windows to create a volume-level backup. The volume-level backup captures the whole image of a data volume (also called logical drive or partition) on your computer. You can use the volume-level backup to restore a computer volume, specific files and folders on the volume or perform bare metal recovery.

You can back up all computer volumes or specific computer volumes.

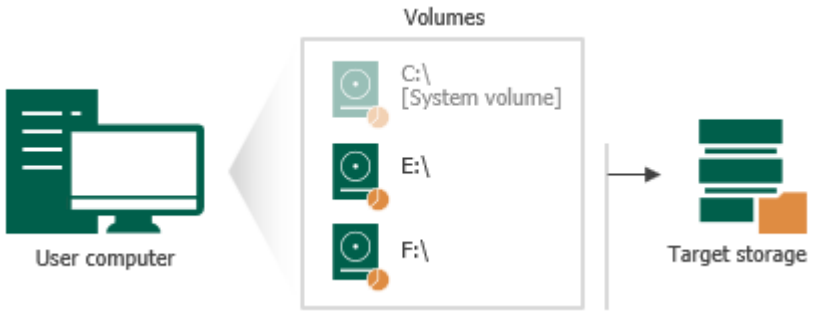
- When you back up the entire computer image, Veeam Agent captures the content of all volumes on your computer. The resulting backup file contains all volume data and Microsoft Windows OS system data: system partition and boot partition. For GPT disks on Microsoft Windows 8.1, 10, 11, 2012, 2012 R2, 2016, 2019 and 2022, Veeam Agent additionally backs up the recovery partition.



- When you back up a specific computer volume, Veeam Agent captures only that data that resides on this specific volume: files, folder, application data and so on.

  If you choose to back up the system volume (volume on which Microsoft Windows is installed), Veeam Agent automatically includes the *System Reserved* partition into the backup scope. You can exclude the *System Reserved* partition from the backup if necessary. In this case, Veeam Agent will capture only data on the system volume.

  To learn more, see System State Data Backup.

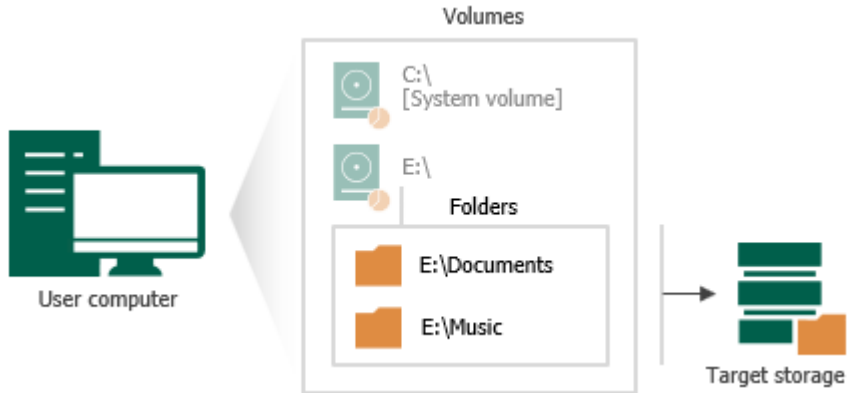


File-Level Backup

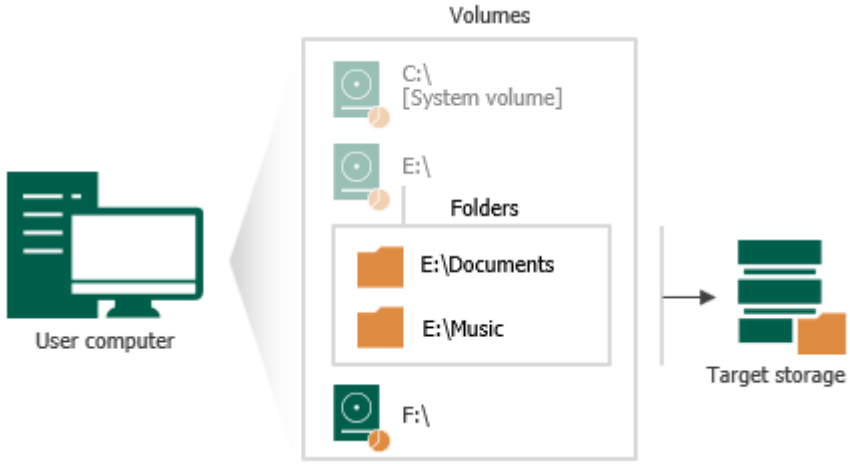
You can set up Veeam Agent for Microsoft Windows to create a file-level backup. The file-level backup captures only data of individual folders on the computer. You can use the file-level backup to restore files and folders that you have added to the backup scope.

Veeam Agent lets you create two types of file-level backups:

- You can include individual folders into the backup. When you recover from such backup, you will be able to restore folders that you have selected to back up, and files in these folders.



- You can create a hybrid backup that will include folders and specific computer volumes. When you recover from such backup, you will be able to restore the following components:
  - For backed-up volume: the entire volume and individual files and folders on this volume.
  - For backed-up folders: folders that you have selected to back up, and files in these folders.

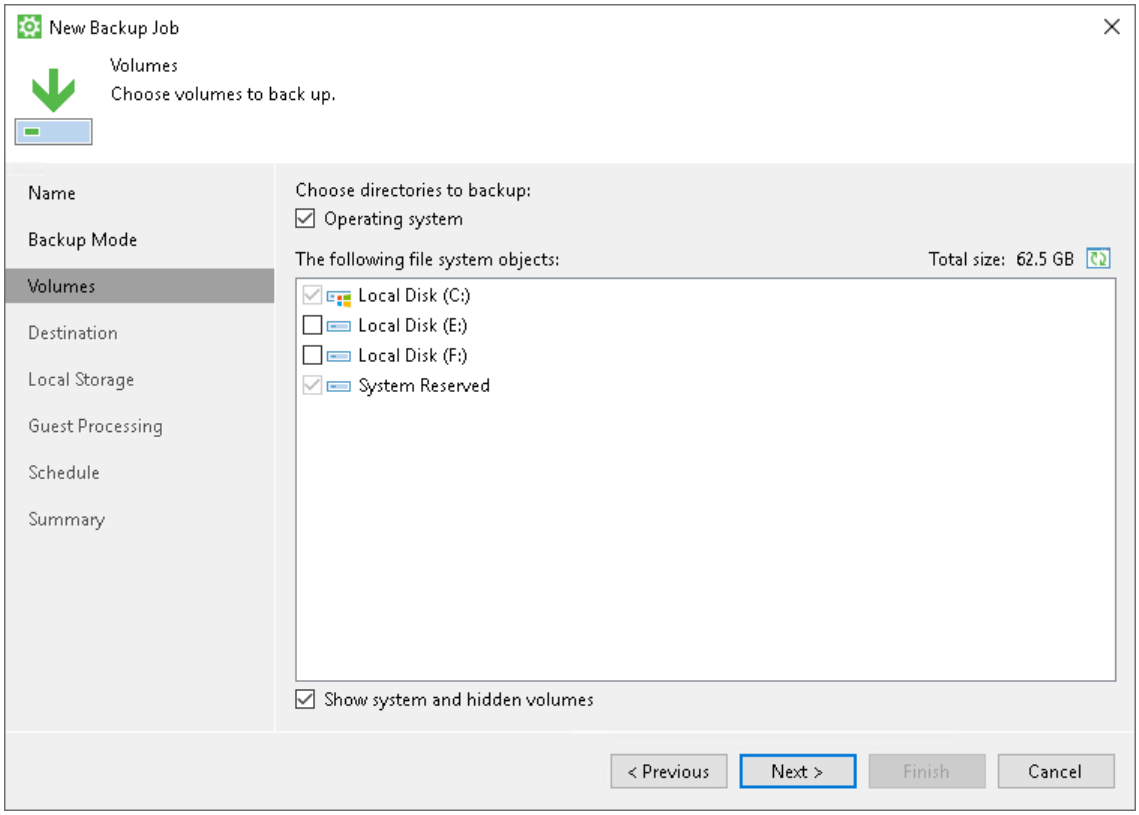


System State Data Backup

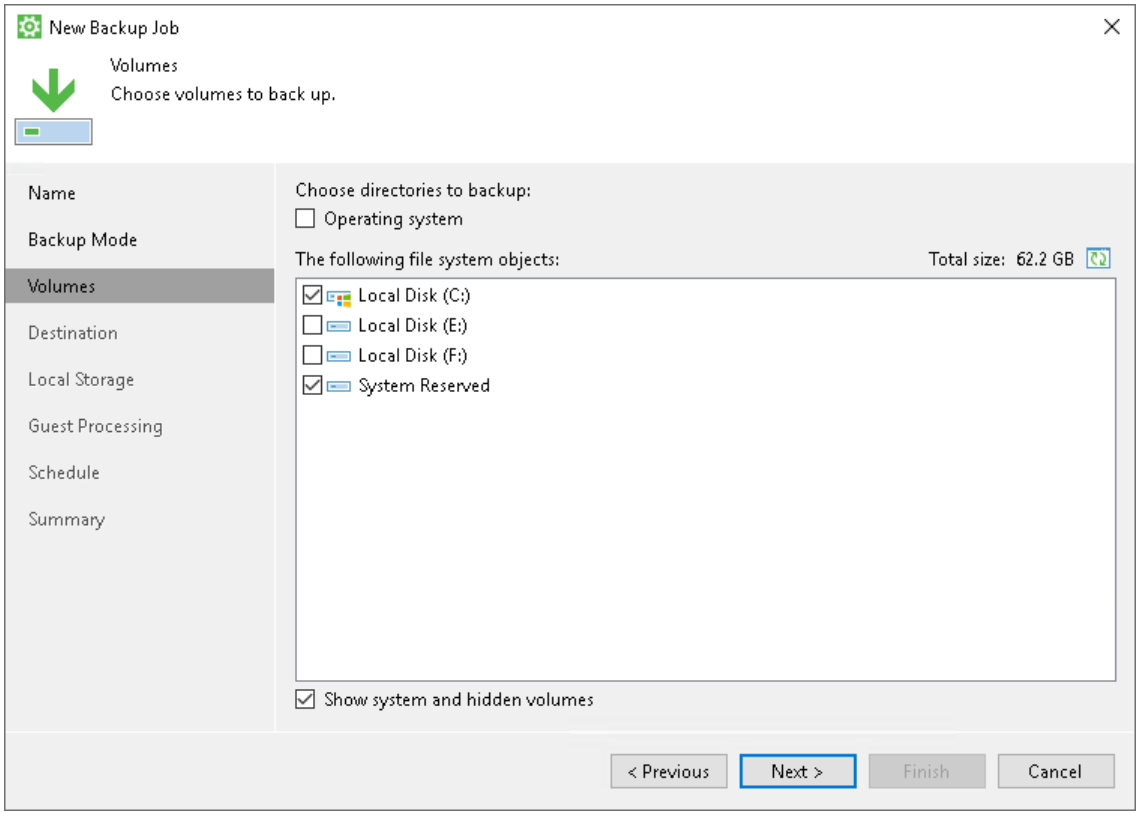
To be able to restore critical components related to the OS and start the OS after recovery, you must include in the backup the system volume (volume on which the OS is installed) and the System Reserved/UEFI or other system partitions. To simplify this process, Veeam Agent for Microsoft Windows offers you to add the *Operating system* component to the backup scope. When you select to back up the operating system data, Veeam Agent automatically includes in the backup all data related to the OS. You can include the operating system data in the volume-level and file-level backup.

System State Backup in Volume-Level Backup

To include the operating system data in the volume-level backup, select the **Operating system** check box. When you select to back up the operating system data, Veeam Agent automatically includes in the backup the system volume and existing system partitions. If some additional system partitions appear on the Veeam Agent computer in the future, for example, after the OS upgrade, Veeam Agent will add these partitions to the backup scope too.

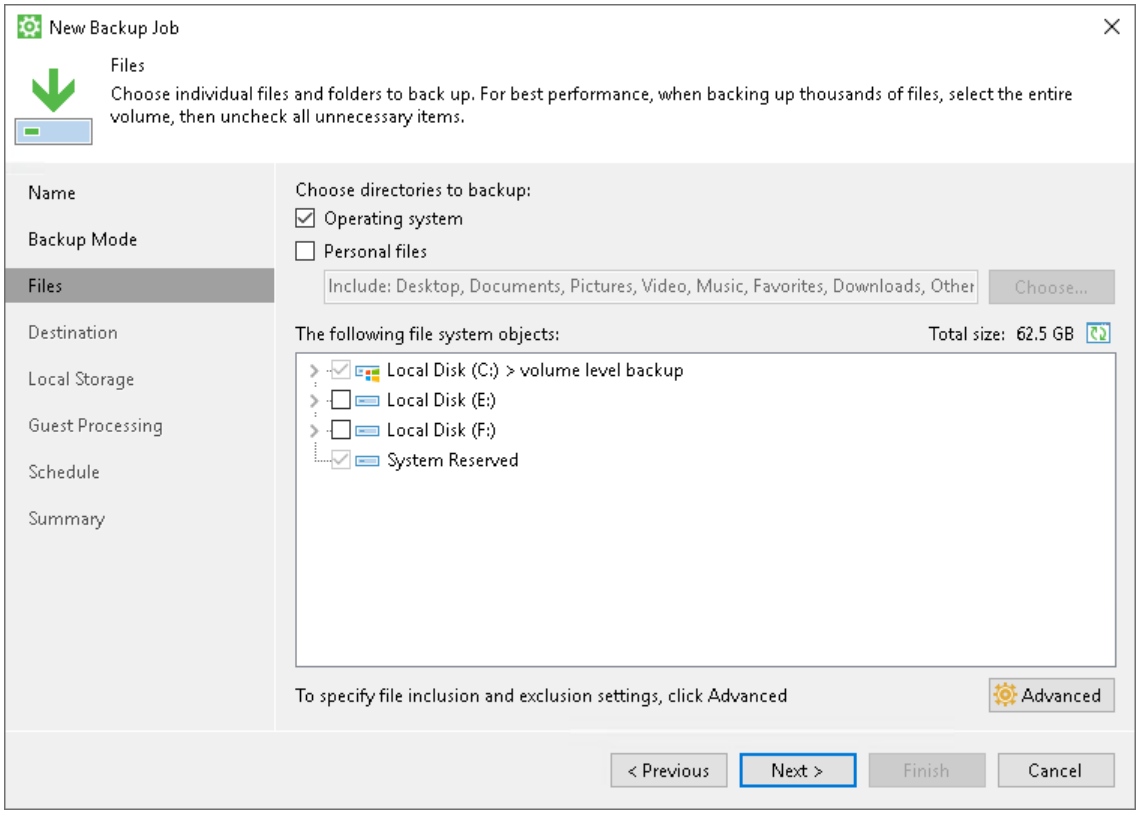


Alternatively, you can explicitly select to back up the system volume. When you select to back up the system volume, Veeam Agent automatically includes existing system partitions in the backup. However, if additional system partitions appear on the Veeam Agent computer, Veeam Agent may be unable to back up such volumes. Thus, we recommend that you use the *Operating system* option to create system state data backup.



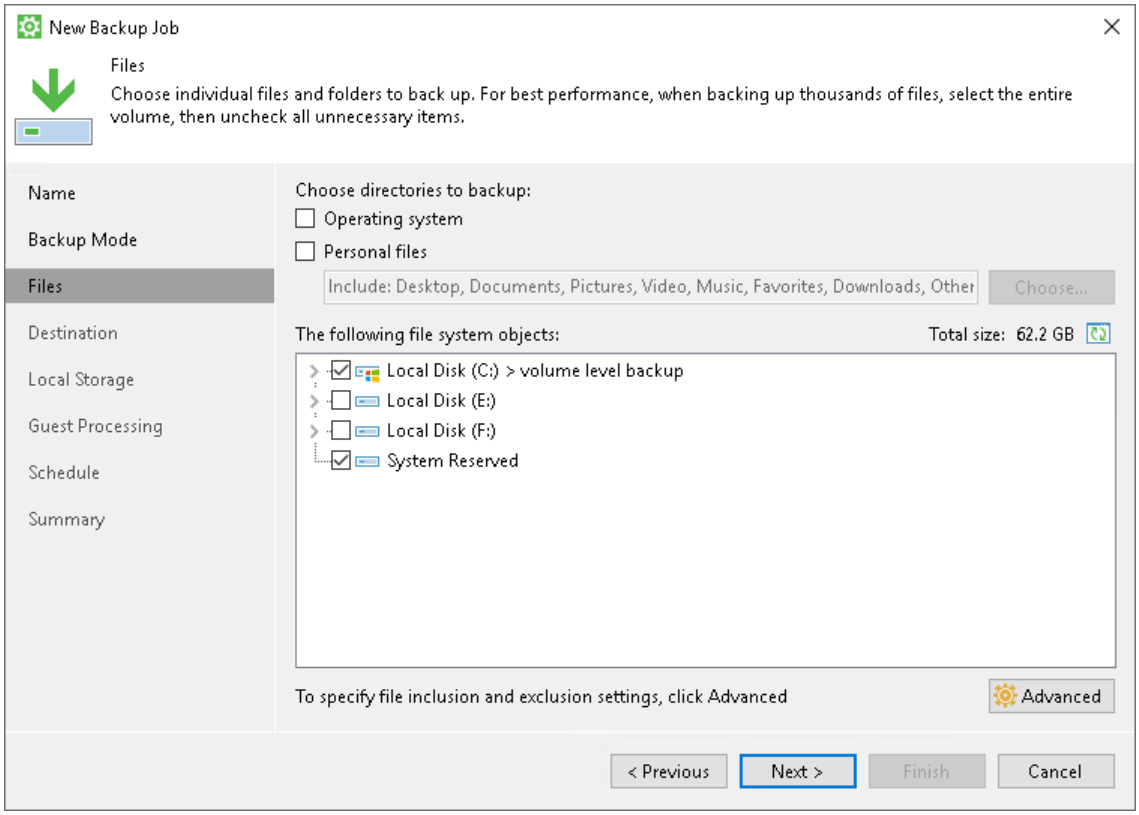
System State Backup in File-Level Backup

To include the operating system data in the file-level backup, select the **Operating system** check box. When you select to back up the operating system data, Veeam Agent automatically includes in the backup all data related to the OS: the system volume and existing system partitions.



Alternatively, you can manually select to back up the system volume and system partitions.

In this case, you will be able to exclude specific folders related to the OS from the backup (for example, the *Users* folder and *Documents* and *Settings* folder). When you select to back up the *Operating system* data, you cannot choose which components related to the OS must be backed up and which must be excluded.

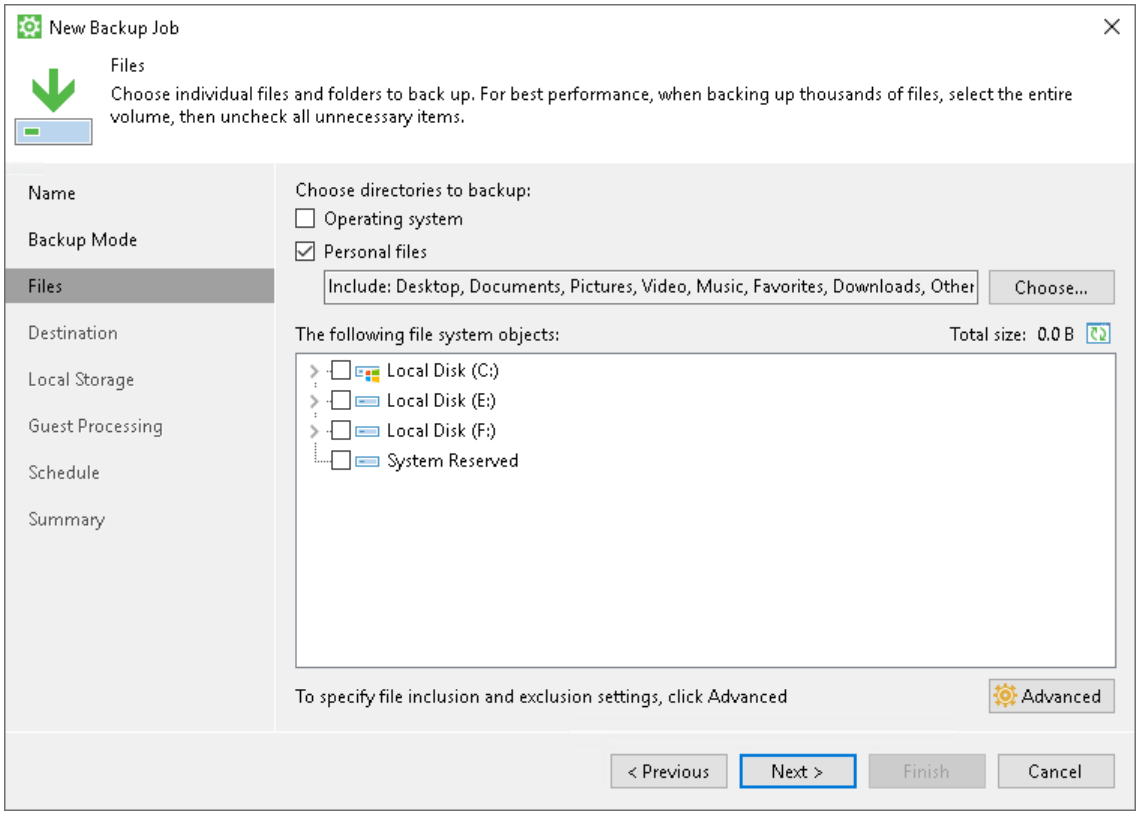


Personal Data Backup

You can include personal data in the backup. In the file-level backup, to simplify this process, Veeam Agent for Microsoft Windows offers you to add the *Personal files* component to the backup scope. When you select to back up the personal data, Veeam Agent automatically includes in the backup data related to Veeam Agent computer user profiles.

Personal Data Backup in File-Level Backup

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

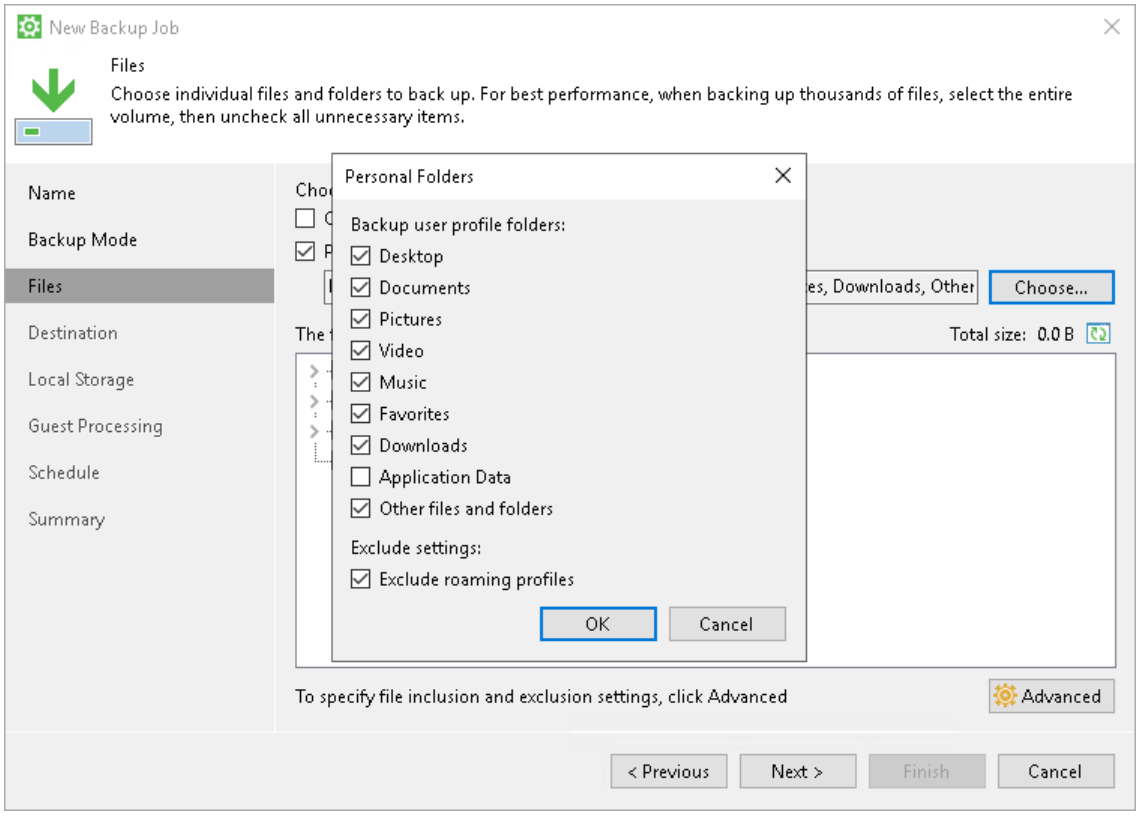


TIP

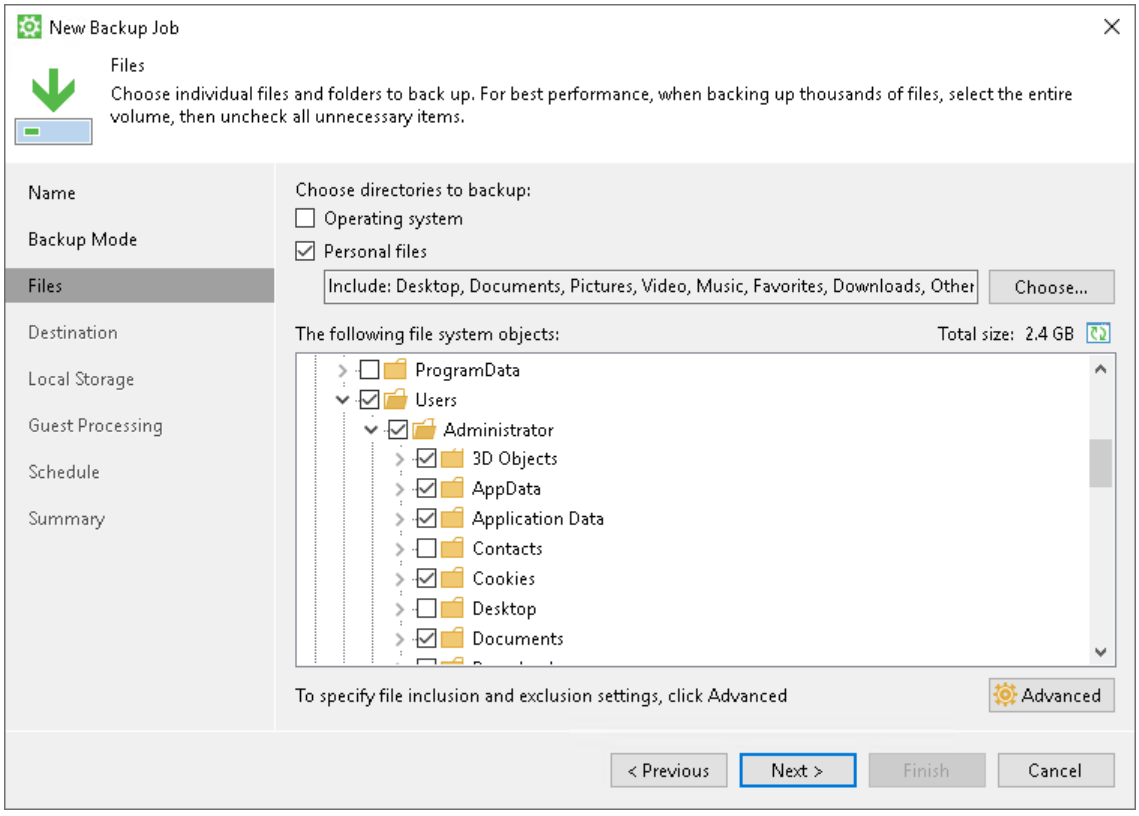
- By default, in the *Personal Folders* window, all options are selected in the **Backup user profile folders** list excluding the **Application Data** option and the **Exclude roaming profiles** option is selected.
- If you want Veeam Agent to back up personal data close to the way personal data was backed up in Veeam Agent 3.0 and 4.0, select all options in the **Backup user profile folders** list and clear the **Exclude roaming profiles** option. Note that in this case, the only difference is that Veeam Agent 6 also backs up selected folders of user profiles that are stored in custom locations.
- If Veeam Agent fails to back up personal data, Veeam Agent displays a warning message in the job session and a warning notification for each folder that Veeam Agent failed to back up. If you do not want to get these warnings, you can disable them with a registry value. To learn more, contact Veeam Customer Support.

You can use the **Other files and folders** 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 **Personal Folders** window. Keep in mind that depending on the **Other files and folders** option, Veeam Agent behaves in one of the following ways:

- If the option is cleared, Veeam Agent backs up only selected personal folders in the *Users* folder on the system volume and personal folders stored in custom locations. Keep in mind, that in such case Veeam Agent backs up only those user profiles that are related to authenticated users. As a result, for example, default and system user profiles will be excluded. Besides that, temporary and corrupted user profiles will be excluded too.
- If the option is selected, Veeam Agent backs up all files and folders in the *Users* folder on the system volume and personal folders stored in custom locations, but excludes personal data according to the options that you cleared.

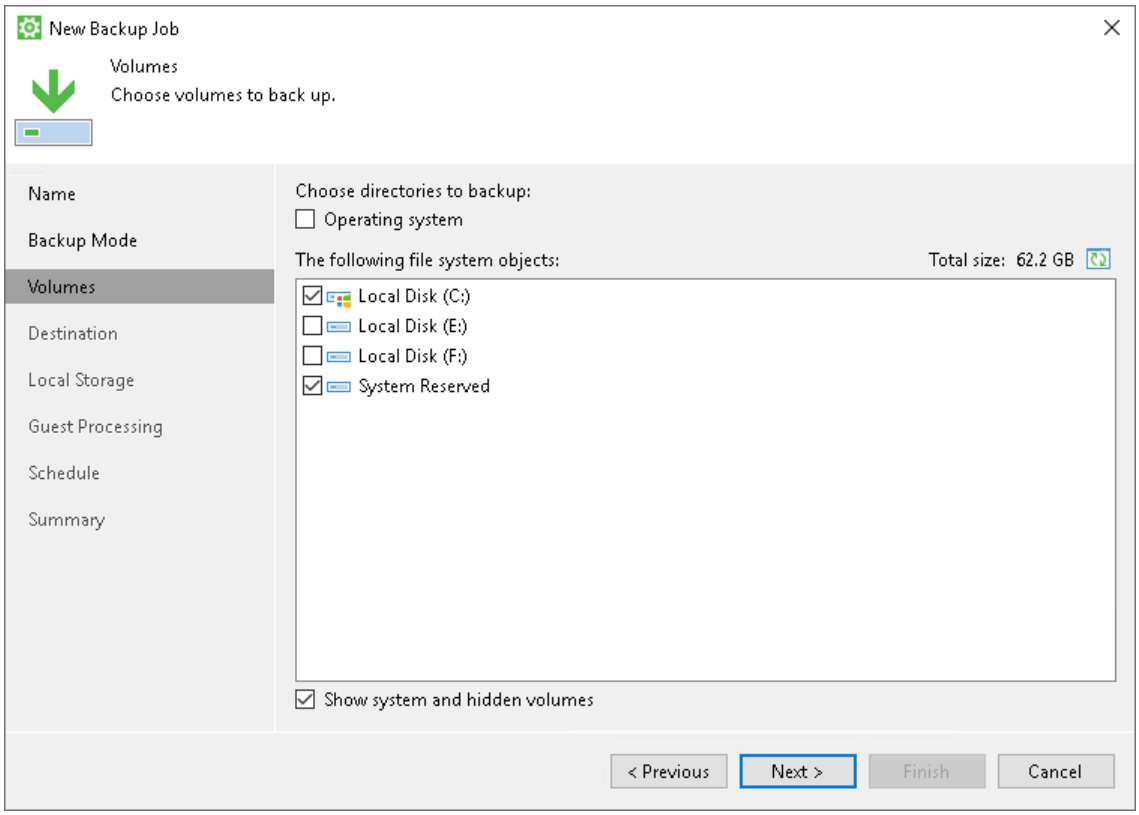


Alternatively, you can explicitly select to back up the *Users* folder. In this case, you still will be able to exclude specific subfolders of the *Users* folder from the backup. But you will need to exclude subfolders for each user manually. You will also need to find user folders stored in custom locations and include subfolders there if necessary. Thus, we recommend that you use the *Personal files* component to create personal data backup.



Personal Data Backup in Volume-Level Backup

Typically, data and settings of the Veeam Agent computer users are located in the Users folder on the system volume, for example, `C:\Users`. Thus, to include the operating system data in the volume-level backup, you must explicitly select to back up the system volume.



How Backup Works

During backup, Veeam Agent for Microsoft Windows performs the following operations:

1. Veeam Agent creates a Microsoft VSS snapshot of the volume whose data you want to back up. The VSS snapshot helps make sure that the data on the volume is consistent and does not change at the moment of backup.
   - In the Free and Workstation product editions, the VSS snapshot type depends on the OS of the Veeam Agent computer. On Microsoft Windows Client OSes, Veeam Agent creates a copy-only VSS snapshot. On Microsoft Windows Server OSes, Veeam Agent creates a full VSS snapshot.
   - In the Server product edition, the VSS snapshot type depends on the specified application-aware processing settings. To learn more, see Application-Aware Processing.

   Veeam Agent does not create a VSS snapshot for the EFI system partition on GPT disks, because its data does not change during backup. For the System Reserved and other system partitions, VSS snapshot can be created if there is enough free disk space on the partition.

   > **NOTE**
   >
   > Condider the following:
   >
   > - By default, Microsoft Windows does not include offline Outlook Data Files (.ost) into a VSS snapshot. As a result, these files are not included into Veeam Agent backups, too.
   > - If the Microsoft VSS technology fails to create a VSS snapshot for some reason, Veeam Agent for Microsoft Windows retries the operation up to 3 times.

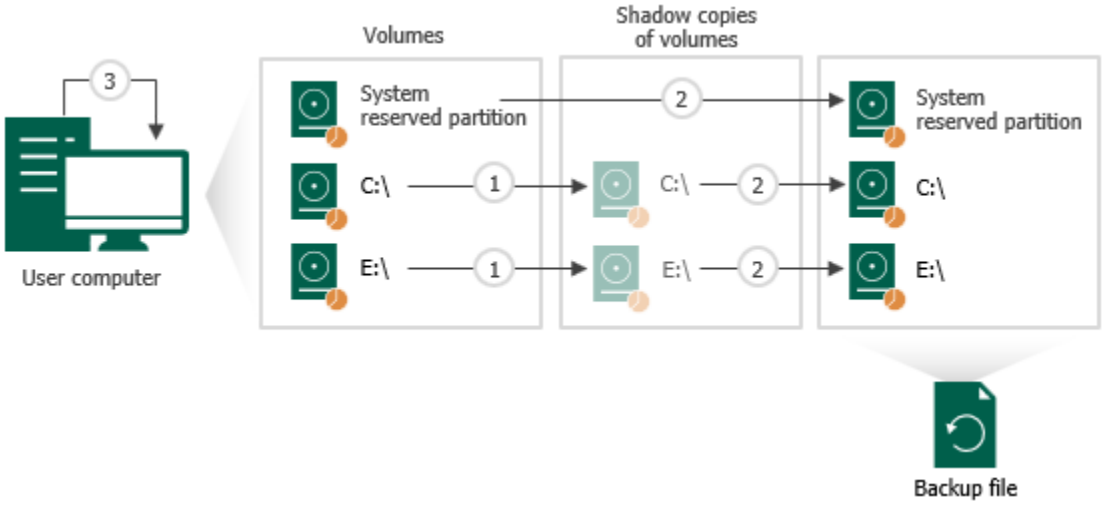
2. Veeam Agent reads data from the created VSS snapshot, compresses it and copies it to the target location.
   - For volume-level backup, Veeam Agent copies data blocks of the whole volume.
   - For file-level backup, Veeam Agent creates a volume inside the backup file in the target location. The content of the volume in the backup file is synchronized with the volume on the source: Veeam Agent for Microsoft Windows copies only those data that you have selected to back up.

   During incremental backup, Veeam Agent uses Changed Block Tracking (CBT) to retrieve only those data blocks that have changed since the previous backup session. To learn more, see Change Block Tracking.

   In the target location, Veeam Agent stores copied data to the backup file.

3. If an application on the computer uses transaction logs to maintain the database consistency, Veeam Agent can truncate transaction logs upon successful backup.
   - In the Free and Workstation product editions, Veeam Agent truncates transaction logs depending on the OS of the Veeam Agent computer. On Microsoft Windows Client OSes, Veeam Agent does not truncate logs. On Microsoft Windows Server OSes, Veeam Agent always truncates logs.
   - In the Server product edition, Veeam Agent truncates logs depending on the specified application-aware processing settings. To learn more, see Application-Aware Processing.

> **IMPORTANT**
>
> The Veeam Agent Service runs under the LocalSystem account. On Microsoft SQL Server 2012, this account does not have necessary permissions to truncate transaction logs. If you want Veeam Agent to automatically truncate transaction logs, you need to manually add the LocalSystem account to a group that has the SQL Server System Administrator rights.


Volumes
Shadow copies of volumes
3
System reserved partition
2
System reserved partition
C:\
1
C:\
2
C:\
E:\
1
E:\
2
E:\
User computer
Backup file

Backup Job

Veeam Agent for Microsoft Windows lets you configure a scheduled backup job that will perform backup automatically in a timely manner. You can set up the backup job once and forget about running the backup operation manually. Veeam Agent for Microsoft Windows will periodically launch the job to back up necessary data on your computer.

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 often you want to back up your data. If necessary, you can re-configure the backup job at any time or remove the job.

Depending on the product edition, you can configure one or more backup jobs in Veeam Agent for Microsoft Windows:

- For the Free product edition, you can configure one backup job only.
- For the Workstation product edition, you can configure an unlimited number of backup jobs targeted at a Veeam Cloud Connect repository plus one backup job targeted at any other supported backup location (local or removable computer drive, network shared folder or Veeam backup repository).
- For the Server product edition, you can configure an unlimited number of backup jobs targeted at any supported backup location.

To learn more about product editions, see Product Editions.

For example, you can configure one backup job to create volume-level backup and another backup job to create file-level backup. Or you can configure backup jobs targeted at different backup locations to keep several copies of your backed-up data. You can also configure multiple backup jobs with individual schedule to fine-tune automatic backup creation process.

Settings of the backup job apply to ad-hoc backups as well: standalone full backups, active full backups and incremental backups.

Backup Job Schedule

Veeam Agent for Microsoft Windows launches the backup job according to the schedule you define. Scheduling options available for the backup job differ depending on the edition of Veeam Agent:

- For the Free and Workstation product editions, you can schedule the job to start at specific time daily or on specific week days. You can also instruct Veeam Agent to automatically perform backup on specific events. To learn more, see Scheduling Options in Free and Workstation Editions.
- For the Server product edition, you can configure daily, monthly and periodic backup job schedule. You can also specify settings for automatic job retries and configure a backup window. To learn more, see Scheduling Options in Server Edition.

If you configure multiple backup jobs in Veeam Agent, you can specify individual schedule for each job. Veeam Agent processes backup jobs sequentially, one after another. If the backup job must start upon schedule at the time when another backup job is already running, the job will wait for the running job to complete, and start afterwards.

For portable devices, Veeam Agent does not start a backup job on the defined schedule if a device is working on battery and the battery level is below 20%.

If a backup job fails, Veeam Agent automatically retries the job. In the Free and Workstation editions, Veeam Agent retries the job every 10 minutes within the next 23 hours. In the Server edition, you can specify retry settings along with other scheduling options. To learn more, see Automatic Job Retries and Job Retry

In any edition, Veeam Agent can wake your computer from sleep at the time when the backup job must start. To learn more, see Computer Wake Up from Sleep.

Scheduling Options in Free and Workstation Editions

You can schedule the backup job to start at specific time daily or on specific week days. You can also instruct Veeam Agent for Microsoft Windows to automatically perform backup on specific events.

Missed Backup Schedule

Veeam Agent for Microsoft Windows does not perform scheduled backups if the computer is powered off. To handle situations of short power outage or computer restart, Veeam Agent provides a tolerance window of 15 minutes for scheduled backups.

For example, you have configured the backup job to run daily at 10:00 PM. At 9:55 PM, there is a power outage that lasts for 10 minutes. When the computer is on again at 10:05, Veeam Agent will automatically launch the scheduled job to back up your data.

Additionally, you can instruct Veeam Agent to resume missed daily backup. If the computer is powered off at the time when the scheduled backup job must start, and you power on the computer later, Veeam Agent will not wait for the next scheduled backup. Instead, Veeam Agent will start the backup job right after the computer is powered on to ensure no necessary data is lost because of the missed backup.

Backup on Specific Events

In addition to the basic job schedule, you can instruct Veeam Agent to launch the backup job on specific events. Veeam Agent lets you trigger backup on the following events:

- Lock — the user locks the computer.
- Log off — the user performs a logout operation on the computer.

- When backup target is connected — the target backup location becomes available: the user attaches a known removable storage device to the computer or a network connection to the backup repository is established.

  You can instruct Veeam Agent to eject the removable storage device after the backup job successfully completes. This helps to protect backup files in the target location from encrypting ransomware, such as CryptoLocker.

Backup on specific event helps you ensure that you capture all changes made within a specific time interval — for example, during a working day. When the necessary event occurs, Veeam Agent automatically launches the scheduled backup job. As a result, you can be sure that all changes made within some period of time are backed up, and you do not lose your data.

If you choose to perform backup on specific events, you can restrict the frequency of backup job sessions. You can instruct Veeam Agent not to start the backup job at specific events more often than once a specified time interval, for example, not more often than every 2 hours. This option does not affect daily schedule. Daily backups are performed according to the defined schedule regardless of the specified time interval.

Backup on specific events helps you fine-tune the backup job schedule. For example, you can specify the following scheduling settings for the backup job:

- The backup job must start automatically at 10:00 PM every day.
- The backup job must start at computer lock.
- The backup job must not run more often than every 2 hours.

Veeam Agent will launch the backup job at the end of the working day, when you lock your computer. In addition, Veeam Agent will perform backup at 10:00 PM regardless of the time interval between the computer lock and scheduled backup.

If you lock your computer later than at 10:00 PM, Veeam Agent will perform backup in the following order. At 10:00 PM, Veeam Agent will launch the backup job upon the daily schedule. If the time interval between the scheduled backup and computer lock is greater than 2 hours, Veeam Agent will additionally perform backup at computer lock. If the time interval between the scheduled backup and computer lock is not greater than 2 hours, Veeam Agent will not perform backup at computer lock.

Automatic Job Retries

Veeam Agent for Microsoft Windows supports automatic retries for the scheduled backup job. If the backup job is started on the defined daily schedule and fails for some reason, Veeam Agent automatically retries the job every 10 minutes within the next 23 hours.

If the backup job fails and Veeam Agent retries the job session, Veeam Agent does not transfer all the data again. Instead, Veeam Agent continues data transfer that was started before the backup job fail. To do so, Veeam Agent compares hash values for data blocks on source and target. After the hash comparison, Veeam Agent transfers only those data blocks that were not transferred before the job fail. If data blocks on source were changed before the automatic retry, Veeam Agent transfers these data blocks as well.

If you edit certain job configuration options before the automatic retry, Veeam Agent may require to transfer all the data to target again. These options include backup scope, data compression, storage optimization, data encryption. Keep in mind that if you back up data to the Veeam backup repository and change data encryption options on the Veeam Backup & Replication side, Veeam Agent transfers all the data to the repository again.

Veeam Agent does not fail the backup job session in case Veeam Agent computer is put into sleep or hibernate mode during the job session, and the backup job is targeted at one of the following locations:

- Local computer drive
- Network shared folder

After the computer is turned on and the connection is restored, Veeam Agent operates in the same way as in case of automatic job retry. Veeam Agent does not transfer all the data again, but continues the job session from the point where it stopped.

Limitations for Automatic Job Retry

- Veeam Agent continues data transfer after the backup job fail only if you configured a job that creates volume-level backups. To learn more about volume-level backups, see Volume-Level Backup.
- Veeam Agent does not perform automatic retry for jobs started manually.
- Veeam Agent does not automatically retry the backup job if the job session is started when the computer is powered on after missed daily backup.
- Veeam Agent retries a job only if the previous job session has failed. Veeam Agent does not perform a retry if a job session has finished with the *Success* or *Warning* status.
- For portable devices, Veeam Agent does not automatically retry the backup job if a device is working on battery and the battery level is below 20%.

Scheduling Options in Server Edition

You can schedule the backup job to start automatically at specific time. Veeam Agent for Microsoft Windows lets you configure the following settings for the job:

- Scheduling settings
- Job retry settings
- Backup window settings

Automatic Startup Schedule

Veeam Agent for Microsoft Windows lets you configure the following scheduling settings for jobs:

- You can schedule the backup job to run at specific time every day or on selected days
- You can schedule the backup job to run periodically at specific time intervals
- You can schedule the backup job to run continuously

Job Started at Specific Time

You can schedule the backup job to start at specific time daily, on specific week days or monthly on selected days.

This type of schedule requires that you define the exact time when the job must be started. For example, you can configure the job to start daily at 10:00 PM or every first Sunday of the month at 12:00 AM.



Job Started at Specific Time Intervals

You can schedule the backup job to start periodically throughout a day at a specific time interval. The time interval between job sessions can be defined in minutes or hours. For example, you can configure a job to start every 30 minutes or every 2 hours.

For periodically run jobs, reference time is midnight (12:00 AM). Veeam Agent for Microsoft Windows always starts counting defined intervals from 12:00 AM, and the first job session will start at 12:00 AM. For example, if you configure a job to run with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.



If necessary, you can specify an offset for periodically run jobs. The offset is an exact time within an hour when the job must start. For example, you can configure the job to start with a 4-hour interval and specify offset equal to 15 minutes. In this case, the job will start at 12.15 AM, 4:15 AM, 8:15 AM, 12:15 PM, 4:15 PM and so on.

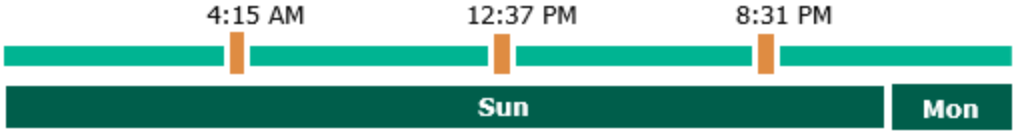


If a session of the periodically run job does not fit into the specified time interval and overlaps the next planned job session, Veeam Agent for Microsoft Windows starts the next backup job session at the nearest scheduled interval. For example, you set up the job to run with a 4-hour interval. The first job session starts at 12:00 AM, takes 5 hours and completes at 5:00 AM. In this case, Veeam Agent for Microsoft Windows will start a new job session at 8:00 AM.



Job Run Continuously

You can schedule the job to run continuously — that is, in a non-stop manner. A new session of the continuously running job starts as soon as the previous job session completes. Continuously run job can help you implement near-continuous data protection (near-CDP) for the most critical applications.



Job Retry

You can instruct Veeam Agent for Microsoft Windows to retry the backup job several times if the initial job session fails. By default, Veeam Agent for Microsoft Windows automatically retries a failed job for 3 times within one job session. If necessary, however, you can define a custom number of retries in the job settings.

If a backup job fails and Veeam Agent retries the job session, Veeam Agent does not transfer all the data again. Instead, Veeam Agent continues data transfer that was started before the backup job fail. To do so, Veeam Agent compares hash values for data blocks on source and target. After the hash comparison, Veeam Agent also transfers only those data blocks that were not transferred before the job fail. If data blocks on source were changed before the retry, Veeam Agent transfers these data blocks as well.

If you edit certain job configuration options before the retry, Veeam Agent may require to transfer all the data to target again. These options include backup scope, data compression, storage optimization, data encryption. Keep in mind that if you back up data to the Veeam backup repository and change data encryption options on the Veeam Backup & Replication side, Veeam Agent transfers all the data to the repository again.

Veeam Agent does not fail the backup job session in case Veeam Agent computer is put into sleep or hibernate mode during the job session, and the backup job is targeted at one of the following locations:

- Local computer drive
- Network shared folder

After the computer is turned on and the connection is restored, Veeam Agent operates in the same way as in case of job retry. Veeam Agent does not transfer all the data again, but continues the job session from the point where it stopped.

Limitations for Job Retry

- Veeam Agent continues data transfer after the backup job fail only if you configured a job that creates volume-level backups. To learn more about volume-level backups, see Volume-Level Backup.
- Veeam Agent does not perform retry for jobs started manually.
- Veeam Agent does not retry the backup job if the job session is started when the computer is powered on after missed daily backup.
- Veeam Agent retries a job only if the previous job session has failed. Veeam Agent does not perform a retry if a job session has finished with the *Success* or *Warning* status.
- For portable devices, Veeam Agent does not retry the backup job if a device is working on battery and the battery level is below 20%.

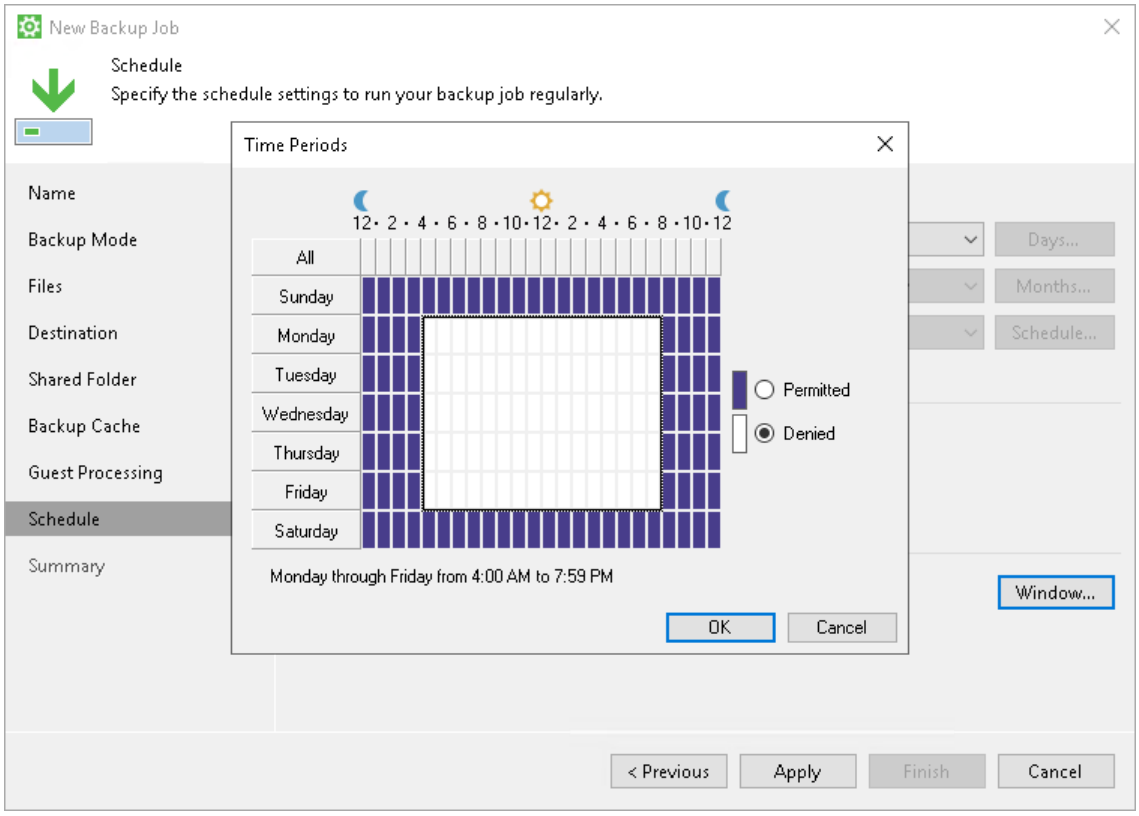
Backup Window

If necessary, you can specify a backup window for the backup job. The backup window is a period of time on week days when the job is permitted to run.

The backup window can be helpful if you do not want the data protection job to produce unwanted overhead for the production environment or do not want the job to overlap production hours. In this case, you can define the time interval during which the job must not run.

If the job exceeds the allowed window, it will be automatically terminated. In this case, data transport and backup chain transformation processes are stopped.

> **IMPORTANT**
>
> The backup window does not affect the process of uploading backup files from the backup cache to the target storage. If Veeam Agent creates one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent uploads backup files to the target location immediately, regardless of the specified backup window.

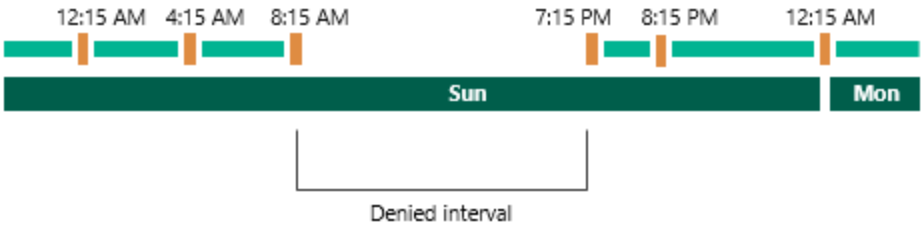


Backup Window for Periodically Run Job

If you define the backup window for the job that runs periodically at specific time intervals, Veeam Agent will immediately start the job after the denied window is over. All subsequent backup job sessions will be performed according to specified scheduling settings.

For example, you have configured the job to run with a 4-hour interval with an offset of 15 minutes. The allowed backup window for the job is 7:00 PM to 8:00 AM. Veeam Agent will run this job in the following way:

1. The first job session will start at 12:15 AM (since midnight is a reference time for periodically run jobs).
2. The next job session will start at 4:15 AM.
3. The job session at 8:15 AM will not be performed, because it falls into the denied period of the backup window.
4. The next job session will start immediately after the denied period is over: at 7:15 PM.
5. After that, Veeam Agent for Microsoft Windows will run the job by the defined schedule: at 8:15 PM, 12:15 AM and so on.



Computer Wake Up from Sleep

If your computer is in the standby mode at the time when the backup job must start, Veeam Agent for Microsoft Windows automatically wakes your computer from sleep. The wake-up feature lets you schedule your backup at night. At the defined time, Veeam Agent for Microsoft Windows will wake up the computer and perform a scheduled task. If necessary, you can additionally instruct Veeam Agent for Microsoft Windows to bring the computer back to the standby mode or power off the computer after the backup is finished.

Veeam Agent for Microsoft Windows wakes up the computer by default, unless the power saving settings on the computer prohibit this. If the wake up operation is not possible for some reason, the computer will remain in the standby mode, and the backup operation will not be performed. You can instruct Veeam Agent for Microsoft Windows to resume missed backup in such situations. To learn more, see Missed Backup Schedule.

> **IMPORTANT**
>
> [For tablets running Microsoft Windows 8.1 or later] If at the moment of backup a computer is in the Connected Standby power saving mode, Veeam Agent for Microsoft Windows will fail to wake it up due to limitations set by the OS itself.

Ad-Hoc Backup

You can create ad-hoc backups of your data when you need.

Ad-hoc backups let you capture your data at a specific point in time. You can create ad-hoc backups before you perform some alterations on your computer: install new software or enable a new feature. Ad-hoc backups help you protect your computer from potential data corruption or data loss that can be caused by these operations. If an error occurs, you can always restore data from the ad-hoc backup and bring your computer system to a state before the alteration was made.

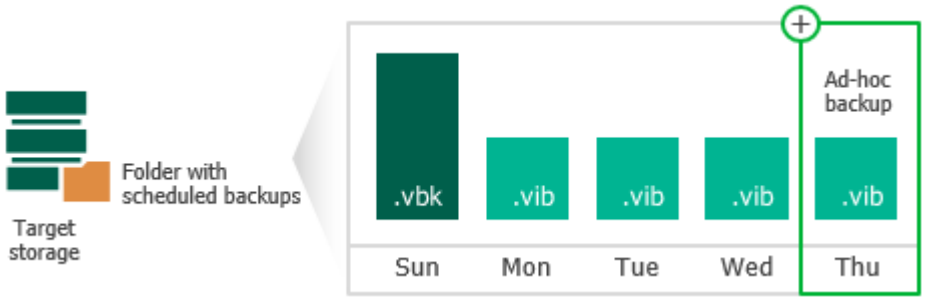
Veeam Agent for Microsoft Windows lets you create the following types of ad-hoc backups:

- Incremental backup
- Standalone full backup

Ad-Hoc Incremental Backup

If you want to create a new backup of your data in addition to backups created with the scheduled backup job, you can perform ad-hoc incremental backup. Ad-hoc incremental backup adds a new restore point to the backup chain. For example, you may want to back up your data before you install new software on your computer or enable a new feature.

For ad-hoc incremental backup, Veeam Agent for Microsoft Windows uses settings specified for the backup job. For example, if you have configured the backup job to perform backup of a specific volume, the ad-hoc incremental backup operation will create an incremental backup of this volume and save it in the target location, next to existing backup files in the backup chain.



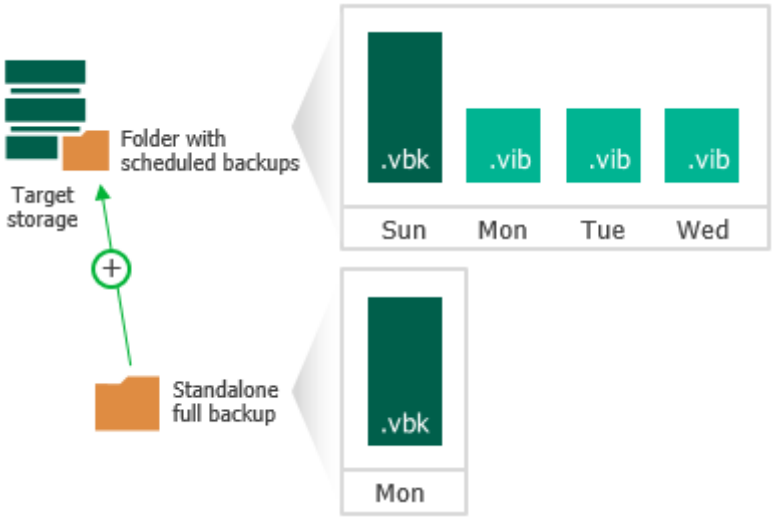
Unlike the backup job started upon schedule, the ad-hoc incremental backup task is not retried automatically. If the task fails for some reason, you will have to start it manually again.

Veeam Agent for Microsoft Windows treats restore points created by ad-hoc incremental backup as regular restore points, and applies to them retention policy settings specified for the backup job. To learn more, see Backup Retention Policy.

Standalone Full Backup

Sometimes you need to create a full backup of your data. For example, you may want to save a copy of your data on a CD or DVD or create a full backup of all data on your computer at some point in time. In these situations, you can perform standalone full backup.

When Veeam Agent for Microsoft Windows performs standalone full backup, it produces a full backup of your data in a separate folder in the target location. The standalone full backup is not associated with subsequent incremental backups. You can use it as an independent restore point for data recovery.



To create a standalone full backup, Veeam Agent for Microsoft Windows uses settings specified for the backup job. For example, if you have configured the backup job to perform backup of a specific volume, the standalone full backup will create a full backup of this volume in a separate folder in the target location.

Unlike the backup job started upon schedule, the standalone full backup task is not retried automatically. If standalone full backup fails for some reason, you will have to start the standalone full backup task manually again.

The standalone full backup is not removed by retention. To remove it, you must manually delete the full backup file from disk.

> **NOTE**
>
> You cannot perform standalone full backup if the backup job is targeted at one of the following locations:
>
> - Veeam backup repository
> - Veeam Cloud Connect repository
> - Object storage

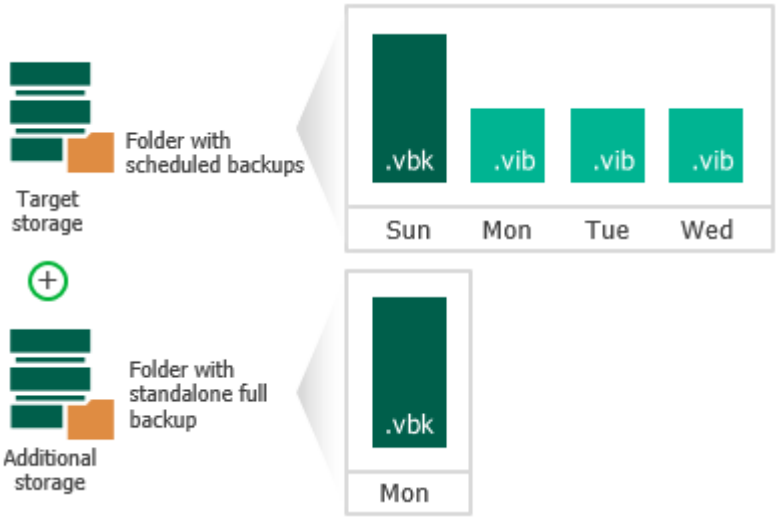
Standalone Full Backup to Another Location

You can create a standalone full backup in a separate location that is not specified as a target location in the backup job settings. For example, you may want to save a copy of your data on a removable storage device while your scheduled backup job is targeted at the network shared folder.

Backup to another location practically does not differ from regular standalone full backup. The only difference is that you must manually select a target location in which Veeam Agent for Microsoft Windows will save the backup file. You can save backup files to the following locations:

- Removable storage device
- Local computer drive
- Network shared folder

You cannot use a Veeam backup repository or Veeam Cloud Connect repository as a target for backup to another location.


Folder with scheduled backups
Target storage
.vbk
.vib
.vib
.vib
Sun
Mon
Tue
Wed
Folder with standalone full backup
Additional storage
.vbk
Mon

Parallel Disk Processing

Veeam Agent for Microsoft Windows supports parallel disk processing. If you included several disks of the Veeam Agent computer in the backup scope, Veeam Agent will process disks simultaneously.

How Parallel Disk Processing Works

During backup, Veeam Agent for Microsoft Windows creates a Microsoft VSS snapshot of the volume whose data you want to back up as described in section How Backup Works. After the VSS snapshot is created, Veeam Agent transfers data blocks of disks to the target storage simultaneously.

The number of disks that are simultaneously processed by Veeam Agent is limited by repository settings on the Veeam Backup & Replication side. During the backup job session, Veeam Backup & Replication compares the number of currently processed disks to the limit specified in the properties of the backup repository. If the number of currently processed disks is greater than the limit, Veeam Agent will not transfer data of a new disk. Only after data transfer for at least one of the disks completes, Veeam Agent starts data transfer for the next disk. To learn more, see the Limitation of Concurrent Tasks section in the Veeam Backup & Replication User Guide.

You can also limit the number of disks that are processed simultaneously with a registry value. Keep in mind that if the number of simultaneously processed disks is limited by both repository settings and registry value, Veeam Agent uses the lower limit. To learn more about the registry value, see this Veeam KB article.

If processing of at least one disk fails, the entire backup job session completes with an error.

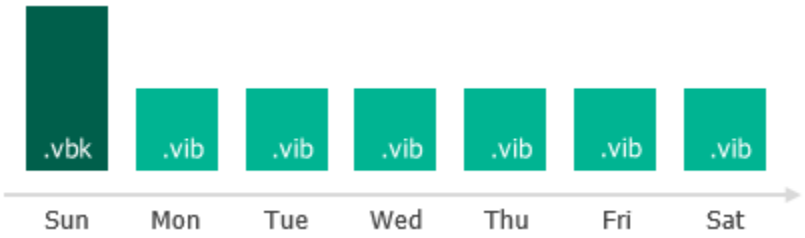
Limitations for Parallel Disk Processing

- Parallel disk processing is available only in the Server edition of Veeam Agent for Microsoft Windows.
- Veeam Agent offers parallel disk processing for backups that are created in the following types of target locations:
    - Veeam backup repository
    - Veeam Cloud Connect repository
- Parallel disk processing is not supported for dynamic disks.
- Parallel disk processing is not performed for file-level backups.

Backup Chain

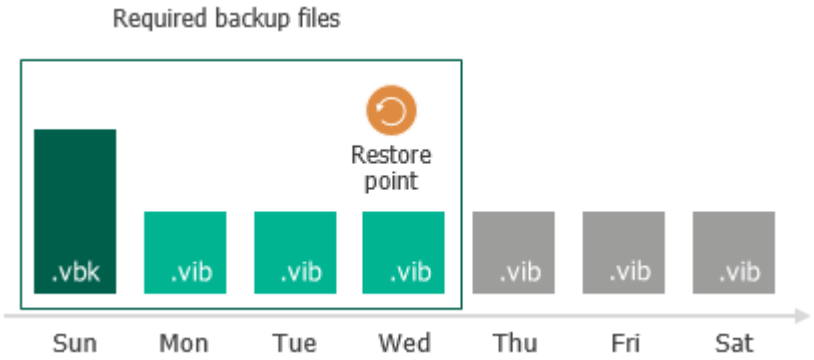
Every backup job session produces a new backup file in the target location. Backup files make up a backup chain. The backup chain can contain files of two types: full backups and incremental backups.

- During the first backup job session, Veeam Agent performs full backup. Veeam Agent 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.



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.

> **NOTE**
>
> For backup jobs with database log backup options enabled, Veeam Agent for Microsoft Windows additionally produces backup files of the following types:
>
> - VLB, VSM and VLM files — for Microsoft SQL Server transaction log backups
> - VLB, VOM and VLM files — for Oracle archived log backups
>
> Keep in mind that Veeam Agent creates VLM files only in backup chains started in Veeam Agent for Microsoft Windows 5.0 and later. If you upgrade Veeam Agent and continue the backup chain that was started in the earlier Veeam Agent version, Veeam Agent will not create VLM files in this backup chain.

Short-Term Retention Policy

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

Short-term retention policy depends on the edition of Veeam Agent for Microsoft Windows:

- In the Free and Workstation editions, Veeam Agent retains restore points for a certain number of days. To learn more, see Retention Policy in Free and Workstation Editions.
- In the Server edition, you can select the logic behind the short-term retention policy. Veeam Agent can retain restore points for a certain number of days or retains a certain number of latest restore points that is defined by the user. To learn more, see Retention Policy in Server Edition.

You can also specify the retention policy for outdated backups — backups for which Veeam Agent does not create new restore points within a specified time period. To learn more, see Retention Policy for Outdated Backups.

Retention Policy in Free and Workstation Editions

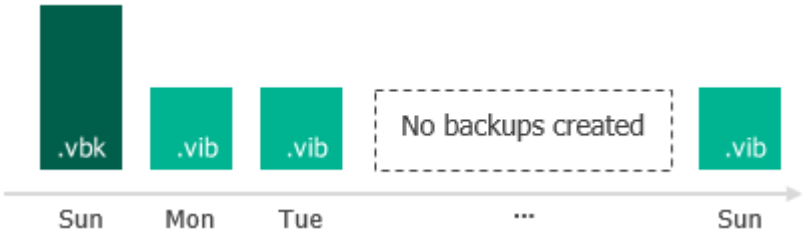
In the Free and Workstation editions, Veeam Agent for Microsoft Windows retains restore points for the last N days; the number of days is defined by the user. During every backup job session, Veeam Agent for Microsoft Windows checks if there is any obsolete restore point in the backup chain. If some restore point is obsolete, it is removed from the chain.

For retention policy settings, Veeam Agent for Microsoft Windows takes into account not calendar days but days on which backup files were successfully created.

For example, you have configured the backup job in the following way:

- The backup job runs daily.
- The retention policy is set to 5 days.

The backup job has successfully run 3 times and created 3 restore points in the backup chain. After that, you have turned off your computer for 10 days. When you turn on your computer, Veeam Agent for Microsoft Windows runs a backup job by schedule and creates a new restore point. The earliest restore point, however, is not removed from the backup chain. At the end of a new backup job session, the backup chain will have only 4 restore points created during 4 days when the backup job was successfully run.



Removing Backups by Retention

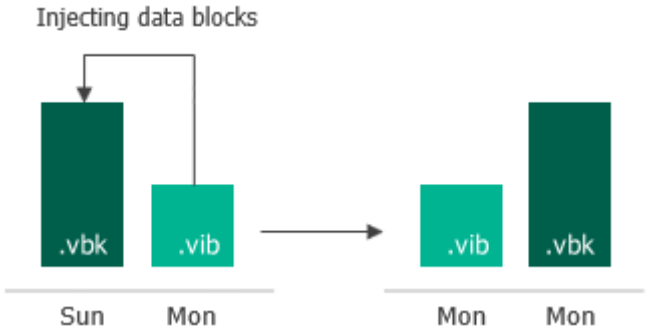
When removing obsolete restore points, Veeam Agent does not just delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of the backup chain, Veeam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

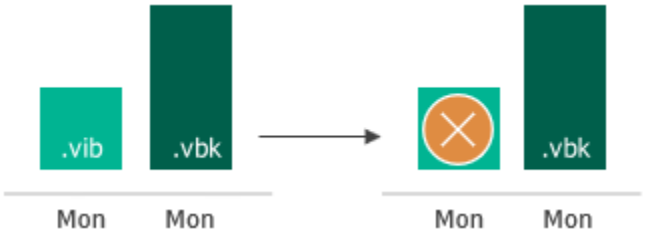


2. If an obsolete restore point exists, Veeam Agent transforms the backup chain. As part of this process, it performs the following operations:

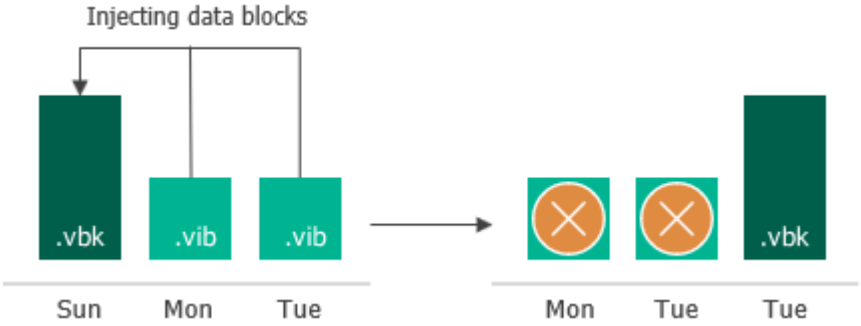
   a. Veeam Agent re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Agent injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup 'moves' forward in 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.



If the backup chain contains several obsolete restore points, the rebuild procedure is similar. Data from several restore points is injected to the re-built full backup file. This way, Veeam Agent makes sure that the backup chain is not broken, and you will be able to recover your data to any restore point.



Retention Policy in Server Edition

In the Server edition, you can select the logic behind the short-term retention policy. Veeam Agent offers the following options:

- Veeam Agent retains restore points for the last N days; the number of days is defined by the user. In this case, Veeam Agent works in a similar way as in the Free or Workstation editions. To learn more, see Retention Policy in Free and Workstation Editions.
- Veeam Agent retains the number of latest restore points defined by the user.

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

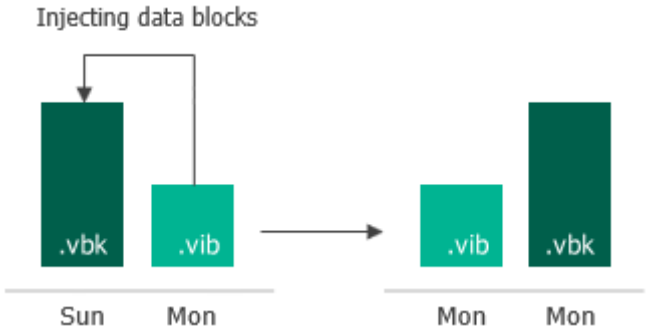
When removing obsolete restore points, Veeam Agent does not just delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of the backup chain, Veeam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

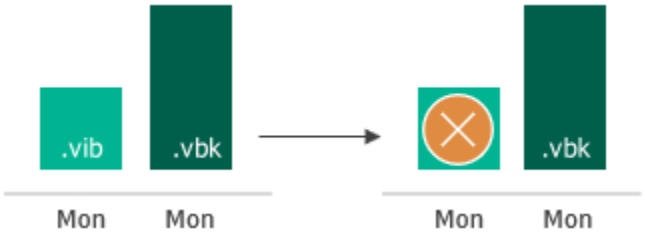


2. If an obsolete restore point exists, Veeam Agent transforms the backup chain. As part of this process, it performs the following operations:

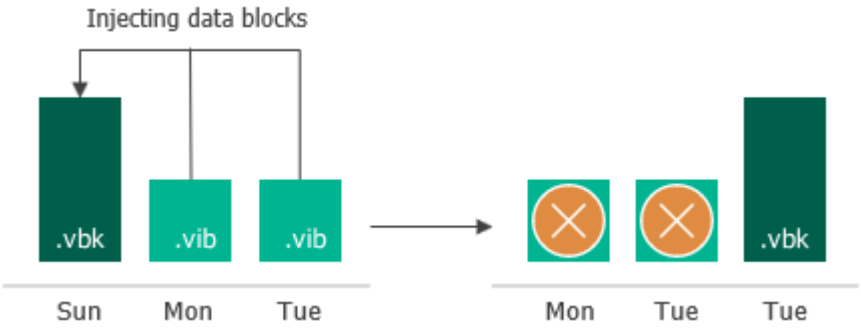
   a. Veeam Agent re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Agent injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup 'moves' forward in 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.



   If the backup chain contains several obsolete restore points, the rebuild procedure is similar. Data from several restore points is injected to the re-built full backup file. This way, Veeam Agent makes sure that the backup chain is not broken, and you will be able to recover your data to any restore point.



Retention Policy for Outdated Backups

In addition to specifying general retention policy settings, you can define retention policy for outdated backups. An outdated backup is a backup for which no new restore points were created within the last N days. Retention policy for outdated backups helps to avoid keeping redundant data in the target location: once the outdated backup retention period is over, an outdated backup is automatically removed from the target location.

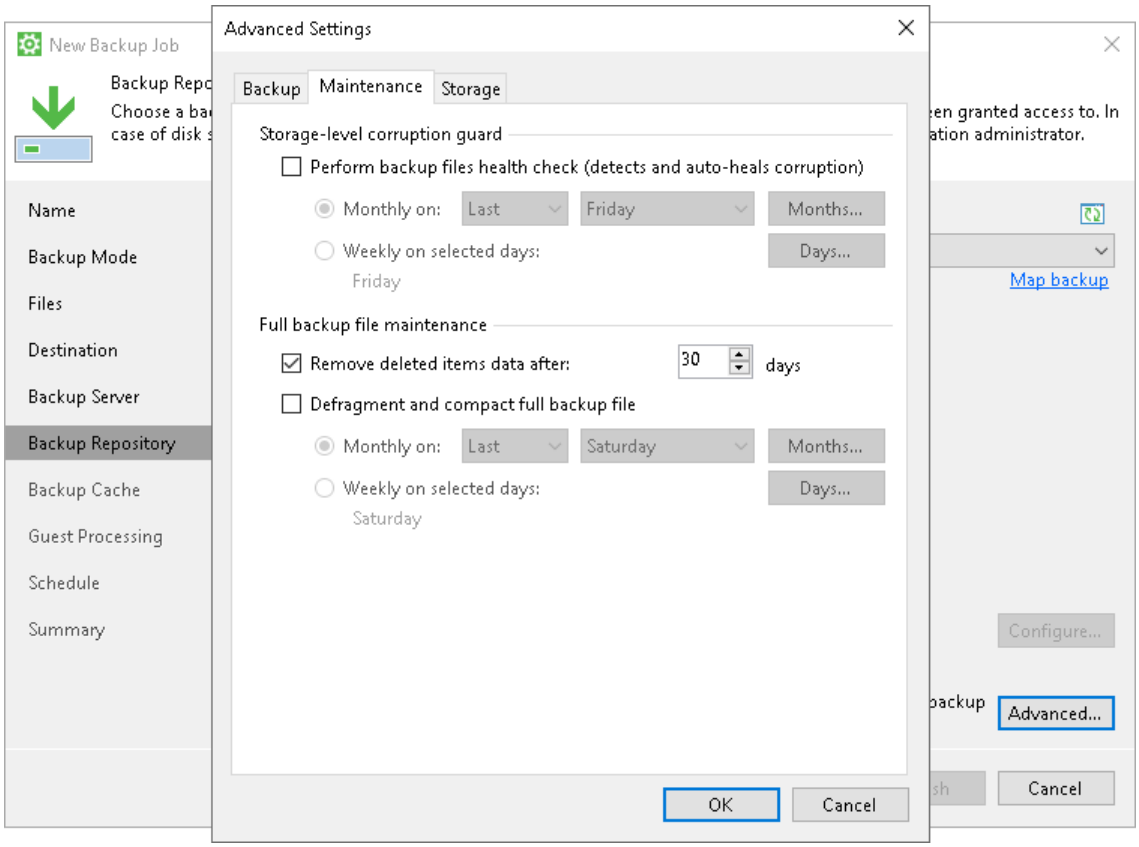
Veeam Agent for Microsoft Windows offers retention policy for outdated backups that are created in the following types of target locations:

- Veeam backup repository
- Veeam Cloud Connect repository

To specify retention policy for outdated backups, you must enable the **Remove deleted items data after <N> days** option in backup job settings and specify the number of days for which data of outdated backups must be retained in the backup repository. By default, Veeam Agent for Microsoft Windows retains outdated backups for 30 days. You can change the number of days to retain outdated backups if necessary.

Consider the following:

- You must use retention policy for outdated backups wisely. We strongly recommend that you set retention policy for outdated backups to 7 days or more to prevent unwanted data loss.
- The **Remove deleted items after <N> days** option lets you control data of backups for which Veeam Agent for Microsoft Windows does not produce new restore points for some time. In addition to it, Veeam Agent for Microsoft Windows applies general retention policy rules to maintain the necessary number of restore points in the backup chain. To learn more, see Backup Retention Policy.



How Retention Policy for Outdated Backups Works

Although you specify retention policy settings for outdated backups in Veeam Agent for Microsoft Windows, actions required to track and delete outdated Veeam Agent backups are taken on the Veeam Backup & Replication side.

To perform necessary actions, Veeam Backup & Replication uses the Veeam Agent backup retention job that runs on the backup server. The Veeam Agent backup retention job runs upon schedule, at 12:30 AM daily.

> **NOTE**
>
> You can change the schedule for the Veeam Agent backup retention job with registry values. For more information, contact Veeam Customer Support.

During the Veeam Agent backup retention job session, Veeam Backup & Replication performs the following operations:

1. Veeam Backup & Replication checks the configuration database to detect Veeam Agent backups that reside in the backup repository.
2. For each Veeam Agent backup, Veeam Backup & Replication checks whether the following conditions are met:
   a. The configuration database contains information about the backup job that created the Veeam Agent backup.

      The configuration database does not contain information about the backup job that created the backup in the following cases:

      - The backup job that created the backup was removed in Veeam Agent for Microsoft Windows.
      - The Veeam Agent backup was imported in the Veeam Backup & Replication console.
      - The Veeam Agent backup is a standalone full backup.

      If the configuration database does not contain information about the backup job that created the backup, Veeam Backup & Replication does not remove such a backup from the backup repository.

   b. The **Remove deleted items after <N> days** option is enabled in the backup job settings. If the option is enabled, Veeam Backup & Replication checks whether the following conditions are met:

      - No new restore points were created by the backup job for the last N days.
      - No new backup job sessions were detected by Veeam Backup & Replication for the last N days.
      - [For backup jobs with database log backup enabled] No database log copies (Microsoft SQL Server transaction log or Oracle archive log copies) were created by the database log backup job for the last N days.

        Where N is the number of days specified for the **Remove deleted items data after <N> days** option.
3. If all the conditions listed in the step 2 are met, Veeam Backup & Replication removes the Veeam Agent backup from the configuration database and deletes actual backup files from the backup repository.

Long-Term Retention Policy (GFS)

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 .

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 object storage, and you do not configure Veeam Agent to perform active full backups periodically, 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:

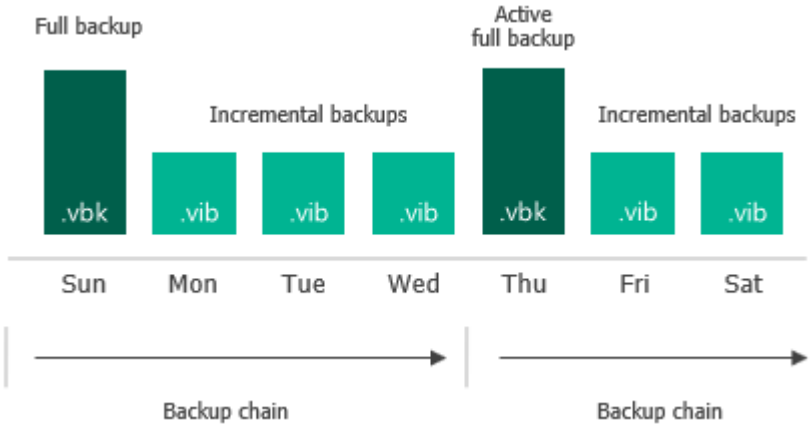
- [Applicable to all backup targets except object storage] While applying the GFS retention policy, Veeam Agent does not create new full backup files. You must configure your backup jobs in a way you do not lose any essential data due to an insufficient number of full backup files. For example, if you 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.

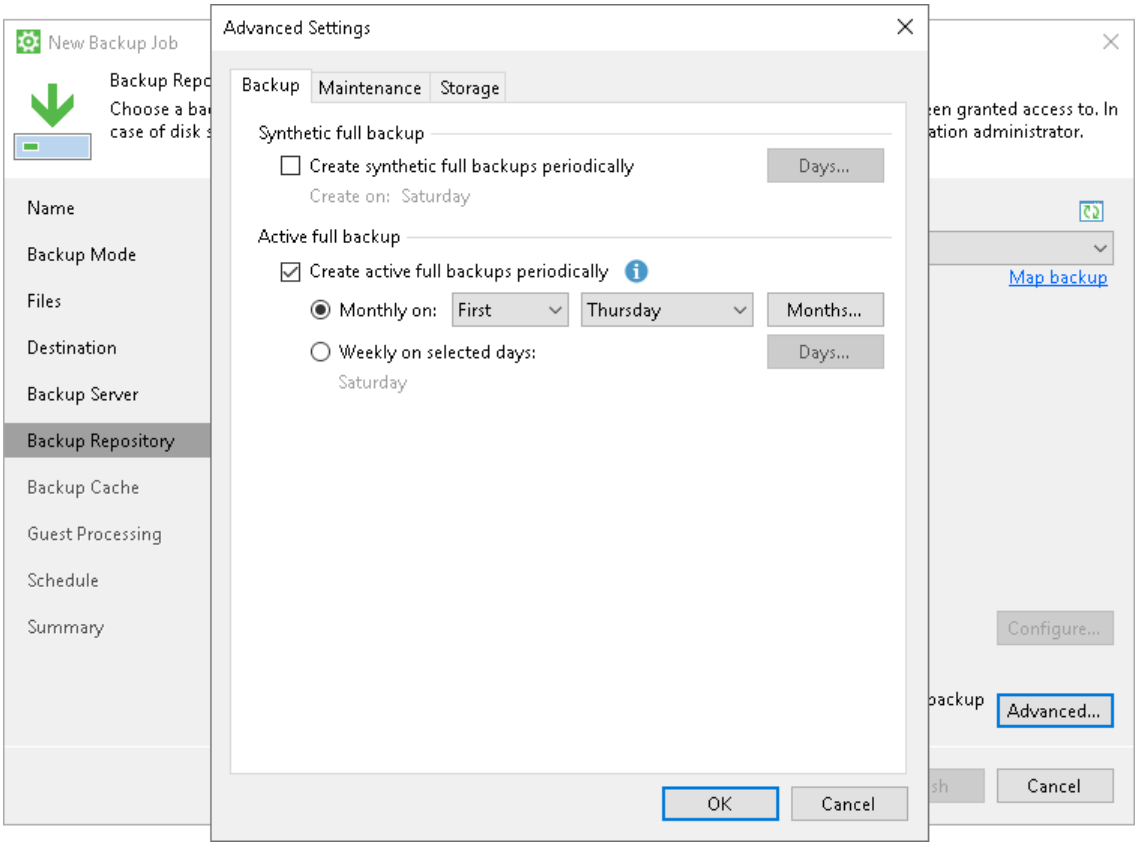
When Veeam Agent performs active full backup, it produces a full backup file and adds this file to the backup chain.

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 create an active full backup manually, use the **Active full backup** command from the Veeam Agent Tray menu. To learn more, see Creating Active Full Backups.
- To schedule active full backups, specify scheduling settings in the **Advanced Settings** window of the **New Backup Job** wizard. You can schedule active full backups to run weekly, for example, every Saturday, or monthly, for example, every first Thursday of a month.

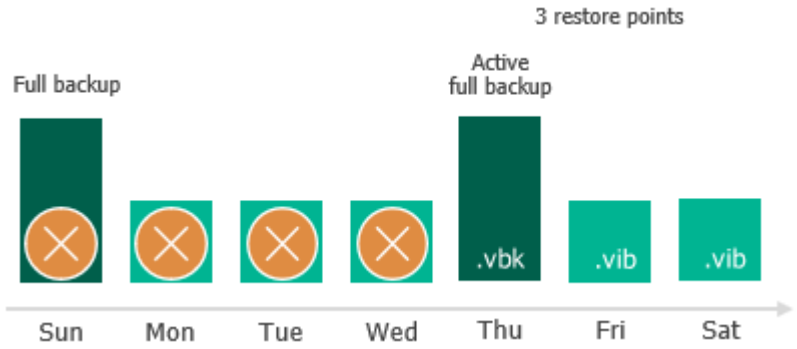


Retention Job for Active Full Backups

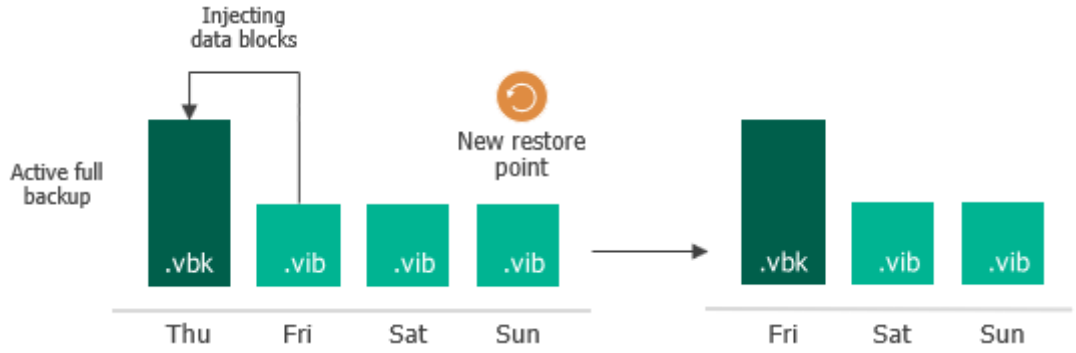
To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental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



Synthetic Full Backup

In some situations, running active full backups periodically may not be an option. Active full backups are resource-intensive and consume considerable amount of network bandwidth. As an alternative, you can create synthetic full backups.

> **NOTE**
>
> Consider the following:
>
> - Synthetic full backup is available only in the Workstation and Server editions of Veeam Agent for Microsoft Windows.
> - Synthetic full backup is not available for backup jobs targeted at object storage.

In terms of data, the synthetic full backup is identical to a regular full backup. Synthetic full backup produces a VBK file that contains all data that you have chosen to back up. The difference between active and synthetic full backup lies in the way how backed-up data is retrieved:

- When you perform active full backup, Veeam Agent for Microsoft Windows reads backed-up data, compresses it and copies it to the target location.
- When you perform synthetic full backup, Veeam Agent for Microsoft Windows does not retrieve all backed-up data from the Veeam Agent computer. Instead, it creates a new incremental backup and then synthesizes a full backup from data you already have on the target location. Veeam Agent for Microsoft Windows accesses the previous full backup file and a chain of subsequent incremental backup files in the backup chain including a new incremental backup, consolidates data from these files and writes consolidated data into a new full backup file. As a result, the created synthetic full backup file contains the same data as an active full backup.

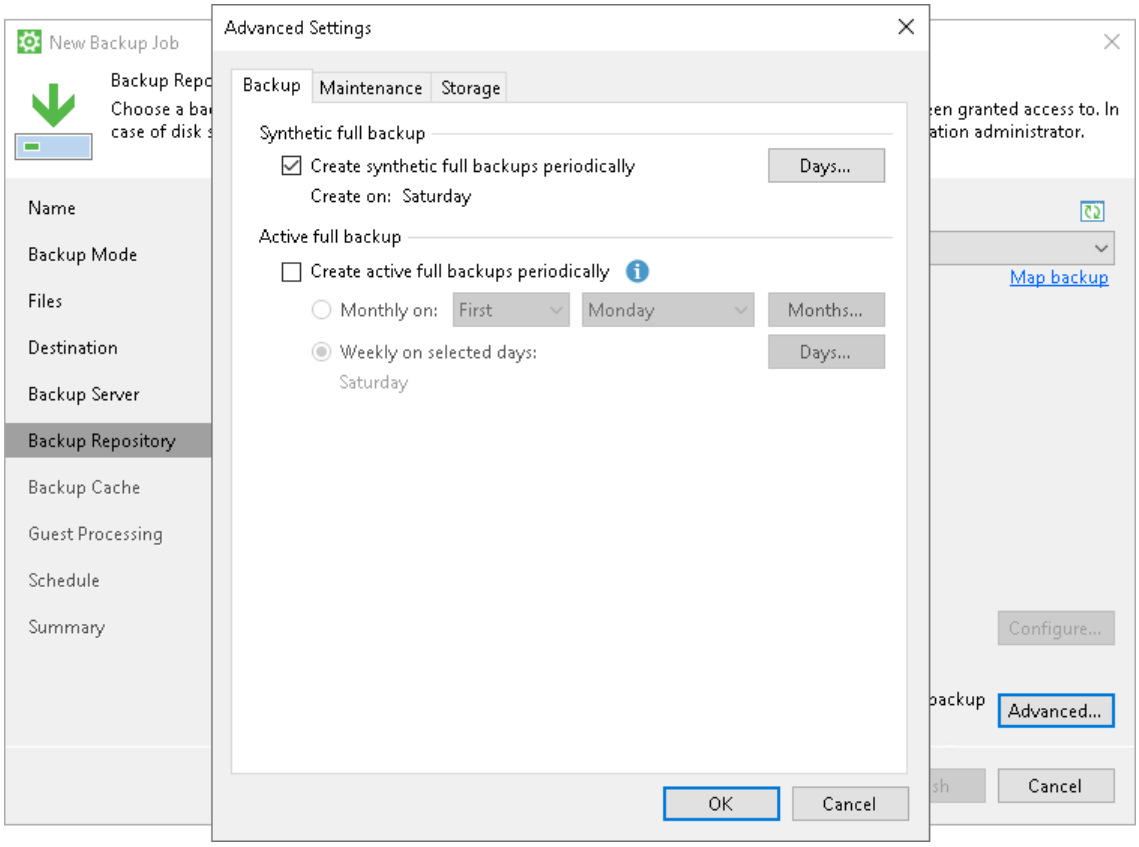
The synthetic full backup has a number of advantages:

- The synthetic full backup does not use network resources: it is created from backup files you already have on the target location.
- The synthetic full backup produces less load on the production environment: it is synthesized right on the target location.

Veeam Agent for Microsoft Windows treats synthetic full backups as regular full backups. As well as any other full backup file, the synthetic full backup file resets the backup chain. All subsequent incremental backup files use the synthetic 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 synthetic full backup becomes outdated, Veeam Agent for Microsoft Windows automatically deletes the previous backup chain. To learn more, see Retention Policy for Synthetic Full Backups.

To create synthetic full backups, you must enable the **Create synthetic full backups periodically** option and schedule creation of synthetic full backups on specific days in the backup job settings.

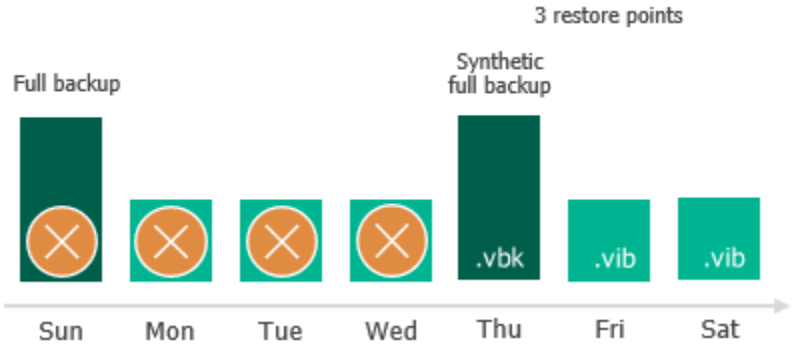


Retention Policy for Synthetic Full Backups

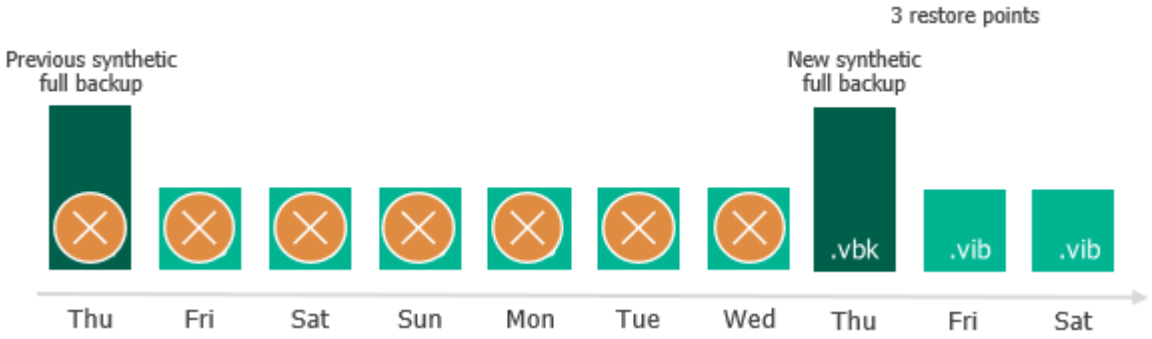
To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental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

For this reason, if you set up the backup job to create synthetic full backups, in some days there will be more restore points on the disk than specified by retention policy settings. Veeam Agent for Microsoft Windows will remove the full backup chain only after the last incremental backup file in the chain becomes outdated.

For example, the retention policy is set to 3 restore points. A full backup file is created on Sunday, incremental backup files are created Monday through Saturday, and synthetic full backup is scheduled on Thursday. Although the retention policy is already breached on Wednesday, the full backup is not deleted. Without the full backup, backup chain is useless, leaving you without any restore point at all. Veeam Agent for Microsoft Windows will wait for the next full backup file and 2 incremental backup files to be created, and only then will delete the whole previous chain, which will happen on Saturday.



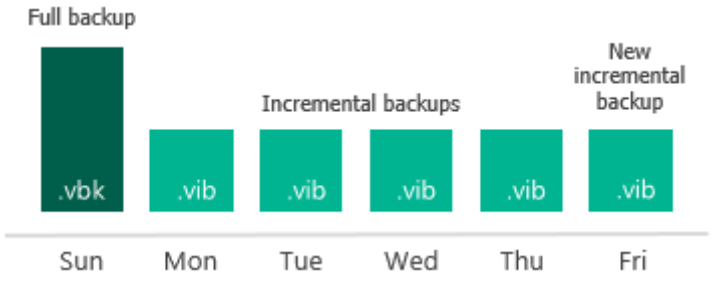
Keep in mind that if the backup job is set up to create synthetic full backups, Veeam Agent for Microsoft Windows will never transform the backup chain. Instead, Veeam Agent for Microsoft Windows will always wait for the next full backup file and the necessary number of incremental backup files to be created, and only then will delete the whole previous chain. In the example above, Veeam Agent for Microsoft Windows will delete the previous chain every Saturday. As a result, although the retention policy is set to 3 restore points, the actual number of backup files on the disk will be greater most of the time.



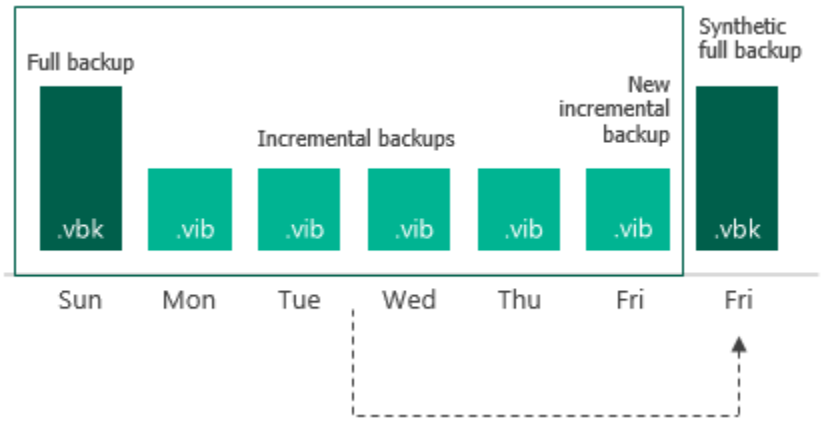
How Synthetic Full Backup Works

To create a synthetic full backup, Veeam Agent for Microsoft Windows performs the following steps:

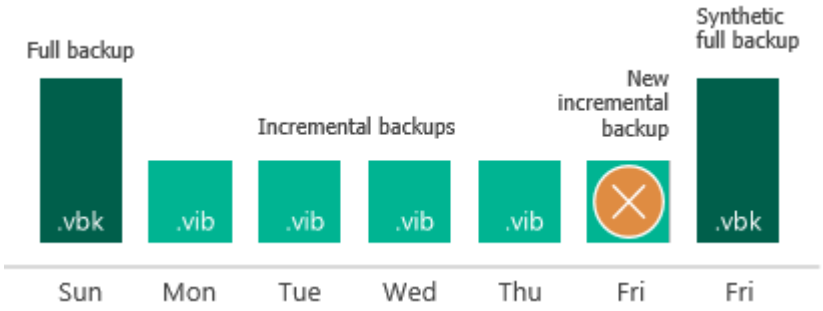
1. On a day when synthetic full backup is scheduled, Veeam Agent for Microsoft Windows triggers a new backup job session. During this session, Veeam Agent for Microsoft Windows first performs incremental backup in a regular manner and adds a new incremental backup file to the backup chain. Incremental backup helps Veeam Agent for Microsoft Windows ensure that the synthetic full backup includes the latest changes of the backed-up data.



2. At the end of the backup job session, Veeam Agent for Microsoft Windows builds a new synthetic full backup using backup files that are already available in the backup chain, including the newly created incremental backup file.



3. When the synthetic full backup is created, Veeam Agent for Microsoft Windows deletes the incremental backup file created at the beginning of the job session. As a result, you have a backup chain that consists of a full backup file, set of incremental backup files and synthetic full backup file.



4. Every next job session creates a new incremental restore point starting from the synthetic full backup until the day on which synthetic full backup is scheduled. On this day, Veeam Agent for Microsoft Windows creates a new synthetic full backup.

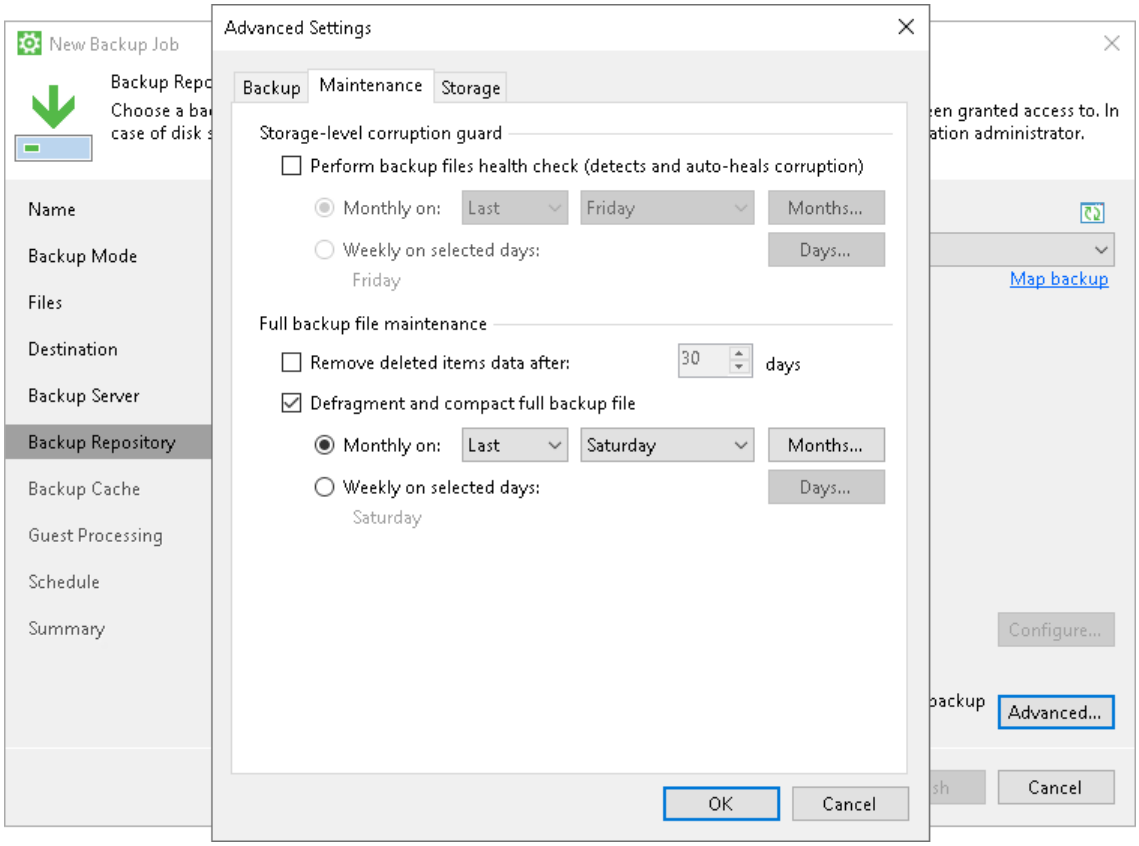
Compact of Full Backup File

If you do not create periodic full backups, the backup job constantly transforms the full backup file in the backup chain to meet retention policy settings. The transformation process, however, has a side effect. In the long run, the full backup file grows large and gets badly fragmented. The file data occurs to be written to non-contiguous clusters on disk, and operations of reading and writing data from and to the backup file slow down.

To resolve the fragmentation problem, you can instruct Veeam Agent for Microsoft Windows to compact the full backup file periodically. During the file compact operation, Veeam Agent creates a new empty file and copies to this file data blocks from the original full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from and to the file increases.

> **NOTE**
>
> Keep in mind that some data blocks belonging to data deleted from the backup source may not be deleted during the compact operation. As a result, the difference in size between the original and the new full backup files may not be equal to the size of the excluded data blocks. In this case, you can manually create an active full backup and reset the backup chain. To learn more about the active full backup, see Active Full Backup.

To compact the full backup file periodically, you must enable the **Defragment and compact full backup file** option in the backup job settings and define the compact operation schedule. By default, the compact operation is performed on the last Saturday of every month. You can change the compact operation schedule and instruct Veeam Agent for Microsoft Windows to perform it weekly or monthly on specific days.



Limitations for Full Backup File Compact

The full backup file compact has the following limitations:

- The **Defragment and compact full backup file** option can be enabled only for backup jobs for which active full and synthetic full backups are not scheduled.
- The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage.
- The compact full backup file operation is not performed during backup job sessions that produce active full backups. If the backup job starts again on the same day when the active full backup was created, Veeam Agent for Microsoft Windows does not perform the compact full backup operation. This limitation helps reduce the number of backup operations — Veeam Agent considers that the full backup is recent and does not need to be rebuilt.

  If such situation occurs, Veeam Agent for Microsoft Windows triggers the full backup file compact operation during the next backup job session that produces an incremental backup file on another day.
- The target location must have enough space to store a file of the full backup size. During the compact process, Veeam Agent for Microsoft Windows creates auxiliary files that exist in the target location until the end of the compact operation.
- If you change the block size in backup job settings, Veeam Agent for Microsoft Windows does not change the block size in the compacted backup file till the next full backup. However, if you change compression settings in backup job settings, during the next compact file operation Veeam Agent for Microsoft Windows changes the compression level for the compacted backup file.
- The file compact operation is not performed during a backup job session that creates a restore point in the backup cache.

- The file compact operation is not performed during the backup cache synchronization process.

Removal of Deleted Drives Data

During the compact operation, Veeam Agent for Microsoft Windows does not copy all data blocks from the VBK file to the newly created file. It copies only data blocks of Veeam Agent computer drives whose information is stored in the Veeam Agent for Microsoft Windows database. If a drive was removed from the Veeam Agent computer, its data is not copied to the new full backup file. This approach helps reduce the size of the full backup file and remove unnecessary data from it.

Backup to Object Storage

If you want to store your data in a cloud-based or on-premises object storage, you can create backup jobs targeted at the object storage or another storage that uses object storage as a back end.

You can store Veeam Agent backups in the following object storage types:

- S3 compatible (including Wasabi Cloud and IBM Cloud)
- Amazon S3
- Google Cloud Storage
- Microsoft Azure Blob Storage

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

- Backup destinations
- Connection types
- 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 the object storage and creates a backup repository in this storage.

  Keep in mind that to connect to object storage, you need to specify 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, an object storage repository is created in Veeam Backup & Replication. Veeam Agent connects to Veeam Backup & Replication and uses this Veeam backup repository.

  To learn more, see Veeam Backup Repository Settings.

- To object storage added as a Veeam Cloud Connect repository. In this case, a Veeam Cloud Connect service provider creates an object storage repository in Veeam Backup & Replication and exposes it as a cloud repository to tenants. Veeam Agent connects to the service provider and uses the Veeam Cloud Connect repository.

  To learn more, see Veeam Cloud Connect Repository Settings.

Connection Types

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 an external cloud service provider.

Considerations and Limitations

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

- Veeam Agent for Microsoft Windows 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. To learn more, 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.

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

> **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 Azure 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 object storage, 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.
- 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.

Backup to Deduplicating Storage Appliances

You can store backups in the deduplicating storage appliances added as backup repositories. To learn the full lists of supported appliances and their requirements and limitations, see the Deduplicating Storage Appliances section in the Veeam Backup & Replication User Guide.

If you want to use immutability with the deduplicating storage appliances, consider the limitations listed in the following subsections:

- HPE StoreOnce Immutability and Veeam Agents
- Dell Data Domain Immutability and Veeam Agents

HPE StoreOnce Immutability and Veeam Agents

Veeam Backup & Replication supports immutability for the HPE StoreOnce Catalyst repositories starting from version 12.0 with cumulative patch P20230223 or P20230412.

If you want to use immutability with HPE StoreOnce Catalyst repositories, make sure that the value for the Maximum ISV Controlled Data Retention setting in HPE StoreOnce exceeds or is equal to the value of each of the following settings configured in Veeam Backup & Replication:

- The immutability period specified in the backup repository settings.
- The long-term retention period configured in backup job settings.

If the value of at least one of these periods exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, consider the following:

- If you use Veeam Backup & Replication version 12.1:
  - If the immutability period specified in the backup repository settings exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, Veeam Backup & Replication applies immutability to the created backups according to the maximum value set for immutability in HPE StoreOnce Catalyst Store.
  - If the long-term retention period configured in backup job settings exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, the immutability period for backups with GFS flags is set according to the maximum value set for immutability in HPE StoreOnce Catalyst Store. For example, if the backup is stored for 1 year, but the maximum value for immutability in HPE StoreOnce Catalyst Store is set to 6 months, the backups will be immutable for 6 months.
- If you use Veeam Backup & Replication version 12.0 with cumulative patch P20230223 or P2023041, Veeam Backup & Replication does not apply immutability to the created backups.

To learn more about immutability for the HPE StoreOnce Catalyst repositories, see the HPE StoreOnce and Immutability section in the Veeam Backup & Replication User Guide.

Dell Data Domain Immutability and Veeam Agents

Starting from Veeam Backup & Replication version 12.1, Veeam Backup & Replication supports the Dell Data Domain retention lock feature.

If you want to use immutability with the Dell Data Domain backup repository, make sure that the immutability period in the backup repository settings lies in the range between the minimum and maximum retention periods configured in Dell Data Domain. The minimum and maximum values are included into the range.

If the immutability period configured in Veeam Backup & Replication lies outside the established range, the immutability is set equal to the nearest range value. If the long-term retention period configured in Veeam Backup & Replication lies outside the established range, the immutability for them is set according to the nearest range value. For example, if the backup is stored for 1 year, but the range for immutability in Dell Data Domain is set to from 2 to 6 months, the backups will be immutable for 6 months.

To learn more about immutability for the Dell Data Domain backup repositories, see the Retention Lock section in the Veeam Backup & Replication User Guide.

Health Check for Backup Files

You can instruct Veeam Agent for Microsoft Windows to periodically perform the health check for your backups.

Veeam Agent offers two different health check mechanisms:

- In the first case, Veeam Agent performs a CRC check for metadata and a hash check for data blocks in the backup file to verify their integrity. The health check verifies the latest restore point in the backup chain to make sure that the restore point is consistent, and you will be able to restore data from this restore point. To learn more, see Standard Health Check.
- In the second case, Veeam Agent does not perform a hash check for data blocks, but verifies metadata for the whole backup, not just the latest restore point. This mechanism uses less traffic than the standard health check as it does not read data from data blocks. This type of health check is intended and is the default option for object storage targets. To learn more, see Health Check for Object Storage.

Health Check Schedule

To run the health check periodically, enable the **Perform backup files health check** option in the backup job settings and define the health check schedule. By default, the health check is performed on the last Friday of every month. You can change the schedule and run the health check weekly or monthly on specific days.

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

- The health check runs automatically during the first incremental backup job session on the days specified in the health check schedule. If the backup job runs several times on a specified day, the health check is performed only with the first run of the backup job on that day. For example, if the job is scheduled to run several times on Saturday, and the health check is scheduled on Saturday, the health check will only be performed during the first backup job session on Saturday.

  The 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, the health check will be performed during the first backup job session following that day.

  For example, you scheduled to run the 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, the health check will be preformed on the following Monday with the first incremental backup job session on that day.

Limitations for Health Check

- The health check is not performed during an active full backup job session started manually or automatically by schedule.
- The health check is not performed during a backup job session that creates a restore point in the backup cache.
- The health check is not performed during the backup cache synchronization process.

Health Check Retries

The health check itself is started during the backup job session or the job retry session if the backup job session has failed. If the attempts are not successful, Veeam Agent for Microsoft Windows will perform the health check during the last job retry in any case.

If the health check detects corrupted data, Veeam Agent for Microsoft Windows completes the backup job with the *Error* status and starts the health check retry process. The health check retry starts as a separate backup job session. During the health check retry, Veeam Agent attempts to transport data blocks for the corrupted restore point from the Veeam Agent computer to the target location.

For a backup job started automatically upon schedule, the number of health check retries is equal to the number of job retries specified in the job settings. For a job started manually, Veeam Agent for Microsoft Windows performs 1 health check retry.

> **NOTE**
>
> Consider the following:
>
> - If Veeam Agent for Microsoft Windows fails to fix the corrupted data during all health check retries, you must retry the job manually. In this case, Veeam Agent will transport the necessary data blocks from the Veeam Agent computer to fix the corrupted restore point.
> - If you try to restore data from a corrupted restore point, Veeam Agent will display a warning message informing you that the restore operation may fail or the restored data may be corrupted.

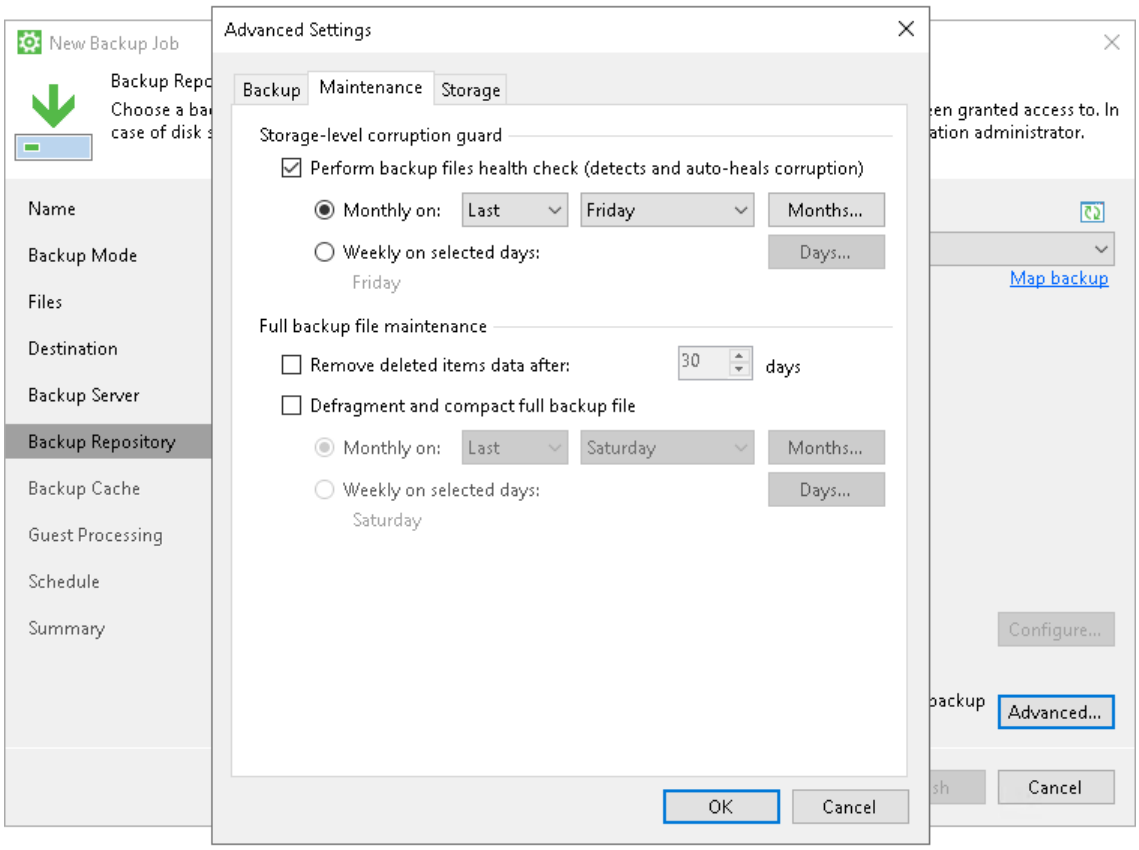
Standard Health Check

During the standard health check, Veeam Agent performs a CRC check for metadata and a hash check for data blocks in the backup file to verify their integrity. The health check helps make sure that the restore point is consistent, and you will be able to restore data from this restore point.

You can use the standard health check for all backup targets.

> **NOTE**
>
> Keep in mind that for the object storage targets, Veeam Agent offers another health check mechanism as default. To learn more, see Health Check for Object Storage.

To run the standard health check periodically, enable the **Perform backup files health check** option in the backup job settings and define the health check schedule.



How Standard Health Check Works

When Veeam Agent for Microsoft Windows saves a new restore point to the backup location, it calculates CRC values for backup metadata and hash values for data blocks in the backup file, and saves these values in the metadata of the backup file, together with the backed-up data. During the health check session, Veeam Agent uses these values to make sure that a verified restore point is consistent.

> **NOTE**
>
> If the backup job is targeted at a Veeam backup repository or cloud repository, and you perform the health check for the encrypted backup files, Veeam Backup & Replication will pass encryption keys to the Veeam backup repository or cloud repository. For more information on encryption, see Data Encryption.

Veeam Agent for Microsoft Windows performs the health check in the following way:

1. During the backup job session, Veeam Agent for Microsoft Windows creates a new restore point in the backup chain.
2. At the end of the backup job session, Veeam Agent for Microsoft Windows performs the health check. It calculates CRC values for backup metadata and hash values for data blocks in the backup file and compares them with the CRC and hash values that are already stored in the backup file.

   During the health check, Veeam Agent for Microsoft Windows verifies the latest restore point in the backup chain (restore point created with the current backup job session — the session during which the health check is performed). If the latest restore point in the backup chain is incomplete (for example, if the current backup job session completed with an error), Veeam Agent checks the restore point preceding the latest one.

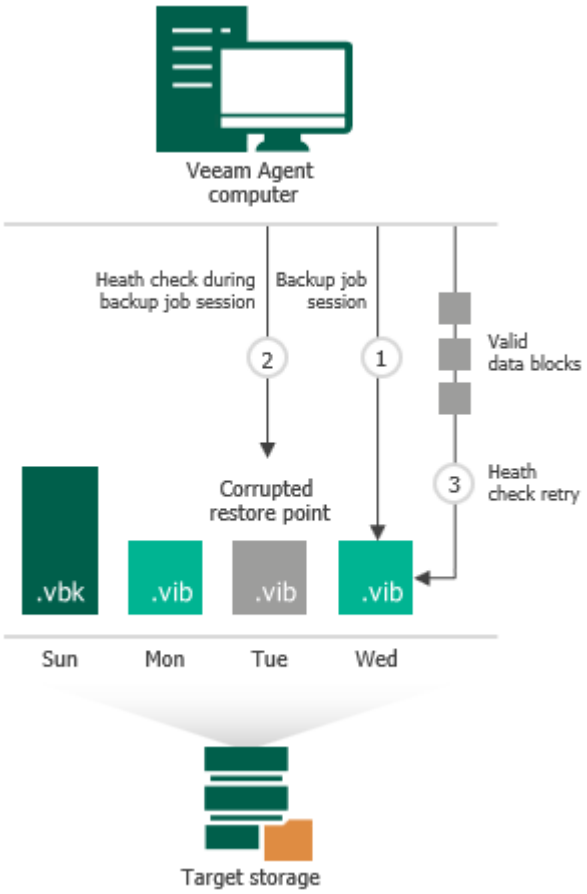
   If the health check does not detect data corruption, the backup job session completes in a regular way.

3. If the health check detects corrupted data, Veeam Agent for Microsoft Windows completes the backup job with the *Error* status and starts the health check retry process. The health check retry starts as a separate backup job session.

   Depending on the revealed data corruption, Veeam Agent performs the following actions:

   - If the health check detects corrupted backup metadata in the full backup file, Veeam Agent marks the backup chain starting from this full restore point as corrupted in the Veeam Agent for Microsoft Windows database. During the health check retry, Veeam Agent transports the entire data selected for backup from the Veeam Agent Computer, creates a new full backup file in the target location and saves transported data blocks to this backup file.
   - If the health check detects corrupted backup metadata in the incremental backup file, Veeam Agent removes information about this incremental restore point and subsequent incremental restore points from the Veeam Agent for Microsoft Windows database. During the health check retry, Veeam Agent transports incremental data relatively to the latest valid restore point in the backup chain from the Veeam Agent computer, creates a new incremental backup file in the target location and saves transported data blocks to this backup file.
   - If the health check detects corrupted data blocks in the full or incremental backup file, Veeam Agent marks the restore point that includes the corrupted data blocks and subsequent incremental restore points as corrupted in the Veeam Agent for Microsoft Windows database. During the health check retry, Veeam Agent transports data blocks from the Veeam Agent computer. In addition, Veeam Agent transports data blocks that have changed since the backup job session that has triggered the health check. Veeam Agent stores these data blocks to the latest restore point that has been created with the current backup job session (session that has triggered the health check retry).

   You can view the health check result in the restore point statistics. If the health check finds corrupted data, it will display information on where corrupt data has been detected — in metadata or blockstore, as well as list all restore points that share the corrupted data blocks.



Health Check for Object Storage

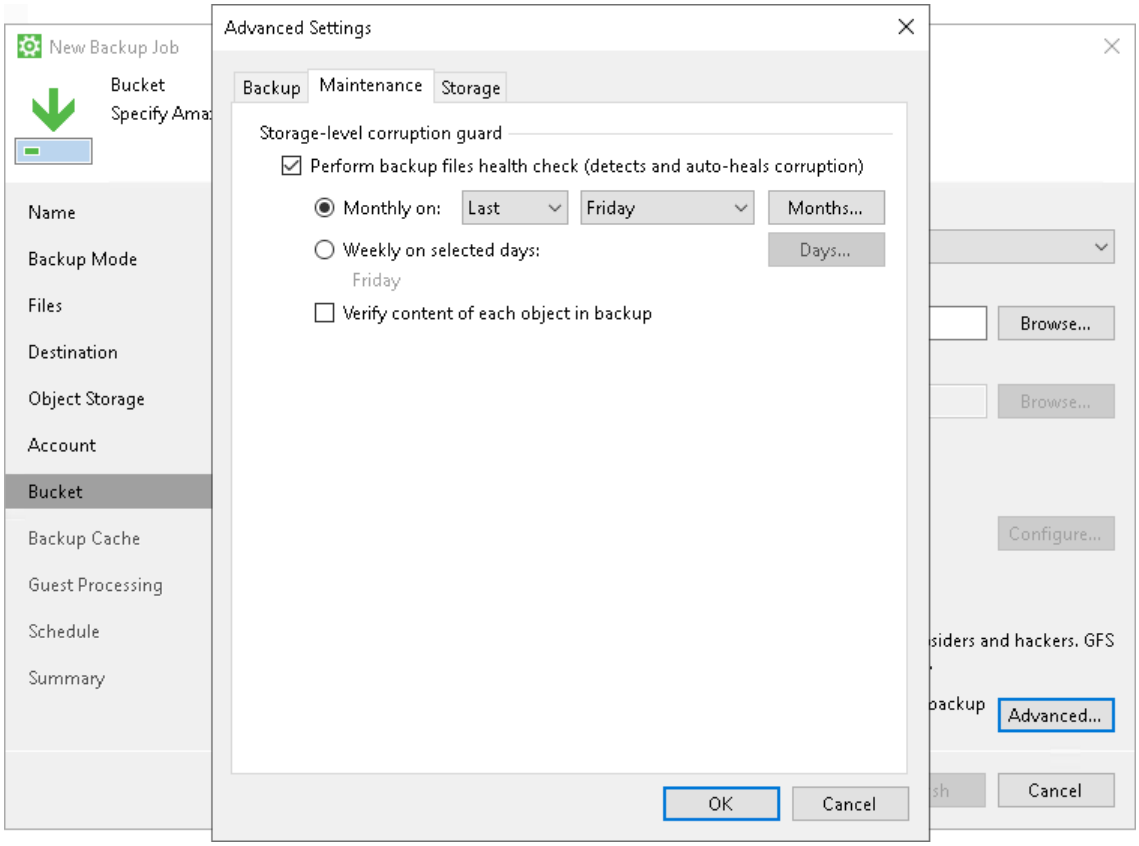
For backup jobs targeted at object storage, Veeam Agent offers a special health check mechanism that differs from the standard health check in the following ways:

- The health check for object storage verifies metadata for the whole backup, not just the latest restore point.
- The health check for object storage does not read data from data blocks; it only lists data blocks to make sure all blocks in the storage are available for rebuilding every restore point in the backup chain.

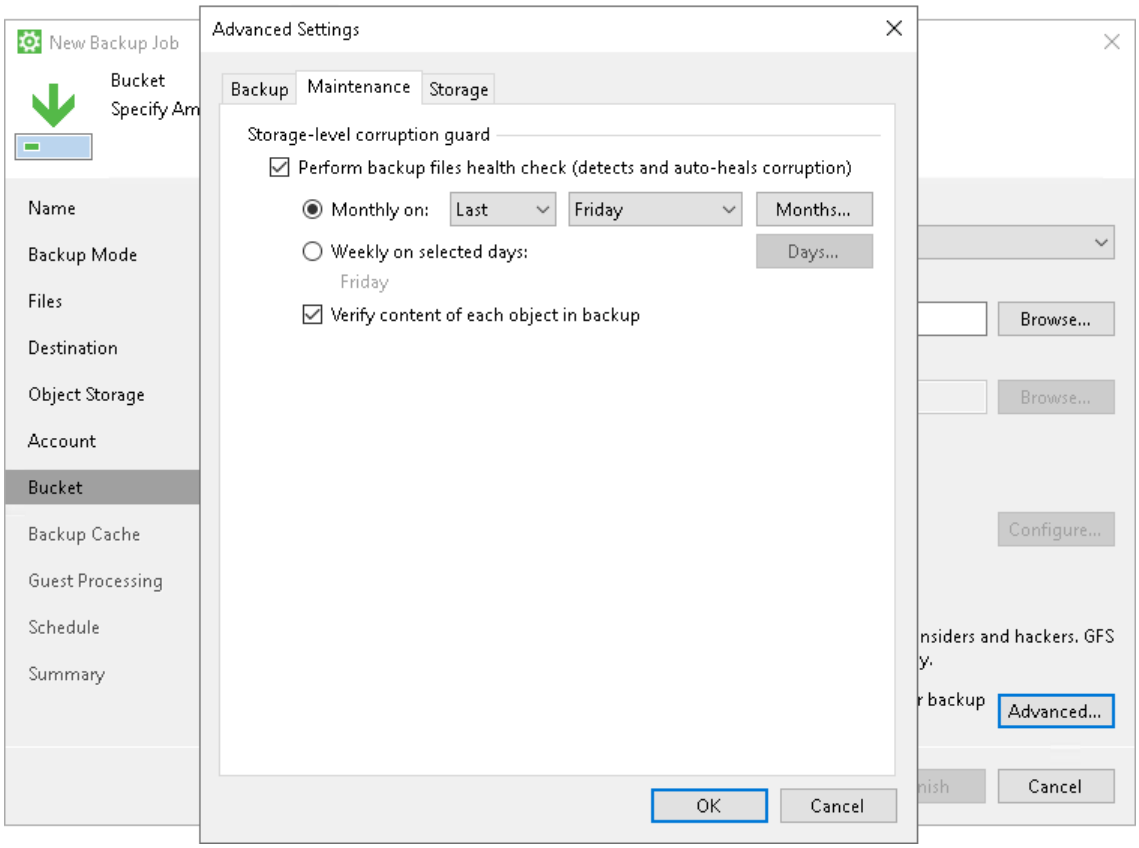
The health check for object storage works faster than the standard health check and helps save traffic.

> **NOTE**
>
> The health check mechanism described in this section is only available for object storage targets.

To run the special health check for object storage periodically, select the **Perform backup files health check** check box in the backup job settings and define the health check schedule. Make sure that the **Verify content of each object in backup** check box is not selected.



If necessary, you can enable the standard health check mechanism for object storage targets. To do so, select the **Verify content of each object in backup** check box in the backup job settings. Keep in mind that enabling this setting may result in additional charges from your object storage provider.



How Health Check for Object Storage Works

Veeam Agent performs the 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 in 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.

   If Veeam Agent detects corrupted data, the health check completes with an error. Depending on the detected data inconsistency, Veeam Agent behaves in one of the following ways:

   - If the health check detects corrupted metadata, Veeam Agent marks the backup as corrupted in the Veeam Agent configuration database; the backup job session fails. 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 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 in the backup chain, Veeam Agent launches the health check retry.

     During the health check retry, Veeam Agent restarts the backup job to create a new restore point and transports data blocks from the Veeam Agent computer including the blocks that contain corrupted data and the blocks that have changed since the backup job session that has triggered the health check. Veeam Agent will not perform another health check after the job retry is finished; the next health check will run according to the defined schedule during another incremental backup job session.

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

You can view the health check result in the restore point statistics. If the health check finds corrupted data, it will display information on where corrupt data has been detected — in metadata or blockstore, as well as list all restore points that share the corrupted data blocks.

NOTE

Consider the following:

In case of immutable backups, Veeam Agent performs the health check only for valid restore points according to the retention policy. Immutable data associated with removed restore points can still remain in the repository depending on the immutability period, but Veeam Agent will not perform the health check for such data.

For information about backup immutability settings, see Backup Immutability.

Changed Block Tracking

To perform incremental backup, Veeam Agent for Microsoft Windows needs to know what data blocks have changed since the previous job session. To get the list of changed data blocks, Veeam Agent for Microsoft Windows uses the changed block tracking mechanism, or CBT. CBT increases the speed and efficiency of incremental backups.

To keep track of changed data blocks, Veeam Agent for Microsoft Windows can use the following mechanisms:

- **Default CBT mechanism** — this mechanism is enabled by default in all installations of Veeam Agent for Microsoft Windows. To learn more, see Default Changed Block Tracking Mechanism.
- **Veeam CBT driver** — this driver helps Veeam Agent for Microsoft Windows keep track of changed data blocks in a more efficient way. This functionality is available if the Veeam Agent computer meets a list of requirements. To learn more, see Veeam Changed Block Tracking Driver.

Default Changed Block Tracking Mechanism

Veeam Agent for Microsoft Windows performs the changed block tracking differently depending on the backup type:

- CBT for volume-level backup
- CBT for file-level backup

CBT for Volume-Level Backup

In case of the volume-level backup, Veeam Agent for Microsoft Windows performs changed block tracking in the following way:

1. During the full backup job session, Veeam Agent reads the Master File Table (MFT) of the backed-up volume. Veeam Agent uses MFT records to create digests with file system metadata, transfers the created digests to the target location and stores them to the resulting backup file.
2. During subsequent incremental job sessions, Veeam Agent performs the following operations:
    a. Reads the Master File Table (MFT) of the backed-up volume and creates the new digests with file system metadata.
    b. Interacts with the target backup location to obtain digests from the backup file that was created during the previous job session.
    c. Compares new and previous digests to detect files whose data blocks have changed on the volume since the previous job session.

    During incremental backup, Veeam Agent for Microsoft Windows reads from the VSS snapshot only data blocks pertaining to files that have changed since the previous job session. If Veeam Agent cannot calculate information about the changed files, for example, if it fails to retrieve digests from the backup file, Veeam Agent will need to read all data blocks from the VSS snapshot. As a result, the backup may take significantly more time.

NOTE

Veeam Agent for Microsoft Windows uses the default CBT mechanism for NTFS volumes only. As a result, for volumes that use other file systems, incremental backup will require greater time, because Veeam Agent for Microsoft Windows will read all data from the VSS snapshot to detect what blocks have changed since the last job session.



CBT for File-Level Backup

In case of the file-level backup, Veeam Agent for Microsoft Windows performs changed block tracking in the following way:

1. During the full backup job session, Veeam Agent creates a new NTFS partition in the backup file. Veeam Agent uses this partition to store all backed-up files and folders.
2. During subsequent incremental job sessions, Veeam Agent performs the following operations:
   a. Compares the last modification time attribute of files on the Veeam Agent computer and files in the backup. This operation allows Veeam Agent to detect files that have changed since the previous job session.
   b. Transfers data blocks that contain metadata related to each changed file and its parent folders from the target backup location to the Veeam Agent computer.

      If the backed-up file system has a complex folder structure with many hierarchy levels, and you back up data to a remote location, during incremental backup, the inbound network traffic on the Veeam Agent computer may exceed by far the outbound traffic. Significant amount of data can be transferred to the Veeam Agent computer even if few files are changed since the previous job session.
   c. Replaces file system metadata in the downloaded data blocks with the current file system metadata.
   d. Transfers data blocks with current metadata from the Veeam Agent computer to the target backup location along with changed files. In the target backup location, Veeam Agent stores data and metadata to the newly created backup file.

NOTE

Consider the following:

- Veeam Agent for Microsoft Windows detects changed files using the last modification time attribute. If you change the file in any way, but the last modification time attribute remains unchanged, Veeam Agent will not back up this file during an incremental job session.
- If the backed-up file has changes, Veeam Agent will copy to the target location not only changed data blocks of the file but the entire file. To save space on the target storage, consider using the volume-level backup. To learn more, see Backup Types.



Veeam Changed Block Tracking Driver

You can set up Veeam Agent for Microsoft Windows to use the Veeam CBT driver instead of the default CBT mechanism. The Veeam CBT driver is a class filter driver for volume devices that helps Veeam Agent keep track of changed data blocks in a more efficient way. The driver is intended for computers running applications with large database files. The Veeam CBT driver is supported for volume-level and file-level backups.

> **NOTE**
>
> In case of the file-level backup, consider the following:
>
> - Veeam Agent does not use the Veeam CBT driver to back up deduplicated files.
> - Veeam Agent uses the Veeam CBT driver to back up files of 50 MB and larger including files with unchanged last modification time attribute.
> - When you run a backup job for the first time after switching to the Veeam CBT driver, the job may take a significant time to finish. This happens because the Veeam CBT driver cannot retrieve all necessary information about changed data blocks from backup files created with the default CBT mechanism. In this case, files for backup of which Veeam Agent uses the Veeam CBT driver are backed up as a whole.
> - The Veeam CBT driver is designed to track data blocks that changed since the last run of the backup job. If you work with a file in an application that downloads the entire file into RAM, after you save the changes, all file blocks will be overwritten. Veeam Agent backs up such a file as a whole upon the next run of the backup job.

To use the Veeam CBT driver, the Veeam Agent computer must meet the following requirements:

- Run a 64-bit version of Microsoft Windows OS.
- Run one of the following OSes:
  - Microsoft Windows 11 (from version 21H2 to version 23H2).
  - Microsoft Windows 10 (from version 1803 to version 22H2).
  - Microsoft Windows Server OS that is supported by Veeam Agent. For more information, see System Requirements.
- Run the Workstation or Server edition of Veeam Agent for Microsoft Windows.

IMPORTANT

Consider the following:

- Prior to installing the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, make sure that update KB3033929 is installed in the OS.

  The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver. To learn more, see this Microsoft KB article.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, 2012 or 2012 R2 if one or more volumes on this computer are encrypted with Microsoft BitLocker (or other encryption tool), or if you plan to use Microsoft BitLocker to encrypt volumes on this computer. Concurrent operation of Microsoft BitLocker and Veeam CBT driver may result in driver failures and may prevent the OS from starting.
- Do not install the Veeam CBT driver on a computer if you plan to use devices with hardware encryption made according to the TCG Opal Security Subsystem Class Specification. Operation of the driver on such devices may lead to a crash of the operating system. To learn more about the TCG Opal Security Subsystem Class Specification, see this Trusted Computing Group webpage.

To enable the advanced CBT mechanism provided by the Veeam CBT driver, you need to install the driver in the Veeam Agent control panel. You can perform this operation at any time you need. To activate the driver after installation, Veeam Agent needs to reboot the computer. After computer reboot, the Veeam CBT driver will start keeping track of changed data blocks on computer volumes whose data you have selected for backup in the Veeam Agent backup job settings.

In contrast to the default CBT mechanism that supports NTFS volumes only, the Veeam CBT driver can keep track of changed data blocks on volumes that use the following file systems:

- FAT (only for volume-level backups)
- NTFS
- ReFS

Information about changed data blocks is registered in special VCT files. VCT files are stored in the C:\ProgramData\Veeam\EndpointData\CtStore folder on the Veeam Agent computer. When the backup job runs, Veeam Agent for Microsoft Windows uses VCT files to find out what data blocks have changed since the last run of the job, and copies only changed data blocks from the backed-up volume.

If you use the Veeam CBT driver, the `C:\ProgramData\Veeam\EndpointData\CtStore` folder accessibility is crucial for a successful backup. Consider the following:

- The folder and its content must not be compressed or encrypted.
- The folder and its parent folders must not be reparse points.

NOTE

Consider the following:

- If the Veeam Agent computer shuts down unexpectedly, the Veeam CBT driver may fail to register information about changed data blocks in a VCT file. In this case, during the next backup job session, Veeam Agent for Microsoft Windows will need to read all data from the backed-up volume to create incremental backup. As a result, incremental backup will require greater time.
- If data blocks are changed on a volume while this volume is mounted on another Windows-based machine, during the next backup job session, Veeam Agent for Microsoft Windows will also read all data from the volume to create incremental backup.
- The Veeam CBT driver cannot detect data block changes made on a volume that is mounted in a non-Windows OS. For example, such changes can be made when you boot your computer using a Linux-based antivirus rescue disk. To continue the backup chain after such changes, you need to create active full backup instead of incremental backup. Alternatively, you can reset CBT. To learn more, see Resetting CBT.

Data Compression

Veeam Agent provides mechanisms of data compression and deduplication. Data compression and deduplication let 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	Compression Algorithm	Description
None	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	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	Lz4	The default recommended compression level. It provides the best ratio between size of the backup file and time of the backup procedure.
High	Zstd 3	Provides additional 10% compression ratio over the Optimal level at the cost of about 10x higher CPU usage.
Extreme	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 for Microsoft Windows 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:

- The **4 MB** option is recommended for backup jobs that can produce very large full backup files — larger than 16 TB. With this option selected, Veeam Agent for Microsoft Windows uses data block size of 4096 KB.

  Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process. Keep in mind, however, that this storage optimization option will provide the largest size of incremental backup files.

- The **1 MB** option is recommended for backup to SAN, DAS or local storage. With this option selected, Veeam Agent uses 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.

- The **512 KB** option is recommended for backup to NAS and onsite backup. With this option selected, Veeam Agent uses data block size of 512 KB. This option reduces the size of an incremental backup file because of reduced data block sizes.

- The **256 KB** option is recommended if you plan to use WAN for offsite backup. With this option selected, Veeam Agent uses 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.

Guest Processing

For Server edition of Veeam Agent for Microsoft Windows, you can specify guest processing options. Veeam Agent for Microsoft Windows offers the following guest processing options:

- Application-aware processing. You can create transactionally consistent backups of servers running applications that support Microsoft VSS. Application-aware processing guarantees that you can perform restore from Veeam Agent backups without data loss.
- Pre-freeze and post-thaw scripts. You can use pre-freeze and post-thaw scripts to quiesce applications that do not support Microsoft VSS.
- Transaction log truncation. You can set up the backup job to truncate transaction logs after the job successfully completes.
- Transaction log backup for Microsoft SQL Server and Oracle. You can set up the backup job to back up transaction logs from servers running Microsoft SQL Server and archived logs of Oracle database systems.
- File system indexing. You can set up the backup job to create a catalog of files and folders on the Veeam Agent computer OS. If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you will be able to search for individual files in Veeam Agent backups and perform 1-click restore in Veeam Backup Enterprise Manager.

  File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the Veeam Agent backup. For more information, see the Veeam Backup Enterprise Manager User Guide.

Supported Applications

Veeam Agent for Microsoft Windows supports VSS-aware processing for the following systems:

Specification	Requirement
Microsoft Active Directory Domain Controllers	The following versions of Microsoft Active Directory Domain Services servers (domain controllers) are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 Minimum supported domain and forest functional level is Windows Server 2003.
Microsoft Exchange	The following versions of Microsoft Exchange are supported: • Microsoft Exchange 2019 • Microsoft Exchange 2016 • Microsoft Exchange 2013 SP1 • Microsoft Exchange 2013

Specification	Requirement
Microsoft SharePoint	The following versions of Microsoft SharePoint Server are supported: • Microsoft SharePoint Server Subscription Edition • Microsoft SharePoint Server 2019 • Microsoft SharePoint Server 2016 • Microsoft SharePoint Server 2013 All editions are supported (Foundation, Standard, Enterprise).
Microsoft SQL Server	The following versions of Microsoft SQL Server are supported: • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 All editions of Microsoft SQL Server except LocalDB are supported.
Oracle	Oracle Database from version 11g to version 21c is supported for the following operating systems (32-bit and 64-bit architecture): • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 **Important notes:** • Automatic Storage Management (ASM) is not supported. • Oracle Real Application Clusters (RAC) are not supported. • Oracle servers using Data Guard are not supported. • Oracle Database Express Edition is supported. • Configurations with different versions of Oracle Database deployed on the same server are not supported. • 32-bit Oracle running on 64-bit operating systems is not supported.

Application-Aware Processing

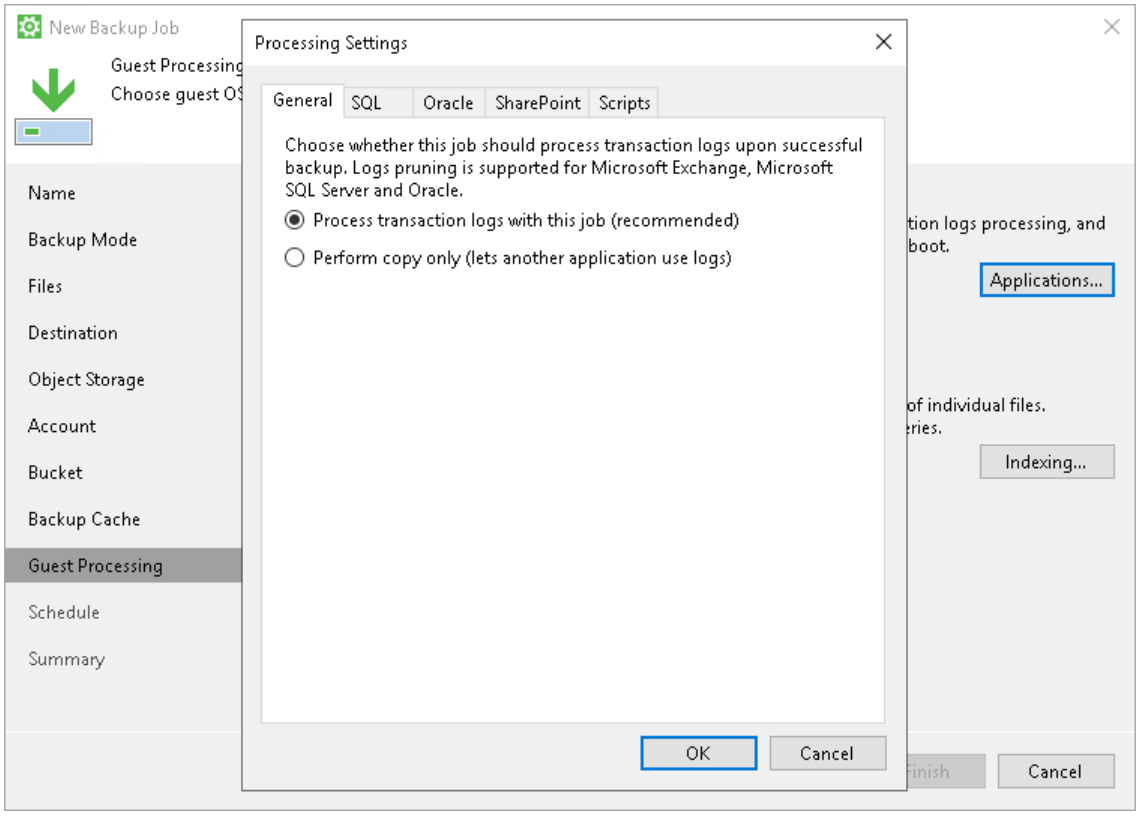
To create transactionally consistent backups of servers that run VSS-aware applications such as Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle, you must enable application-aware processing for the backup job.

Application-aware processing is Veeam's proprietary technology based on Microsoft VSS. Microsoft VSS is responsible for quiescing applications and creating a consistent view of application data on the OS of the Veeam Agent computer. Use of Microsoft VSS ensures that there are no unfinished database transactions or incomplete application files when Veeam Agent creates a Microsoft VSS snapshot and starts copying backed-up data to the target location. For more information about Microsoft VSS, see this Microsoft article.

In the Server edition of Veeam Agent, the type of the VSS snapshot depends on application-aware processing settings:

- If application-aware processing is disabled for the backup job, Veeam Agent creates a copy-only VSS snapshot.
- If application-aware processing is enabled and the **Perform copy only** option is selected, Veeam Agent creates a copy-only VSS snapshot.
- If application-aware processing is enabled and the **Process transaction logs with this job** option is selected, Veeam Agent creates a full VSS snapshot.

To learn more, see Specify Application-Aware Processing Settings.



Application-aware processing is supported for Microsoft Windows 2008 R2 SP1 and later. To use application-aware processing, you must have the latest updates installed on the Veeam Agent computer OS. To learn more, see Supported Applications.

> **IMPORTANT**
>
> If your computer OS runs an application that does not support Microsoft VSS (there is no VSS writer for this particular type of application, for example, MySQL), Veeam Agent for Microsoft Windows will not be able to utilize Microsoft VSS and application-aware processing for this application. To process such applications, you can use pre-freeze and post-thaw scripts. For more information, see Pre-Freeze and Post-Thaw Scripts.

Pre-Freeze and Post-Thaw Scripts

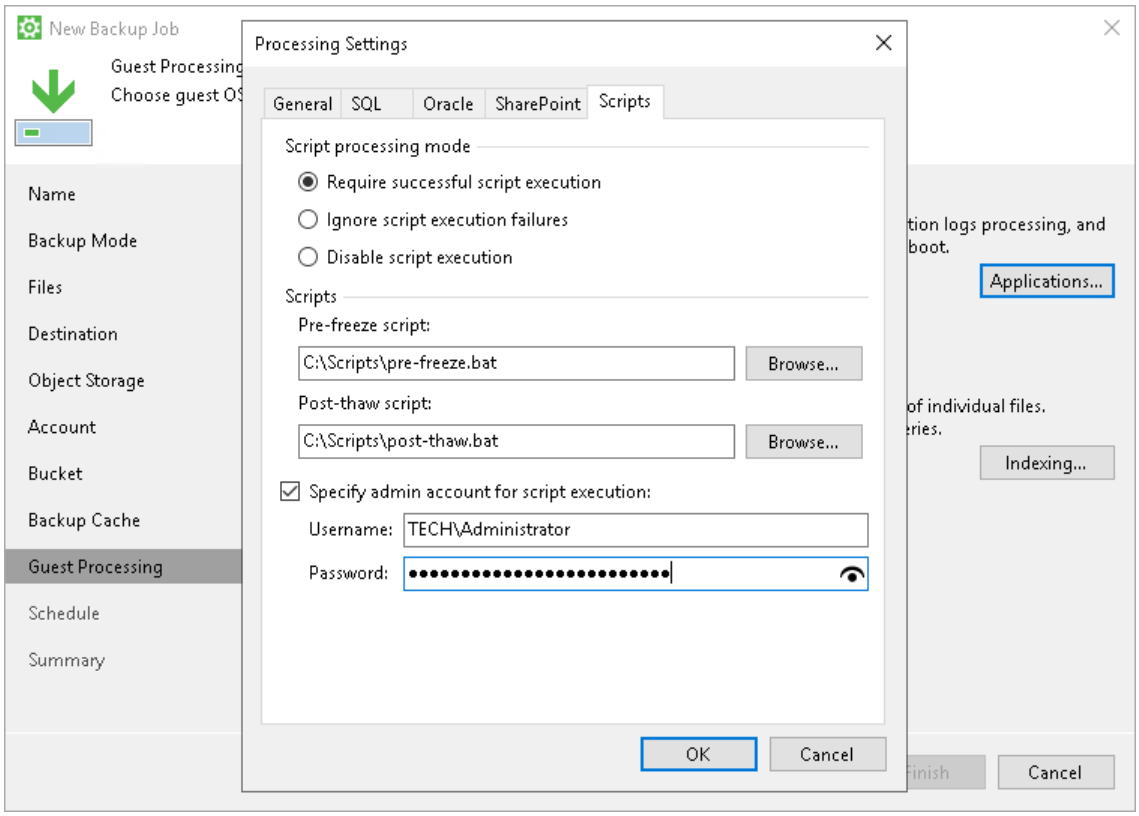
If Veeam Agent computer runs applications that do not support Microsoft VSS, you can instruct Veeam Agent for Microsoft Windows to run custom scripts during the backup job session. For example, the pre-freeze script may quiesce the file system and application data to bring the computer OS to a consistent state before Veeam Agent for Microsoft Windows creates a Microsoft VSS snapshot. After the VSS snapshot is created, the post-thaw script may bring the OS and applications to their initial state.

Veeam Agent for Microsoft Windows supports scripts in the EXE, BAT and CMD file format.

Scripts must be created beforehand. You must specify paths to them in the backup job settings. Scripts must reside on a local drive of the Veeam Agent computer.

When the backup job starts, Veeam Agent for Microsoft Windows executes scripts specified for the job. A script is considered to be executed successfully if "0" is returned.

The default time period for script execution is 10 minutes. If the script fails to execute before the timeout expires, Veeam Agent for Microsoft Windows displays an error message in the job session and error or warning messages issued during script execution.



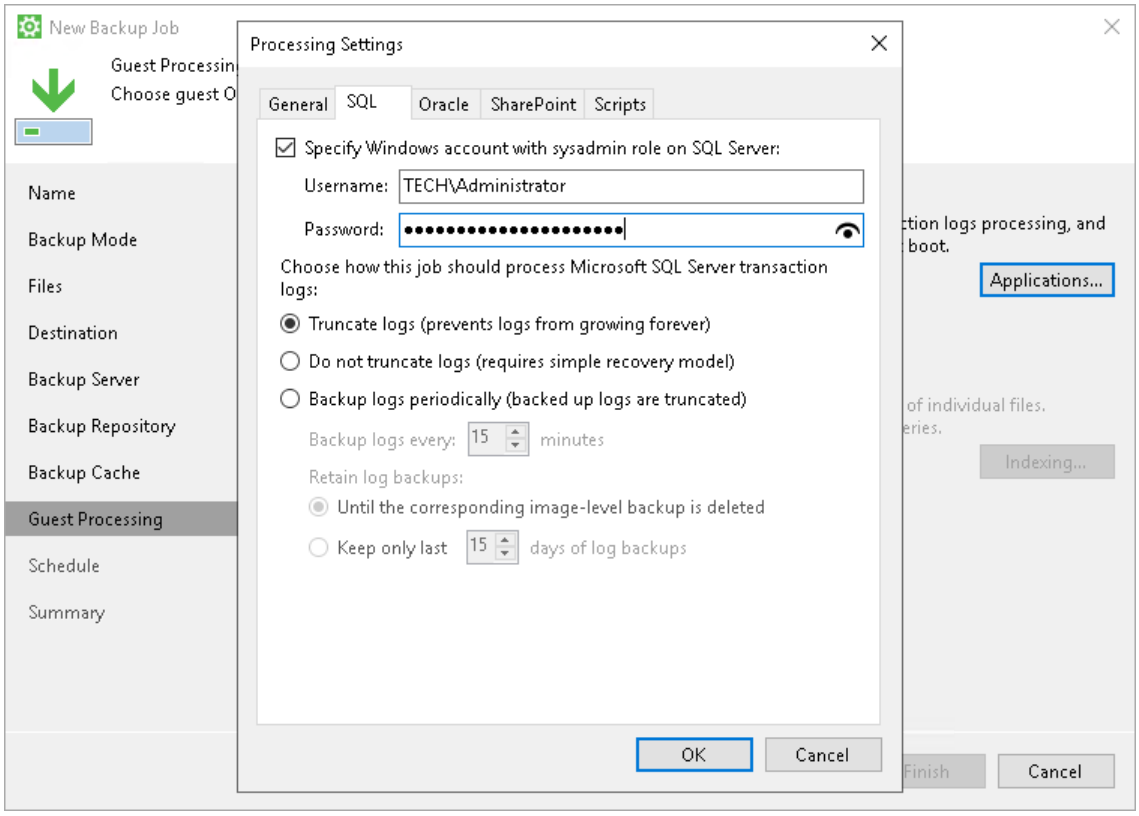
Limitations for Pre-Freeze and Post-Thaw Scripts

Veeam Agent for Microsoft Windows has one limitation for pre-freeze and post-thaw scripts: you cannot stop a job when the pre-freeze or post-thaw script is executed. If the script hangs up, Veeam Agent for Microsoft Windows waits for 10 minutes and then continues running the job depending on the script processing mode.

Transaction Log Truncation

If you back up database systems that use transaction logs, for example, Microsoft SQL Server, you can instruct Veeam Agent for Microsoft Windows to truncate transaction logs so that logs do not overflow the storage space. Veeam Agent for Microsoft Windows provides the following options of transaction logs handling:

- Truncate logs
- Do not truncate logs
- Back up logs periodically



Truncate Logs

You can instruct Veeam Agent for Microsoft Windows to truncate logs after a backup is successfully created. With this option selected, Veeam Agent for Microsoft Windows behaves in the following way:

- If the backup job completes successfully, Veeam Agent for Microsoft Windows produces a backup file and truncates transaction logs on the Veeam Agent computer. As a result, you have the backup file that contains a computer image, image of a specific data volume or individual folders at a specific point in time.

  In this scenario, you can recover a database to the point in time when the backup file was created. As transaction logs on the Veeam Agent computer are truncated, you cannot use them to get the restored database to some point in time between backup job sessions.

- If the backup job fails, Veeam Agent for Microsoft Windows does not truncate transaction logs on the Veeam Agent computer. In this scenario, you can restore computer data from the most recent point in the backup and use database system tools to apply transaction logs and get the database system to the necessary point in time after the restore point.

Do not Truncate Logs

You can choose not to truncate transaction logs. We recommend this option if you use another backup tool together with Veeam Agent for Microsoft Windows.

For example, you can use Veeam Agent for Microsoft Windows to create a computer image backup and instruct the native Microsoft SQL Server log backup job to back up transaction logs. If you truncate transaction logs with Veeam Agent for Microsoft Windows, the chain of transaction logs will be broken, and the Microsoft SQL Server log backup job will not be able to produce a consistent log backup.

With this option selected, Veeam Agent for Microsoft Windows produces a backup file and does not trigger transaction log truncation. As a result, you have a backup file that contains a computer image, image of a specific data volume or individual folders captured at a specific point in time, and transaction logs. You can use transaction logs to restore the Veeam Agent computer to any point in time between job sessions. To do this, you must recover data from the backup file and use database system tools to apply transaction logs and get the database system to the necessary point in time.

Back Up Logs Periodically

This option can be used if you back up Microsoft SQL Server or Oracle database system.

You can choose to back up database logs with Veeam Agent for Microsoft Windows. With this option selected, Veeam Agent for Microsoft Windows creates a backup and additionally copies Microsoft SQL Server transaction logs or Oracle archived logs and saves them to the backup location next to the backup files. To learn more, see Microsoft SQL Server and Oracle Logs Backup.

In this scenario, you can use transaction logs to restore the Veeam Agent computer to any point in time between backup job sessions. To do that, you must recover data from the Veeam Agent backup and use Veeam Explorer for Microsoft SQL Server or Veeam Explorer for Oracle to perform transaction log replay and get the database system to a necessary point in time.

Copy Only Backup

Some organizations prefer to back up Microsoft SQL Server databases and transaction logs with native Microsoft SQL Server tools or 3rd party backup tools. To restore database systems in a proper way, database administrators must be sure that they have database backups and a sequence of transaction log backups associated with these backups at hand.

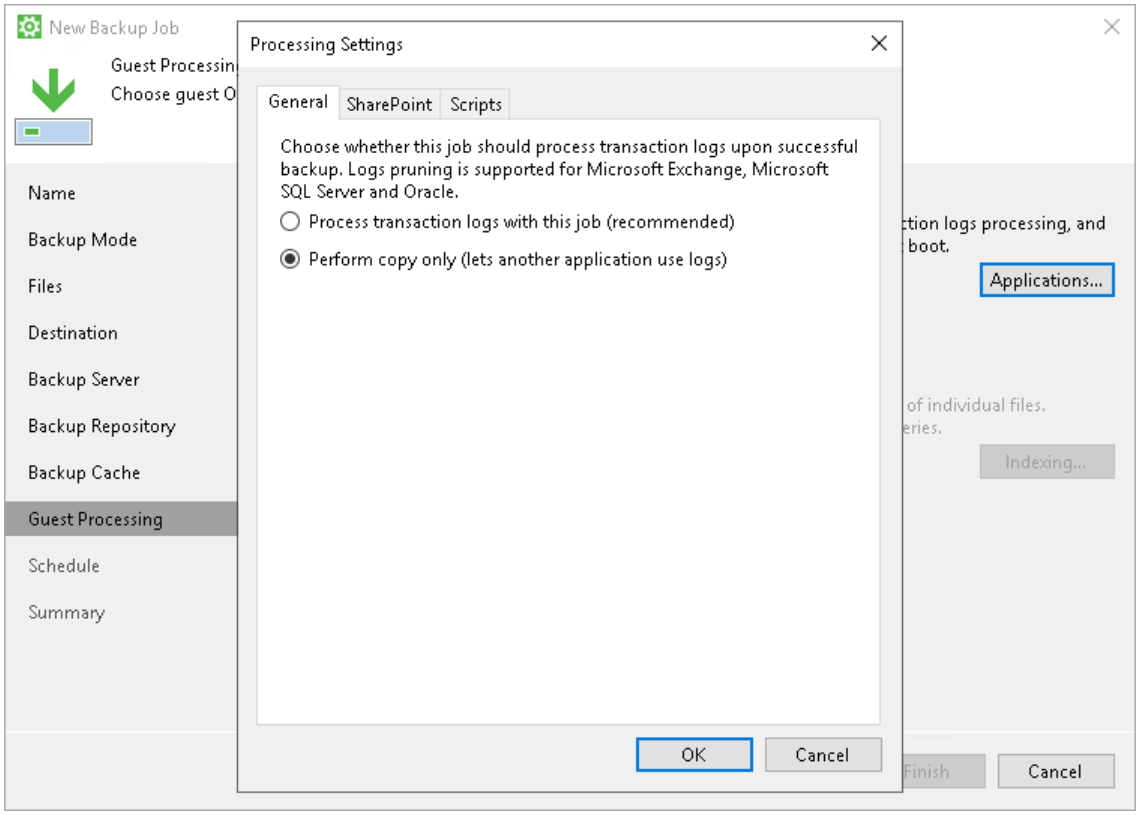
If you use native Microsoft SQL Server tools or 3rd party backup tools and also want to back up a machine that runs Microsoft SQL Server with Veeam Agent for Microsoft Windows, you must enable the **Perform copy only** option in the backup job settings.

The **Perform copy only** option indicates that a chain of database backups is created with native Microsoft SQL Server means or by a 3rd party tool, and instructs Veeam Agent to preserve this chain (backup history). If the **Perform copy only** option is enabled, Veeam Agent produces the backup of the Copy Backup type that is independent of the existing chain of database backups and does not contain transaction log data. As a result, the backup does not change the log sequence number and transaction log backup time. To learn more about Copy Backup and other VSS backup types, see this Microsoft article.

IMPORTANT

Consider the following:

- Veeam Agent for Microsoft Windows does not truncate transaction logs after copy-only backup. For this reason, if you instruct the backup job to perform copy-only backup, you cannot specify transaction log handing settings for this job.
- Veeam Agent for Microsoft Windows supports one transaction log backup job per Veeam Agent computer. If you plan to configure several backup jobs using Veeam Agent for Microsoft Windows, you can enable database log backup settings for one job only.



Microsoft SQL Server and Oracle Logs Backup

NOTE

This and subsequent sections describe application-aware processing of Microsoft SQL Server and Oracle database systems in Veeam Agent for Microsoft Windows. You can perform item-level recovery of Microsoft SQL Server and Oracle systems if you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication. For more information, see Veeam Backup & Replication Documentation.

Microsoft SQL Server Log Backup

You can instruct the Veeam Agent backup job to create volume level or file-level backups and also periodically back up database transaction logs. If Microsoft SQL Server fails, you can restore Microsoft SQL Server from the necessary restore point of the Veeam Agent backup. If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you can also use Veeam Explorer for Microsoft SQL Server to apply transaction logs and get databases on the Microsoft SQL Server to the necessary state between backups.

Requirements for Microsoft SQL Server Transaction Log Backup

- Veeam Agent for Microsoft Windows supports transaction log backups for the following systems:
  - Microsoft SQL Server 2022
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2017
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014 SP2
  - Microsoft SQL Server 2012 SP3
  - Microsoft SQL Server 2008 R2 SP3
  - Microsoft SQL Server 2008 SP4
- The database whose logs you want to back up must use the *Full* or *Bulk-logged* recovery model. In this case, all changes of the Microsoft SQL Server state will be written to transaction logs, and you will be able to replay transaction logs to restore the Microsoft SQL Server. You can use the Microsoft SQL Server Management Studio to switch to one of these models. For more information, see this Microsoft article.

Oracle Log Backup

Veeam Agent for Microsoft Windows supports backup of Oracle database archived logs. If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you can use Veeam Explorer for Oracle to apply archived logs and get Oracle databases to the necessary state between backups.

Database archived logs are created by the Oracle system. The Oracle database can run in one of the following logging modes:

- ARCHIVELOG turned on — logs are saved and can be used for recovery purposes.
- ARCHIVELOG turned off — no archived logs are saved. We do not recommend this mode, because it does not provide proper disaster recovery.

With ARCHIVELOG turned on, the Oracle system stores database archived logs in a certain location on the machine that runs the database system, as specified by the database administrator. Veeam Agent for Microsoft Windows allows you to set up the following ways of log handling:

- Instruct the backup job to collect log files from the Oracle system and ship them to the backup location where they are stored next to regular backup files created by Veeam Agent for Microsoft Windows.
- Skip log processing — log files remain untouched and are preserved within the Veeam Agent backup.

If you enable application-aware processing for Oracle, during the job session Veeam Agent for Microsoft Windows collects information about the database and processes archived logs according to job settings. Application-specific settings are configured at the **Guest Processing** step of the **New Backup Job** wizard — you can specify how logs should be managed for Oracle databases.

Requirements for Oracle Archived Log Backup

- Veeam Agent for Microsoft Windows supports archived log backup and restore for Oracle database version 11.2 and later.
- Automatic Storage Management (ASM) is not supported.
- The database must run in the ARCHIVELOG mode.

Database Log Backup Job

To back up database logs (Microsoft SQL Server transaction logs and Oracle archived logs), you must specify advanced settings for transaction log backup in the Veeam Agent backup job settings. The resulting job will comprise two jobs:

- Parent backup job — the backup job that creates a volume-level or file-level backup. The backup job becomes the parent job after you enable database log backup options at the **Guest Processing** step of the **New Backup Job** wizard.
- Child job — a transaction log backup job. Veeam Agent for Microsoft Windows automatically creates the child job if transaction log backup is enabled for the backup job. Session data of the transaction log backup job is stored in the Veeam Agent for Microsoft Windows database and displayed in the Veeam Agent control panel. To learn more, see Transaction Log Backup Statistics.

The parent job runs in a regular manner — it starts by schedule or is started manually by the user. The transaction log backup job is triggered by the parent backup job. This sequence ensures that the restore point is present when it comes to transaction log replay.

> **NOTE**
>
> Veeam Agent for Microsoft Windows supports one transaction log backup job per Veeam Agent computer. If you plan to configure several backup jobs using Veeam Agent for Microsoft Windows, you can enable database log backup settings for one job only.

Sessions of Transaction Log Backup Jobs

The transaction log backup job runs permanently in the background, shipping transaction logs to the backup location at a specific time interval (by default, every 15 minutes). A sequence of time intervals between sessions of the parent backup job makes up a session of the transaction log backup job.

The transaction log backup session starts and stops in the following way:

- The initial session starts when the parent backup job schedule is enabled. After that, the session starts with every new session of the parent backup job.
- The session ends before the next session of the parent backup job or when this parent backup job is disabled.

How Microsoft SQL Server Log Backup Works

The transaction log backup for Microsoft SQL Server is performed in the following way:

1. Veeam Agent for Microsoft Windows launches the parent backup job by schedule.
2. The parent backup job creates a volume-level or file-level backup and stores it to the backup location.

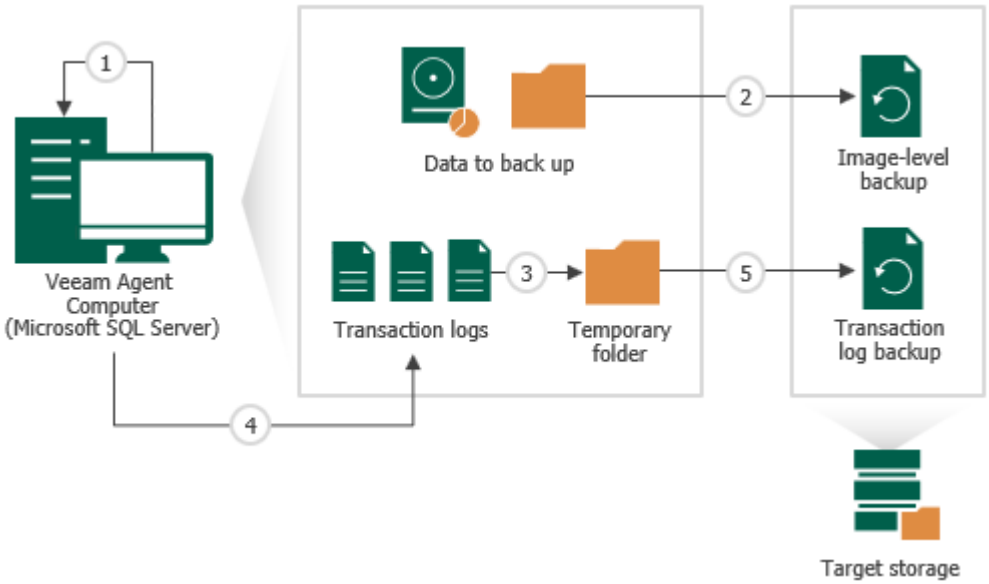
3. A new session of the transaction log backup job starts. Veeam Agent for Microsoft Windows copies transaction log files from the log archive destination (set by the Microsoft SQL Server administrator) to a temporary folder on the Veeam Agent computer file system.
4. Veeam Agent for Microsoft Windows detects what databases currently exist on the Microsoft SQL Server and maps this data with the information kept in the Veeam Agent for Microsoft Windows database. This periodic mapping reveals the databases for which Veeam Agent for Microsoft Windows must process transaction logs during this time interval.
5. Veeam Agent for Microsoft Windows transports transaction log backup copies from the temporary folder to the backup location and saves them as VLB files. As soon as copies of transaction log backups are saved to the backup location, transaction log backups in the temporary folder on the Veeam Agent computer are removed.

> **TIP**
>
> Default location of the temporary folder where Veeam Agent copies transaction log files to is `C:\ProgramData\Veeam\Endpoint\SqlLogBackup`. If it is necessary to change the location, you can use a registry value. To learn more, see this Veeam KB article.

The session of the transaction log backup job remains working until the next start of the parent backup job. When a new session of the parent job starts, the transaction log backup job stops the current session and then starts a new session, performing steps 1–5.

Transaction logs that for some reason were not processed during the log backup interval remain in the temporary folder and are processed during the next log backup interval. To detect these remaining logs, Veeam Agent for Microsoft Windows enumerates log files in the temporary folder.

> **NOTE**
>
> If a new session of the transaction log backup starts and the parent backup job has not created a new restore point yet, the transaction log backup job will remain in the idle state, waiting for a new restore point to be created.



How Oracle Archived Log Backup Works

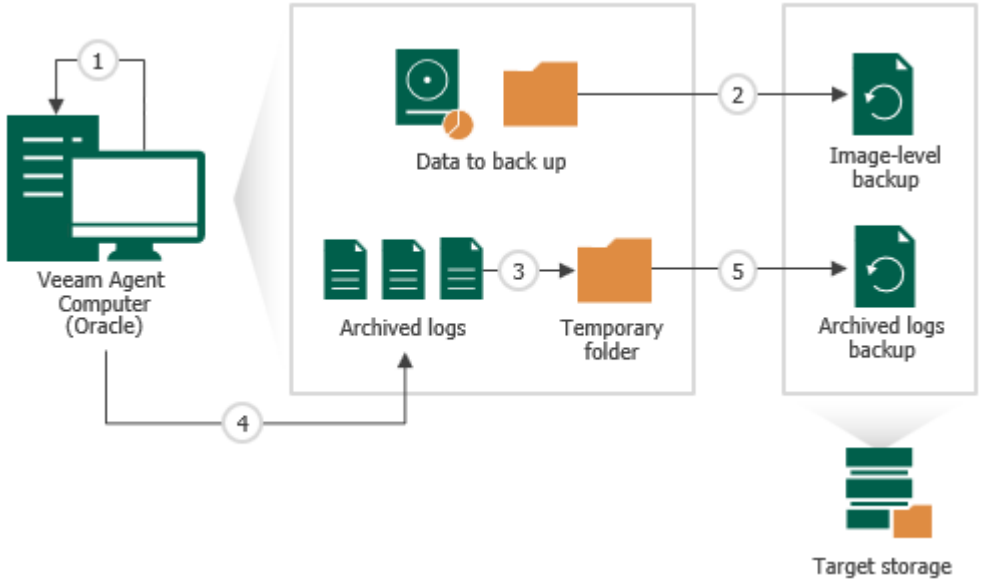
The archived log backup for Oracle is performed in the following way:

1. Veeam Agent for Microsoft Windows launches the parent backup job by schedule.
2. The parent backup job creates a volume-level or file-level backup and stores it to the backup location.
3. A new session of the archived log backup starts. Veeam Agent for Microsoft Windows scans the Oracle system and collects information about databases whose logs must be processed, including:
   - List of all databases
   - Database state — a database is on or off, in which logging mode it runs
   - Paths to all database files (configuration logs and so on) and other data required for backup

   Veeam Agent for Microsoft Windows copies archived log files from the log archive destination (set by the Oracle administrator) to a temporary folder on the Veeam Agent computer.
4. Veeam Agent for Microsoft Windows maps information about the Oracle system collected at the step 3 with information kept in the Veeam Agent for Microsoft Windows database. This periodic mapping helps reveal databases for which Veeam Agent for Microsoft Windows must ship archived logs to the backup location during this time interval.
5. Archived log backup files are transferred from the temporary folder on the Veeam Agent computer to the backup location.

Archived logs that for some reason were not processed during the log backup interval remain in the temporary folder and are processed during the next log backup interval. To detect these remaining logs, Veeam Agent for Microsoft Windows enumerates log files in the temporary folder.

> **NOTE**
>
> If a new session of the archived log backup starts and the parent backup job has not created a new restore point yet, the transaction log backup job will remain in the idle state, waiting for a new restore point to be created.



Retention for Database Log Backups

Transaction log backups are stored in files of the proprietary Veeam format — VLB. Veeam Agent for Microsoft Windows keeps transaction log backups together with the chain of backup files on the target location.

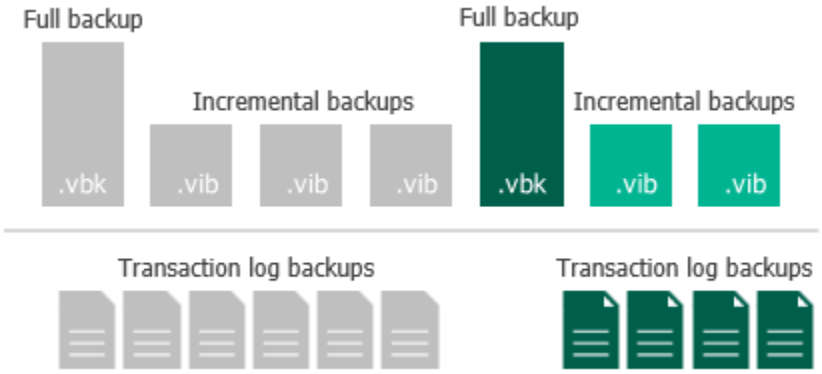
Veeam Agent for Microsoft Windows removes transaction log backups by retention. You can choose one of the following retention methods:

- Retain logs according to the image-level backup
- Retain logs for the specified number of days

Retain Logs with Image-Level Backup

By default, Veeam Agent for Microsoft Windows retains transaction log backups together with the corresponding backup file. When Veeam Agent for Microsoft Windows removes a restore point from the backup chain, it also removes a chain of transaction logs relating to this restore point.

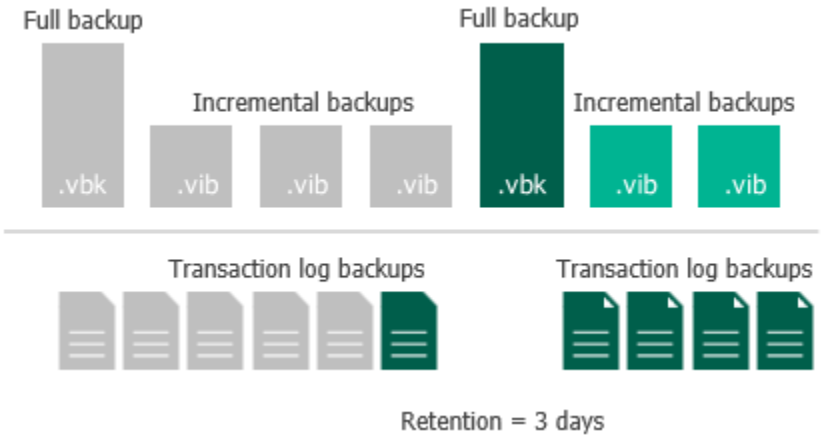
This method allows you to have both the file-level or volume-level backup and necessary transaction log backups at hand. If you need to recover a database to some state, you can restore a machine running Microsoft SQL Server or Oracle from the necessary restore point and perform transaction log replay to bring the database to the desired state.



Retain Logs for a Number of Days

You can instruct Veeam Agent for Microsoft Windows to keep transaction logs only for a specific period of time. This retention setting can be used, for example, if you want to save on storage space and plan to retain transaction log backups for the last few days. In this case, you will be able to perform transaction log replay only to one of the most recent states.

If you select this retention method, you must make sure that retention policies for the Veeam Agent backup and transaction log backup are consistent. The restore point of the volume-level or file-level backup must always be preserved. If a backup of the database itself is missing, you will not be able to perform transaction log replay.

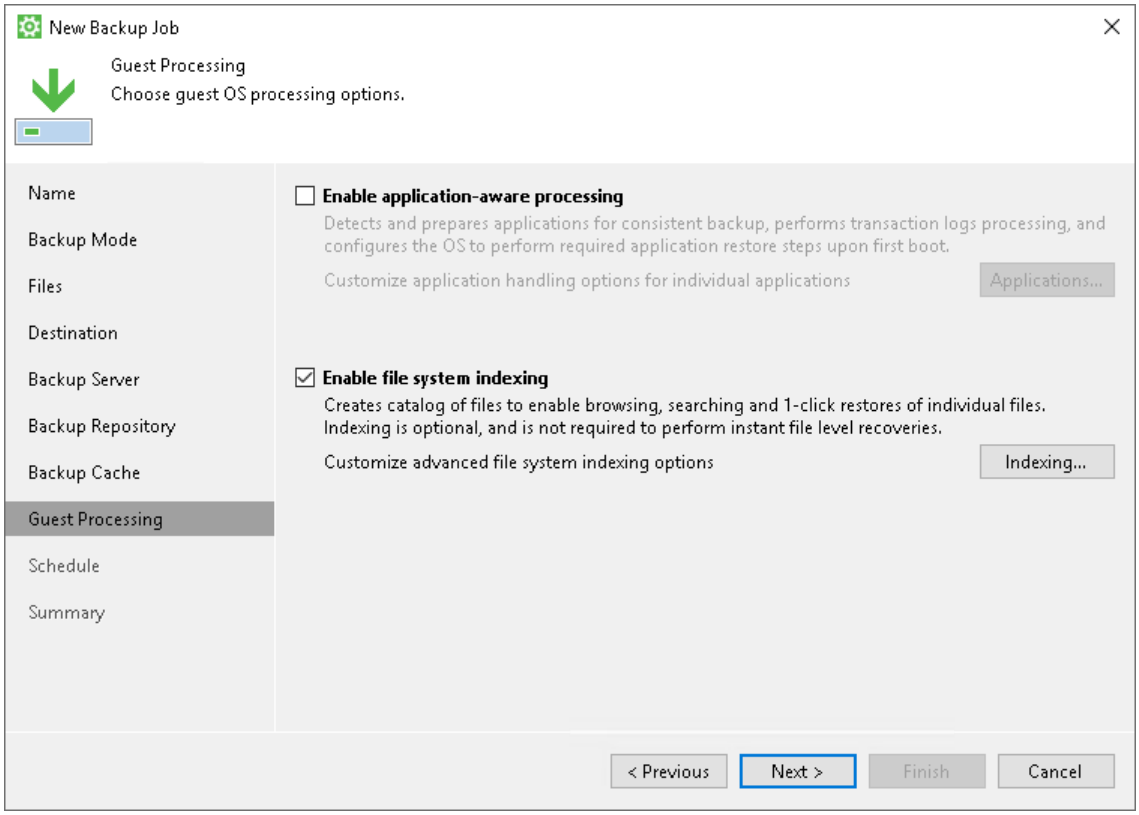


File System Indexing

You can instruct Veeam Agent for Microsoft Windows to create an index of files and folders on the Veeam Agent computer OS during backup. If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you will be able to search for individual files inside Veeam Agent backups and perform 1-click restore in Veeam Backup Enterprise Manager.

NOTE

File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the Preparing for File Browsing and Searching section in the Veeam Backup Enterprise Manager User Guide.



How File Indexing Works

When you run a backup job with the file indexing option enabled, Veeam Agent for Microsoft Windows performs the following operations:

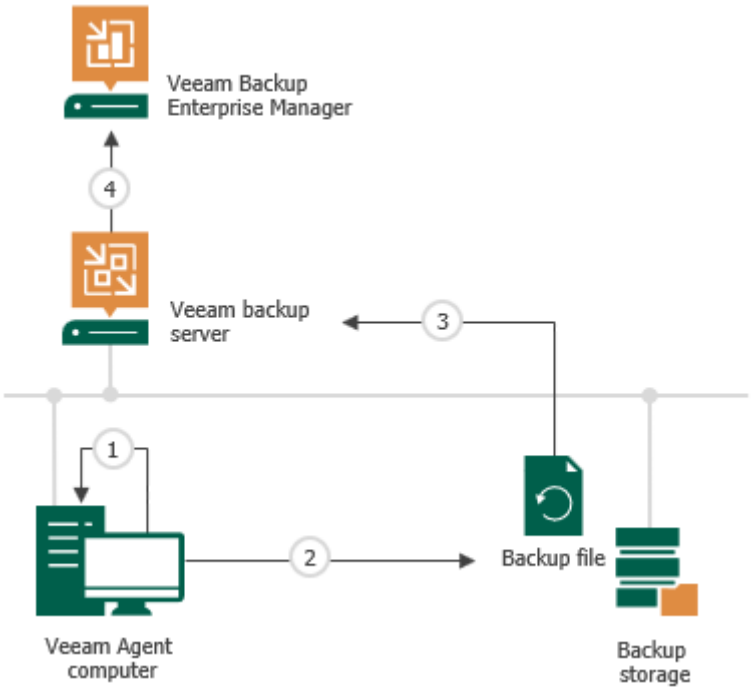
1. When the backup job starts, Veeam Agent for Microsoft Windows starts indexing the file system. The indexing procedure is carried out in parallel with the backup procedure. If indexing takes long, Veeam Agent for Microsoft Windows will not wait for the indexing procedure to complete. It will start copying data to the target location and continue file indexing.
2. When file indexing is complete, Veeam Agent for Microsoft Windows collects indexing data, writes it to an archive file and stores this archive file to the backup file along with the backed-up data.
3. If the backup job is set up to create backups in a Veeam backup repository, when the job completes, Veeam Guest Catalog Service running on the backup server also saves indexing data in the Veeam Catalog folder on the backup server.

   To learn more about the Veeam Guest Catalog Service, see the Veeam Backup Catalog section in the Veeam Backup & Replication User Guide.
4. During the next catalog replication session, the global Veeam Guest Catalog Service replicates data from the backup server to the Veeam Catalog folder on the Veeam Backup Enterprise Manager server.

NOTE

Consider the following:

- If the backup job is set up to create backups in a Veeam Cloud Connect repository, Veeam Backup & Replication running on the SP backup server does not save indexing data in the Veeam Catalog folder.
- Due to the peculiarities of file indexing algorithms, file indexing takes more time if you backup volumes with a file system different from NTFS or volumes with data deduplication enabled.



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.

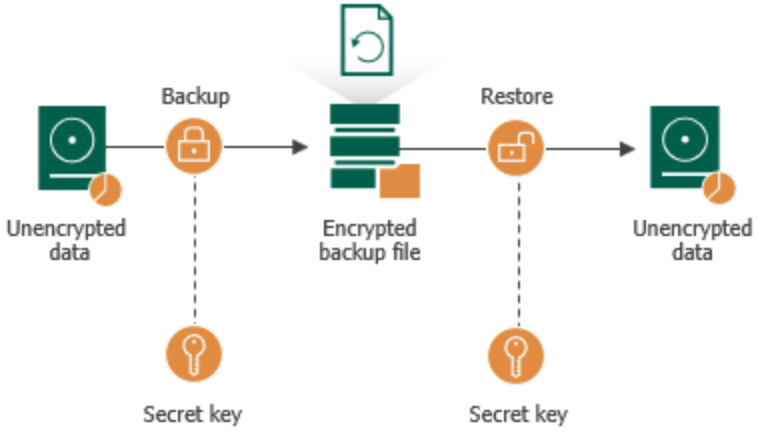
To create encrypted backups, you must enable the encryption option and specify a password that will be used for data encryption. To learn more, see Storage Settings.

> **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.

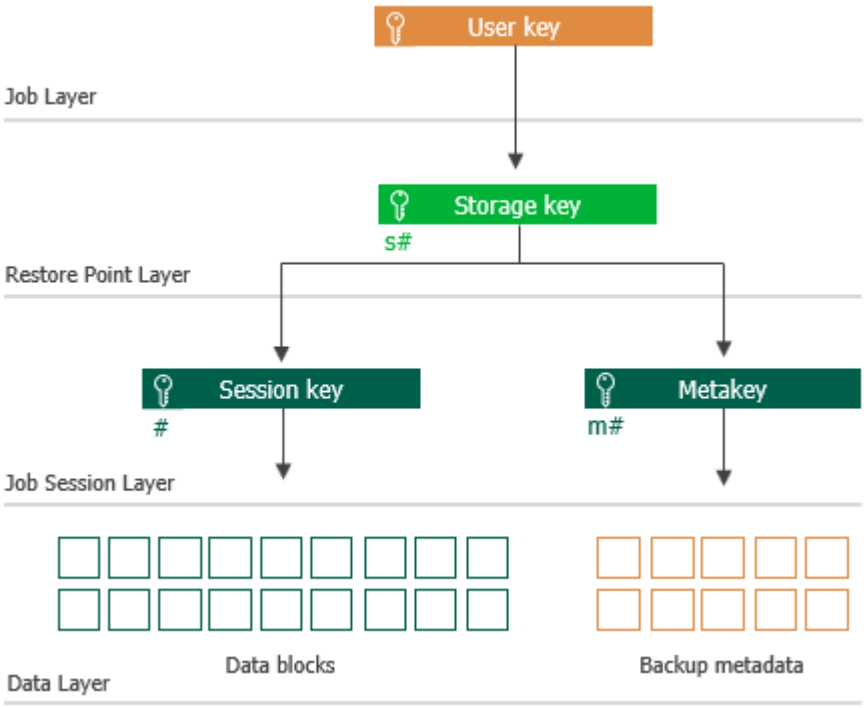
Encryption Algorithms

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.

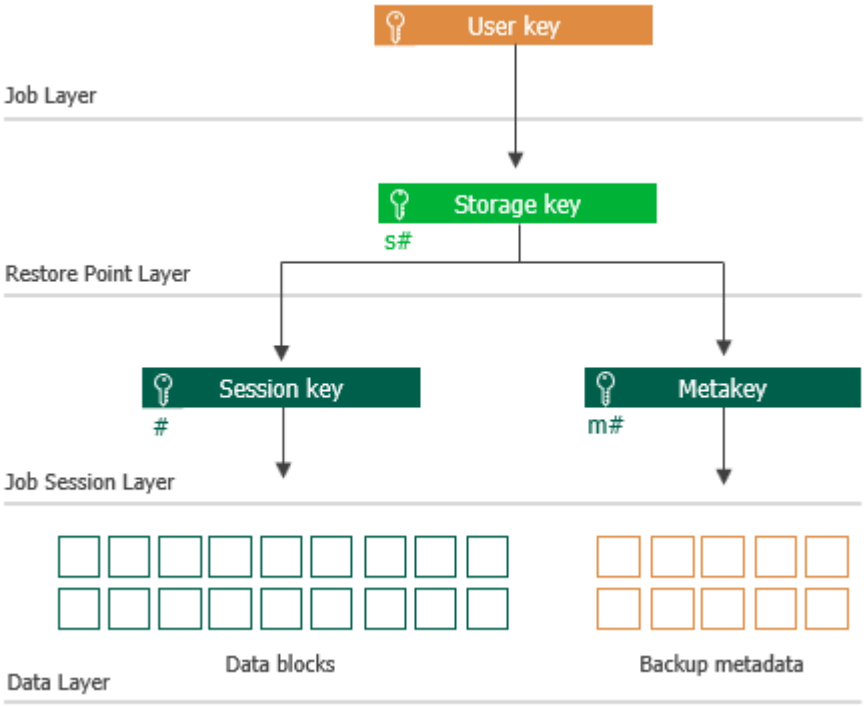

User key
Job Layer
Storage key
s#
Restore Point Layer
Session key
#
Metakey
m#
Job Session Layer
Data blocks
Backup metadata
Data Layer

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.

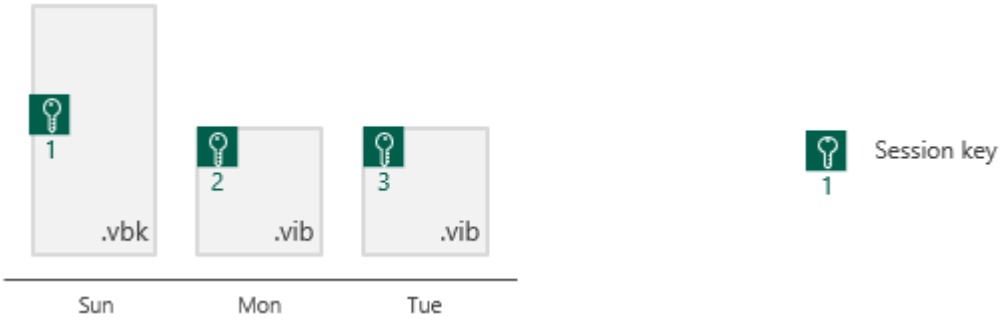


Session Keys and Metakeys

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.

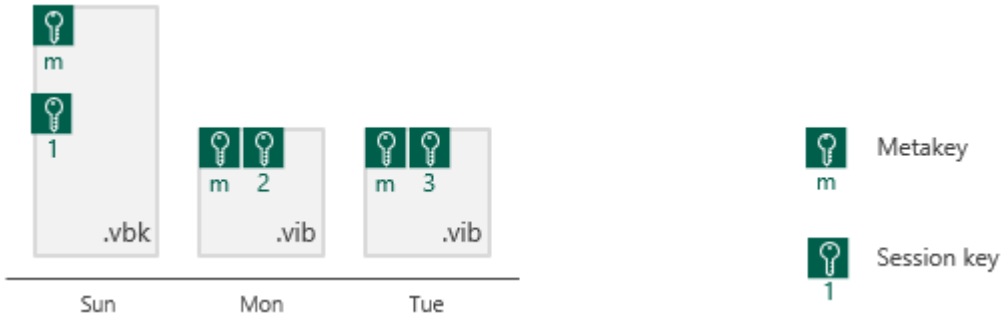
Veeam Agent generates a new session key for every backup job session. For example, if you have created an encrypted backup job and run 3 job sessions, Veeam Agent will produce 3 backup files that will be encrypted with 3 different session keys:

- 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.

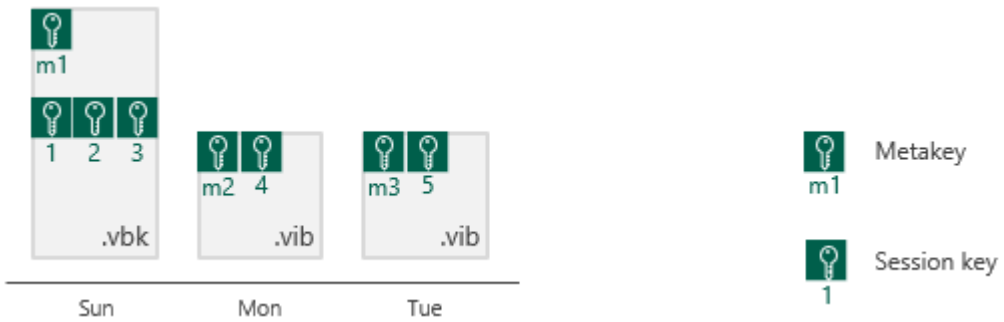


In the encryption process, session keys and metakeys are encrypted with keys of a higher layer — storage keys. Cryptograms of session keys and metakeys are stored in the resulting file next to encrypted data blocks. Metakeys are additionally kept in the Veeam Agent database.

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.

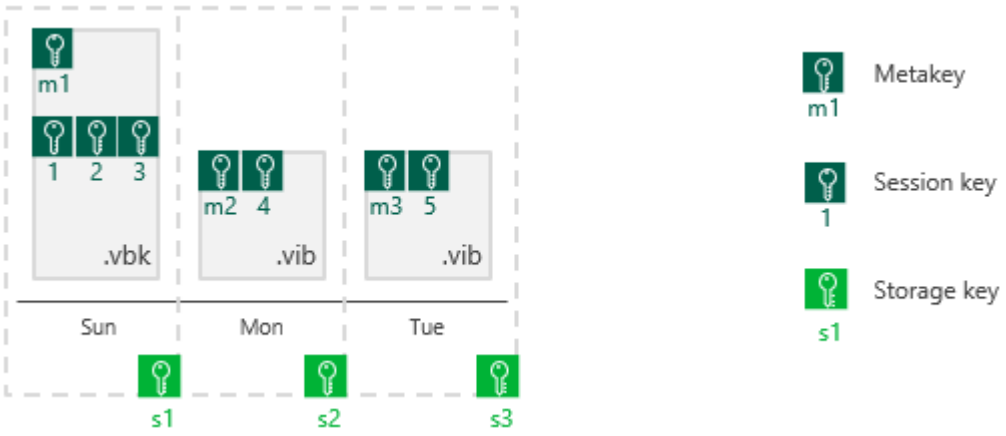
To restore data from such "composed" backup file, Veeam Agent would require a bunch of session keys. For example, if the backup chain contains restore points for 2 months, Veeam Agent would have to keep session keys for a 2-month period.



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.

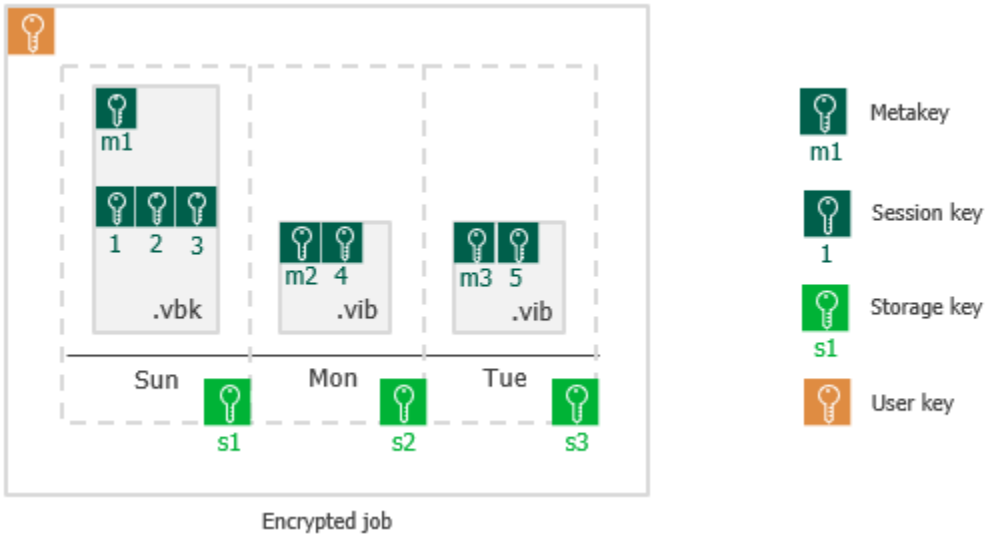
In the encryption process, storage keys are encrypted with a key of a higher layer — a user key. Cryptograms of storage keys are stored in the resulting file next to encrypted data blocks, and cryptograms of session keys and metakeys.

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.

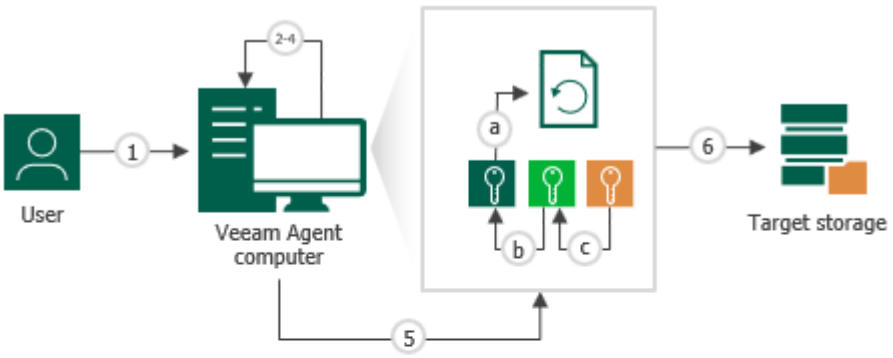
According to the security best practices, you should change passwords for encrypted jobs regularly. When you change a password for the job, Veeam Agent creates a new user key and uses it to encrypt new restore points in the backup chain. If you lose a password that was specified for encryption, you can 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.

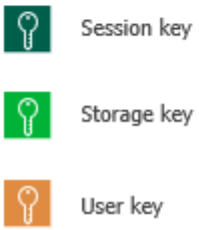
How Data Encryption Works

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.





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 in one of the following situations:

  - You encrypt and decrypt the backup file on the same Veeam Agent computer using the same Veeam Agent database.
  - You have included encryption keys into the Veeam Recovery Media and perform bare metal recovery after booting from this Veeam Recovery Media. To learn more, see Specify Recovery Media Options.

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

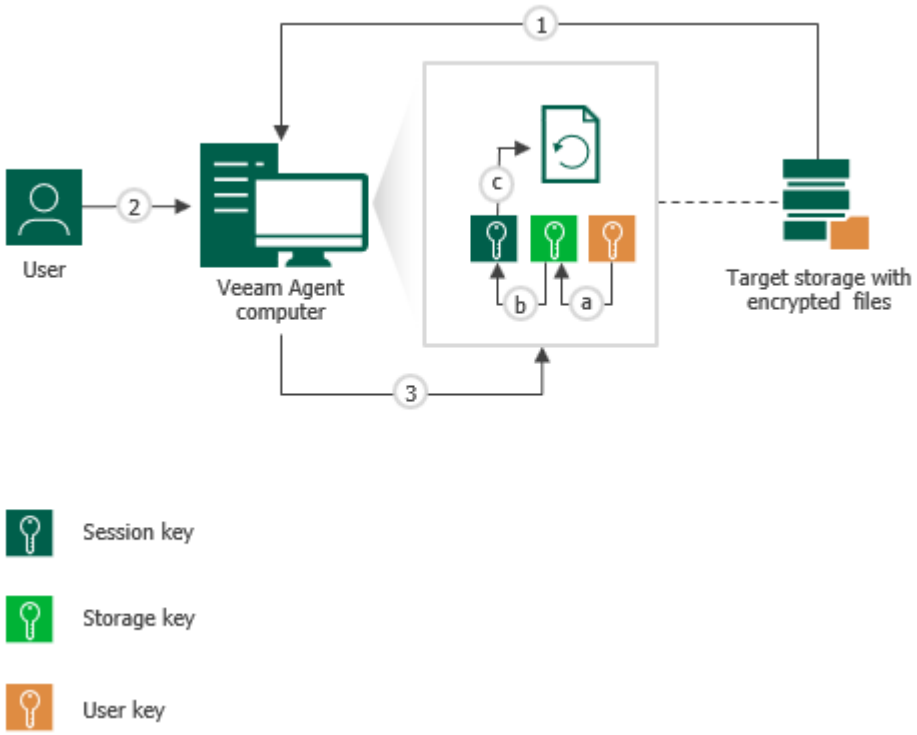
Data decryption is performed on the source or target side depending on the backup target. As a result, encryption keys are not passed to the untrusted side, which helps avoid data interception.

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.

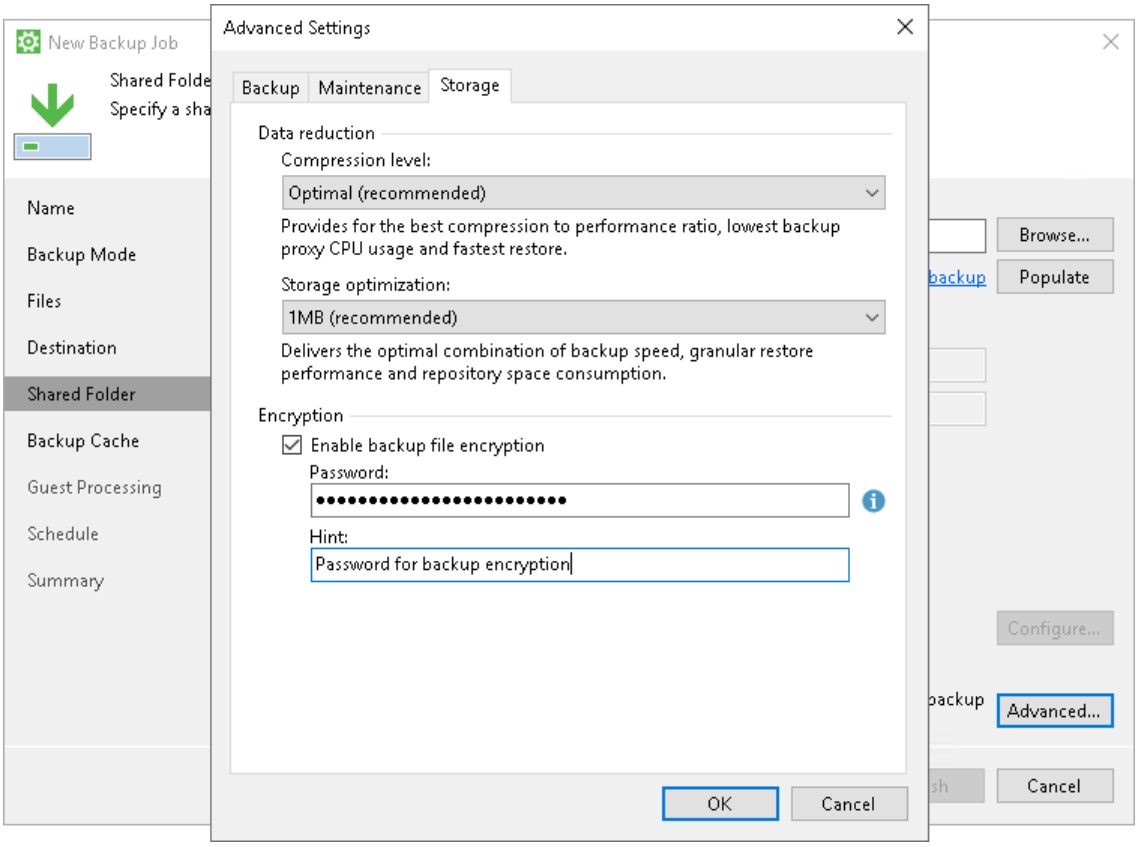
After the encrypted file is unlocked, you can work with it as usual.



Backup Job Encryption

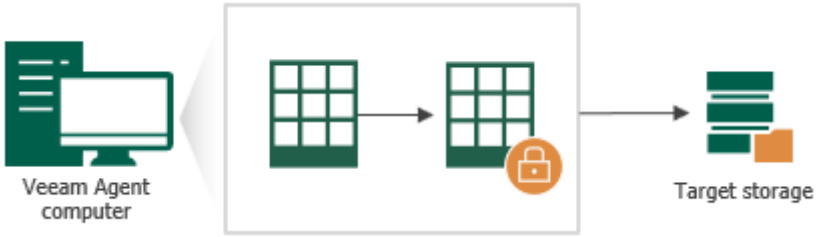
Encryption for the backup job is configured in the advanced job settings. You should enable the encryption option and specify a password to protect data in backup files produced by the backup job.

> **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.



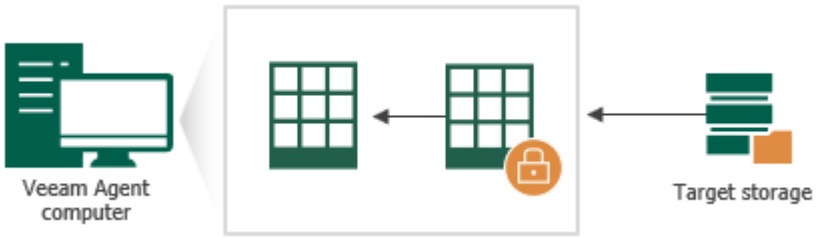
The backup job processing with encryption enabled includes the following steps:

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.



Resuming Encrypted Backup Chain

In some situations, encryption keys may be unavailable in the Veeam Agent for Microsoft Windows database, and Veeam Agent cannot create a new encrypted restore point in the backup chain. For example, this may happen after you change the password for encryption and then recover the entire Veeam Agent computer to a restore point that was created before you have changed the password. In this case, information about backup in the Veeam Agent database will become outdated and will not match backup metadata residing on the target location. To continue the existing encrypted backup chain, you need to provide the latest password in the Veeam Agent control panel.

When the backup job is started (either manually or upon the defined schedule), Veeam Agent detects the latest encrypted backup created by this job in the target location and displays a window in the Veeam Agent control panel offering to enter a password and continue the backup chain. You can choose to perform one of the following operations:

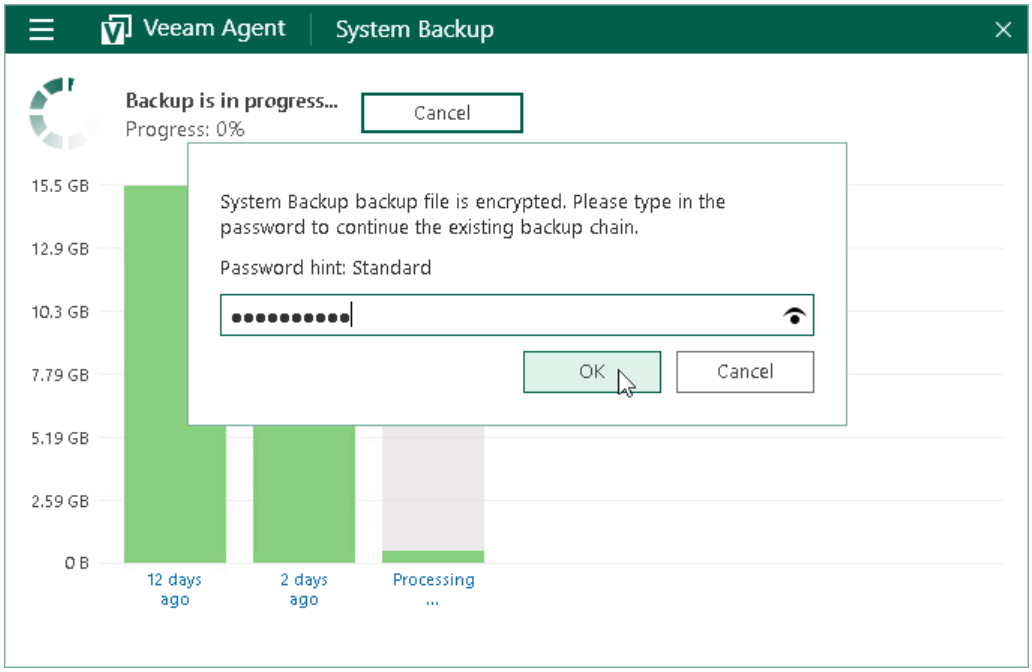
- To continue the existing encrypted backup chain, you can enter the password specified for encryption and click **OK**. If the password has changed more than once, you need to specify the latest password.

  After you provide the correct password, Veeam Agent will use this password to decrypt backup metadata on the target location and update information about backup in its database. After that, Veeam Agent will create the new incremental backup file in the existing encrypted backup chain. To encrypt this backup file and subsequent backup files, Veeam Agent will use the password that is kept in its database at the time when continue the backup chain.

  You will be able to use this password to restore data from any restore point in the backup chain, including restore points that were encrypted with an older password and restore points that were created before you have enabled the encryption option for the job.

- You can click **Cancel** to close the notification window and cancel the job. In this case, the next time the backup job is started, Veeam Agent will again prompt to enter the password.

> **NOTE**
>
> Veeam Agent for Microsoft Windows displays the notification window for 1 hour. If you do not choose any option, after this time period expires, Veeam Agent will automatically close the window and cancel the job. If email notification settings are enabled for the backup job, Veeam Agent will also send an email report informing that the job was canceled.



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 Cache

A remote storage specified as a target location for backup files may be unavailable at the time when the backup job must start. In this case, Veeam Agent cannot create a regular restore point upon the defined schedule. As a result, the backup chain on the remote storage will not contain a sequence of restore points that precisely complies with the backup schedule.

To overcome this limitation, Veeam Agent offers the concept of the backup cache. The backup cache is a temporary local storage in which Veeam Agent creates backup files in case the backed-up data cannot be transferred to a remote location. When the target location becomes available, Veeam Agent uploads backup files from the backup cache to the remote storage, adding regular restore points to the backup chain.

The backup cache lets you perform scheduled backup in due time ensuring that the resulting backup chain will contain "snapshots" of your data at desired points in time. This may be helpful, for example, for laptop users who go on business trips with no or limited access to the corporate network in which the backup location resides.

Technically, the backup cache is a local folder on the computer on which Veeam Agent is installed. A user can define a folder for the backup cache and the size of the backup cache in the backup job settings.

The backup cache is available if the following types of storage are chosen as a target location:

- Network shared folder
- Object storage
- Backup repository managed by a Veeam backup server
- Cloud repository managed by a Veeam Cloud Connect service provider

How Backup Cache Works

When you create a backup job targeted at a remote storage, you can select to use the backup cache in its properties. The procedure of data backup with the backup cache enabled is performed in the following way:

1. The user enables the backup cache in the properties of the backup job targeted at a remote location.
2. During a regular backup job session, Veeam Agent for Microsoft Windows creates in the backup cache a map of data blocks on the remote location. Information about data blocks on the remote location is saved in a file with digests and stored in the folder `C:\ProgramData\Veeam\EndpointData\CacheDigests`.

   Veeam Agent for Microsoft Windows will use the created digests to create incremental backup files in the backup cache when the remote storage itself is unavailable at the time of scheduled backup.
3. If the target location is unavailable at the time when the scheduled backup job must start, Veeam Agent for Microsoft Windows creates the new restore point in the backup cache.

   The target location is considered as unavailable in the following conditions:

   - [For network shared folder] Veeam Agent for Microsoft Windows Service that runs on the protected computer cannot connect to the network shared folder. In this case, Veeam Agent for Microsoft Windows will immediately start creating the new restore point in the backup cache.
   - [For object storage] Veeam Agent for Microsoft Windows Service that runs on the protected computer cannot connect to the object storage.

- [For Veeam backup repository] Veeam Agent for Microsoft Windows Service cannot connect to the Veeam Backup Service that runs on the backup server to which the backup repository specified as a target location for Veeam Agent backups is connected.
- [For Veeam Cloud Connect repository] Veeam Agent for Microsoft Windows Service cannot connect to one of the following services on the Veeam Cloud Connect provider side:
  - *Veeam Backup Service* that runs on the backup server used for managing the Veeam Cloud Connect infrastructure.
  - *Veeam Cloud Connect Service* that runs on the backup server used for managing the Veeam Cloud Connect infrastructure.
  - *Veeam Cloud Gateway Service* that runs on a cloud gateway deployed in the Veeam Cloud Connect infrastructure.

In case the connection to the target location is lost when the backup job is already running, Veeam Agent for Microsoft Windows performs backup based on the following rules:

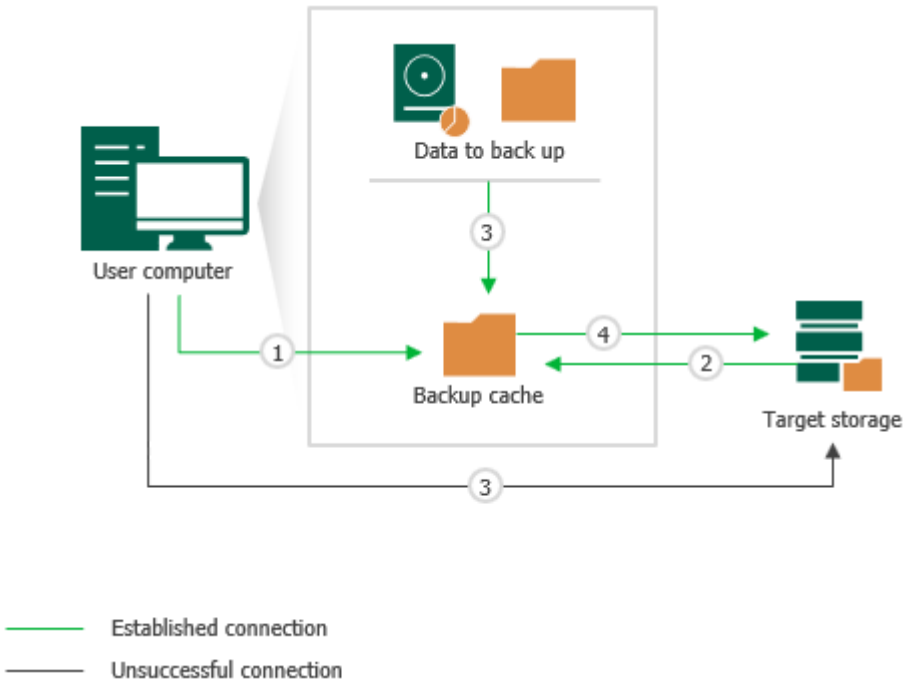
- [For network shared folder] Veeam Agent for Microsoft Windows immediately switches to the backup cache and writes to the backup cache all data that must be backed up within the current backup job session. If some data has already been transferred to the target location, Veeam Agent for Microsoft Windows starts the data transfer operation from the beginning and transfers all backed-up data to the backup cache.
- [For object storage, Veeam backup repository and Veeam Cloud Connect repository] Veeam Agent for Microsoft Windows tries to reconnect to the target location. The reconnection process may last 30 minutes or more. After the reconnection period expires, Veeam Agent for Microsoft Windows switches to the backup cache and writes to the backup cache only remaining data that has not been transferred to the target location yet. Data that has been already transferred to the target location remains in the backup repository.

The process of data backup to the backup cache practically does not differ from the regular one. The difference is that the resulting backup file is saved to the local folder instead of the remote storage.

If the target location becomes available after Veeam Agent for Microsoft Windows has started creating a restore point in the backup cache, Veeam Agent for Microsoft Windows will not switch back to the target location. Instead, Veeam Agent for Microsoft Windows will create a restore point in the backup cache and then upload this restore point to the target location.

4. After the remote storage becomes available, Veeam Agent for Microsoft Windows uploads backup files that were created in the backup cache to the target location. If more than one restore point was created in the backup cache, these restore points are uploaded to the target location sequentially, one by one.

   Until all restore points are uploaded from the backup cache to the target location, Veeam Agent for Microsoft Windows will continue to create new restore points in the backup cache even if the target location is available at the time when the backup job is running.



Limitations for Backup Cache

The backup cache has the following limitations:

- The backup cache is available only in Workstation and Server editions of Veeam Agent for Microsoft Windows.
- You cannot use the backup cache for a file-level backup job.
- You cannot restore data from backup files that reside in the backup cache. Until restore points are uploaded from the backup cache to the target location, these restore points are not considered as a fully valid part of the backup chain.
- Veeam Agent for Microsoft Windows does not support creating full backups (including active full backups and synthetic full backups) in the backup cache except for the very first full backup file in the backup chain.
- Veeam Agent for Microsoft Windows does not support creating encrypted backups in the backup cache. If encryption options are specified for the backup job, Veeam Agent will create unencrypted backup files in the backup cache. When the target location becomes available, Veeam Agent will encrypt data prior to uploading it to the remote storage.
- Veeam Agent for Microsoft Windows does not support creating transaction log backups in the backup cache. You cannot enable transaction log backup and the backup cache for the backup job simultaneously.
- Restore points created in the backup cache cannot be uploaded to the target location after you perform the following operations:
  - Change target location for backup files in the properties of the backup job
  - Change a folder defined for the backup cache
  - Move or delete backup files on the target location
  - [For Veeam backup repository] Enable or disable data encryption settings in Veeam Backup & Replication

If the backup cache contains one or more restore points at the time when you perform one of these operations, you need to delete restore points from the backup cache.

- You cannot delete restore points from the backup cache while Veeam Agent for Microsoft Windows is performing the following operations:
  - Creating a new restore point in the backup cache.
  - Uploading a restore point from the backup cache to the target location.

Backup to Rotated Drives

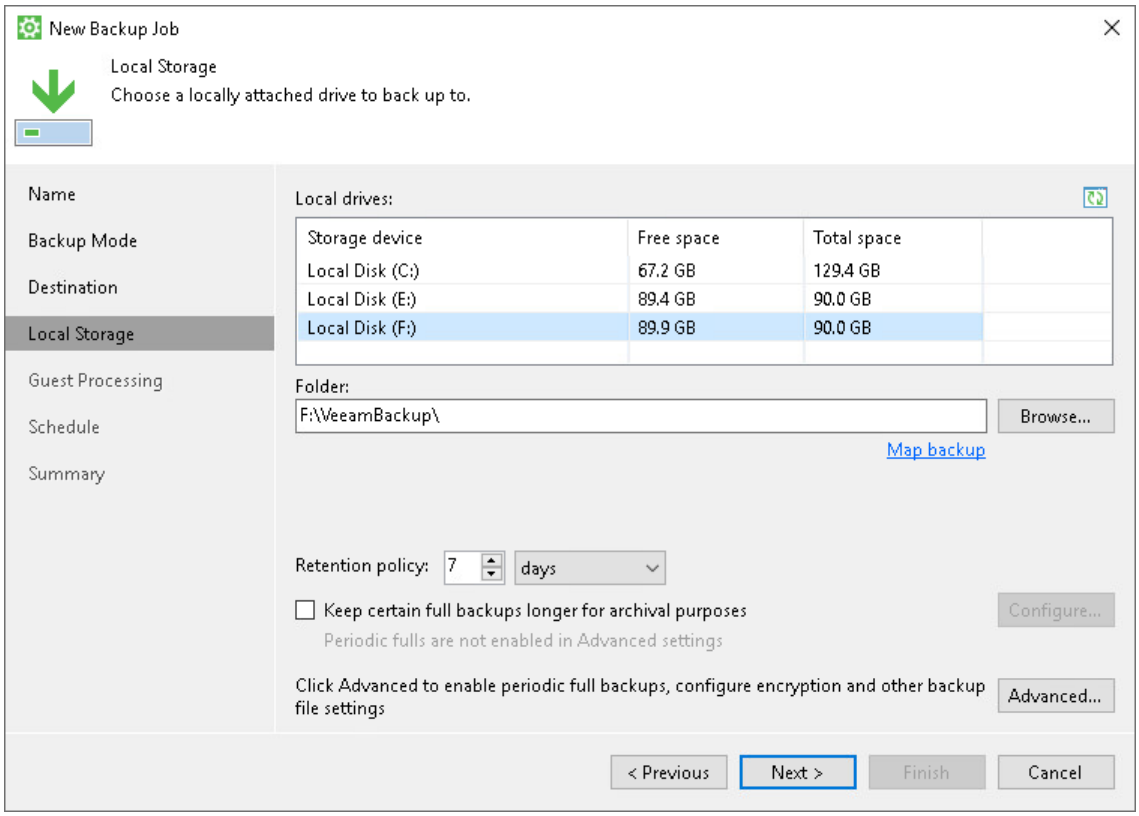
You can use rotated drives as a target location for backups. This scenario can be helpful if you want to store backups on several external hard drives (for example, USB or FireWire) and plan to swap these drives between different locations regularly.

Backup on rotated drives is performed in the following way:

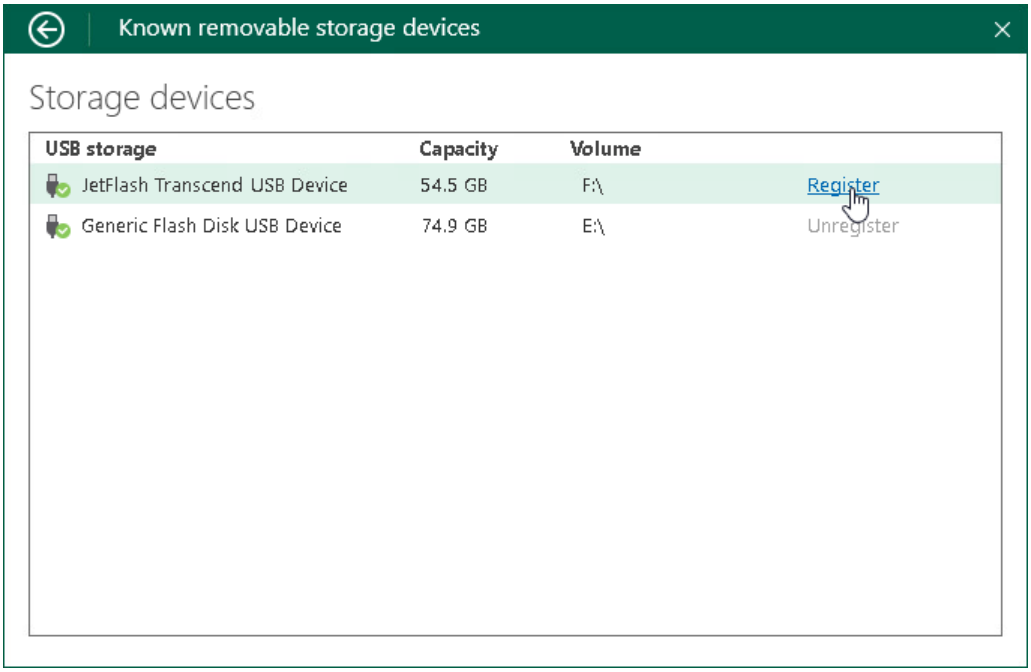
1. Veeam Agent for Microsoft Windows creates a backup chain on an external drive that you use as a backup target. The backup chain consists of the first full backup and a set of subsequent incremental backups.
2. When you swap drives and attach a new external drive, Veeam Agent creates a separate backup chain on the new drive.
3. After you swap drives again, Veeam Agent detects if there is a backup chain on the currently attached drive. If the backup chain exists, Veeam Agent continues the existing chain: it creates a new incremental backup file and adds it to the existing backup files.

To use rotated drives for backup, you must perform the following actions:

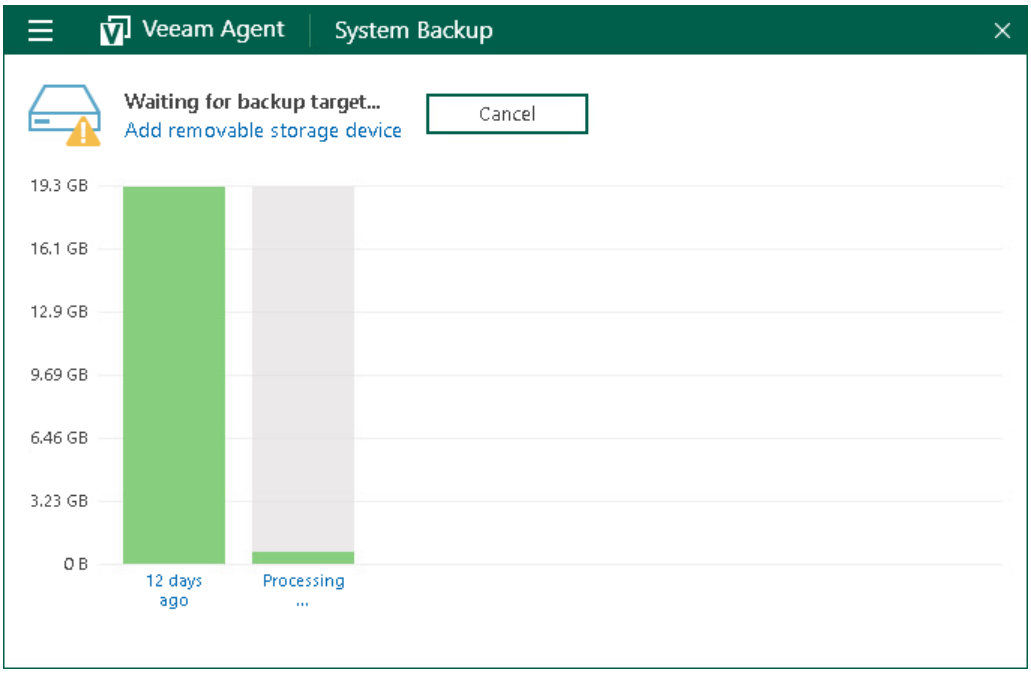
1. Attach one of external drives from the set to your computer.
2. Configure the backup job to store backups on the currently connected external drive. To do this:
   a. At the **Local Storage** step of the wizard, select the connected drive.
   b. From the **Local drives** list, select the necessary volume on the connected drive and specify a folder where backups must be stored.
   c. Save the job settings.



3. When you need to swap files, disconnect the drive that was used previously and attach a new drive to your computer.
4. Register a newly connected drive as a known removable storage in Veeam Agent for Microsoft Windows. To do this:
   a. Double-click the Veeam Agent icon in the system tray to open the control panel.
   b. From the main menu, select **Settings.**
   c. Click the **Manage registered storage devices** link.
   d. Click **Register** next to the newly connected drive.



If you do not register the newly connected drive before the backup job starts, Veeam Agent will be unable to detect the backup target and launch the backup job. Veeam Agent will display a warning in the system tray and in the control panel. To register a new device, click the **Add removable storage device** link in the **Status** view of the control panel and register the newly connected drive as described above. To learn more, see Managing Rotated Drives.



5. After you register the newly connected drive, you can start a new backup session manually or wait Veeam Agent to start a new session.

NOTE

Keep in mind that you cannot target a backup job at a certain set of rotated drives. If the backup job to rotated drive starts, and the drive that was used previously is not connected, Veeam Agent creates a backup file on any registered drive that is currently attached to the Veeam Agent computer.

Backup of External Drives

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

> **IMPORTANT**
>
> Veeam Agent supports backup of external drives that support Microsoft VSS: HDD, SSD, and so on. USB flash drives (USB sticks) are not supported, because it is impossible to create a VSS snapshot on a device of this type. To learn how to check if your drive is supported, see this Veeam KB article.

You can include an external drive in any type of backup: entire computer backup, volume-level backup or file-level backup.

- For entire computer backup, you can instruct Veeam Agent for Microsoft Windows to back up data of all external drives the are currently connected to the Veeam Agent computer. To do this, you must enable the **Include external USB drives** option at the **Backup Mode** step of the **New Backup Job** wizard.

  An external drive whose data you want to back up must be connected to the Veeam Agent computer at the time when the backup job must start.

  If an external drive that was backed up within a previous backup job session is not connected to the Veeam Agent computer when the backup job must start, Veeam Agent for Microsoft Windows will back up data of all existing drives and skip the absent one. The backup job session will complete successfully.

- For volume-level backup, you can include in the backup a specific volume that resides on an external drive. To do this, you must select the necessary volume at the **Volumes** step of the **New Backup Job** wizard.

  If a USB drive that contains the volume included in the backup is not connected to the Veeam Agent computer when the backup job must start, the backup job will complete with an error.

- For file-level backup, you can include in the backup data of a specific volume that resides on an external drive (entire volume or specific folders with files). To do this, you must select the necessary object at the **Files** step of the **New Backup Job** wizard.

  If a USB drive that contains a volume or folder included in the backup is not connected to the Veeam Agent computer when the backup job must start, the backup job will complete with an error.

> **NOTE**
>
> Veeam Agent for Microsoft Windows does not back up external drives used as rotated drives. USB drives registered as a known removable storage in Veeam Agent for Microsoft Windows are excluded from the backup.

Data Restore

Veeam Agent for Microsoft Windows offers two data restore scenarios:

- You can perform volume-level restore to recover the entire system image of your computer or specific computer volumes. To learn more, see Volume-Level Restore.
- You can perform file-level restore to recover individual files and folders. To learn more, see File-Level Restore.

When performing volume-level restore, you can resize restored volumes to fit available space on target location. To learn more, see Volume Resize.

Volume-Level Restore

If data on a computer volume gets corrupted, you can restore this volume from the backup. For volume-level restore, you can use backups that were created at the volume level. File-level backups cannot be used for volume restore.

When you perform volume-level restore, Veeam Agent for Microsoft Windows restores the entire content of the volume. It retrieves from the backup data blocks pertaining to a specific volume and copies them to the necessary location.

Keep in mind that you cannot browse the volume in the backup and select individual application items, files and folders for restore. For granular file-level restore, you can use the file-level restore option. To learn more, see File-Level Restore.

A volume can be restored to its original location or new location. If you restore the volume to its original location, Veeam Agent for Microsoft Windows overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Agent for Microsoft Windows overwrites data in the target location with data retrieved from the backup.

A volume can be restored to a new location that has greater or less space than the size of the volume in the backup. Depending on the amount of free disk space on target location, you can select either to shrink or to extend the volume during restore. To learn more, see Volume Resize.

Limitations for Volume-Level Restore

Volume restore has the following limitations:

- You cannot restore the system volume to its original location.
- You cannot restore a volume to the volume on which the swap file is currently hosted.
- You cannot restore a volume to the volume where the backup file used for restore is located.

To overcome the first two limitations, you can create a Veeam Recovery Media and use the **Veeam Bare Metal Recovery** wizard for volume-level restore. To learn more, see Veeam Recovery Media.

File-Level Restore

If you have lost or modified files and folders on your computer by mistake, you can restore a copy of the necessary objects from the backup. For file-level restore, you can use a backup of any type:

- Volume-level backup
- File-level backup

Veeam Agent for Microsoft Windows does not extract files and folders from the backup file. Instead, it uses Veeam's proprietary driver to publish the backup content directly into the computer file system, under `C:\VeeamFLR\<Volume N>`. For accessing the backup file content, Veeam Agent for Microsoft Windows uses a separate program — Virtual Disk Driver (VDK) that is provided with the product.

After the backup content is mounted, you can use a built-in Veeam Backup browser or Microsoft Windows Explorer to browse and copy necessary files and folders to your local machine drive, save them in a network shared folder or point applications to files and work with them in a regular way.

Volume Resize

With Veeam Agent for Microsoft Windows, you can resize backup volumes during volume-level restore. When you select to resize a volume, Veeam Agent for Microsoft Windows restores data from the backup and resizes the restored volume to the specified size.

There are two ways to resize a volume depending on the amount of free disk space on the target location:

- **Volume shrink** — you can shrink a volume when you restore it to a new location that has less space than the size of the volume in the backup. You can also shrink a volume that is restored to its original location to free disk space on the target location. To learn more, see How Volume Shrink Works.
- **Volume extend** — you can extend a backup volume when you restore it to a new location that has more available disk space than the size of the backup volume. To learn more, see How Volume Extend Works.

Volume resize may be also helpful when you need to restore data after hardware upgrade. For example, you may want to resize volumes in the following situations:

- Shrink backup data to restore system volumes of your computer to a smaller disk after you replace an old HDD drive with a faster but less capacitive SSD drive.
- Extend the backup volume during volume-level restore to a new, more capacitive HDD drive.

You can restore and resize volumes:

- With the **Volume Restore** wizard when you restore volumes under Microsoft Windows system. For more information, see Restoring Volumes.
- With the **Veeam Bare Metal Recovery** wizard when you perform restore from the Veeam Recovery Media. For more information, see Restoring from Veeam Recovery Media.

The volume resize option is available only in the **Manual restore** mode at the **Disk Mapping** step of the wizard.

Limitations for volume resize

Volume resize has the following limitations:

- You cannot restore a volume to the volume of the smaller size if the amount of data stored on the backup volume exceeds the free space on the target disk.
- You can only resize basic volumes that use the NTFS file system.
- If you resize a BitLocker encrypted volume during restore, the restored volume will be unencrypted.

How Volume Shrink Works

When you restore a volume to a target location of the smaller size, Veeam Agent for Microsoft Windows performs the following operations:

1. When you select the **Resize** option to shrink a volume, Veeam Agent for Microsoft Windows mounts the backup volume to a temporary NTFS folder on the system drive, for example: `C:\Users\Username\AppData\Local\Temp`.
2. Veeam Agent for Microsoft Windows mounts the created NTFS folder as a VHD disk next to other disks that are present on the computer.

Mounting VBK file content as a VHD disk makes it possible for Veeam Agent for Microsoft Windows to use Microsoft Windows system's disk management tools to measure current size of the backup volume and maximum and minimum size for the restored volume.

3. Veeam Agent for Microsoft Windows sends a query request to the mounted VHD disk to calculate its size, amount of stored data and free disk space by which the volume can be shrunk.

   This step may take some time depending on the size of the backup volume and its data fragmentation ratio.

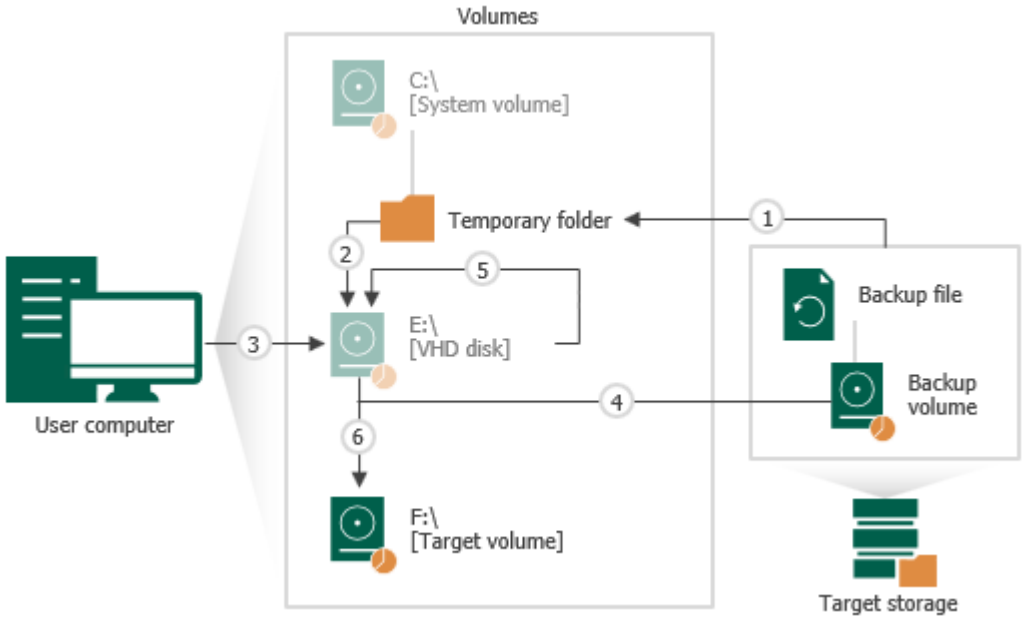
   When the query is complete and you specify the desired size for the restored volume, Veeam Agent for Microsoft Windows unmounts the VHD disk.

4. When you start the restore process, Veeam Agent for Microsoft Windows creates on the target disk a volume of the specified size and restores to that volume the amount of backed-up data that fits the specified size.

5. Veeam Agent for Microsoft Windows mounts the backup volume as a VHD disk as described in steps 1 and 2 and starts to shrink it to the size of the target volume. During the process of volume shrink, empty data blocks from the part of the mounted VHD disk that does not fit the size of the target volume are moved to the part of the disk that contains actual data.

6. Veeam Agent for Microsoft Windows captures on the VHD disk data blocks that are moved during shrink and writes them to the target volume.

   When all data blocks are written to the target volume, Veeam Agent for Microsoft Windows unmounts the VHD disk.



How Volume Extend Works

When you restore a volume to a target location of the larger size, Veeam Agent for Microsoft Windows performs the following operations:

1. When you select the *Resize* option to extend a volume, Veeam Agent for Microsoft Windows mounts the backup volume to a temporary NTFS folder on the system drive, for example: `C:\Users\Username\AppData\Local\Temp`.

2. Veeam Agent for Microsoft Windows mounts the created NTFS folder as a VHD disk next to other disks that are present on the computer.

Mounting VBK file content as a VHD disk makes it possible for Veeam Agent for Microsoft Windows to use Microsoft Windows system's disk management tools to measure current size of the backup volume and maximum and minimum size for the restored volume.

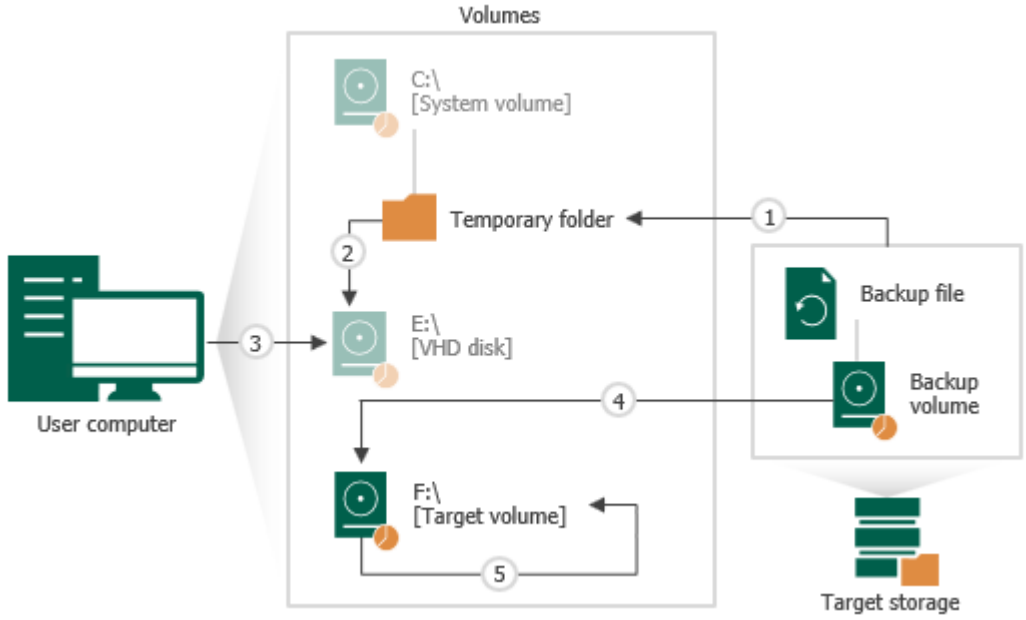
3. Veeam Agent for Microsoft Windows sends a query request to the mounted VHD disk to calculate its size, amount of stored data and free disk space by which the volume can be extended.

   This step may take some time depending on the size of the backup volume and its data fragmentation ratio.

   When the query is complete and you specify the desired size for the restored volume, Veeam Agent for Microsoft Windows unmounts the VHD disk.

4. When you start the restore process, Veeam Agent for Microsoft Windows creates on the target disk a volume of the same size as the backup volume and restores to that volume all data blocks from the backup volume.

5. When all data blocks are written to the target location, Veeam Agent for Microsoft Windows extends the size of the target volume to the specified size.



Veeam Recovery Media

Veeam Agent for Microsoft Windows lets you create a Veeam Recovery Media — a recovery image of your computer.

The recovery image is a "copy" of your OS with the limited functionality — it contains all data required to run Microsoft Windows Recovery Environment (Windows RE), and provides an alternative way to boot your computer. If the OS installed on the computer fails to start for some reason, you can boot the Windows RE from the recovery image. After booting, you can do the following:

- You can use Veeam Agent for Microsoft Windows and Microsoft Windows tools to diagnose problems and fix errors on your computer.
- You can restore data from a backup to your computer. For this scenario, you must have a backup created with Veeam Agent for Microsoft Windows or system image created with Microsoft Windows.

The recovery image can be helpful if one of the following errors occur:

- The OS on the computer fails to start.
- The computer is blocked with malware and you cannot get access to your data.
- You want to perform bare metal restore from the backup on the computer without the OS and other software installed.
- You want to restore the system volume of the computer and so on.

You can create a recovery image on different kinds of media:

- Removable storage devices such as USB drives or SD cards
- CD/DVD/BD
- ISO images on local or external computer drives

When you boot from the Veeam Recovery Media, you can use the Veeam Agent for Microsoft Windows recovery environment to fix the OS system errors on your computer or restore data from the backup. Veeam Agent for Microsoft Windows offers a set of tools for the computer system image and data recovery:

- Bare Metal Recovery — the Veeam Agent for Microsoft Windows wizard to recover data on the original computer or a new computer.
- Windows Recovery Environment — a built-in Microsoft Windows tool to recover the computer system image.
- Tools — Veeam Agent for Microsoft Windows and Microsoft Windows utilities for advanced computer administration.

Limitations for Veeam Recovery Media

- You cannot restore dynamic volumes using a Veeam Recovery Media. To restore dynamic volumes, you can recover data from the volume-level backup on a working computer system. To learn more, see Restoring Volumes.
- The Veeam Recovery Media is based on the Microsoft Windows RE. Due to Microsoft limitations, Microsoft Windows RE automatically reboots after 72 hours of continuous use. All data that has not been saved before reboot will be lost.

Drivers in Veeam Recovery Media

The Veeam Recovery Media created with Veeam Agent for Microsoft Windows contains the following data:

- Set of files required to start your computer OS from the recovery media.
- Diagnostic tools from Microsoft and Veeam.
- Drivers required to run hardware and devices on your computer in a regular way. When you boot your computer from the Veeam Recovery Media, drivers included into the Veeam Recovery Media are automatically loaded on the recovered OS.
- Network connection settings from your computer. When you boot your computer from the Veeam Recovery Media, network settings included into the Veeam Recovery Media are automatically applied and can be used to connect to the remote backup storage.
- If you have enabled data encryption options for the backup job, you can also include a decryption key into the Veeam Recovery Media. To learn more, see Creating Veeam Recovery Media.

> **NOTE**
>
> The Veeam Recovery Media contains all locales (languages) that are included in the OS of the Veeam Agent Computer.

You can include the following drivers in the Veeam Recovery Media:

- Drivers that are currently installed on your computer. Veeam Agent for Microsoft Windows detects hard disk controller drivers, network adapter drivers and USB controller drivers and includes them into the Veeam Recovery Media.
- Additional storage and network drivers. If you use non-standard drivers, you can include them in the created Veeam Recovery Media manually. For example, you can include drivers for a discrete network card, third-party USB 3.0 controllers and non-standard hard disk controllers.

> **TIP**
>
> If you do not include some drivers in the Veeam Recovery Media, you can load them from the computer drive when you perform bare metal recovery. To learn more, see Restoring from Veeam Recovery Media.

BitLocker Encrypted Volumes Support

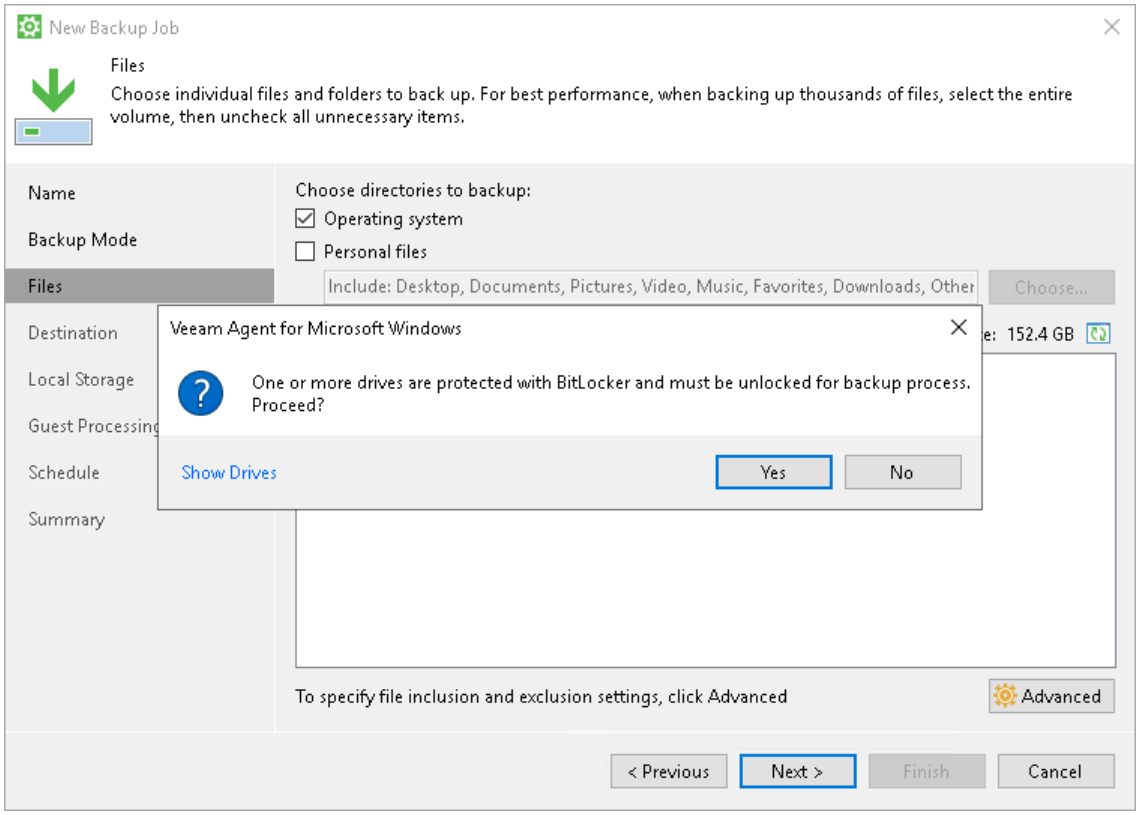
Veeam Agent for Microsoft Windows supports scenarios of data backup and restore to/from volumes encrypted with Microsoft Windows BitLocker.

Data Backup

You can create backups of BitLocker encrypted volumes and store backups created with Veeam Agent for Microsoft Windows on BitLocker encrypted volumes.

BitLocker encrypted volumes (both source and target) must be unlocked at the moment when Veeam Agent for Microsoft Windows starts the backup operation.

- If the volume added to the backup scope is locked at the moment of backup, the backup job will be unable to process it and will fail.
- If the volume on which the backup file must be stored is locked at the moment of backup, the backup job will be unable to save the resulting file, and the job will fail.



Data Restore

You can restore data from backups stored on BitLocker encrypted volumes and restore data to BitLocker encrypted volumes.

Veeam Agent for Microsoft Windows restores volumes in their initial state:

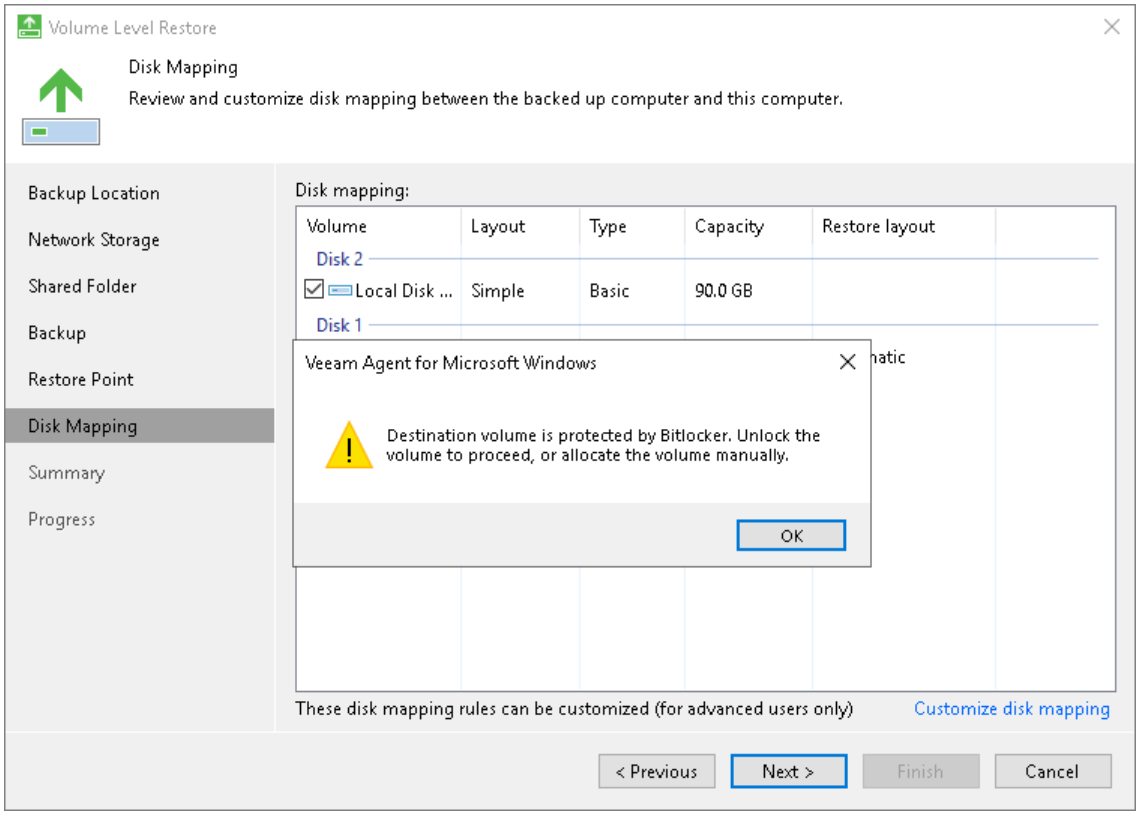
- If you restore an encrypted volume to its original location, the restored volume will be encrypted.
- If you restore an unencrypted volume to an encrypted volume, the restored volume will be unencrypted.

IMPORTANT

If you resize a BitLocker encrypted volume during restore, the restored volume will be unencrypted. To learn more about volume resize, see Volume Resize.

BitLocker encrypted volumes must be unlocked at the moment when you perform the restore operation.

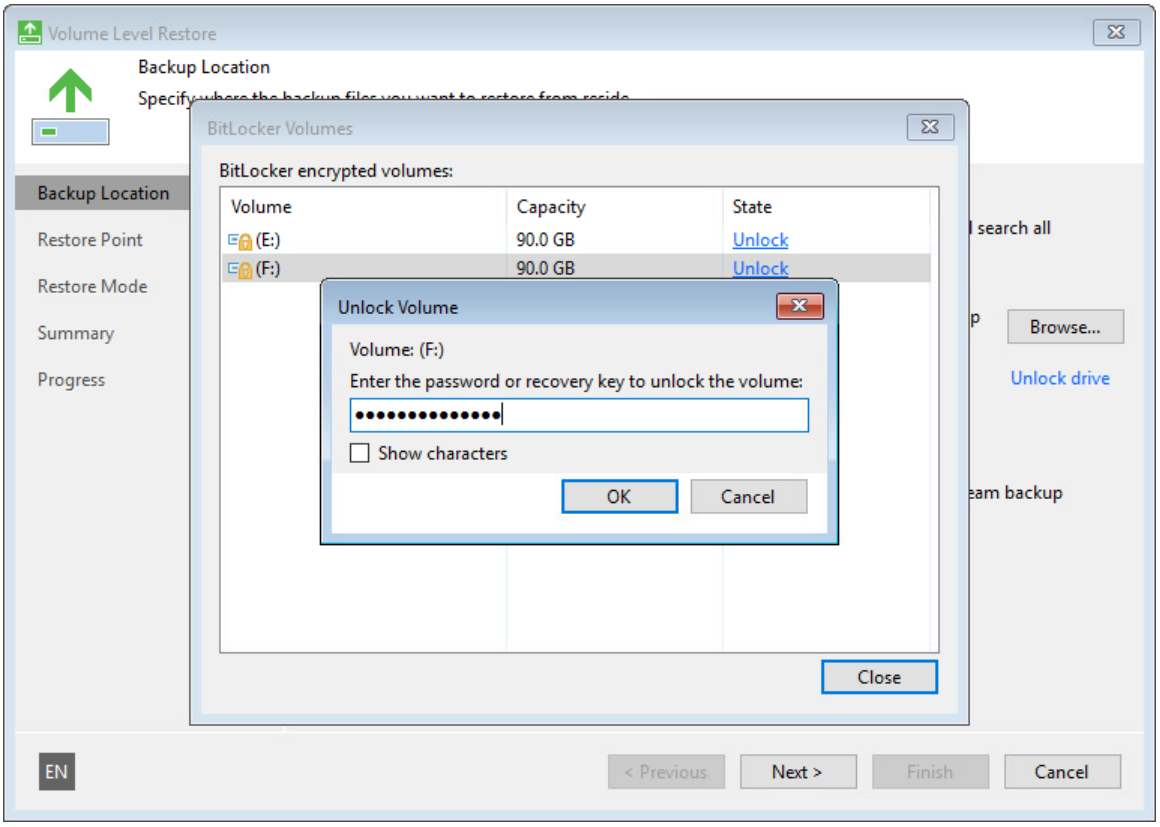
- If the backup file is stored on a locked volume, Veeam Agent for Microsoft Windows will fail to access it, and you will not be able to restore data from it.
- If you perform volume-level restore, and the target volume is locked, Veeam Agent for Microsoft Windows will display a warning and will ask you to unlock the volume. You can do this using the Microsoft Windows UI.



Veeam Recovery Media

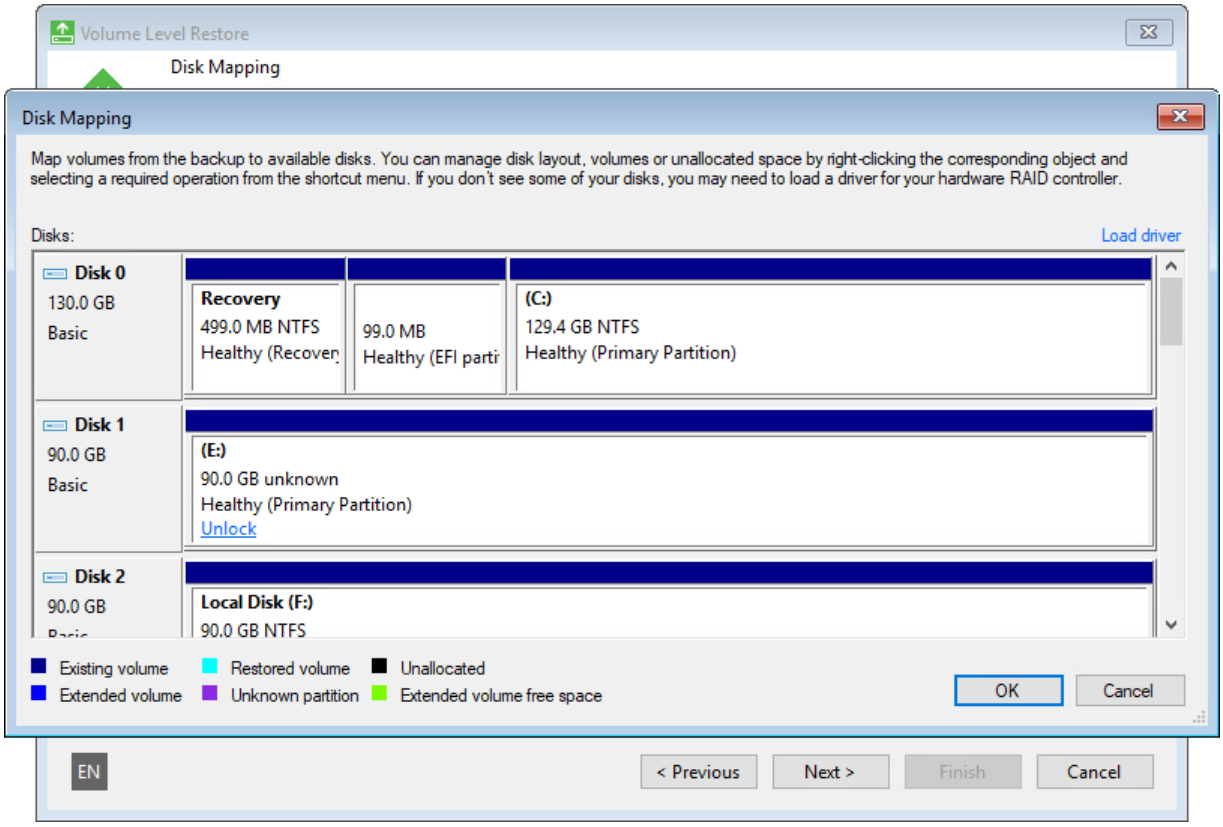
If you boot from the Veeam Recovery Media, you can restore data from backups stored on BitLocker encrypted volumes and restore data to BitLocker encrypted volumes.

- If the backup file that you want to use for data restore resides on a locked volume, Veeam Agent for Microsoft Windows cannot access this backup file. To unlock the volume with the backup file, click **Unlock drive** under the **Backup file** field and enter a password for the volume.

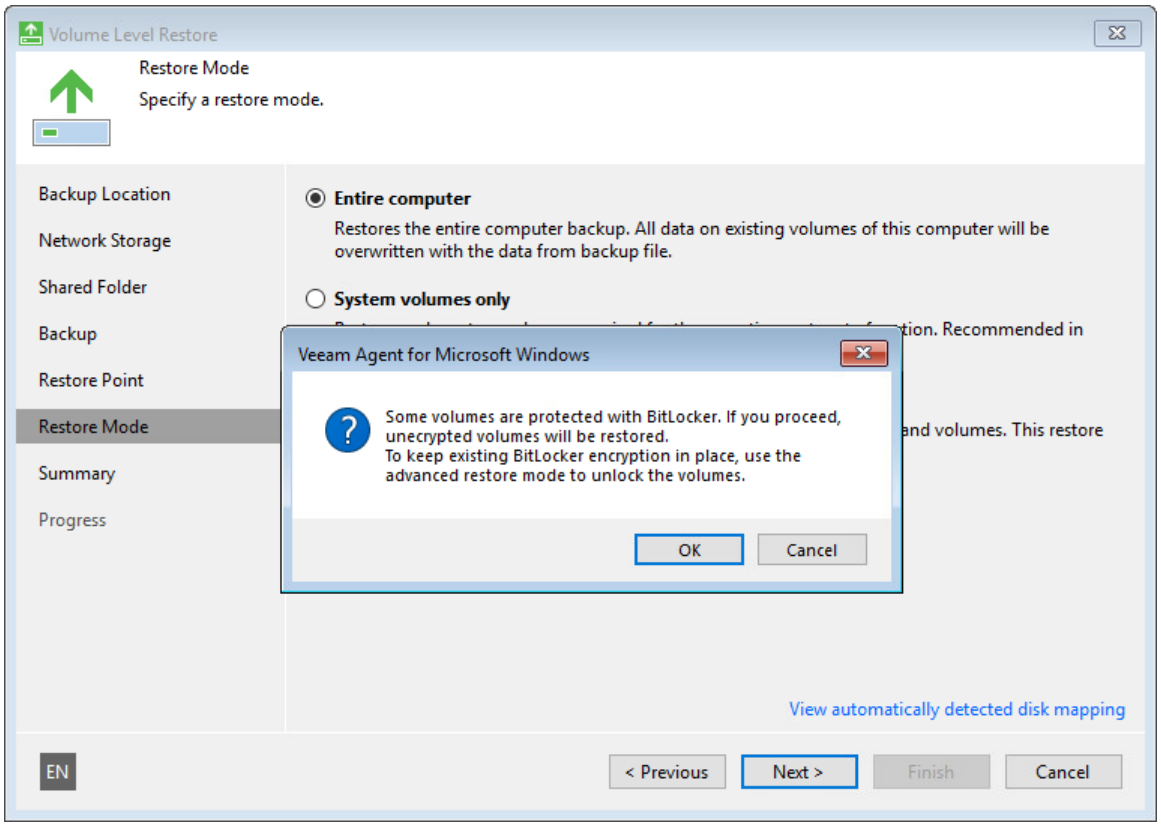


- If the target volume is BitLocker encrypted and locked, at the **Restore Mode** step of the wizard, Veeam Agent for Microsoft Windows displays a warning informing about it. You can use one of the following scenarios:
  - You can restore data to the target volume and keep BitLocker encryption enabled for the volume. To do this, you must unlock the volume before you start data restore.

    To unlock the volume, click **Cancel** in the warning window. At the **Restore Mode** step of the wizard, select **Manual Restore**. At the **Disk Mapping** step of the wizard, click **Customize disk mapping** and click **Unlock** under the necessary volume.



- You can restore data to the target volume and disable BitLocker encryption for the volume. To do this, click **OK** in the warning window. Veeam Agent for Microsoft Windows will delete existing BitLocker encrypted partitions on the volume, format the disk and restore data from the backup as unencrypted.



IMPORTANT

Veeam Agent for Microsoft Windows cannot back up volumes formatted as FAT32 and encrypted with BitLocker. In general, FAT32 does not allow storing VSS snapshots on the same volume. When Veeam Agent for Microsoft Windows triggers a VSS snapshot of a FAT32 formatted volume, the VSS snapshot is stored on another, non-FAT32 volume on the computer.

If BitLocker is enabled, the VSS cannot save the snapshot on another volume due to Microsoft limitations, and the backup process fails.

Integration with Veeam Backup & Replication

If you plan to use Veeam Agent for Microsoft Windows 6.0 or later with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.0 or later on the Veeam backup server. Veeam Agent for Microsoft Windows 5 supports integration with Veeam Backup & Replication 12 as well.

> **NOTE**
>
> You can also use Veeam Backup & Replication to manage Veeam Agent for Microsoft Windows on computers in your infrastructure. Within the Veeam Agent management scenario, you can remotely deploy Veeam Agent for Microsoft Windows to your computers, as well as configure and manage Veeam Agent backup jobs in Veeam Backup & Replication. To learn more, see the Veeam Agent Management Guide.
>
> The current guide covers subjects related to Veeam Agent for Microsoft Windows operating in the standalone mode.

You can store backup files created with Veeam Agent for Microsoft Windows on backup repositories managed by Veeam Backup & Replication. To do this, you must select a backup repository as a target location in the properties of the Veeam Agent backup job. To store Veeam Agent backups, you can use a simple backup repository or a scale-out backup repository.

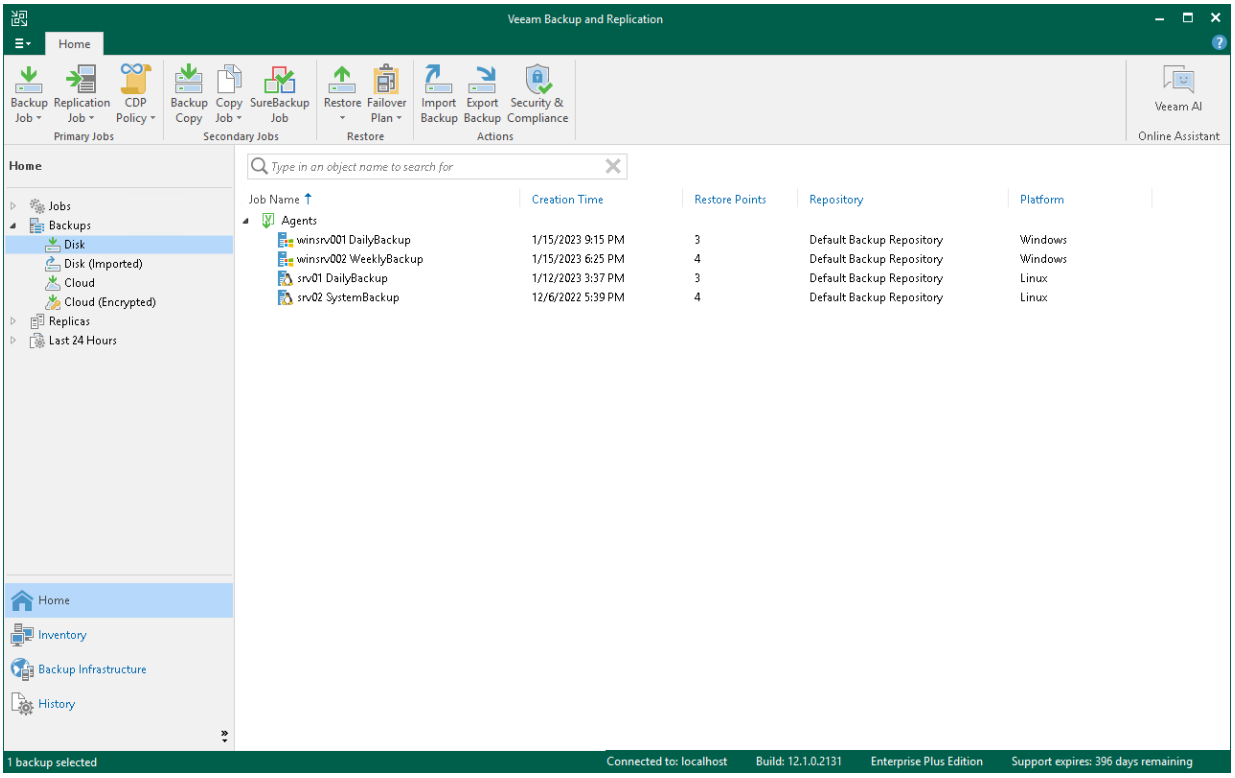
Veeam Agent for Microsoft Windows works with the backup repository as with any other target location. Backup files are stored in a separate folder; you can perform standard restore operations using these files.

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

- The Veeam Agent for Microsoft Windows backup job is displayed in the list of jobs in Veeam Backup & Replication.
- Backup files created with Veeam Agent for Microsoft Windows are displayed in the list of backups, under the **Backups** > **Disk** or **Backups** > **Object Storage** 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 folders, application items; restore computer disks and convert them to the VMDK, VHD or VHDX format; restore Veeam Agent backups to Microsoft Azure, Amazon Elastic Compute Cloud or to Hyper-V VMs.
- Perform administrative tasks: disable and delete Veeam Agent backup jobs, remove Veeam Agent backups and so on.


Veeam Backup and Replication
Home
Backup Job
Replication Job
CDP Policy
Backup Copy
Copy Job
SureBackup Job
Restore
Failover Plan
Import Backup
Export Backup
Security & Compliance
Veeam AI
Primary Jobs
Secondary Jobs
Restore
Actions
Online Assistant
Home
Type in an object name to search for
Jobs
Backups
Disk
Disk (Imported)
Cloud
Cloud (Encrypted)
Replicas
Last 24 Hours
Job Name
Creation Time
Restore Points
Repository
Platform
Agents
winsrv001 DailyBackup 1/15/2023 9:15 PM 3 Default Backup Repository Windows
winsrv002 WeeklyBackup 1/15/2023 6:25 PM 4 Default Backup Repository Windows
srv01 DailyBackup 1/12/2023 3:37 PM 3 Default Backup Repository Linux
srv02 SystemBackup 12/6/2022 5:39 PM 4 Default Backup Repository Linux
Home
Inventory
Backup Infrastructure
History
1 backup selected
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

Backup to Veeam Cloud Connect Repository

If you want to store your data in the cloud, you can connect to a Veeam Cloud Connect service provider (SP) and create Veeam Agent backups in a cloud repository.

Limitations for Backup to Cloud Repository

Backup to a Veeam Cloud Connect repository has the following limitations:

- You can store backups in a Veeam Cloud Connect repository if you use the Workstation or Server edition of Veeam Agent for Microsoft Windows only.
- You cannot use a Veeam Cloud Connect repository as a target for standalone full backup. To learn more, see Standalone Full Backup.
- Veeam Agent for Microsoft Windows does not support creating transaction log backups in the cloud repository. You cannot enable transaction log backup options in the properties of the backup job targeted at the cloud repository.

Managing Veeam Agent in Veeam Backup & Replication

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

To learn more, see the Veeam Agent Management Guide.

Planning and Preparation

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

System Requirements

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

> **NOTE**
>
> The following system requirements apply to Veeam Agent for Microsoft Windows operating in the standalone mode.
>
> To learn about system requirements for Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication, see the System Requirements section in the Veeam Agent Management Guide.

Specification	Requirement
Hardware	CPU: x86-64 processor. Memory: 2 GB RAM or more. Memory consumption varies depending on number and size of processed disks. Disk Space: 200 MB for product installation. Network: 1 Mbps or faster. High latency and reasonably unstable WAN links are supported. System firmware: BIOS or UEFI. Drive encryption: Microsoft BitLocker (optional). BitLocker encrypted volumes must be unlocked at the moment when Veeam Agent starts the backup or restore operation. Only Microsoft BitLocker is supported for drive encryption. Other drive encryption products are not supported.
OS	Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported[1]: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server General Availability Channel (from version 1803 to version 20H2) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1[2] • Microsoft Windows 11 (from version 21H2 to version 23H2) • Microsoft Windows 10 (from version 1909 to version 22H2)[3] • Microsoft Windows 10 Long-Term Servicing Channel (versions 2015, 2016, 2019) • Microsoft Windows 8.1 • Microsoft Windows 7 SP1

Specification	Requirement
	[1] Consider the following: • Small Business Server, Server Essentials, and Server Storage editions of Microsoft Windows Server OSes are supported. • Server Core installations of Microsoft Windows Server OSes are supported for Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication only. To learn more, see the Veeam Agent Management Guide. Veeam Agent operating in the standalone mode does not support Server Core installations. • Windows Embedded / Windows IoT OSes are supported (except for custom builds by certain vendors that do not have components required for Veeam Agent operation). • Microsoft Failover Clusters are supported for Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication only. To learn more, see the Veeam Agent Management Guide. Veeam Agent operating in the standalone mode does not support Microsoft Failover Clusters. [2] Veeam CBT driver is supported only if Microsoft Windows update KB3033929 is installed on the Veeam Agent computer. [3] Microsoft Windows 10 Education is supported starting from Veeam Agent 6.0 build 10586.
File System	Microsoft Windows FAT32/exFAT, NTFS, ReFS file systems are supported. The supported file system must reside on a volume that is 64 TB or smaller, because Veeam Agent uses the Microsoft Software Shadow Copy Provider to create a volume shadow copy during the backup. To learn more about the limitation, see this Microsoft article.
Software	The following required 3rd party software is included in the setup program: • Microsoft .NET Framework 4.5.2 • Windows Universal C Runtime Library When installing the product, the setup program checks whether all prerequisite software is available on the target computer. If some of the required software components are missing, the missing software is installed automatically. If you plan to use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install Veeam Backup & Replication 12 on the Veeam backup server.
Database	SQLite database engine (installed with the product).

Consider the following:

- Veeam Agent for Microsoft Windows works with only those hard drive types that are supported by the Microsoft Windows OS. Thus, Veeam Agent supports the 512 bytes and 4 KB sector hard drives only. Other hard drive types are not supported. To learn more, see this Microsoft article.
- Supported culture settings depend on the version of Microsoft Windows OS installed on your computer. For more information, see this Microsoft article.

Backup Source

Veeam Agent for Microsoft Windows supports backup of data that resides in the following types of storage:

- Local (internal) storage of the protected computer.
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives (USB sticks and SD cards are not supported).
- Storage Area Network (SAN), such as iSCSI connected volumes.

Keep in mind that Veeam Agent cannot work with third-party volume managers installed on the protected computer. Such managers may not allow Veeam Agent to interact with necessary interfaces and services properly.

Backup Target

Backup can be performed to the following types of storage:

Disk-based storage

- Local (internal) storage of the protected computer (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives, and raw device mapping (RDM) volumes.

  > **IMPORTANT**
  >
  > Storage devices with the exFAT file system are not supported as a backup target.

- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share.
- Storage Area Network (SAN), such as iSCSI connected volumes.
- On-premises object storage.
- Veeam Backup & Replication 12 backup repository.

Cloud storage

- Cloud-based object storage.
- Veeam Cloud Connect 12 cloud repository.

Network

Consider the following:

- If you back up to a repository managed by a Veeam backup server, Veeam Agent for Microsoft Windows must be able to establish a direct IP connection to the Veeam Backup & Replication server. Veeam Agent cannot work with Veeam Backup & Replication that is located behind a NAT gateway.
- Domain names of the Veeam Agent computer, Veeam Backup & Replication server and other servers in the Veeam backup infrastructure must be resolvable into IPv4 or Ipv6 addresses.

Permissions

Depending on the scenario, the user accounts must have the permissions listed in the following subsections:

- Permissions for Backup to Object Storage
- Permissions for Guest Processing

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"
}
```

Permissions for Guest Processing

To use guest processing, make sure to configure user accounts according to the requirements listed in this section.

Consider the following general requirements when choosing a user account:

- [For file indexing] Choose a user account that has administrator privileges.
- When using Active Directory accounts, make sure to provide a user account in the *DOMAIN|Username* format.
- When using local user accounts, make sure to provide a user account in the *Username or HOST|Username* format.
- To process a Domain Controller server, make sure that you are using a user account that is a member of the *DOMAIN|Administrators* group.
- To back up a Read-Only Domain controller, a delegated RODC administrator account is sufficient. For more information, see Microsoft Docs.

Depending on the application you need to back up, the user must have the permissions listed in the table below:

Application	Required Permission
Microsoft SQL Server	To back up Microsoft SQL Server data, the user whose account you plan to use must be: • Local Administrator on the Veeam Agent computer. • System administrator (has the *Sysadmin* role) on the target Microsoft SQL Server. If you need to provide minimal permissions, the user account must be assigned the following roles and permissions: • SQL Server instance-level role: *public* and *dbcreator*. • Database-level roles and roles for the model system database: *db_backupoperator*, *db_denydatareader*, *public*; for the master system database — *db_backupoperator*, *db_datareader*, *public*; for the msdb system database — *db_backupoperator*, *db_datareader*, *public, db_datawriter*. • Securables: *view any definition*, *view server state, connect SQL*.
Microsoft Active Directory	To back up Microsoft Active Directory data, the user account must be a member of the built-in *Administrators* group.
Microsoft Exchange	To back up Microsoft Exchange data, the user account must have the Local Administrator permissions in Microsoft Exchange.
Oracle	To back up Oracle data, the user account must be configured as follows: • The user account must be a member of both the *Local Administrators* group and the *ORA_DBA* group (if OS authentication is used). • The user account must be granted *SYSDBA* privileges.
Microsoft SharePoint	To back up Microsoft SharePoint server, the user account must have the *Farm Administrator* role. To back up Microsoft SQL databases of the Microsoft SharePoint Server, the user account must have the same privileges as for the Microsoft SQL Server.

Ports

The following tables describe network ports that must be opened to ensure proper communication of Veeam Agent operating in the standalone mode with other infrastructure components.

To learn about ports required to enable proper work of Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication, see the Ports section in the Veeam Agent Management Guide.

> **IMPORTANT**
>
> The list of ports required for computers booted from the Veeam Recovery Media is the same as the list of ports required for Veeam Agent computers.

Communication Between Veeam Agent Components

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

From	To	Protocol	Port	Notes
Veeam Agent Computer	Veeam Agent Computer	TCP	9395+, 6183+	Ports used locally on the Veeam Agent computer for communication between Veeam Agent components and Veeam Agent for Microsoft Windows Service. If the default port number is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.
	Veeam Update Notification Server (autolk.veeam.com)	TCP	443	Default port used to download information about available updates from the Veeam Update Notification Server over the Internet.

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	Veeam Backup Server	TCP	10001	Default port used by Veeam Agent for Microsoft Windows operating in the standalone mode for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.
	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	49152-65535	Dynamic RPC port range. For more information, see this Microsoft 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.
	Shared folder CIFS (SMB) share	TCP UDP	137 to 139, 443, 445	Ports used as a transmission channel from the Veeam Agent computer to the target CIFS (SMB) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS. Port 443 is used to connect the target CIFS (SMB) share over QUIC. For more information, see this Microsoft article.
	Gateway Microsoft Windows server	TCP UDP	137 to 139, 445	If a CIFS (SMB) share is used as a backup repository and a Microsoft Windows server is selected as a gateway server for this CIFS share, these ports must be opened on the gateway Microsoft Windows server.

From	To	Protocol	Port	Notes
				Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.
		TCP	49152-65535	Dynamic RPC port range. For more information, see this Microsoft 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 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 Connection Types.

From	To	Protocol	Port	Notes
Veeam Agent Computer	Amazon S3 object storage	TCP	443	Used to communicate with the Amazon S3 object storage through the following endpoints: • `*.amazonaws.com` (for both *Global* and *Government* regions) • `*.amazonaws.com.cn` (for *China* region) All AWS service endpoints are specified in the AWS documentation.
			80	Used to verify the certificate status through the following endpoints: • `*.amazontrust.com` 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.
	Microsoft Azure object storage	TCP	443	Used to communicate with the Microsoft Azure object storage through the following endpoints: • `xxx.blob.core.windows.net` (for *Global* region) • `xxx.blob.core.chinacloudapi.cn` (for *China* region) • `xxx.blob.core.usgovcloudapi.net` (for *Government* region) 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.
			80	Used to verify the certificate status through the following endpoints: • `ocsp.digicert.com` • `ocsp.msocsp.com` Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to

From	To	Protocol	Port	Notes
				change. The actual list of addresses can be found in the certificate itself. For more details, see also this Microsoft article.
	Google Cloud storage	TCP	443	Used to communicate with Google Cloud storage through the following endpoints: • `storage.googleapis.com` All cloud endpoints are specified in this Google article.
			80	Used to verify the certificate status through the following endpoints: • `ocsp.pki.goog` • `pki.goog` • `crl.pki.goog` 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.
	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.

Communication with Mail Servers

The following table describes network ports that must be opened to ensure proper communication with mail servers.

From	To	Protocol	Port	Notes
Veeam Agent Computer	SMTP server	TCP	25	Default port used by the SMTP server.
		TCP	587	Port used by the SMTP server if SSL is enabled.

From	To	Protocol	Port	Notes
	Gmail REST API (gmail.googleapis.com)	TCP	443	Port used for communication with Google Mail services.
	Microsoft Graph REST API (graph.microsoft.com, login.microsoftonline.com)	TCP	443	Port used for communication with Microsoft Exchange Online organizations.

Installation and Configuration

You can install Veeam Agent for Microsoft Windows on any computer whose data you plan to protect — server, desktop, laptop or tablet.

Before You Begin

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

- The computer on which you plan to install Veeam Agent must satisfy system requirements specified in this document. To learn more, see System Requirements.
- Make sure the operating system on the computer you want to protect is up-to-date. Otherwise, the correct functioning of Veeam Agent is not guaranteed.
- If your computer runs Microsoft Windows 11 version 22H2 or 23H2, make sure that the Smart App Control feature is disabled. Otherwise, it may cause installation issues.

  For information about Smart App Control, see this Microsoft article.
- You must run the Veeam Agent setup file under the Administrator account or any user account that has Administrator privileges on the computer where you plan to install the product.
- Veeam Agent for Microsoft Windows requires the following components:
  - SQLite database engine
  - Microsoft .NET Framework 4.5.2 or later
  - Windows Universal C Runtime Library

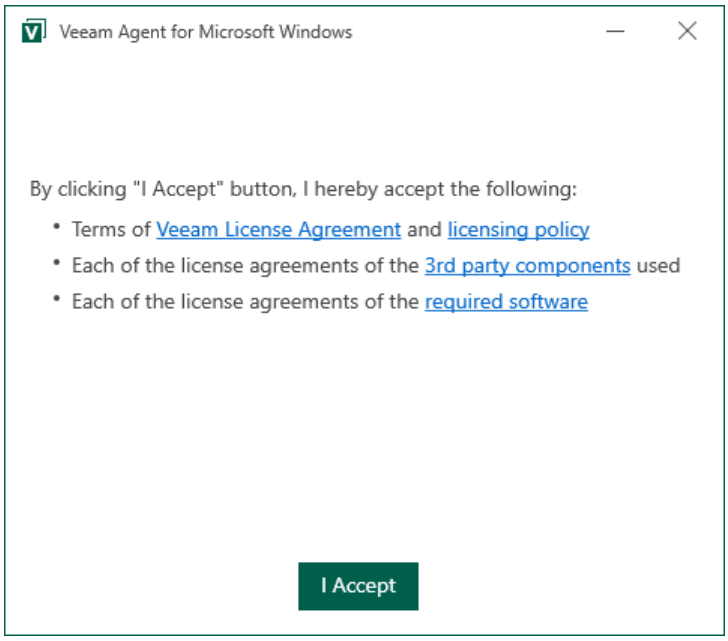
  If these components are not pre-installed on the computer, the setup will install them during the product installation process.
- The product program files are placed to the `%ProgramFiles%\Veeam\Endpoint Backup` folder on the system volume. Make sure that you have enough free space on the system volume to install the product. Veeam Agent requires at least 200 MB.
- [Recommended] If you want to create a recovery image of your computer on a USB storage device, CD/DVD/BD or make an ISO image, prepare the necessary device/media or make sure that you have enough free disk space in the target location. On average, the size of the created recovery image is 500 MB.

  During the recovery image creation, Veeam Agent formats the removable storage device. If you have important information on the device, create a copy of this data in some other location.

Installing Veeam Agent for Microsoft Windows

To install Veeam Agent for Microsoft Windows:

1. Download the setup archive for Standalone Veeam Agent for Microsoft Windows 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 setup file to launch the installation wizard and click **Next**.
3. Click **I Accept** to accept license agreements and install Veeam Agent for Microsoft Windows.



After the installation process is complete, you can instruct Veeam Agent for Microsoft Windows to create a recovery image for your computer. To learn more, see Creating Veeam Recovery Media.

Installing Veeam Agent for Microsoft Windows in Unattended Mode

You can install Veeam Agent for Microsoft Windows in the unattended mode using the command line interface. The unattended installation mode does not require user interaction — the installation runs automatically in the background, and you do not have to respond to the installation wizard prompts. You can use the unattended installation mode to automate the Veeam Agent installation process in large-scale environments.

Prerequisite Software

During the product installation, Veeam Agent for Microsoft Windows automatically sets up the following required prerequisite components:

- SQLite database engine

  Veeam Agent for Microsoft Windows 6.0 and later uses SQLite database instead of Microsoft SQL Server 2012 Express LocalDB. If you install Veeam Agent 6.0 and later on a computer with an existing SQL Server database, migration to the new database will be performed during the upgrade of Veeam Agent. If necessary, you can skip migration to the new database. To learn more, see Installation Without Database Migration.

- Windows Universal C Runtime Library

Veeam Agent for Microsoft Windows also sets up Microsoft .NET Framework 4.5.2 if it does not detect this component on the computer during the product installation.

In some cases, installation of prerequisite software requires computer reboot. This can happen, for example, if you have an earlier version of a prerequisite component installed on the computer and during the installation process this component is used by third-party software.

In this situation, unattended setup will install Veeam Agent for Microsoft Windows but will not start the Veeam Agent for Microsoft Windows service. After you reboot the computer, the Veeam Agent for Microsoft Windows service will be started and Veeam Agent for Microsoft Windows will be fully functioning.

Installation

The syntax of the command to install Veeam Agent for Microsoft Windows in the unattended mode depends on the version of Veeam Agent:

- To install Veeam Agent for Microsoft Windows version 6.1, use a command with the following syntax:

```
<path_to_exe> /silent /accepteula /acceptthirdpartylicenses /acceptlicensi
ngpolicy /acceptrequiredsoftware
```

- To install Veeam Agent for Microsoft Windows version 6.0, use a command with the following syntax:

```
<path_to_exe> /silent /accepteula /acceptthirdpartylicenses
```

where `<path_to_exe>` — path to the Veeam Agent for Microsoft Windows installation file.

Veeam Agent for Microsoft Windows uses the following codes to report about the installation results:

- 1000 — Veeam Agent for Microsoft Windows has been successfully installed.
- 1001 — prerequisite components required for Veeam Agent for Microsoft Windows have been installed on the machine. Veeam Agent for Microsoft Windows has not been installed. The machine needs to be rebooted.
- 1002 — Veeam Agent for Microsoft Windows installation has failed.
- 1004 — migration to SQLite database has failed.
- 1101 — Veeam Agent for Microsoft Windows has been installed. The machine needs to be rebooted.

Installation Without Database Migration

If you do not want to migrate the existing SQL database during the installation of Veeam Agent, you can skip migration to the new database. In this case, you will need to create backup jobs from scratch.

The syntax of the command to skip migration during the installation of Veeam Agent for Microsoft Windows in the unattended mode, depends on the version of Veeam Agent:

- To install Veeam Agent for Microsoft Windows version 6.1 and skip migration, use a command with the following syntax:

```
<path_to_exe> /silent /accepteula /acceptthirdpartylicenses /acceptlicensi
ngpolicy /acceptrequiredsoftware /skipmigration
```

- To install Veeam Agent for Microsoft Windows version 6.0 and skip migration, use a command with the following syntax:

```
<path_to_exe> /silent /accepteula /acceptthirdpartylicenses /skipmigration
```

To learn more about database migration, see Upgrading Veeam Agent for Microsoft Windows.

Using Sysprep and Veeam Agent for Microsoft Windows

You can pre-install Veeam Agent in a custom Microsoft Windows system image that will be used for deployment on different computers. To do this, you should perform a set of configuration steps in the reference Microsoft Windows system installation that will be included in a deployment image.

To configure a custom Microsoft Windows system image with Veeam Agent:

1. Install Veeam Agent in a Microsoft Windows system image. To learn more, see Installing Veeam Agent for Microsoft Windows.
2. Configure the backup job in the way you want it to work on computers with pre-installed Veeam Agent. To learn more, see Creating Backup Jobs.

> **NOTE**
>
> It is advised to configure the backup job for the entire computer backup. In case of volume-level backup, it may be necessary to reconfigure the backup job after Microsoft Windows is deployed to the target computer and include the necessary volumes in the backup once again. This may happen if volumes' GUIDs were changed at the stage of Microsoft Windows generalization with Sysprep.

3. Create a registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Endpoint Backup\SysprepMode (DWORD)=1`.

   This registry value is used to regenerate the job ID when Veeam Agent starts for the first time on the new computer. If you do not create the registry value, the backup job may fail as soon as it is started on the new computer.
4. Run the Sysprep tool in the Generalize mode to remove any system-specific data. If you need to run the Sysprep tool in the Audit mode, do not forget to re-create the registry value afterwards.
5. Deploy the image on the necessary computers in any convenient way. To learn more about deployment of Microsoft Windows system to new computers, see this Microsoft article.

When you deploy the created image on the computer, Veeam Agent will re-generate internal IDs of the backup jobs. As a result, the backup job will be fully functional.

> **NOTE**
>
> After Veeam Agent for Microsoft Windows starts on the new computer for the first time, the registry value is changed to 0 so that the job ID is not changed during subsequent starts of Veeam Agent for Microsoft Windows.

Upgrading Veeam Agent for Microsoft Windows

For Veeam Agent for Microsoft Windows, upgrade to newer versions is supported. You can start the upgrade process from the Veeam Agent control panel when the new version becomes available. To learn how to check for product updates, see Checking for New Product Versions and Updates.

Before You Begin

Before you upgrade Veeam Agent for Microsoft Windows to version 6.1, check the following prerequisites:

- Make sure that you do not have backup jobs targeted at Microsoft OneDrive.

  Starting from Veeam Agent for Microsoft Windows 6.0, backup to Microsoft OneDrive is deprecated. To continue working with backups created with an earlier version of Veeam Agent and stored in a Microsoft OneDrive storage, download these backups and move them to another storage. To learn more, see Downloading Backups from Microsoft OneDrive.

- Make sure that your local Microsoft SQL Server instance and other SQL components that were installed with the previous version of Veeam Agent work correctly.

  Veeam Agent for Microsoft Windows 6.0 and later uses SQLite database instead of Microsoft SQL Server 2012 Express LocalDB. Migration to the new database will be performed during the upgrade of Veeam Agent. If any required SQL components are missing, migration will fail.

- Make sure that there are no running jobs.

  If you have any running jobs, let them complete successfully before you start the upgrade. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If the protected computer runs VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived logs) is enabled in the backup job for the computer, disable this backup job too.

During the upgrade process, configuration and backup files that were created with the previous version of Veeam Agent are not impacted in any way.

Upgrade Process

> **NOTE**
>
> Consider the following:
>
> - In some cases, upgrade to the new version of Veeam Agent may require computer reboot.
> - You can also download the Veeam Agent setup archive from this Veeam webpage. Save the downloaded archive on the computer where you plan to install the new version of the product and double-click the setup archive to start the upgrade.

To upgrade Veeam Agent for Microsoft Windows:

1. Double-click the Veeam Agent icon in the system tray, or right-click the Veeam Agent icon in the system tray and select **Control Panel**.
2. Open the **About** tab.
3. If the new version of Veeam Agent is available, click **Download**.
4. When the download is complete, click **Install** to run the setup archive.

5. To upgrade Veeam Agent, you must accept the terms of the license agreements. Read the license agreements and click **Accept and Update**.
6. To preserve settings from the previous product installation, click **Yes** in the opened window.

   If the migration fails for any reason, the upgrade process will stop. In this case, you will be able to continue using the earlier version of Veeam Agent as the existing Microsoft SQL Server database and preinstalled SQL components are not deleted during the migration.

   > **NOTE**
   >
   > Migration will not start if at least one of the following conditions is met:
   >
   > - You use Veeam Agent version 3.0 or earlier. In this case, a new database will be created during the upgrade.
   > - Migration to SQLite database was performed earlier.

7. After the installation is complete, click **Finish**.

Unattended Upgrade

You can upgrade Veeam Agent to a newer version in the unattended mode using the same command that is used for unattended installation. To learn more, see Installing Veeam Agent for Microsoft Windows in Unattended Mode.

If necessary, you can skip the migration of the SQL database during the unattended upgrade. To learn more, see Installation Without Database Migration.

Configuring Advanced Settings

Connection Settings for Veeam Backup Server

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

To connect Veeam Agent for Microsoft Windows to Veeam backup server, use Veeam Agent Configurator. To learn more, see the SetVBRSettings section in the Veeam Agent Configurator Reference.

Uninstalling Veeam Agent for Microsoft Windows

To uninstall Veeam Agent for Microsoft Windows:

1. From the **Start** menu, select **Control Panel** > **Programs and Features**.
2. In the programs list, right-click Veeam Agent and select **Uninstall**. Wait for the process to complete.

The prerequisite components installed and used by Veeam Agent are not removed during the uninstall process. To remove each of the remaining components, right-click it in the programs list and select **Uninstall**.

What You Do Next

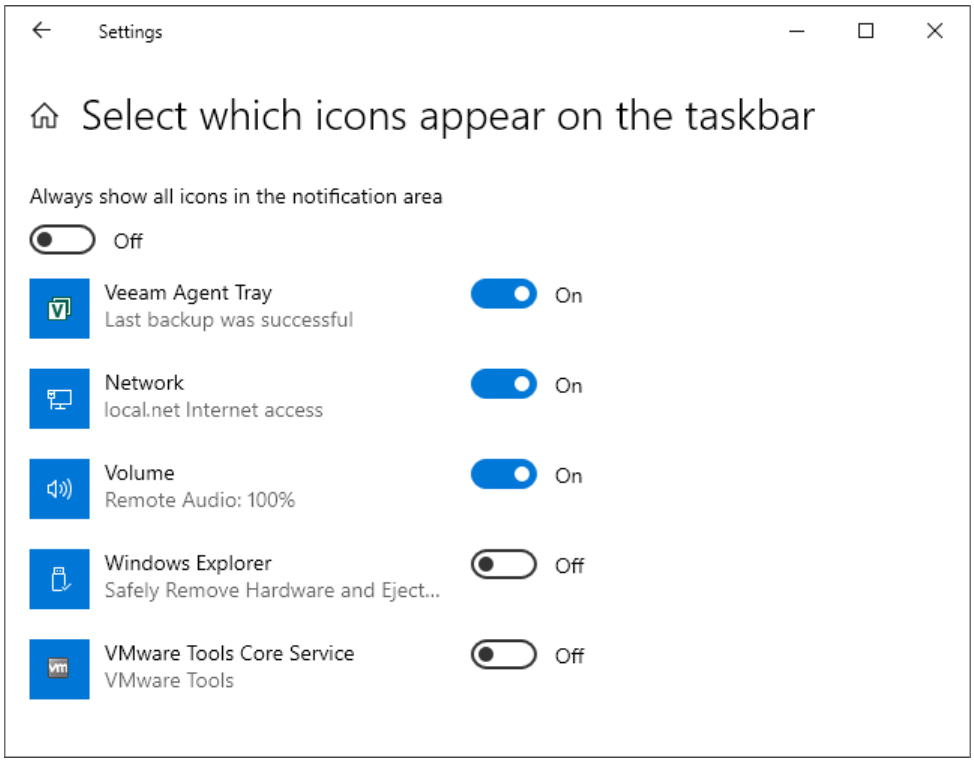
After the product installation, Veeam Agent for Microsoft Windows displays its icon in the system tray. You can use the system tray icon to perform main operations in Veeam Agent for Microsoft Windows:

- Configure the backup job and start ad-hoc backup operations
- Launch restore wizards
- Open the Veeam Agent control panel
- Monitor the state of backup tasks and so on

Depending on the current settings of your Microsoft Windows OS, the Veeam Agent for Microsoft Windows icon may not be displayed in the system tray.

To bring the icon to the system tray:

1. In Microsoft Windows, open the **Notification Area Settings** window. To do this, do either of the following:
   - Click the arrow in the system tray and click **Taskbar Settings**.
   - From the Microsoft Windows main menu, select **Control Panel** and navigate to **Taskbar and Navigation**. In the **Taskbar** section, select **Notification Area**.
2. In the **Notification Area Settings** window, select **On** for the Veeam Agent Tray.
3. In the **Behaviors** column, set the **Show icon and notification** setting for it.



Getting Started

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

1. Create a Veeam Recovery Media.

   The Veeam Recovery Media provides an alternate way to boot the Microsoft Windows RE. If your computer fails to start or the hard disk gets corrupted, you can boot the Windows RE from the Veeam Recovery Media and restore your data.

   To learn more, see Creating Veeam Recovery Media.

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

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

   - Backup scope: entire computer image, individual computer volumes or specific computer folders.
   - Backup destination: where you want to store created backups.
   - Backup schedule: how often you want to back up your data.

   After that, you can configure the backup job. The backup job runs automatically by the defined schedule, 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 required restore point.

   To learn more, see Creating Backup Jobs.

3. Specify Veeam Agent settings.

   You can define resource usage settings during backup, instruct Veeam Agent to automatically check for new product versions and so on. To learn more, see Specifying Settings.

4. Monitor backup task performance.

   You can use the Veeam Agent control panel to check how backup tasks are being performed, what errors have occurred during backup job sessions and so on. To learn more, see Reporting.

5. In case of a disaster, you can restore the entire computer image or specific data on the computer. To learn more, see Performing Restore.

Licensing

You can use Veeam Agent for Microsoft Windows as a free product. In this case, you do not need to obtain and install any license.

To work with a commercial version of Veeam Agent for Microsoft Windows, you must obtain a license and install it on the protected computer. If you do not install a license, you will be able to use the Free edition of the product only.

If you plan to use a commercial version of the product with Veeam Backup & Replication, you must install and manage the license in the Veeam Backup & Replication console or in Veeam Backup Enterprise Manager. To learn more, see Managing License.

Product Editions

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

- *Server* — a commercial edition that provides access to all product functions. The Server edition is intended for performing data protection tasks on servers that run the Microsoft Windows OS. To use the Server edition of Veeam Agent for Microsoft Windows, you must obtain and install a license on the protected computer. The license must have a number of instances that is enough to protect a machine with the Server product edition.
- *Workstation* — a commercial edition that offers capabilities for performing data protection tasks on desktop computers and laptops that run the Microsoft Windows OS. To use the Workstation edition of Veeam Agent for Microsoft Windows, you must obtain and install a license on the protected computer. The license must have a number of instances that is enough to protect a machine with the Workstation product edition.
- *Free* — a free edition that offers limited capabilities. In contrast to the Workstation and Server editions, the Free edition does not require a license.

For more information about product editions, pricing and features available for them, see this Veeam webpage.

To learn more about instance licensing, see this Veeam webpage.

When you install a license on the protected computer, you can select the product edition of Veeam Agent for Microsoft Windows: Workstation or Server (if both editions are supported by the license). To learn more, see Selecting Product Edition.

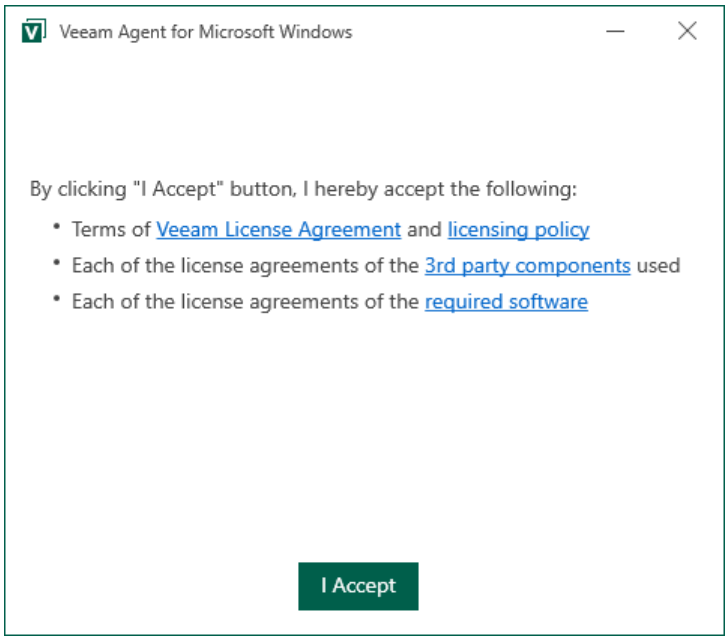
If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you should manage product licenses and editions from the Veeam Backup & Replication console. To learn more, see Managing License.

If the license has expired and you have used backup job options available for the Workstation and Server editions, you must disable these options in the properties of the backup job. Otherwise, the backup job will fail.

License Agreements

When you install Veeam Agent for Microsoft Windows, you must accept the terms of license agreements.

To view the license agreements, click the corresponding links in the installation window.



Installing License

When you launch the Veeam Agent control panel for the first time, Veeam Agent displays a notification window offering to install a license. You can choose to install the license immediately or postpone this operation.

- If you choose to install the license, you can immediately browse for the license key on your computer and complete the license installation process.
- If you choose to postpone the license installation process, you will be able to install a license later at any time you need.

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

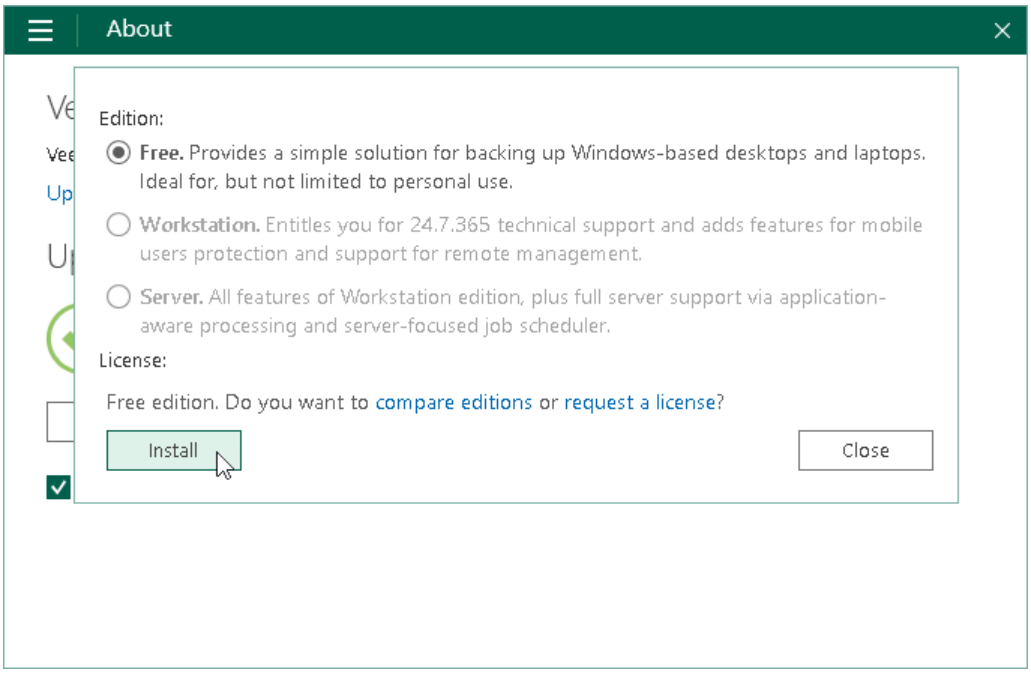
> **NOTE**
>
> If you plan to use a Veeam Backup & Replication repository as a target location for Veeam Agent backups, you must install a license in Veeam Backup & Replication. The license must have enough instances to protect machines with Veeam Agents that back up data to the Veeam Backup & Replication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

To install a license:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **About**.
3. In the **Version** section, click the following link:
   a. **Update license to get additional features** — if the license is not installed yet, and you run the Free edition of Veeam Agent for Microsoft Windows.
   b. **Manage license and edition** — if the license is already installed on the Veeam Agent computer, and you want to change the license or select the product edition.
4. In the dialog window, click **Install** and browse for the LIC file.

   Veeam Agent for Microsoft Windows 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 for Microsoft Windows will select the product edition based on the type of the Microsoft Windows OS installed on the Veeam Agent computer.

You can change the product edition manually if needed. To learn more, see Selecting Product Edition.



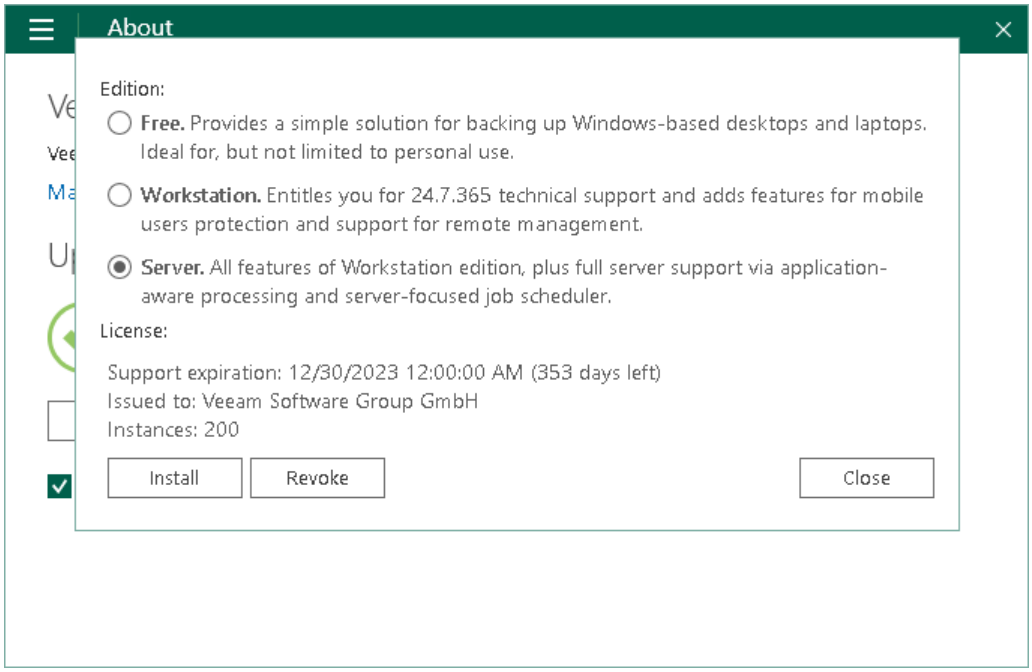
Selecting Product Edition

When you install a license, Veeam Agent for Microsoft Windows automatically selects the product edition that is allowed by the license. If a license supports both the Workstation and Server editions, Veeam Agent for Microsoft Windows will select the product edition based on the type of the Microsoft Windows OS installed on the Veeam Agent computer.

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

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **About**.
3. In the **Version** section, click **Manage license and edition**.
4. In the dialog window, in the **Edition** section, select the desired product edition. To learn more about editions of Veeam Agent for Microsoft Windows, see Product Editions.

> **NOTE**
>
> After you switch from the Server edition to the Workstation edition, or vice versa, Veeam Agent for Microsoft Windows will disable the backup job. 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.

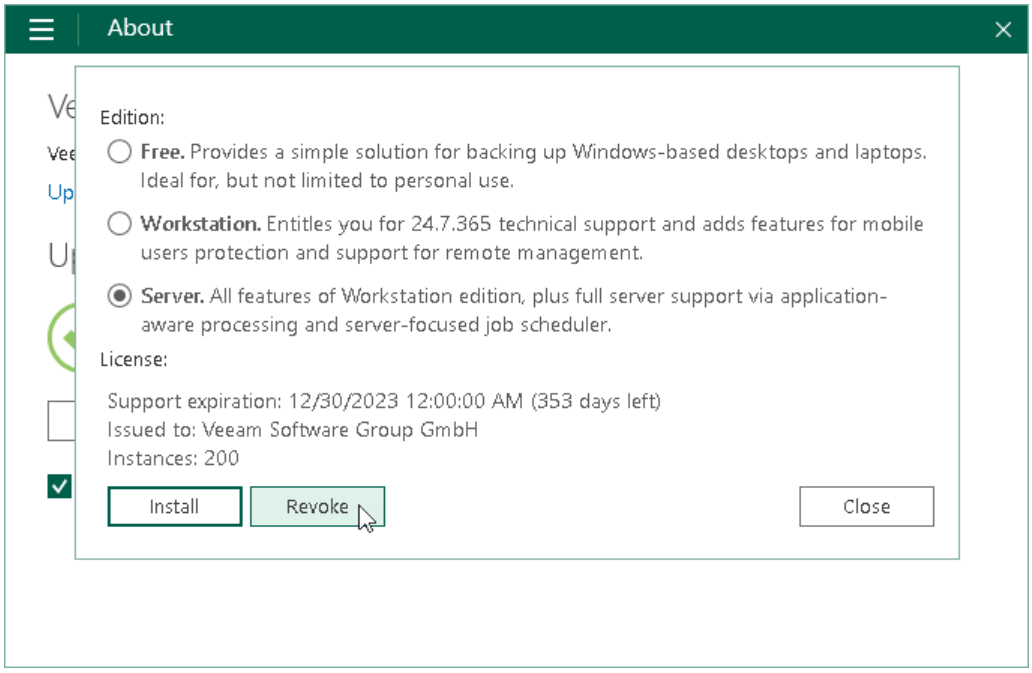


Revoking License

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 Microsoft Windows.

To revoke a license:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **About**.
3. In the **Version** section, click **Manage license and edition**.
4. In the dialog window, click **Revoke**.



Performing Backup

To protect your computer and data, you can perform the following operations:

- Create a Veeam Recovery Media. You can use the Veeam Recovery Media to boot the Microsoft Windows RE from the recovery media in case the OS on your computer fails to start. To learn more, see Creating Veeam Recovery Media and Creating Veeam Recovery Media with Command Line Interface.
- Back up your data. You can back up your data to protect the entire computer image, individual volumes or folders on your computer. Veeam Agent lets you configure a scheduled backup job with the default settings right after the product installation, configure a backup job with custom settings or create ad-hoc backups at any time you need. You can use data backup to restore necessary information if data on your computer gets corrupted or you delete some files and folders by mistake. To learn more, see Creating Backup Jobs.

Creating Veeam Recovery Media

You can create a Veeam Recovery Media — a recovery media for your computer. The Veeam Recovery Media contains all data that is required to run the Microsoft Windows RE. If your computer stops working or the hard disk fails, you can boot from the Veeam Recovery Media, instead of booting from the hard drive. After booting, you can use Veeam and Microsoft tools to fix errors, recover the system image of your computer and your data.

NOTE

In some cases, Windows Recovery Environment components may be missing on the system, and Veeam Agent for Microsoft Windows will not find them during the Veeam Recovery Media creation. In such case you will be prompted to do one of the following:

- Insert the Windows Installation Media so that Veeam Agent for Microsoft Windows can load the necessary components from it.
- Download and install Windows Assessment and Deployment Kit (MS ADK).

Keep in mind that the Veeam Recovery Media created with MS ADK components will not contain the following tools:

- Windows Recovery Environment
- Memory Diagnostic
- Startup Repair

Before You Begin

Before you create a Veeam Recovery Media, check the following prerequisites:

Removable Storage Device Scenario (USB, SD Card and Other)

- The removable storage device must be inserted into a corresponding slot on the computer or connected to the computer.
- The removable storage device must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- During the recovery image creation, Veeam Agent for Microsoft Windows formats the removable storage device. If you have important information on the device, create a copy of this data in some other location.
- If you want to include specific storage and network drivers into the recovery image, place them to a local folder on your computer or in a network shared folder to which you have access and read permissions. During the recovery image creation process, you will be able to define a path to this folder, and Veeam Agent for Microsoft Windows will include the drivers into the recovery image.
- [For Microsoft Windows 2008 R2 and later] If you want your computer to detect a Wi-Fi network and connect to it after you boot from the recovery image, enable the Wireless LAN Service feature on your computer. In this case, Veeam Agent for Microsoft Windows will add wireless networking support files to the Veeam Recovery Media. To learn more about the Wireless LAN Service, see this Microsoft article.

CD/DVD/BD Scenario

- An empty or re-writable CD/DVD/BD must be inserted into a CD/DVD/BD drive on the computer.
- The CD/DVD/BD must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- If you want to include specific storage and network drivers into the recovery image, place them to a local folder on your computer or in a network shared folder on which you have read permissions. During the recovery image creation, you will be able to define a path to this folder, and Veeam Agent for Microsoft Windows will include the drivers into the recovery image.
- [For RW CD/DVD/BD] During the recovery image creation, Veeam Agent for Microsoft Windows erases information on the CD/DVD/BD. If you have important information on the CD/DVD/BD, create a copy of this data in some other location.
- [For Microsoft Windows 2008 R2 and later] If you want your computer to detect a Wi-Fi network and connect to it after you boot from the recovery image, enable the Wireless LAN Service feature on your computer. In this case, Veeam Agent for Microsoft Windows will add wireless networking support files to the Veeam Recovery Media. To learn more about the Wireless LAN Service, see this Microsoft article.

Local Target and Shared Folder Scenario (ISO)

- If you want to include specific storage and network drivers into the recovery image, place them to a local folder on your computer or in a network shared folder on which you have read permissions. During the recovery image creation, you will be able to define a path to this folder, and Veeam Agent for Microsoft Windows will include the drivers into the recovery image.
- [For shared folders] If you plan to save the created ISO file in a network shared folder, make sure that you have access to this folder and write permissions on it.

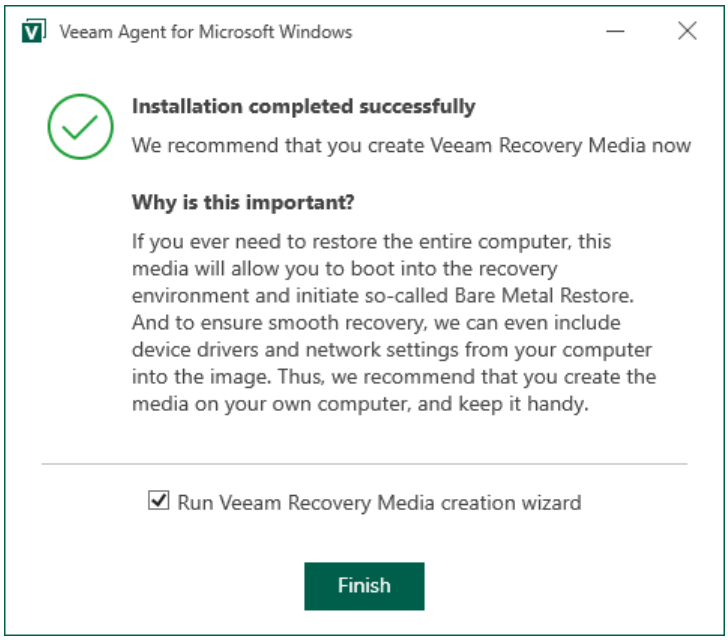
- [For Microsoft Windows 2008 R2 and later] If you want your computer to detect a Wi-Fi network and connect to it after you boot from the recovery image, enable the Wireless LAN Service feature on your computer. In this case, Veeam Agent for Microsoft Windows will add wireless networking support files to the Veeam Recovery Media. To learn more about the Wireless LAN Service, see this Microsoft article.

Step 1. Launch Create Recovery Media Wizard

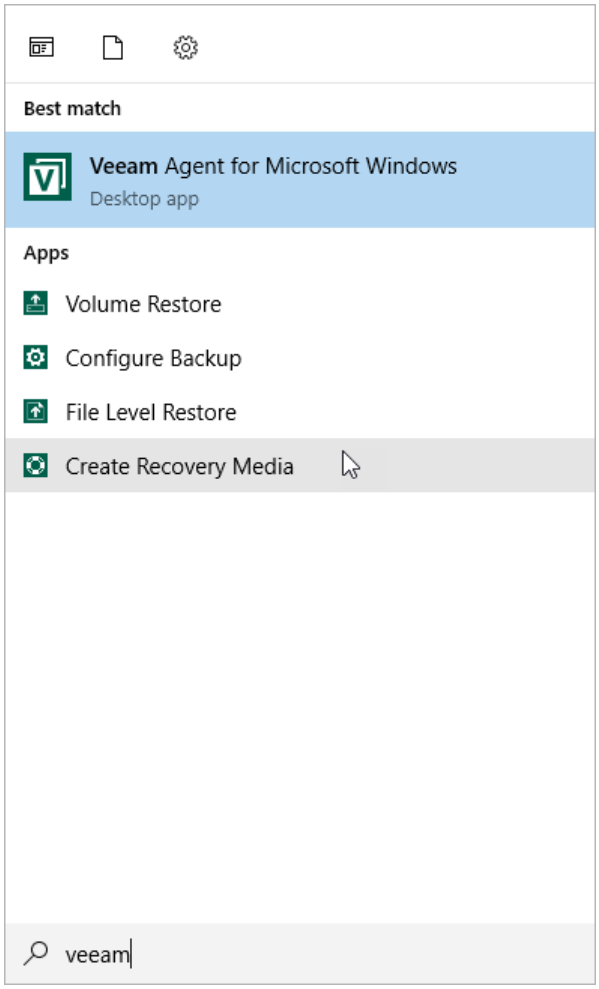
You can launch the **Create Recovery Media** wizard right after the product installation process or at any time later.

To launch the **Create Recovery Media** wizard after installation:

1. At the last step of the installation wizard, select the **Run Veeam Recovery Media creation wizard** check box.
2. Click **Finish**. Veeam Agent for Microsoft Windows will automatically launch the **Create Recovery Media** wizard.



To launch the **Create Recovery Media** wizard at any time, from the Microsoft Windows Start menu, select **All Programs** > **Veeam** > **Tools** > **Create Recovery Media** or use the Microsoft Windows search to find the **Create Recovery Media** option on your computer.


Best match
Veeam Agent for Microsoft Windows
Desktop app
Apps
Volume Restore
Configure Backup
File Level Restore
Create Recovery Media
veeam

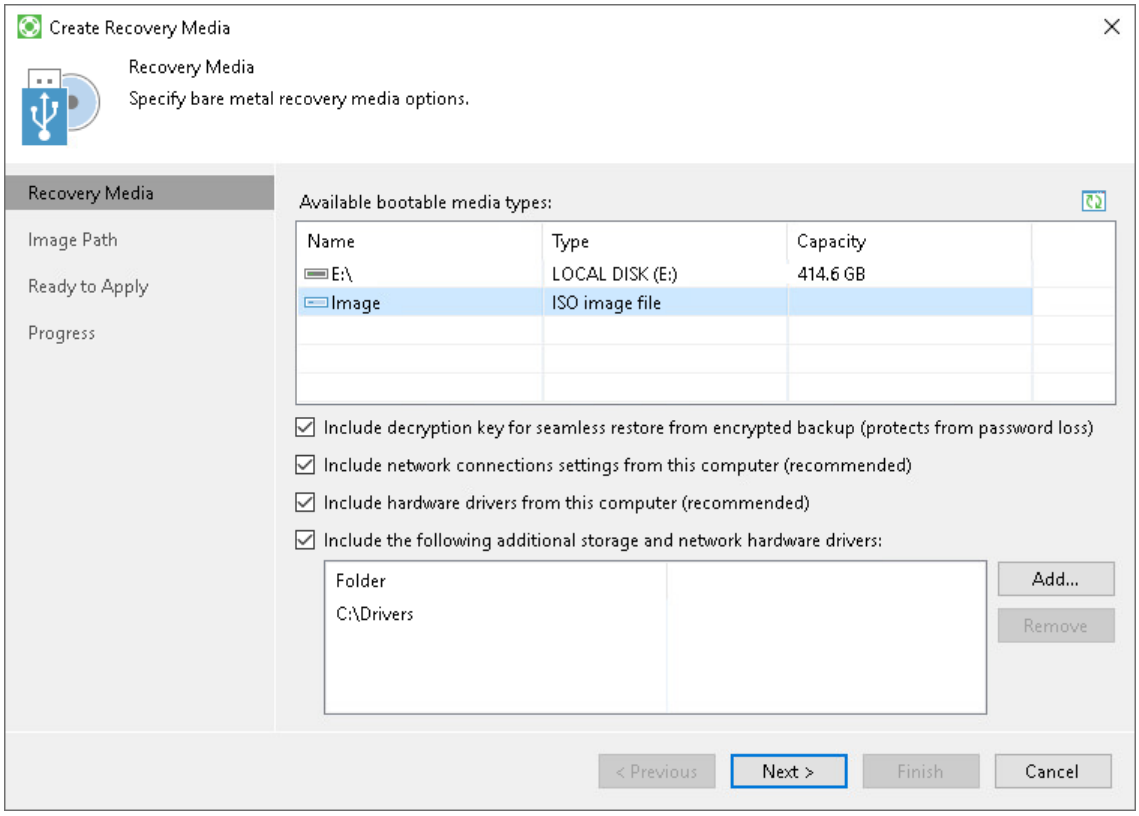
Step 2. Specify Recovery Media Options

At the **Recovery Media** step of the wizard, specify on which type of media you want to create a recovery image and what drivers you want to include in the recovery image.

1. In the **Available bootable media types** list, select a media for the recovery image. You can create the following types of recovery images:
   - Recovery image on a removable storage device. You can create a recovery image on a USB drive, SD card and so on. Veeam Agent for Microsoft Windows displays all removable storage devices currently attached to your computer. Select the necessary one in the list.
   - Recovery image on an optical disk. You can create a recovery image on a CD, DVD or BD. Veeam Agent for Microsoft Windows displays all CD, DVD and BD drives available on your computer. Select the necessary one in the list.
   - ISO file with the recovery image. You can create a recovery image in the ISO file format and save the resulting file locally on your computer or in a network shared folder.
2. If you have enabled data encryption options for the backup job and want to include the decryption key in the recovery image, select the **Include decryption key for seamless restore from encrypted backup** check box. In this case, when you use the created recovery image to perform bare metal recovery, you will not have to enter the password used for encryption.
3. If you want to include in the recovery image current network settings, make sure that the **Include network connections settings from this computer** check box is selected. When you use the created Veeam Recovery Media to boot your computer, these settings will be automatically applied and will be used to connect to the remote backup storage.
4. If you want to include in the recovery image storage and network drivers that are currently installed on your computer, make sure that the **Include hardware drivers from this computer** check box is selected. Veeam Agent for Microsoft Windows will detect hard disk controller drivers, network adapter drivers and USB controller drivers and include them into the recovery image. When you use the created Veeam Recovery Media to boot your computer, these drivers will be automatically injected into Windows RE.
5. If you want to include in the recovery image additional storage and network drivers that you may need when booting from the recovery image, select the **Include the following additional storage and network hardware drivers** check box, click **Add** and select a folder containing necessary drivers. The folder that you select must contain all files of the driver package (files in CAT, INF and SYS formats).

   We strongly recommend that you enable this option if you use drivers that are not included into the Microsoft Windows installation DVD. For example, you can include drivers for a discrete network card, third party USB 3.0 controllers and non-standard hard disk controllers.

> **IMPORTANT**
>
> Consider the following:
>
> - When you boot your computer from the Veeam Recovery Media, Veeam Agent for Microsoft Windows does not automatically install additional drivers included in the recovery image. You need to install such drivers manually using the **Load Driver** tool. To learn more, see Using Veeam Agent and Microsoft Windows Tools.
> - We do not recommend to include large amount of additional drivers (1 GB and more) in the Veeam Recovery Media. When you boot your computer from the Veeam Recovery Media, Veeam Agent for Microsoft Windows loads all additional drivers stored in the Veeam Recovery Media into your computer RAM. If the total size of the recovery environment is approximately equal to or greater than the amount of RAM, Windows RE will fail to load.


Create Recovery Media
Recovery Media
Specify bare metal recovery media options.
Recovery Media
Image Path
Ready to Apply
Progress
Available bootable media types:
Name
Type
Capacity
E:\
LOCAL DISK (E:)
414.6 GB
Image
ISO image file
Include decryption key for seamless restore from encrypted backup (protects from password loss)
Include network connections settings from this computer (recommended)
Include hardware drivers from this computer (recommended)
Include the following additional storage and network hardware drivers:
Folder
C:\Drivers
Add...
Remove
< Previous
Next >
Finish
Cancel

Step 3. Specify Path to ISO

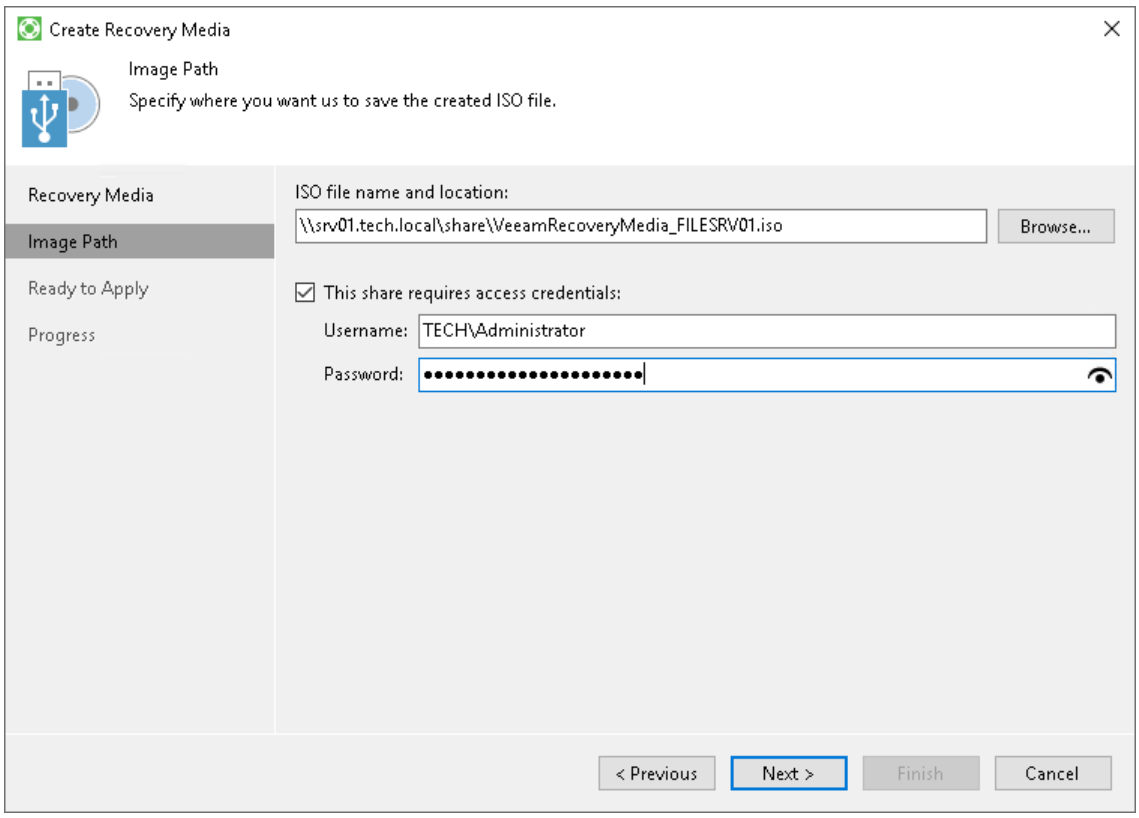
The **Image Path** step of the wizard is available if you have selected to create an ISO file with the recovery image.

Select a location where you want to save the ISO file.

1. In the **ISO file name and location** field, specify a real path to the folder where you want to save the created recovery image and the ISO file name. You can save the ISO file in the following locations:
   - Local folder: select the necessary folder on your computer.
   - Network shared folder: specify a UNC path to a network shared folder. Keep in mind that a UNC path always starts with two back slashes (\\).

   We strongly recommend that you store the recovery image in a location other than a local computer drive. If you choose to save the recovery image in a local folder on your computer, you can copy it to an external location afterwards. In this case, the recovery image will always be available should computer volumes get corrupted or the computer fail to start.
2. If you chose to save the ISO file in a network shared folder and this folder requires authentication, select the **This share requires access credentials** check box and enter the user name and password in the **Username** and **Password** fields. The user name must be specified in the *DOMAIN|UserName* format.

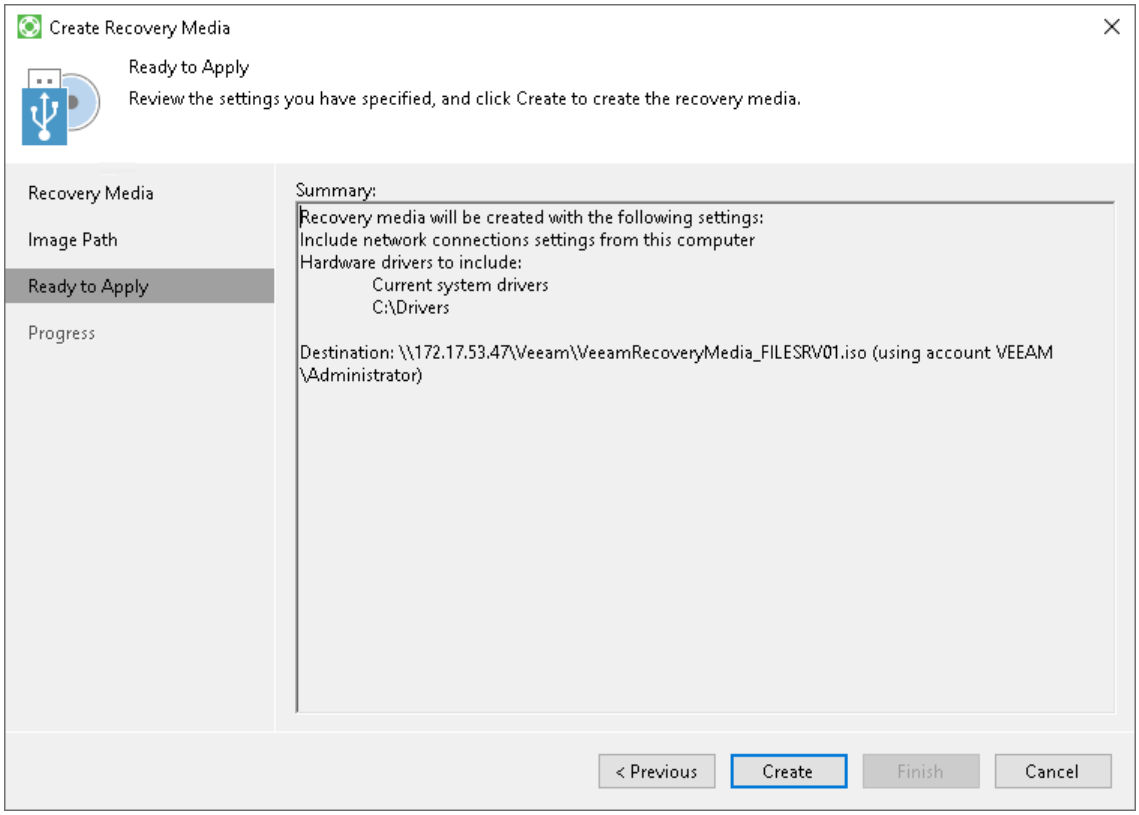
   To view the entered password, click and hold the eye icon on the right of the **Password** field.



Step 4. Review Recovery Image Settings

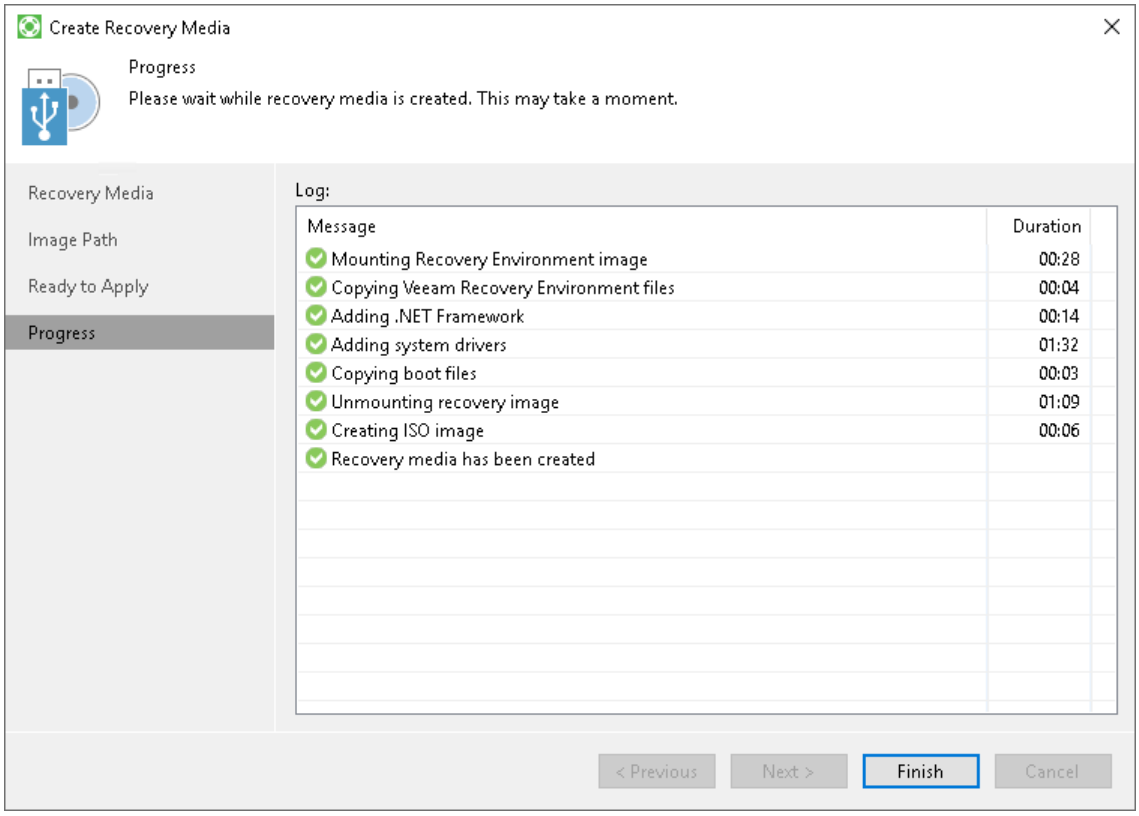
At the **Ready to Apply** step of the wizard, review settings of the recovery image that you plan to create and click **Create**.

Veeam Agent for Microsoft Windows will collect files necessary for recovery image creation and write the resulting recovery image to the specified target or burn it to CD/DVD/BD.



The process of recovery image creation may take some time. Wait for the process to complete and click **Finish** to exit the wizard.

If you want to interrupt the process of recovery image creation, click **Cancel** or close the wizard window.


Create Recovery Media
Progress
Please wait while recovery media is created. This may take a moment.
Recovery Media
Image Path
Ready to Apply
Progress
Log:
Message
Duration
Mounting Recovery Environment image
00:28
Copying Veeam Recovery Environment files
00:04
Adding .NET Framework
00:14
Adding system drivers
01:32
Copying boot files
00:03
Unmounting recovery image
01:09
Creating ISO image
00:06
Recovery media has been created
< Previous
Next >
Finish
Cancel

What You Do Next

[For ISO] After the recovery image is created, you can burn the created ISO to a CD/DVD/BD. To do this, you can use native Microsoft Windows tools or third-party software.

Creating Veeam Recovery Media with Command Line Interface

In addition to creating the Veeam Recovery Media with the **Create Recovery Media** wizard, you can also use the command line interface to create the recovery image and save it as an ISO file. To create the Veeam Recovery Media, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /createreco
verymediaiso /f:<location>\<name>.iso
```

where:

- `<location>` — path to the folder in which the recovery image ISO file will be created. All folders that are mentioned in the path must be created in advance. Names of folders in the path must not contain spaces.
- `<name>` — name of the resulted ISO file. The file name must not contain spaces.

NOTE

Consider the following:

- When you create the Veeam Recovery Media using the command line interface, Veeam Agent for Microsoft Windows includes in the recovery image storage and network drivers that are currently installed on the Veeam Agent computer, and current network settings of this computer. If you want to include additional drivers or data decryption key in the recovery image, you must create the Veeam Recovery Media using the **Create Recovery Media** wizard. To learn more, see Creating Veeam Recovery Media.
- If you do not use the `/f:` option to specify a path to the folder in which to save the resulting ISO file, Veeam Agent for Microsoft Windows will save the ISO file to the `C:\Users\%UserProfile%\Documents` folder with the `VeeamRecoveryMedia_<machine>.iso` name, where `<machine>` — name of your Veeam Agent computer.
- You cannot save the ISO file to a network shared folder using the command line interface.

You can use the last exit code to verify if the backup job has completed successfully. To check the last exit code, use the %ERRORLEVEL% variable in cmd.exe. Veeam Agent can provide the following exit codes:

- 0 — recovery image successfully created
- 1 — the create recovery image operation failed

Example of Use

The example below creates an ISO file with the `VeeamRE` name in the E:\Veeam\RecoveryImage folder.

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /createreco
verymediaiso /f:E:\Veeam\RecoveryImage\VeeamRE.iso
```

Creating Backup Jobs

To back up your data, you must configure a backup job. The backup job defines how, where and when to back up data. You can choose one of the following backup types:

- Backup of an entire computer image
- Backup of specific computer volumes, for example, a system volume or secondary volume
- Backup of individual folders, for example, documents folder or folder with music

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. The required space depends on the size of backed-up data and backup job settings.
- Available backup job options depend on the edition of Veeam Agent for Microsoft Windows. Make sure that you have obtained and installed a license that has the desired number of instances. To learn more, see Licensing.
- [For Veeam Backup & Replication repository targets] You can store created backups in a backup repository only if the backup server runs Veeam Backup & Replication 12. If you plan to use a commercial version of Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install a license in Veeam Backup & Replication that has a sufficient number of instances to protect machines with Veeam Agent. To learn more, see Managing License.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must preconfigure user access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
- [For Veeam Cloud Connect repository targets] If you plan to use a cloud repository as a target for backups, make sure that the service provider has communicated to you the necessary data: cloud gateway settings, user account settings and certificate thumbprint.
- A user account under which you launch the **New Backup Job** wizard must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.

Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.
- Keep in mind that Veeam Agent stops running the backup job after 3 weeks.

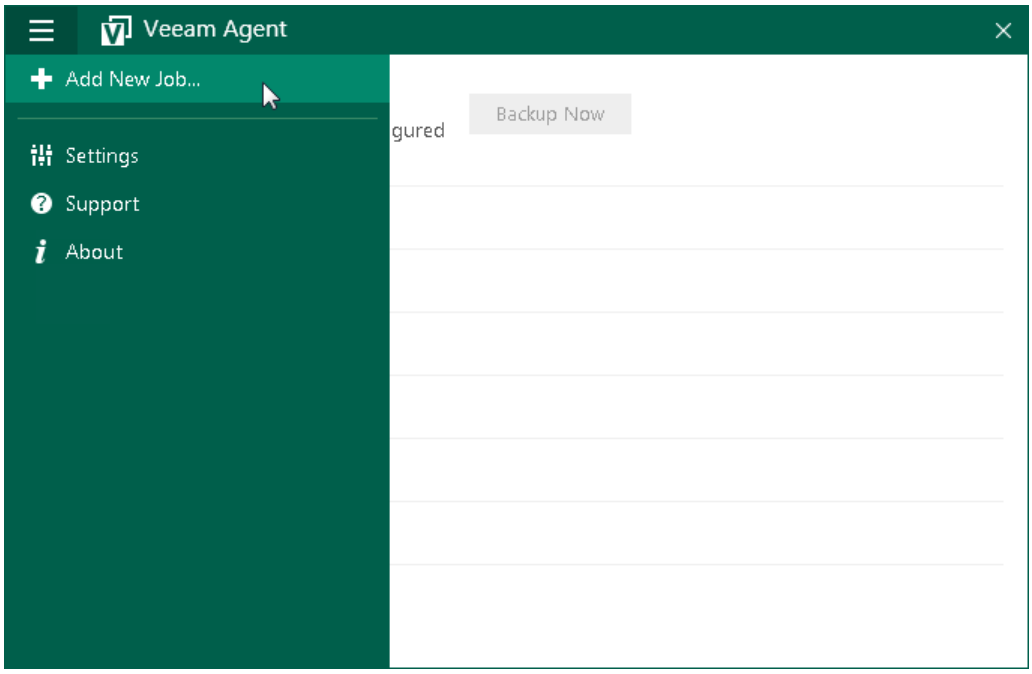
Step 1. Launch New Backup Job Wizard

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

- [If no backup jobs are configured] Double-click the Veeam Agent for Microsoft Windows icon in the system tray.
- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Backup** > **Configure backup**.

> **NOTE**
>
> The **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent for Microsoft Windows.

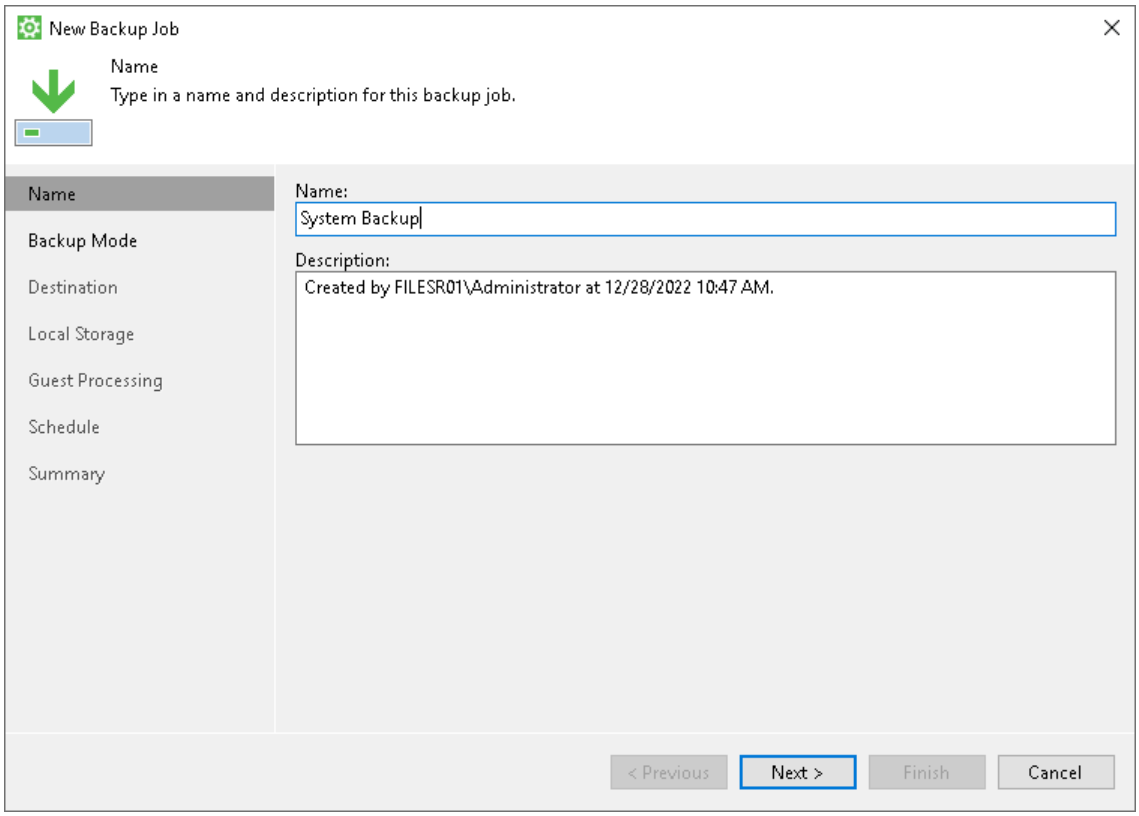
- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**. Then, from the main menu, select **Add New Job**.
- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Tools** > **Configure Backup** or use the Microsoft Windows search to find the *Configure Backup* option on your computer.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the backup job.

1. In the **Name** field, enter a name for the backup job.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the job, date and time when the job was created.

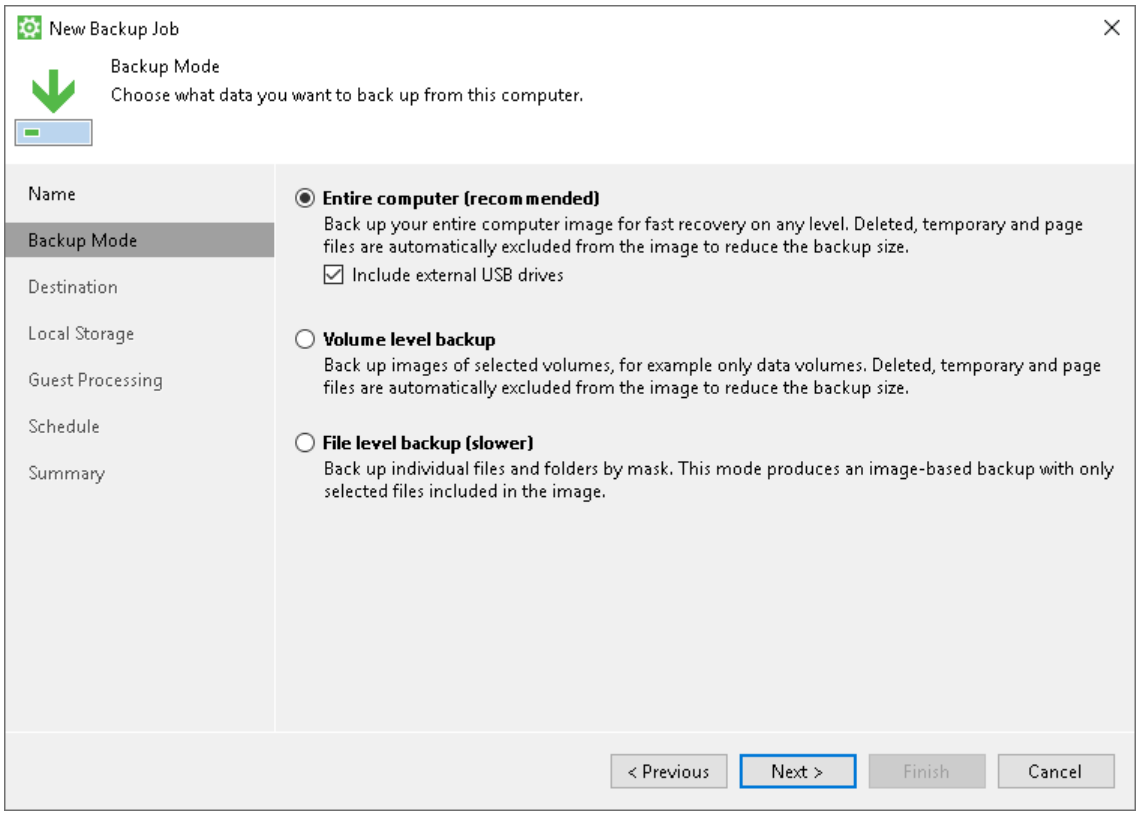


Step 3. Select Backup Mode

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

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:
   - **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on. With this option selected, you will pass to the Destination step of the wizard.
   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, all volumes except the system one. When you restore data from such backup, you will be able to recover data on these volumes only: files, folders, application data and so on. With this option selected, you will pass to the Volumes step of the wizard.
   - **File level backup** — select this option if you want to create a backup of individual folders on your computer. When you backup data in this mode, you can configure additional rules to include/exclude files of the specific type in/from your backup. When you restore data from such backup, you will be able to recover backed-up files and folders. With this option selected, you will pass to the Files step of the wizard.
2. [For entire computer backup] If you want to include in the backup one or more external USB drives, select the **Include external USB drives** check box. With this option selected, Veeam Agent for Microsoft Windows will include in the backup all supported external drives that are connected to the Veeam Agent computer at the time when the backup job starts. Veeam Agent for Microsoft Windows supports backup of external drives that support Microsoft VSS: HDD, SSD, and so on. USB flash drives (USB sticks) are not supported. To learn more, see Backup of External Drives.

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


New Backup Job
Backup Mode
Choose what data you want to back up from this computer.
Name
Backup Mode
Destination
Local Storage
Guest Processing
Schedule
Summary
Entire computer (recommended)
Back up your entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
Include external USB drives
Volume level backup
Back up images of selected volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
File level backup (slower)
Back up individual files and folders by mask. This mode produces an image-based backup with only selected files included in the image.
< Previous
Next >
Finish
Cancel

Step 4. Specify Backup Scope Settings

Specify backup scope for the backup job:

- Select volumes to back up — if you have selected the **Volume level backup** option at the Backup Mode step of the wizard.
- Select folders to back up — if you have selected the **File level backup** option at the Backup Mode step of the wizard.

Selecting Volumes to Back Up

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

At this step of the wizard, you must specify the backup scope — define what volumes you want to include in the backup.

To specify the backup scope, choose volumes and objects that you want to include in the backup. You can include the following data in the backup:

- Computer volumes (located on local drives or external USB drives). To include individual volumes of your computer to the backup scope, select check boxes next to necessary volumes.

  If you select all volumes at this step of the wizard, Veeam Agent will create a backup of the entire computer image. However, if a new volume appears on a Veeam Agent computer, Veeam Agent will not include this volume in the backup scope automatically. Veeam Agent will back up only those volumes that are explicitly selected for backup.

  > **NOTE**
  >
  > You cannot include in the backup volumes located on virtual hard disks (VHD or VHDX).

- Mount points. To include individual volumes mounted on your computer to the backup scope, select check boxes next to necessary mount points.

  In the list of objects to back up, Veeam Agent displays available mount points after volumes.

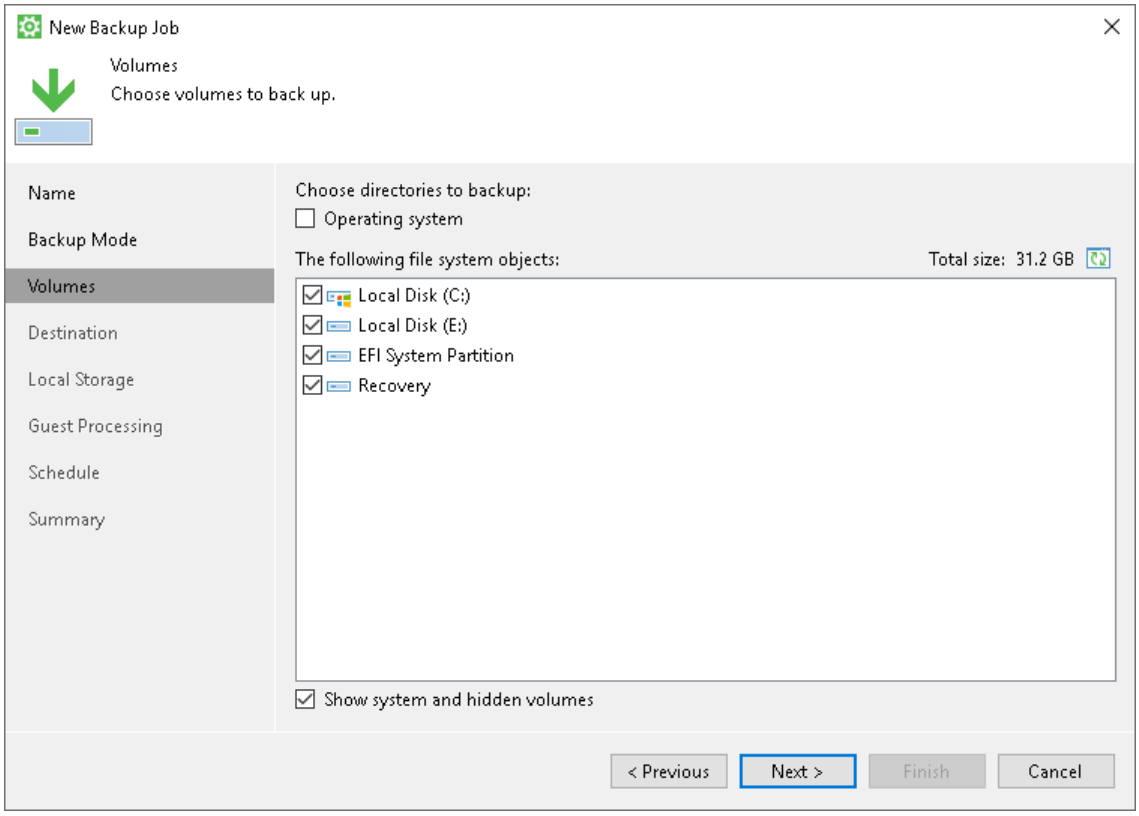
- System state data. To include system state data into the backup, do one of the following:

  - In the **Choose directories to backup** list, select the **Operating system** check box.
  - In the **The following file system objects** list, select the check box next to the system volume. Typically, the system volume is the **Local Disk (C:)** volume.
  - Select the Show system and hidden volumes check box at the bottom of the window. In the **The following file system objects** list, select the **System Reserved** check box and the check box next to the system volume. Typically, the system volume is the Local Disk (C:) volume.

  Veeam Agent for Microsoft Windows will include in the backup scope the Microsoft Windows system partition and boot partition of your computer. For GPT disks on Microsoft Windows 8.1, 10, 11, 2012, 2012 R2, 2016, 2019 and 2022, Veeam Agent will additionally back up the recovery partition. To learn more, see System State Data Backup.

When you include a system volume in the backup, Veeam Agent automatically includes the System Reserved/UEFI or other system partitions in the backup too. If you do not want to back up the system state data, you can clear the **System Reserved/EFI System Partition** check box. However, in this case Veeam Agent does not guarantee that the OS will boot properly when you attempt to recover from such backup. To learn more, see System State Data Backup.

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



Selecting Folders to Back Up

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

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

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

At this step of the wizard, you must specify the backup scope — define what folders with files or entire volumes you want to include in the backup.

To specify the backup scope, select check boxes next to necessary objects. You can include the following data in the backup:

- Operating system data — data related to the OS installed on your computer.
- Personal files — data related to user profiles. With this option enabled, Veeam Agent for Microsoft Windows will include in the backup scope settings and data related to Veeam Agent computer user profiles.

  You can specify what personal data to include in the backup and choose whether to exclude roaming profiles from the backup. To do this, click **Choose** next to the **Personal files** field and select the necessary options in the **Personal Folders** window. To learn more, see Personal Data Backup.

- System reserved data — system data required to boot the OS installed on your computer. With this option enabled, Veeam Agent for Microsoft Windows will include in the backup scope Microsoft Windows system partition and boot partition of your computer. For GPT disks on Microsoft Windows 8.1, 10, 11, 2012, 2012 R2, 2016, 2019 and 2022, Veeam Agent for Microsoft Windows will additionally back up the recovery partition. To learn more, see System State Data Backup.
- Individual folders. To learn more, see Selecting Folders.
- Individual computer volumes and mount points (located on local drives or external USB drives). To learn more, see Selecting Volumes.

IMPORTANT

Consider the following:

- Veeam Agent for Microsoft Windows does not include the following Microsoft Windows objects in the backup: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.

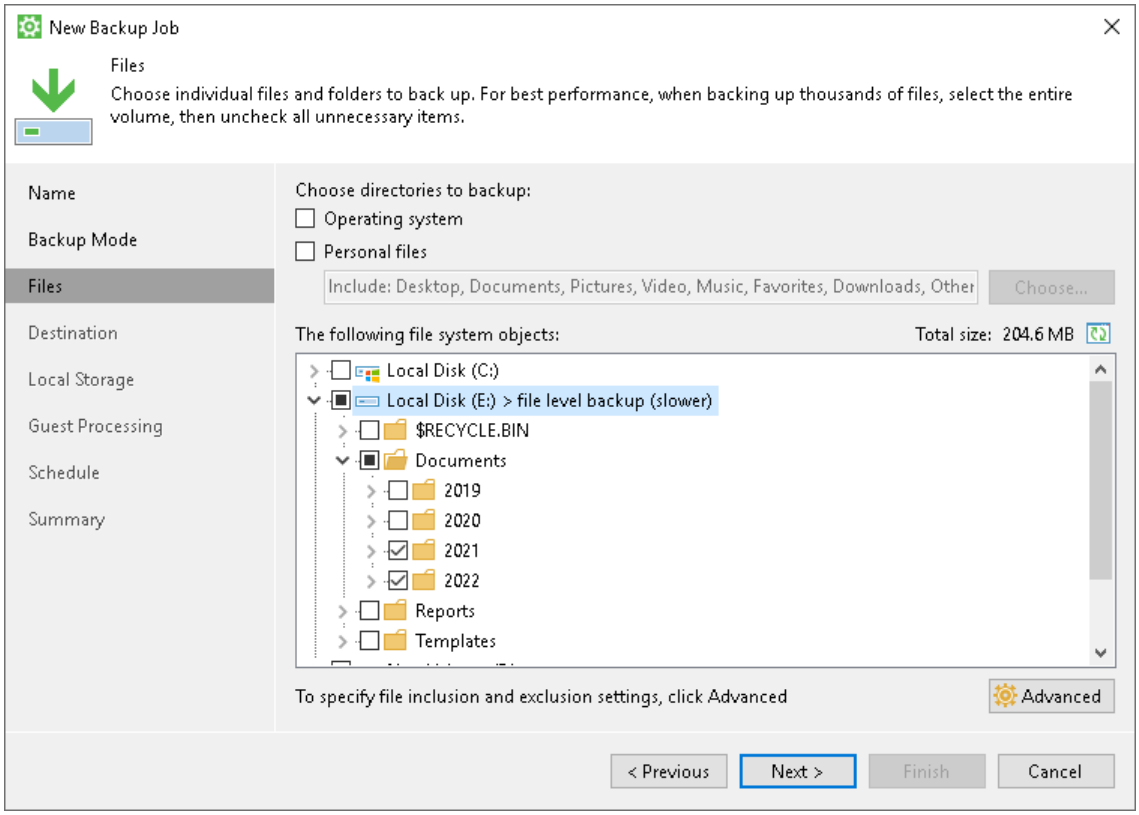
  Also, Veeam Agent does not include in the file-level backup files encrypted with Windows Encrypting File System (EFS).
- If you have a file-level backup job configured and need to extend the volume where backed-up files reside, we strongly recommend to create an active full backup after the volume is extended. Otherwise, Veeam Agent may skip files during the job run even if these files are added to the backup scope. To learn more, see Creating Active Full Backups.

Selecting Folders

To include a folder in the file-level backup:

1. In the **The following file system objects** list, browse to the folder that you want to back up and select the check box next to this folder.

   After you select a folder, Veeam Agent will display the *file level backup* mark next to the volume that contains this folder.
2. If you want to include or exclude files of a specific type in/from the backup, click **Advanced**. To learn more, see Configuring Filters.



Alternatively, if you want to quickly include a large number of folders in the backup, you can select folders in the following way:

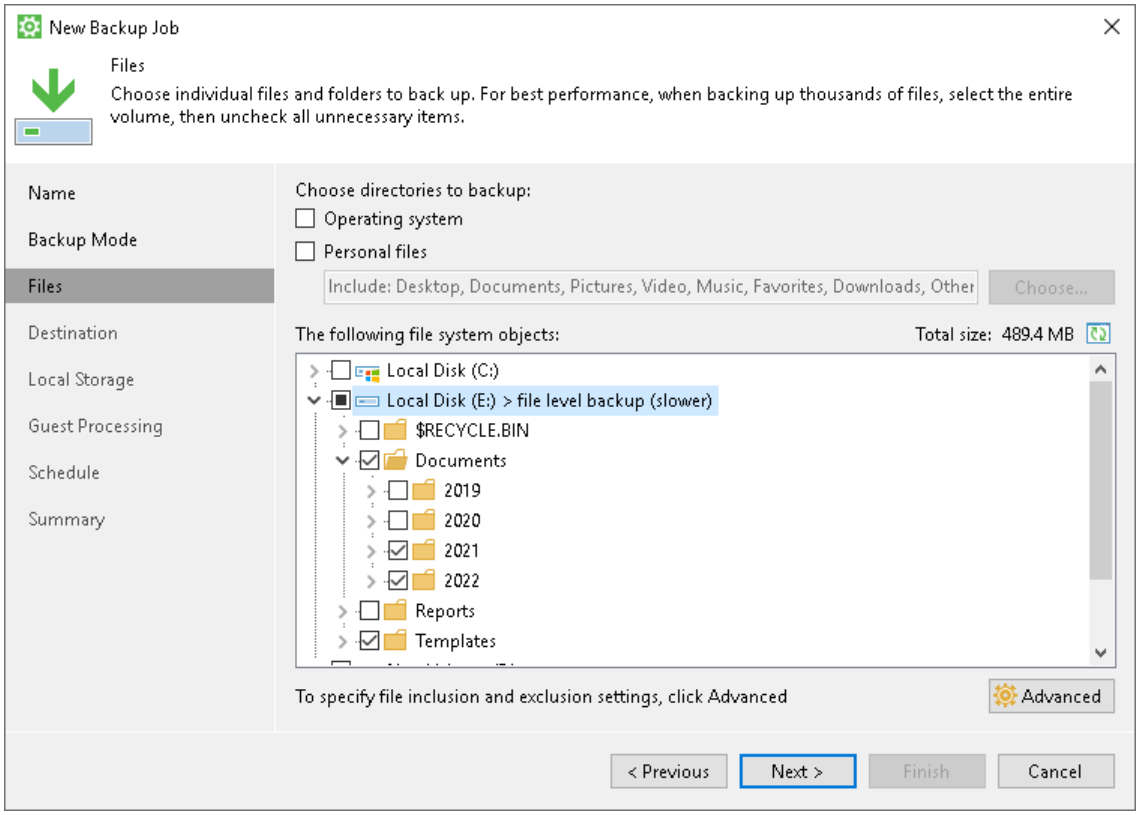
1. Select the check box next to the volume that contains folders you want to back up.

   Veeam Agent will display the *volume level backup* mark next to the selected volume.

2. Expand the volume and clear the check boxes next to one or more folders that you want to exclude from the backup.

3. Select the check box next to the volume once again.

   Veeam Agent will display the *file level backup* mark next to the volume. You can include or exclude files that reside on this volume in/from the backup. To learn more, see Configuring Filters.



Selecting Volumes

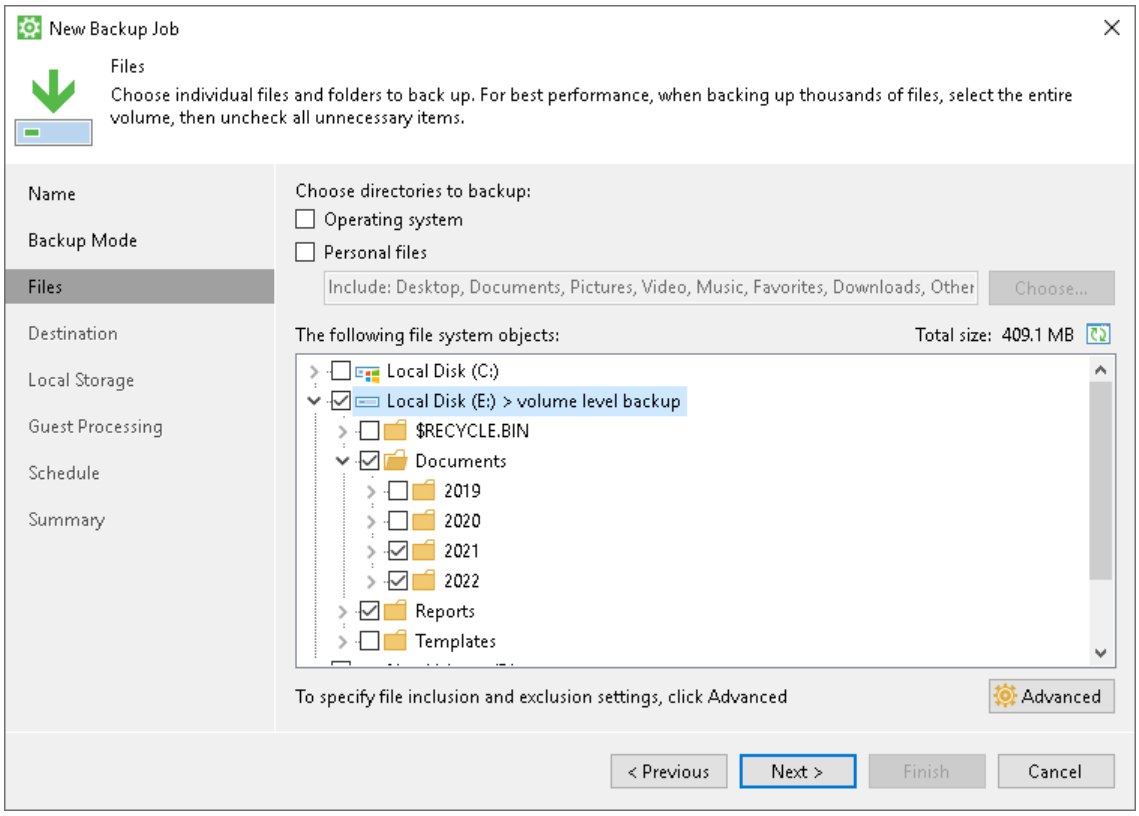
You can include individual volumes in the backup at the **Files** step of the wizard. This may be useful if you want to have a volume-level backup of the volume with specific folders excluded. Volume-level backup also offers better performance in case you back up a complex folder structure with many files.

You can also include individual mount points in the backup at the **Files** step of the wizard, but you cannot exclude folders from mount points.

To include a volume or a mount point in the file-level backup:

1. In the **The following file system objects** list, select the check box next to the item that you want to back up.
2. If you want to exclude a folder on the selected volume from the backup, expand the volume and clear the check box next to the necessary folder.

> **IMPORTANT**
>
> Consider the following:
>
> - If you select a volume for backup, you cannot use filters to include or exclude files of a specific type in/from the backup. You can only exclude specific folders that reside on the volume. If you want to include or exclude files, you must select individual folders for backup. To learn more, see Selecting Folders.
> - If you select a deduplicated volume for backup, make sure that you do not exclude any folders from the backup. Otherwise, the backup files may get corrupted.



Configuring Filters

To include or exclude files of a specific type in/from the file-level backup, you can configure filters.

> **NOTE**
>
> Veeam Agent for Microsoft Windows applies filters to files in specific folders that you include in the backup. Filters are not applied to computer volumes and mount points selected for backup. If you plan to create a hybrid backup that will contain volumes, mount points, and folders, filters will be applied to files in folders only.

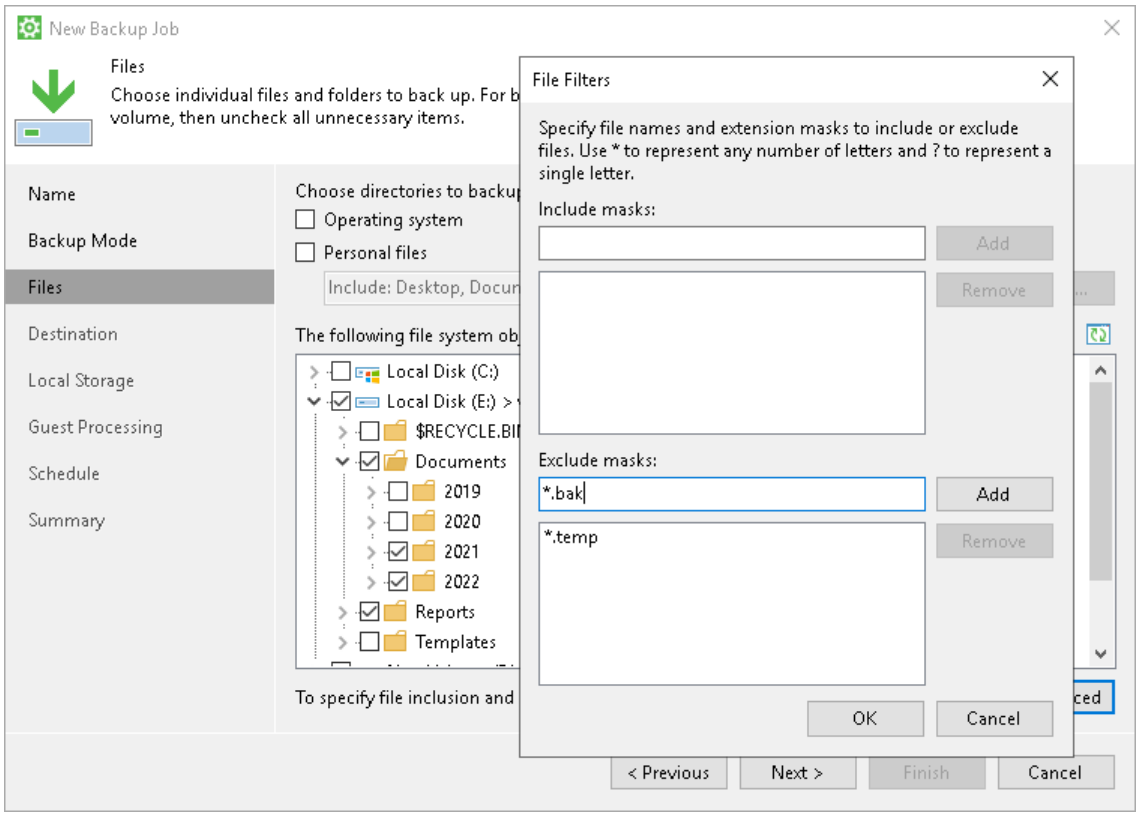
To configure a filter:

1. At the **Files** step of the wizard, click **Advanced**.
2. Specify what files you want to back up:
   - In the **Include masks** field, specify file names and masks for file types that you want to back up, for example, `MyMovie.avi`, `*filename*`, `*.docx`, `*.mp3`. Veeam Agent will create a backup only for selected files. Other files will not be backed up.
   - In the **Exclude masks** field, specify file names and masks for file types that you do not want to back up, for example, `OldPhotos.rar`, `*.temp`, `*.tmp`, `*.back`. Veeam Agent will back up all files except files of the specified type.
3. Click **Add**.
4. Repeat steps 2–3 for each mask that you want to add.

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

- Include mask: `*.avi`
- Exclude mask: `*movie*`

Veeam Agent will include in the backup all files of the AVI format that do not contain *movie* in their names.



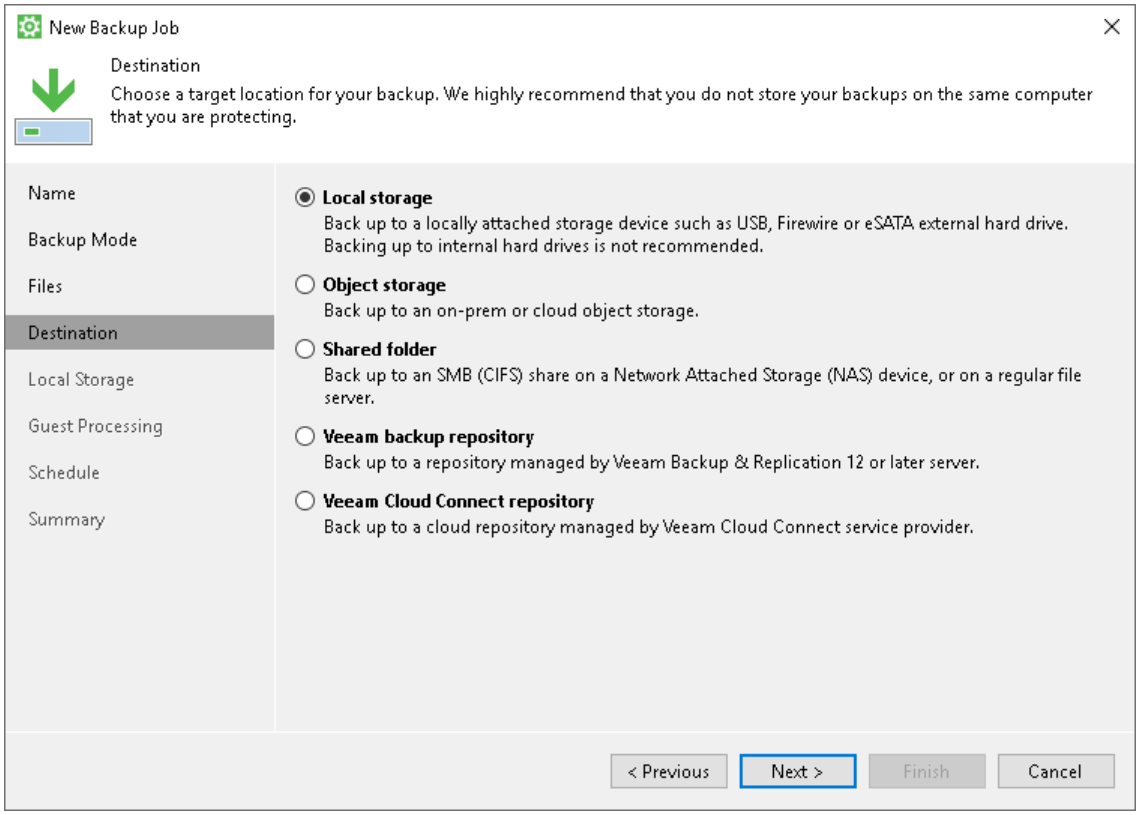
Step 5. Select Backup Destination

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

You can store backup files in one of the following locations:

- **Local storage** — select this option if you want to save the backup on a removable storage device attached to the computer or on a local computer drive. With this option selected, you will pass to the Local Storage step of the wizard.
- **Object storage** — select this option if you want to save the backup in object storage. With this option selected, you will pass to the Object storage step of the wizard.
- **Shared folder** — select this option if you want to save the backup in a network shared folder. With this option selected, you will pass to the Shared folder step of the wizard.
- **Veeam backup repository** — select this option if you want to save the backup 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 save the backup 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.

> **IMPORTANT**
>
> Consider the following:
>
> - We strongly recommend that you store backups in the external location like USB storage device or shared network folder. You can also keep your backup files on the separate non-system local drive.
> - If you select to store the backup in a local folder included in the backup scope, Veeam Agent will automatically exclude this folder from the backup.
> - For the Free product edition, the **Object storage** and the **Veeam Cloud Connect repository** options are not available.


New Backup Job
Destination
Choose a target location for your backup. We highly recommend that you do not store your backups on the same computer that you are protecting.
Name
Backup Mode
Files
Destination
Local Storage
Guest Processing
Schedule
Summary
Local storage
Back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.
Object storage
Back up to an on-prem or cloud object storage.
Shared folder
Back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.
Veeam backup repository
Back up to a repository managed by Veeam Backup & Replication 12 or later server.
Veeam Cloud Connect repository
Back up to a cloud repository managed by Veeam Cloud Connect service provider.
< Previous
Next >
Finish
Cancel

Step 6. 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 **Shared folder** 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.

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 **Local drives** list, select a drive 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. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.
4. Specify short-term backup retention policy settings:
   - [For Free and Workstation product editions] In the **Keep backups for <N> days (excluding days with no backup)** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days. After this period is over, Veeam Agent will remove the earliest restore points from the backup chain.

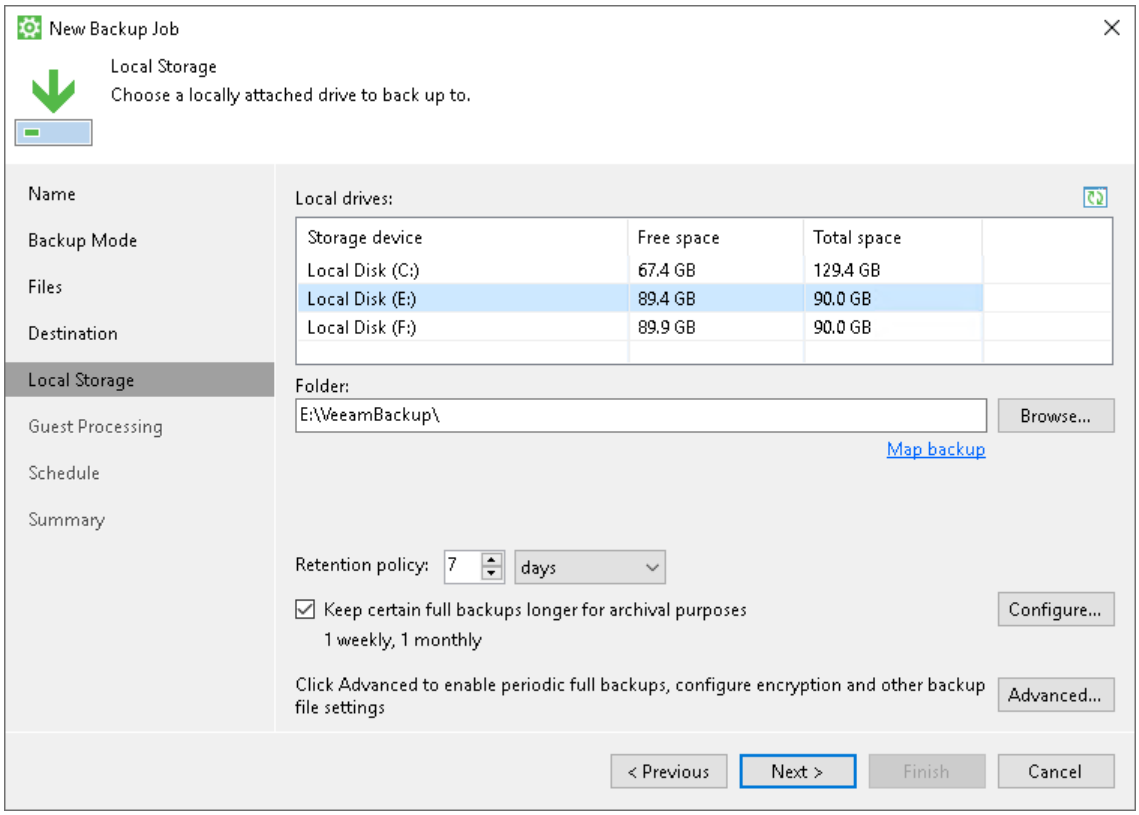
     To learn more, see Backup Retention Policy in Free and Workstation Editions.
   - [For Server product edition] In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.
     - Select the **restore points** option if you want Veeam Agent to remove restore points from the backup chain when the number of restore points exceeds the specified limit.
     - Select the **days** option if you want Veeam Agent to remove the earliest restore points from the backup chain when the specified period is over.

     To learn more, see Backup Retention Policy in Server Edition.

5. [For Workstation and Server product editions] To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep some periodic full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the Long-Term Retention Policy section in the Veeam Backup & Replication User Guide.

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

> **IMPORTANT**
>
> USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, we recommend that you do not use such USB storage devices as a backup target.



Mapping Backup Job

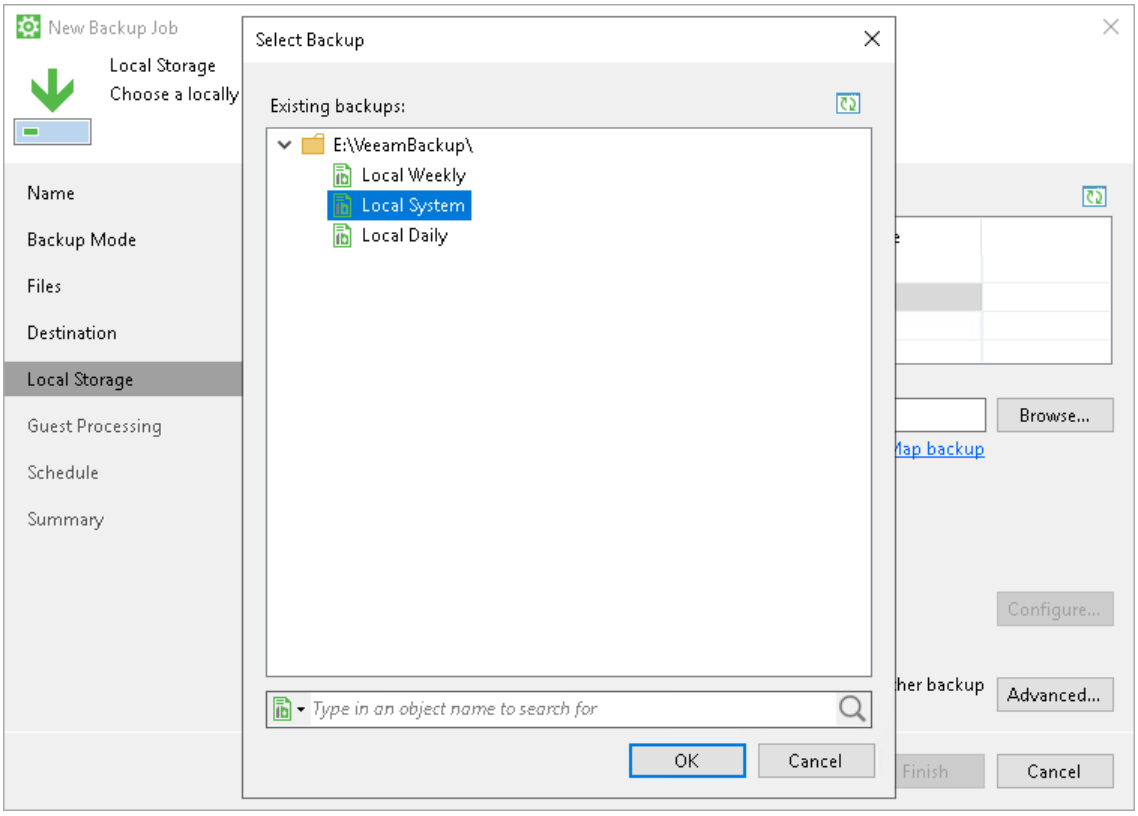
If you have selected to map the job to the already created backup that is stored on a local drive, perform the following steps:

1. In the **Folder** field, specify the same path as was specified in the **Folder** field for the job that was used to create the backup.

2. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays backups stored in the folder that is specified in the **Folder** field and its first-level subfolders.

3. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Object Storage Settings

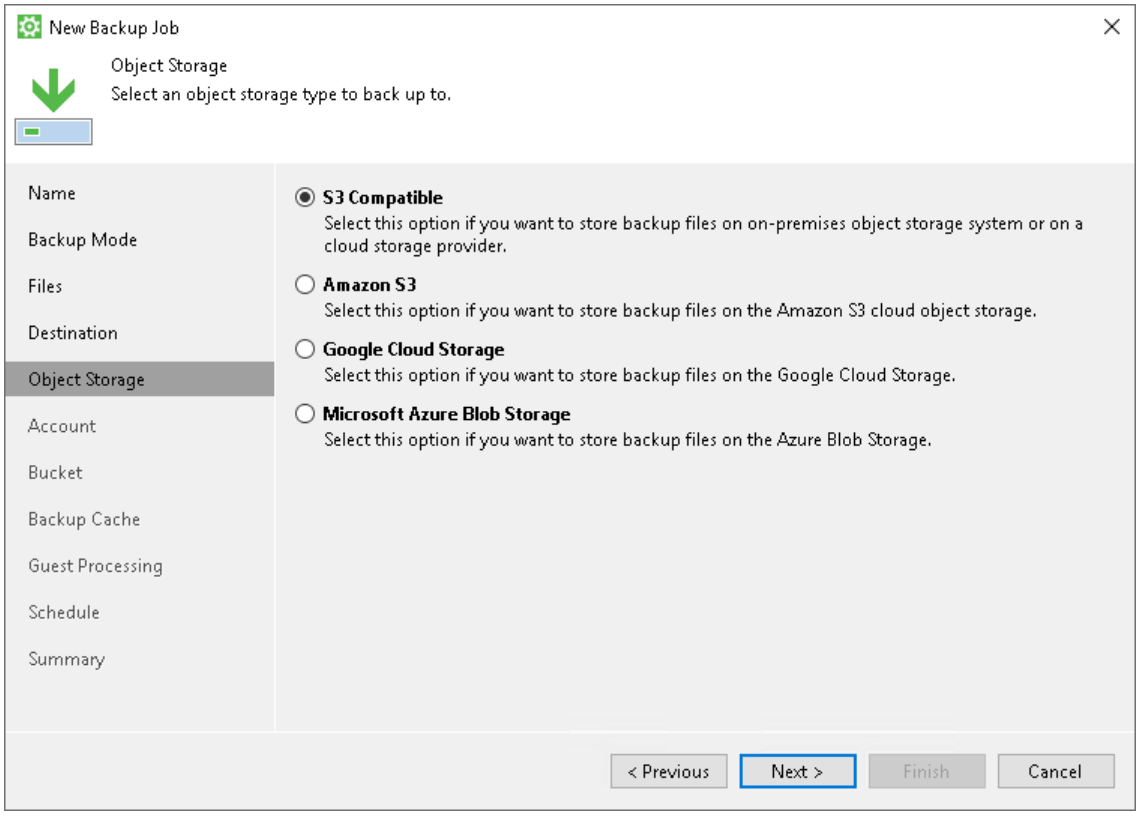
The **Object Storage** step of the wizard is available if you have selected the **Object storage** option at the Destination step of the wizard.

At the **Object Storage** step of the wizard, select the object storage. You can select one of the following options:

- **S3 compatible** — select this option if you want to create a backup in the S3 compatible storage. With this option selected, you will pass to the Account step of the wizard.

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

- **Amazon S3** — select this option if you want to create a backup in the Amazon S3 storage. 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 the Google Cloud storage. With this option selected, you will pass to the Account step of the wizard.
- **Microsoft Azure Blob Storage** — select this option if you want to create a backup in the Microsoft Azure storage. 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 in the S3 compatible storage, specify the following settings:

1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files in object storage.

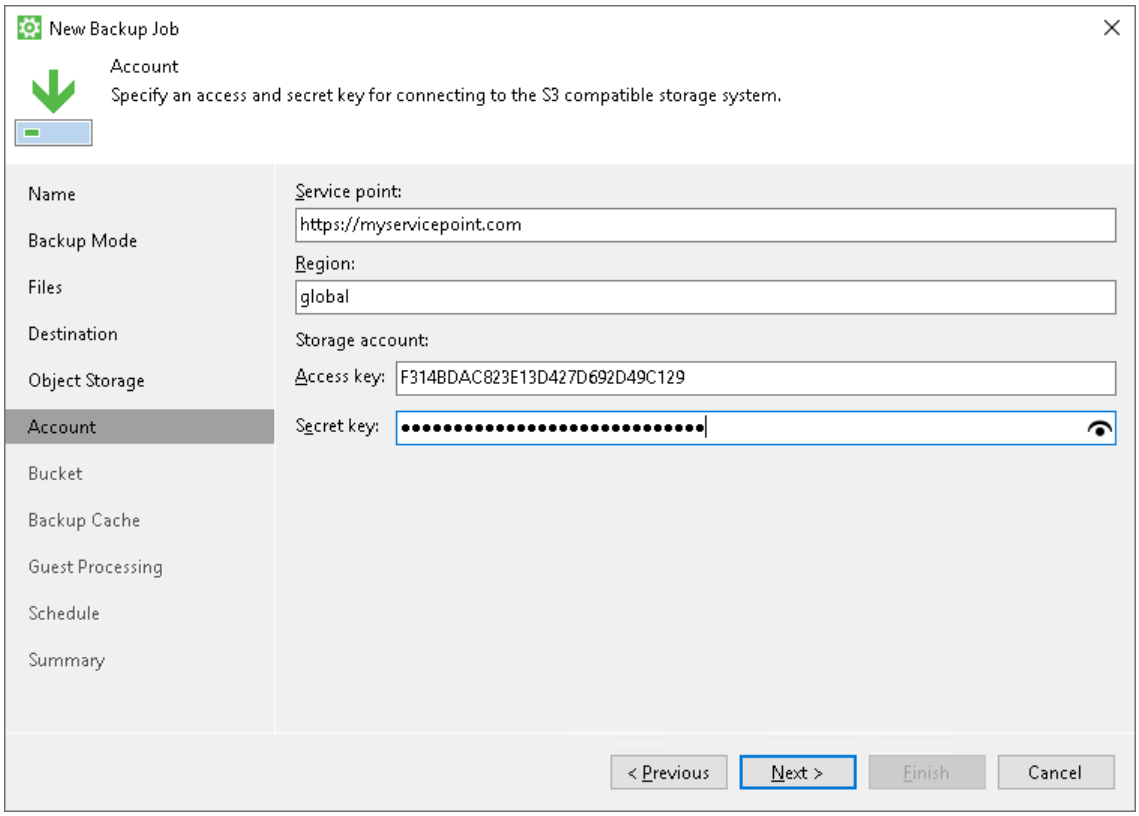
To connect to the S3 compatible storage, specify the following:

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

   > **NOTE**
   >
   > If you want to connect to the repository using an IPv6 address and port number, you must use the following format: `IPv6:port`, where:
   >
   > - `IPv6` is the ipv6-literal.net notation of the IPv6 address.
   > - `port` is the number of the port that Veeam Agent will use to connect to the cloud storage.
   >
   > For example: `https://2001-db8-1--bb8-c0b8-112.ipv6-literal.net:9000`

2. In the **Region** field, specify the storage region based on your regulatory and compliance requirements.
3. In the **Access key** field, enter the access key ID.

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



Specifying Bucket Settings

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

Specify settings for the bucket in the storage:

1. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.

> **NOTE**
>
> You cannot select a folder that is managed by the Veeam Backup & Replication server.

If necessary, you can create a new folder. To do this, click the **New Folder** option in the **Select Folder** window.

3. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.

4. In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

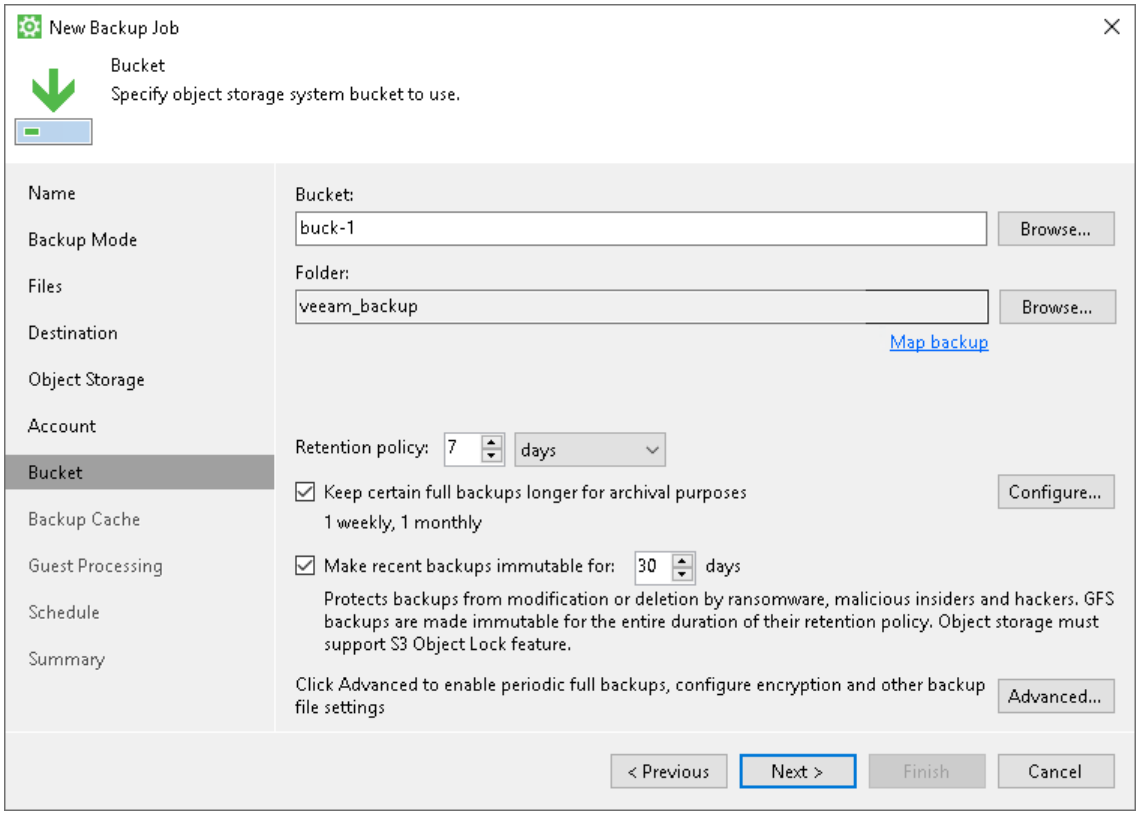
   To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see Long-Term Retention Policy.

5. To protect recent backups from modifications, select the **Make recent backups immutable for <N> days** check box and specify the number of days for which you want to keep your backups immutable. By default, Veeam Agent keeps backups immutable for 30 days. To learn more, see Backup Immutability.

   > **NOTE**
   >
   > If you use the GFS retention scheme and enable immutability for a backup, the restore points with GFS flags become immutable for the whole GFS retention period. You will not be able to delete such restore points till the end of the GFS retention period.

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

After that, Veeam Agent will create a new repository in the cloud storage where you can store backups.



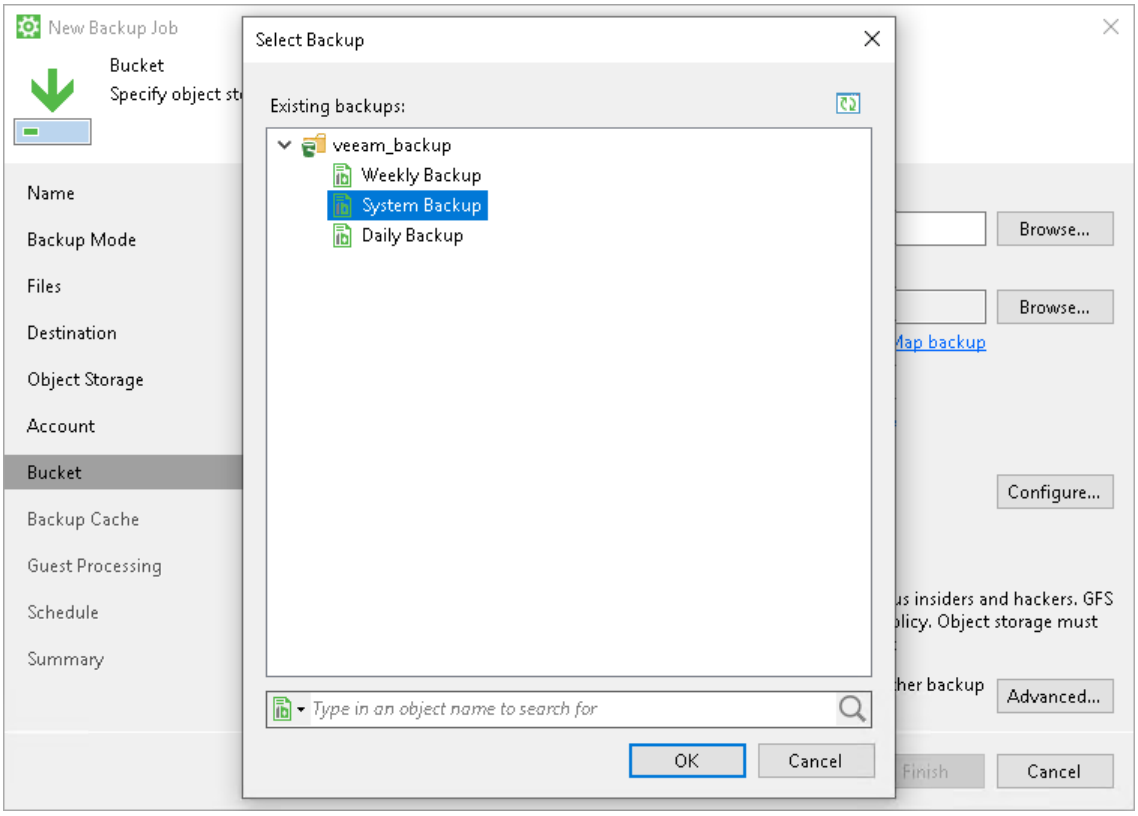
Mapping Backup Job

Starting from Veeam Agent for Microsoft Windows version 6.1, you can map the job to the already created backup that is stored in the S3 compatible storage. To map the backup job, perform the following steps:

1. In the **Bucket** field, specify a bucket where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.

      > **NOTE**
      >
      > You cannot select a folder that is managed by the Veeam Backup & Replication server.
3. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same account used to connect to the S3 compatible storage.
4. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Amazon S3 Settings

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

1. Specify account settings.
2. Specify bucket settings.

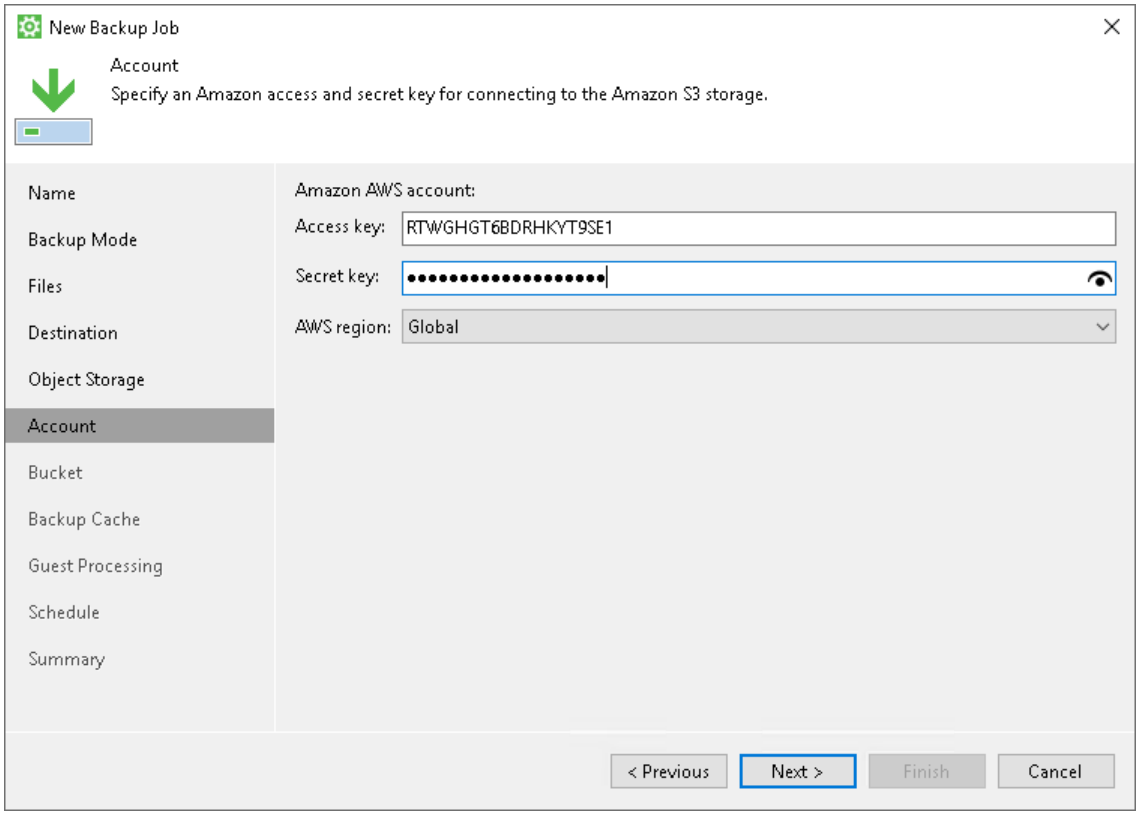
Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files in object storage.

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

1. In the **Access key** field, enter the access key ID.
2. In the **Secret key** field, enter the secret access key.

3. From the **AWS region** drop-down list, select the AWS region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Global** region.



Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to save backup files in object 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 article.

Specify settings for the bucket in the storage:

1. From the **Data center** drop-down list, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket in the storage:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
   a. Select the **Browse** option.

b. In the **Select Folder** window, do the following:

i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.

ii. Select the necessary folder and click **OK**.

> **NOTE**
>
> You cannot select a folder that is managed by the Veeam Backup & Replication server.

If necessary, you can create a new folder. To do this, click the **New Folder** option in the **Select Folder** window.

4. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.

5. In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

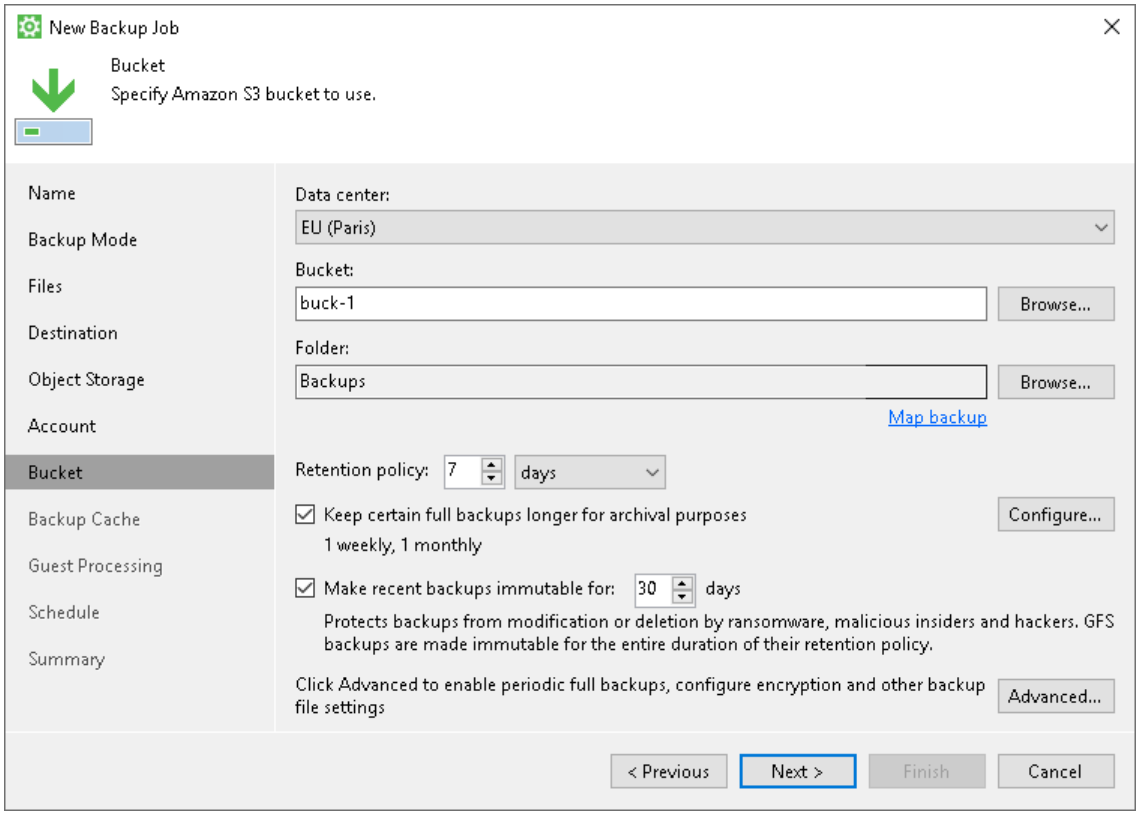
   To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see Long-Term Retention Policy.

6. To protect recent backups from modifications, select the **Make recent backups immutable for <N> days** check box and specify the number of days for which you want to keep your backups immutable. By default, Veeam Agent keeps backups immutable for 30 days. To learn more, see Backup Immutability.

   > **NOTE**
   >
   > If you use the GFS retention scheme and enable immutability for a backup, the restore points with GFS flags become immutable for the whole GFS retention period. You will not be able to delete such restore points till the end of the GFS retention period.

7. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

After that, Veeam Agent will create a new repository in the cloud storage where you can store backups.



Mapping Backup Job

Starting from Veeam Agent for Microsoft Windows version 6.1, you can map the job to the already created backup that is stored in the Amazon S3 storage. To map the backup job, perform the following steps:

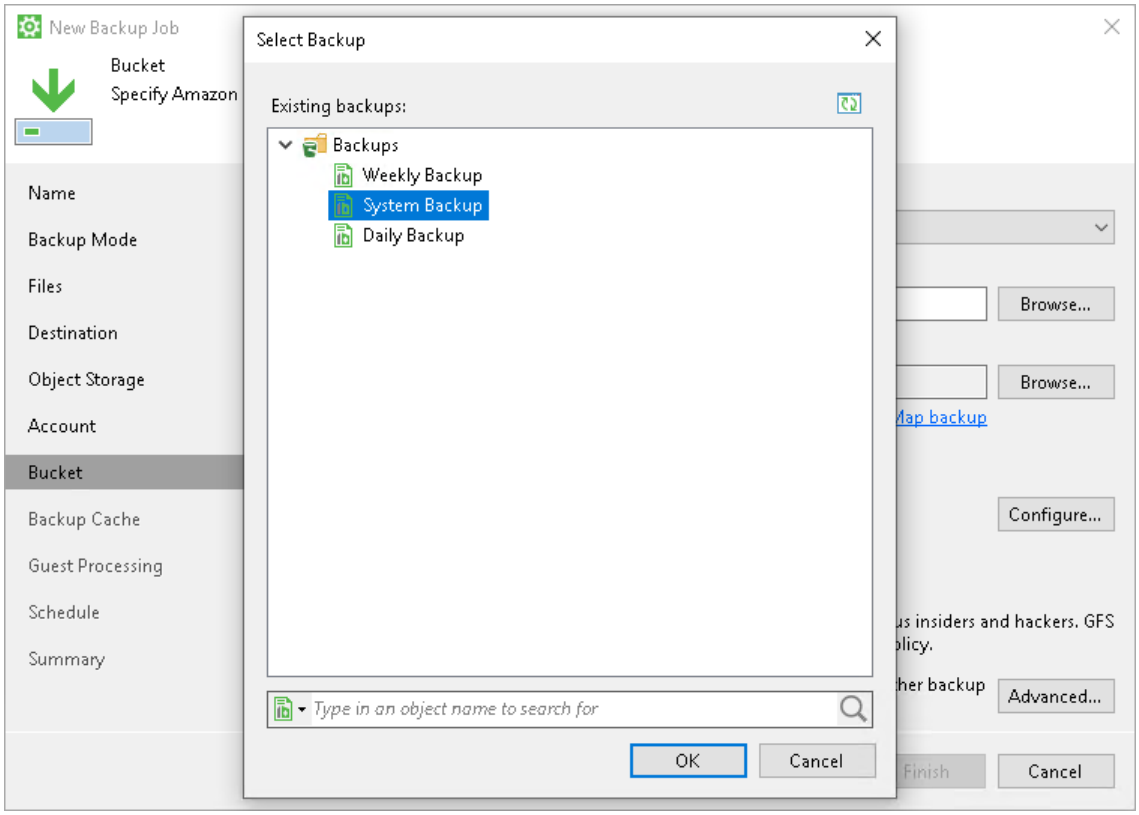
1. From the **Data center** drop-down list, select the geographic region where the created backup is stored.
2. In the **Bucket** field, specify a bucket where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.

> **NOTE**
>
> You cannot select a folder that is managed by the Veeam Backup & Replication server.

4. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same account used to connect to the Amazon S3 storage.

5. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Google Cloud Storage Settings

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

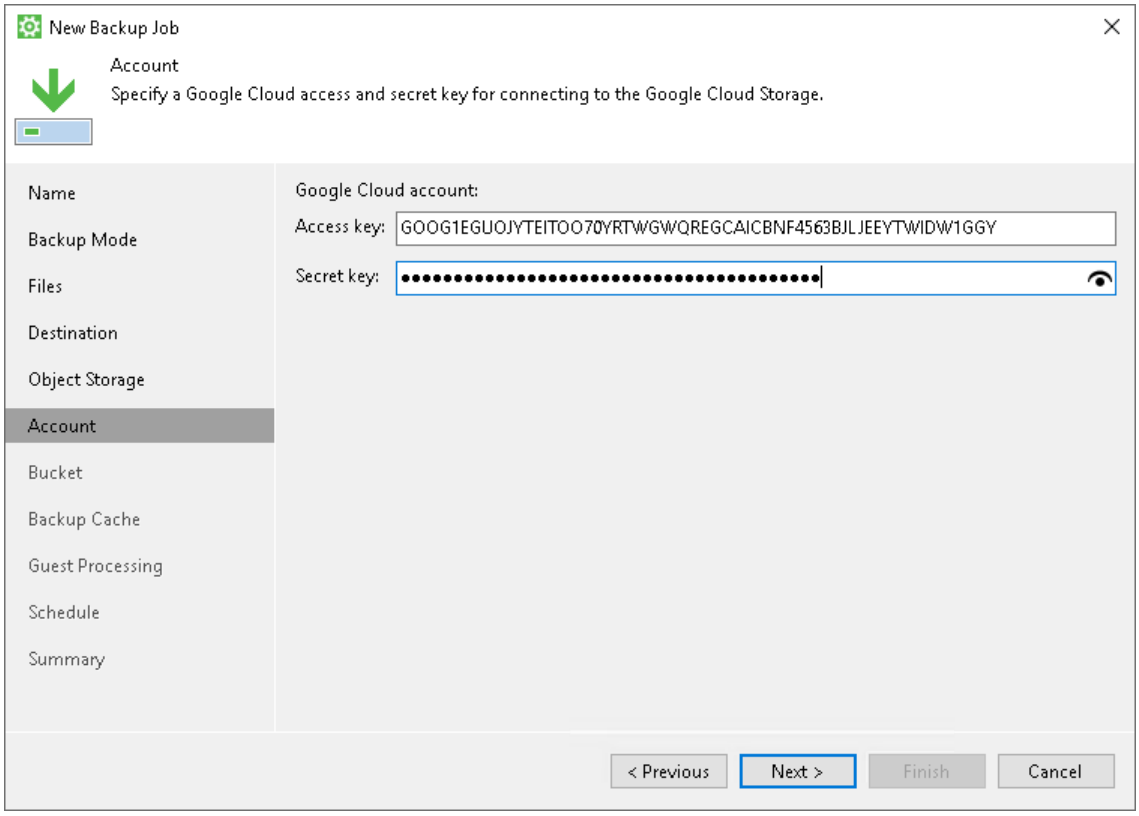
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files in object storage.

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

If you have not created the HMAC keys beforehand, you can create the keys in the Google Cloud console, as described in Google Cloud documentation.



Specifying Bucket Settings

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

Specify settings for the bucket in the storage:

1. From the **Data center region** drop-down list, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.

> **NOTE**
>
> You cannot select a folder that is managed by the Veeam Backup & Replication server.

If necessary, you can create a new folder. To do this, click the **New Folder** option in the **Select Folder** window.

4. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

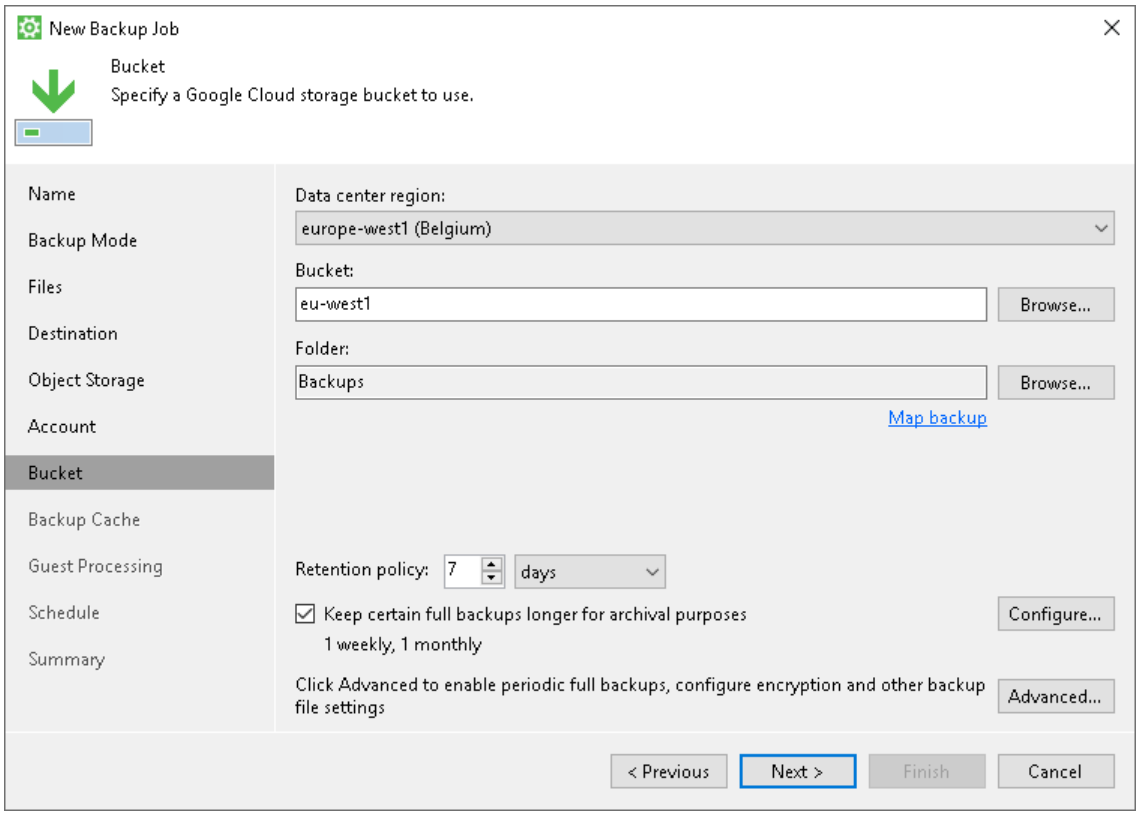
   To learn more, see Mapping Backup Job.

5. In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

   To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see Long-Term Retention Policy.

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

After that, Veeam Agent will create a new repository in the cloud storage where you can store backups.



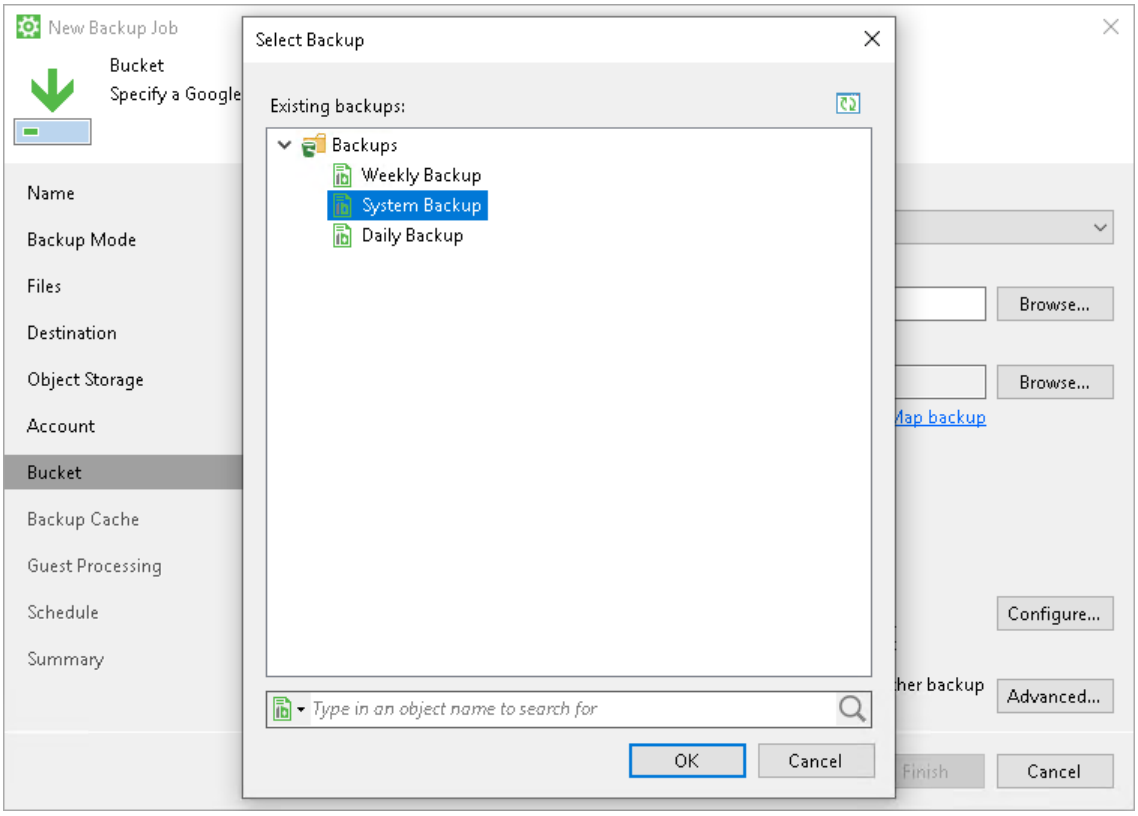
Mapping Backup Job

Starting from Veeam Agent for Microsoft Windows version 6.1, you can map the job to the already created backup that is stored in the Google Cloud storage. To map the backup job, perform the following steps:

1. From the **Data center region** drop-down list, select the geographic region where the created backup is stored.
2. In the **Bucket** field, specify a bucket where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder where the created backup is stored:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.

      > **NOTE**
      >
      > You cannot select a folder that is managed by the Veeam Backup & Replication server.
4. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same account used to connect to the Google Cloud storage.
5. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Microsoft Azure Blob Storage Settings

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

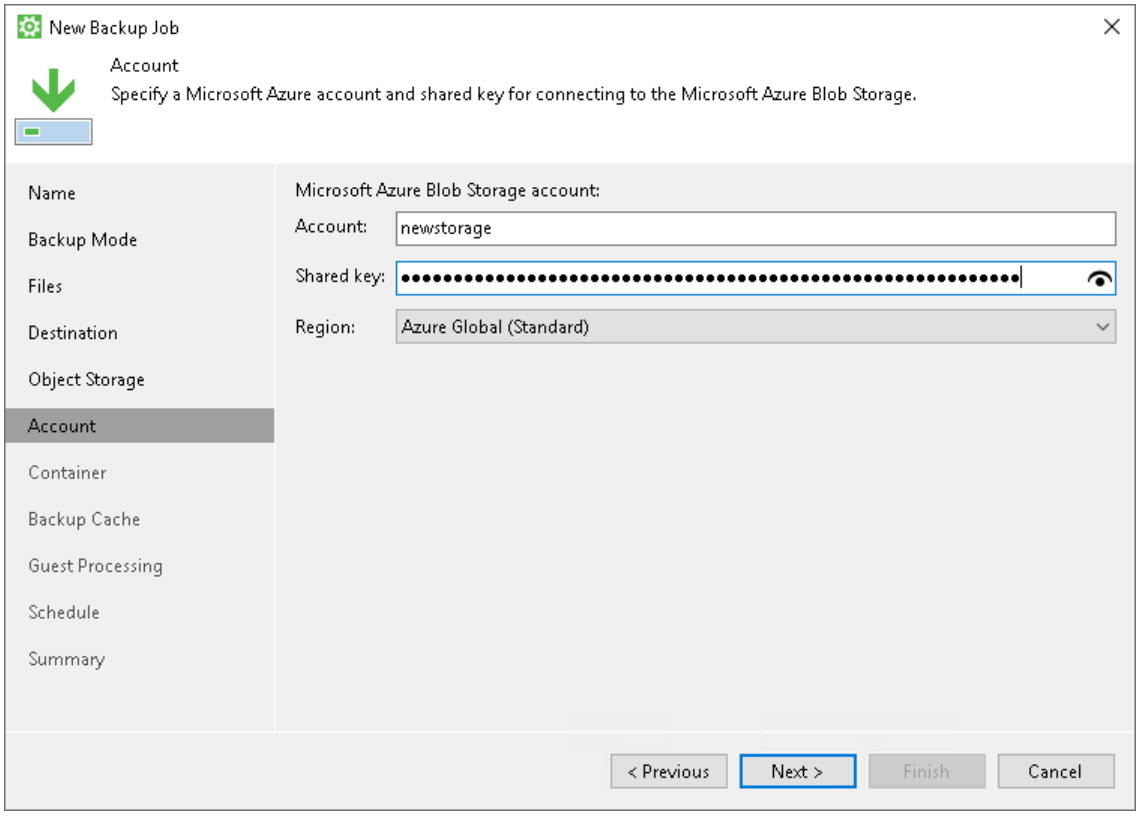
1. Specify account settings.
2. Specify container settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files in object storage.

1. In the **Account** field, enter the storage account name.
2. In the **Shared key** field, enter the storage account shared key.
3. From the **Region** drop-down list, select the Microsoft Azure region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Azure Global (Standard)** region.

> **NOTE**
>
> The **Allow storage account key access** option for **Shared Key authorization** must be enabled in the storage account. For information on how to find this option, see Microsoft Docs.



Specifying Container Settings

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

Specify settings for the container in the storage:

1. From the **Container** drop-down list, select a container in the storage.
2. In the **Folder** field, specify a folder in the container:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the container name or click the arrow to the left of the container name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.

      > **NOTE**
      >
      > You cannot select a folder that is managed by the Veeam Backup & Replication server.

      If necessary, you can create a new folder. To do this, click the **New Folder** option in the **Select Folder** window.
3. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.

4. In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

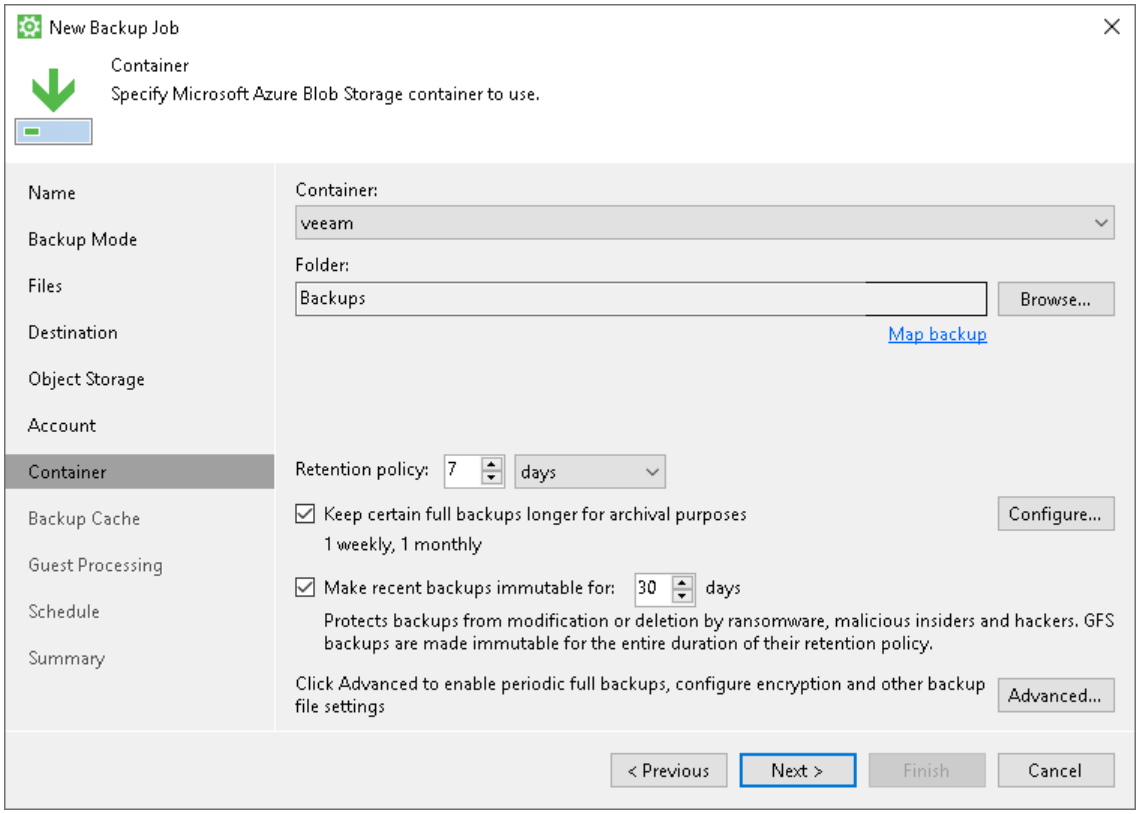
   To use the GFS (Grandfather-Father-Son) retention scheme, select the Keep certain full backups for archival purposes check box and click Configure. In the Configure GFS window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see Long-Term Retention Policy.

5. To protect recent backups from modifications, select the **Make recent backups immutable for <N> days** check box and specify the number of days for which you want to keep your backups immutable. By default, Veeam Agent keeps backups immutable for 30 days. To learn more, see Backup Immutability.

   > **NOTE**
   >
   > If you use the GFS retention scheme and enable immutability for a backup, the restore points with GFS flags become immutable for the whole GFS retention period. You will not be able to delete such restore points till the end of the GFS retention period.

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

After that, Veeam Agent will create a new repository in the cloud storage where you can store backups.



Mapping Backup Job

Starting from Veeam Agent for Microsoft Windows version 6.1, you can map the job to the already created backup that is stored in the Microsoft Azure Blob storage. To map the backup job, perform the following steps:

1. From the **Container** drop-down list, select a container where the created backup is stored.
2. In the **Folder** field, specify a folder where the created backup is stored:
   a. Select the **Browse** option.

b. In the **Select Folder** window, do the following:

i. Double-click the container name or click the arrow to the left of the container name to view the list of available folders.

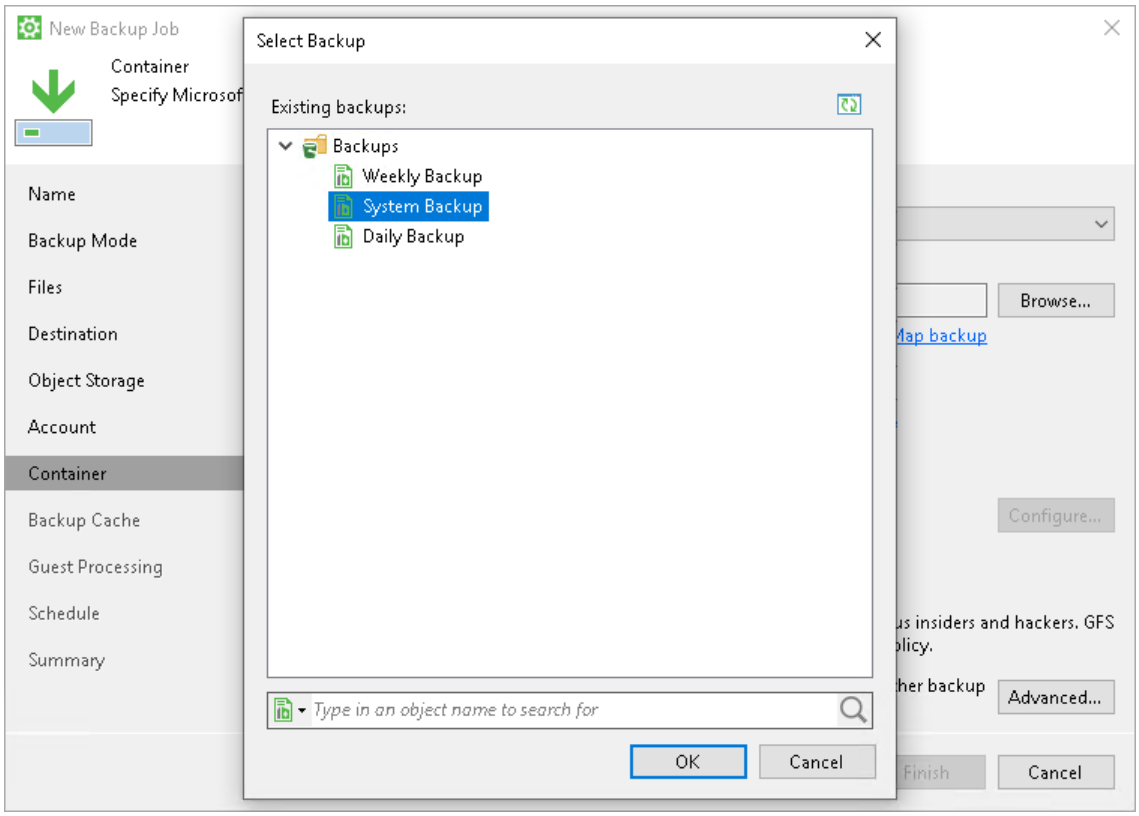
ii. Select the necessary folder and click **OK**.

> **NOTE**
>
> You cannot select a folder that is managed by the Veeam Backup & Replication server.

3. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same account used to connect to the Microsoft Azure Blob storage.

4. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Shared Folder Settings

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

Specify shared folder settings:

1. In the **Shared folder** field, type a UNC name of the network shared folder in which you want to store backup files. Keep in mind that the UNC name always starts with two back slashes (\\).

2. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

To learn more, see Mapping Backup Job.

3. If the network shared folder requires authentication, select the **This share requires access credentials** check box and specify a user name and password of the account that has *Full Control* access permissions on this shared folder. The user name must be specified in the down-level logon name format. For example, *DOMAIN|UserName* or *HOSTNAME|UserName*.

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

   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the *NT AUTHORITY|SYSTEM* account of the computer where the product is installed. You can use this scenario if the Veeam Agent computer is joined to the Active Directory domain. In this case, you can grant *Full Control* access permissions on the shared folder and underlying file system to the computer account *(DOMAIN|COMPUTERNAME$)*.

4. To view how much free space is available in the selected shared folder, click **Populate**.

5. Specify short-term backup retention policy settings:

   - [For Free and Workstation product editions] In the **Keep backups for <N> days (excluding days with no backup)** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

     To learn more, see Backup Retention Policy in Free and Workstation Editions.

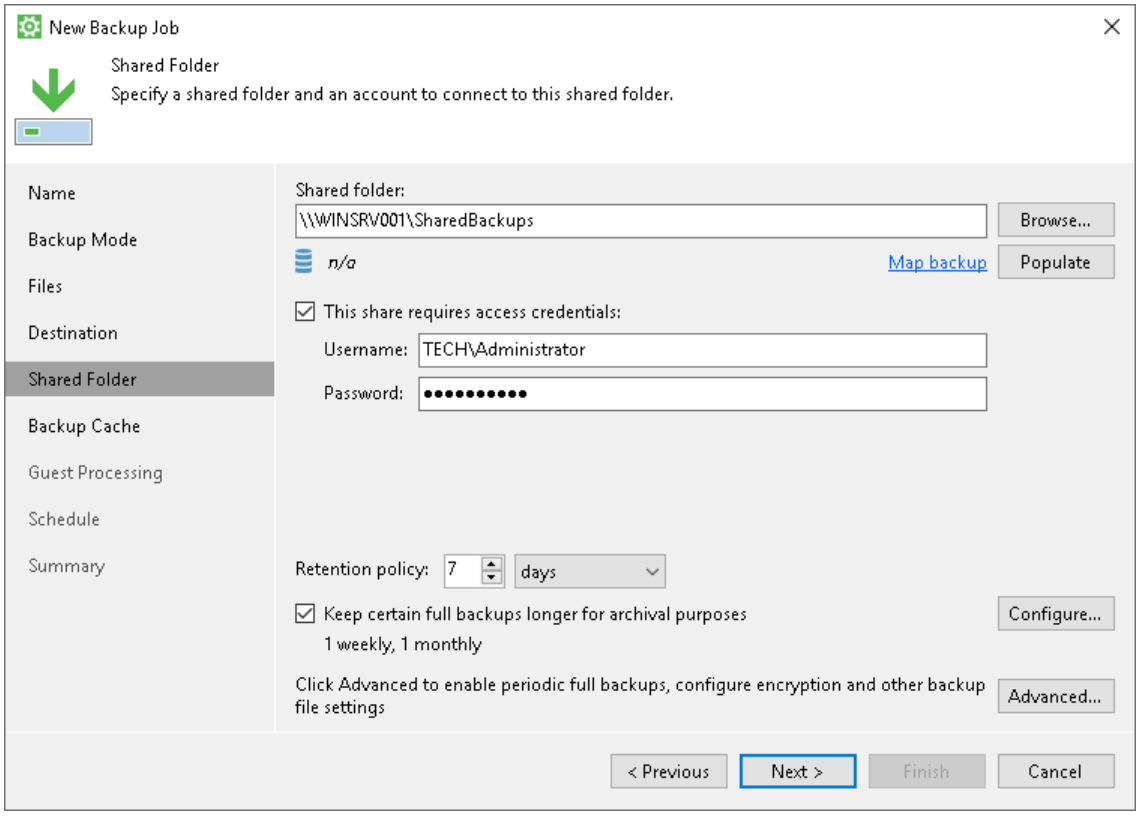
   - [For Server product edition] In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

     - Select the **restore points** option if you want Veeam Agent to remove restore points from the backup chain when the number of restore points exceeds the specified limit.
     - Select the **days** option if you want Veeam Agent to remove the earliest restore points from the backup chain when the specified period is over.

     To learn more, see Backup Retention Policy in Server Edition.

6. [For Workstation and Server product editions] To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep some periodic full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

7. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

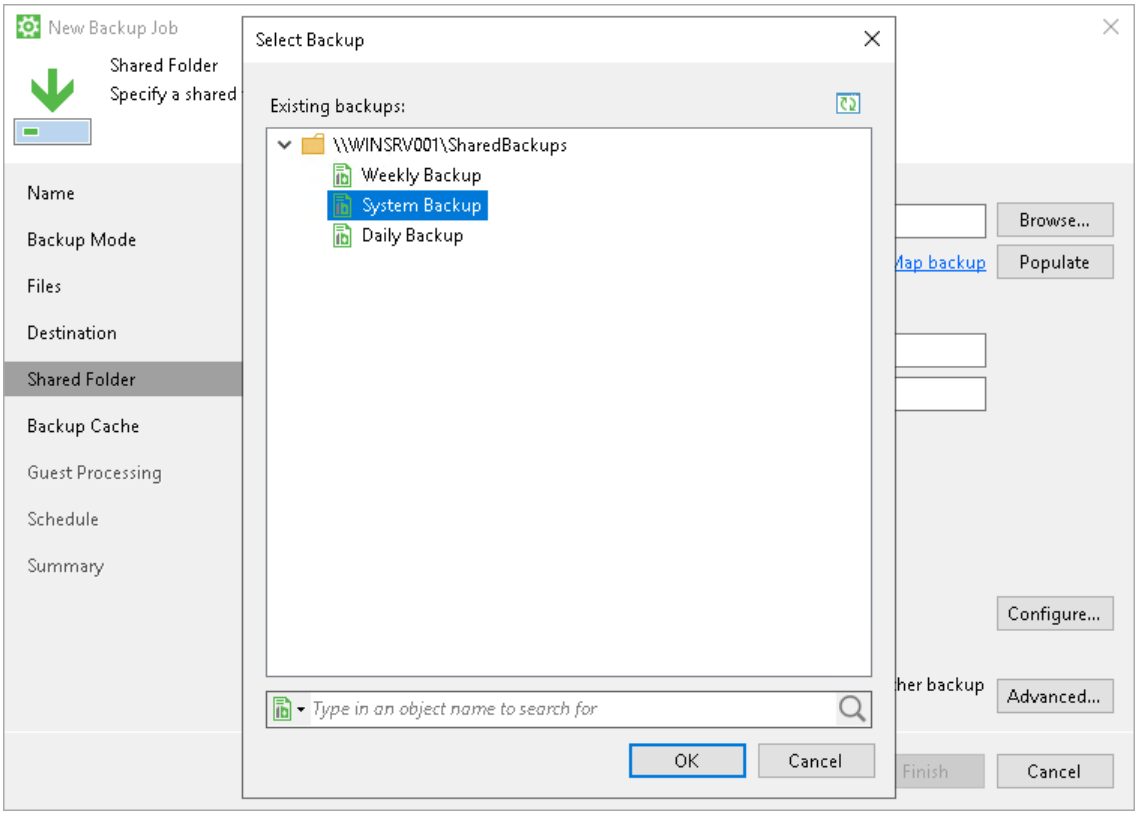


Mapping Backup Job

If you have selected to map the job to the already created backup that is stored in a network shared folder, perform the following steps:

1. In the **Shared folder** field, specify the same path as was specified in the **Shared folder** field for the job that was used to create the backup.
2. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window.

   Keep in mind that Veeam Agent displays backups stored in the folder that is specified in the **Shared folder** field and its first-level subfolders.
3. If you map the job to an encrypted backup, and encryption keys are not available in the Veeam Agent database, you must provide the password specified for encryption. In the displayed window, enter the password and click **OK**.



Veeam Backup Repository Settings

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

1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, 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 in a Veeam 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 a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup server. By default, Veeam Agent for Microsoft Windows uses port 10001.
3. Select the **Specify your personal credentials** check box. In the **Username** and **Password** fields, specify a user name and password of the account that has access to this backup repository. Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

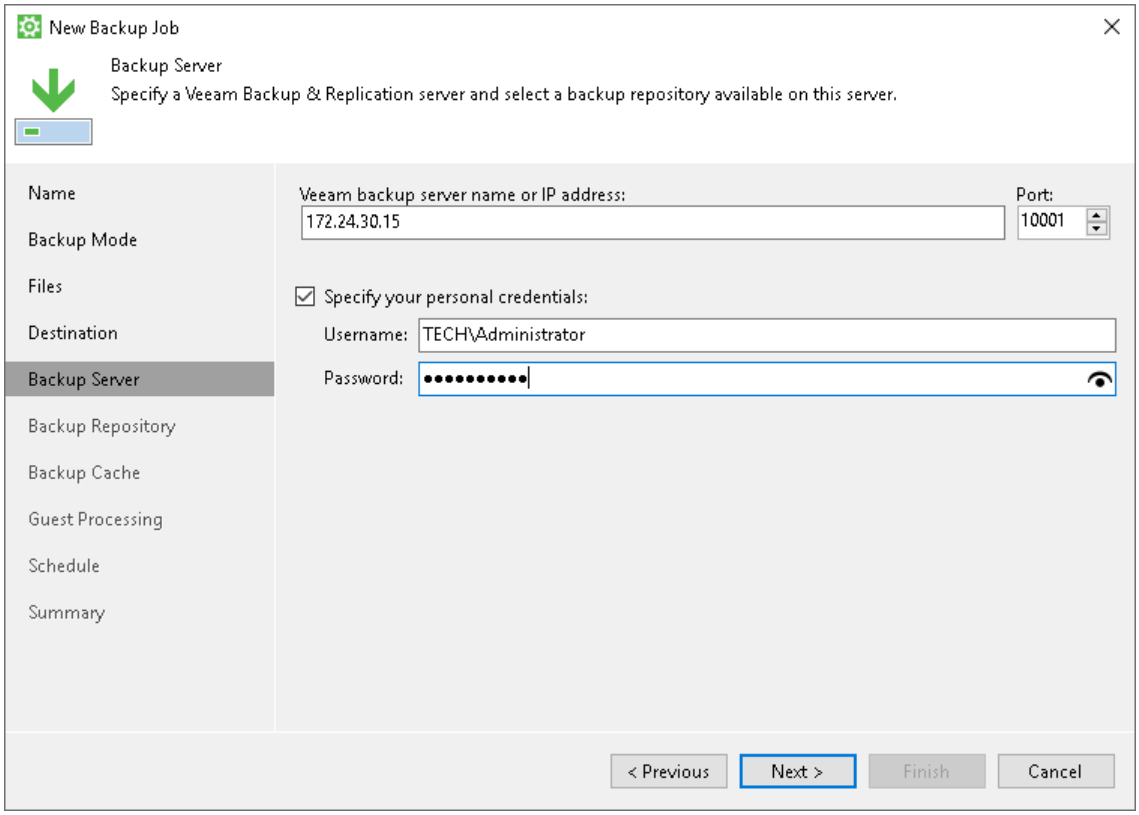
   If you do not select the **Specify your personal credentials** check box, Veeam Agent for Microsoft Windows will connect to the backup repository using the *NT AUTHORITY\SYSTEM* account of the computer where the product is installed. You can use this scenario if the Veeam Agent computer is joined to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

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

IMPORTANT

Consider 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 in advance, 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 in the backup repository.



Selecting Backup Repository

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

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. The **Backup repository** list displays only those backup repositories on which you have permissions to store data.

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

To refresh the list of backup repositories, click the **Refresh** button at the top right corner of the **Backup repository** field. Backup repositories list refresh may be required if you change permission settings for a specific backup repository on the Veeam backup server and want to display this backup repository in the **New Backup Job** wizard. To learn more, see Setting Up User Permissions on Backup Repositories.

2. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.

3. Specify short-term backup retention policy settings:

   - [For Free and Workstation product editions] In the **Keep backups for <N> days (excluding days with no backup)** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days. After this period is over, Veeam Agent will remove the earliest restore points from the backup chain.

     To learn more, see Backup Retention Policy in Free and Workstation Editions.

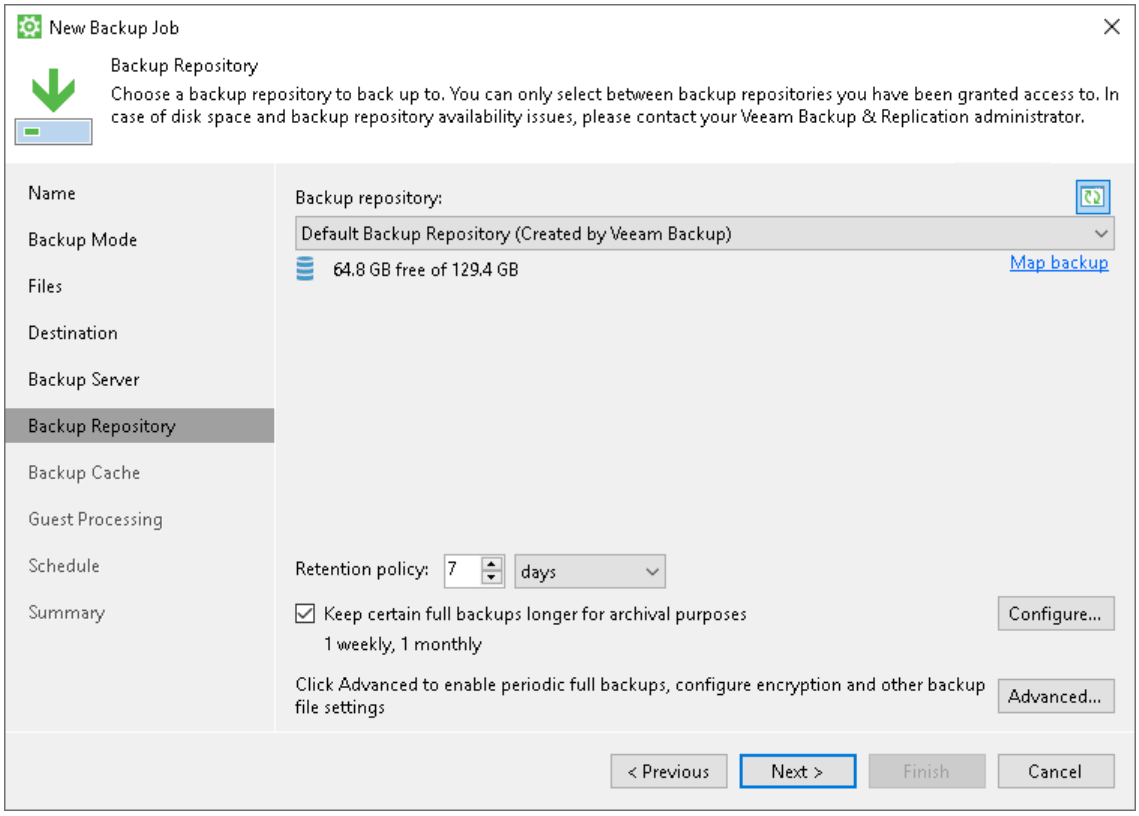
   - [For Server product edition] In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

     - Select the **restore points** option if you want Veeam Agent to remove restore points from the backup chain when the number of restore points exceeds the specified limit.
     - Select the **days** option if you want Veeam Agent to remove the earliest restore points from the backup chain when the specified period is over.

     To learn more, see Backup Retention Policy in Server Edition.

4. [For Workstation and Server product editions] To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep some periodic full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

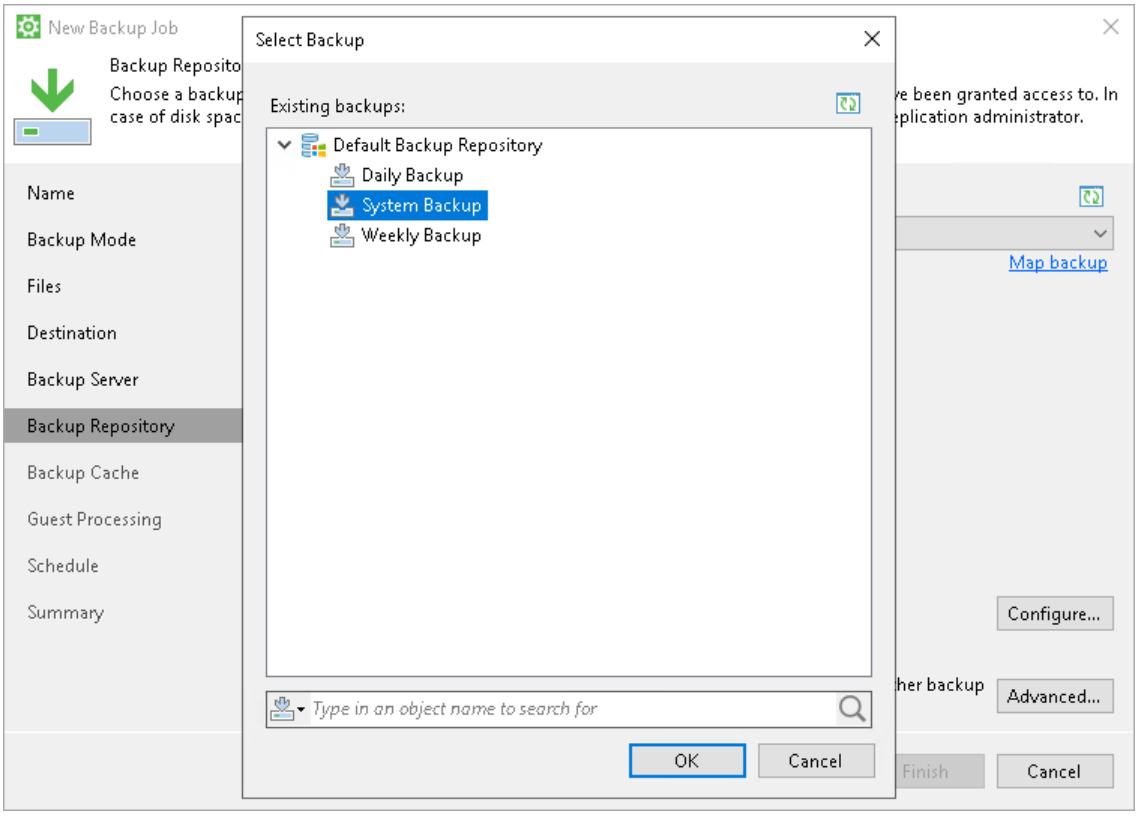
5. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



Mapping Backup Job

If you have selected to map the job to the already created backup that is stored in a Veeam backup repository, perform the following steps:

1. If you map the job to an encrypted backup, you must decrypt the backup on the Veeam Backup & Replication side before mapping. To learn more, see the Restoring Data from Encrypted Backups section in the Veeam Backup & Replication User Guide.
2. Click the **Map backup** link and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window. Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same account used to connect to the repository.



The backup job mapping can be helpful in case of the backup seeding. If you want to seed backup files, you must place these files in a specific folder on the target location. In the Veeam backup repository, Veeam Agent stores backups in the folders with paths of the following format:

```
<path_to_folder>\<domain_name>_<user_name>\<backup_job_name>
```

where:

- `<path_to_folder>` — path to the folder in the Veeam backup repository.
- `<domain_name>` — domain name specified to connect to the repository.
- `<user_name>` — user name specified to connect to the repository.
- `<backup_job_name>` — name of the backup job.

For example:

```
C:\Backup\TECH_Administrator\System Backup
```

To learn more about backup seeding scenarios for Veeam backup repositories, see Moving Veeam Agent Backups to Veeam Backup Repository.

Veeam Cloud Connect Repository Settings

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

1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.
3. Select the cloud repository.

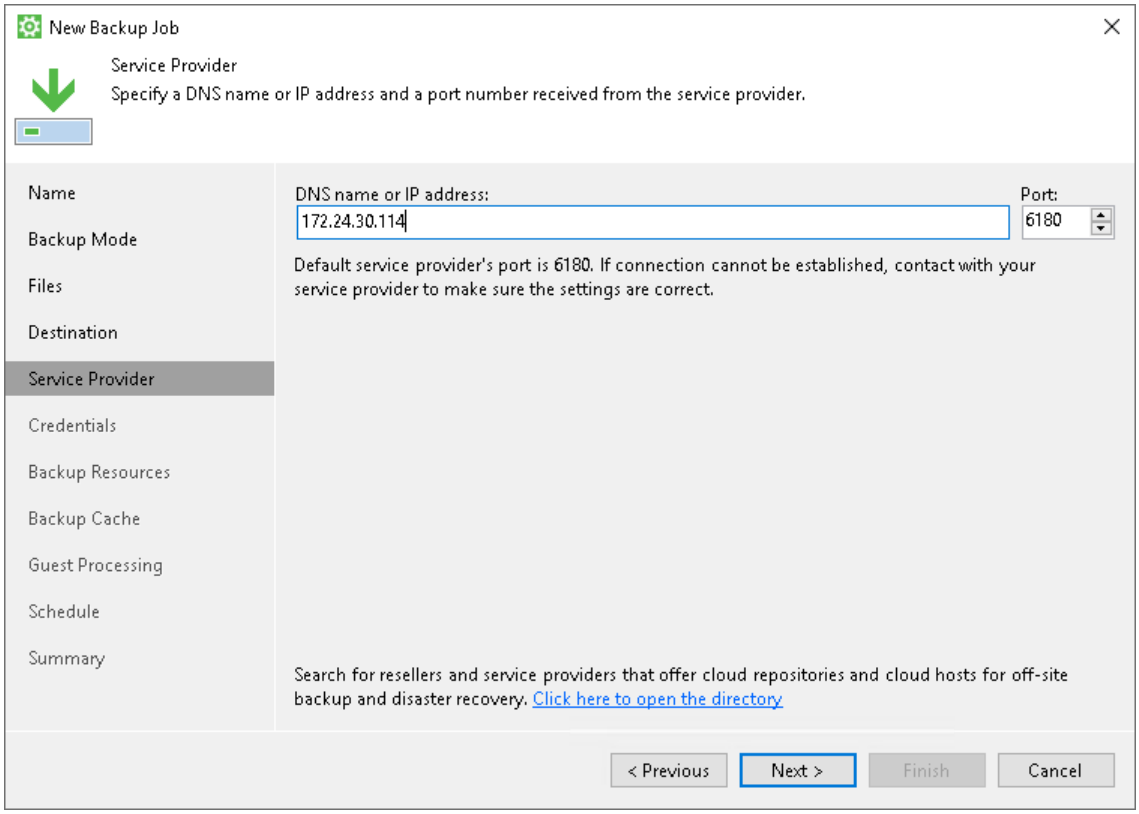
Specifying Service Provider Settings

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

Specify settings for the cloud gateway that the 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 for Microsoft Windows will communicate with the cloud gateway. By default, port 6180 is used.

> **TIP**
>
> You can look for service providers who offer Repository as a Service using Veeam Backup & Replication. The list of service providers is published on the Veeam website and constantly updated. You can select the necessary service provider from the list and contact this service provider to get the cloud repository service.
>
> To find a service provider, click the *Click here to open the directory* link. Veeam Agent for Microsoft Windows will open a webpage on the Veeam website. Use the filter on the webpage to find the necessary service provider by the type of provided cloud services, service provider datacenter location or service area.



Specifying User Account Settings

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

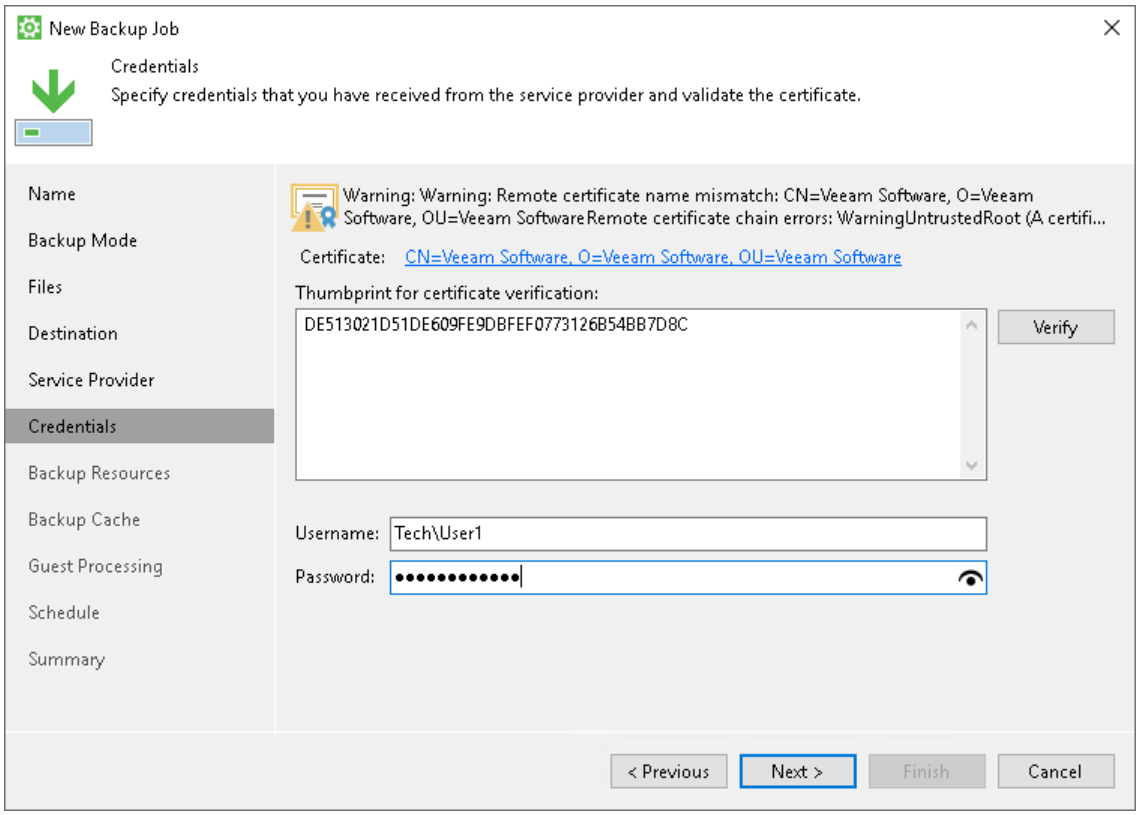
Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the cloud repository.

1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   - To view the TLS certificate, click the certificate link.
   - To verify the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Thumbprint for certificate verification** field. Click **Verify**. Veeam Agent for Microsoft Windows will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. In the **Username** field, enter the user name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The user name of the subtenant account must be specified in the *TENANT|SUBTENANT* format.
3. In the **Password** field, provide a password for the tenant or subtenant account.



Selecting Cloud Repository

The **Backup Resources** step of the wizard is available if you have chosen to save backup files in 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 backup repositories on which you have permissions to store data.

   To refresh the list of cloud repositories, click the **Refresh** button at the top right corner of the **Available cloud repositories** field. Cloud repositories list refresh may be required if you change permission settings for a specific cloud repository and want to display this cloud repository in the **New Backup Job** wizard.

2. If you want to map the job to a specific backup that was previously created on the same Veeam Agent computer, click the **Map Backup** link and select the backup.

   To learn more, see Mapping Backup Job.

3. Specify short-term backup retention policy settings:

   - [For Free and Workstation product editions] In the **Keep restore points for the last <N> days when computer was used** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

     To learn more, see Backup Retention Policy in Free and Workstation Editions.

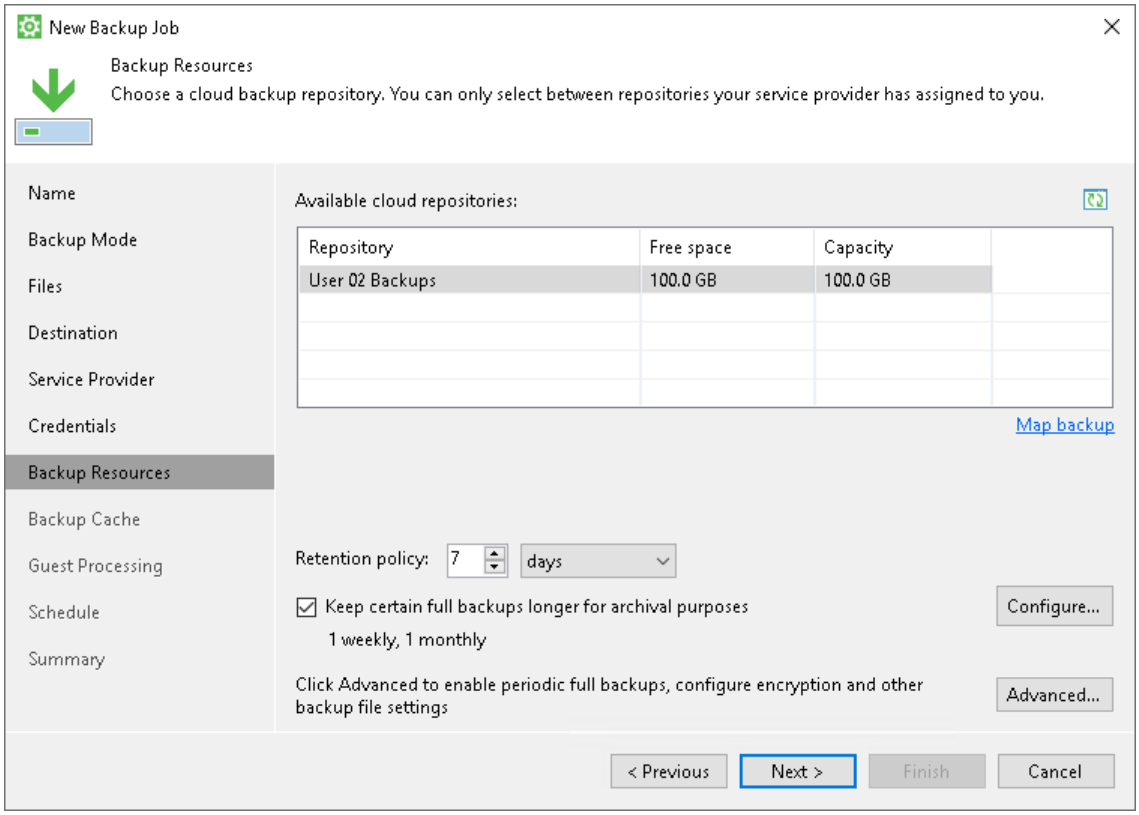
   - [For Server product edition] In the **Retention policy** field, specify the number of restore points or days for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files for 7 days.

     - Select the **restore points** option if you want Veeam Agent to remove restore points from the backup chain when the number of restore points exceeds the specified limit.
     - Select the **days** option if you want Veeam Agent to remove the earliest restore points from the backup chain when the specified period is over.

     To learn more, see Backup Retention Policy in Server Mode.

4. [For Workstation and Server product editions] To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep some periodic full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

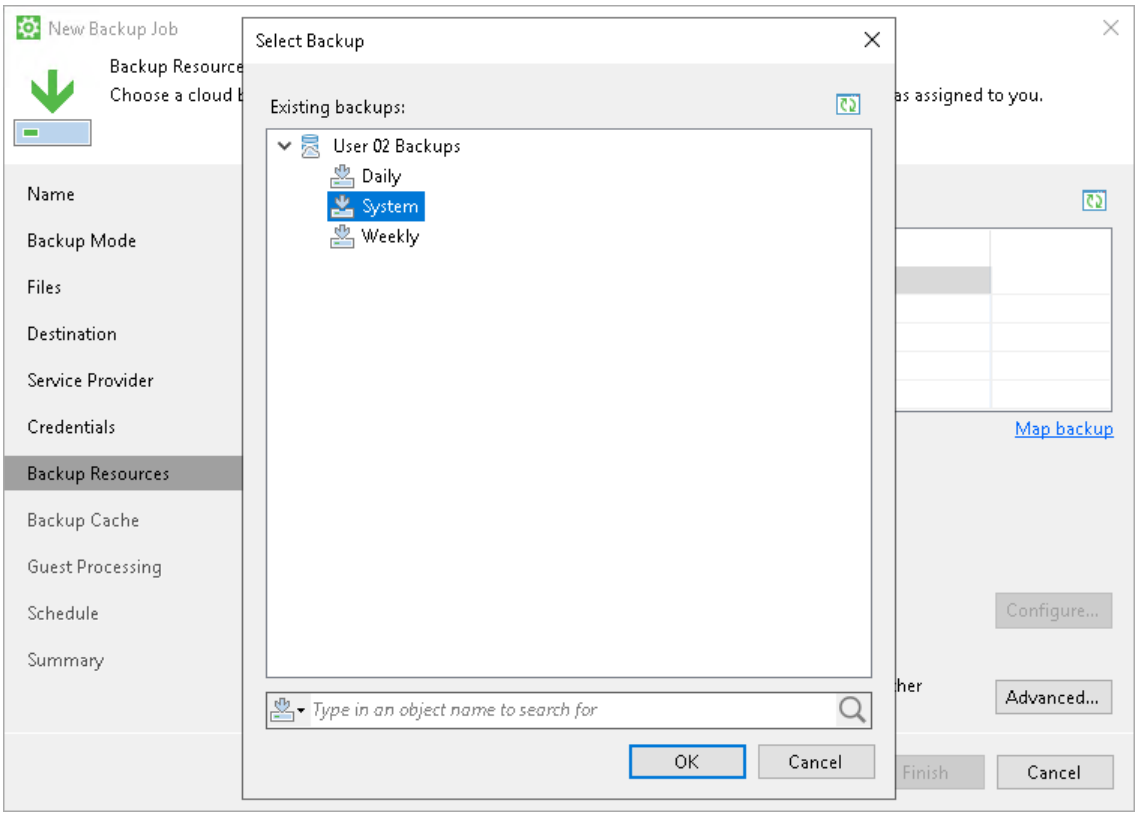
5. Click Advanced to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



Mapping Backup Job

If you have selected to map the job to the already created backup, perform the following steps:

1. Click **Map backup** and select the desired backup. To find the backup, you can use the search field at the bottom of the **Select Backup** window. Keep in mind that Veeam Agent displays only those backups that were created on the same Veeam Agent computer with the same tenant or subtenant account used to connect to the repository.
2. If you map the job to an encrypted backup, and encryption keys in the cloud repository database do not coincide with the encryption keys in the Veeam Agent database, you must provide the password specified for encryption after the job start. In the dialog window, enter the password and click **OK**. To learn more, see Resuming Encrypted Backup Chain.



The backup job mapping can also be helpful in case of the backup seeding. If you want to seed backup files, you must place these files in a specific folder on the target location. On the cloud repository, Veeam Agent stores backups in the folders with paths of the following format:

- If a tenant account is specified in the **Username** field at the **Credentials** step of the wizard:

  `<path_to_repository>\<tenant_name>\<backup_job_name>`

- If a subtentant account is specified in the **Username** field at the **Credentials** step of the wizard:

  `<path_to_repository>\<tenant_name>\Users\<subtenant_name>\<backup_job_name>`

where:

- `<path_to_repository>` — path to the folder on the cloud repository.
- `<tenant_name>` — name of the tenant account.
- `<subtenant_name>` — name of the subtenant account.
- `<backup_job_name>` — name of the backup job.

For example:

- `C:\Backup\TechCompany\System Backup`

  or

- `C:\Backup\TechCompany\Users\User01\System Backup`

To learn more about backup seeding scenarios for cloud repositories, see Moving Veeam Agent Backups to Veeam Cloud Connect Repository.

Step 7. Specify GFS Retention Policy

This step of the wizard is available if you use the Workstation or Server edition of Veeam Agent for Microsoft Windows.

> **NOTE**
>
> If you want to store your backups in object storage, and you do not configure Veeam Agent to perform active full backups periodically, Veeam Agent still requires a full backup to assign a GFS flag to a full restore point. In this case, Veeam Agent creates a full backup based on the last incremental backup. If some data blocks required to create the full backup reside in object storage, the full backup contains links that point at such data blocks. Veeam Agent does not retrieve actual data blocks from the object storage to avoid extra costs.

To configure GFS retention policy settings for the backup job:

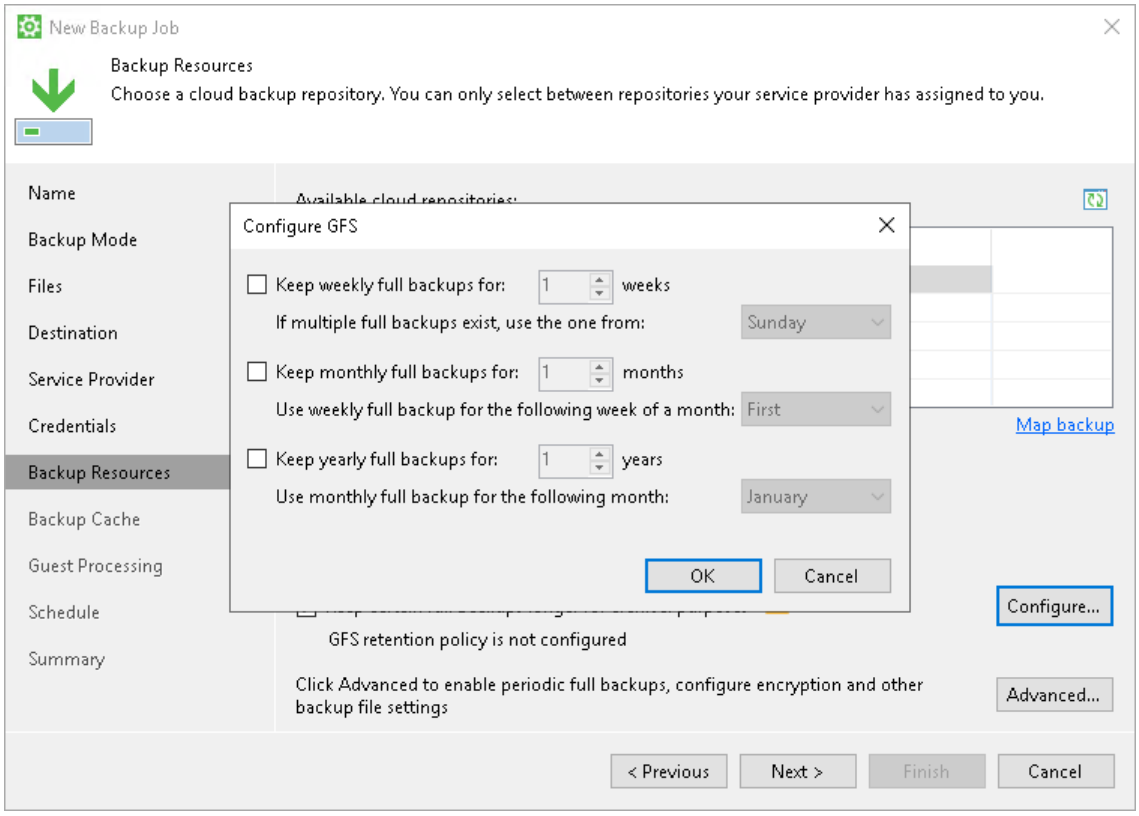
1. Click the **Configure** button at one of the following steps of the wizard:
   - Local Storage — if you have selected the **Local storage** option at the Destination step of the wizard.
   - Shared Folder — if you have selected the **Shared folder** option at the Destination step of the wizard.
   - Bucket/Container — if you have selected the **Object storage** option at the Destination step of the wizard.
   - Backup Repository — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
   - Backup Resources — if you have selected the **Veeam Cloud Connect repository** option at the Destination 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 number of weeks during which you want to prevent restore points from being modified and deleted.
      - 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.
      - [For object storage target if active full backup schedule is not enabled] In the **Create weekly full on this day** list, select a week day when Veeam Agent must create a full backup and 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 to 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 the Assignment of GFS Flags section in the Veeam Backup & Replication User Guide.

Step 8. Specify Advanced Backup Settings

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

- Backup settings
- Maintenance settings
- Storage settings

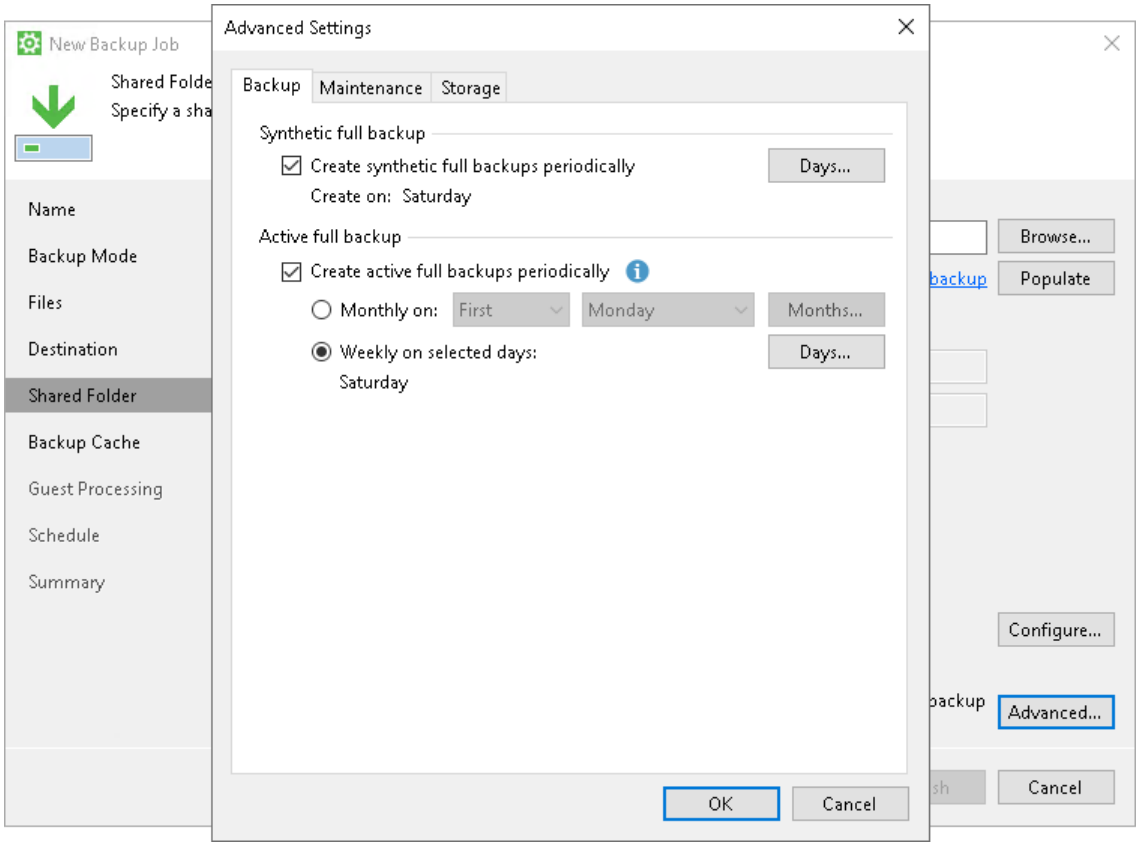
Backup Settings

To specify settings for a backup chain created with the backup job:

1. Click **Advanced** 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.
   - Bucket/Container — if you have selected the **Object storage** option at the Destination step of the wizard.
   - Shared Folder — if you have selected the **Shared folder** option at the Destination step of the wizard.
   - Backup Repository — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
   - Backup Resources — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.
2. If you want to periodically create synthetic full backups, on the **Backup** tab, select the **Create synthetic full backups periodically** check box and click **Days** to schedule synthetic full backups on the necessary week days.
3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

Keep in mind that to create active and synthetic full backups on selected days, Veeam Agent must run the backup job on these days. To learn more about backup job schedule, see Scheduling Settings.

> **NOTE**
>
> Consider the following:
>
> - Synthetic full backup is available only in the Workstation and Server editions of Veeam Agent for Microsoft Windows.
> - Synthetic full backup is not available for backup jobs targeted at object storage.
> - Before scheduling periodic full backups, you must make sure that you have scheduled the backup job to run on the enough free space on the target location. As an alternative, you can create active full backups manually when needed. For more information, see Creating Active Full Backups.
> - If you schedule the active full backup and synthetic full backup on the same day, Veeam Agent for Microsoft Windows will perform only active full backup. Synthetic full backup will be skipped.



Maintenance Settings

To specify maintenance settings for the backup chain created with the backup job:

1. Click **Advanced** 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.
   - Bucket/Container — if you have selected the **Object storage** option at the Destination step of the wizard.
   - Shared Folder — if you have selected the **Shared folder** option at the Destination step of the wizard.
   - Backup Repository — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
   - Backup Resources — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.
2. Click the **Maintenance** tab.
3. To periodically perform a health check for the latest restore point in the backup chain, enable the **Perform backup files health check** option in the **Storage-level corruption guard** section and specify the health check schedule. For more information, see Health Check for Backup Files.
4. [For object storage target] Veeam Agent offers a special health check mechanism for object storage targets. To run the health check for object storage, enable the **Perform backup files health check** option in the **Storage-level corruption guard** section and specify the health check schedule. For more information about the health check for object storage, see Enabling Health Check for Object Storage Target.

5. [For Veeam backup repository and cloud repository targets] Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup job in the target location. If Veeam Agent for Microsoft Windows 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. For more information, see Retention Policy for Outdated Backups.

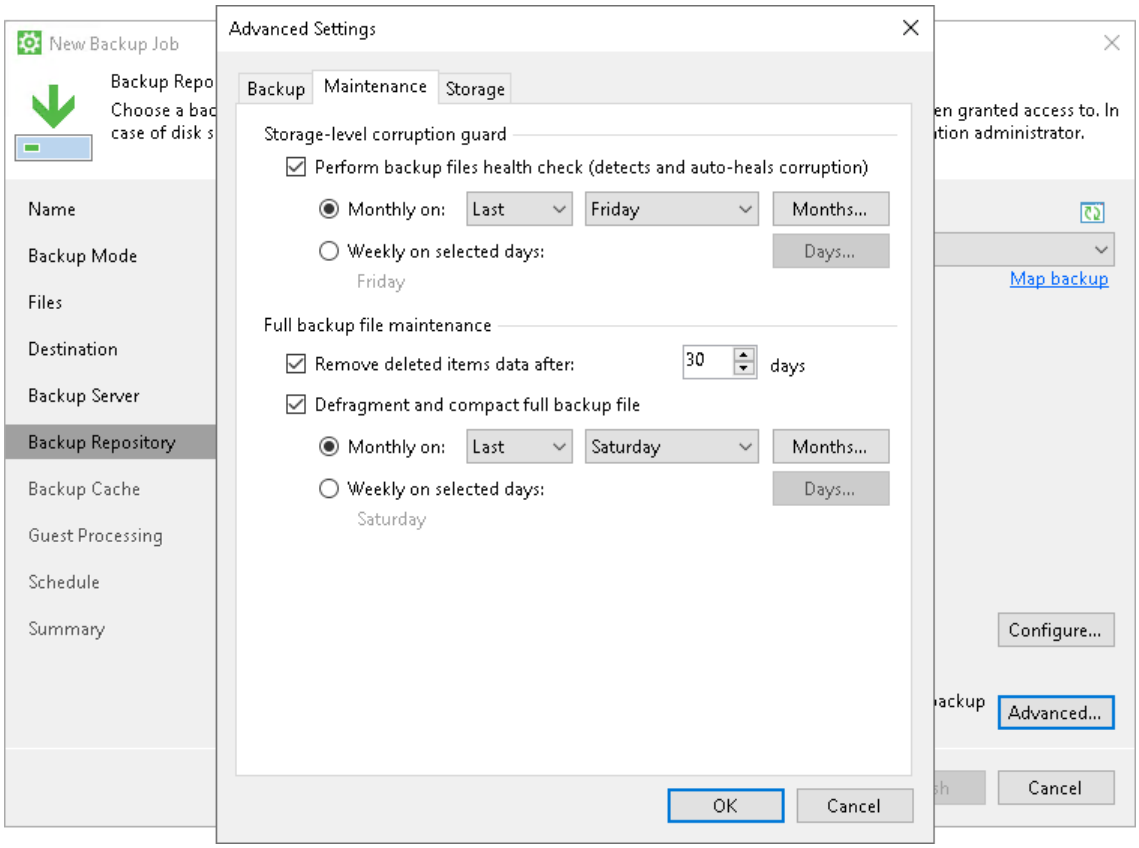
   > **NOTE**
   >
   > The **Remove deleted items data after** option is available only if you have selected the **Veeam backup repository** or **Veeam Cloud Connect repository** option at the Destination step of the wizard.

6. To periodically compact a full backup, select the **Defragment and compact full backup file** check box and specify the schedule for the compact operation.

   During the compact operation, Veeam Agent for Microsoft Windows creates a new empty file and copies to this file data blocks from the full backup file. As a result, the full backup file gets defragmented, and the speed of reading from and writing to the backup file increases.

   If the full backup file contains data blocks for deleted drives, Veeam Agent for Microsoft Windows will remove these data blocks. For more information, see Compact of Full Backup File.

   > **NOTE**
   >
   > The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage.

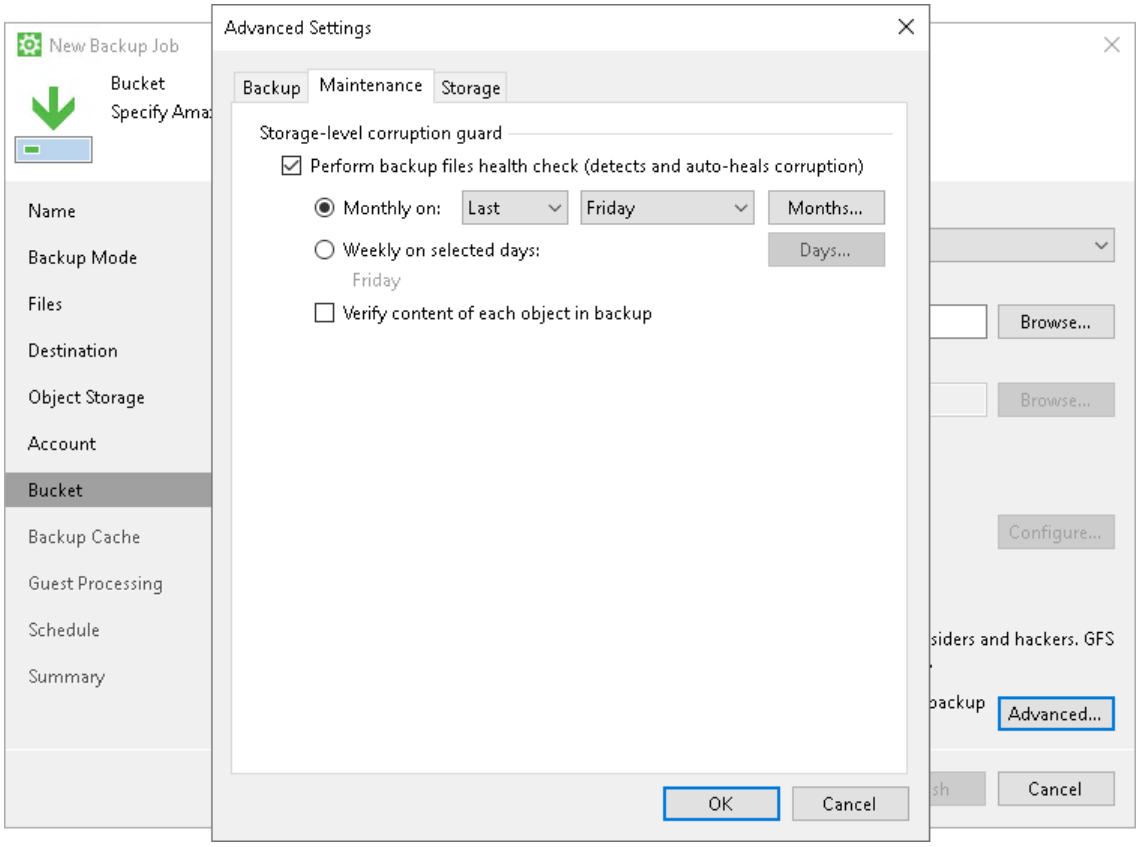


Enabling Health Check for Object Storage Target

To periodically perform a health check for backups that reside in object storage, enable the Perform backup files health check option in the Storage-level corruption guard section and specify the health check schedule.

Veeam Agent offers a special health check mechanism for object storage targets as default. Unlike the standard health check, the health check for object storage verifies metadata for the whole backup, not just the latest restore point, and does not read data from data blocks. For more information, see Health Check for Object Storage.

If necessary, you can switch from the health check for object storage to the standard health check. To do so, select the **Verify content of each object in backup** check box in the backup job settings. Keep in mind that enabling this setting may result in additional charges from your object storage provider. For information on how the standard health check works, see Standard Health Check.



Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** 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.
   - Bucket/Container — if you have selected the **Object storage** option at the Destination step of the wizard.
   - Shared Folder — if you have selected the **Shared folder** option at the Destination step of the wizard.
   - Backup Repository — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.

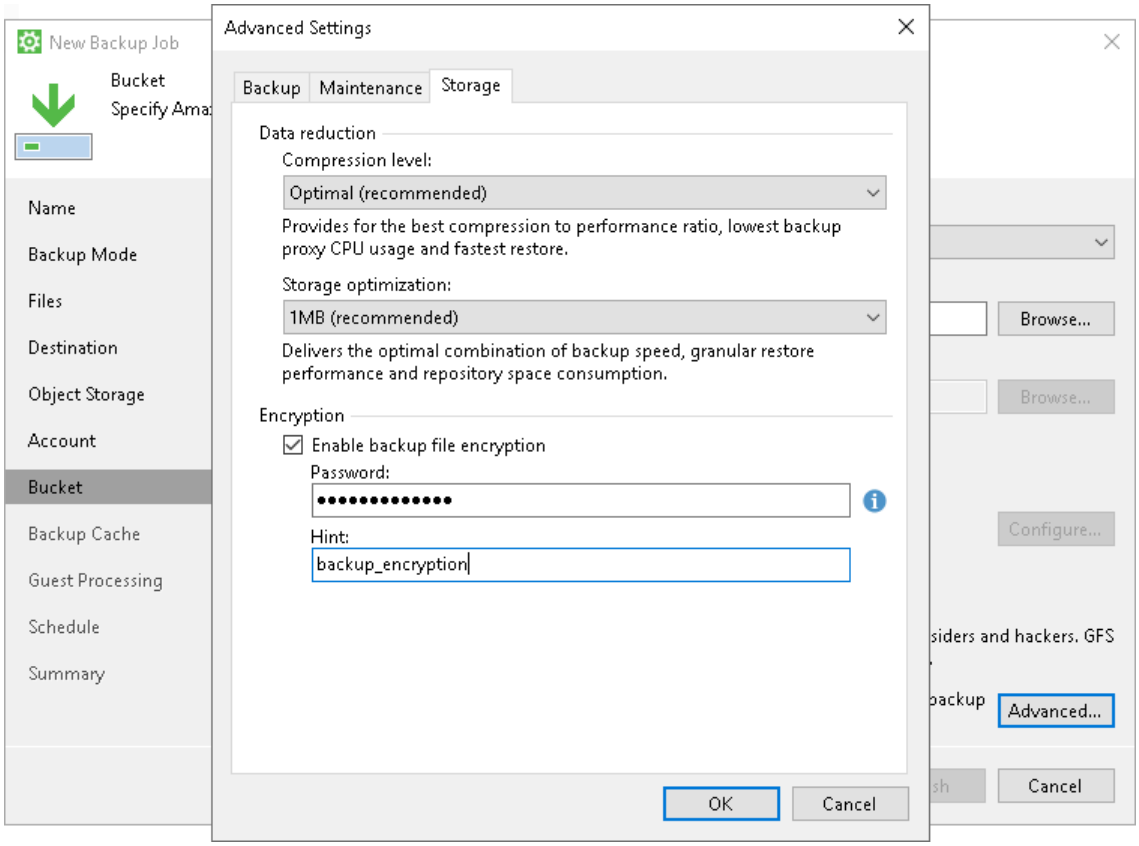
- Backup Resources — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.

2. Click the **Storage** tab.
3. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
4. In the **Storage optimization** section, select what size of data blocks you plan to use: *4 MB*, *1 MB*, *512 KB*, *256 KB*. Veeam Agent for Microsoft Windows will use data blocks of the chosen size to optimize the size of backup files and job performance.
5. 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 in a Veeam backup repository. Encryption of Veeam Agent backups stored in 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 for Microsoft Windows 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 for Microsoft Windows does not encrypt the previous backup chain created with this job.


New Backup Job
Bucket
Specify Ama
Name
Backup Mode
Files
Destination
Object Storage
Account
Bucket
Backup Cache
Guest Processing
Schedule
Summary
Browse...
Browse...
Configure...
siders and hackers. GFS
backup
Advanced...
Cancel
Advanced Settings
Backup
Maintenance
Storage
Data reduction
Compression level:
Optimal (recommended)
Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.
Storage optimization:
1MB (recommended)
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.
Encryption
Enable backup file encryption
Password:
Hint:
backup_encryption
OK
Cancel

Step 9. Specify Backup Cache Settings

The **Backup Cache** step of the wizard is available if you have chosen to save backup files in a remote storage: in object storage, in a network shared folder, in a Veeam backup repository or in a Veeam Cloud Connect repository.

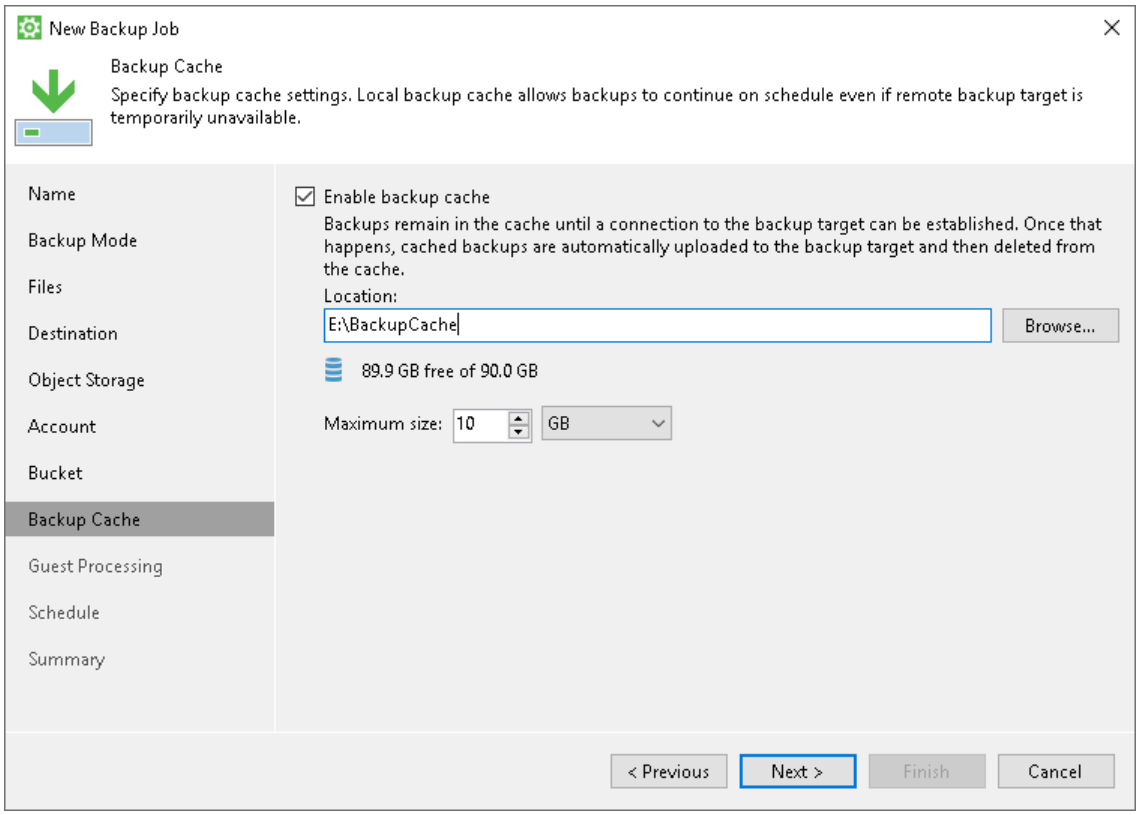
Specify backup cache settings:

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

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

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

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

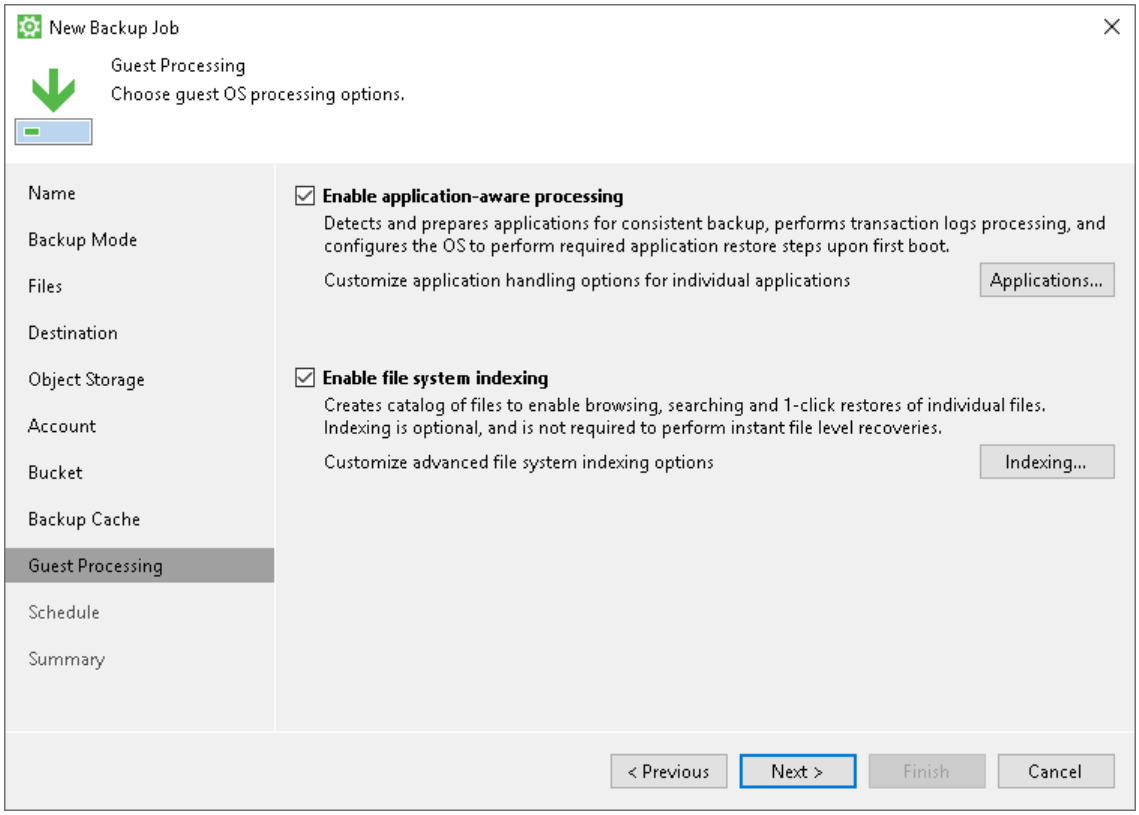


Step 10. Specify Guest Processing Settings

The **Guest Processing** step of the wizard is available in the Server edition of Veeam Agent for Microsoft Windows.

You can enable the following settings for guest OS processing:

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



Application-Aware Processing

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

To enable application-aware processing:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.

3. In the **Processing Settings** window, on the **General** tab, specify if Veeam Agent must process transaction logs [For Microsoft Exchange, Microsoft SQL and Oracle] or copy-only backups must be created.

   a. Select **Process transaction logs with this job** if you want Veeam Agent to process transaction logs.

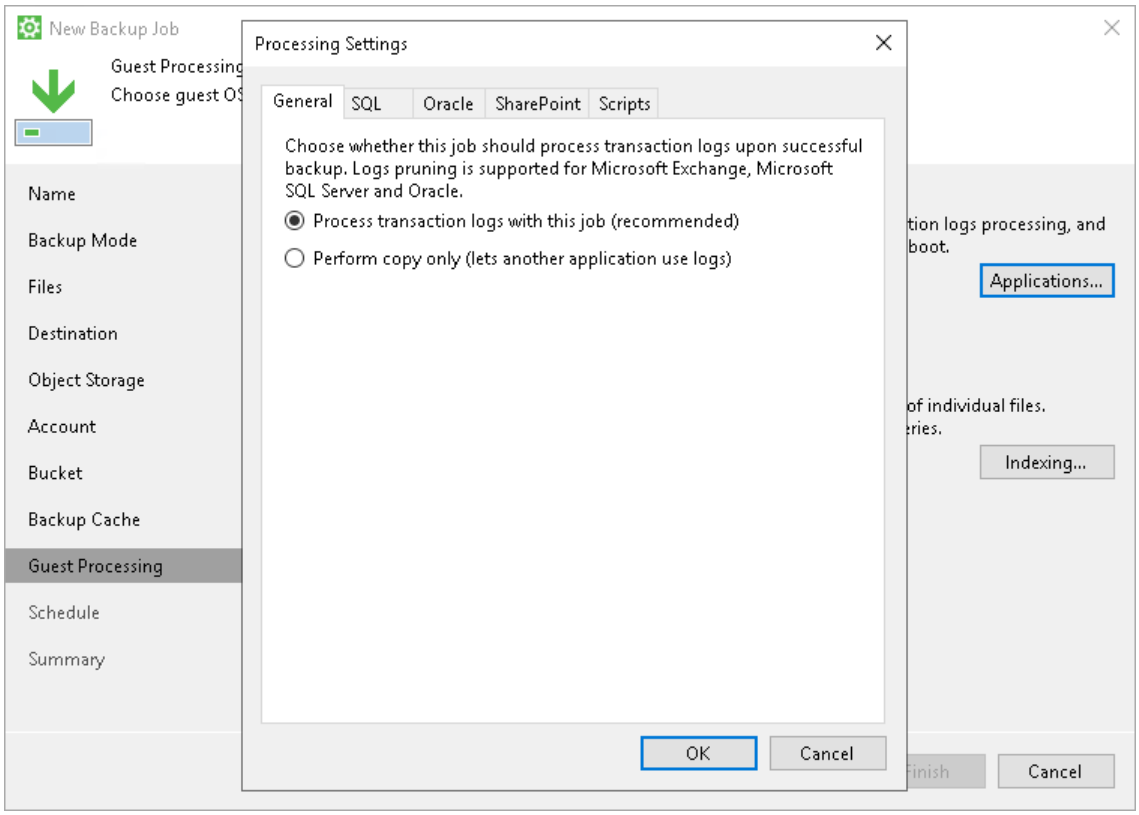
      - [For Microsoft Exchange] With this option selected, Veeam Agent will wait for backup to complete successfully and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.
      - [For Microsoft SQL Server and Oracle] You will have to specify settings for transaction log handling on the **SQL** and **Oracle** tabs of the **Processing Settings** window. For more information, see Microsoft SQL Server Transaction Log Settings and Oracle Archived Log Settings.

   b. Select **Perform copy only** if you use another tool to maintain consistency of the database state. Veeam Agent will create a copy-only backup. The copy only backup preserves the chain of full/differential backup files and transaction logs. After a copy-only backup, Veeam Agent does not trigger truncation of transaction logs. For more information, see this Microsoft article.

IMPORTANT

Consider the following:

- [For Microsoft Exchange] Veeam Agent for Microsoft Windows performs truncation of Microsoft Exchange transaction logs only if all disks that contain Microsoft Exchange databases and logs are included in a volume-level backup job.
- [For Microsoft SQL Server and Oracle] If both Microsoft SQL Server and Oracle Server are installed on one guest OS, you can enable log backup settings for one application only: either Microsoft SQL Server or Oracle.



Microsoft SQL Server Transaction Log Settings

If you back up Microsoft SQL Server, you can specify how Veeam Agent for Microsoft Windows must process database transaction logs:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the **Processing Settings** window, on the **General** tab, select **Process transaction logs with this job**.
4. In the **Processing Settings** window, click the **SQL** tab.
5. To specify a user account that Veeam Agent will use to connect to the Microsoft SQL Server, select the **Specify Windows account with sysadmin role on SQL Server** check box and enter a user name and password for the Microsoft Windows user account. This account must have the roles and permissions as specified in section Permissions for Guest Processing.

   > **NOTE**
   >
   > You cannot use Microsoft SQL Server accounts (for example, the SA account) to connect to the database.

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

     We recommend that you enable this option only for databases with log truncation managed by a database administrator or databases that use the *Simple* recovery model. If you enable this option for databases that use the *Full* or *Bulk-logged* recovery model, transaction logs may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs.
   - Select **Backup logs periodically** to back up transaction logs with Veeam Agent. Veeam Agent will periodically copy transaction logs to the backup location and store them together with the image-level backup. During the backup job session, transaction logs will be truncated.

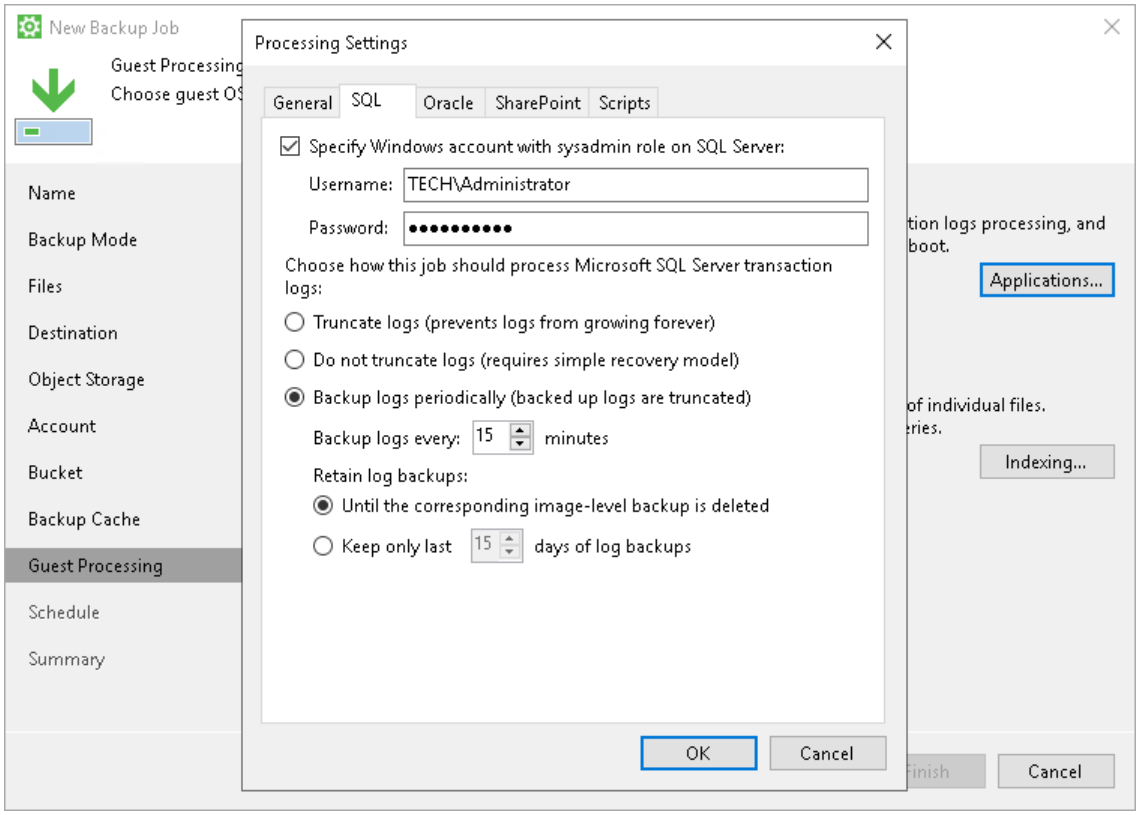
     For more information, see Microsoft SQL Server and Oracle Logs Backup and Restore.

     > **NOTE**
     >
     > You can enable transaction log backup in one backup job only. If you have already configured a job that is set up to back up transaction logs, you will not be able to select the **Backup logs periodically** option in the properties of another backup job.

If you have selected to back up transaction logs with Veeam Agent, you must specify settings for transaction log backup:

1. In the **Backup logs every <N> minutes** field, specify the frequency for transaction log backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
2. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup location.
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
   - Select **Keep only last <N> days of log backups** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backup. For more information, see Retention for Transaction Log Backups.

> **IMPORTANT**
>
> Veeam Agent for Microsoft Windows automatically excludes its configuration database from application-aware processing during backup. Transaction logs for the configuration database are not backed up.



Oracle Archived Log Settings

If you back up an Oracle database, you can specify how Veeam Agent for Microsoft Windows must process archived logs:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.

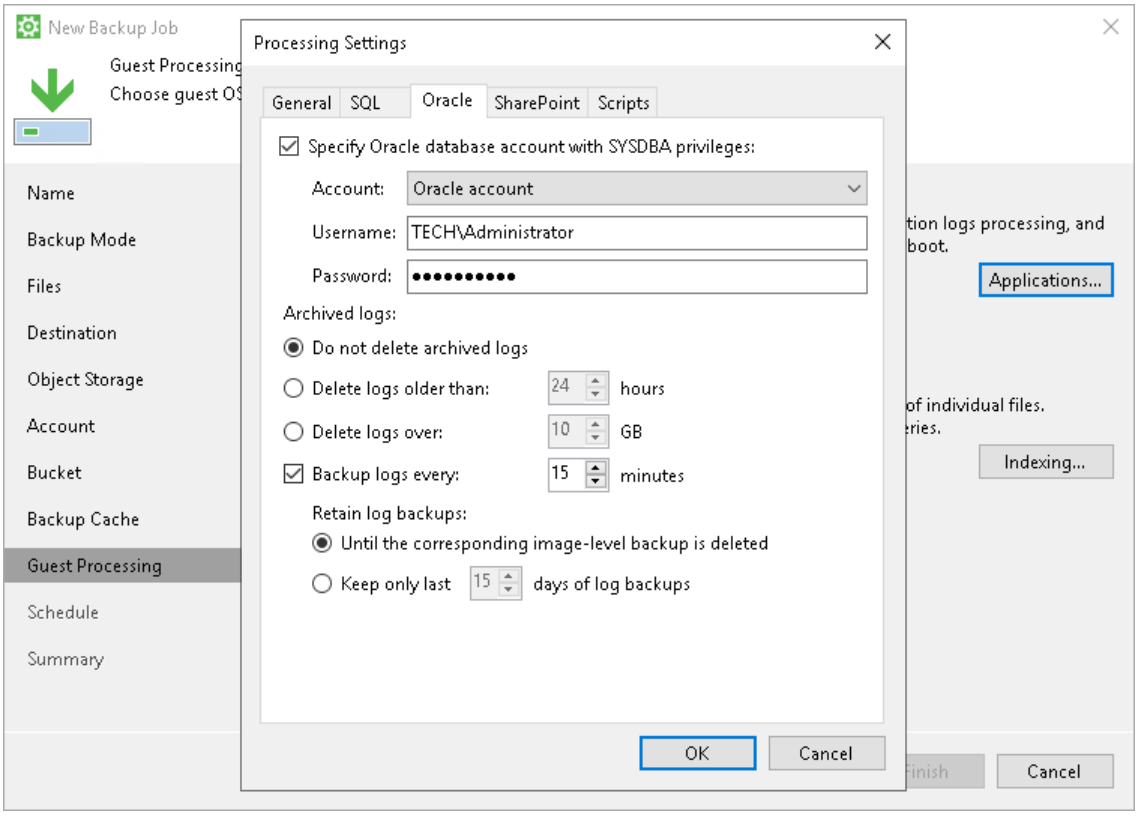
3. In the **Processing Settings** window, on the **General** tab, select **Process transaction logs with this job**.
4. In the **Processing Settings** window, click the **Oracle** tab.
5. Specify a user account that Veeam Agent for Microsoft Windows will use to connect to the Oracle database:
   a. Select the **Specify Oracle database account with SYSDBA privileges** check box.
   b. In the **Account** field, select what type of user account you plan to use: *Oracle account* or *Windows account*.
   c. In the **Username** and **Password** fields, enter a username and password for the account.

   The specified account must have SYSDBA rights on the Oracle database.
6. In the **Archived logs** section, specify if Veeam Agent for Microsoft Windows must delete archived logs on the Oracle database:
   - Select **Do not delete archived logs** if you want Veeam Agent for Microsoft Windows to preserve archived logs. When the backup job completes, Veeam Agent for Microsoft Windows will not delete archived logs.

     We recommend that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.
   - Select **Delete logs older than <N> hours** or **Delete logs over <N> GB** if you want Veeam Agent for Microsoft Windows to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent for Microsoft Windows will wait for the backup to complete successfully and then trigger archived logs deletion through Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next backup job session.

     > **TIP**
     >
     > If you configure backup job to back up archived logs, Veeam Agent also triggers archived logs deletion after each log backup job session.
7. To back up Oracle archived logs with Veeam Agent for Microsoft Windows, select the **Backup log every <N> minutes** check box and specify the frequency for archived log backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

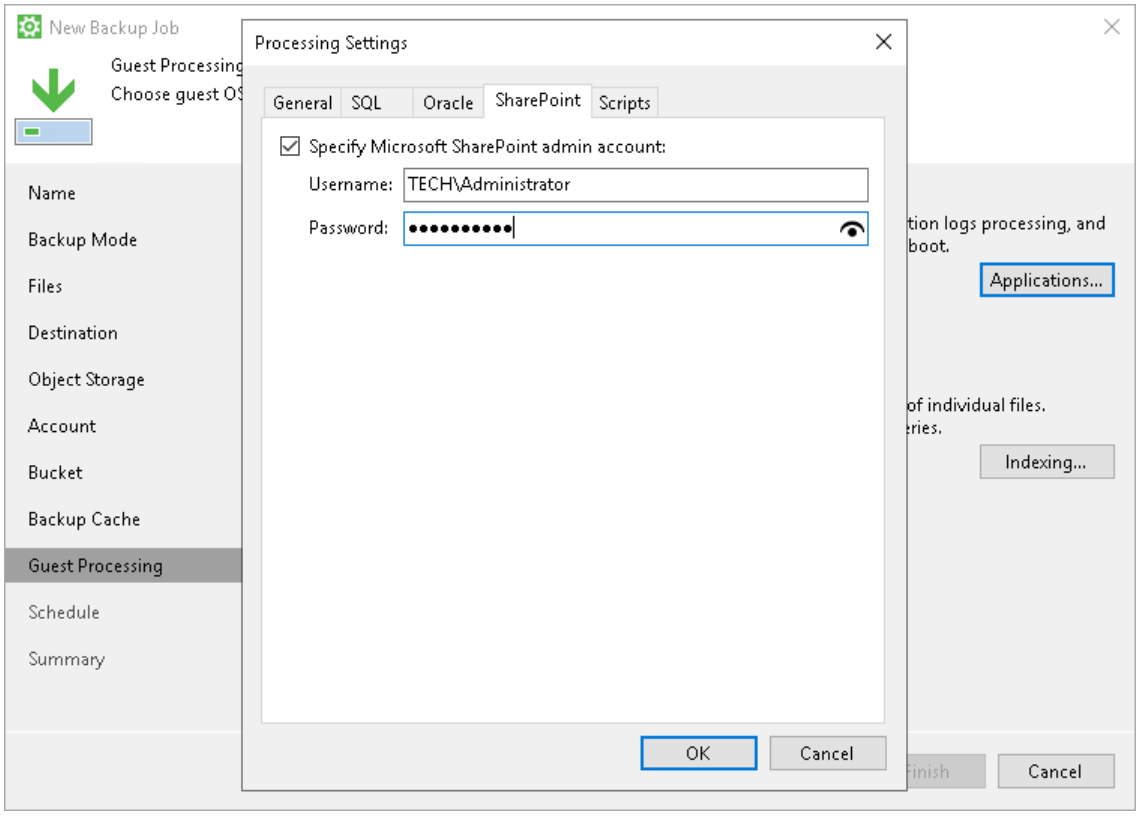
   > **NOTE**
   >
   > You can enable archived log backup in one backup job only. If you have already configured a job that is set up to back up archived logs, you will not be able to select the **Backup logs every <N> minutes** option in the properties of another backup job.
8. In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for Veeam Agent backups and archived log backups.
   - Select **Keep only last <n> days t**o keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the Veeam Agent backups. For more information, see Retention for Archived Log Backups.



Microsoft SharePoint Account Settings

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

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the **Processing Settings** window, click the **SharePoint** tab.
4. Select the **Specify Microsoft SharePoint admin account** check box and enter a user name and password for the user account.



Pre-Freeze and Post-Thaw Scripts

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

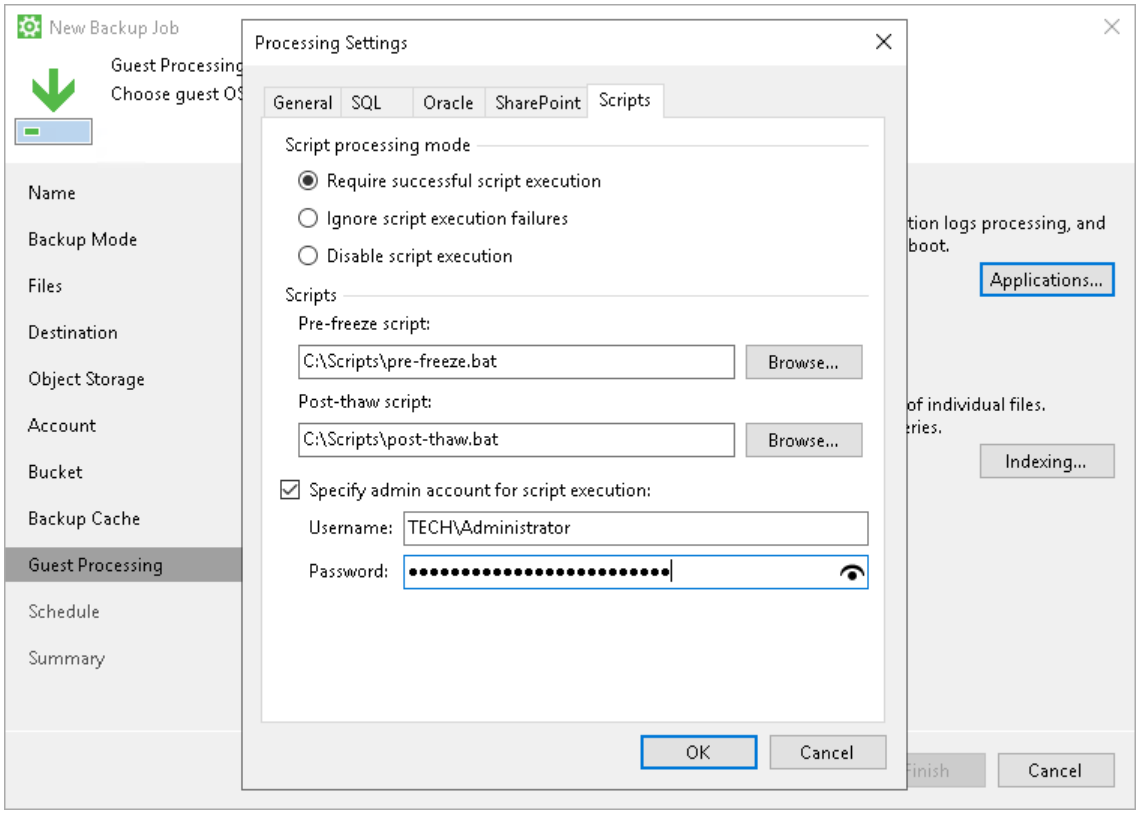
To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step, click **Applications**.
2. In the **Processing Settings** window, click the **Scripts** tab.
3. In the **Script processing mode** section, specify the scenario for scripts execution:
   - Select **Require successful script execution** if you want Veeam Agent for Microsoft Windows to stop the backup process if the script fails.
   - Select **Ignore script execution failures** if you want to continue the backup process even if script errors occur.
   - Select **Disable script execution** if you do not want to run scripts.
4. In the **Scripts** section, specify paths to pre-freeze and post-thaw scripts. Scripts must reside on a local drive of the Veeam Agent computer.

   Veeam Agent for Microsoft Windows supports the following types of scripts:
   - Program files in the EXE, BAT and CMD format
   - Windows script files in the JS, VBS and WSF format
   - PowerShell script files in the PS1 format

You can use scripts of other formats as well, but we cannot guarantee correct processing of such scripts.

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



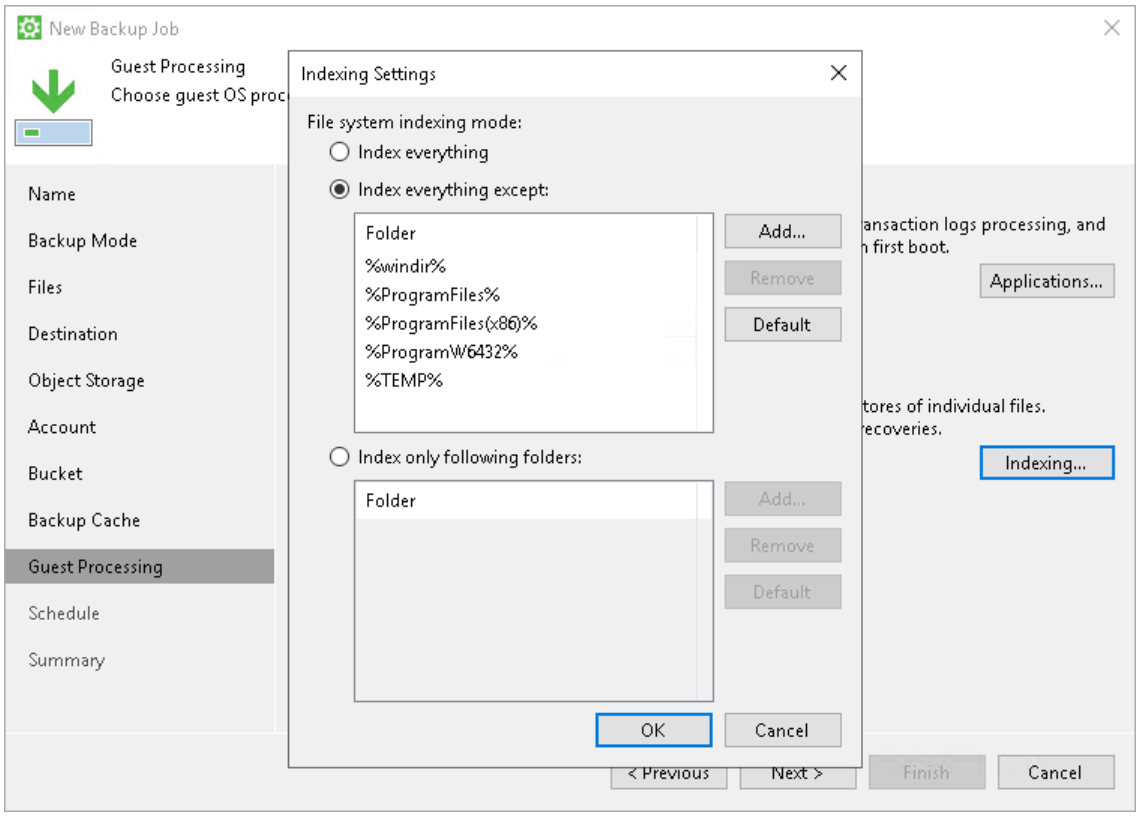
File Indexing

To specify file indexing options:

1. At the **Guest Processing** step of the wizard, click **Indexing**.
2. In the **Indexing Settings** window, specify the indexing scope:
   - Select **Index everything** if you want to index all files within the backup scope that you have specified at the Backup mode step of the wizard. Veeam Agent for Microsoft Windows will index all files that reside:
     - on your computer OS (for entire computer backup)
     - on the volumes that you have selected for backup (for volume-level backup)
     - in the directories that you have selected for backup (for file-level backup)
   - Select **Index everything except** if you want to index all files on your computer OS except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders using the **Add** and **Remove** buttons on the right. You can also use system environment variables to form the list, for example: *%windir%*, *%ProgramFiles%* and *%Temp%*.

     To reset the list of folders to its initial state, click **Default**.

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



Step 11. Specify Backup Schedule

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

- Scheduling Settings in Free and Workstation Editions
- Scheduling Settings in Server Edition

Scheduling Settings in Free and Workstation Editions

At the **Schedule** step of the wizard, set up Veeam Agent for Microsoft Windows to run the backup job periodically at specific time or after specific computer events:

- Select the time to launch the backup job.
- Select events that trigger the backup job launch.

> **IMPORTANT**
>
> If the power scheme on your computer does not allow using wake up timers, Veeam Agent for Microsoft Windows will ask you to change the power scheme settings. Click **Yes** to allow Veeam Agent for Microsoft Windows to wake your computer from sleep for backup.
>
> You can manually change the power scheme settings on your computer. To do this, navigate to **Control Panel** > **All Control Panel Items** > **Power Options** > **Edit Plan Settings**.

Selecting Time to Launch Backup Job

In the **Periodically** section, specify time to launch the backup job:

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

   You can leave the **Daily at** check box unchecked to configure the backup job without daily schedule. In this case, you will be able to use the configured backup job to perform backup automatically at specific events. You can also use the configured backup job to create ad-hoc incremental and standalone full backups. To learn more, see Performing Ad-Hoc Backups.
2. If you have selected the *On these days* option, click the **Days** button and clear check boxes for the days when the job must not start.
3. Select the action that Veeam Agent for Microsoft Windows must perform in case your computer is powered off at the time when the scheduled backup job must start.
   - *Backup once powered on* — select this option if you want Veeam Agent for Microsoft Windows to start the scheduled backup job when you power on the computer.

- *Skip backup* — select this option if you want Veeam Agent for Microsoft Windows not to start the scheduled backup job when the computer is powered on. Veeam Agent for Microsoft Windows will perform backup at the next scheduled time.

4. If you want Veeam Agent for Microsoft Windows to perform a finalizing action after the backup job completes successfully, select the necessary action:

   - *Keep running* — select this option if the computer must keep on working.
   - *Sleep* — select this option if you want Veeam Agent for Microsoft Windows to bring your computer to the standby mode.
   - *Shutdown* — select this option if you want Veeam Agent for Microsoft Windows to shut down your computer.
   - *Hibernate* — select this option if you want Veeam Agent for Microsoft Windows to bring your computer to the hibernate mode. This option is available if the hibernate mode is enabled on your computer. To learn more, see this Microsoft article.

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

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

Selecting Events that Trigger Backup Job Launch

In the **At the following events** section, specify computer events that trigger the backup job launch:

- Select the **Lock** check box if you want to start the scheduled backup job when the user locks the computer.

  > **NOTE**
  >
  > The backup job does not always start right after the lock event is created. For example, when you put the Veeam Agent computer to sleep, the operating system creates the lock event before the entering sleep event but the backup job starts after the computer resumes from the sleep mode. The backup job does not start if the computer stayed in the sleep mode longer than 15 minutes.

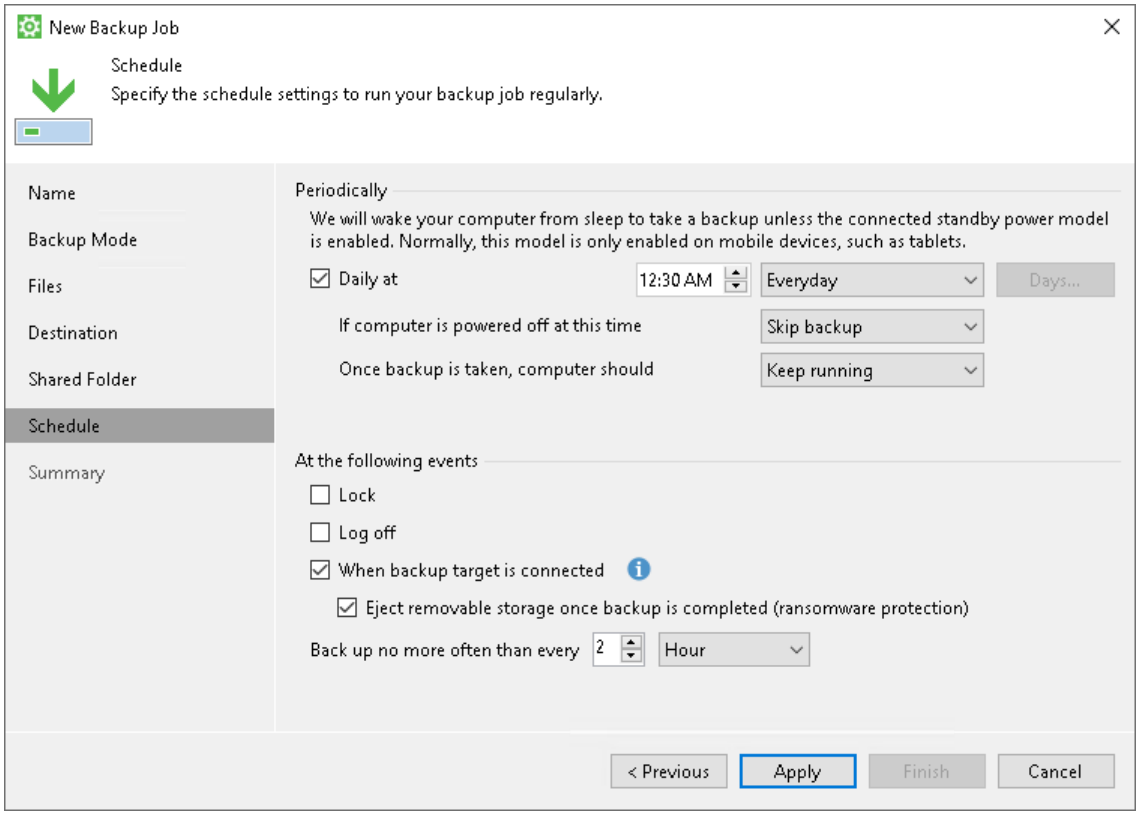
- Select the **Log off** check box if you want to start the scheduled backup job when the user working with the computer performs a logout operation.
- Select the **When backup target is connected** check box if you want to start the scheduled backup job when the backup storage becomes available. With this option selected, Veeam Agent will detect state changes for networks and drives. When such change is detected, Veeam Agent will check if the target backup repository is accessible. If so, it will start the backup job.
- Select the **Eject removable storage once backup is completed** check box if you want Veeam Agent for Microsoft Windows to unmount the storage device after the backup job completes successfully. With this option selected, backup files on the removable storage will be protected from encrypting ransomware, such as CryptoLocker.

  Veeam Agent applies this setting only to backup jobs triggered by computer events. In case of backup jobs scheduled to run at specific time, Veeam Agent will ignore this setting, and the storage device will not be unmounted after the backup job completes successfully.

> **IMPORTANT**
>
> The *Eject removable storage once backup is completed* option does not guarantee a bulletproof protection against ransomware. To ensure your backups are safe, keep the OS up to date and regularly scan your backup repository for virus threats using modern antivirus software.

- Use the **Back up no more often than every <N> <time units>** field to restrict the frequency of backup job sessions. Specify a minutely, hourly or daily interval between the backup job sessions.

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



Scheduling Settings in Server Edition

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

> **IMPORTANT**
>
> If the power scheme on your computer does not allow using wake up timers, Veeam Agent for Microsoft Windows will ask you to change the power scheme settings. Click **Yes** to allow Veeam Agent for Microsoft Windows to wake your computer from sleep for backup.
>
> You can manually change the power scheme settings on your computer. To do this, navigate to **Control Panel** > **All Control Panel Items** > **Power Options** > **Edit Plan Settings**.

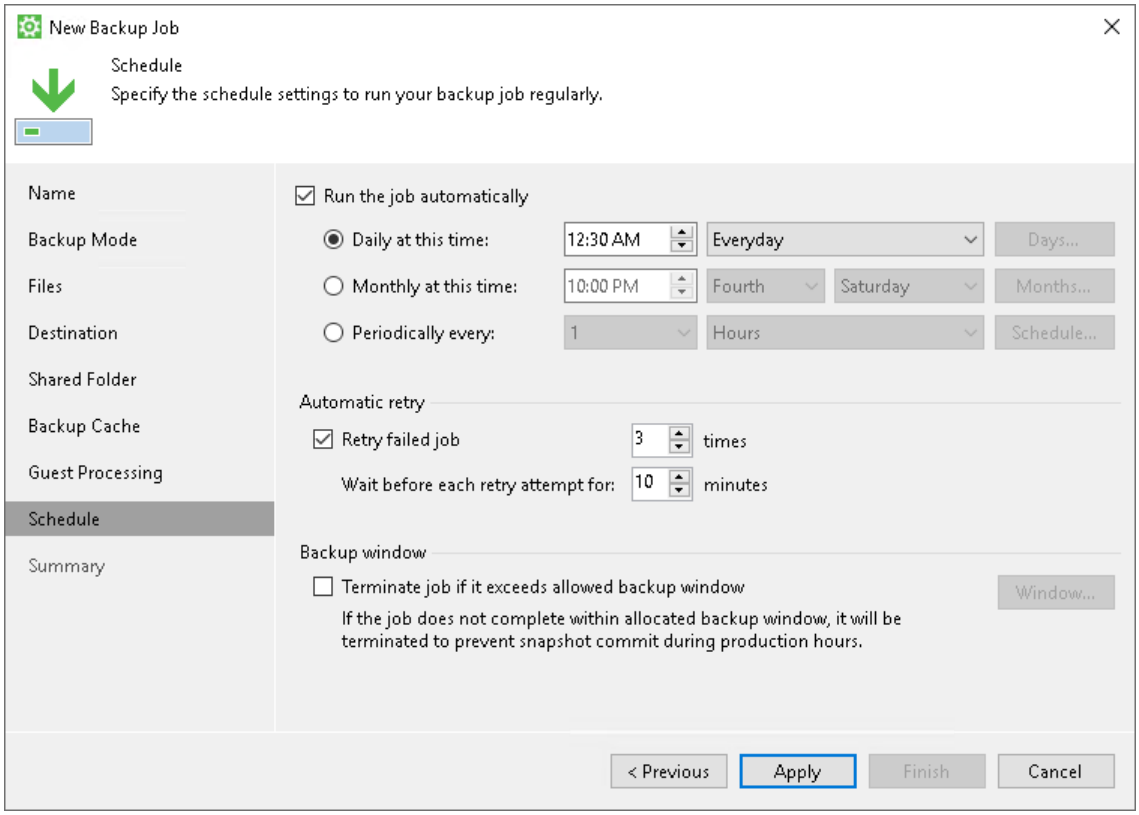
To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

     A repeatedly run job is started by the following rules:

     - Veeam Agent for Microsoft Windows always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
     - If you define permitted hours for the job, after the denied interval is over, Veeam Agent for Microsoft Windows will immediately start the job and then run the job by the defined schedule.

     For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.
   - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.
3. In the **Automatic retry** section, define whether Veeam Agent for Microsoft Windows must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Agent for Microsoft Windows will retry the job for the defined number of times without any time intervals between the job runs.
4. In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:
   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.
   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.


New Backup Job
Schedule
Specify the schedule settings to run your backup job regularly.
Name
Backup Mode
Files
Destination
Shared Folder
Backup Cache
Guest Processing
Schedule
Summary
Run the job automatically
Daily at this time:
12:30 AM
Everyday
Days...
Monthly at this time:
10:00 PM
Fourth
Saturday
Months...
Periodically every:
1
Hours
Schedule...
Automatic retry
Retry failed job
3
times
Wait before each retry attempt for:
10
minutes
Backup window
Terminate job if it exceeds allowed backup window
Window...
If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.
< Previous
Apply
Finish
Cancel

Step 12. Review Backup Job Settings

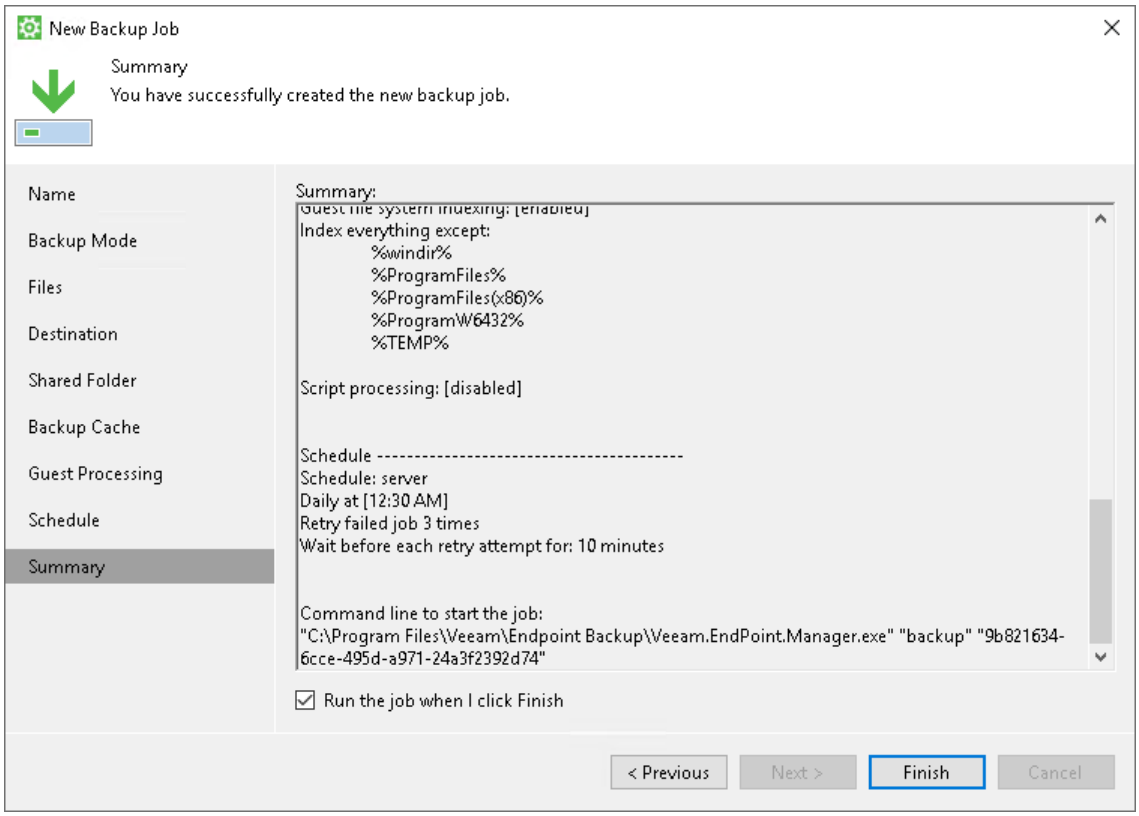
At the **Summary** step of the wizard, complete the backup job configuration process.

1. Review settings of the configured backup job.

   In addition to backup job settings, Veeam Agent for Microsoft Windows displays a command to start the job using the command-line interface.

2. To start the job after you close the wizard, select the **Run the job when I click Finish** check box.

3. Click **Finish**.



What You Do Next

After you configure the scheduled backup job, Veeam Agent for Microsoft Windows displays a clock over its icon in the system tray. The clock identifies that your computer is protected with the scheduled backup job. Veeam Agent for Microsoft Windows will periodically start the scheduled backup job to back up selected data and add a new restore point to the backup chain in the target location.

If necessary, you can also perform the following backup operations when you need it:

- Create a standalone full backup
- Create an incremental backup
- Create an active full backup

If some of your data gets lost or corrupted, you can do the following:

- Recover all computer volumes or specific volumes from the backup
- Recover individual files and folders from the backup

Managing Backup Jobs

After you configure the scheduled backup job, you can perform the following actions with it:

- Edit the backup job settings
- Disable and enable the backup job
- Remove the backup job

Editing Backup Job Settings

If you want to change settings of a 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, change the target location or job scheduling settings.

To access backup job settings, do one of the following:

- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**. Then hover over the name of the backup job whose settings you want to change, and select **Edit job**.
- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Backup** > **Configure backup**.

> **NOTE**
>
> The **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent for Microsoft Windows.

Then edit the job settings as required. To learn more about available job settings, see Creating Backup Jobs.

If you change the target location for the backup job, during the next backup job session Veeam Agent for Microsoft Windows will perform full data backup. All subsequent backup sessions will produce incremental backups — Veeam Agent for Microsoft Windows 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 Microsoft Windows will create a new incremental backup. The backup will contain the following data:

- All data blocks pertaining to new data added to the backup scope.
- 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).

> **TIP**
>
> 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.

Editing Encryption Settings

If you change encryption settings for the backup job, during the next backup job session Veeam Agent for Microsoft Windows will create active full backup — encrypted (if encryption was enabled) or unencrypted (if encryption was disabled). All subsequent backup sessions will produce incremental backups.

Enabling or disabling encryption does not affect backup files that were created before you have changed encryption settings.

If the backup chain contains encrypted and unencrypted backup files, you need to provide a password to restore data from any restore point in this chain. After all encrypted backup files are removed from the backup chain according to retention policy, you will be able to restore data from remaining unencrypted restore points without providing a password.

Disabling and Enabling 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 Microsoft Windows. 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.

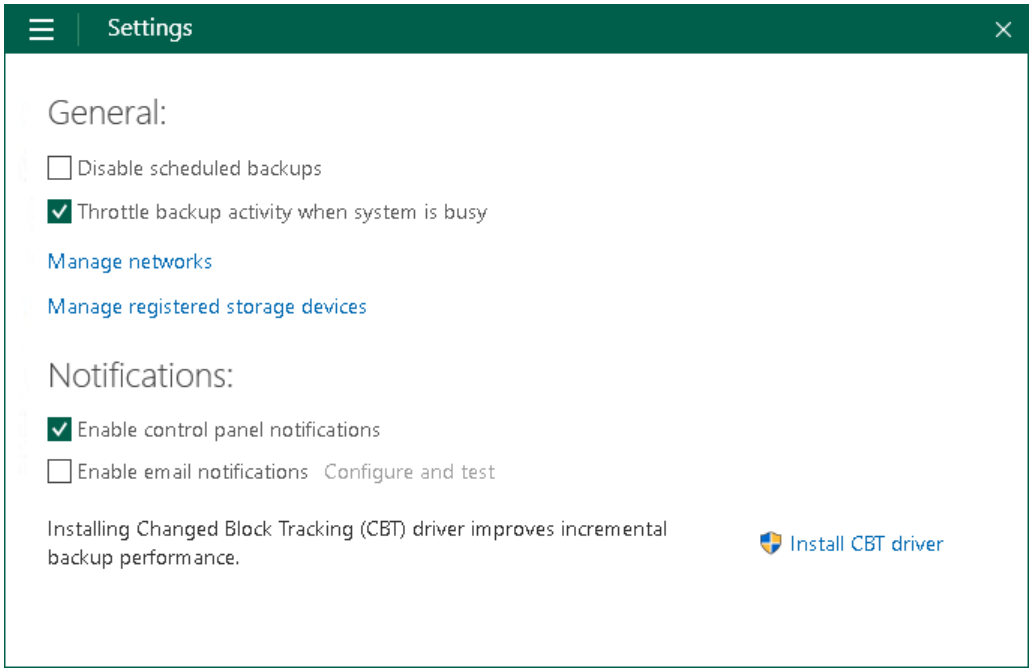
The disabling option does not put on hold the backup cache synchronization process. If Veeam Agent has created one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent will immediately upload backup files to the target location.

To disable scheduled backups:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Select the **Disable scheduled backups** check box.

To enable scheduled backups:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Clear the **Disable scheduled backups** check box.


Settings
General:
Disable scheduled backups
Throttle backup activity when system is busy
Manage networks
Manage registered storage devices
Notifications:
Enable control panel notifications
Enable email notifications
Configure and test
Installing Changed Block Tracking (CBT) driver improves incremental backup performance.
Install CBT driver

Removing Backup Job

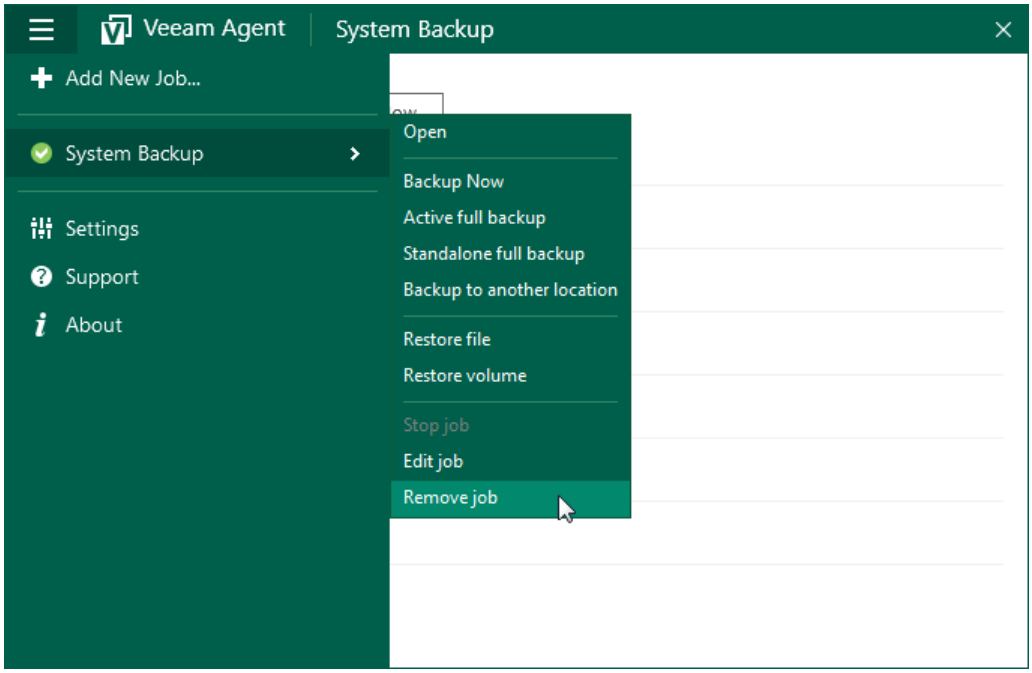
You can remove a backup job configured in Veeam Agent for Microsoft Windows. When you remove a backup job, Veeam Agent for Microsoft Windows also removes information about backup job sessions from the Veeam Agent database. After you remove the job, information about sessions of this job is not displayed in the **Status** view of the control panel any longer.

> **NOTE**
>
> You cannot remove a backup job that is currently running. You must stop the job first.

Backup files created by the deleted backup job remain intact in the target location.

To remove a backup job:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. In the main menu, hover over the name of the backup job that you want to remove, and select **Remove job**.
3. In the displayed window, click **Yes**.



Controlling Backup Post-Job Action

In the Free and Workstation product editions, you can set up Veeam Agent to perform a finalizing action after the backup job completes successfully:

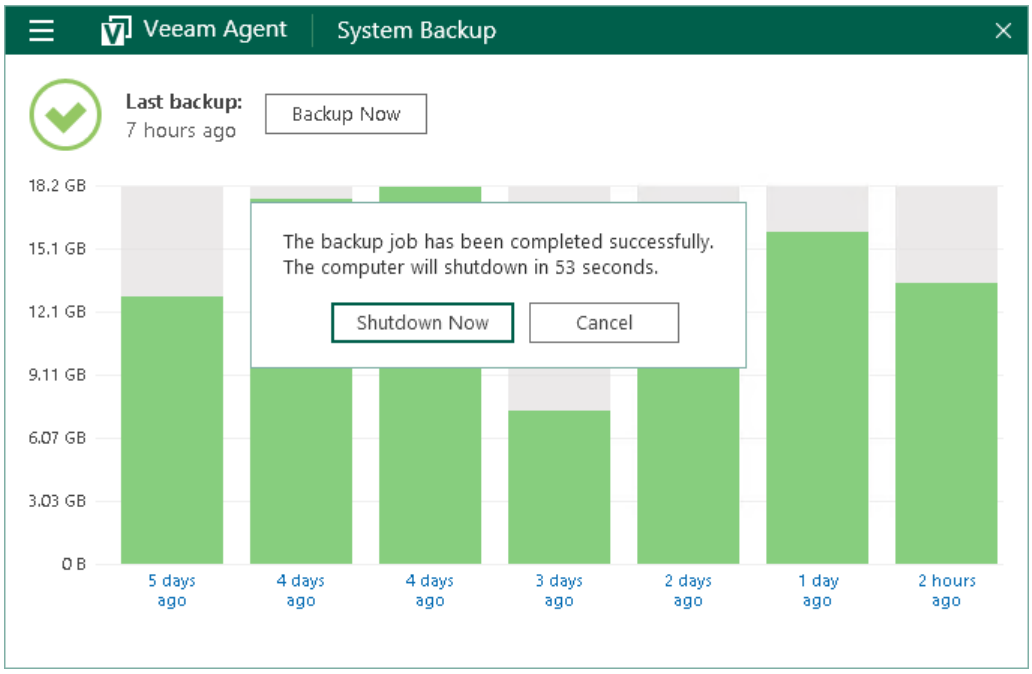
- *Sleep* — bring your computer to the standby mode.
- *Hibernate* — bring your computer to the hibernate mode.
- *Shutdown* — shut down your computer.

To learn more, see Specify Backup Schedule.

When the backup job completes, Veeam Agent opens control panel and prompts a dialog with a countdown to the specified action. Timeout between the backup job completion and the backup post-job action is 60 seconds.

- To proceed to the backup post-job action immediately, click **Sleep/Hibernate/Shutdown Now**.
- To cancel the action (for example, if you want to continue working or to save your data before turning off the computer), click **Cancel**.

If you do not select any option, Veeam Agent will perform the specified action when timeout expires.



Performing Ad-Hoc Backups

In addition to running scheduled backups, you can create ad-hoc backups of your data at any time you need. Veeam Agent for Microsoft Windows lets you perform the following types of ad-hoc backups:

- Incremental ad-hoc backup
- Active full backup
- Standalone full backup
- Backup to another location

Creating Incremental Backups

You can create an ad-hoc incremental backup of your data in addition to the scheduled backup. Ad-hoc incremental backup may be necessary if you want to capture your data at a specific point in time, for example, before you install new software on your computer. Ad-hoc incremental backup lets you produce an additional restore point in the backup chain at any time and does not require you to reconfigure the scheduling settings in the backup job.

Before you perform ad-hoc incremental backup, check the following prerequisites:

- The backup job that you want to use to perform ad-hoc incremental backup must be configured and successfully run at least once.
- You cannot perform ad-hoc incremental backup if a backup task of any type is currently running. These include a scheduled backup, standalone full backup, active full backup or ad-hoc incremental backup.

To perform ad-hoc incremental backup:

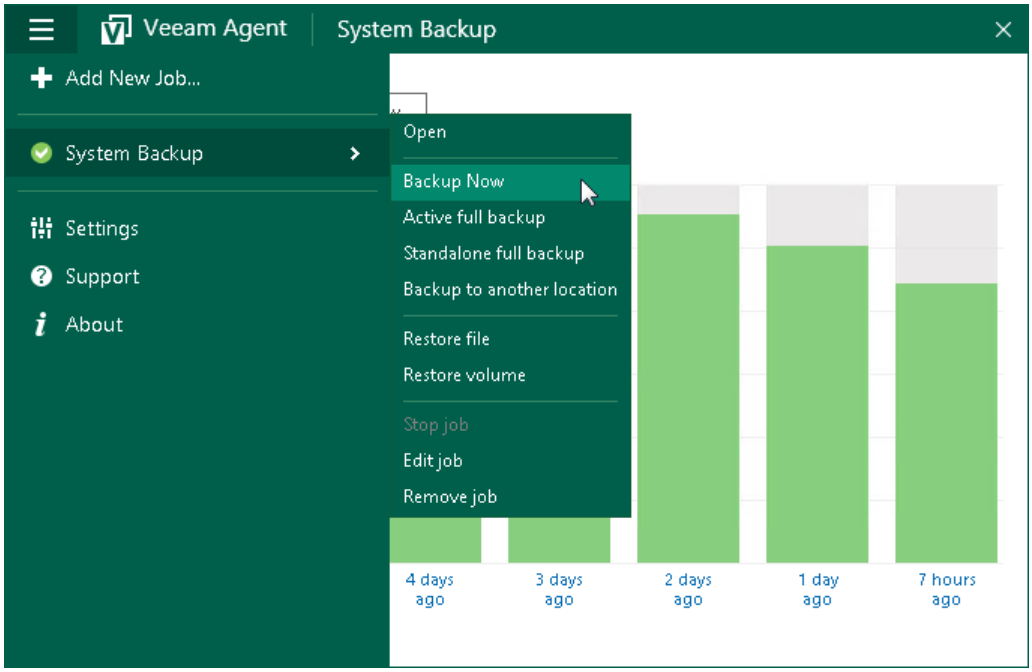
1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. Do either of the following:
    - If the Veeam Agent control panel currently displays statistics of the job that you want to use to perform ad-hoc incremental backup, in the job statistics window, click **Backup Now**.
    - If you want to perform ad-hoc incremental backup using another backup job configured in Veeam Agent, in the main menu, hover over the name of the necessary job and select **Backup now**.

If only one job is configured in Veeam Agent for Microsoft Windows, you can also start the ad-hoc incremental backup task from the system tray menu:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **Backup now**.

> **NOTE**
>
> The **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent for Microsoft Windows.

Veeam Agent for Microsoft Windows will perform incremental backup using settings of the scheduled backup job and add a new restore point to the backup chain in the target location.


Veeam Agent
System Backup
Add New Job...
System Backup
Settings
Support
About
Open
Backup Now
Active full backup
Standalone full backup
Backup to another location
Restore file
Restore volume
Stop job
Edit job
Remove job
4 days ago
3 days ago
2 days ago
1 day ago
7 hours ago

Creating Active Full Backups

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

> **IMPORTANT**
>
> If you have a file-level backup job configured in Veeam Agent and you need to extend the volume where backed-up files reside, we strongly recommend to create an active full backup after the volume is extended. Otherwise, Veeam Agent may skip files during the job run even if these files are added to the backup scope.

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

- The backup job must be configured.
- You cannot create an active full backup if a backup task of any type is currently running. This includes a scheduled backup, standalone full backup, active full backup or ad-hoc incremental backup.
- A user account under which you start the **Active full backup** operation must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.

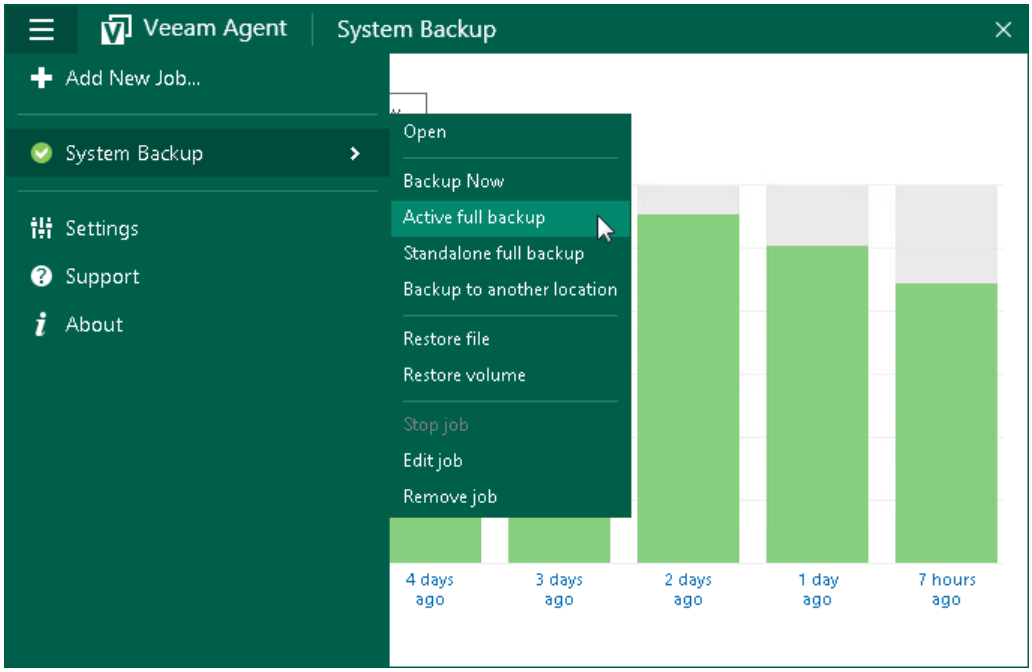
To perform active full backup:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. In the main menu, hover over the name of the backup job that you want to use to create an active full backup, and select Active full backup. Veeam Agent for Microsoft Windows will create a full backup file using settings of the backup job and add this backup file to the backup chain.

If only one job is configured in Veeam Agent for Microsoft Windows, you can also start the active full backup task from the system tray menu:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **Active full backup**.

> **NOTE**
>
> The **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent for Microsoft Windows.


Veeam Agent
System Backup
Add New Job...
System Backup
Settings
Support
About
Open
Backup Now
Active full backup
Standalone full backup
Backup to another location
Restore file
Restore volume
Stop job
Edit job
Remove job
4 days ago
3 days ago
2 days ago
1 day ago
7 hours ago

Creating Standalone Full Backups

If you want to back up your data at a specific point in time, you can create a standalone full backup. The standalone full backup is independent: it is not followed by subsequent incremental backups and is not removed by retention. You can use the standalone full backup to create an additional restore point from which you can recover your data.

Before you create a standalone full backup, check the following prerequisites and limitations:

- The backup job must be configured.
- A user account under which you start the Standalone full backup operation must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.
- You cannot create a standalone full backup if a backup task of any type is currently running. This includes a scheduled backup, standalone full backup, active full backup or ad-hoc incremental backup.
- You cannot create a standalone full backup if you have chosen to store backup files in one of the following locations:
  - Veeam backup repository
  - Veeam Cloud Connect repository
  - Object storage

  If you want to create a full backup file not associated with the backup chain, you can perform standalone full backup to another location. To learn more, see Performing Backup to Another Location.

To create a standalone full backup:

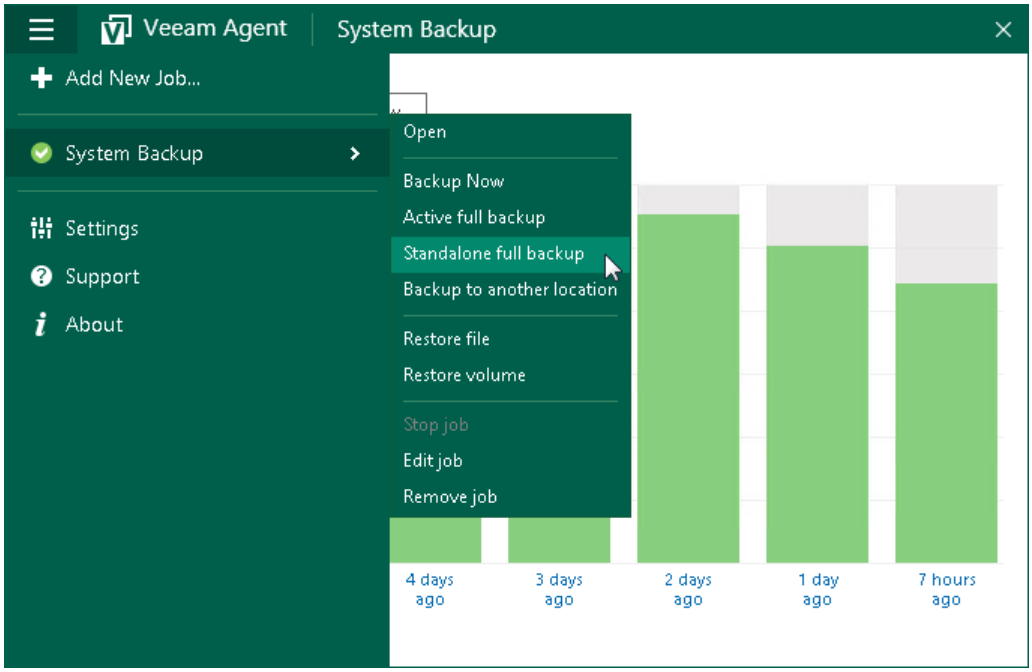
1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. In the main menu, hover over the name of the backup job that you want to use to create a standalone full backup, and select **Standalone full backup**. Veeam Agent for Microsoft Windows will create a full backup file using settings of the backup job. The resulting full backup file will be saved in the target location specified in the job settings, and placed to a separate folder. The folder is named in the following way: `<BackupJobName>.adhoc.<DateandTime>`.

If only one job is configured in Veeam Agent for Microsoft Windows, you can also start the standalone full backup task from the system tray menu:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **Standalone full backup**.

> **NOTE**
>
> The **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent for Microsoft Windows.

You can also create a standalone full backup in a location that is not specified in the backup job settings. To learn more, see Performing Backup to Another Location.


Veeam Agent
System Backup
Add New Job...
System Backup
Settings
Support
About
Open
Backup Now
Active full backup
Standalone full backup
Backup to another location
Restore file
Restore volume
Stop job
Edit job
Remove job
4 days ago
3 days ago
2 days ago
1 day ago
7 hours ago

Performing Backup to Another Location

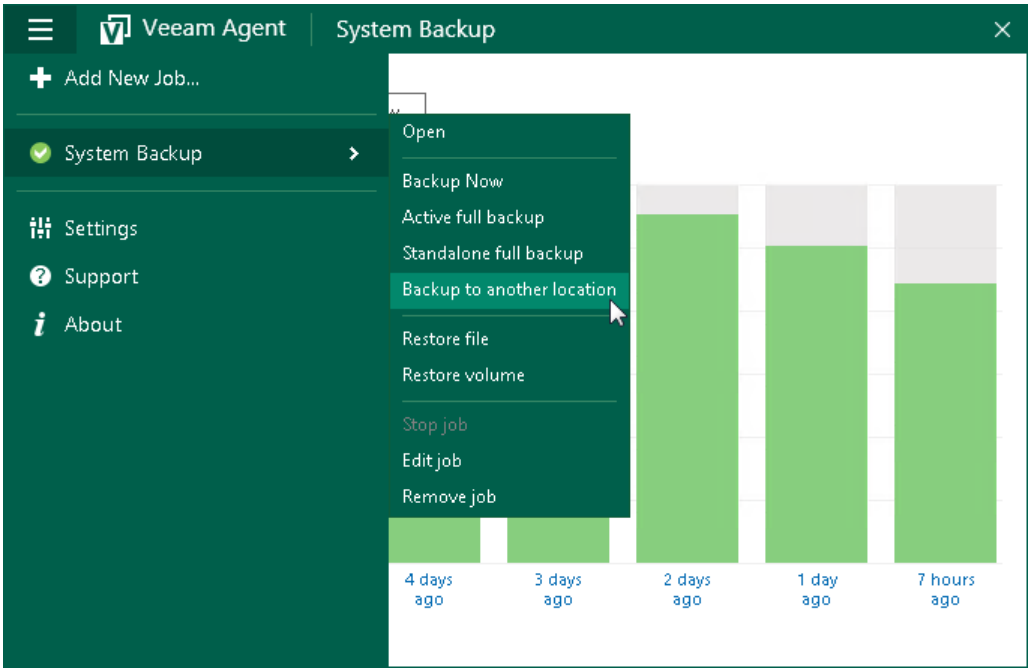
You can create a standalone full backup in a separate location that is not specified as a target location in the backup job settings. Performing backup to another location is similar to creating regular standalone full backups. The main difference is that you must manually select a target location in which Veeam Agent for Microsoft Windows will save the backup file.

Before you perform backup to another location, check the following prerequisites:

- The backup job must be configured.
- You cannot perform backup to another location if a backup task of any type is currently running. This includes a scheduled backup, standalone full backup, active full backup or ad-hoc incremental backup.
- A user account under which you start the **Backup to another location** operation must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.

To perform backup to another location:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. In the main menu, hover over the name of the backup job that you want to use to perform backup, and select **Backup to another location**.



NOTE

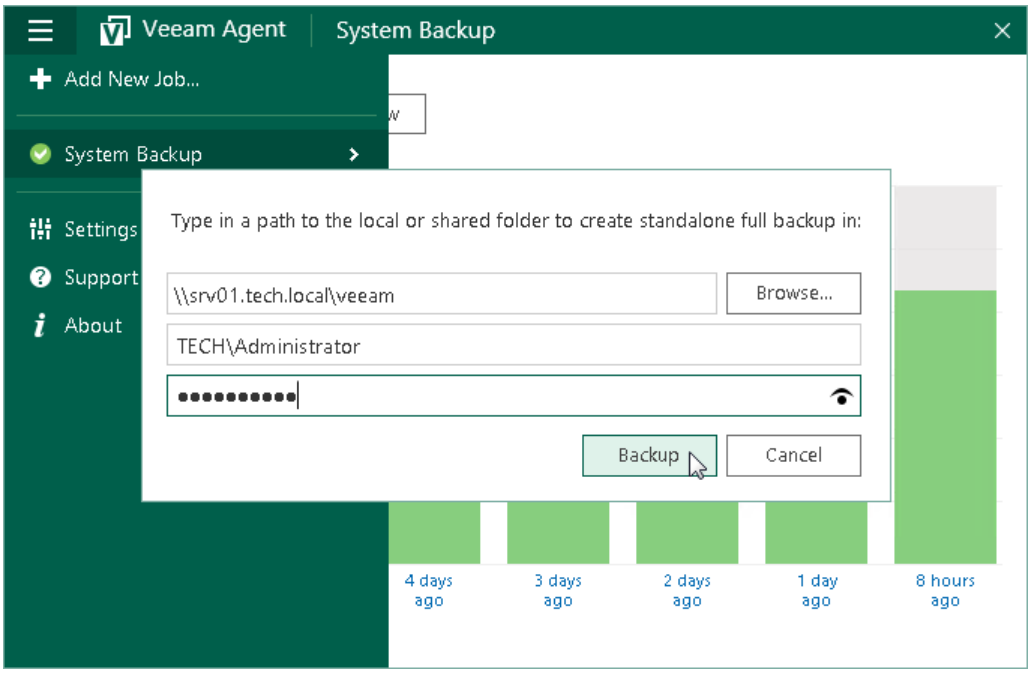
If only one job is configured in Veeam Agent for Microsoft Windows, you can also start the standalone full backup task from the system tray menu:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select Backup > Backup to another location.

Note that the **Backup** option is not available in the system tray menu if multiple backup jobs are configured in Veeam Agent.

3. In the standalone full backup dialog window, specify the target location for the backup file:
   - If you want to save the backup file in a folder on a local drive or a removable storage device, click **Browse** and select the necessary folder or type a path to the folder where backup file must be saved.
   - If you want to save the backup file in a network shared folder, type a UNC name of the network shared folder. Keep in mind that the UNC name always starts with two back slashes (\\). If the network shared folder requires authentication, specify a user name and password of the account that has access permissions on this shared folder. The user name must be specified in the *DOMAIN\UserName* format.
4. Click **Backup**.

   Veeam Agent for Microsoft Windows will create a full backup file using settings of the selected backup job. The resulting full backup file will be saved in a separate folder in the specified location. The folder is named in the following way: `<BackupJobName>.adhoc.<DateandTime>`.



Performing Backup with Command Line Interface

In addition to running scheduled backup jobs and performing ad-hoc backups from the Veeam Agent tray agent or control panel, you can create backups with the command line interface. For example, you can use commands for running a backup job in custom scripts to set up more detailed backup schedule than the daily schedule configured with the control panel.

You can run a backup job from the command line interface to create the following types of backups:

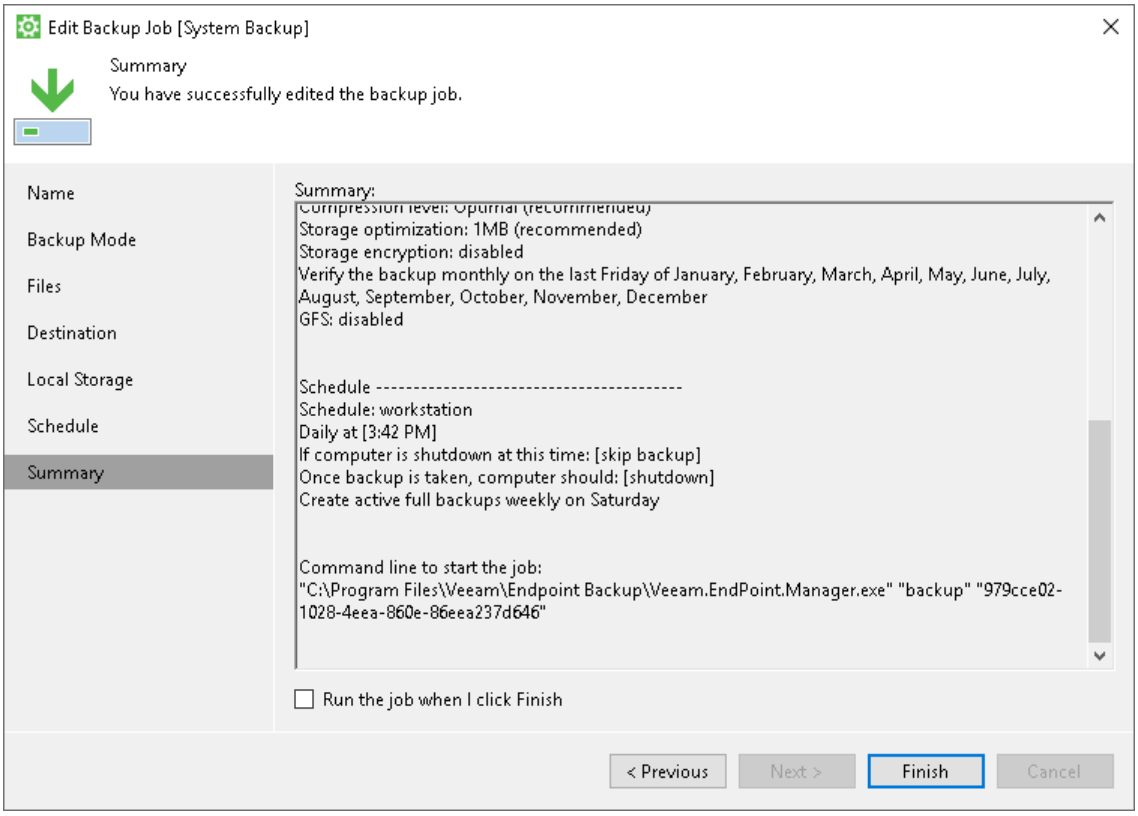
- Full or incremental backup (regular restore point in the backup chain)
- Active full backup
- Standalone full backup
- Backup to another location

> **IMPORTANT**
>
> If you create backups with the command line interface, Veeam Agent will ignore the following network connection restrictions:
>
> - Disabled backup over metered connections
> - Disabled backup over VPN connections
> - Backup over selected wireless networks
>
> To learn more about network usage settings, see Restricting Network Connections Usage.

Before you create a backup from the command line interface, check the following prerequisites:

- The backup job must be configured.
- You cannot run a backup job from the command line interface if a backup task for this job is currently running. This includes a scheduled backup, standalone full backup or ad-hoc incremental backup.

  If more than one backup job is configured, you can run multiple backup jobs at the same time.
- To create a standalone full backup or backup to another location, you must run the command line interface with administrative privileges.
- If more than one backup job is configured, you must specify the job ID in the *"00000000-0000-0000-0000-000000000000"* format. You can find the job ID at the **Summary** step of the backup job wizard.



Creating Backups

To perform backup, use a command with the following syntax:

- If one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /backu
p
```

- If more than one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /backu
p "<ID>"
```

where `<ID>` — unique job ID generated by Veeam Agent for Microsoft Windows.

Creating Active Full Backups

To create an active full backup, use a command with the following syntax:

- If one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /activ
efull
```

- If more than one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /activefull "<ID>"
```

where <ID> — unique job ID generated by Veeam Agent for Microsoft Windows.

Creating Standalone Full Backups

To create a standalone full backup, use a command with the following syntax:

- If one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone
```

- If more than one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone "<ID>"
```

where <ID> — unique job ID generated by Veeam Agent for Microsoft Windows.

Performing Backup to Another Location

To create a standalone full backup to a different location than a location that is specified in the backup job settings, use a command with the following syntax:

- If one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone <location>
```

- If more than one backup job is configured:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone <location> "<ID>"
```

where:

- <location> — path to a folder in which the backup should be created.
- <ID> — unique job ID generated by Veeam Agent for Microsoft Windows.

> **IMPORTANT**
>
> You can specify a network shared folder as a target location for standalone full backup only if read and write permissions on this folder are granted to *Everyone* or to the *LocalSystem* account of the Veeam Agent computer. You cannot specify credentials to access the network shared folder in the command.

Monitoring Backup Job Status

When you start a backup job from the command line interface, it runs automatically in the background. You can view information about the backup job session or the created restore point in the control panel. To learn more, see Viewing Statistics in Control Panel.

You can also use the last exit code to verify if the backup job has completed successfully. To check the last exit code, use the *%ERRORLEVEL%* variable in `cmd.exe`.

Veeam Agent for Microsoft Windows can provide the following exit codes:

- 0 — backup successfully created
- -1 — backup job failed to start or completed with error
- 5 — backup job is currently running and cannot be started from the command line interface

Deleting Backups

Backup files created with Veeam Agent for Microsoft Windows are removed automatically according to the retention policy settings.

If necessary, you can remove the backup files manually with a file manager, for example, Microsoft Windows Explorer. In this case, delete the whole backup chain from the target location. After you remove the whole backup chain from the target location, during the next backup job session, Veeam Agent for Microsoft Windows will produce a new full backup. All subsequent backups will be incremental.

> **IMPORTANT**
>
> Do not delete individual backup files from the backup chain. If you delete a full or incremental backup file, the chain will be broken. In this case, Veeam Agent for Microsoft Windows may fail to perform the scheduled backup next time.

Deleting Backups with Command Line Interface

You can use the command line interface to delete Veeam Agent backups from a Veeam Cloud Connect repository or object storage.

When you delete a backup from a Veeam Cloud Connect repository, Veeam Agent for Microsoft Windows deletes actual backup files from the repository and removes records about the backup from the Veeam Backup & Replication database on the SP backup server. After information about the backup is removed from the SP backup server, Veeam Backup & Replication removes this information from its database and console on the tenant backup server, too.

Before you delete a backup, check the following prerequisites:

- To perform the delete backup operation, you must run the command line interface with administrative privileges.
- The delete backup operation cannot be performed if a backup or a restore task is currently running.
- Check the following backup job settings:
  - The target location from which you want to delete a backup must be specified as a target location for backup files in the backup job settings.
  - Credentials of the user account whose backup you want to delete must be specified in the backup job settings.

  To learn more, see Veeam Cloud Connect Repository Settings and Object Storage Settings.

To delete a Veeam Agent backup, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /deleteback
up
```

> **TIP**
>
> If more than one backup job is configured, Veeam Agent for Microsoft Windows will provide a list of backup jobs. To delete a backup, type the number that is displayed next to the backup job whose backup you want to delete.

Veeam Agent for Microsoft Windows can provide the following exit codes:

- 0 — backup job was successfully deleted
- -1 — the delete backup job operation failed

Managing Backup Cache

You can perform the following operations with the backup cache:

- Monitor backup cache activity
- Pause backup cache synchronization
- Delete restore points from the backup cache

Monitoring Backup Cache Activity

You can use the Veeam Agent control panel to view information about backup cache activity. In the **Backup Cache** view, Veeam Agent for Microsoft Windows displays a list of restore points that were created in the backup cache, their status and size of the resulting backup file. For restore points that are being uploaded or have been already uploaded to the target location, Veeam Agent for Microsoft Windows also displays the upload speed.

Viewing Restore Points in Backup Cache

To view information about backup cache activity, open the **Backup Cache** view in one of the following ways:

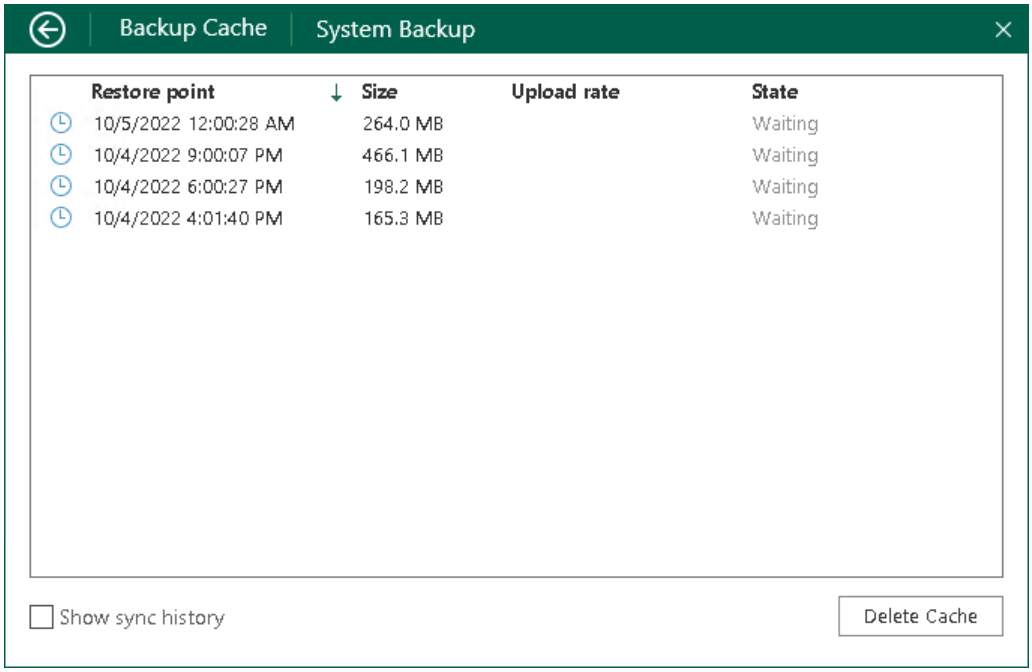
- If one backup job is configured:

  Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **View cache**. The Veeam Agent control panel will open, and you will pass immediately to the **Backup Cache** view.

  > **NOTE**
  >
  > The **View cache** option is not available in the system tray menu if more than one backup job is configured in Veeam Agent for Microsoft Windows.

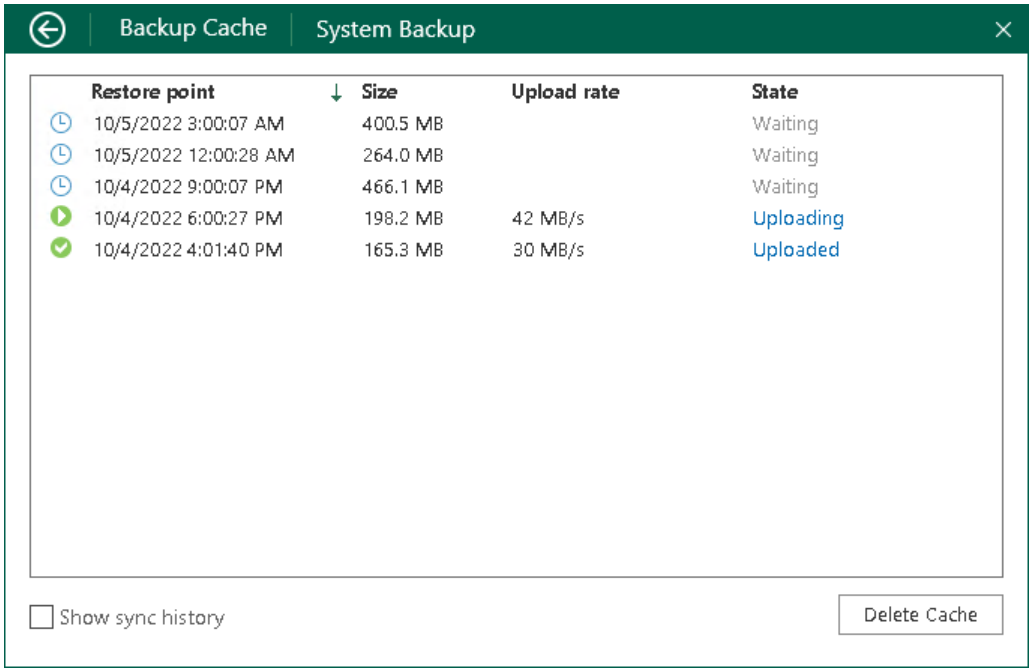
- If more than one backup job is configured:

  Double-click the Veeam Agent for Microsoft Windows icon, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**. In the main menu, hover over the name of the job that created restore points in the backup cache and select **Open backup cache**.



Viewing Backup Cache History

By default, the **Backup Cache** view contains a list of restore points that are waiting for upload or currently being uploaded to the target location. Restore points that have already been uploaded to the target location are not displayed in the list. To view such restore points, in the **Backup Cache** view, select the **Show sync history** check box.

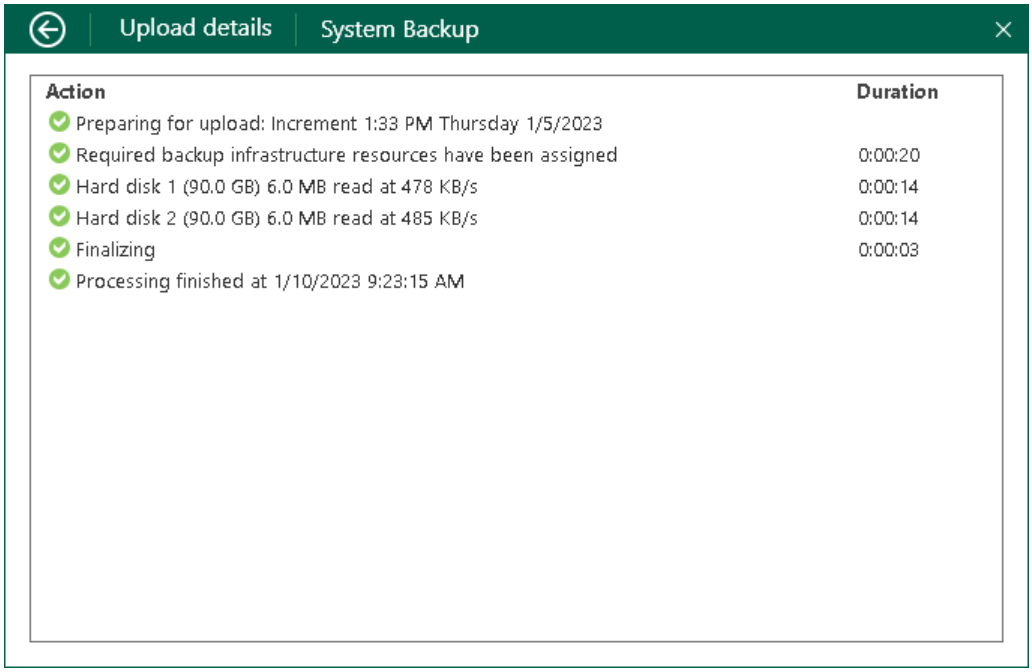


Viewing Upload Details for Restore Points

For every restore point that is being uploaded or has been uploaded to the target location, you can also view detailed information on the upload process:

1. Open the **Backup Cache** view in one of the following ways:
   - [If the backup cache is enabled in the properties of one job] Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **View cache**.
   - [If the backup cache is enabled in the properties of multiple jobs] Double-click the Veeam Agent for Microsoft Windows icon, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**. In the main menu, hover over the name of the job that created restore points in the backup cache and select **Open backup cache**.
2. In the **Backup Cache** view, click one of the following links next to the necessary restore point:
   - **Uploading** — for a restore point that is currently being uploaded to the target location.
   - **Uploaded** — for a restore point that has been already uploaded to the target location.

In the **Upload details** view, Veeam Agent for Microsoft Windows will provide detailed information about operations performed as part of the restore point upload process.


Upload details
System Backup
Action
Duration
Preparing for upload: Increment 1:33 PM Thursday 1/5/2023
Required backup infrastructure resources have been assigned
0:00:20
Hard disk 1 (90.0 GB) 6.0 MB read at 478 KB/s
0:00:14
Hard disk 2 (90.0 GB) 6.0 MB read at 485 KB/s
0:00:14
Finalizing
0:00:03
Processing finished at 1/10/2023 9:23:15 AM

Pausing Backup Cache Synchronization

After at least one restore point is created in the backup cache, Veeam Agent for Microsoft Windows starts monitoring availability of the target location. To perform this operation, Veeam Agent for Microsoft Windows starts the backup cache synchronization job that runs in the background.

The backup cache synchronization job can be paused automatically by Veeam Agent for Microsoft Windows or manually.

Veeam Agent pauses the backup cache synchronization job automatically in case Veeam Agent computer is put into sleep or hibernate mode during the job session, and the backup job is targeted at one of the following locations:

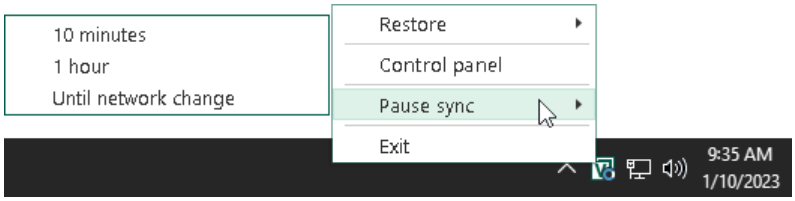
- Local computer drive
- Network shared folder

If the connection was lost during data transfer, Veeam Agent does not transfer all the data again. Instead, Veeam Agent continues data transfer that was started before the connection loss. After the connection is restored, Veeam Agent transfers only those data blocks that were not transferred before.

You can pause the backup cache synchronization job manually, for example, if you know that the target location will not become available for a while and want to reduce impact of Veeam Agent for Microsoft Windows on your OS performance.

To pause backup cache synchronization manually:

- Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
- Select one of the following options:
  - **Pause sync** > **10 minutes** — to pause backup cache synchronization for 10 minutes.
  - **Pause sync** > **1 hour** — to pause backup cache synchronization for 1 hour.
  - **Pause sync** > **Until network change** — to pause backup cache synchronization until new network settings are applied to the network adapter of the Veeam Agent computer.



Deleting Restore Points from Backup Cache

You can delete restore points from the backup cache manually if needed. For example, it is required to delete restore points after Veeam Agent for Microsoft Windows creates one or more restore points at the backup cache, and then you change the target location for backup files in the backup job settings.

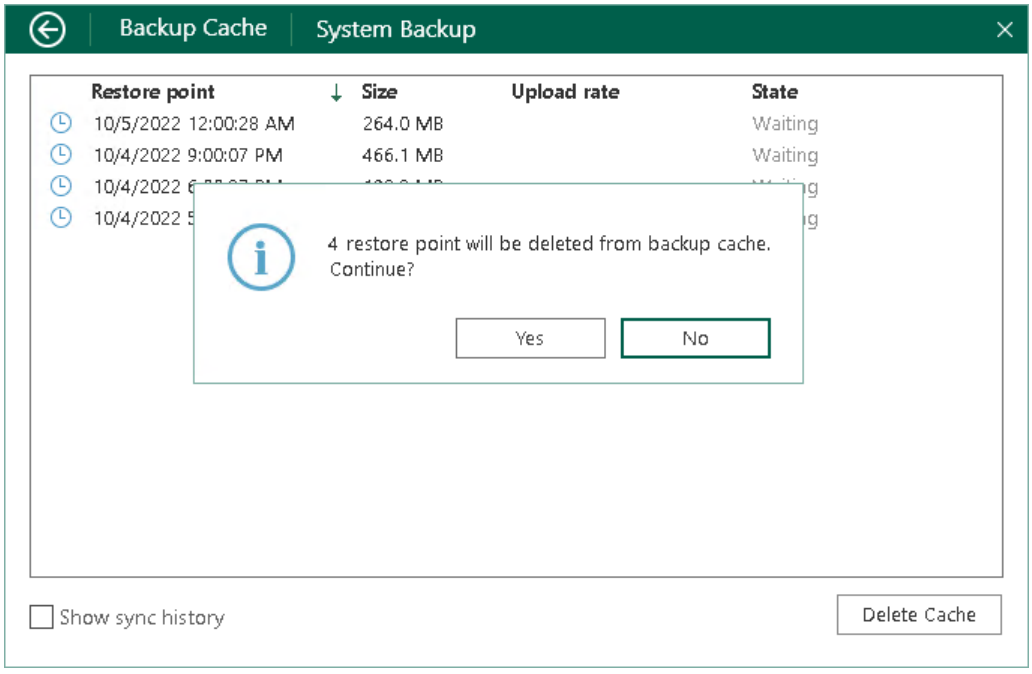
To delete restore points from the backup cache:

1. Open the **Backup Cache** view in one of the following ways:
   - [If the backup cache is enabled in the properties of one job] Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **View cache**.

     > **NOTE**
     >
     > The **View cache** option is not available in the system tray menu if the backup cache is enabled for more than one backup job configured in Veeam Agent for Microsoft Windows.

   - [If the backup cache is enabled in the properties of multiple jobs] Double-click the Veeam Agent for Microsoft Windows icon, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**. In the main menu, hover over the name of the job that created restore points in the backup cache and select **Open backup cache**.
2. In the **Backup Cache** view, click **Delete Cache**.
3. In the window notifying that restore points will be deleted from the backup cache, click **Yes**.

> **NOTE**
>
> The first backup job session following the deletion of restore points from the backup cache must complete successfully and create backup files on the target location. During this session, Veeam Agent for Microsoft Windows will create a new map of target location data blocks in the backup cache. If you delete restore points from the backup cache, and then run the backup job when the target location is unavailable, the backup job will fail.



Performing Restore

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

- Restoring from Veeam Recovery Media
- Using Veeam Agent and Microsoft Windows Tools
- Using Microsoft Windows Recovery Environment
- Restoring Volumes
- Restoring Files and Folders
- Restoring Data from Encrypted Backups

Restoring from Veeam Recovery Media

If the OS on your computer fails to start, you can use the Veeam Recovery Media to recover your computer. The Veeam Recovery Media will help you boot the computer in the limited mode. After booting, you can use Veeam Agent for Microsoft Windows or standard Microsoft Windows tools to diagnose problems and fix errors. You can also use a backup created with Veeam Agent for Microsoft Windows to restore the whole system image of your computer or specific volumes on your computer.

Before You Begin

Before you boot from the recovery image and recover your data, check the following prerequisites:

- You must have a successfully created recovery image on any type of media: CD/DVD/BD or removable storage device.
- To recover data on your computer, you must have both the Veeam Recovery Media and data backup. For data recovery, you can use a volume-level backup created with Veeam Agent for Microsoft Windows or system image created with Microsoft Windows. Make sure that the backup or system image is available on the computer drive (local or external), in object storage, in a network shared folder, in the backup repository managed by a Veeam backup server or in the cloud repository.

  > **NOTE**
  >
  > For a backup created by a backup copy job, you can perform bare metal restore if the backup is stored in the Veeam backup repository. For more information about backup copy jobs, see Performing Backup Copy for Veeam Agent Backups.

- The media type on which you have created the recovery image must be set as a primary boot source on your computer.
- Recovery images for Microsoft Windows 32-bit OSes can be booted in the BIOS system only. Recovery images for Microsoft Windows 64-bit OSes can be booted in the BIOS and UEFI systems.

Consider the following:

- When you create a Veeam Recovery Media, Veeam Agent for Microsoft Windows stores settings for languages added to the list of input languages on your computer. If necessary, you can switch between languages using a hotkey combination when working with the **Veeam Recovery Media** wizard. The default key combination is typically **[Shift]** + **[Alt]**.
- NIC Teaming is not supported by Veeam Recovery Media due to Windows Recovery Environment limitations. To avoid network connection issues in Veeam Recovery Media, we recommend to disable NIC Teaming in the network switch configuration.
- You can open the Command Prompt at any moment. To do this, press **[Shift]** + **[F10]** on the keyboard.
- If you perform restore on a tablet, you can use a virtual keyboard to enter necessary restore settings in the **Veeam Recovery Media** wizard.

Step 1. Boot from Veeam Recovery Media

To boot from the Veeam Recovery Media:

1. [For CD/DVD/BD] Power on your computer. Insert the media with the recovery image to the drive and power off the computer.

   [For removable storage device] Attach the removable storage device with the recovery image to your computer.

2. Start your computer.
3. You will be offered to boot the OS from the CD/DVD/BD or attached removable storage. Press any key on the keyboard to continue.
4. Wait for Veeam Agent for Microsoft Windows to load files from the Veeam Recovery Media. Loading the OS from the Veeam Recovery Media usually takes more time than loading the OS from the local computer drive.
5. After the OS has loaded, make sure network settings are specified correctly and configure network if necessary. To learn more, see Select Network Adapter or Wireless Network.
6. Choose the necessary recovery tool to use. Veeam Agent for Microsoft Windows offers the following tools:
   - Bare Metal Recovery — the Veeam Recovery Media wizard to recover data on the original computer or perform bare metal recovery.
   - Windows Recovery Environment — built-in Microsoft Windows tools to recover the computer system image.
   - Tools — Veeam Agent for Microsoft Windows and Microsoft Windows utilities for advanced computer administration.

> **TIP**
>
> Consider the following:
>
> - To shut down or restart your computer, click the **Power Options** button at the bottom right corner of the Veeam Recovery Media screen and select the necessary option: **Shut down** or **Restart**.
> - You can use the Veeam Recovery Media to start the Microsoft Windows OS in the safe mode. To do this, click the **Power Options** button at the bottom right corner of the Veeam Recovery Media screen and select **Boot in safe mode**. In the displayed window, select the necessary safe boot mode (*Minimal*, *Network* or *Repair*), and click **OK**.


Veeam Recovery Media 6.1.0
Created from Microsoft Windows Server 2019 (1809, 64-bit)
Bare Metal Recovery
Restore Veeam Agent for Windows backup to the original or a new computer.
Windows Recovery Environment
Launch Microsoft Windows system image recovery environment.
Tools
Browse tools for system management and diagnostics.

Step 2. Select Network Adapter or Wireless Network

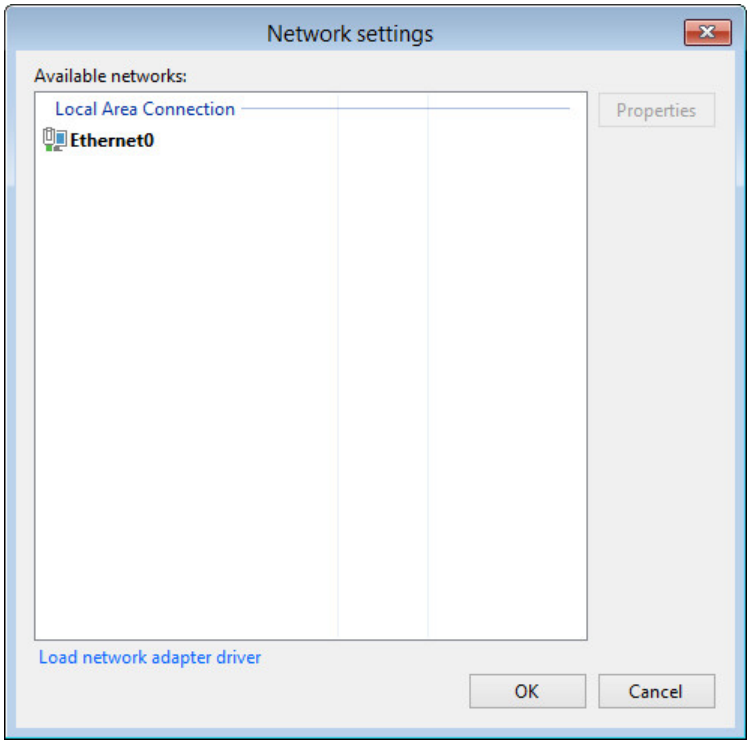
To open the **Network settings** window, click the **Network Settings** button at the bottom right corner of the **Veeam Recovery Media** screen.

> **TIP**
>
> The *Network Settings* button appearance may vary depending on the detected network connection: Ethernet or wireless. If your computer is connected to a wireless network, the *Network Settings* button will indicate Wi-Fi signal strength.

Select a network adapter or wireless network that you want to use to connect to the network shared folder or Veeam backup repository where the backup resides.

- If network connection settings are included in the Veeam Recovery Media, or if there is a DHCP server in your network, Veeam Agent for Microsoft Windows will configure the network settings automatically and display available network adapters in the list.
- If you want to access the network shared folder or Veeam backup repository using a wireless network, select the necessary network in the list and click **Next**. If the wireless network is password protected, you will be prompted to specify a password for this network.
- You can manually configure TPC/IP v4 settings for adapters if necessary. To do this, select an adapter in the list and click **Properties**.

> **NOTE**
>
> You will be prompted to configure network settings manually if Veeam Agent for Microsoft Windows does not detect available networks and there are no network settings included in the Veeam Recovery Media.



Installing Network Adapter Drivers

The list of networks can be empty. This can happen in two situations:

- The driver for the network adapter is included in the Veeam Recovery Media but failed to be installed automatically for some reason.
- The driver for the network adapter is not included in the Veeam Recovery Media.

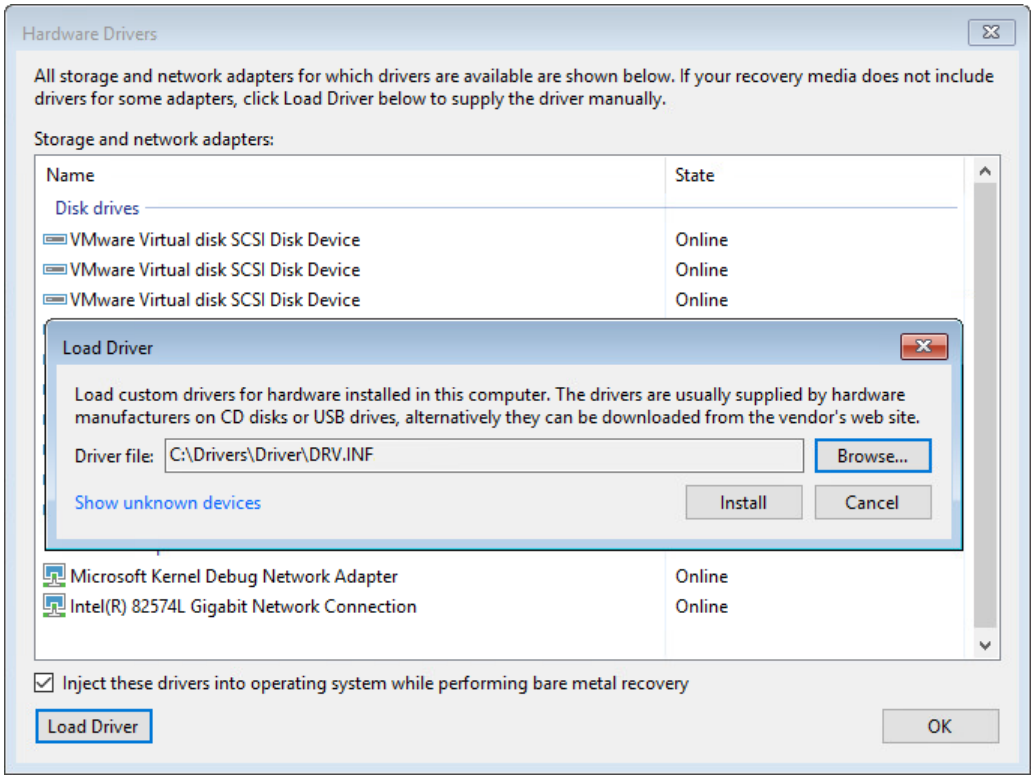
To install drivers that were included in the Veeam Recovery Media:

1. At the **Network settings** window, click Load network adapter driver.
2. In the **Hardware Drivers** window, select the necessary device.

   If you want to include in the restored operating system all the drivers that were saved to the Veeam Recovery Media, select the **Inject these drivers into operating system while performing bare metal recovery** option. In case the option is not selected, the restored operating system will include only default Windows hardware drivers.
3. Click the **Install** link next to the selected device.

To install drivers that were not included in the Veeam Recovery Media:

1. At the **Network settings** window, click **Load network adapter driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the **Show unknown devices** link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.



Step 3. Launch Veeam Recovery Media Wizard

To launch the Veeam Recovery Media wizard, on the Veeam Recovery Media screen, click Bare Metal Recovery.

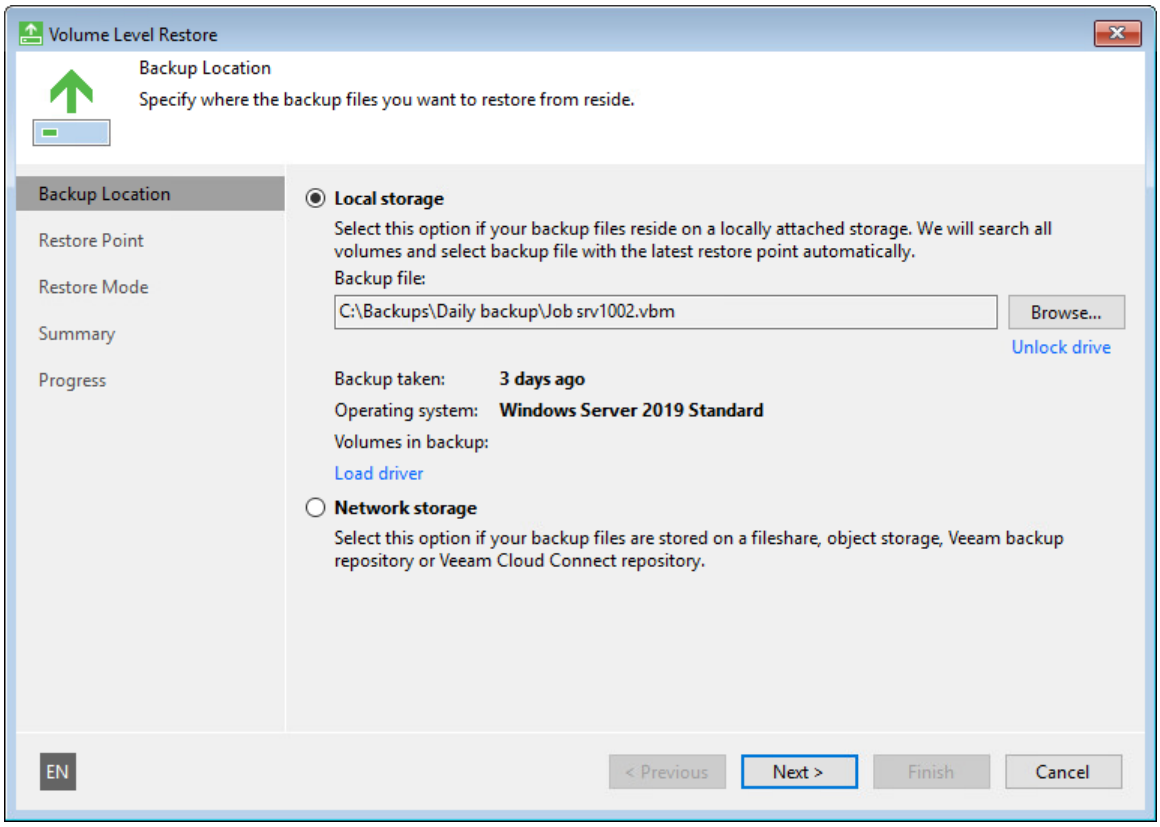


Step 4. Specify Backup File Location

At the **Backup Location** step of the wizard, specify where the backup file that you want to use for data recovery is located.

By default, Veeam Agent for Microsoft Windows automatically locates the latest backup on the computer drive and you pass immediately to the Restore Point step of the wizard. If Veeam Agent for Microsoft Windows fails to locate the backup on the local computer drive for some reason, or the backup file is located in object storage, in a network shared folder, in a backup repository or cloud repository, select where the backup file resides:

- **Local storage** — select this option if the backup file resides on the local computer drive, external drive or removable storage device that is currently connected to your computer. Click **Browse** and select a backup metadata file (VBM).
- **Network storage** — select this option if the backup file resides in object storage, in a network shared folder, in a backup repository managed by a Veeam backup server or in a cloud repository exposed to you by a Veeam Cloud Connect service provider. In this case, the Veeam Recovery Media wizard will include additional steps for specifying the backup file location settings.



Installing Drivers for Remote Storage Devices

A removable storage device with the backup file may not be displayed in the list of devices. This can happen in two situations:

- The driver for the remote storage device is included in the Veeam Recovery Media but failed to be installed automatically for some reason.
- The driver for the remote storage device is not included in the Veeam Recovery Media.

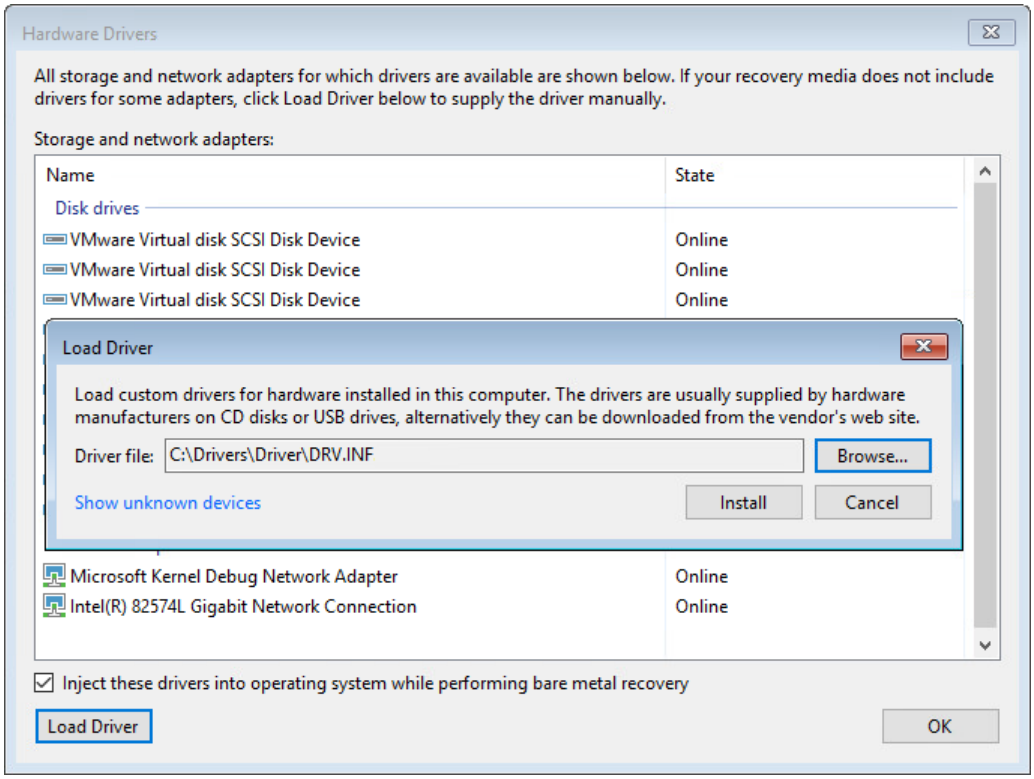
To install drivers that were included in the Veeam Recovery Media:

1. At the **Backup Location** step of the wizard, click **Load driver**.
2. In the **Hardware Drivers** window, select the necessary device.

   If you want to include in the restored operating system all the drivers that were saved to the Veeam Recovery Media, select the **Inject these drivers into operating system while performing bare metal recovery** option. In case the option is not selected, the restored operating system will include only default Windows hardware drivers.
3. Click the **Install** link next to the selected device.

To install drivers that were not included in the Veeam Recovery Media:

1. At the **Backup Location** step of the wizard, click **Load driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the **Show unknown devices** link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.

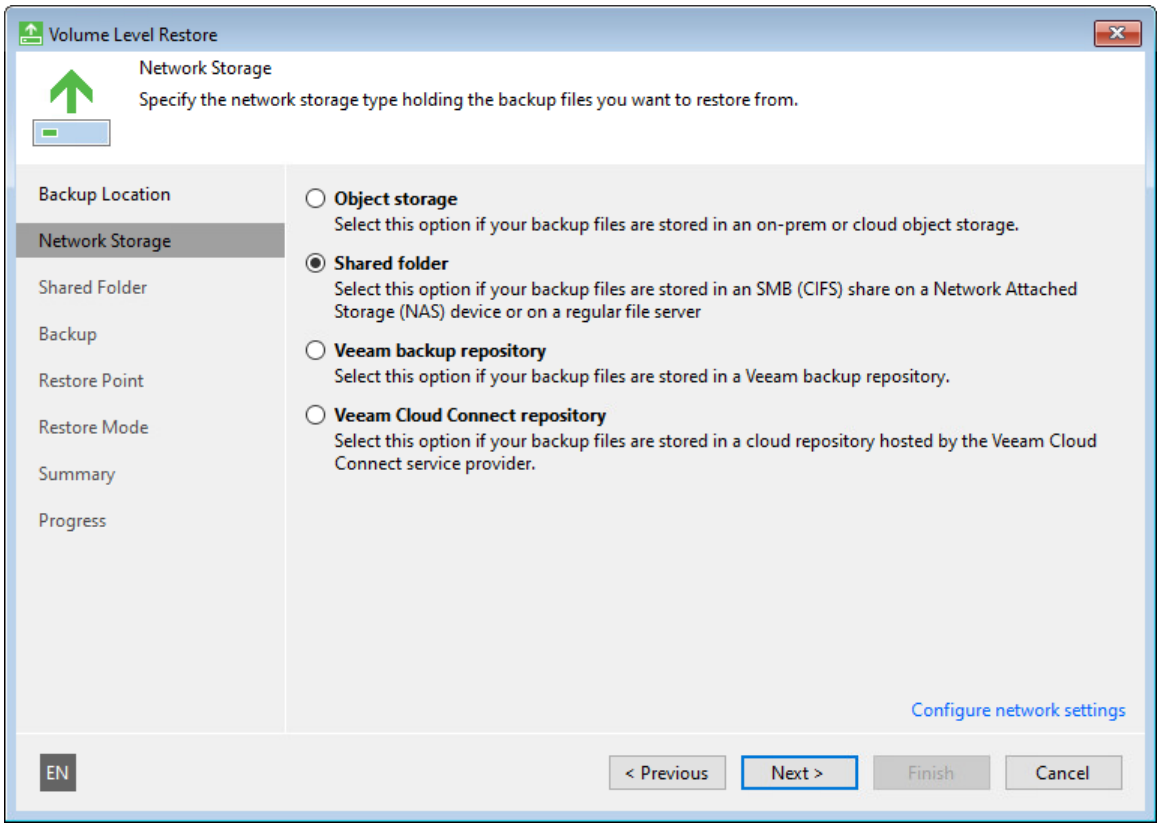


Step 5. Select Network Storage Type

The **Network Storage** step of the wizard is available if you have selected to restore data from a backup file that resides in a remote location — in object storage, in a network shared folder, in a backup repository or in a cloud repository.

Select where the backup file resides:

- **Object storage** — select this option if the backup file resides in object storage. With this option selected, you will pass to the Object Storage step of the wizard.
- **Shared folder** — select this option if the backup file resides in a network shared folder. With this option selected, you will pass to the Shared Folder step of the wizard.
- **Veeam backup repository** — select this option if the backup file resides in a backup repository managed by a 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 the backup file resides in a cloud repository exposed to you by a Veeam Cloud Connect service provider. With this option selected, you will pass to the Service Provider step of the wizard.



Step 6. Specify Network Storage Settings

Specify settings for the remote storage that contains a backup file from which you plan to restore data:

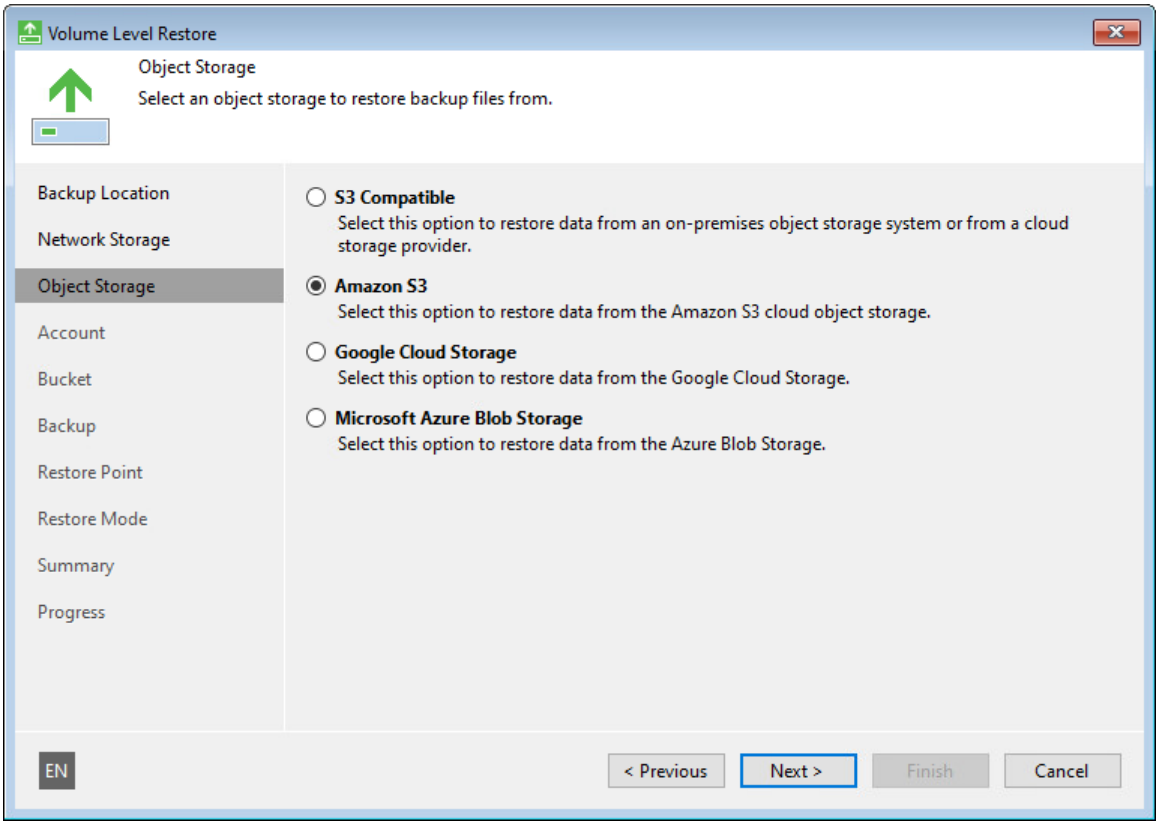
- Shared folder settings — if you have selected the **Shared folder** option at the Network Storage step of the wizard.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Network Storage step of the wizard.
- Veeam Cloud Connect repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Network Storage step of the wizard.

Object Storage Settings

The **Object Storage** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

Specify settings for the object storage:

- Specify S3 compatible settings.
- Specify Amazon S3 settings.
- Specify Google Cloud Storage settings.
- Specify Microsoft Azure Blob Storage settings.



S3 Compatible Settings

If you have selected to restore data from a backup file located in the S3 compatible storage, specify the following settings:

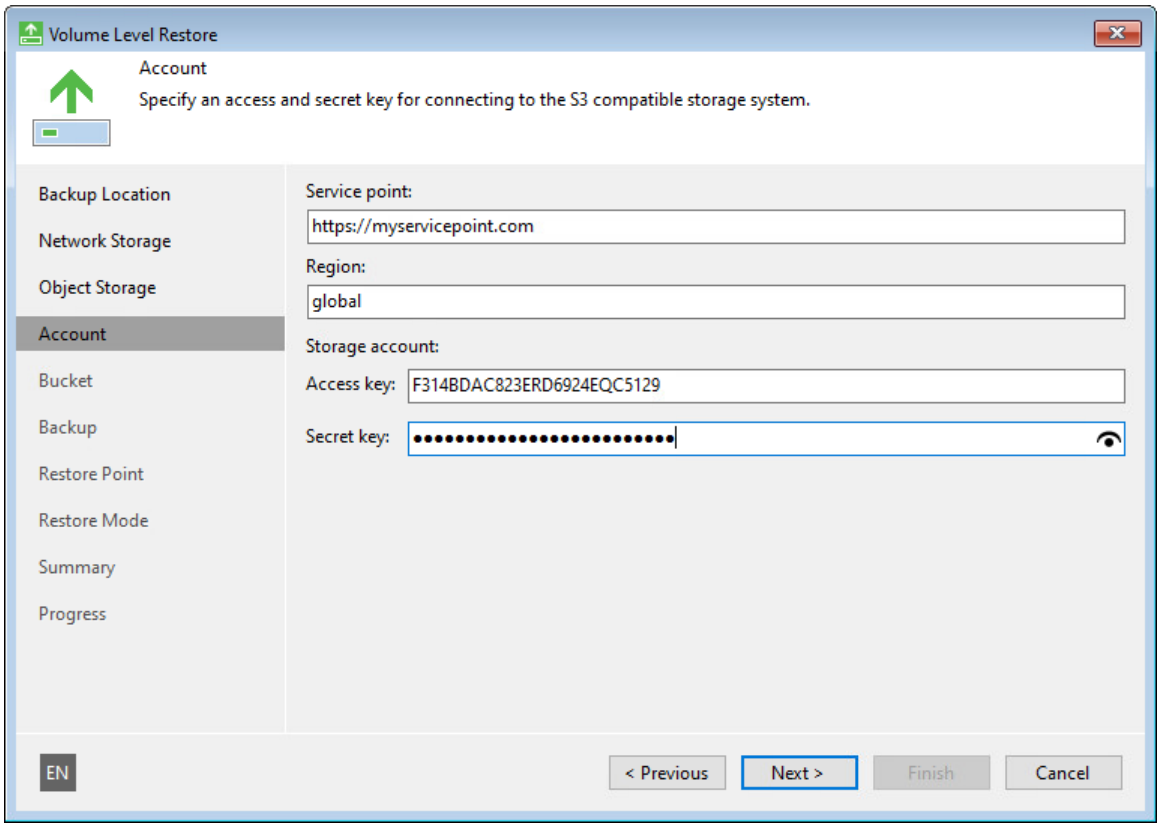
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Service point** field, specify the address of your S3 compatible storage.
2. In the **Region** field, specify the storage region.
3. In the **Access key** field, enter the access key ID.
4. In the **Secret key** field, enter the secret access key.

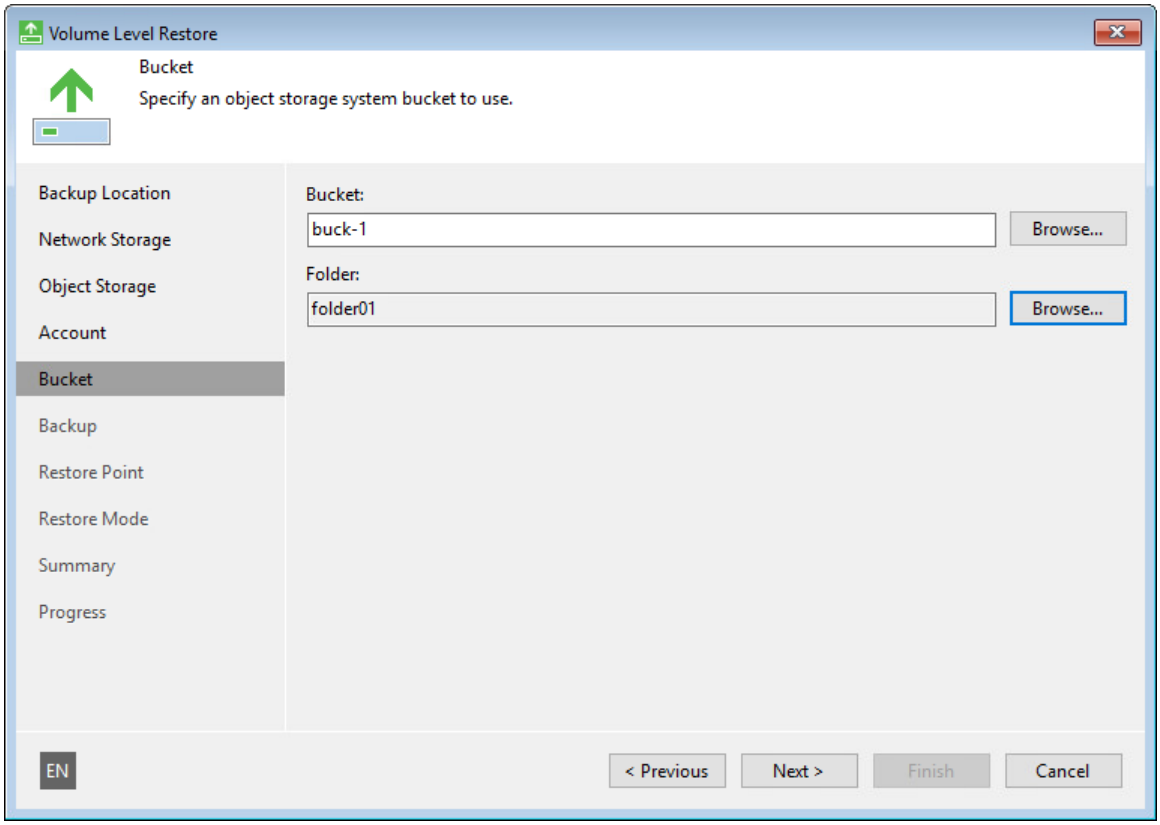


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



Amazon S3 Settings

If you have selected to restore data from a backup file located in the Amazon S3 storage, specify the following settings:

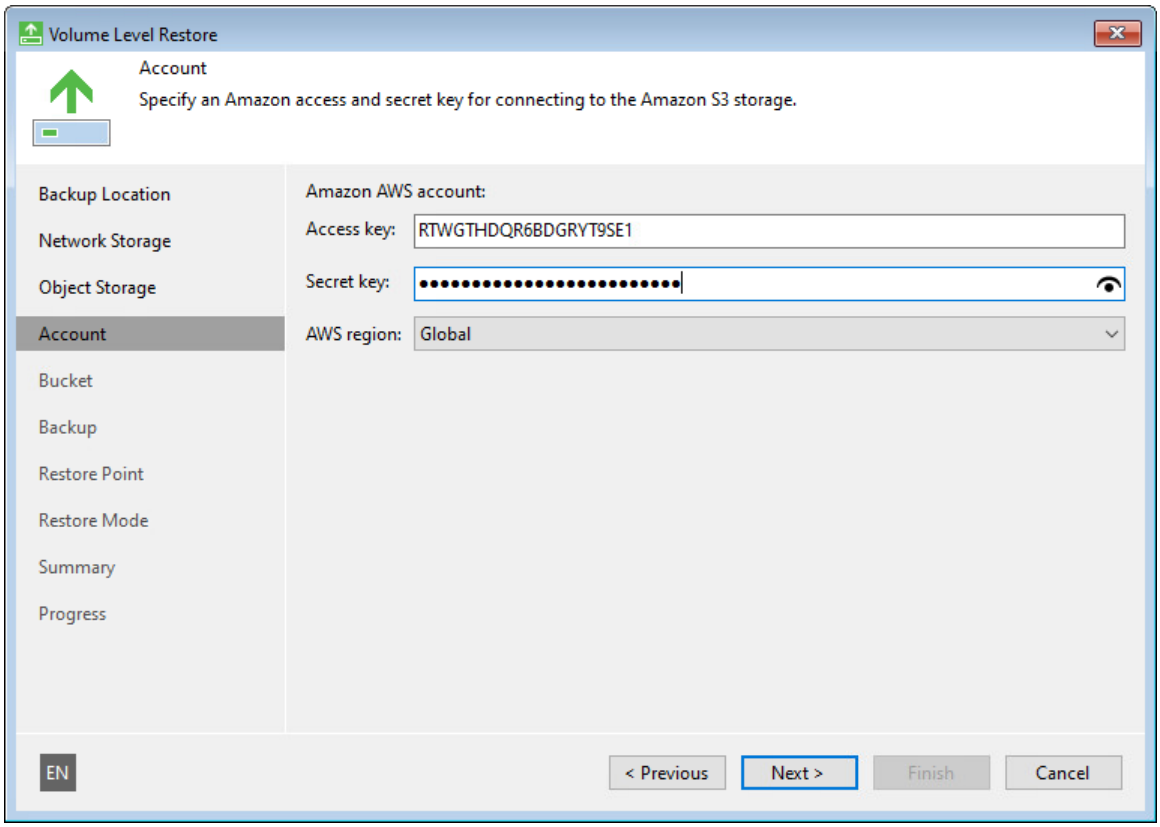
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Access key** field, enter the access key ID.
2. In the **Secret key** field, enter the secret access key.
3. From the **AWS region** drop-down list, select the AWS region. By default, Veeam Agent uses the **Global** region.

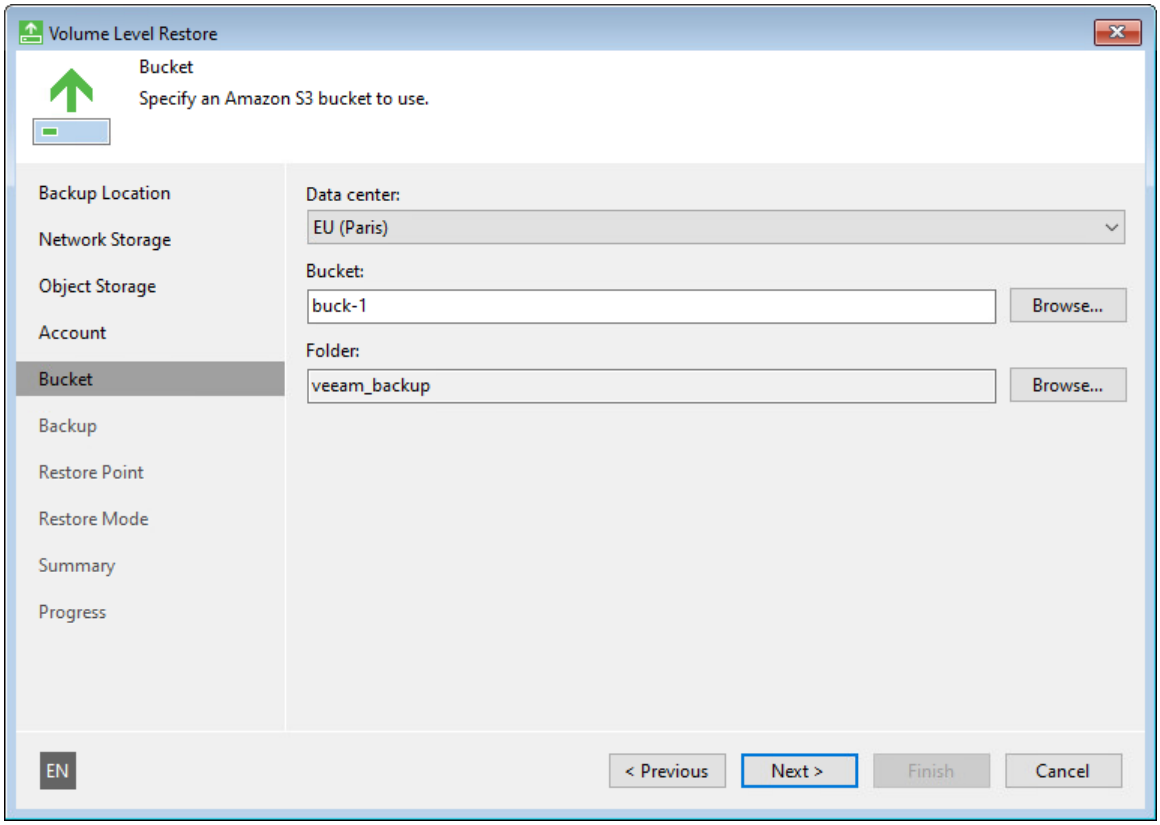


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.



Google Cloud Storage Settings

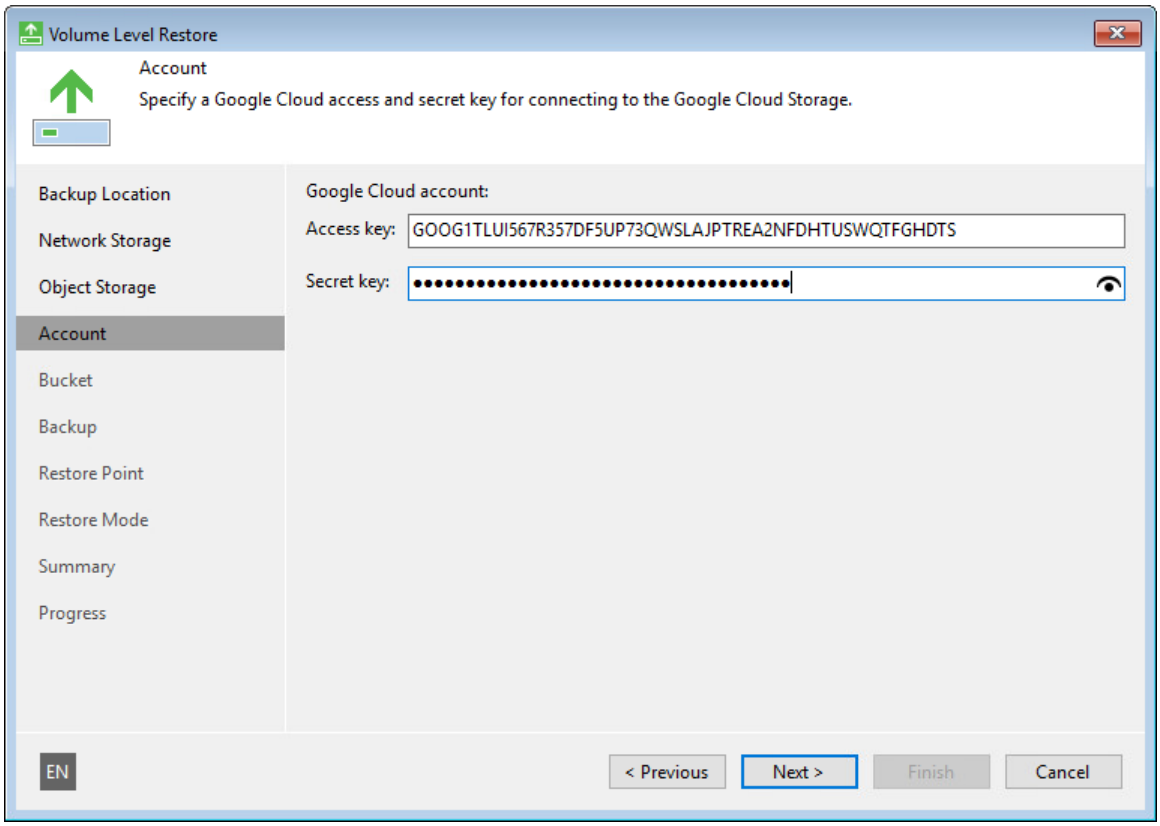
If you have selected to restore data from a backup file located in the Google Cloud storage, specify the following settings:

1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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



Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center region** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
   a. Select the **Browse** option.

b. In the **Select Bucket** window, do the following:

i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.

ii. Select the necessary bucket and click **OK**.

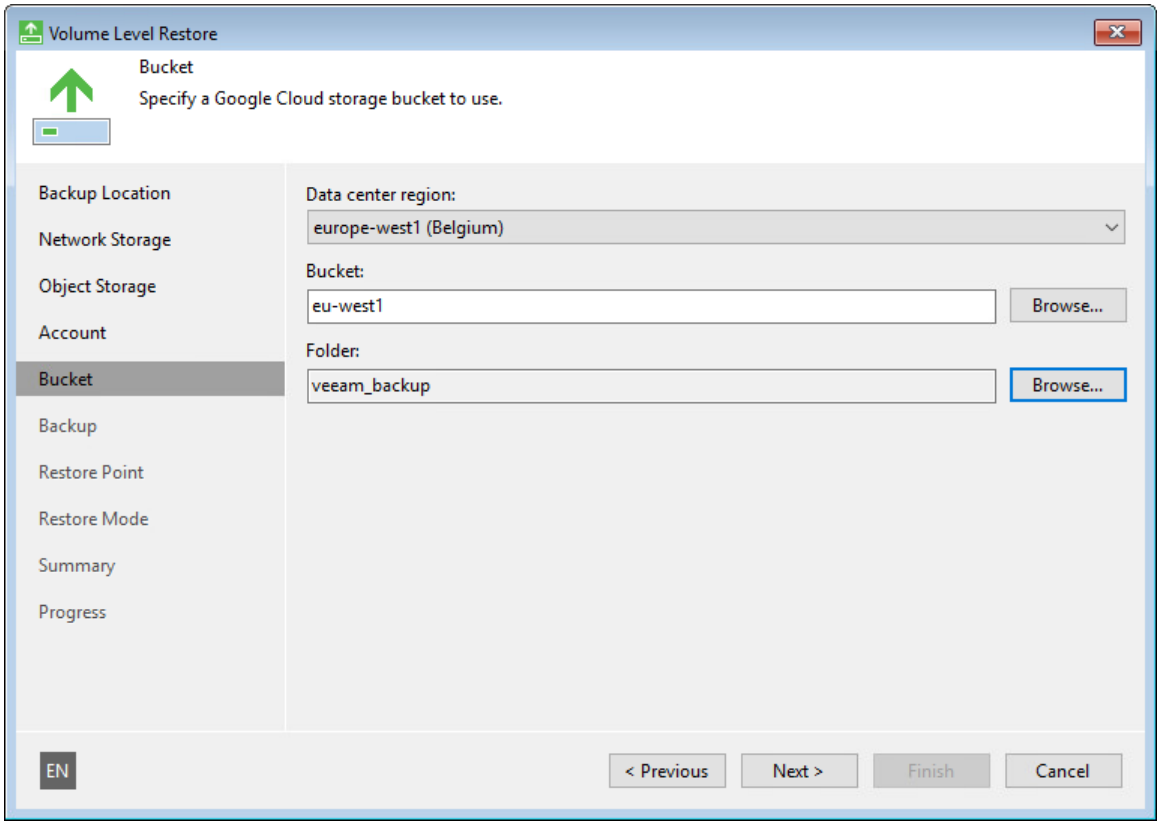
3. In the **Folder** field, specify a folder in the bucket:

a. Select the **Browse** option.

b. In the **Select Folder** window, do the following:

i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.

ii. Select the necessary folder and click **OK**.



Microsoft Azure Blob Storage Settings

If you have selected to restore data from a backup file located in the Microsoft Azure Blob storage, specify the following settings:

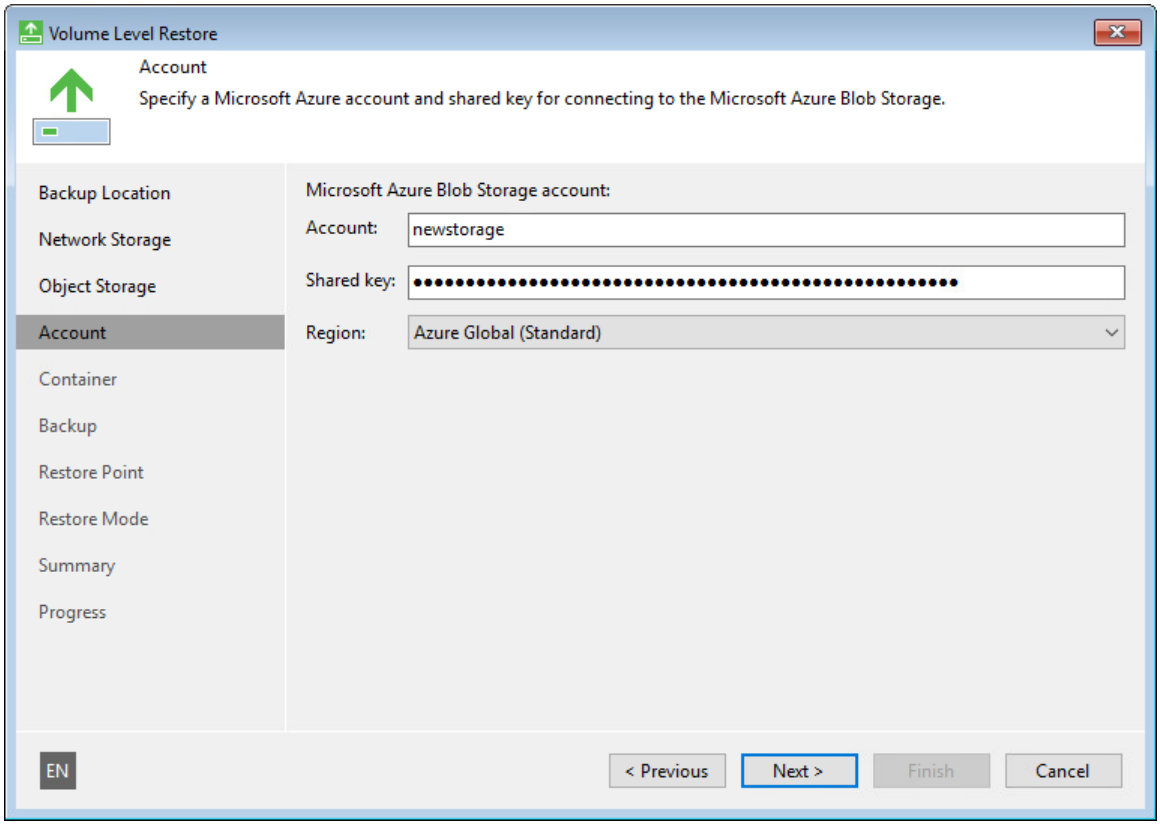
1. Specify account settings.
2. Specify container settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

To connect to the Microsoft Azure Blob 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. From the **Region** drop-down list, select the Microsoft Azure region. By default, Veeam Agent uses the **Azure Global (Standard)** region.

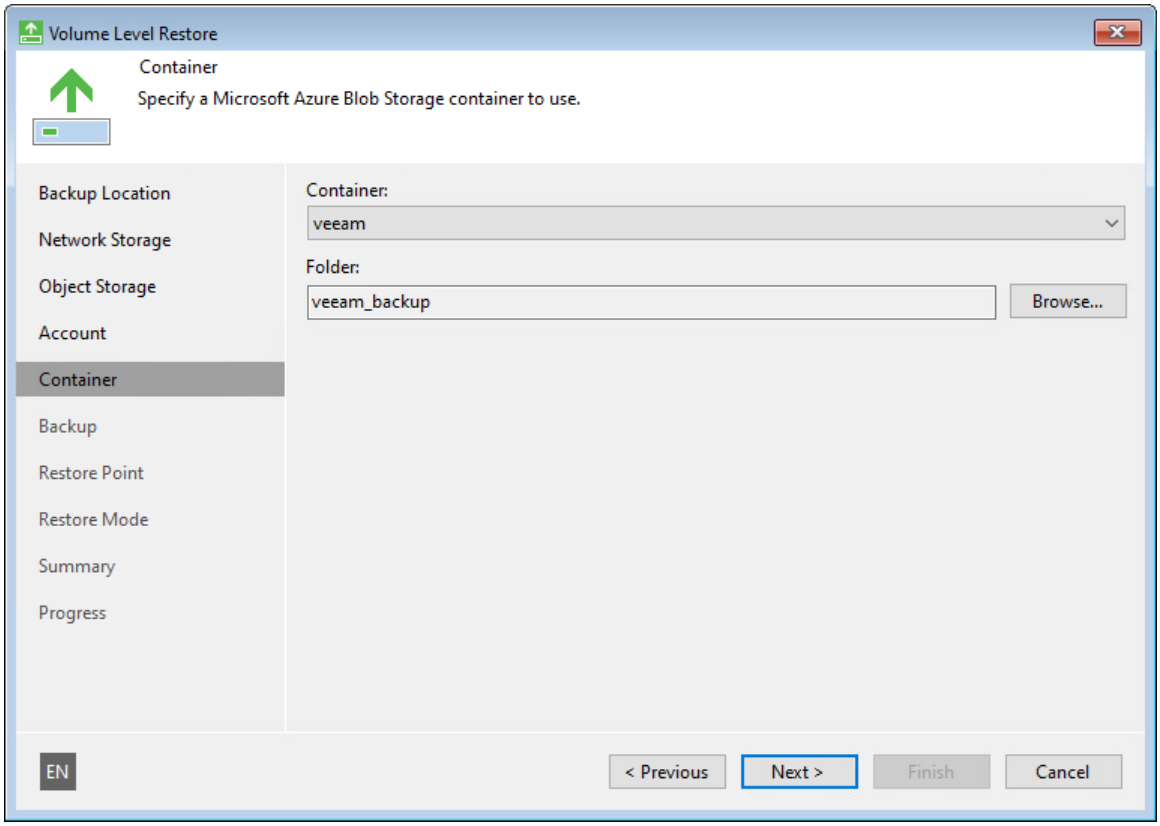


Specifying Container Settings

The **Container** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft Azure Blob storage and specified account settings to connect to the storage.

Specify settings for the container in the storage:

1. From the **Container** drop-down list, select a container in the storage.
2. In the **Folder** field, specify a folder in the container:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the container name or click the arrow to the left of the container name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



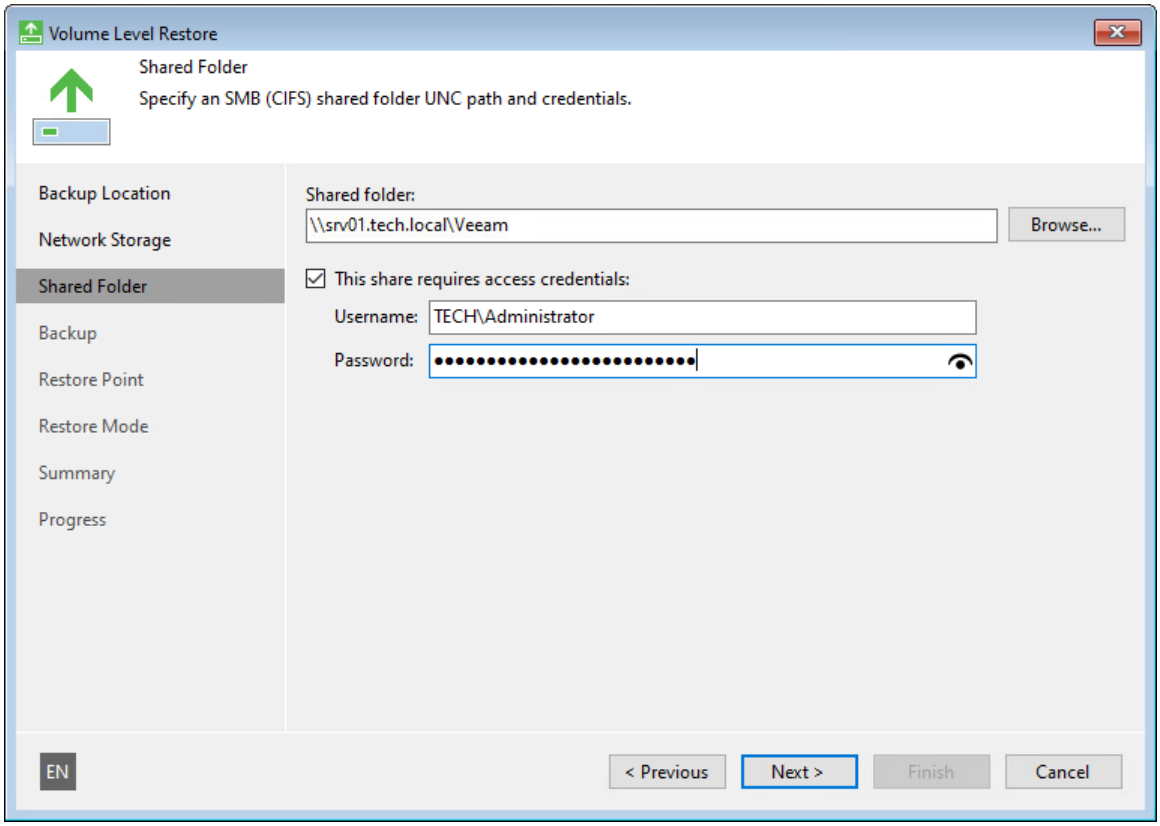
Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have selected to restore data from a backup file located in a network shared folder.

Specify settings for the network shared folder:

1. In the **Shared folder** field, enter a UNC name of the network shared folder with a backup file. Keep in mind that the UNC name always starts with two back slashes (\\).
2. If the network shared folder requires authentication, select the **This share requires access credentials** check box and specify a user name and password of the account that has *Full Control* access permissions on this shared folder. The user name must be specified in the down-level logon name format. For example, *DOMAIN*|*UserName* or *HOSTNAME*|*UserName*.

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



Backup Server Settings

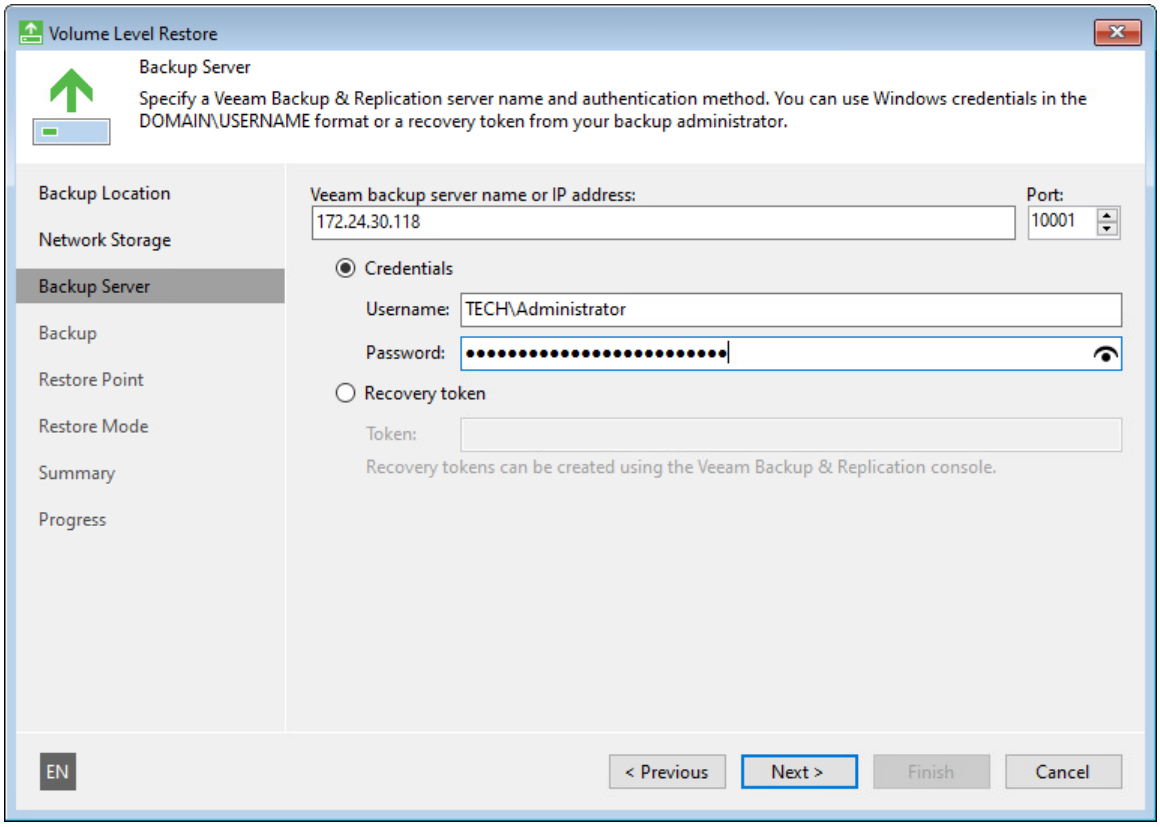
The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located in a backup repository.

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

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup server. By default, Veeam Agent for Microsoft Windows uses port 10001.
3. Select one of the following authentication methods to access the Veeam backup repository:
   - **Credentials** — in the **Username** and **Password** fields, enter a user name and password of the account that has access to this backup repository.

     Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

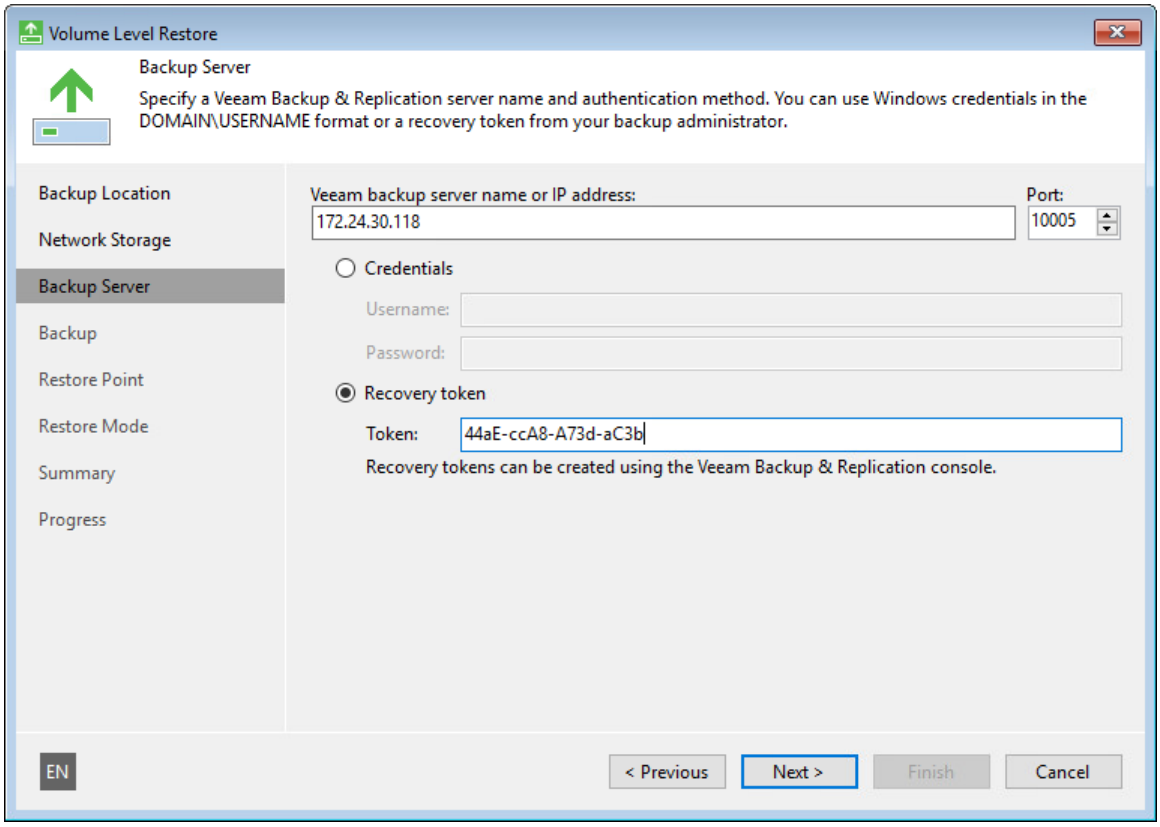
     > **NOTE**
     >
     > If you want to perform bare metal restore from a backup created by Veeam Agent operating in the managed mode and stored in the Veeam backup repository, you must use an account that has the Veeam Backup Administrator or Veeam Restore Operator role on the Veeam backup server. For more information about user roles, see the Users and Roles section in the Veeam Backup & Replication User Guide.



- **Recovery token** — in the **Token** field, enter the recovery token created on the Veeam Backup & Replication side.

  The recovery token must be created beforehand. To learn more, see the Creating Recovery Token section in the Veeam Agent Management Guide.

  After you click **Next**, you will be prompted to check the Veeam backup server certificate. Click **View Certificate** to check the certificate. Click **Continue** to connect to the Veeam backup server.



After you click **Next**, you will be prompted to check the Veeam backup server certificate. Click **View Certificate** to check the certificate. Click **Continue** to connect to the Veeam backup server.

Service Provider Settings

If you have selected to restore data from a backup file located in a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

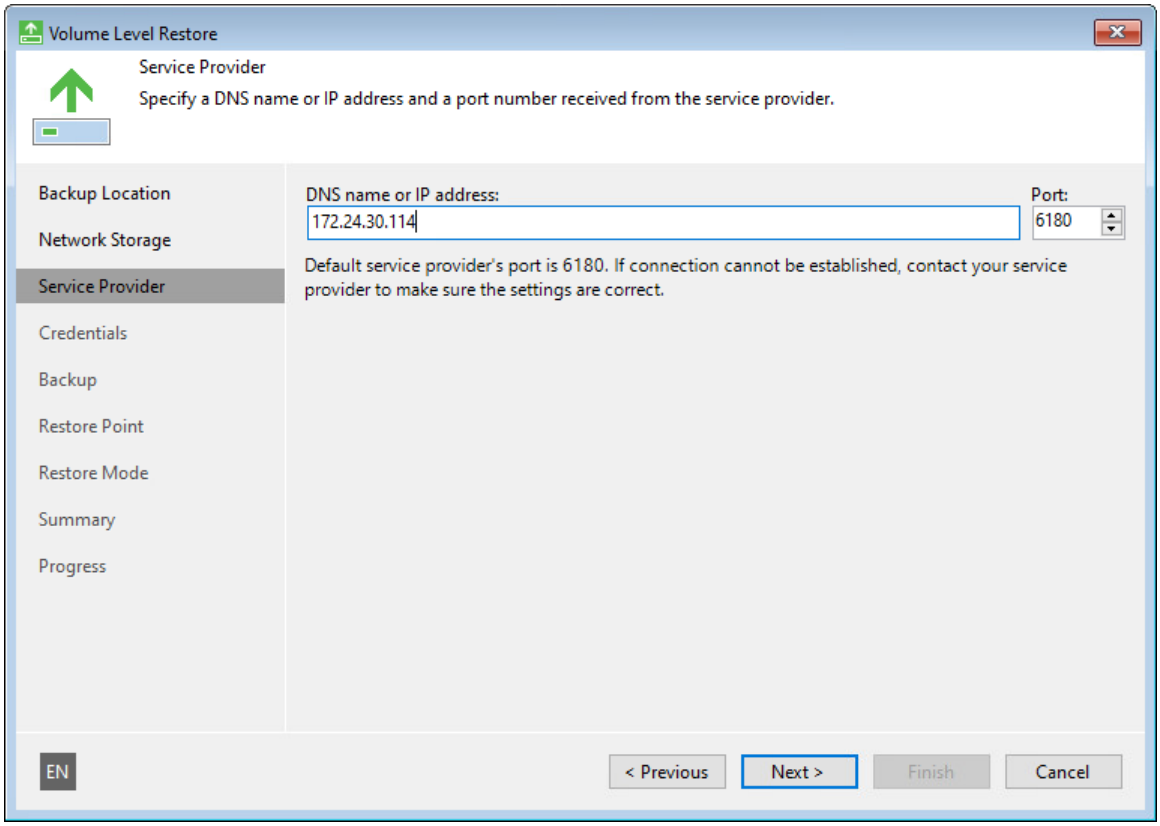
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

Specifying Service Provider Settings

The **Service provider** step of the wizard is available if you have chosen to restore data from a cloud repository exposed to you by a Veeam Cloud Connect service provider.

Specify service provider settings that the 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 for Microsoft Windows will communicate with the cloud gateway. By default, port 6180 is used.



Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to restore data from a cloud repository and specified settings for the cloud gateway.

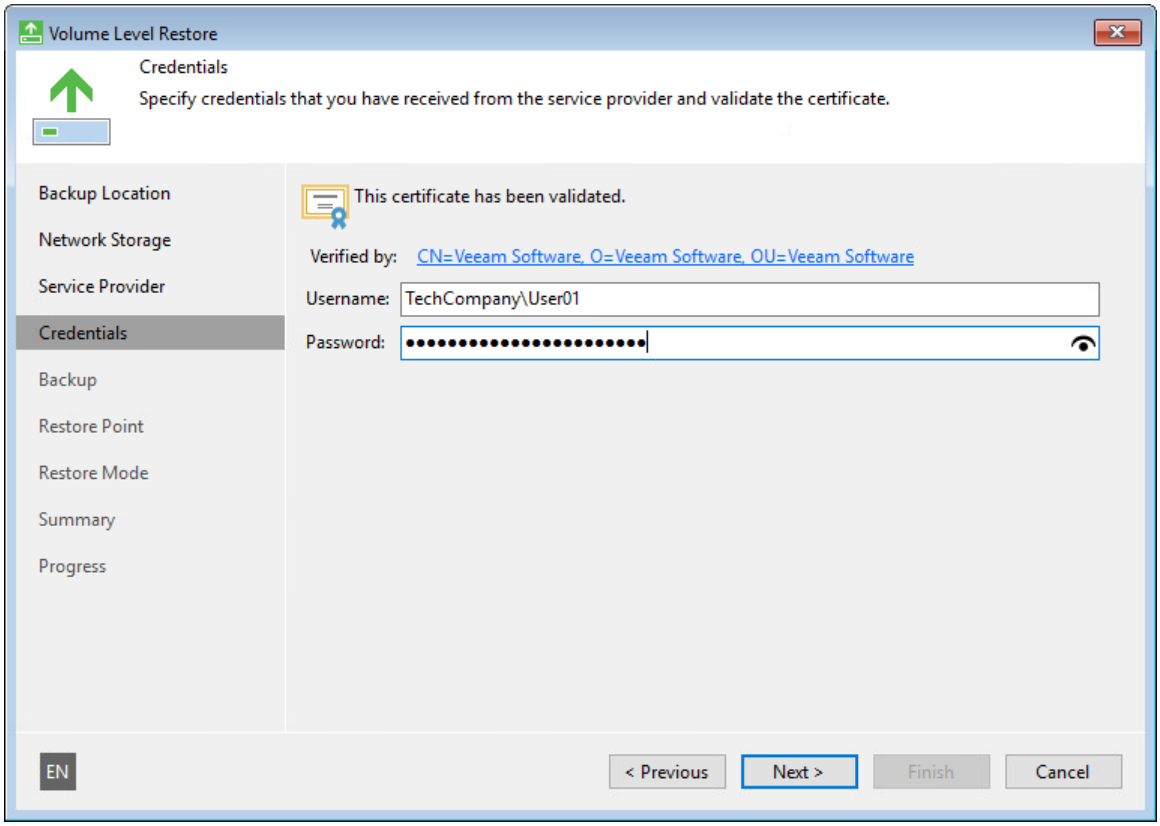
Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the service provider.

1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   - To view the TLS certificate, click the certificate link.
   - To verify if the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Fingerprint for certificate verification** field. Click **Verify**. Veeam Agent for Microsoft Windows will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. In the **Username** field, enter the user name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The user name of the subtenant account must be specified in the *TENANT\SUBTENANT* format.
3. In the **Password** field, provide a password for the tenant or subtenant account.


Volume Level Restore
Credentials
Specify credentials that you have received from the service provider and validate the certificate.
Backup Location
Network Storage
Service Provider
Credentials
Backup
Restore Point
Restore Mode
Summary
Progress
This certificate has been validated.
Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software
Username: TechCompany\User01
Password:
EN
< Previous
Next >
Finish
Cancel

Step 7. Select Backup

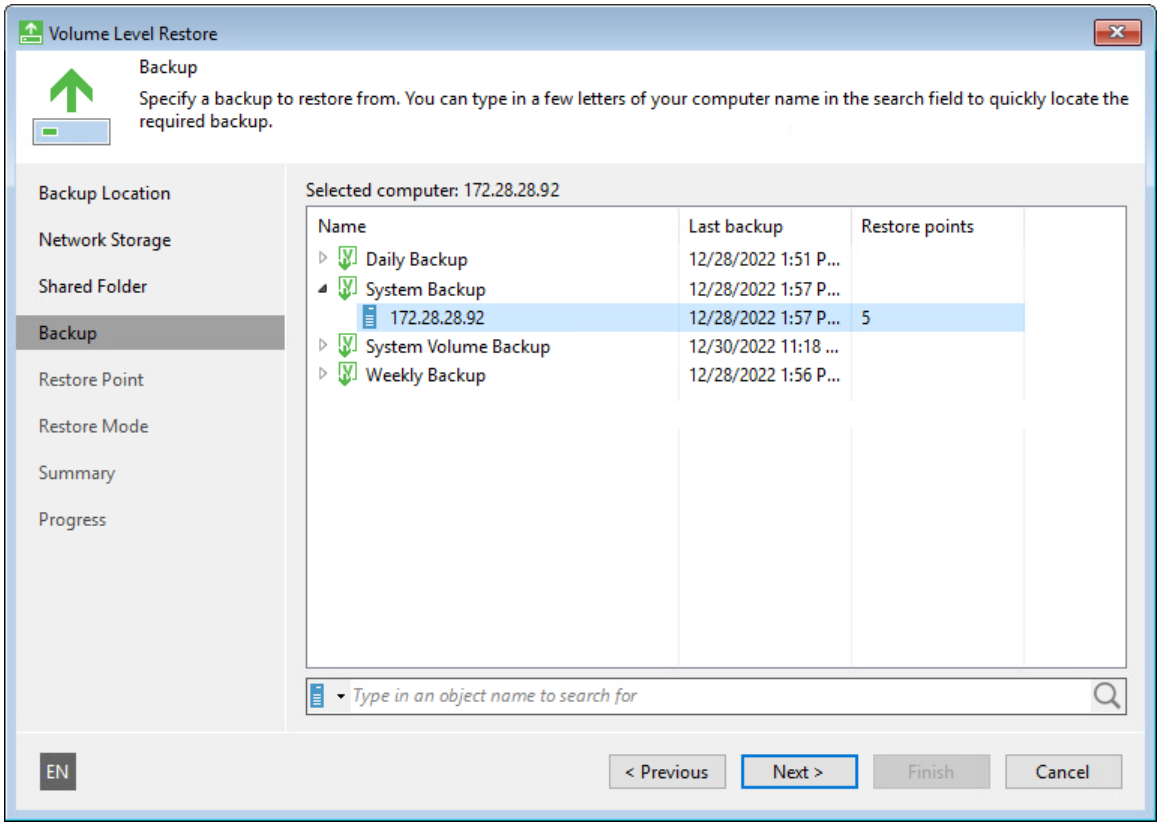
The **Backup** step of the wizard is available if you have chosen to restore data from a backup file that resides in a remote location — in object storage, in a network shared folder, in a Veeam backup repository or Veeam Cloud Connect repository.

From the list of backups, select a backup from which you want to recover data. To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

In the list of backups, Veeam Agent for Microsoft Windows displays only those backups that meet the following criteria:

1. Backups created at the volume level. File-level backups are not displayed.
2. [For backup repository target] Backups 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 Backup Administrator on the backup server, the list of backups will include all Veeam Agent backups stored in the backup repository.
3. [For cloud repository target] Backups 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 tenant account and its subtenant accounts.
   - 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 want to restore data from an encrypted backup, and the Veeam Recovery Media from which you booted your computer does not contain encryption keys required to unlock the backup file, you need to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.

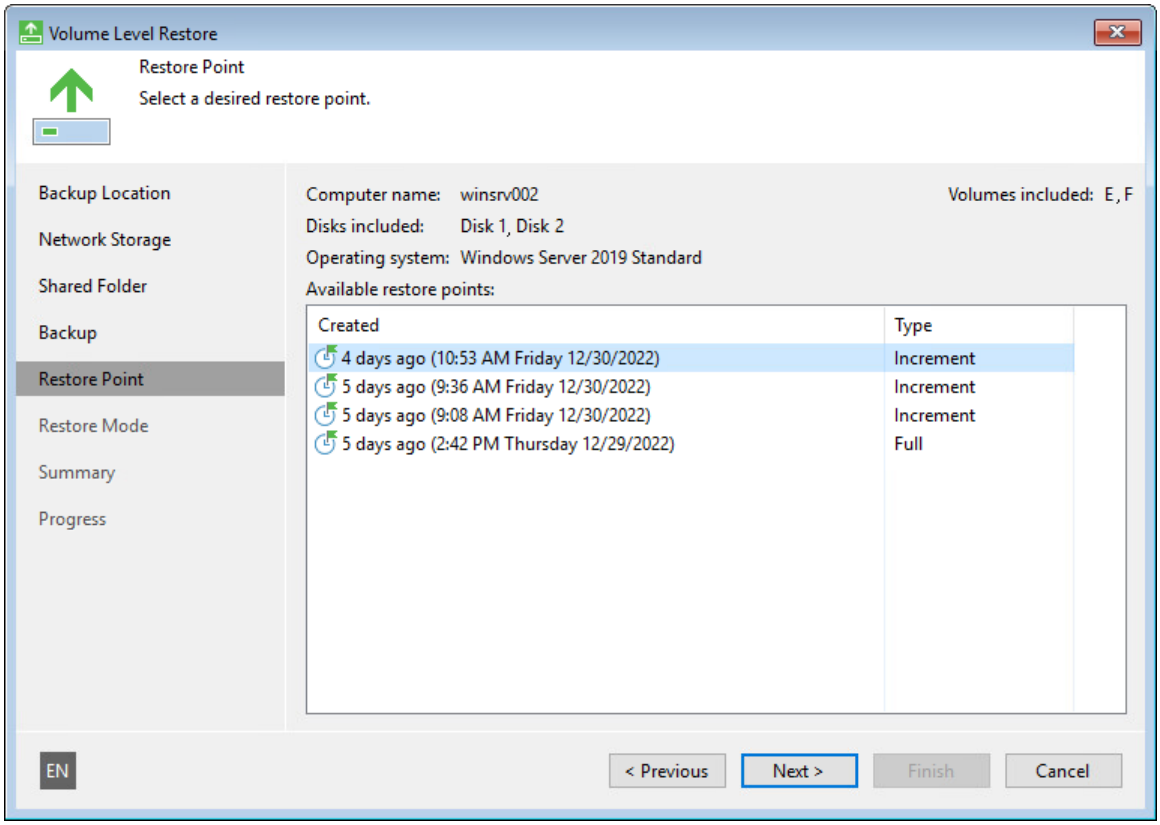

Volume Level Restore
Backup
Specify a backup to restore from. You can type in a few letters of your computer name in the search field to quickly locate the required backup.
Backup Location
Network Storage
Shared Folder
Backup
Restore Point
Restore Mode
Summary
Progress
Selected computer: 172.28.28.92
Name
Last backup
Restore points
Daily Backup
12/28/2022 1:51 P...
System Backup
12/28/2022 1:57 P...
172.28.28.92
12/28/2022 1:57 P...
5
System Volume Backup
12/30/2022 11:18 ...
Weekly Backup
12/28/2022 1:56 P...
Type in an object name to search for
EN
< Previous
Next >
Finish
Cancel

Step 8. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Agent for Microsoft Windows uses the latest restore point. However, you can select any valid restore point to recover files and folders to a specific point in time.

Veeam Agent displays only restore points of volume-level backups. For example, if you have run 2 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Agent will display only 2 restore points in the list.



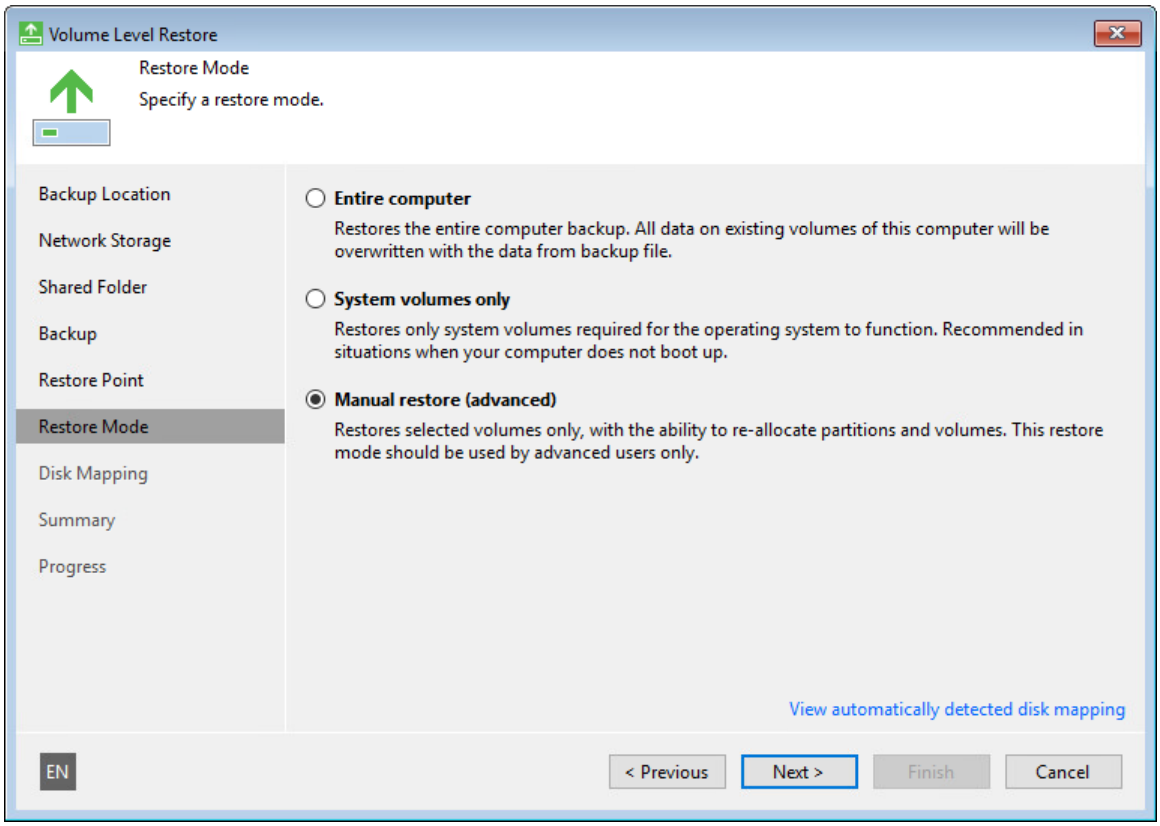
Step 9. Select Data Restore Mode

At the **Restore Mode** step of the wizard, select the data restore mode:

- **Entire computer** — select this option if you want to restore the whole system image of your computer. In this case, Veeam Agent for Microsoft Windows will attempt to map volumes from the backup to existing computer volumes and will overwrite existing data with data restored from the backup.
- **System volumes only** — select this option if you want to restore only system state data and the system volume (volume on which the Microsoft OS is installed). In this case, Veeam Agent for Microsoft Windows will restore the Microsoft Windows system partition and boot partition from the backup to your computer. For GPT disks on Microsoft Windows 8.1, 10, 11, 2012, 2012 R2, 2016, 2019 and 2022 Veeam Agent for Microsoft Windows will additionally restore the recovery partition.
- **Manual restore** — select this option if you want to choose what computer volumes you want to restore and manually allocate disk space on restored volumes. This option is recommended for users who have experience in working with Microsoft Windows disks and partitions.

To view the current disk allocations settings on your computer, at the bottom of the wizard click **View automatically detected disk mapping**.

> **IMPORTANT**
>
> You will not be able to restore data in the *Entire computer* or *System volumes only* mode, if disks on a computer have not enough space to embed volume data from the backup. In this situation, you will be prompted to use the *Manual restore* mode.



Step 10. Map Restored Disks

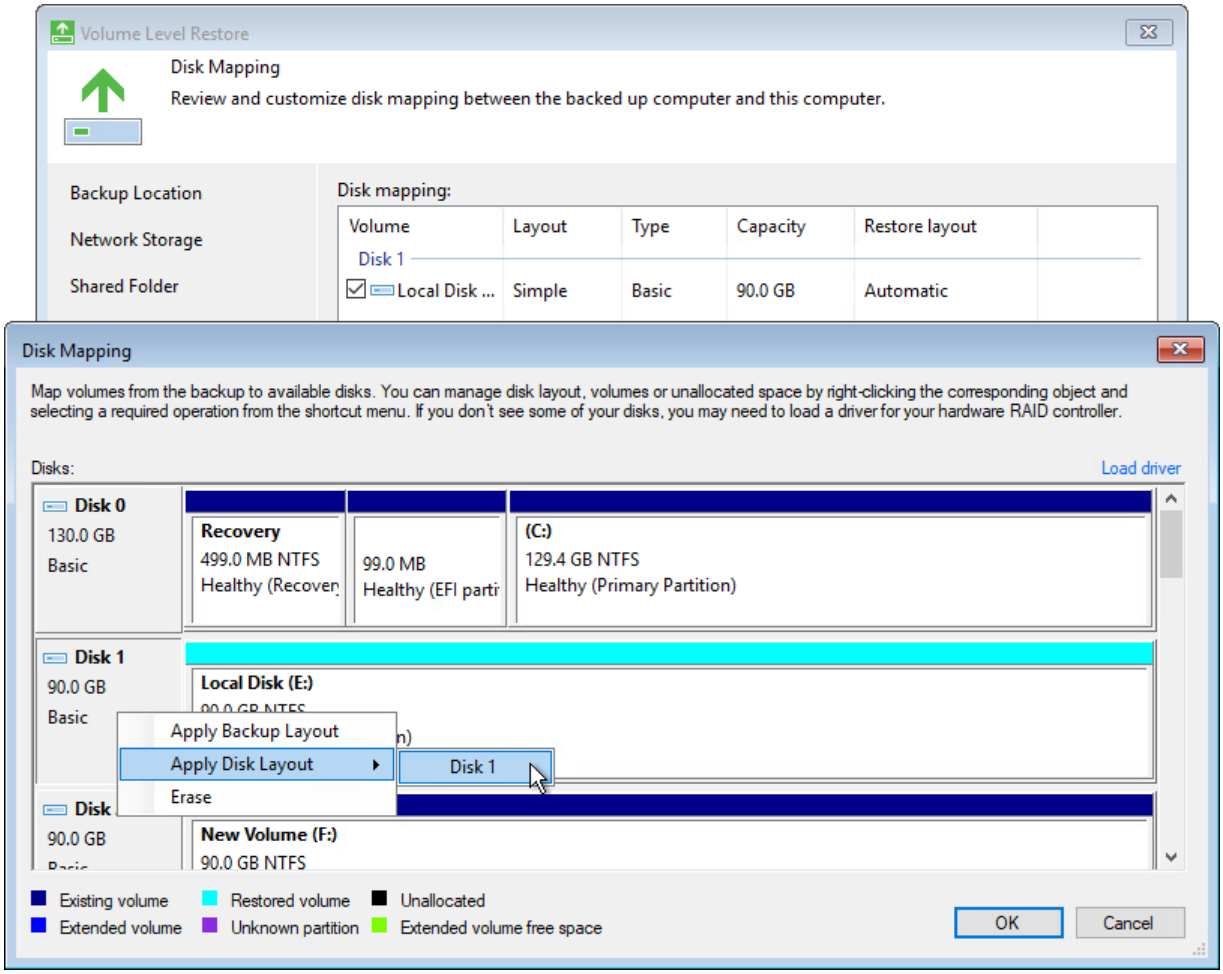
The **Disk Mapping** step of the wizard is available if at the Restore Mode step of the wizard you have chosen to restore data in the *Manual* mode.

You can map volumes that you want to restore from the backup to disks on the target computer.

> **IMPORTANT**
>
> We strongly recommend that you change disk mapping settings only if you have experience in working with Microsoft Windows disks and partitions. If you make a mistake, your computer data may get corrupted.

To map volumes:

1. Select check boxes next to volumes that you want to restore from the backup.
2. [For restore to a new location] By default, Veeam Agent for Microsoft Windows restores all volumes to their initial location. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. To map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**. In the **Disk Mapping** window, specify how volumes must be restored:
    - Right-click the target disk on the left and select the necessary disk layout:
        - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.
        - **Apply Disk Layout** — select this option if you want to apply to the current disk settings of another disk.
        - **Erase** — select this option if you want to discard the current disk settings.

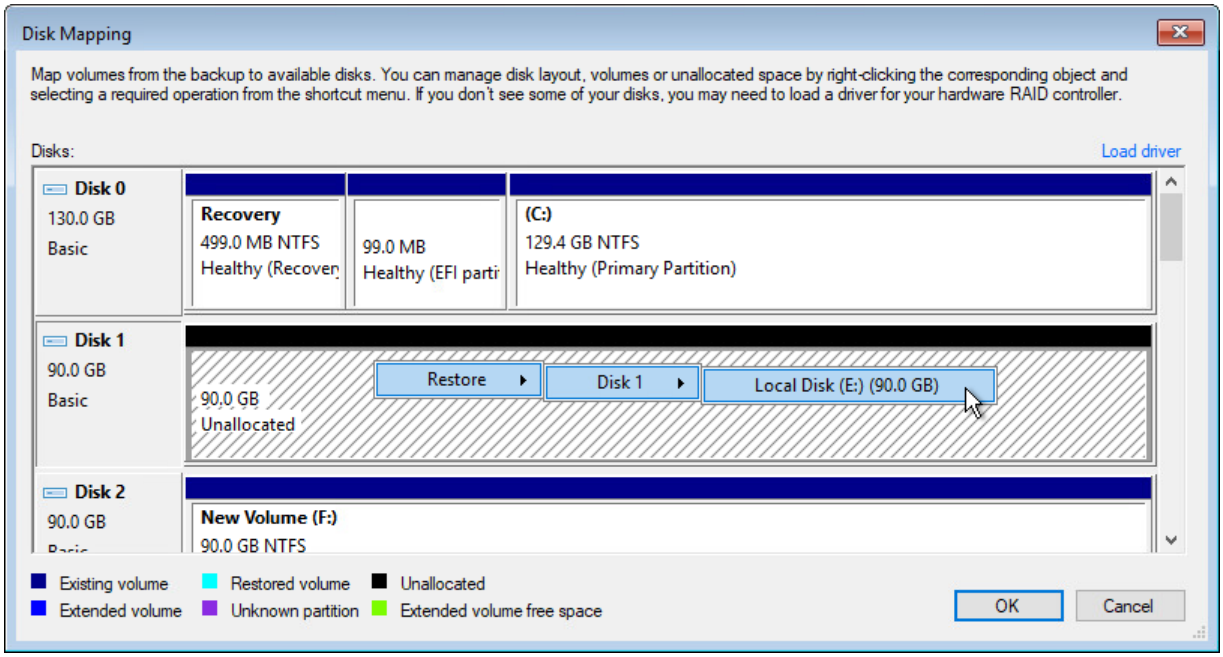


- Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

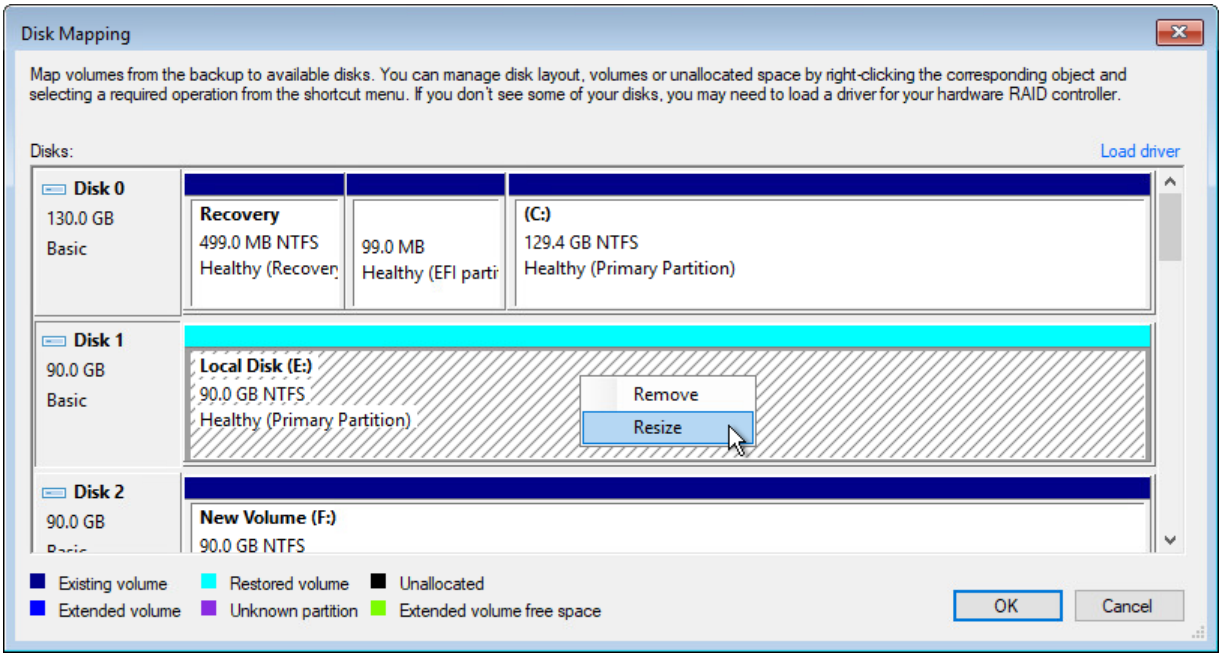
  If you restore to a dynamic disk, after you select the volume to place on the disk, you will pass to the **Allocate Volume** window. To close the window, click **OK.**

  > **NOTE**
  >
  > When you use the Veeam Recovery Media, you can recover volumes from dynamic disks only as simple volumes. If you want to restore such volumes as spanned, striped, mirrored, or parity volumes, you need to perform the following operations:
  >
  > 1. Using the Veeam Recovery Media, restore the system volume from any disk and data volumes from basic disks.
  > 2. Using Veeam Agent, restore volumes from dynamic disks. To learn more, see Restoring Volumes.
  >
  > To learn more about volume types that you can create on dynamic disks, see this Microsoft article.

  If you want to change disk layout configured by Veeam Agent for Microsoft Windows, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



3. [For restore with volume resize] You can resize a volume mapped by Veeam Agent for Microsoft Windows to a target computer disk. To resize a volume, right-click it in the **Disk Mapping** window and select **Resize**. With this option selected, you will pass to the Volume Resize window.



NOTE

If you map a backup volume that is larger than the amount of available space on the target disk, Veeam Agent for Microsoft Windows will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Agent for Microsoft Windows will prepare to shrink the volume to the size of available disk space.

Installing Storage Adapter Drivers

A computer disk may not be available in the list of disks. This can happen in two situations:

- The driver for the storage adapter is included in the Veeam Recovery Media but failed to be installed automatically for some reason.
- The driver for the storage adapter is not included in the Veeam Recovery Media.

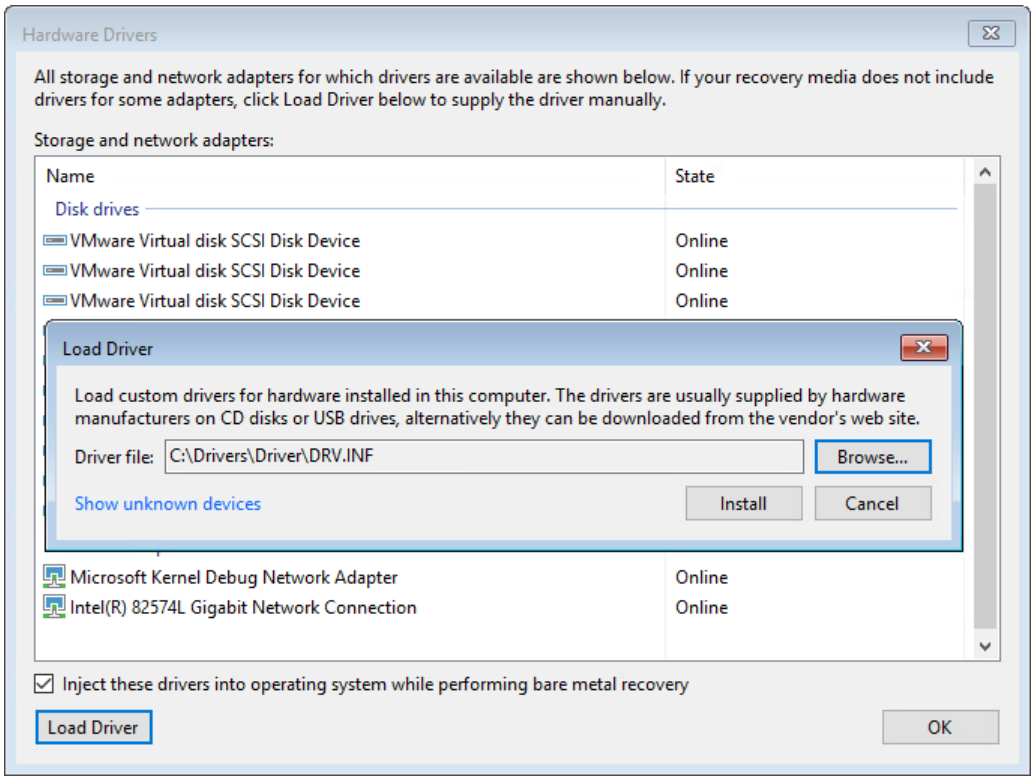
To install drivers that were included in the Veeam Recovery Media:

1. At the **Disk Mapping** step of the wizard, click **Load driver**.
2. In the **Hardware Drivers** window, select the necessary device.

   If you do not want to save drivers for listed devices to the restored operating system, clear the **Inject these drivers into operating system while performing bare metal recovery** check box.
3. Click the **Install** link next to the selected device.

To install drivers that were not included in the Veeam Recovery Media:

1. At the Disk Mapping step of the wizard, click **Load driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the Show unknown devices link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.



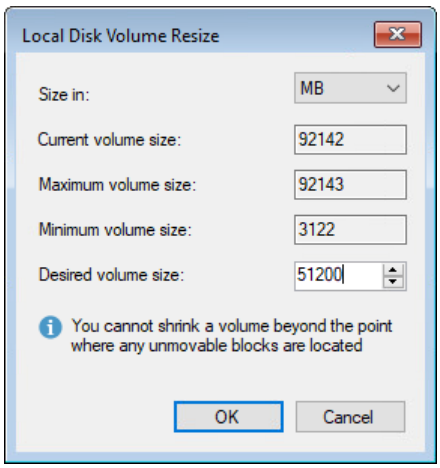
Step 11. Resize Restored Volumes

At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. You can resize a volume if you have chosen to restore data in the *Manual* mode and customize disk layout. A volume will be shrunk or extended to the specified size during the process of data restore.

> **NOTE**
>
> By default, Veeam Agent for Microsoft Windows displays volume size in megabytes (MB). This allows you to specify the desired size for the volume precisely. You can also choose to display volume size in gigabytes (GB). This may be helpful when you need to resize volumes on larger computer disks and want to simplify disk size calculations.
>
> When you use GB as a volume size unit, you can specify volume size with integral numbers, for example, 1 GB, 60 GB or 200 GB, but not 0,8 GB, 60,5 GB or 200,7 GB. However, if the maximum volume size is in fact greater than the displayed value for less than 1 GB, Veeam Agent for Microsoft Windows will automatically add the exceeding amount of disk space to the extended volume. For example, if the maximum volume size is 60,2 GB, Veeam Agent for Microsoft Windows will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Agent for Microsoft Windows will extend the volume to 60,2 GB.

To resize a volume:

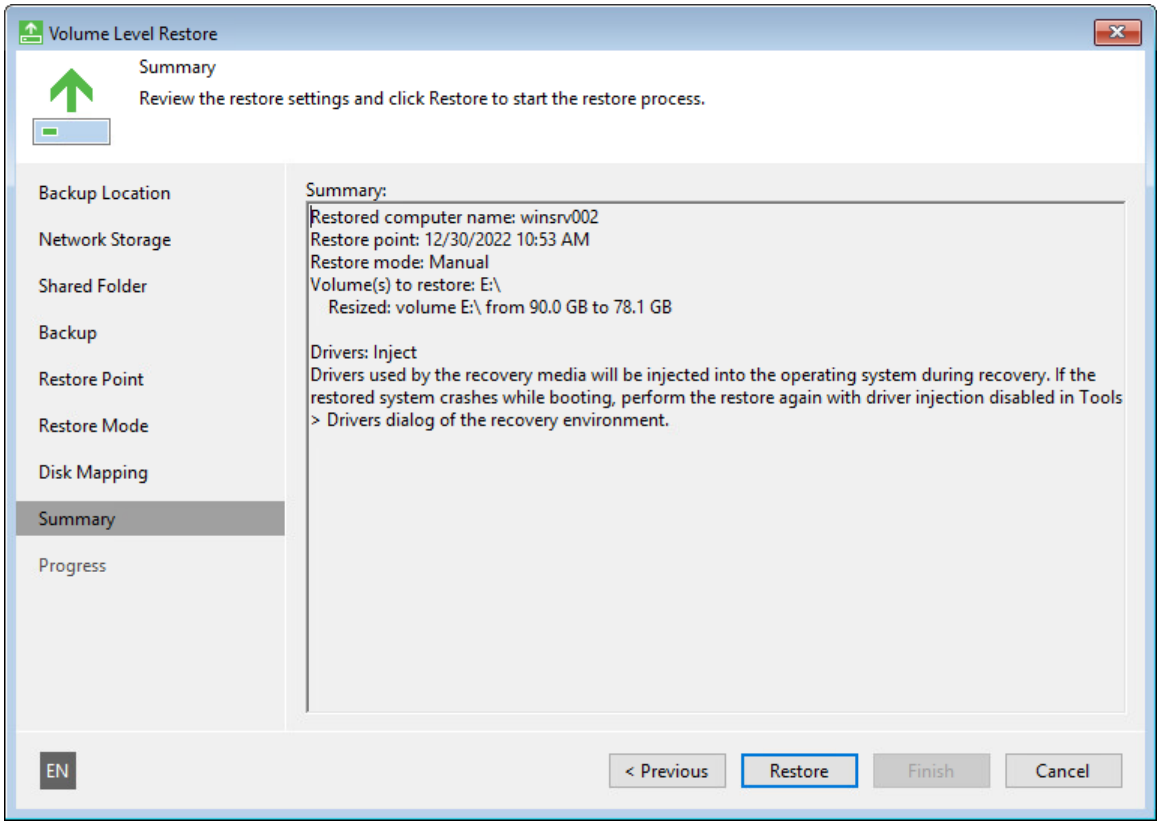
1. Specify a volume you want to resize:
   a. Right-click a restored volume mapped to a target disk and select **Resize**.
   b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Agent for Microsoft Windows will prompt you to shrink the restored volume.
2. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.



Step 12. Start Restore Process

At the **Summary** step of the wizard, finalize the recovery process.

1. Review the specified recovery settings.
2. Click **Restore** to start the recovery process. Veeam Agent for Microsoft Windows will perform partition re-allocation operations if necessary, restore the necessary data from the backup and overwrite data on your computer with it.



Using Veeam Agent and Microsoft Windows Tools

When you boot from the Veeam Recovery Media, you can use a set of tools to repair typical causes of unbootable OS, diagnose your computer and perform advanced administration tasks. Veeam Agent for Microsoft Windows offers its native tools and standard Microsoft Windows recovery tools.

> **IMPORTANT**
>
> Veeam Agent for Microsoft Windows includes Microsoft Windows Tools in the Veeam Recovery Media. If some of Microsoft Windows Tools components are missing on the computer, some of Microsoft Windows Tools may not be available when you boot from the Veeam Recovery Media.

To open the tools view, on the **Veeam Recovery Media** screen, click **Tools**. Then choose the necessary tool from the list:

- **Command Prompt** — use this option to start the Microsoft Windows command prompt (`cmd.exe`).
- **Reset Password** — use this option to reset a password for the built-in Administrator account to none. The next time you boot your computer from the hard disk under the Administrator account, you will not have to specify any password. Consider the following:
  - The password reset option does not function on domain controller machines.
  - If the built-in Administrator account is disabled, this account will be enabled by the password reset option.
- **Load Driver** — use this option to load from external sources drivers that are not available on the Veeam Recovery Media. Drivers can be loaded from the computer drive or from a network shared folder.
- **Memory Diagnostic** (Microsoft utility) — use this option to check the system memory of your computer and detect potential problems. The utility can be started during the current work session or when you boot your computer the next time. To learn more, see this Microsoft article.
- **Startup Repair** (Microsoft utility) — use this option to fix system problems that may prevent Microsoft Windows from starting, for example, missing and damaged system files or the corrupted boot sector. To learn more, see this Microsoft article.
- **Export Logs** — use this option to export the Veeam Agent for Microsoft Windows debug logs to a ZIP file and save this file on a removable storage appliance attached to your computer.

> **NOTE**
>
> Do not save the archive file with debug logs on the local disk `X:` of the recovery image OS. This local disk is a temporary storage that will be automatically deleted after you finish working with the Veeam Recovery Media.

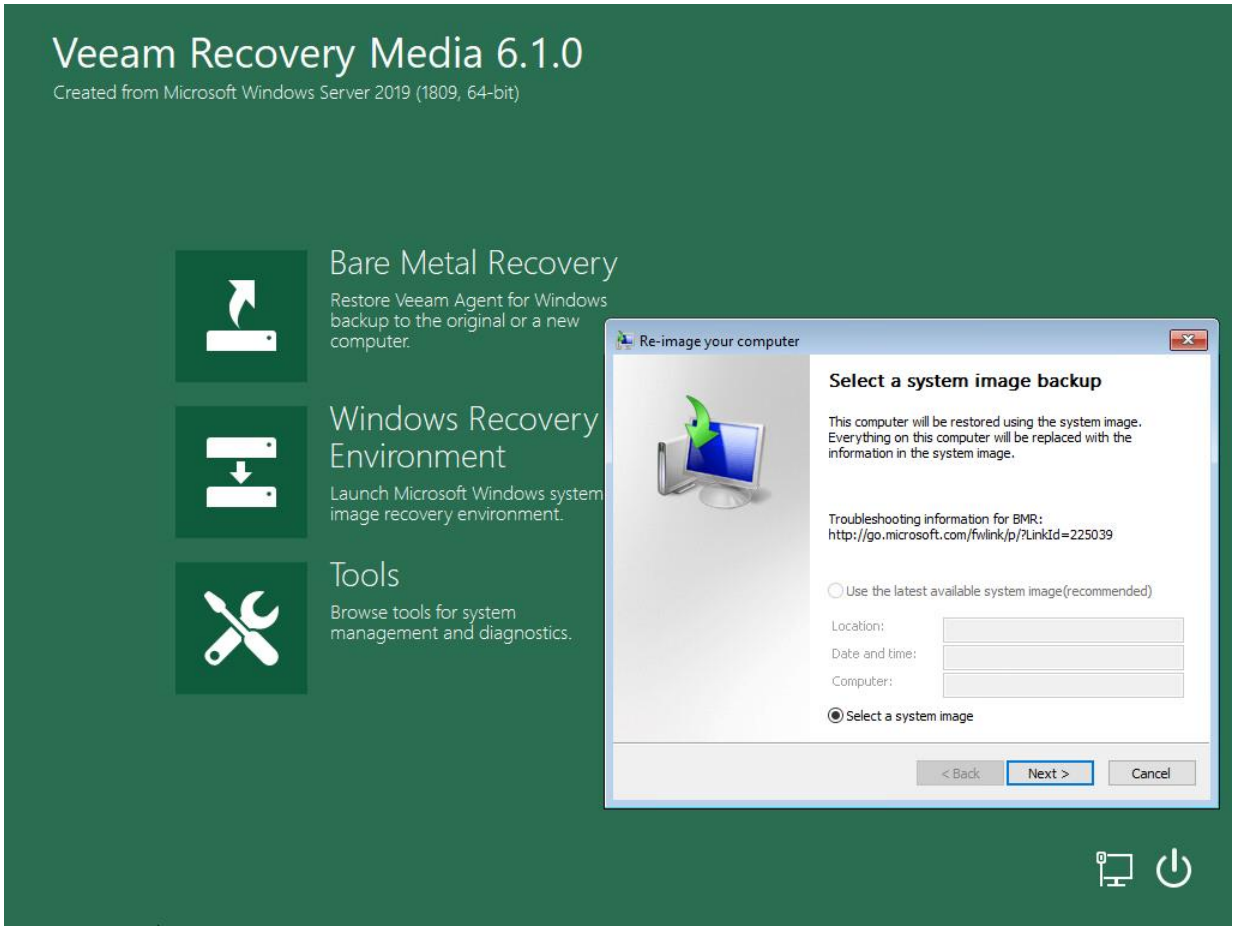

Tools
Command Prompt
Opens Microsoft Windows command prompt.
Memory Diagnostic
Runs Microsoft Windows memory diagnostic tool.
Reset Password
Resets Local Administrator account's password.
Startup Repair
Fixes problems that are preventing Microsoft Windows from starting.
Load Driver
Select and load driver for storage controller, network adapter or other hardware.
Export Logs
Saves recovery appliance debug log files to a removable storage.

Using Microsoft Windows Recovery Environment

If you have a Microsoft system image on the computer drive or a DVD archive with Microsoft system images, you can recover your computer using the Microsoft Windows System Image Recovery tool.

To access the Microsoft Windows System Image Recovery tool, on the Veeam Recovery Media screen, click **Windows Recovery Environment**.

The process of recovery does not differ from the process performed in Microsoft Windows. To learn more, see this Microsoft article.



Restoring Volumes

You can restore a specific computer volume or all volumes from the volume-level backup.

Volumes can be restored to their original location or to a new location.

- If you restore a volume to its original location, Veeam Agent for Microsoft Windows will overwrite the data on the original volume with the data restored from the backup.
- If you restore volume data to a new location, Veeam Agent for Microsoft Windows will restore data from the backup and write it to the selected destination. If necessary, you can specify new disk mapping settings for the restored volume.

Before You Begin

Before you begin the volume-level restore process, check the following prerequisites and limitations.

General

- The volume-level backup from which you plan to restore data must be successfully created at least once.
- [For backups stored in network shared folders and on backup repositories] You must have access to the target location where the backup file resides.
- [For backup repository targets] If you plan to restore data from a backup stored in a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
- A user account under which you start the restore operation must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.

ReFS Restore

If you restore a ReFS volume from a backup that was made on another machine, the Veeam Agent computer where you perform restore must run the OS that supports the specific ReFS version. For example, you can restore a ReFS 3.x volume only to a computer that runs one of the following OSes:

- Microsoft Windows 10 version 1803 or later
- Microsoft Windows Server 2016 or later

NTFS Restore

- If you restore an NTFS volume from a backup that was made on another machine, and data deduplication was enabled for the volume, the Veeam Agent computer where you perform restore must run the same OS version or later as the backed-up machine OS.
- If you restore an NTFS volume from a backup that was made on another machine, and the allocation unit size of the volume was set to 128K or greater, the Veeam Agent computer where you perform restore must run one of the following OSes:
    - Microsoft Windows 10 version 1803 or later
    - Microsoft Windows Server 2019 or later

Volume-Level Restore Limitations

Volume-level restore has the following limitations:

- You cannot restore the system volume to its original location.
- You cannot restore a volume to the volume on which the Microsoft Windows swap file is hosted.
- You cannot restore a volume to the volume where the backup file that you use for restore is located.

To overcome the first two limitations, you can boot from the recovery image and use the **Volume Level Restore** wizard for volume-level restore. To learn more, see Restoring from Veeam Recovery Media.

Step 1. Launch Volume Level Restore Wizard

To launch the **Volume Level Restore** wizard, do either of the following:

- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Restore** > **Entire volumes**.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**. In the control panel, click a bar of the necessary backup job session. Click **Restore Volumes** at the bottom of the window.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**. In the main menu, hover over the name of the job that that created the backup from which you want to restore data, and select **Restore volume**.
- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Tools** > **Volume Restore**.

If Veeam Agent for Microsoft Windows automatically detects backups of your computer in the target location, you will pass immediately to the Restore Point step of the wizard.

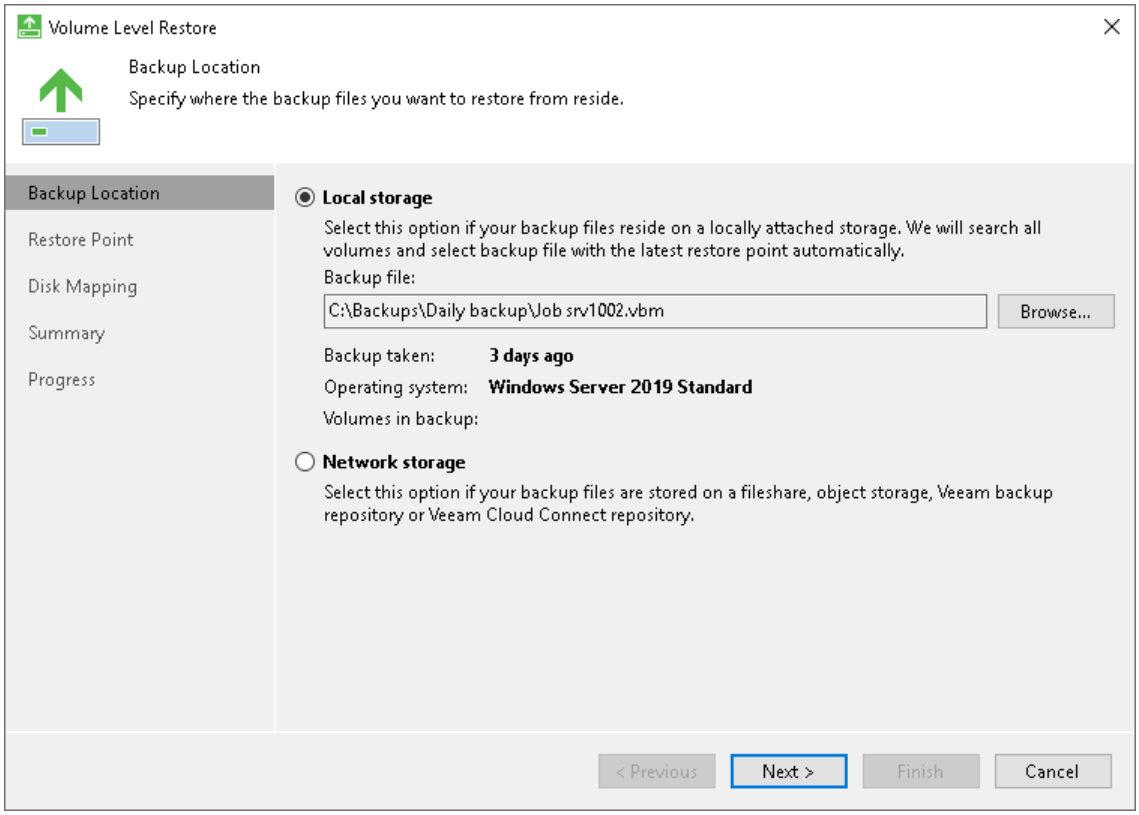


Step 2. Specify Backup File Location

At the **Backup Location** step of the wizard, specify where the backup file that you plan to use for restore resides.

If you configured only one backup job, Veeam Agent automatically locates the latest backup of this backup job on the target storage, and you pass immediately to the Restore Point step of the wizard. If there are several backup jobs configured or Veeam Agent fails to locate the backup for some reason, specify where the backup file resides:

- **Local storage** — select this option if the backup file resides on the computer drive, external drive or removable storage device that is currently connected to your computer. Click **Browse** and select a backup metadata file (VBM).
- **Network storage** — select this option if the backup file resides in object storage, in a network shared folder, in a backup repository managed by a Veeam backup server or in a cloud repository exposed to you by a Veeam Cloud Connect service provider. In this case, the Volume Level Restore wizard will include additional steps for specifying file location settings.

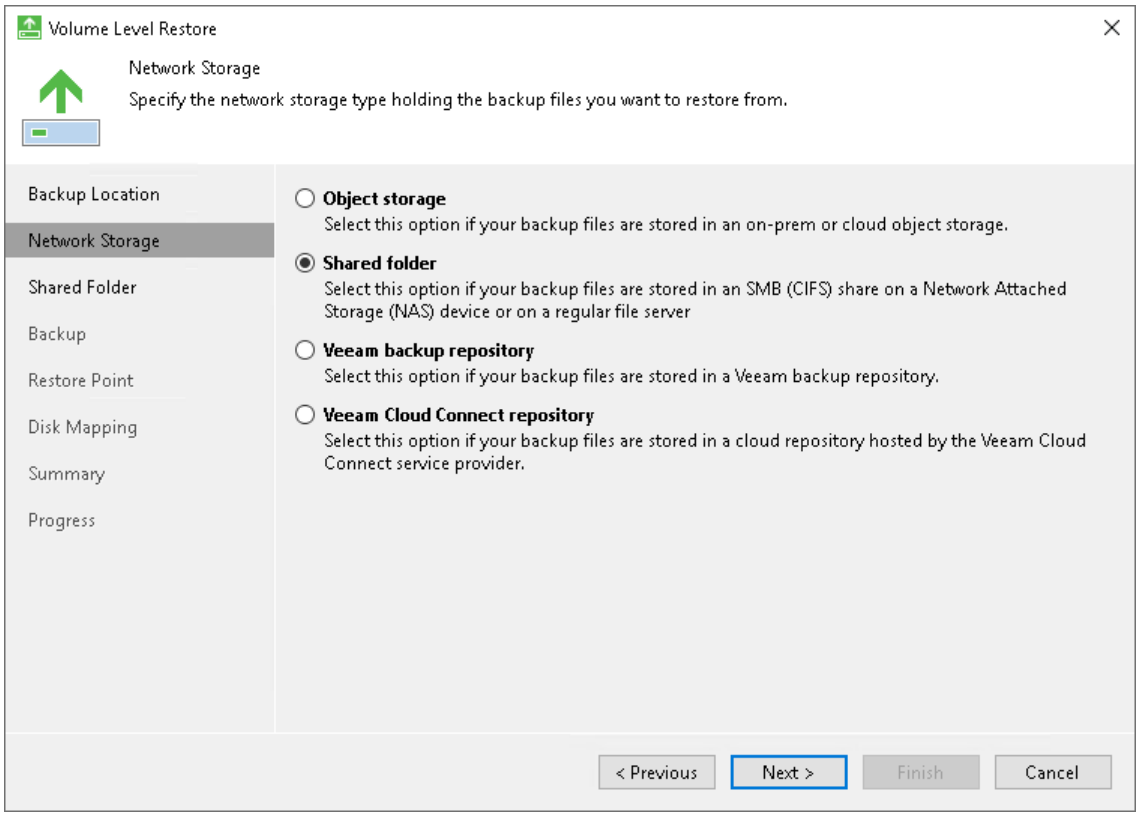


Step 3. Select Network Storage Type

The **Network Storage** step of the wizard is available if you have chosen to restore data from a backup file that resides in a remote location — in object storage, in a network shared folder, in a backup repository or in a cloud repository.

Select where the backup file is located:

- **Object storage** — select this option if the backup file resides in object storage. With this option selected, you will pass to the Object Storage step of the wizard.
- **Shared folder** — select this option if the backup file resides in a network shared folder. With this option selected, you will pass to the Shared Folder step of the wizard.
- **Veeam backup repository** — select this option if the backup file resides in a backup repository managed by a 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 the backup file resides in a cloud repository exposed to you by a Veeam Cloud Connect service provider. With this option selected, you will pass to the Service Provider step of the wizard.



Step 4. Specify Network Storage Settings

Specify settings for the network storage that contains a backup file from which you plan to restore data:

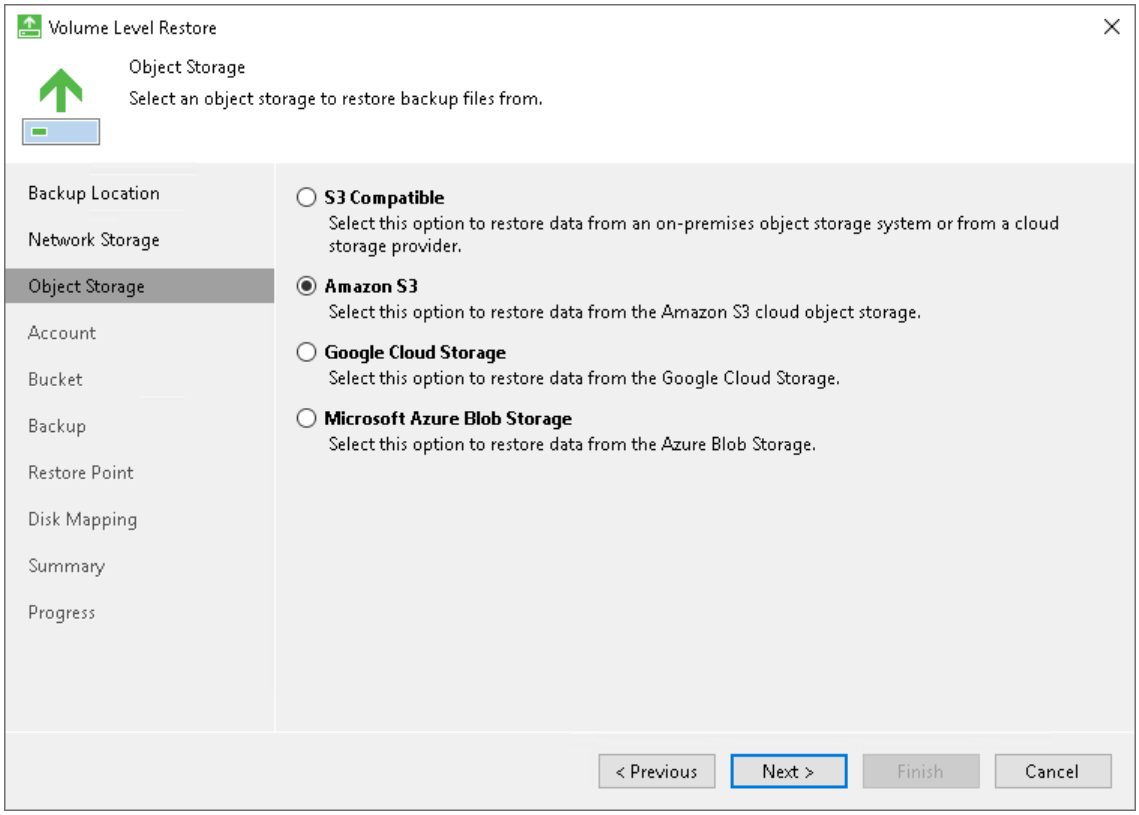
- Object storage settings — if you have selected the **Object storage** option at the Network Storage step of the wizard.
- Shared folder settings — if you have selected the **Shared folder** option at the Network Storage step of the wizard.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Network Storage step of the wizard.
- Veeam Cloud Connect repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Network Storage step of the wizard.

Object Storage Settings

The **Object Storage** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

Specify settings for the object storage:

- Specify S3 compatible settings.
- Specify Amazon S3 settings.
- Specify Google Cloud Storage settings.
- Specify Microsoft Azure Blob Storage settings.



S3 Compatible Settings

If you have selected to restore data from a backup file located in the S3 compatible storage, specify the following settings:

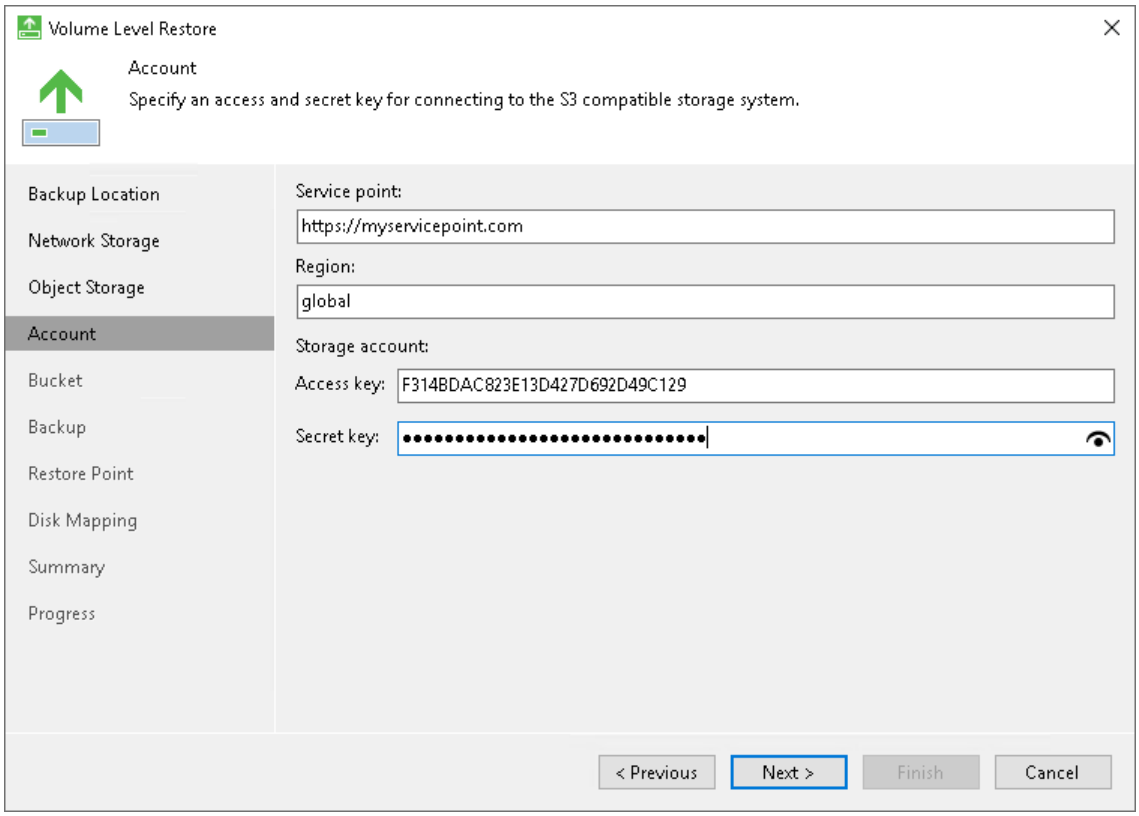
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Service point** field, specify the address of your S3 compatible storage.
2. In the **Region** field, specify the storage region.
3. In the **Access key** field, enter the access key ID.
4. In the **Secret key** field, enter the secret access key.

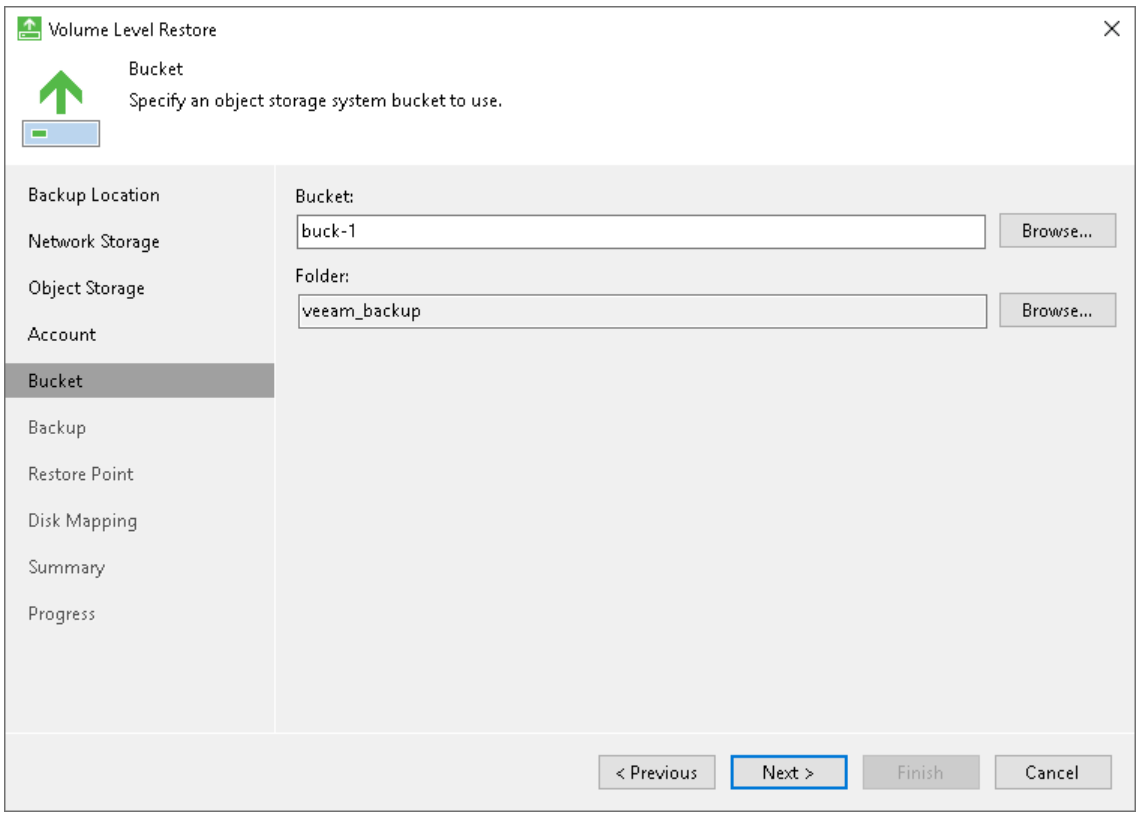


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



Amazon S3 Settings

If you have selected to restore data from a backup file located in the Amazon S3 storage, specify the following settings:

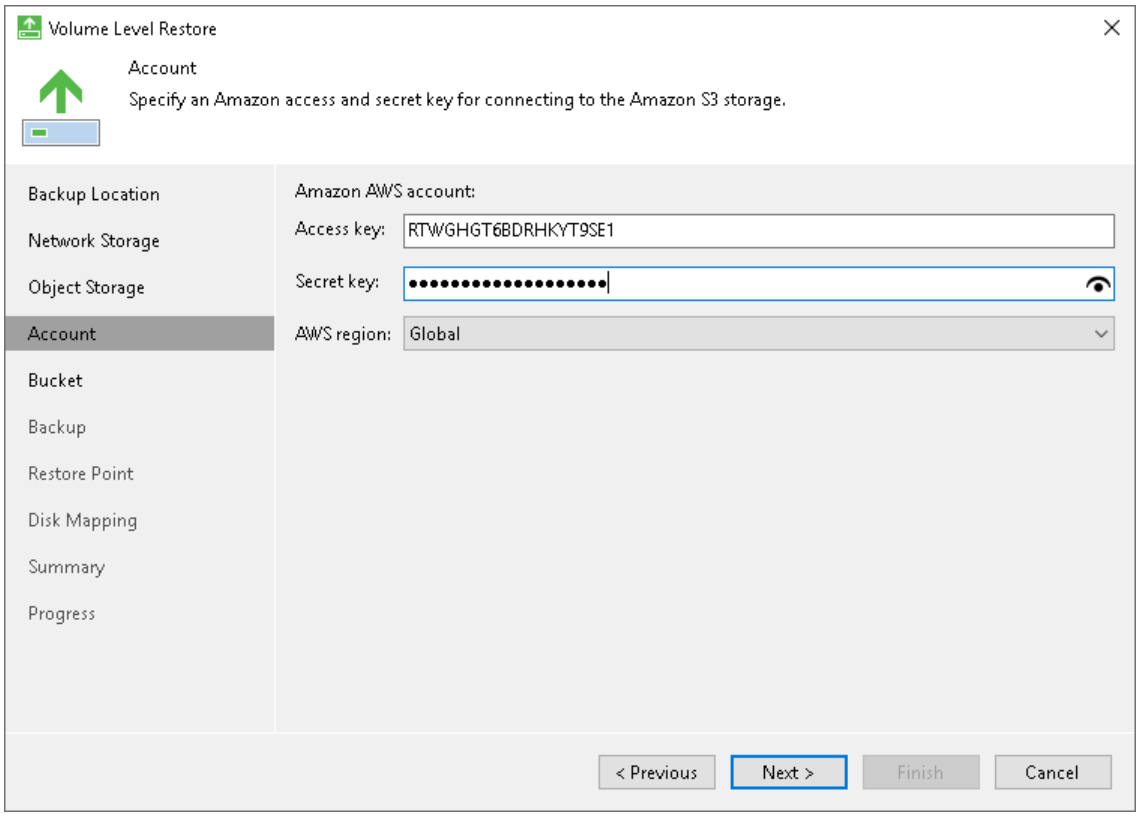
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Access key** field, enter the access key ID.
2. In the **Secret key** field, enter the secret access key.
3. From the **AWS region** drop-down list, select the AWS region. By default, Veeam Agent uses the **Global** region.

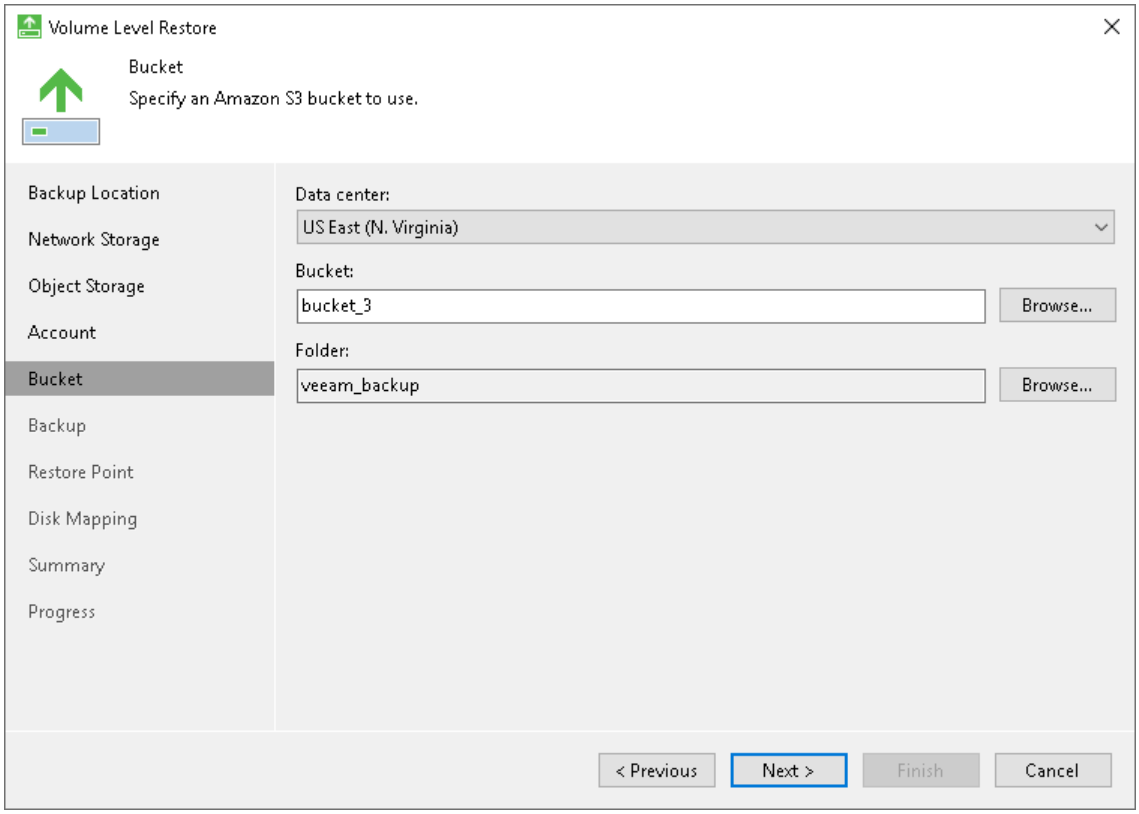


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
   a. Select the **Browse** option.
   b. In the **Select Bucket** window, do the following:
      i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
      ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
   a. Select the **Browse** option.
   b. In the **Select Folder** window, do the following:
      i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
      ii. Select the necessary folder and click **OK**.



Google Cloud Storage Settings

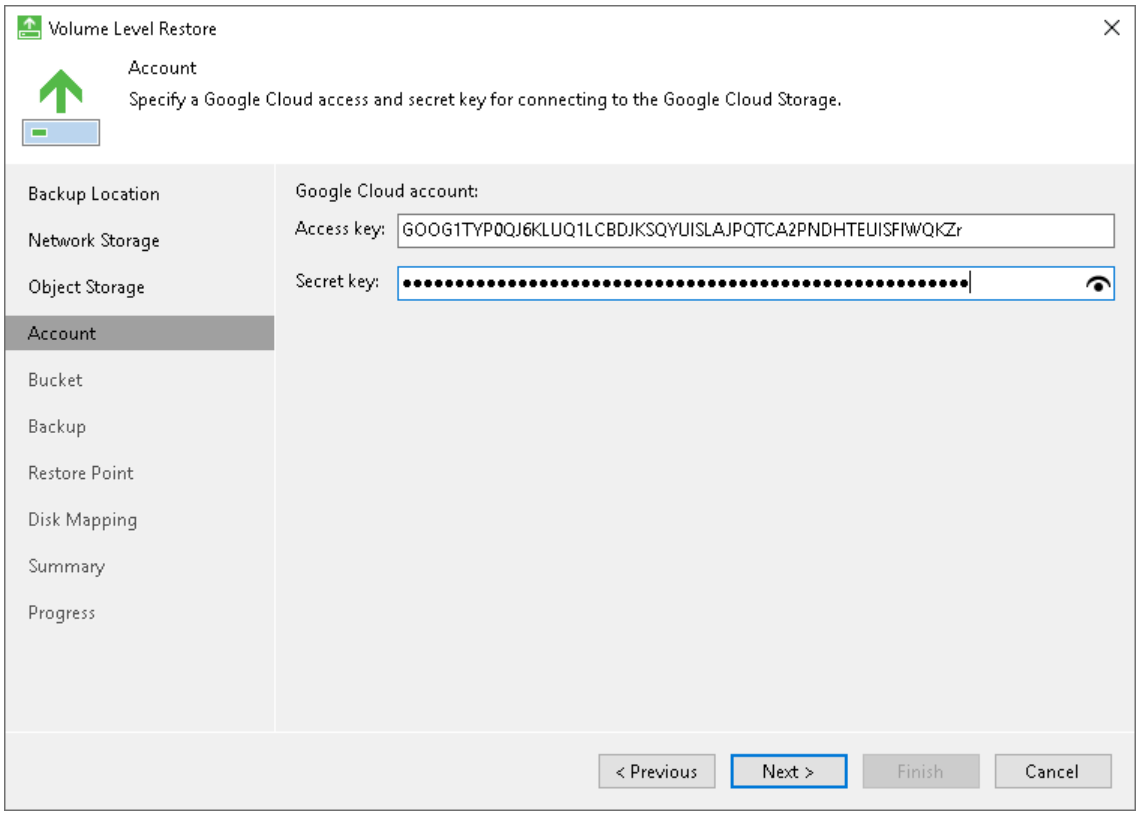
If you have selected to restore data from a backup file located in the Google Cloud storage, specify the following settings:

1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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



Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center region** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.

b. In the **Select Bucket** window, do the following:

i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.

ii. Select the necessary bucket and click **OK**.

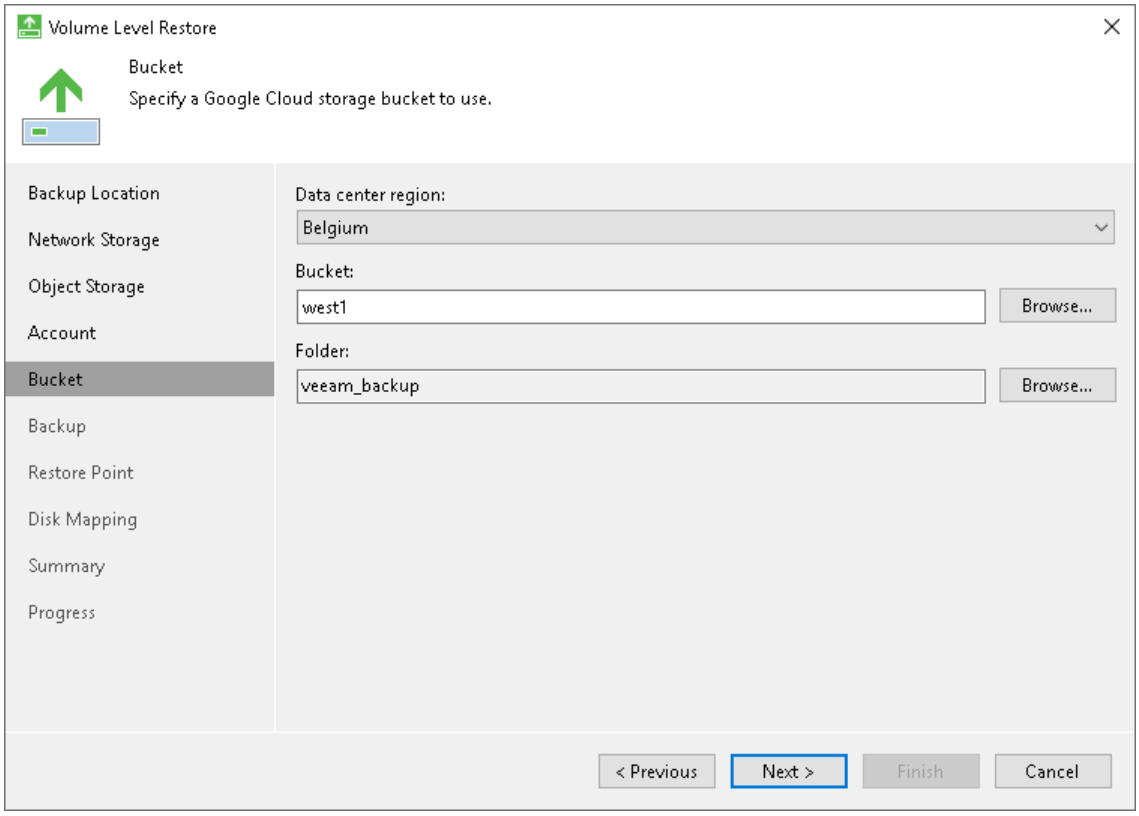
3. In the **Folder** field, specify a folder in the bucket:

a. Select the **Browse** option.

b. In the **Select Folder** window, do the following:

i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.

ii. Select the necessary folder and click **OK**.



Microsoft Azure Blob Storage Settings

If you have selected to restore data from a backup file located in the Microsoft Azure Blob storage, specify the following settings:

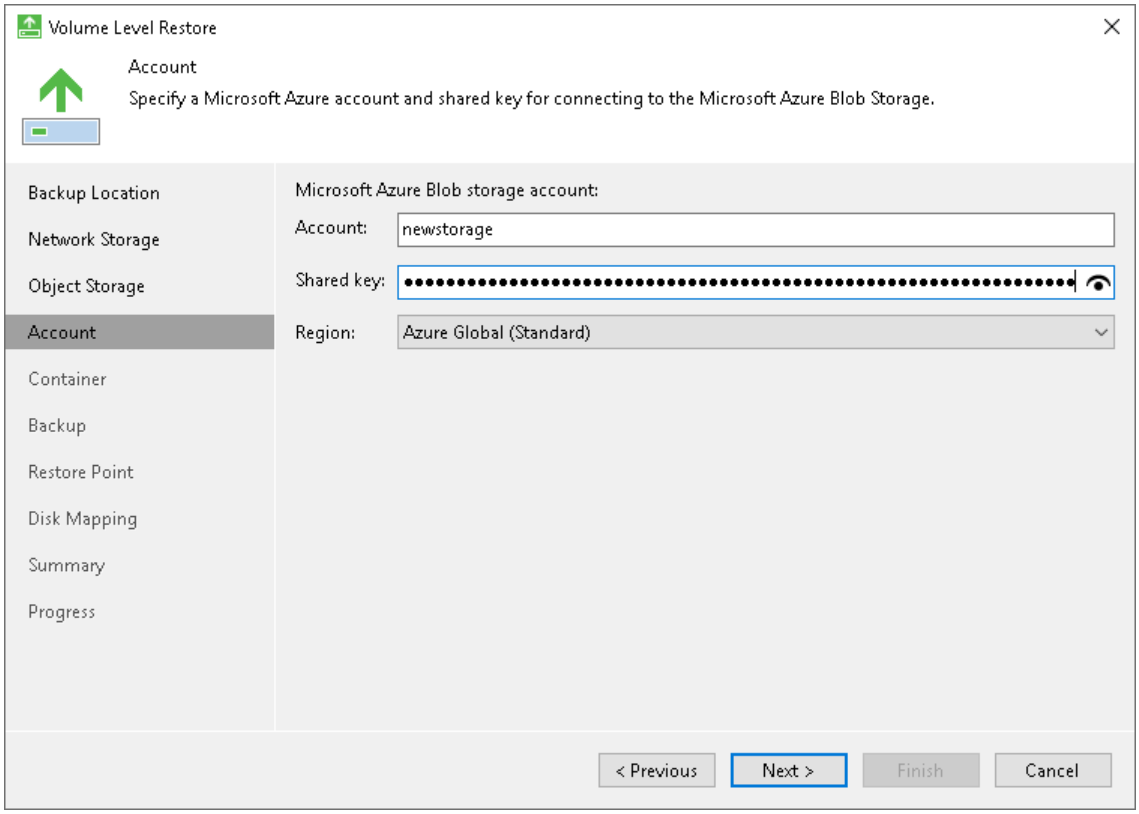
1. Specify account settings.
2. Specify container settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

To connect to the Microsoft Azure Blob 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. From the **Region** drop-down list, select the Microsoft Azure region. By default, Veeam Agent uses the **Azure Global (Standard)** region.

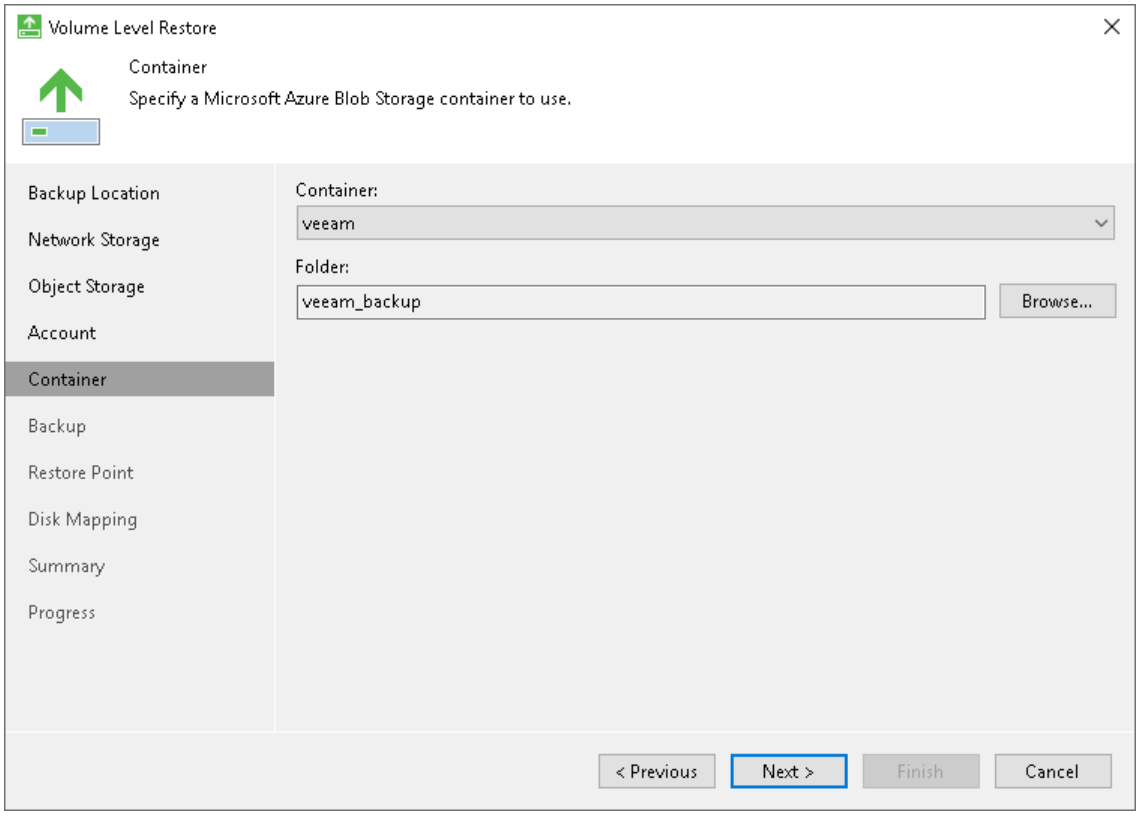


Specifying Container Settings

The **Container** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft Azure Blob storage and specified account settings to connect to the storage.

Specify settings for the container in the storage:

1. From the **Container** drop-down list, select a container in the storage.
2. In the **Folder** field, specify a folder in the container:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the container name or click the arrow to the left of the container name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



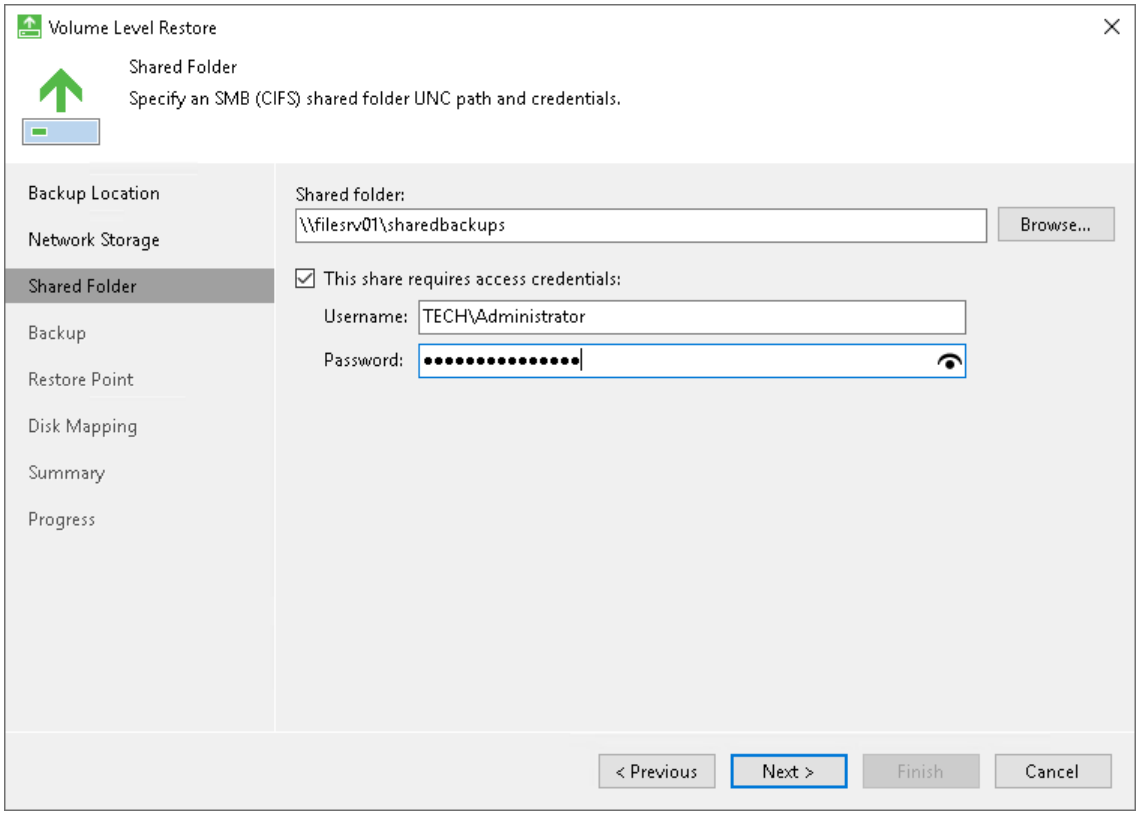
Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have chosen to restore data from a backup file located in a network shared folder.

Specify settings for the network shared folder:

1. In the Shared folder field, enter a UNC name of the network shared folder with the backup file. Keep in mind that the UNC name always starts with two back slashes (\\).
2. If the network shared folder requires authentication, select the **This share requires access credentials** check box and specify a user name and password of the account that has *Full Control* access permissions on this shared folder. The user name must be specified in the down-level logon name format. For example, *DOMAIN\UserName* or *HOSTNAME\UserName*.

   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the *NT AUTHORITY\SYSTEM* account of the computer where the product is installed.
3. To view the entered password, click and hold the eye icon on the right of the **Password** field.



Backup Server Settings

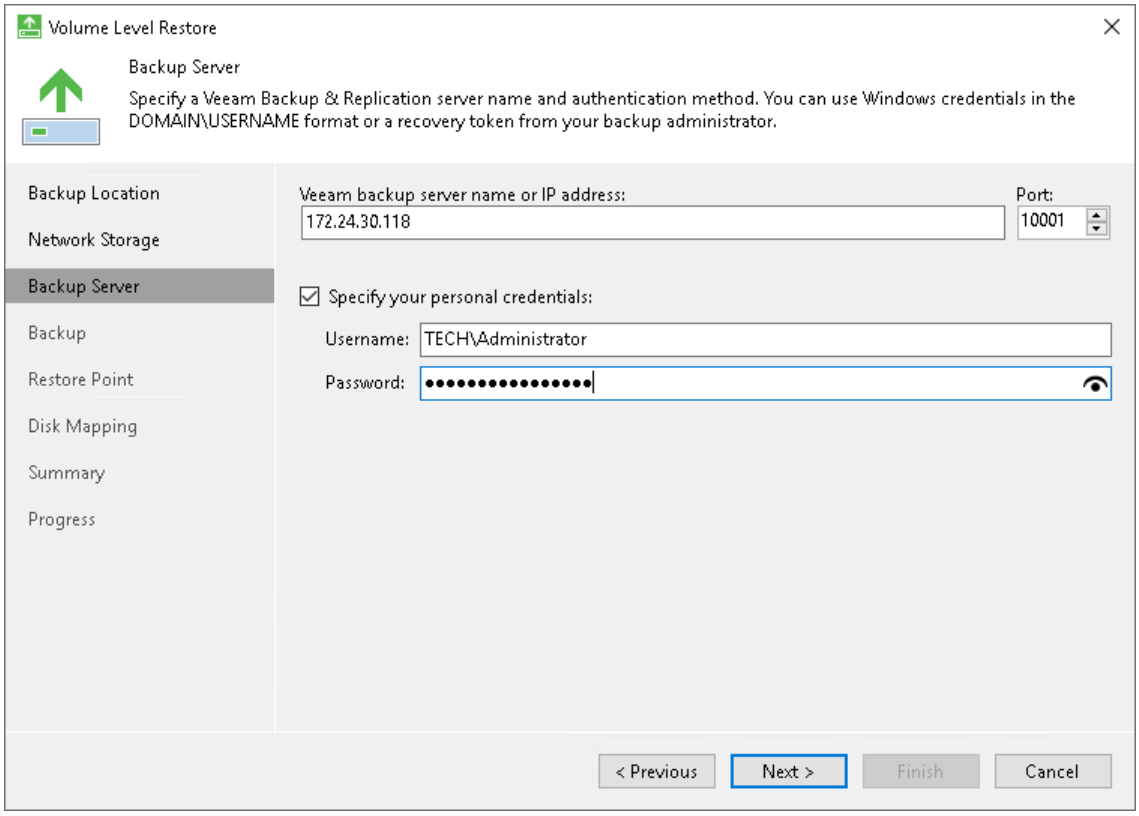
The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located in a backup repository.

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

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup server. By default, Veeam Agent for Microsoft Windows uses port 10001.
3. Select the **Specify your personal credentials** check box. In the **Username** and **Password** fields, enter a user name and password of the account that has access to this backup repository. Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

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

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



Service Provider Settings

If you have selected to restore data from a backup file located on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

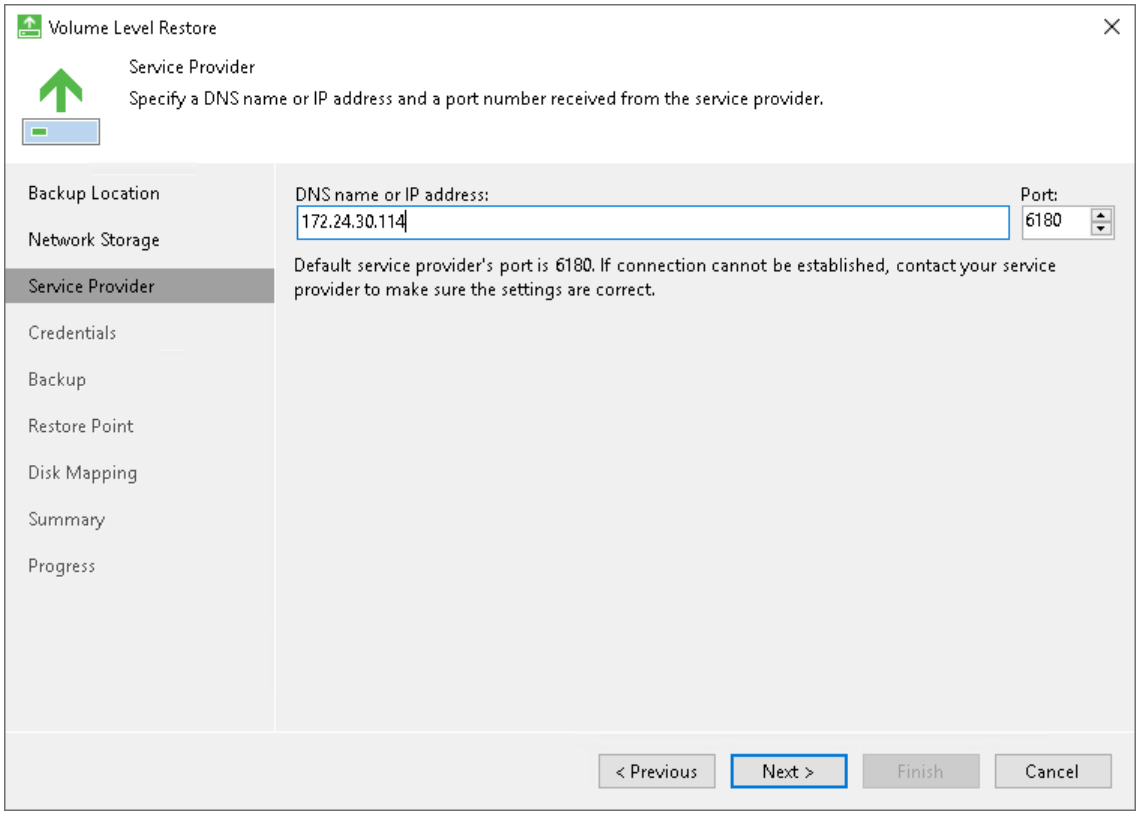
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

Specifying Service Provider Settings

The **Service provider** step of the wizard is available if you have chosen to restore data from a cloud repository exposed to you by a Veeam Cloud Connect service provider.

Specify service provider settings that the 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 for Microsoft Windows will communicate with the cloud gateway. By default, port 6180 is used.



Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to restore data from a cloud repository and specified settings for the cloud gateway.

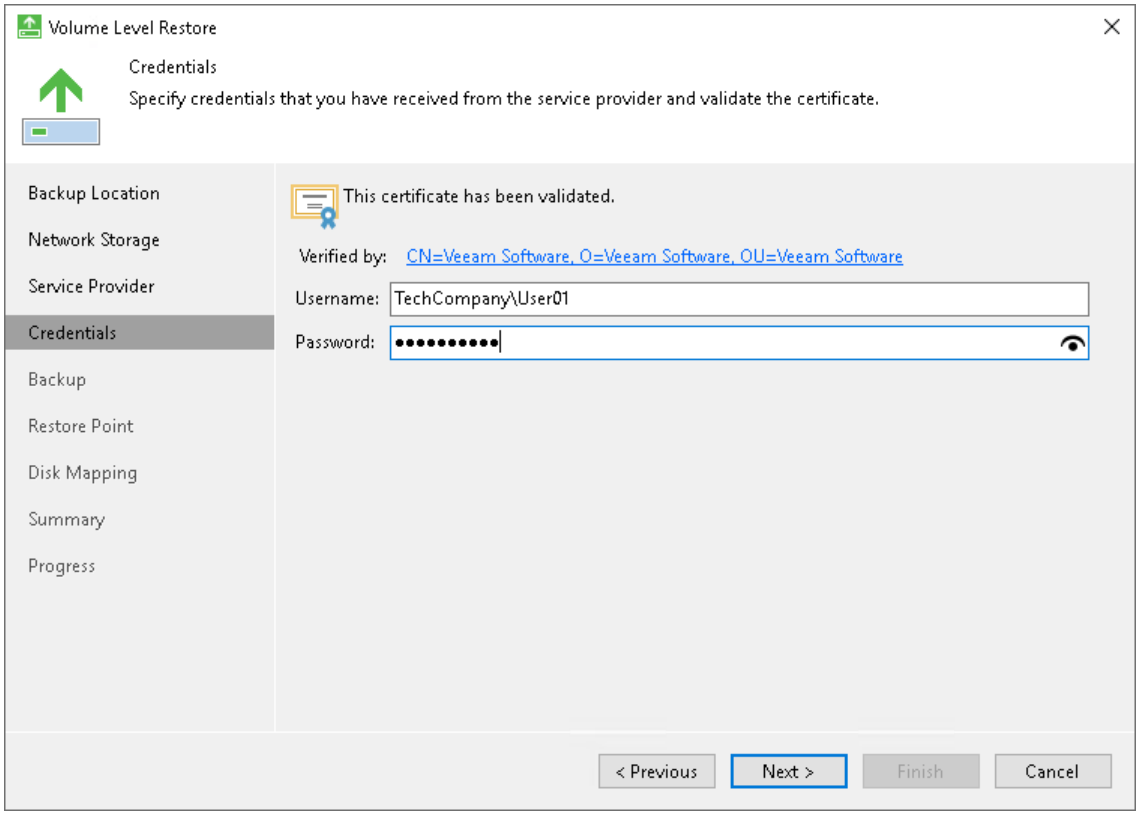
Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the service provider.

1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   - To view the TLS certificate, click the certificate link.
   - To verify if the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Fingerprint for certificate verification** field. Click **Verify**. Veeam Agent for Microsoft Windows will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. In the **Username** field, enter the user name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The user name of the subtenant account must be specified in the *TENANT|SUBTENANT* format.
3. In the **Password** field, provide a password for the tenant or subtenant account.


Volume Level Restore
Credentials
Specify credentials that you have received from the service provider and validate the certificate.
Backup Location
Network Storage
Service Provider
Credentials
Backup
Restore Point
Disk Mapping
Summary
Progress
This certificate has been validated.
Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software
Username: TechCompany\User01
Password: ••••••••••
< Previous
Next >
Finish
Cancel

Step 5. Select Backup

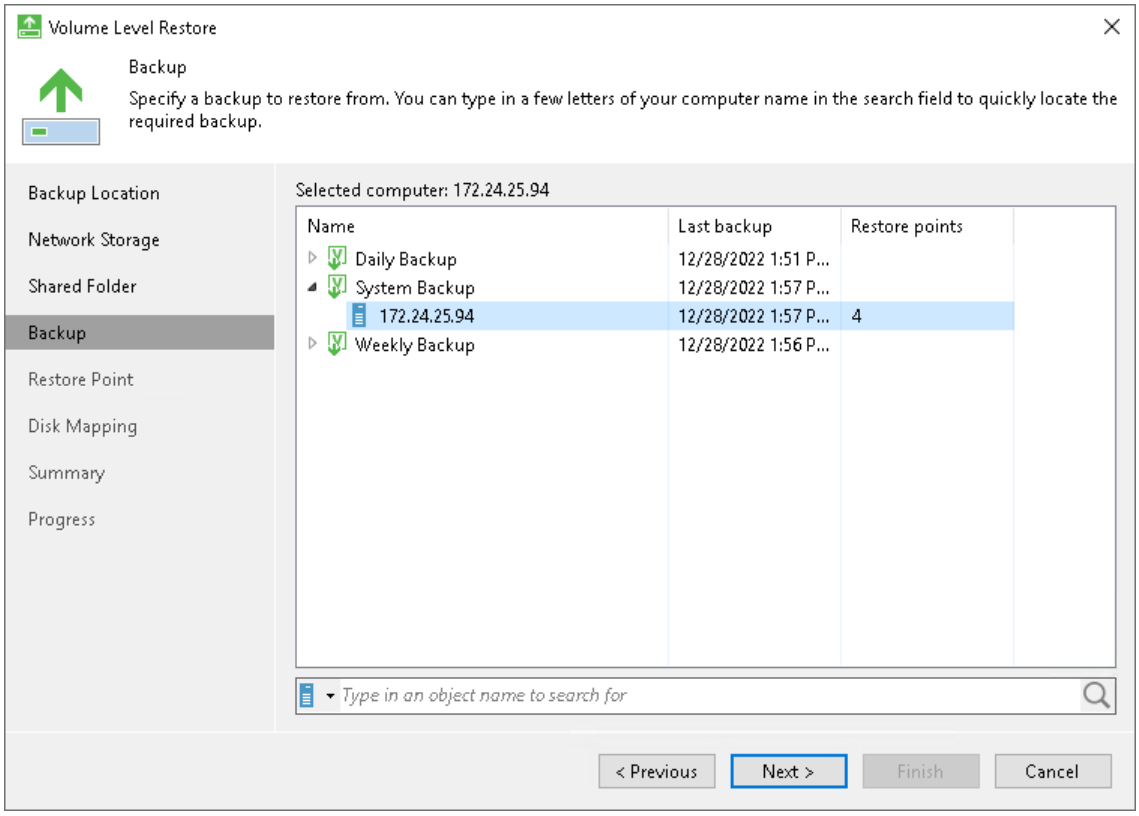
The **Backup** step of the wizard is available if you have chosen to restore data from a backup file located in object storage, in a network shared folder or in a backup repository.

From the list of backups, select a backup from which you want to recover data. To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

In the list of backups, Veeam Agent for Microsoft Windows displays only those backups that meet the following criteria:

1. Backups created at the volume level. File-level backups are not displayed.
2. [For backup repository target] Backups 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 in the backup repository.
3. [For cloud repository target] Backups 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.

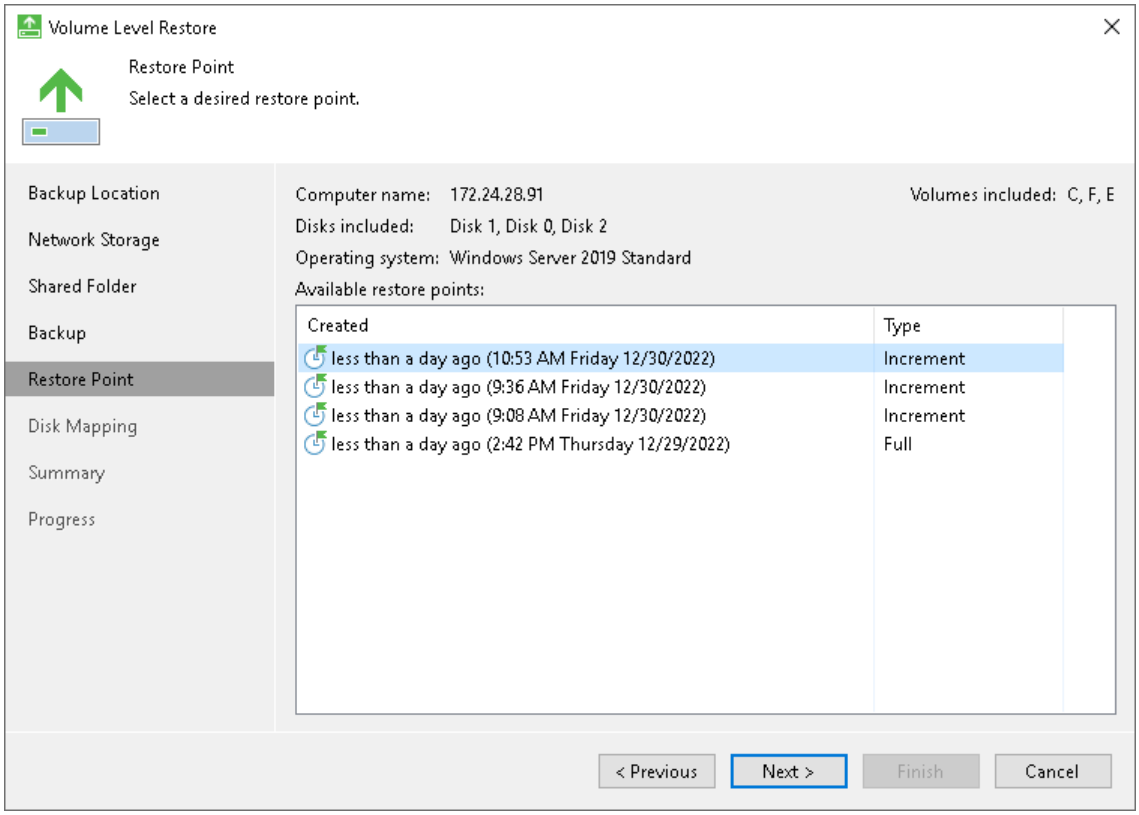

Volume Level Restore
Backup
Specify a backup to restore from. You can type in a few letters of your computer name in the search field to quickly locate the required backup.
Backup Location
Network Storage
Shared Folder
Backup
Restore Point
Disk Mapping
Summary
Progress
Selected computer: 172.24.25.94
Name
Last backup
Restore points
Daily Backup
12/28/2022 1:51 P...
System Backup
12/28/2022 1:57 P...
172.24.25.94
12/28/2022 1:57 P...
4
Weekly Backup
12/28/2022 1:56 P...
Type in an object name to search for
< Previous
Next >
Finish
Cancel

Step 6. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Agent for Microsoft Windows uses the latest restore point. However, you can select any valid restore point to recover volumes to a specific point in time.

Veeam Agent for Microsoft Windows displays restore points for volume-level backups only. For example, if you have run 3 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Agent for Microsoft Windows will display only 3 restore points in the list.



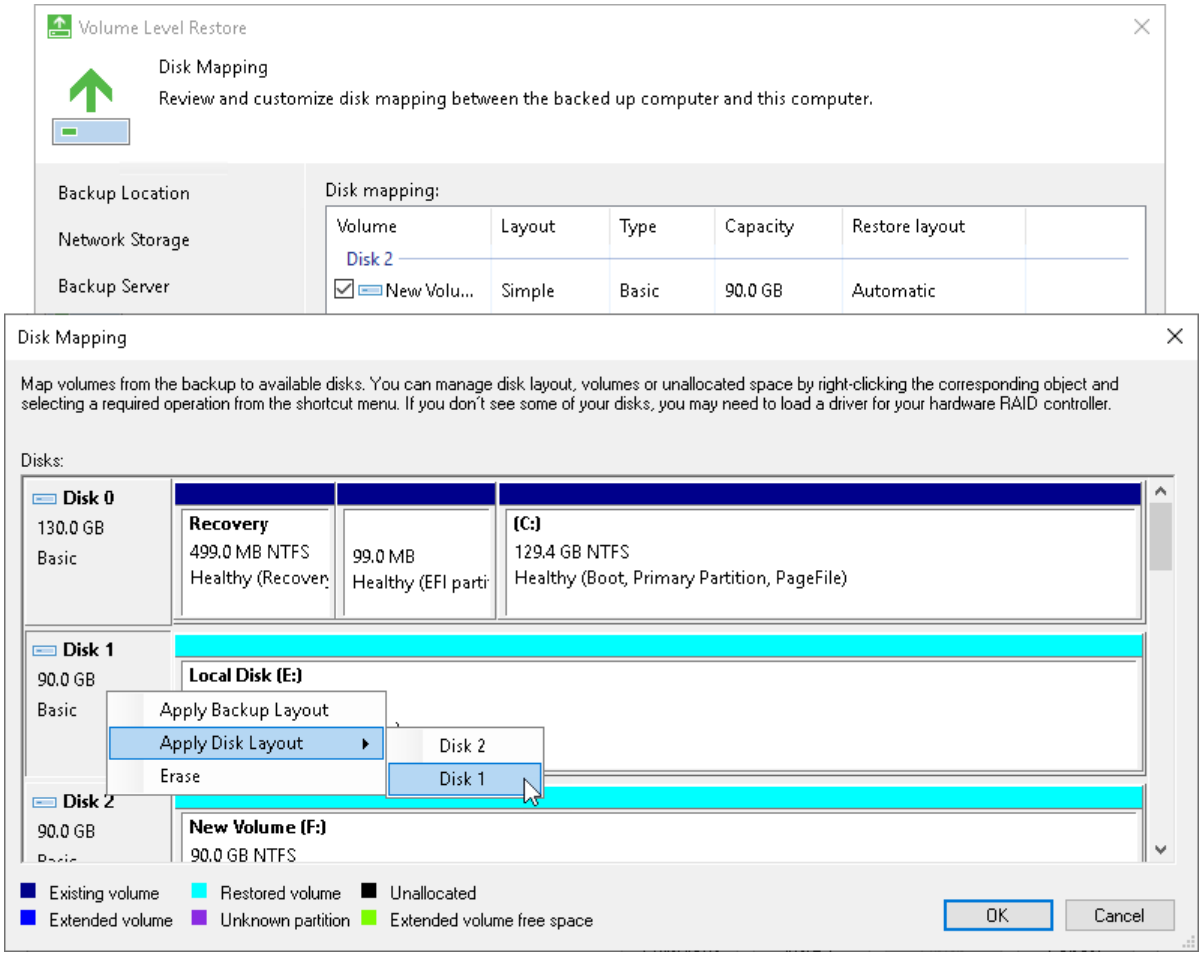
Step 7. Map Restored Disks

At the **Disk Mapping** step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on your computer.

> **IMPORTANT**
>
> We strongly recommend that you change disk mapping settings only if you have experience in working with Microsoft Windows disks and partitions. If you make a mistake, your computer data may get corrupted.

To select volumes to restore:

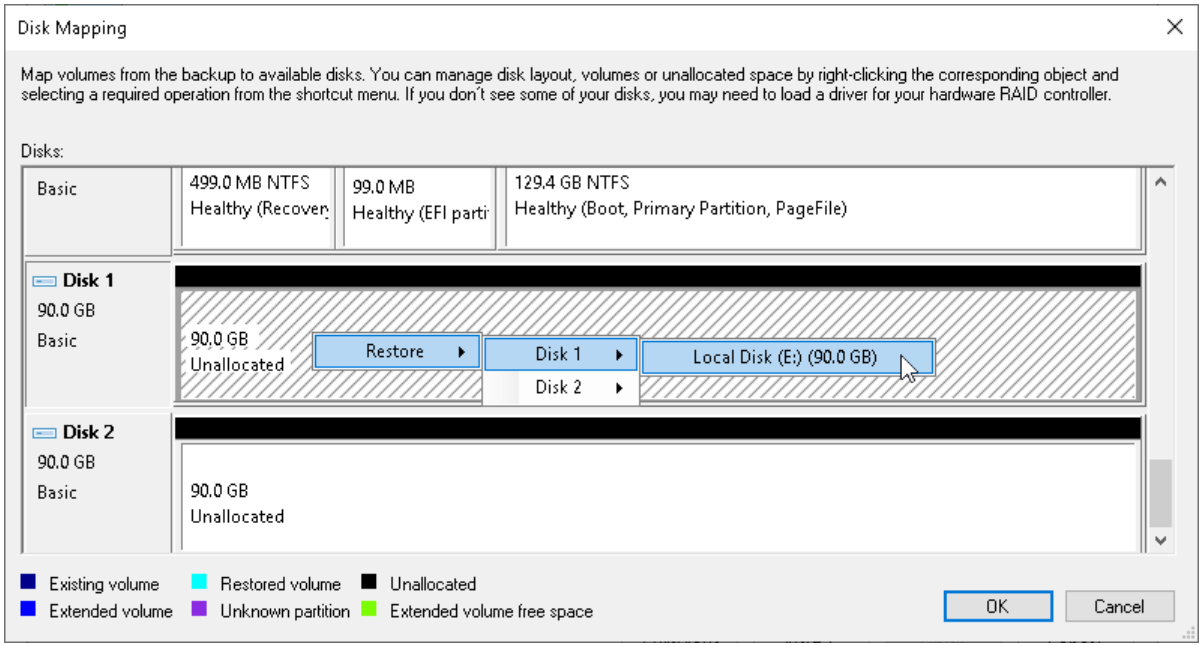
1. Select check boxes next to volumes that you want to restore from the backup.
2. [For restore to a new location] By default, Veeam Agent for Microsoft Windows restores volumes to their initial location. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. To map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**. In the **Disk Mapping** window, specify how volumes must be restored:
    - Right-click the target disk on the left and select the necessary disk layout:
        - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.
        - **Apply Disk Layout** — select this option if you want to apply to the current disk settings of another disk.
        - **Erase** — select this option if you want to discard the current disk settings.



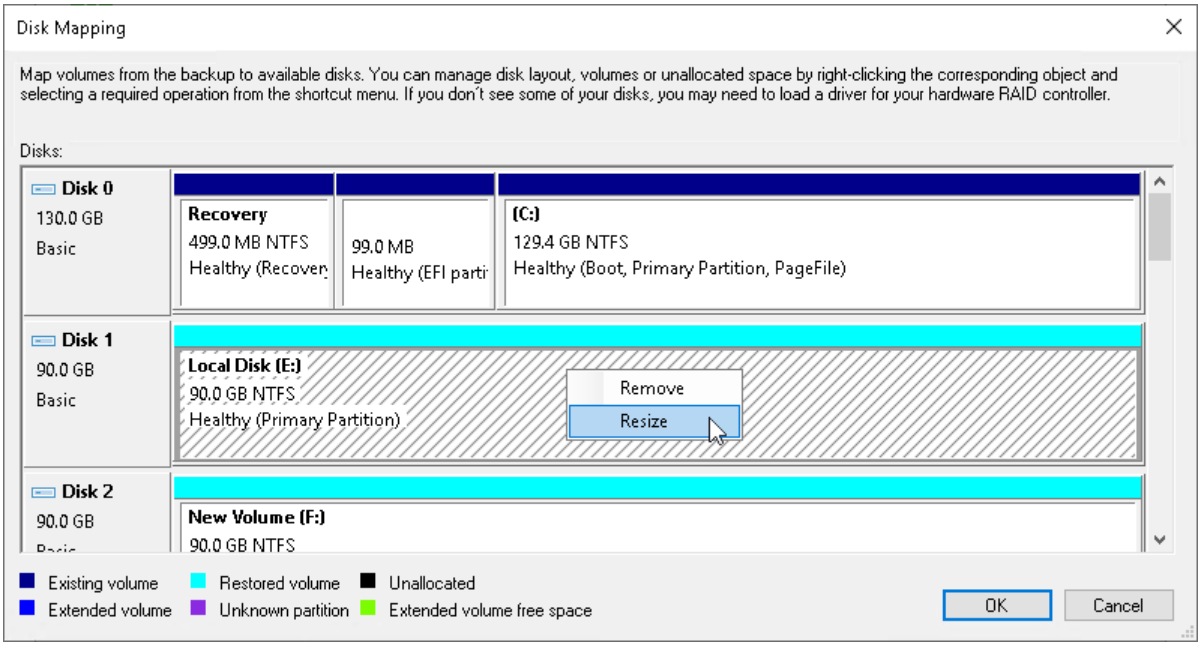
- Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

  If you restore to a dynamic disk, you can specify the type and size of the target volume before mapping. After you select the volume to place on the disk, you will pass to the Allocate Volume window.

  If you want to change disk layout configured by Veeam Agent for Microsoft Windows, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



3. [For restore with volume resize] You can resize a volume mapped by Veeam Agent for Microsoft Windows to a target computer disk. To resize a volume, right-click it in the **Disk Mapping** window and select **Resize**. With this option selected, you will pass to the Volume Resize window.



NOTE

If you map a backup volume that is larger than the amount of available space on the target disk, Veeam Agent for Microsoft Windows will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Agent for Microsoft Windows will prepare to shrink the volume to the size of available disk space.

Allocating Restored Volumes to Dynamic Disks

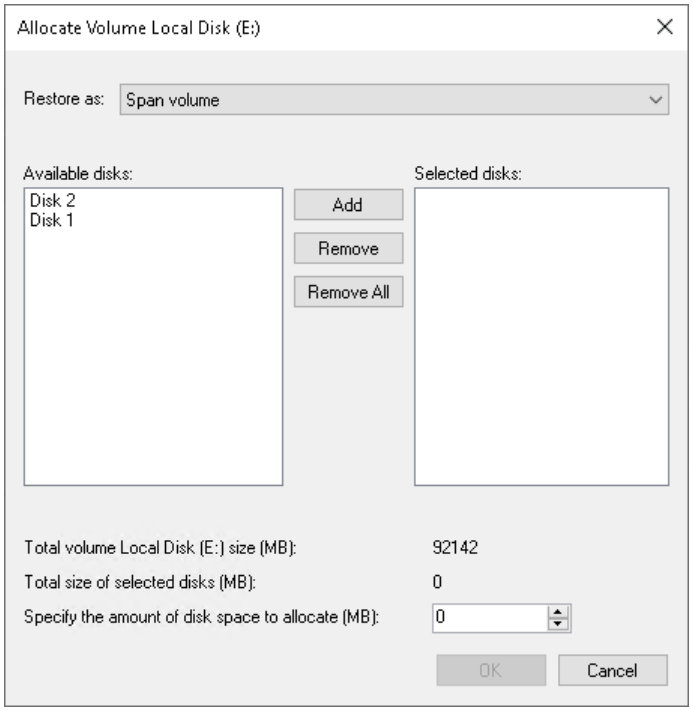
At the **Disk Mapping** step of the wizard, you can set the necessary type and size for the restored volumes. A volume will get the specified type and size during the process of data restore.

You can do this only if all the following conditions are met:

- You restore data to a dynamic disk. To learn more about dynamic volume types, see this Microsoft article.
- At the **Restore Mode** step of the wizard, you have selected the **Manual restore** option.
- At the **Disk Mapping** step of the wizard, you have clicked the **Customize disk mapping** link.

To set volume type and size:

1. Right-click unallocated space of a dynamic disk and select what volume from the backup you want to place on this disk. Veeam Agent for Microsoft Windows will prompt you to set the restored volume type and size.
2. In the **Allocate** window, specify the restored volume type:
    - If you want to restore the volume as a simple volume, from the **Restore as** drop-down list, select the **Simple volume** option and click **OK**.
    - If you want to restore the volume as a spanned, striped, mirrored, or parity volume, from the **Restore as** drop-down list, select the desired option and specify the following settings:
        i. In the **Available disks** list, select volume extents you want to restore. You can add or delete volume extents using the **Add**, **Remove**, and **Remove All** buttons.
        ii. In the **Specify the amount of disk space to allocate** field, specify the total size of restored extents.
        iii. Click **OK**.



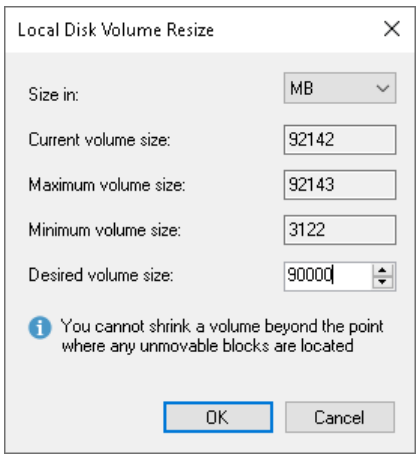
Step 8. Resize Restored Volumes

At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. You can resize a volume if you have chosen to restore data in the *Manual* mode and customize disk layout. A volume will be shrunk or extended to the specified size during the process of data restore.

> **NOTE**
>
> By default, Veeam Agent for Microsoft Windows displays volume size in megabytes (MB). This allows you to specify the desired size for the volume precisely. You can also choose to display volume size in gigabytes (GB). This may be helpful when you need to resize volumes on larger computer disks and want to simplify disk size calculations.
>
> When you use GB as a volume size unit, you can specify volume size with integral numbers, for example, 1 GB, 60 GB or 200 GB, but not 0,8 GB, 60,5 GB or 200,7 GB. However, if the maximum volume size is in fact greater than the displayed value for less than 1 GB, Veeam Agent for Microsoft Windows will automatically add the exceeding amount of disk space to the extended volume. For example, if the maximum volume size is 60,2 GB, Veeam Agent for Microsoft Windows will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Agent for Microsoft Windows will extend the volume to 60,2 GB.

To resize a volume:

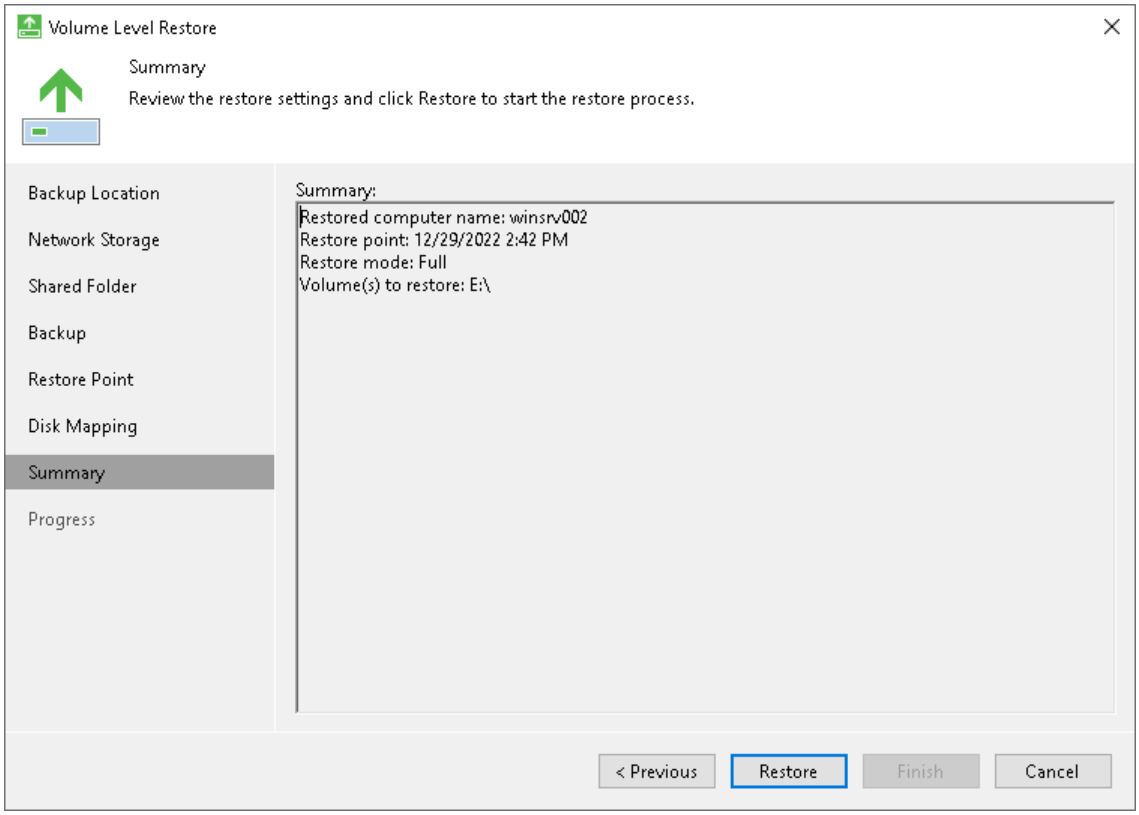
1. Specify a volume you want to resize:
   a. Right-click a restored volume mapped to a target disk and select **Resize**.
   b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Agent for Microsoft Windows will prompt you to shrink the restored volume.
2. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.



Step 9. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of volume-level restore.

1. Review settings of the restore process.
2. Click **Restore** to start the recovery process. Veeam Agent for Microsoft Windows will perform partition re-allocation operations if necessary, restore the necessary volume data from the backup and overwrite volume data on your computer with the restored data.



Restoring Files and Folders

If some files and folders on your computer get lost or corrupted, you can restore them from backups. For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

When you perform file-level restore, Veeam Agent for Microsoft Windows publishes the backup content directly into the computer file system and displays it in the Veeam Backup browser. You can restore files and folders to their initial location, copy files and folders to a new location or target applications to restored files and work with them as usual.

Before You Begin

Before you begin the file-level restore process, check the following prerequisites.

General

- The backup from which you plan to restore data must be successfully created at least once.
- [For backups stored in network shared folders and on backup repositories] You must have access to the target location where the backup file resides.
- [For backup repository targets] If you plan to restore data from a backup stored in a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
- A user account under which you start the restore operation must have administrative privileges on the Veeam Agent computer. If the account under which you are currently logged on to Microsoft Windows does not have administrative privileges, you will be prompted to enter administrator credentials.

> **NOTE**
>
> When you restore files or folders, target EFS settings are applied to the restored objects. For example, if you restore files or folders to a folder encrypted with EFS, the restored objects are encrypted.

ReFS Restore

If you restore files or folders from a ReFS volume-level backup that was made on another machine, the Veeam Agent computer where you perform restore must run the OS that supports the specific ReFS version. For example, you can restore files from a ReFS 3.x volume only to a computer that runs one of the following OSes:

- Microsoft Windows 10 version 1803 or later
- Microsoft Windows Server 2016 or later

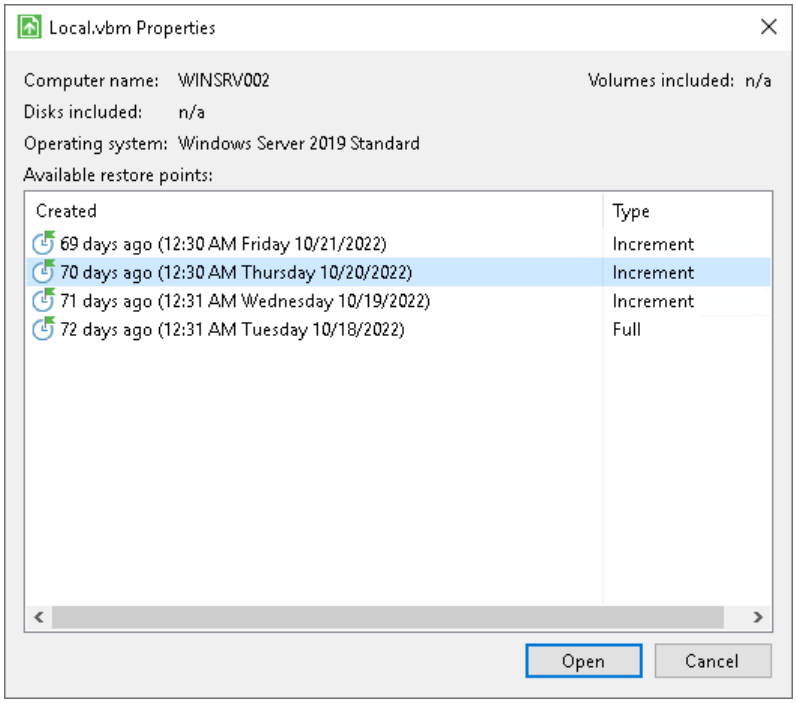
NTFS Restore

- If you restore files or folders from an NTFS volume-level backup that was made on another machine, and data deduplication is enabled for some volumes of the backup, the Veeam Agent computer where you perform restore must run the same OS version or later as the backed-up machine OS.
- If you restore files or folders from an NTFS volume-level backup that was made on another machine, and the allocation unit size of volumes is set to 128K or greater, the Veeam Agent computer where you perform restore must run one of the following OSes:
    - Microsoft Windows 10 version 1803 or later
    - Microsoft Windows Server 2019 or later

Step 1. Launch File Level Restore Wizard

To launch the **File Level Restore** wizard, do either of the following:

- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Restore** > **Individual files**.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**. In the control panel, click a bar of the necessary backup job session. Click **Restore Files** at the bottom of the window. Veeam Agent for Microsoft Windows will automatically publish the backup content into the computer file system and open the Veeam Backup browser.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**. In the main menu, hover over the name of the job that that created the backup from which you want to restore data, and select **Restore file**.
- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **File Level Restore**.
- In Microsoft Windows Explorer, double-click the necessary VBK or VBM file or right-click the file and select **Extract**. In the displayed window, select the restore point from which you want to recover files and click **Open**. Veeam Agent for Microsoft Windows will automatically publish the backup content into the computer file system and open the Veeam Backup browser.

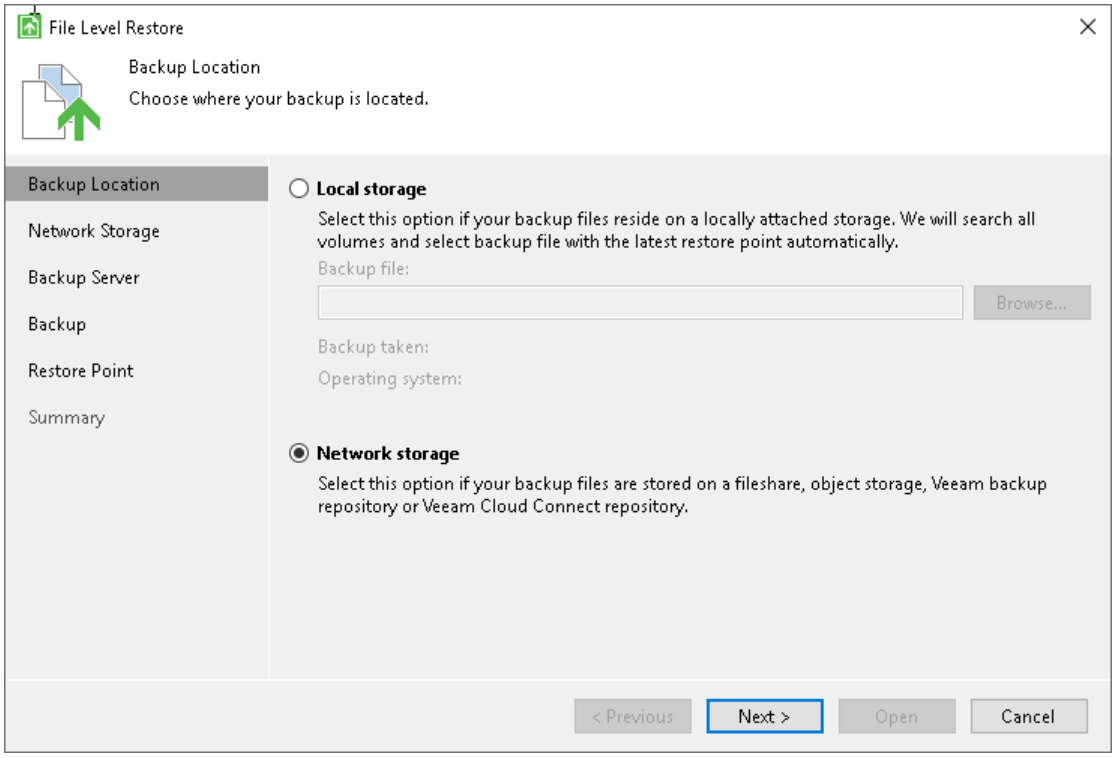


Step 2. Specify Backup File Location

At the **Backup Location** step of the wizard, specify where the backup file that you plan to use for restore resides.

If you configured only one backup job, Veeam Agent automatically locates the latest backup of this backup job on the target storage, and you pass immediately to the Restore Point step of the wizard. If there are several backup jobs configured or Veeam Agent fails to locate the backup for some reason, specify where the backup file resides:

- **Local storage** — select this option if the backup file resides on the computer drive, external drive or removable storage device that is currently connected to your computer. Click **Browse** and select a backup metadata file (VBM).
- **Network storage** — select this option if the backup file resides in object storage, in a network shared folder, in a backup repository managed by a Veeam backup server or in a cloud repository exposed to you by a Veeam Cloud Connect service provider. In this case, the Veeam Recovery Media wizard will include additional steps for specifying the backup file location settings.



Step 3. Select Remote Storage Type

The **Remote Storage** step of the wizard is available if you have chosen to restore data from a backup file that resides in a remote location — in object storage, in a network shared folder, in a backup repository or in a cloud repository.

Specify where the backup file resides:

- **Object storage** — select this option if the backup file is located in object storage. With this option selected, you will pass to the Object Storage step of the wizard.
- **Shared folder** — select this option if the backup file is located in a network shared folder. With this option selected, you will pass to the Shared Folder step of the wizard.
- **Veeam backup repository** — select this option if the backup file 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 the backup file resides in a cloud repository exposed to you by a Veeam Cloud Connect service provider. With this option selected, you will pass to the Service Provider step of the wizard.

Step 4. Specify Remote Storage Settings

Specify settings for the remote storage that contains a backup file from which you plan to restore data:

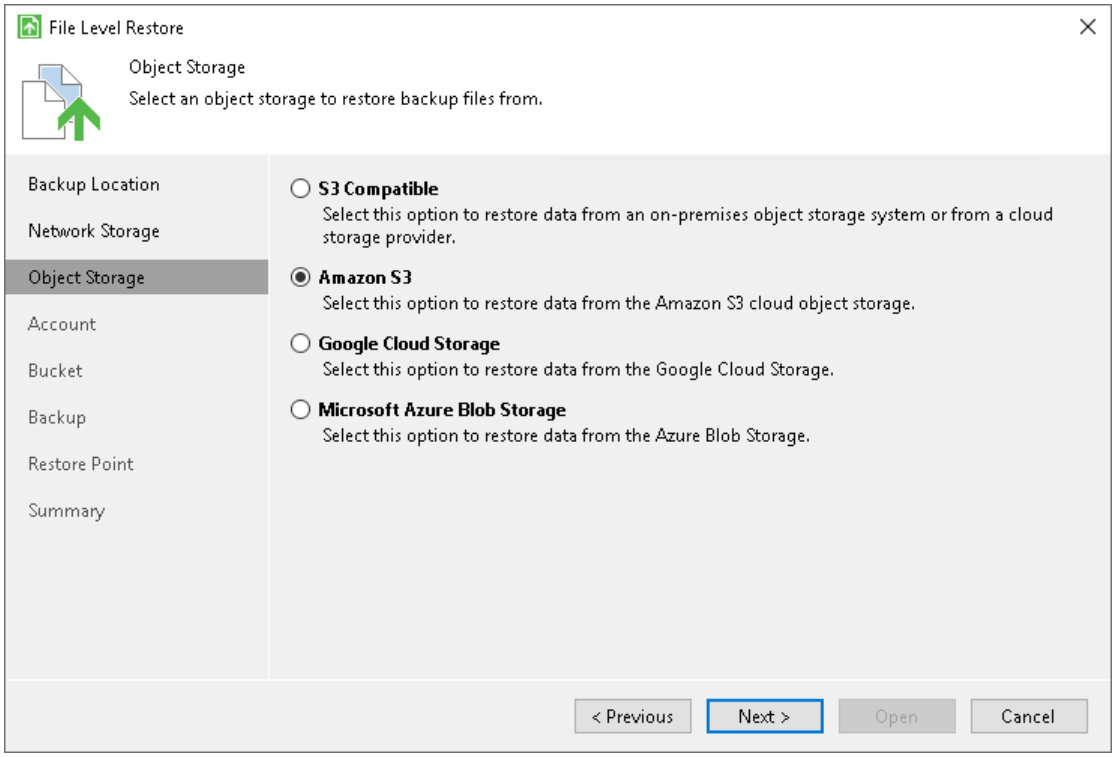
- Object storage settings — if you have selected the **Object storage** option at the Remote Storage step of the wizard.
- Shared folder settings — if you have selected the **Shared folder** option at the Remote Storage step of the wizard.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Remote Storage step of the wizard.
- Veeam Cloud Connect repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Remote Storage step of the wizard.

Object Storage Settings

The **Object Storage** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

Specify settings for the object storage:

- Specify S3 compatible settings.
- Specify Amazon S3 settings.
- Specify Google Cloud Storage settings.
- Specify Microsoft Azure Blob Storage settings.



S3 Compatible Settings

If you have selected to restore data from a backup file located in the S3 compatible storage, specify the following settings:

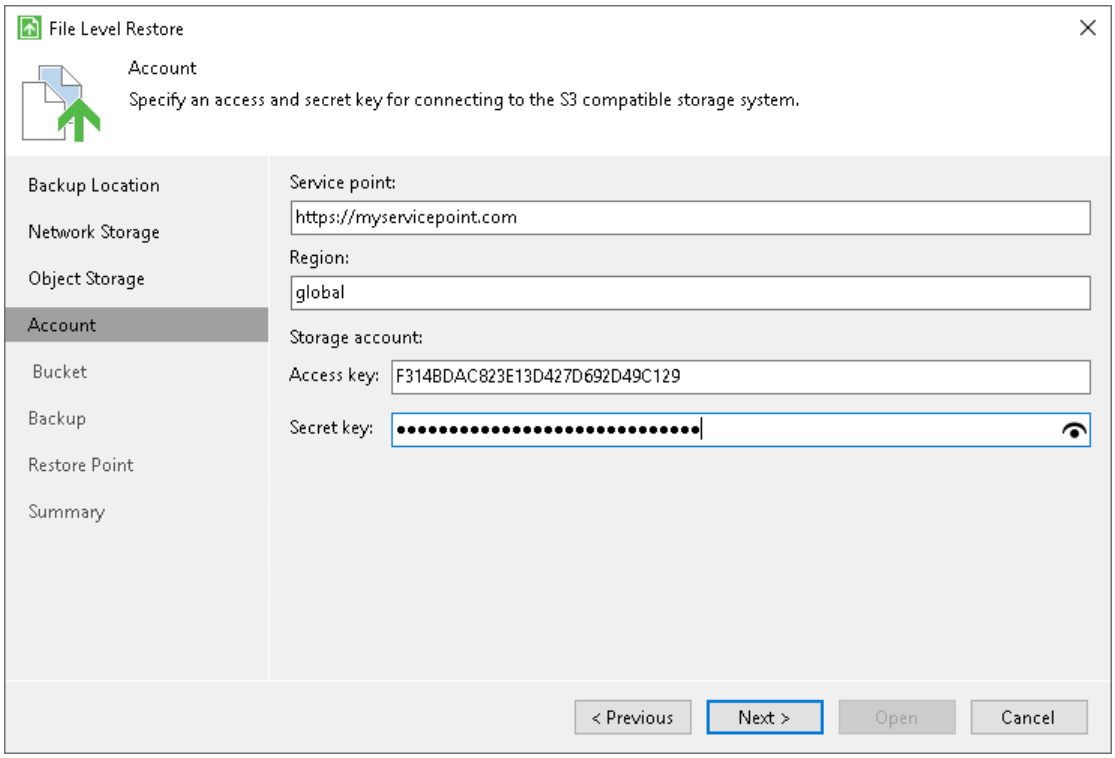
1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Service point** field, specify the address of your S3 compatible storage.
2. In the **Region** field, specify the storage region.
3. In the **Access key** field, enter the access key ID.
4. In the **Secret key** field, enter the secret access key.



Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.

b. In the **Select Bucket** window, do the following:

i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.

ii. Select the necessary bucket and click **OK**.

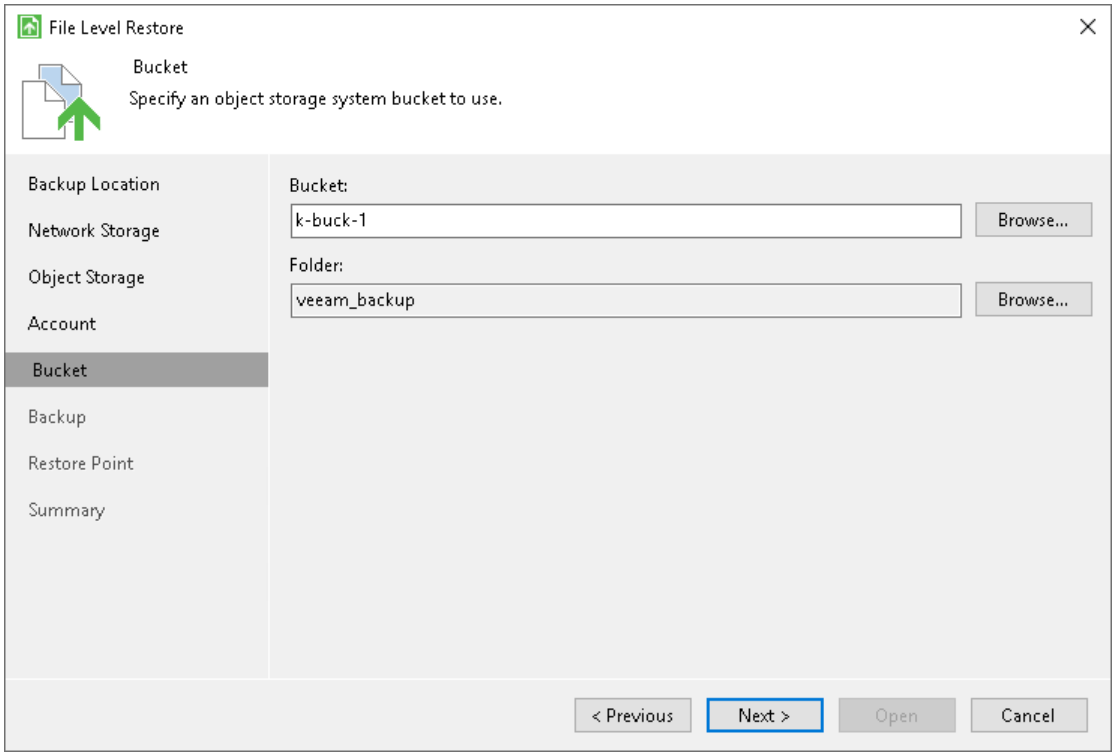
2. In the **Folder** field, specify a folder in the bucket:

a. Select the **Browse** option.

b. In the **Select Folder** window, do the following:

i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.

ii. Select the necessary folder and click **OK**.



Amazon S3 Settings

If you have selected to restore data from a backup file located in the Amazon S3 storage, specify the following settings:

1. Specify account settings.
2. Specify bucket settings.

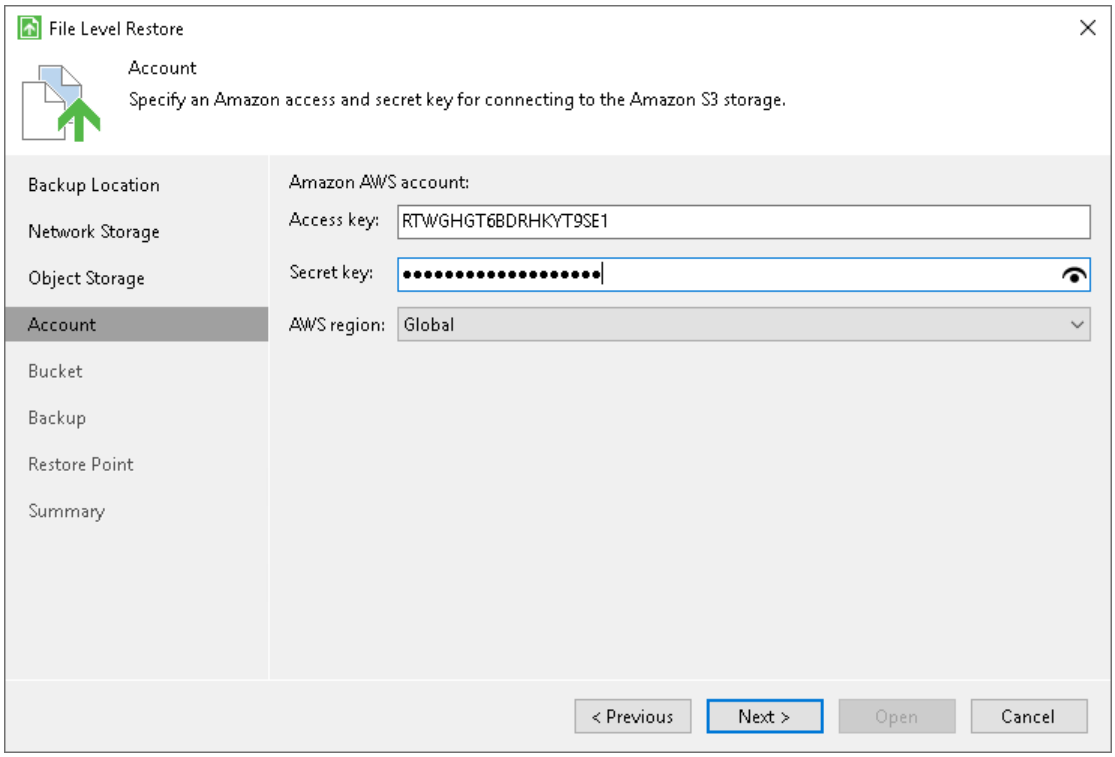
Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

1. In the **Access key** field, enter the access key ID.

2. In the **Secret key** field, enter the secret access key.
3. From the **AWS region** drop-down list, select the AWS region. By default, Veeam Agent uses the **Global** region.

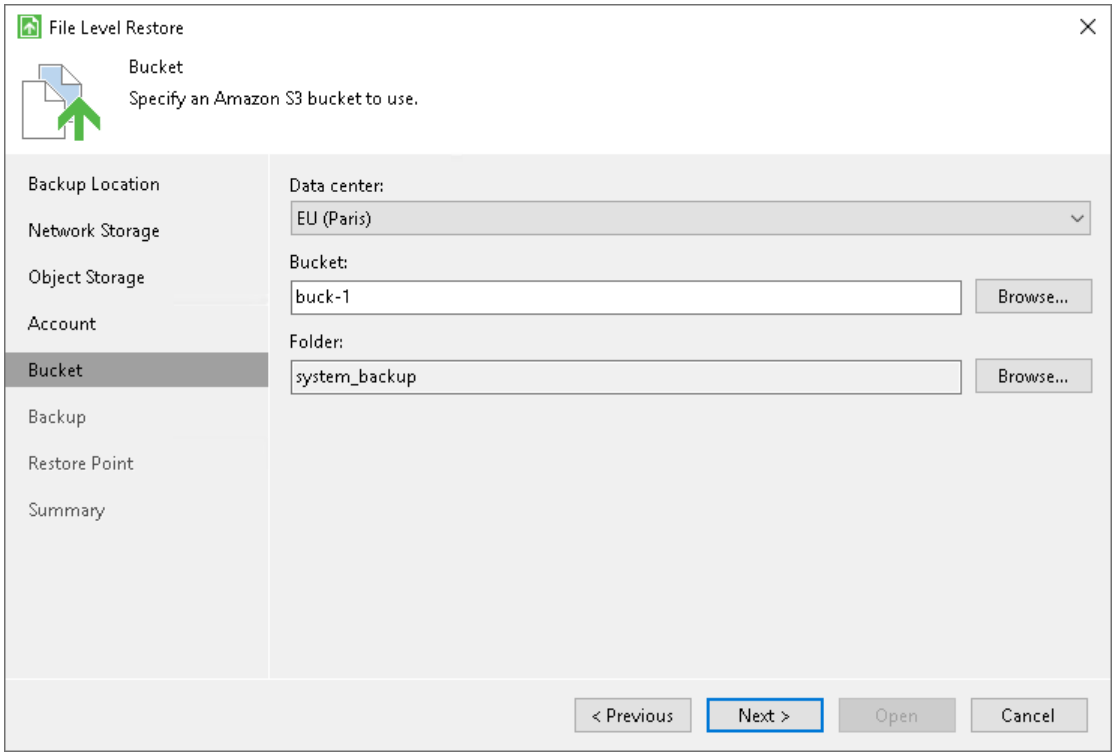


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



Google Cloud Storage Settings

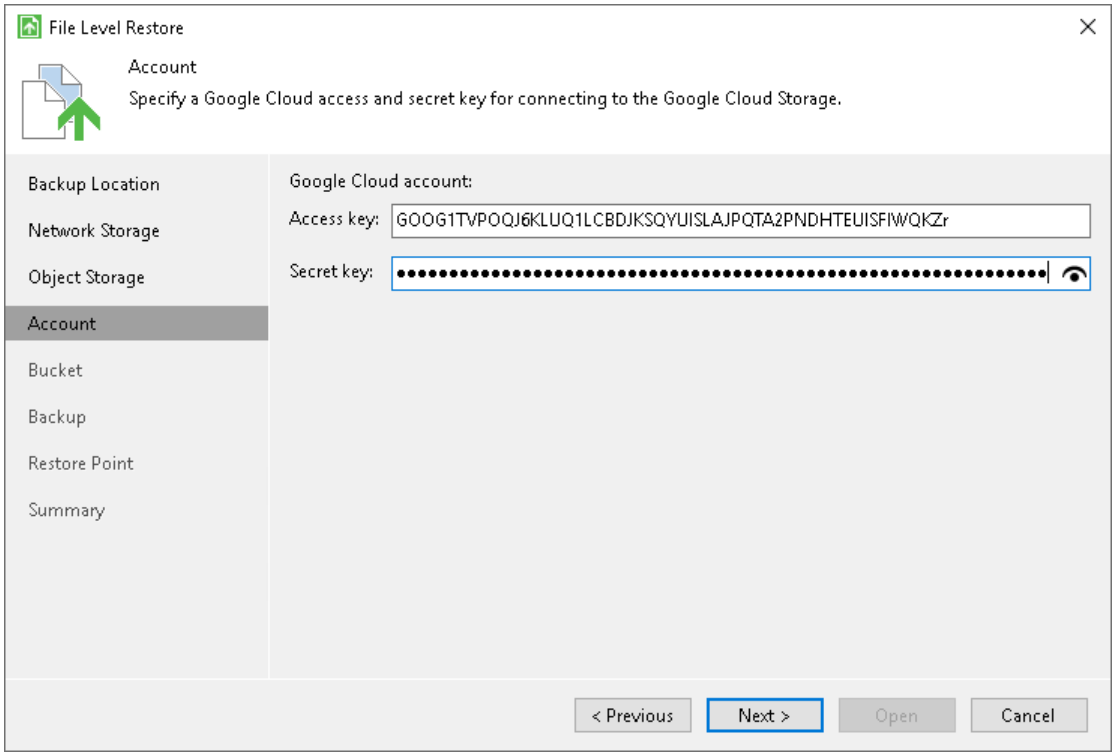
If you have selected to restore data from a backup file located in the Google Cloud storage, specify the following settings:

1. Specify account settings.
2. Specify bucket settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

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

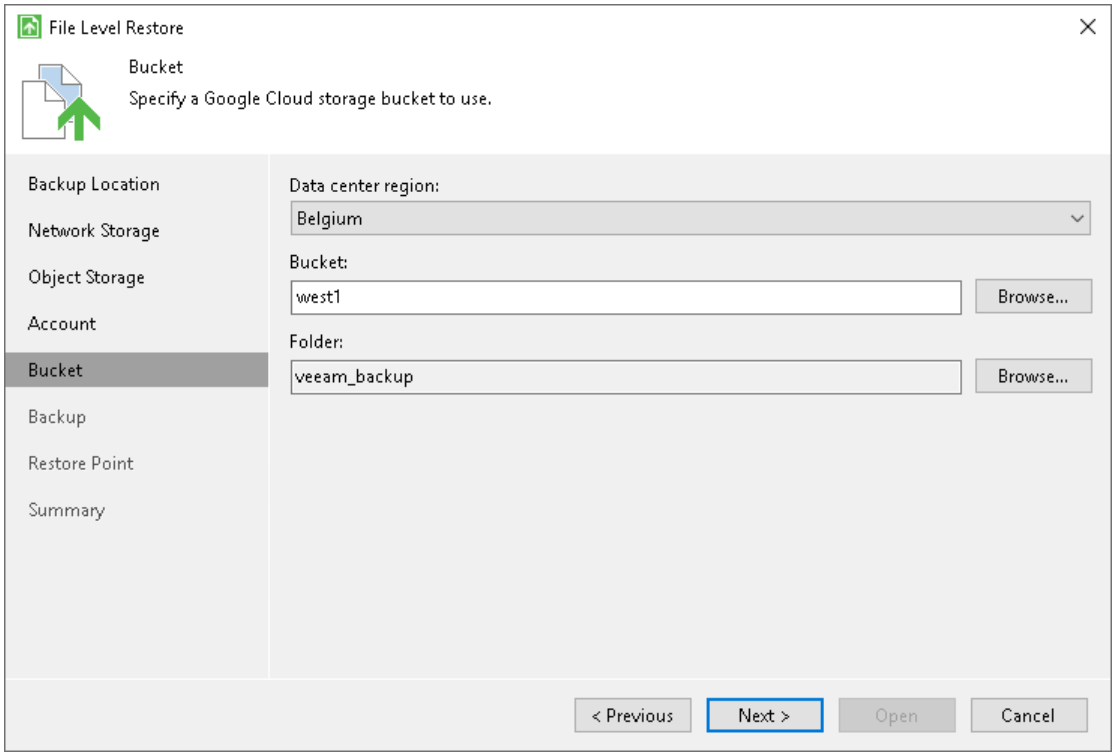


Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to restore data from a backup file located in object storage and specified account settings to connect to the storage.

Specify settings for the bucket in the storage:

1. From the **Data center region** drop-down list, select the geographic region where the backup file is stored.
2. In the **Bucket** field, specify a bucket in the storage:
    a. Select the **Browse** option.
    b. In the **Select Bucket** window, do the following:
        i. Double-click the region name or click the arrow to the left of the region name to view the list of available buckets.
        ii. Select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the bucket name or click the arrow to the left of the bucket name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



Microsoft Azure Blob Storage Settings

If you have selected to restore data from a backup file located in the Microsoft Azure Blob storage, specify the following settings:

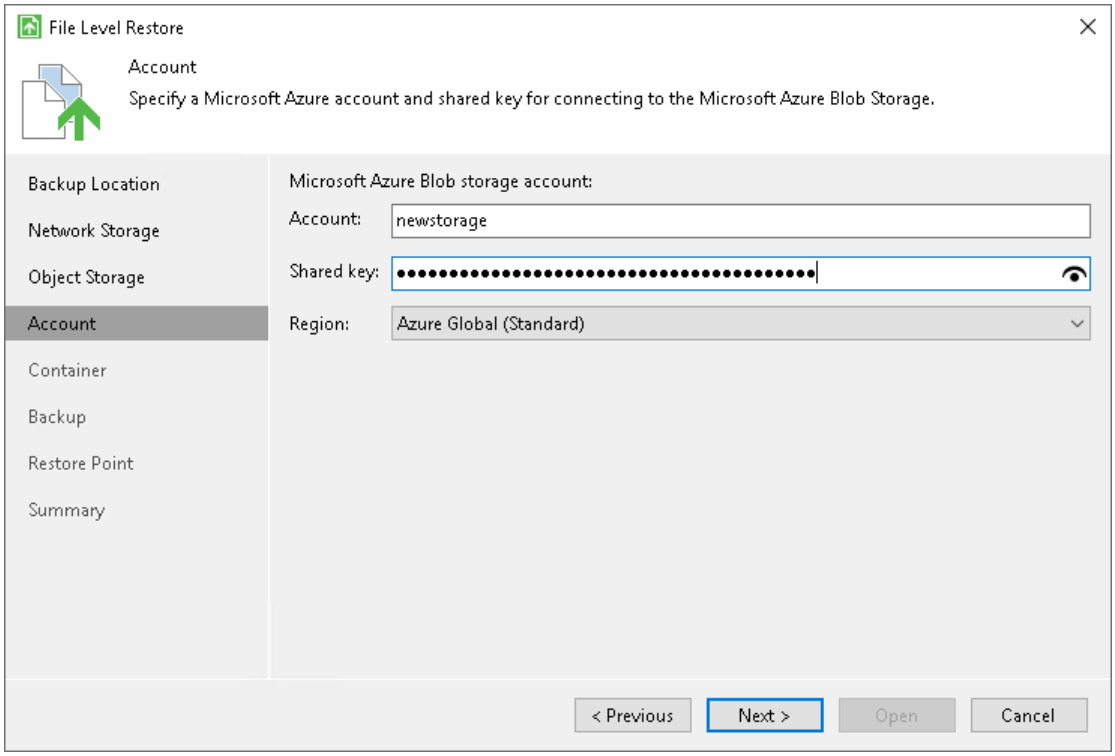
1. Specify account settings.
2. Specify container settings.

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to restore data from a backup file located in object storage.

To connect to the Microsoft Azure Blob 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. From the **Region** drop-down list, select the Microsoft Azure region. By default, Veeam Agent uses the **Azure Global (Standard)** region.

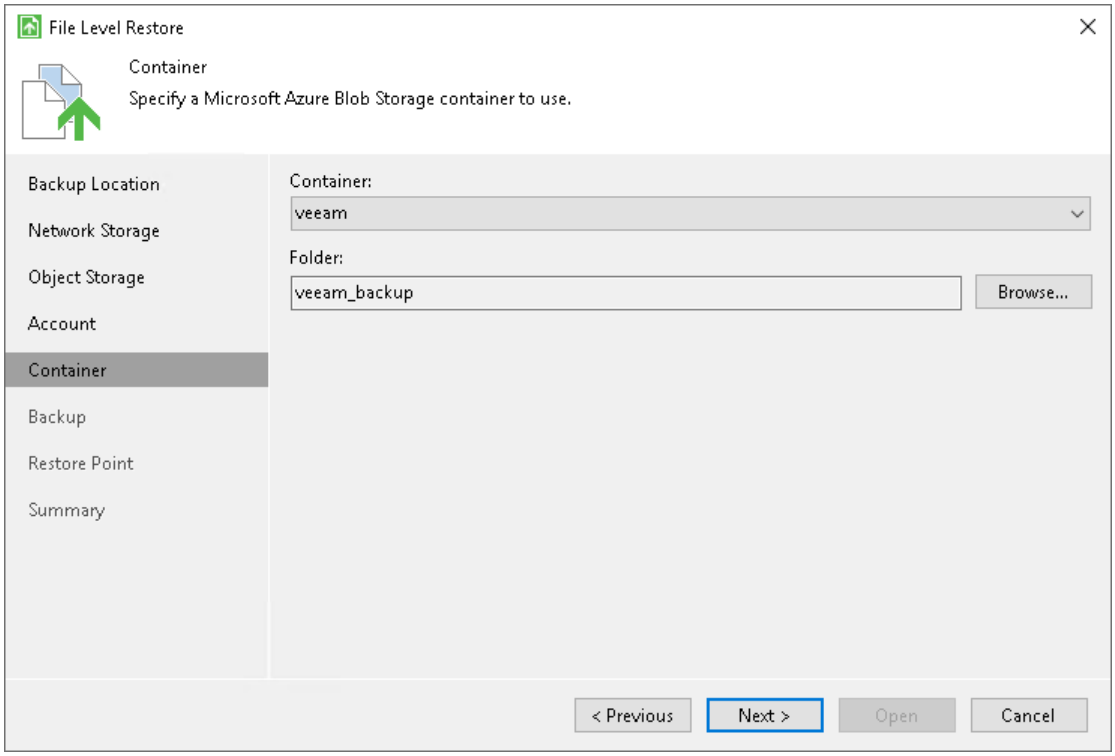


Specifying Container Settings

The **Container** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft Azure Blob storage and specified account settings to connect to the storage.

Specify settings for the container in the storage:

1. From the **Container** drop-down list, select a container in the storage.
2. In the **Folder** field, specify a folder in the container:
    a. Select the **Browse** option.
    b. In the **Select Folder** window, do the following:
        i. Double-click the container name or click the arrow to the left of the container name to view the list of available folders.
        ii. Select the necessary folder and click **OK**.



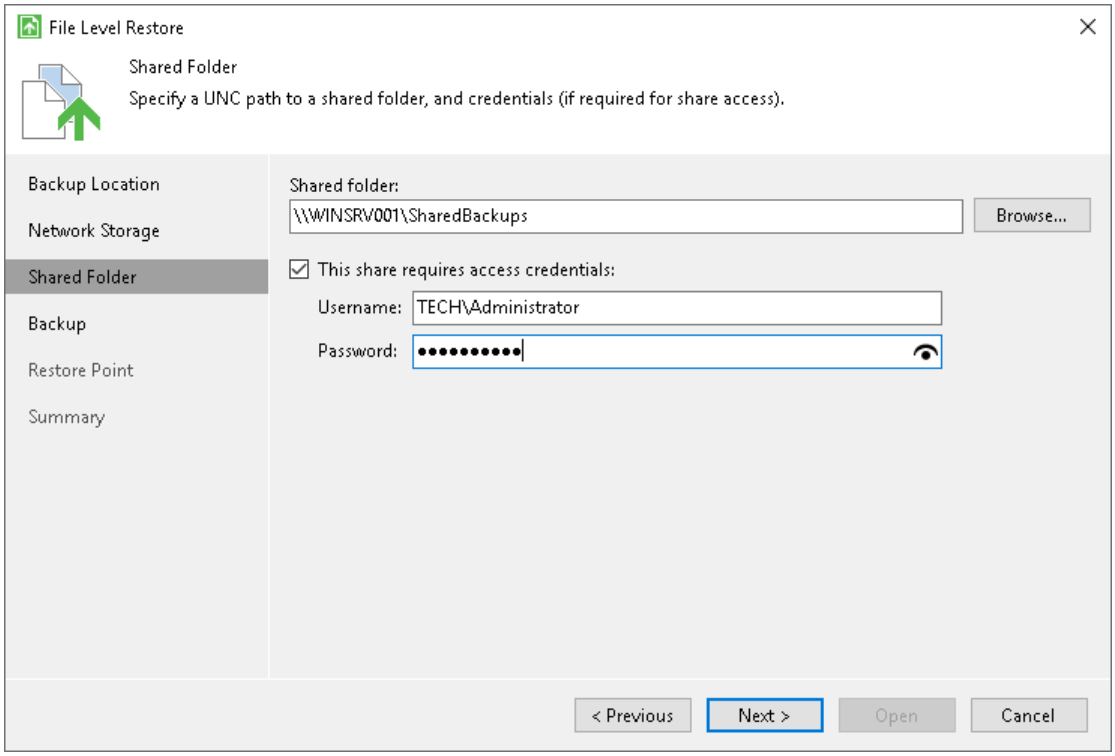
Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have chosen to restore data from a backup file located in a network shared folder.

Specify settings for the network shared folder:

1. In the **Shared folder** field, type in a UNC name of the network shared folder with the backup file. Keep in mind that the UNC name always starts with two back slashes (\\).
2. If the network shared folder requires authentication, select the **This share requires access credentials** check box and specify a user name and password of the account that has *Full Control* access permissions on this shared folder. The user name must be specified in the down-level logon name format. For example, *DOMAIN|UserName* or *HOSTNAME|UserName*.

   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the *NT AUTHORITY|SYSTEM* account of the computer where the product is installed.
3. To view the entered password, click and hold the eye icon on the right of the **Password** field.



Backup Server Settings

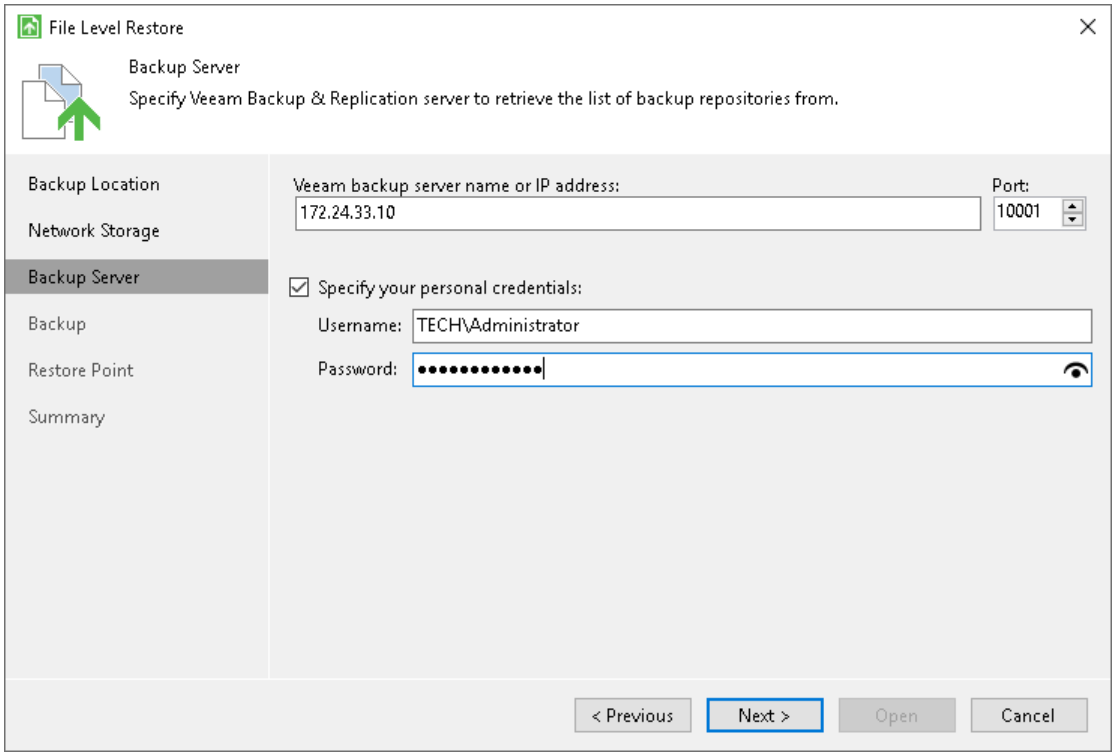
The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located in a backup repository.

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

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup server. By default, Veeam Agent for Microsoft Windows uses port 10001.
3. Select the **Specify your personal credentials** check box. In the **Username** and **Password** fields, enter a user name and password of the account that has access to this backup repository. Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

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

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



Service Provider Settings

If you have selected to restore data from a backup file located on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

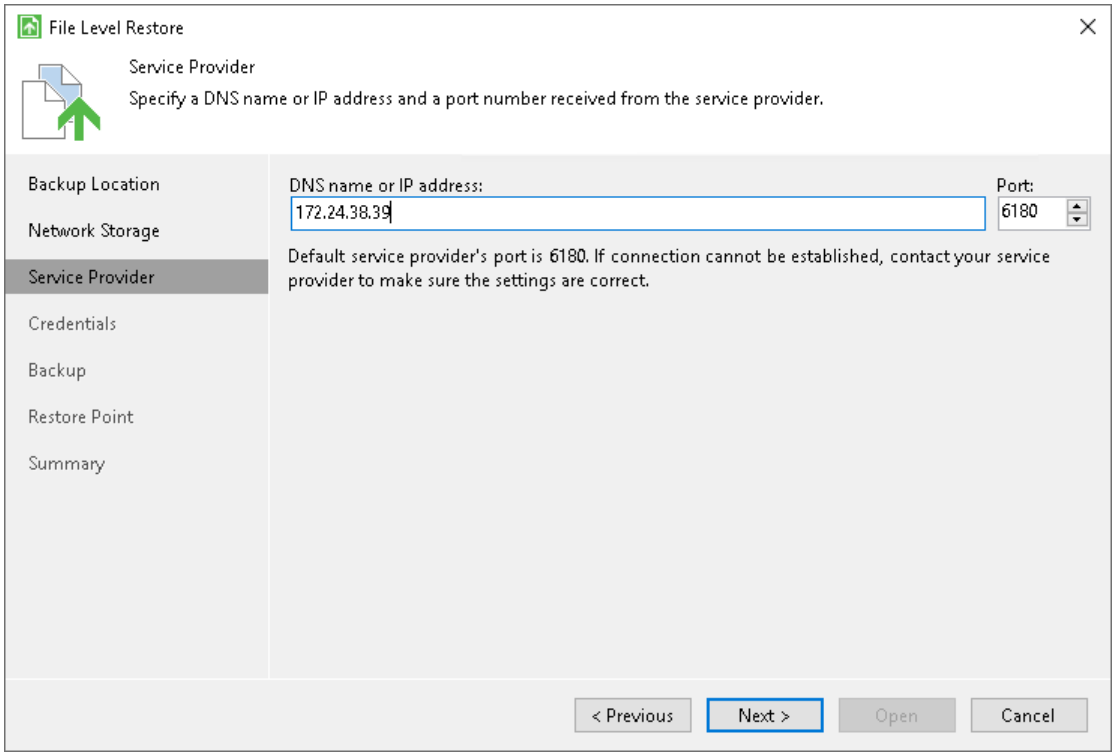
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

Specifying Service Provider Settings

The **Service provider** step of the wizard is available if you have chosen to restore data from a cloud repository exposed to you by a Veeam Cloud Connect service provider.

Specify service provider settings that the 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 for Microsoft Windows will communicate with the cloud gateway. By default, port 6180 is used.



Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to restore data from 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 service provider.

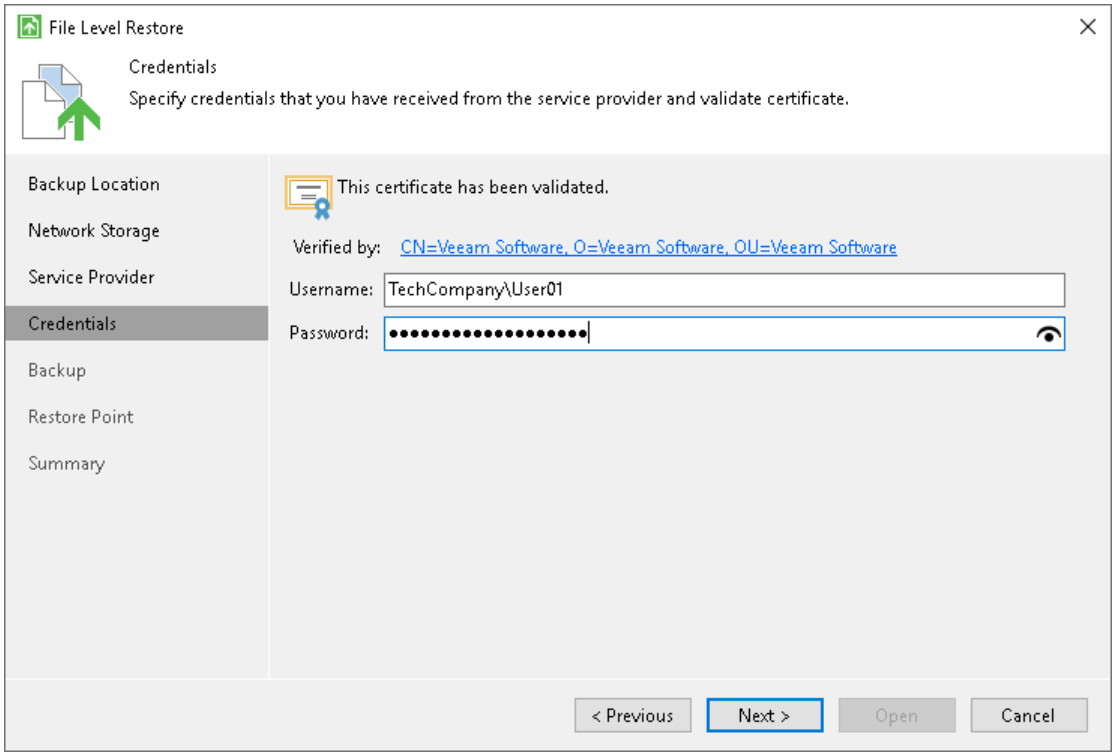
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   - To view the TLS certificate, click the certificate link.
   - To verify if the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Fingerprint for certificate verification** field. Click **Verify**. Veeam Agent for Microsoft Windows will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. In the **Username** field, enter the user name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The user name of the subtenant account must be specified in the *TENANT\SUBTENANT* format.

3. In the **Password** field, provide a password for the tenant or subtenant account.


File Level Restore
Credentials
Specify credentials that you have received from the service provider and validate certificate.
Backup Location
Network Storage
Service Provider
Credentials
Backup
Restore Point
Summary
This certificate has been validated.
Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software
Username: TechCompany\User01
Password: ••••••••••••••••••••
< Previous
Next >
Open
Cancel

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 object storage, in a network shared folder, in a backup repository or in a cloud repository.

From the list of backups, select a backup from which you want to recover data. To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

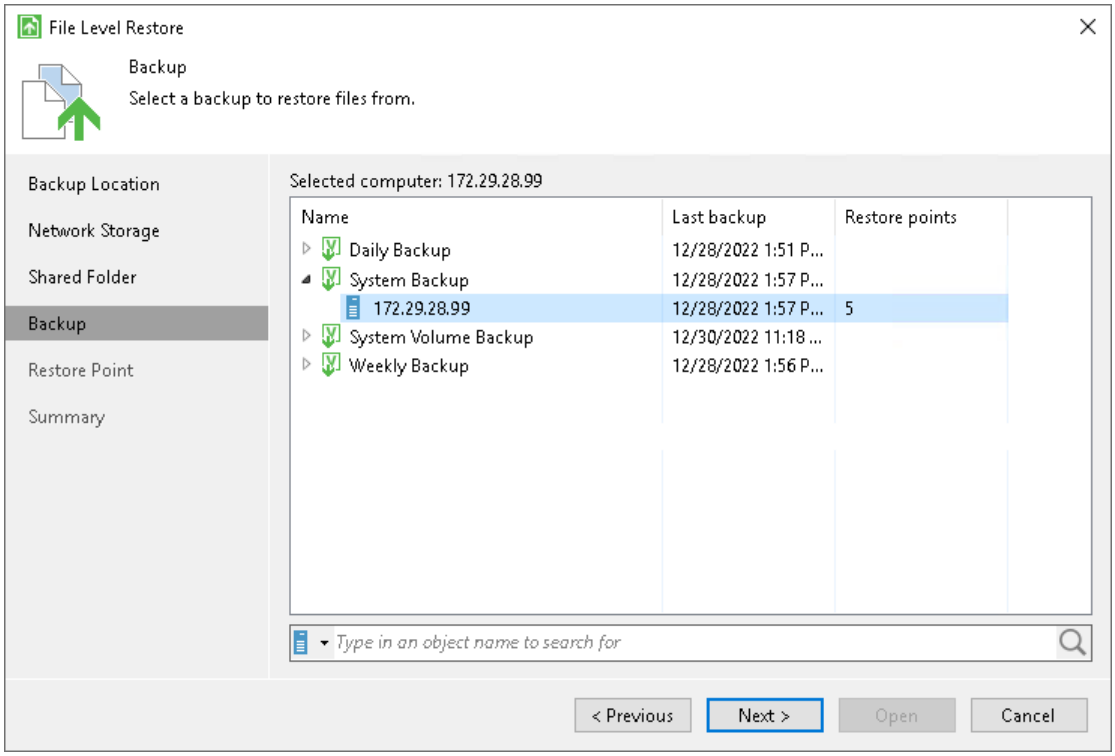
If you restore data from a backup stored in the backup repository, Veeam Agent for Microsoft Windows displays only those backups that are accessible by the user whose credentials are specified at the Backup Server step of the wizard:

- 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 in the backup repository.

If you restore data from a backup stored in the cloud repository, Veeam Agent for Microsoft Windows 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.

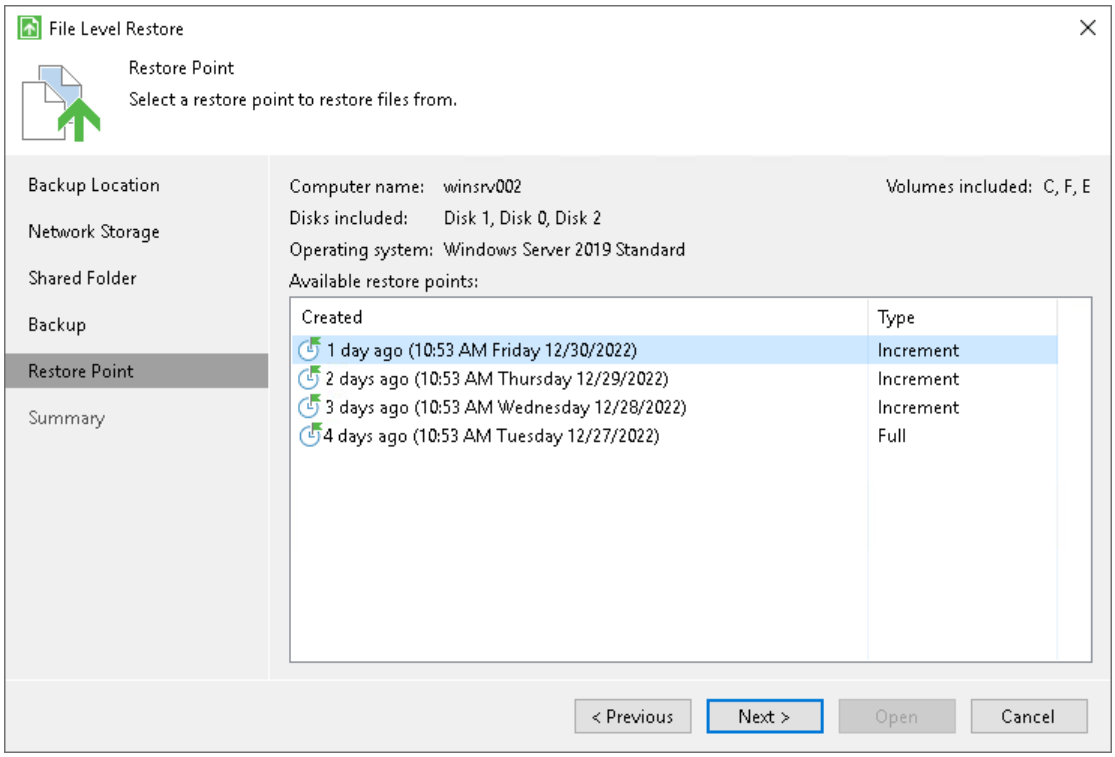
> **NOTE**
>
> If you restore data from an encrypted backup that was created on another Veeam Agent computer, you need to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.


File Level Restore
Backup
Select a backup to restore files from.
Backup Location
Network Storage
Shared Folder
Backup
Restore Point
Summary
Selected computer: 172.29.28.99
Name
Last backup
Restore points
Daily Backup
12/28/2022 1:51 P...
System Backup
12/28/2022 1:57 P...
172.29.28.99
12/28/2022 1:57 P...
5
System Volume Backup
12/30/2022 11:18 ...
Weekly Backup
12/28/2022 1:56 P...
Type in an object name to search for
< Previous
Next >
Open
Cancel

Step 6. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

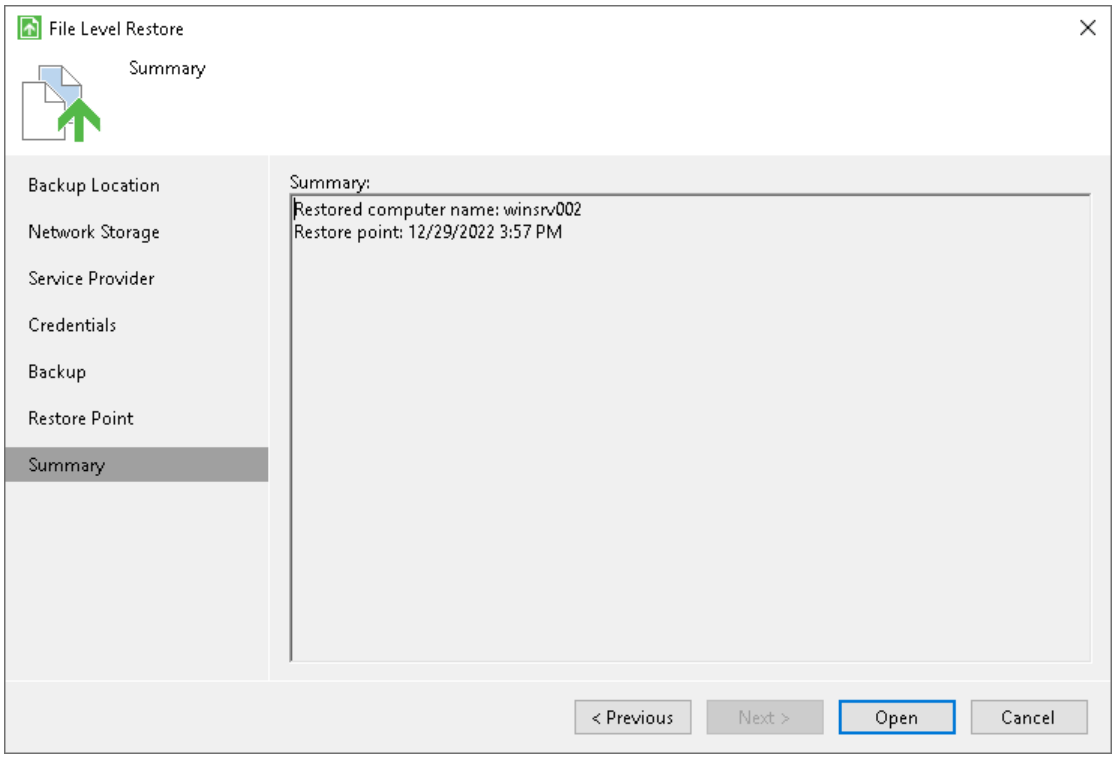
By default, Veeam Agent for Microsoft Windows uses the latest restore point. However, you can select any valid restore point to recover files and folders to a specific point in time.



Step 7. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of file-level restore.

1. Review settings of the restore process.
2. Click **Open**. Veeam Agent for Microsoft Windows will retrieve the content of the backup file, publish it directly into the file system of your computer and display it in the Veeam Backup browser.



Step 8. Save Restored Files

When the restore process is complete, Veeam Agent for Microsoft Windows opens the Veeam Backup browser displaying the content of the backup file.

You can perform the following operations with restored files and folders:

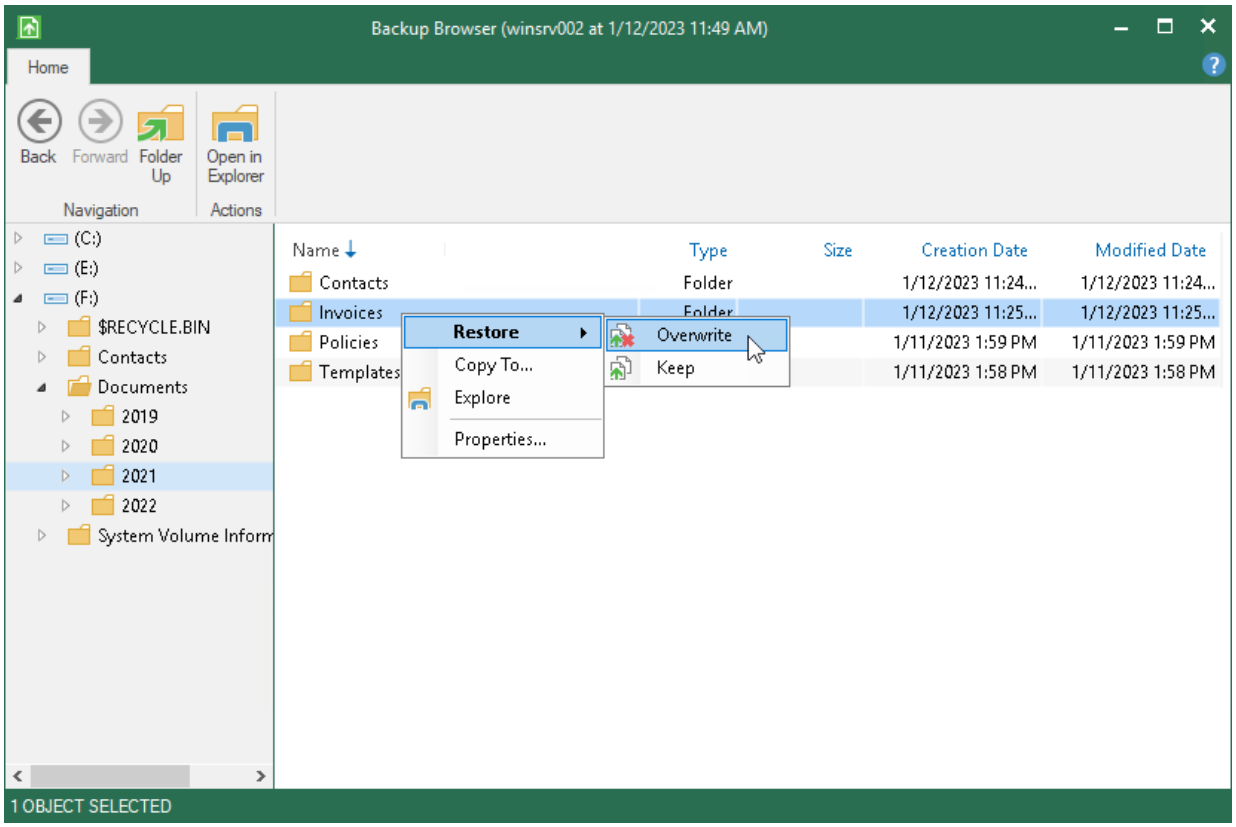
- Save files and folders to their initial location
- Save files and folders to a new location
- Open files in Microsoft Windows Explorer

After you finish working with files and folders, close the Veeam Backup browser.

Saving Files to Initial Location

To save restored files or folders to their initial location, right-click the necessary item in the file system tree or in the details pane on the right and select one of the following commands:

- 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-* prefix to the restored file or folder name and save it in the same location where the original file resides.



Saving Files to New Location

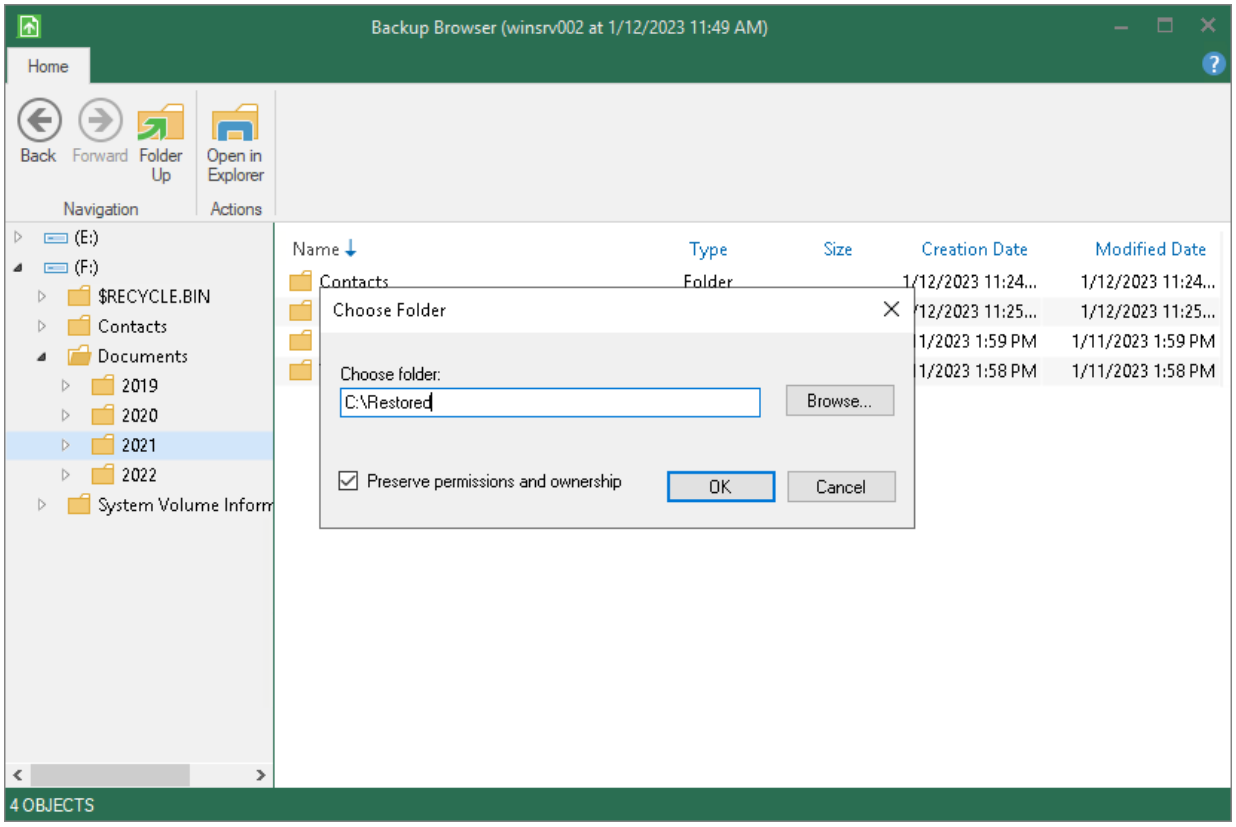
To save restored files or folders on your computer or to a network shared folder, right-click the necessary item in the file system tree or in the details pane on the right and select **Copy To**.

When restoring file objects, you can choose to preserve their original NTFS permissions:

- Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored items. Veeam Agent for Microsoft Windows will copy selected files or folders with associated Access Control Lists, preserving granular access settings.

  If access settings of a file or folder that you want to restore are inherited from a parent folder, when you restore this file or folder without the parent folder, its access settings will not be preserved.

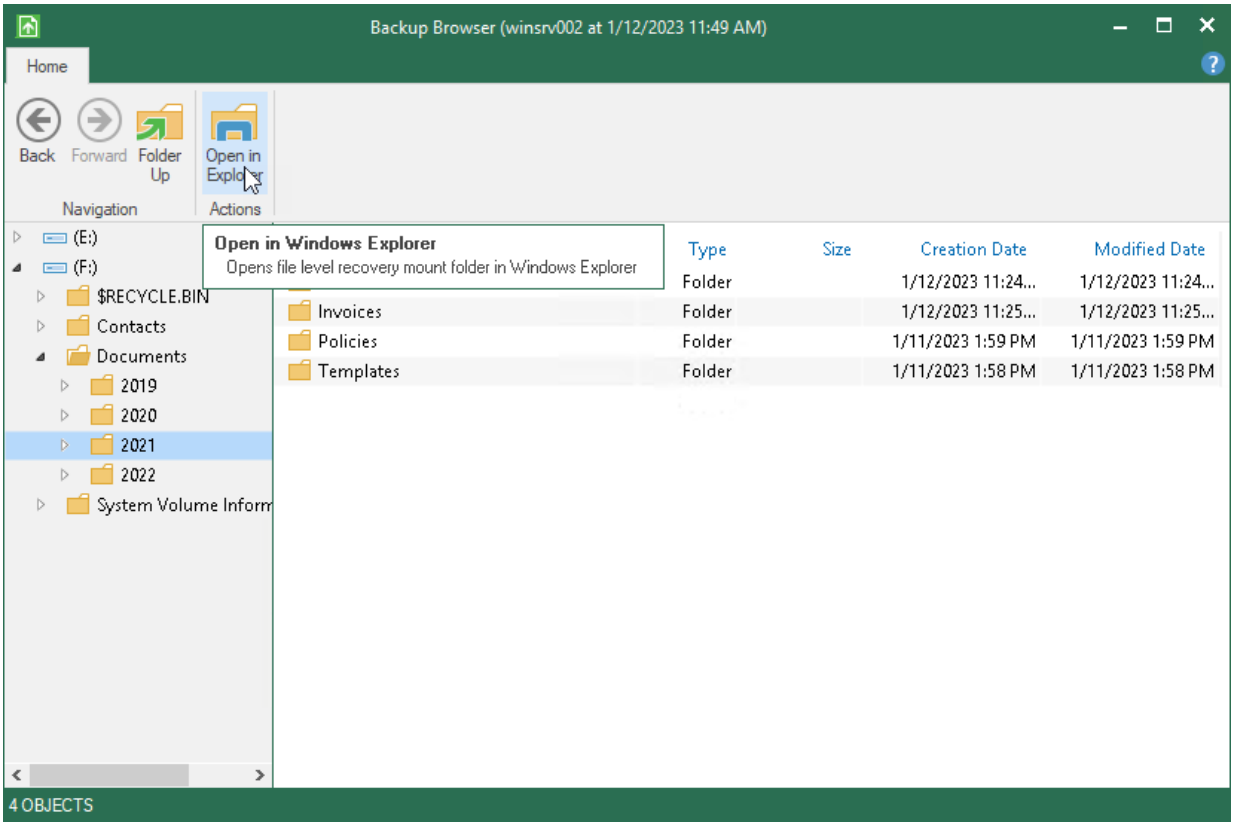
- Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored items. Veeam Agent for Microsoft Windows will change security settings: the user who launched the Veeam Agent for Microsoft Windows will be set as the owner of the restored items. Access permissions will be inherited from the folder to which the restored items are copied.



Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders. To do this, do either of the following:

- In Veeam Backup browser, select the necessary file or folder and click **Open in Explorer** on the toolbar. Veeam Agent for Microsoft Windows will open the selected folder or file in Microsoft Windows Explorer.
- Open Microsoft Windows Explorer and browse for restored files and folders. The backup content is mounted under the `C:\VeeamFLR\ServerName` folder.



We recommend that you use the Veeam Backup browser instead of Microsoft Windows Explorer for file-level restore. Use of the Veeam Backup browser has the following advantages:

1. You can browse the guest OS file system ignoring the file system ACL settings.
2. You can preserve permissions and ownership during file-level restore.

If you open the file system through the Microsoft Windows Explorer, these capabilities will not be available.

To learn more, see *SeBackupPrivilege* and *SeRestorePrivilege* in this Microsoft article.

Elevating Access Rights

You can switch to another system user with the Veeam Backup browser. This may be helpful when you work under an account that does not have Administrator privileges and do not have the access rights to restore the file you need.

To switch the user, do the following:

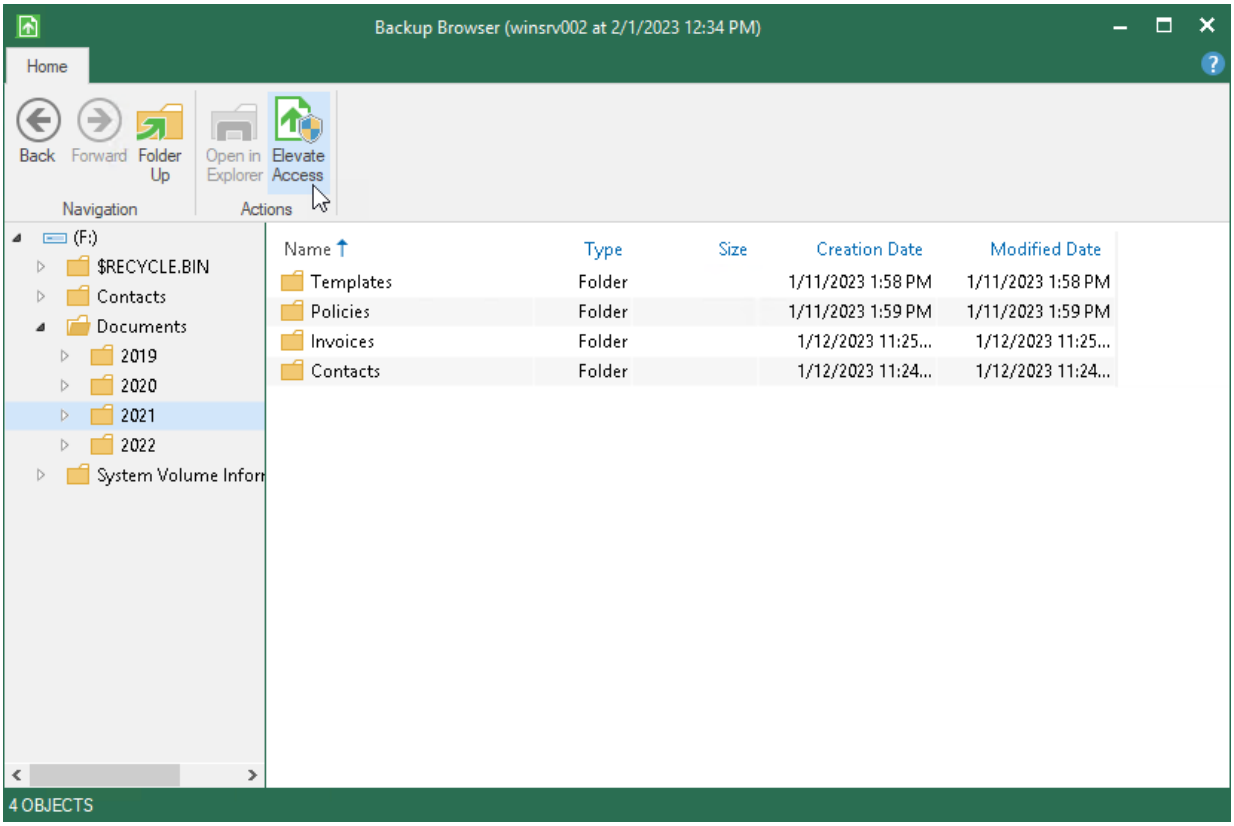
1. Open the **File Level Restore** wizard from the Veeam Agent control panel.
2. In Veeam Backup browser, click **Elevate Access** on the toolbar.

   Keep in mind that Veeam Agent displays the **Elevate Access** button only if you work under an account without Administrator privileges. To allow users without Administrator privileges to open the Veeam Backup browser and restore from the file-level backup, do one of the following:

   - If Veeam Agent operates in the standalone mode, use a registry value. For more information, contact Veeam Customer Support.
   - If Veeam Agent operates in the managed mode, use the Veeam Backup & Replication console. For more information, see the Veeam Agent for Microsoft Windows Settings section in the Veeam Agent Management Guide.

3. In the dialog window, provide credentials of the system user you need.

After that, Veeam Agent restarts the Veeam Backup browser with the updated access rights.



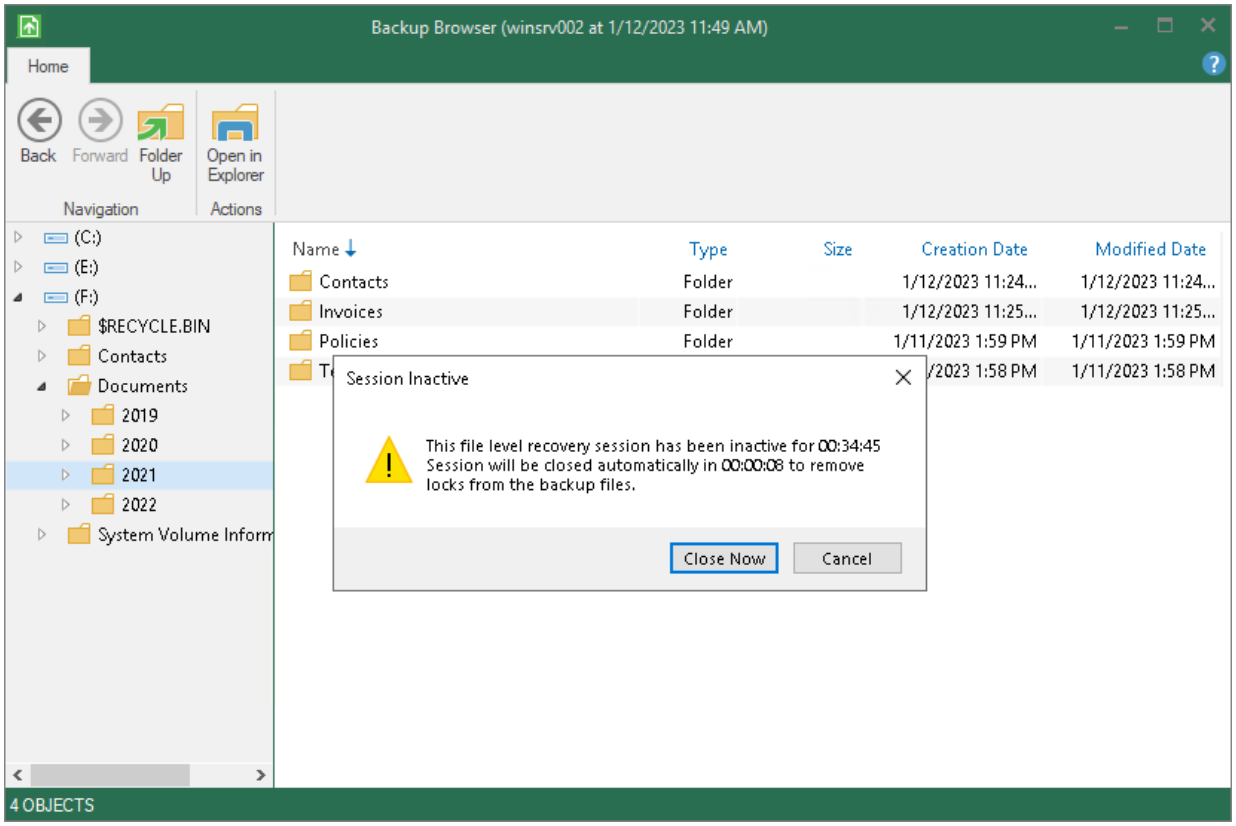
Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows displays a warning that the Veeam Backup browser is to be closed within 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 30 minutes. After this period expires, Veeam Agent for Microsoft Windows will display the warning again.
- You can perform no action at all. In this case, the Veeam backup browser will be automatically closed in 5 minutes.


Backup Browser (winsrv002 at 1/12/2023 11:49 AM)
Home
Back
Forward
Folder Up
Open in Explorer
Navigation
Actions
(C:)
(E:)
(F:)
$RECYCLE.BIN
Contacts
Documents
2019
2020
2021
2022
System Volume Inform
Name
Type
Size
Creation Date
Modified Date
Contacts
Folder
1/12/2023 11:24...
1/12/2023 11:24...
Invoices
Folder
1/12/2023 11:25...
1/12/2023 11:25...
Policies
Folder
1/11/2023 1:59 PM
1/11/2023 1:59 PM
/2023 1:58 PM
1/11/2023 1:58 PM
Session Inactive
This file level recovery session has been inactive for 00:34:45
Session will be closed automatically in 00:00:08 to remove locks from the backup files.
Close Now
Cancel
4 OBJECTS

Restoring Data from Encrypted Backups

When you restore data from an encrypted backup, Veeam Agent for Microsoft Windows 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 for Microsoft Windows database, you do not need to specify the password. Veeam Agent for Microsoft Windows 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.

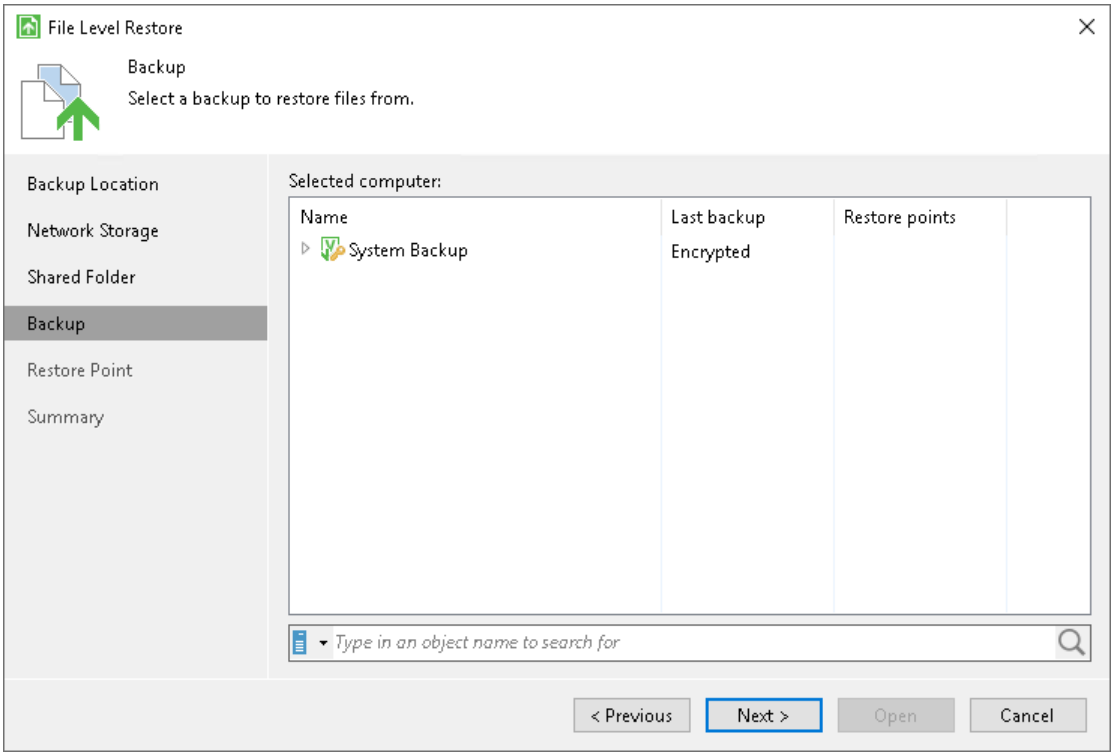
  Automatic data decryption can be performed in one of the following situations:

  - You encrypt and decrypt the backup file on the same Veeam Agent computer using the same Veeam Agent for Microsoft Windows database.
  - You have included encryption keys into the Veeam Recovery Media and perform bare metal recovery after booting from this Veeam Recovery Media. To learn more, see Specify Recovery Media Options.

- If encryption keys are not available in the Veeam Agent for Microsoft Windows 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 for Microsoft Windows, you can use the latest password to restore data form all restore points in the backup chain, including restore points that were encrypted with an old password and restore points that were created before you have enabled the encryption option for the job.

To decrypt a backup file:

1. Launch the necessary data restore wizard:
   - If you want to perform file-level or volume-level restore from an encrypted backup that was created on another Veeam Agent computer, right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Restore** > **Individual files** or **Restore** > **Entire volumes**. To learn more, see Restoring Files and Folders and Restoring Volumes.
   - If you want to perform bare metal recovery from an encrypted backup, boot from the Veeam Recovery Media and launch the **Veeam Recovery Media** wizard. To learn more, see Restoring from Veeam Recovery Media.
2. At the **Backup Location** step of the wizard, specify where the encrypted backup file that you plan to use for restore resides. If the backup file resides in a remote location, at subsequent steps of the wizards, select the backup location type and specify settings to connect to the backup location.
3. At the **Backup** step of the wizard, select the encrypted backup.

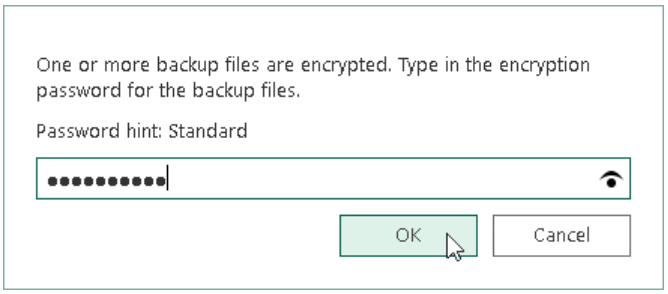


4. Veeam Agent for Microsoft Windows will display the **Specify Password** window. In the **Hint** field of the **Specify Password** window, Veeam Agent for Microsoft Windows displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.

5. 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. In Veeam Agent for Microsoft Windows, you can use the latest password to restore data form all restore points in the backup chain, including those restore points that were encrypted with an old password.

   If you enter correct password, Veeam Agent for Microsoft Windows will decrypt the backup metadata. You will be able to pass to the Restore Point step of the wizard and continue the restore operation in a regular manner.



Reporting

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

- You can view information about performed backups in the Control Panel.
- You can get information about the backup state using the Veeam Agent for Microsoft Windows tray agent.
- You can get information about the backup progress using the Veeam Agent for Microsoft Windows taskbar button.
- You can get information about Veeam Agent for Microsoft Windows events using the events bar in the Control Panel.
- You can get information about Veeam Agent for Microsoft Windows events using Windows Notification Center.
- You can get information about performed backups in email reports.

Viewing Statistics in Control Panel

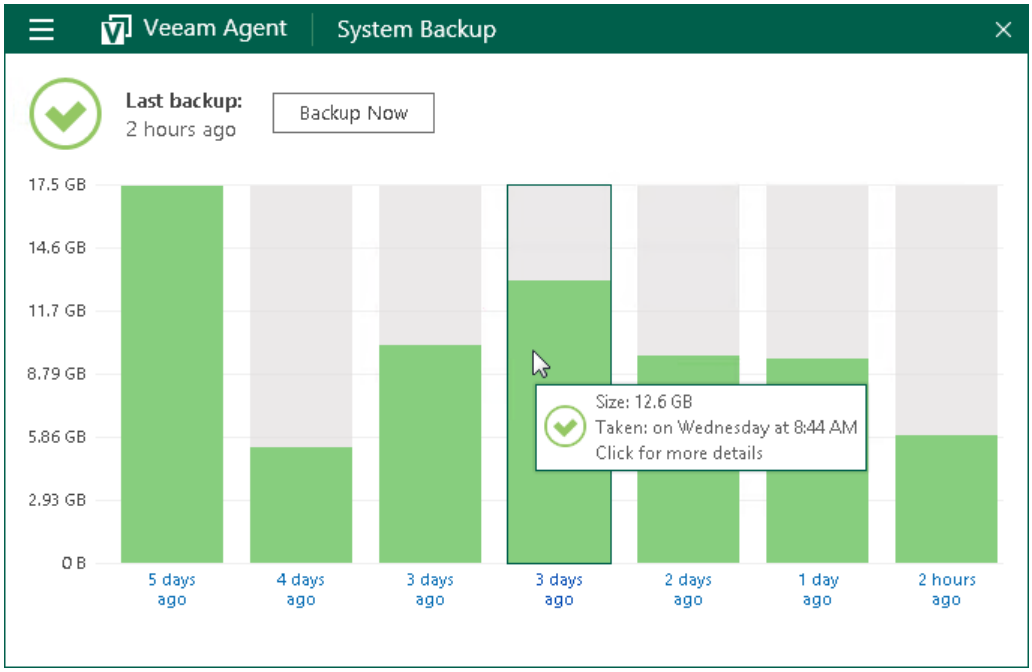
You can use the Veeam Agent control panel to view statistics about performed backups. To open the Control Panel, do either of the following:

- Double-click the Veeam Agent icon in the system tray.
- Right-click the Veeam Agent icon in the system tray and select **Control Panel**.

For every configured backup job, Veeam Agent displays statistics in a separate view in the control panel. To identify the job whose statistics is currently displayed in the Control Panel, check the name of the job at the top of the Control Panel window.

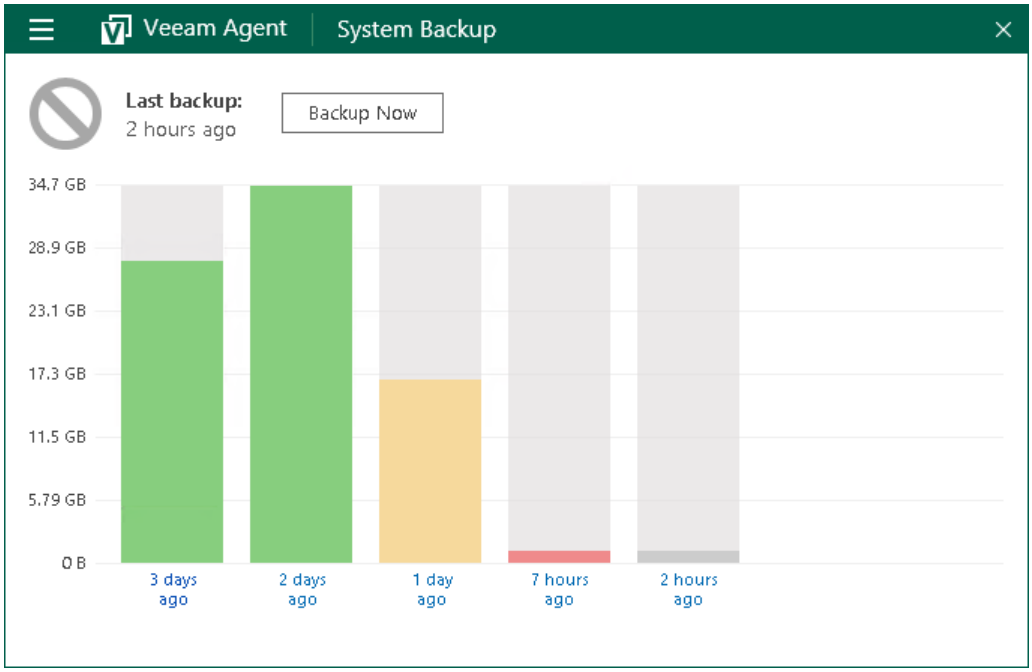
If you configured multiple backup jobs in Veeam Agent, after you open the Control Panel, the Control Panel displays statistics for the first job that you configured. To switch to another job, in the main menu, hover over the name of the necessary job and select **Open**.

The Control Panel displays information about backup job sessions that run previously and a backup job session that is currently running. Every bar represents a separate backup job session. To view general information about a specific job session, hover the mouse over the necessary bar in the chart. Veeam Agent will provide the following details: backup status, backup time and size of the resulting backup file.



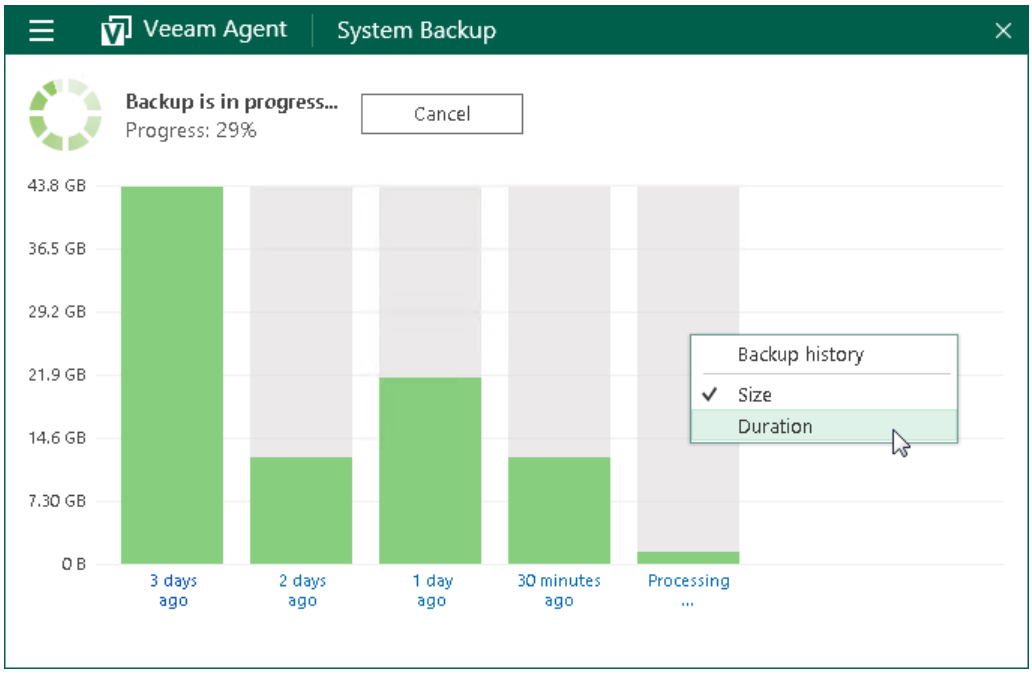
The bar color identifies the status of the backup job session. The backup job session can complete with one of the following statuses:

- *Success* (green color) — the backup job is currently running or has completed successfully.
- *Warning* (yellow color) — the backup job has completed with a warning. Veeam Agent for Microsoft Windows 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.
- *Error* (red color) — the backup job has completed with an error. The resulting backup file has not been created.
- *Canceled* (gray color) — the user has canceled the backup job session. The resulting backup file has not been created.

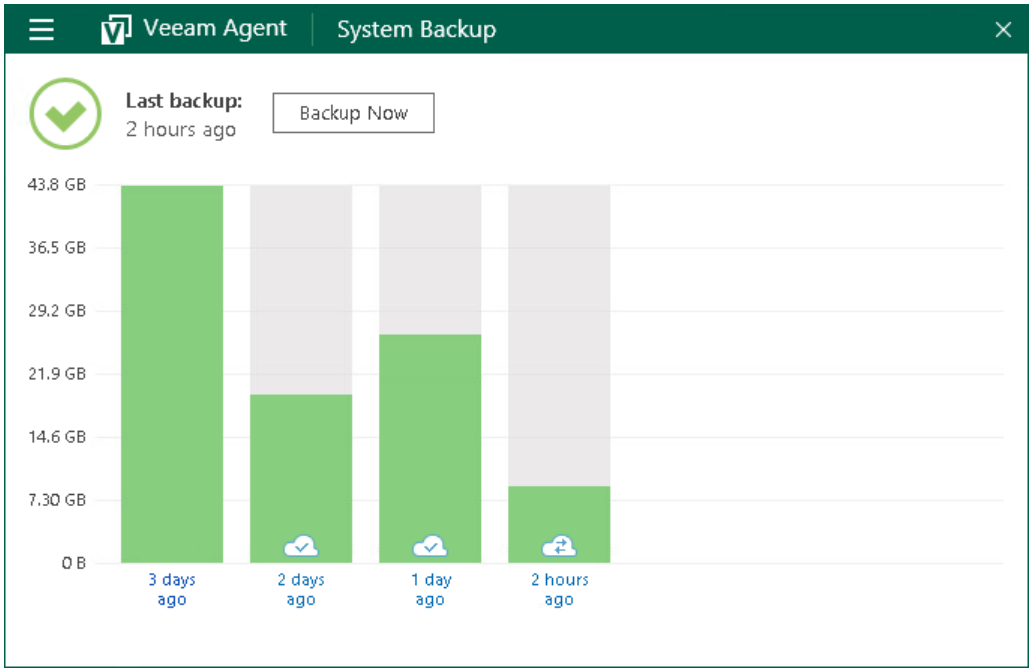


By default, Veeam Agent displays the size of created backup files. To display the duration of backup job sessions:

1. Double-click the Veeam Agent icon in the system tray or right-click the icon and select **Control Panel**.
2. In the backup statistics view, right-click the backup job sessions chart.
3. In the **Backup history** menu, select the **Duration** option.



If the backup cache is enabled for the job, Veeam Agent for Microsoft Windows also displays status of the restore point created within the job session. To learn more, see Viewing Status of Restore Points in Backup Cache.


Veeam Agent
System Backup
Last backup:
2 hours ago
Backup Now
43.8 GB
36.5 GB
29.2 GB
21.9 GB
14.6 GB
7.30 GB
0 B
3 days ago
2 days ago
1 day ago
2 hours ago

Viewing Statistics for Separate Restore Points

You can view the following information about separate restore points in the backup chain:

- View general statistics — for any separate restore point.
- View transaction log backup statistics — for restore points created by the backup job with transaction log backup enabled.

General Statistics

Veeam Agent for Microsoft Windows provides the following information about separate restore points in the backup chain:

- Backed-up items: items that you have chosen to back up.
- Backup duration: duration of the backup job session.
- Restore point size: size of the resulting backup file.
- Total backup size: total size of all backup files created by the backup job in the target location.

  Keep in mind that if you store your backups in a scale-out backup repository with a performance tier located in object storage, the total backup size may differ from the size of all restore points in the backup chain. In this case, Veeam Agent displays only the size of the restore points stored in the performance tier.

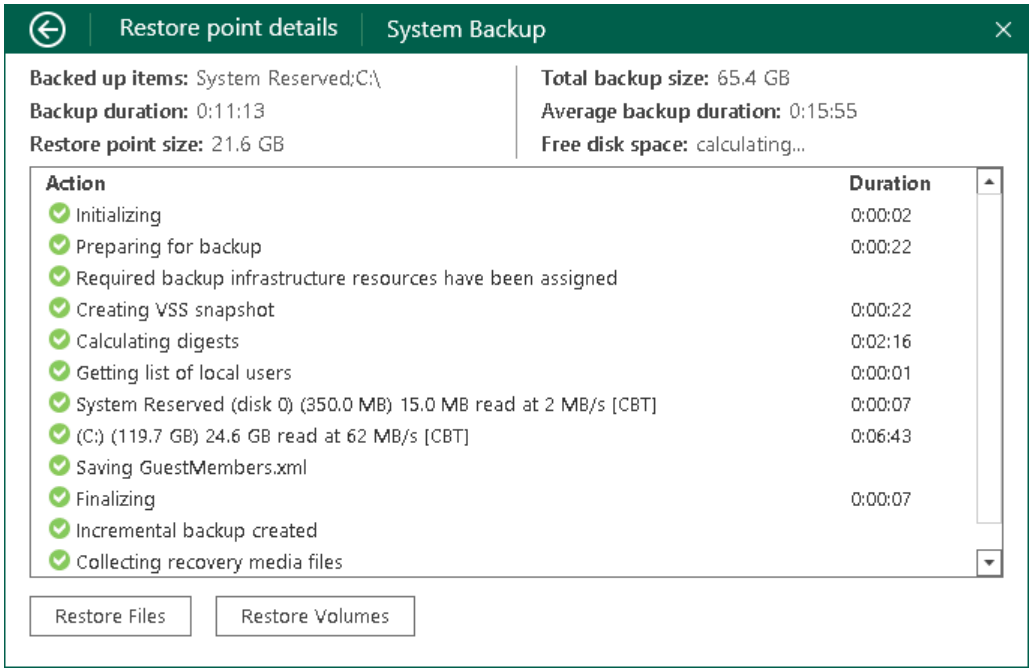
  For more information about the scale-out backup repository, see the Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.
- Average backup time: average time of all successful backup job sessions displayed in the chart.
- Free disk space: amount of free disk space remaining in the target location.
- Details on operations performed during the backup job session.

To view the restore point statistics:

1. Double-click the Veeam Agent icon in the system tray or right-click the icon and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

   If multiple backup jobs are configured in Veeam Agent, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.
3. Click the necessary bar in the chart.
4. Veeam Agent will display detailed statistics on the selected backup job session. To get back to a chart view, click the arrow icon at the top left corner of the window.

If transaction log backup is enabled for the job, you can also view transaction log backup statistics. To learn more, see Transaction Log Backup Statistics.



Transaction Log Backup Statistics

If transaction log backup is enabled for the job, you can use the Veeam Agent control panel to view transaction log backup statistics.

Veeam Agent for Microsoft Windows provides the following information about transaction log processing:

- Protected databases: number of databases that were backed up at least once during the last session.
- Unprotected databases: number of databases that failed to be backed up during the last session.
- Excluded databases: databases excluded from processing. Databases may be excluded for the following reasons: database status is *Offline*, database recovery model is set to *Simple*, database is read-only, database was deleted after the latest full backup, database is added to the list of exclusions.
- Average log size: average amount of data read from the OS through all intervals.
- Max log size: maximal amount of data read from the OS over all 15-min intervals.
- Total log size: total amount of data written to the target location.
- SLA: how many log backup intervals completed in time with successful log backup (calculated as percentage of total number of intervals).
- Misses: how many intervals were missed (number of intervals).
- Max delay: difference between the configured log backup interval and time actually required for log backup. If exceeded, a warning is issued.
- Details on operations performed during the transaction log backup job session.

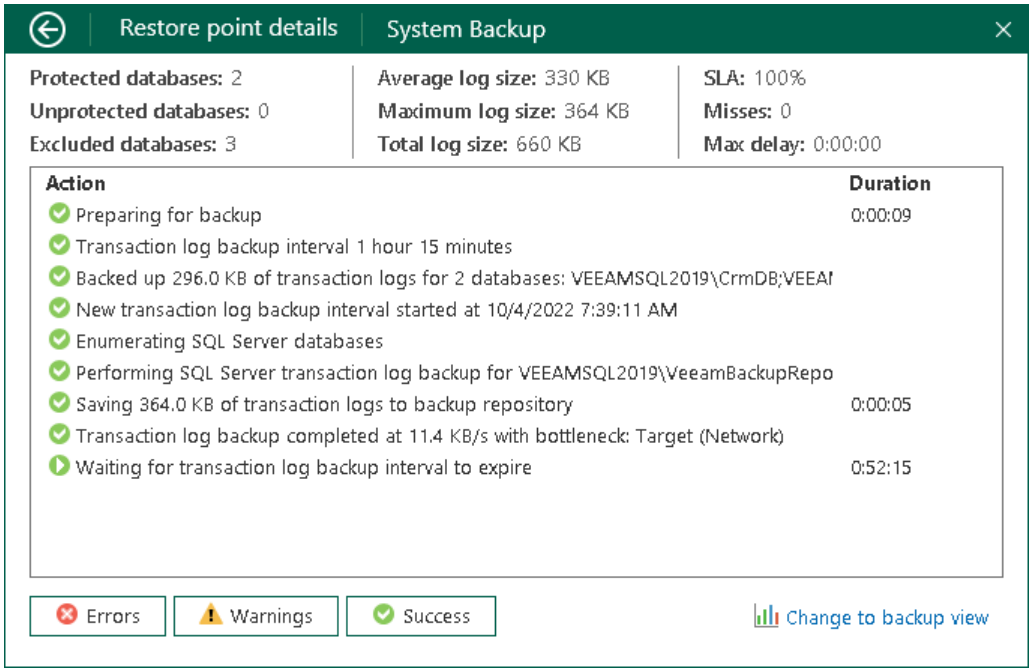
To view statistics on the transaction log backup processing:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

If multiple backup jobs are configured in Veeam Agent for Microsoft Windows, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.

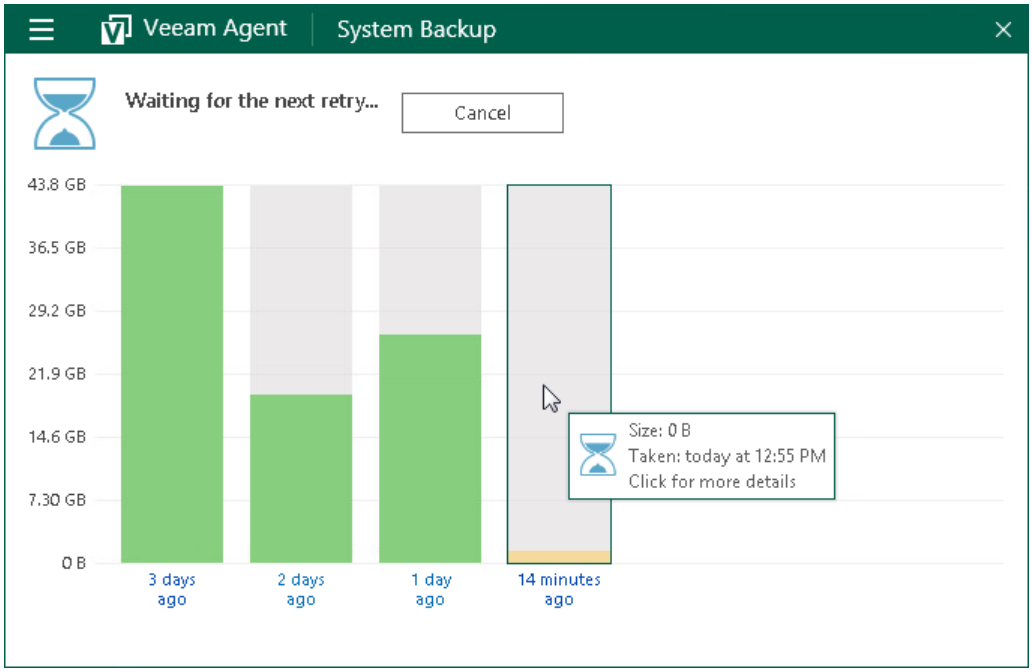
3. Click the necessary bar in the chart.
4. In the **Restore point details** window, click the **Change to database view** link at the bottom right corner of the window. Veeam Agent for Microsoft Windows will display detailed statistics on the transaction log backup. To get back to the general statistics for the selected restore point, click the **Change to backup view** link.

   To get back to a chart view, click the arrow icon at the top left corner of the window.



Viewing Information About Job Retries

If the backup job started by schedule has failed for some reason, Veeam Agent for Microsoft Windows retries the job. All backup job retries are performed within one backup job session. For this reason, Veeam Agent for Microsoft Windows displays them as one bar in the chart.



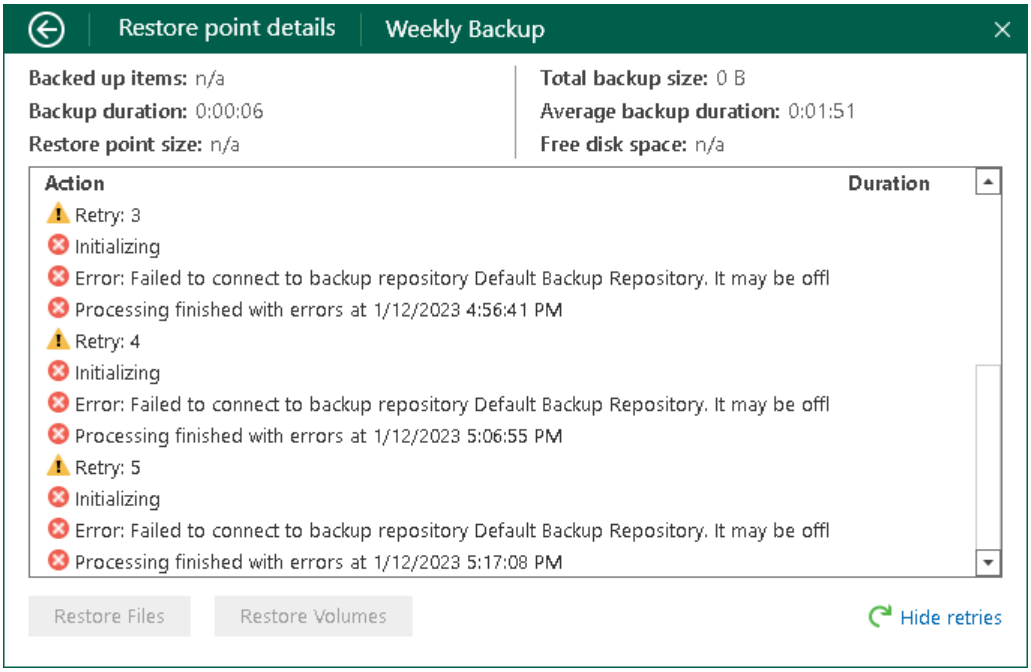
NOTE

For portable devices, Veeam Agent for Microsoft Windows does not automatically retry the backup job if a device is working on battery and the battery level is below 20%.

To view detailed information about the backup job retries:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

   If multiple backup jobs are configured in Veeam Agent for Microsoft Windows, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.
3. Click the necessary bar in the chart.
4. At the bottom right corner of the window, click the **Show retries** link.
5. After you view details, you can hide them. To do this, at the bottom right corner of the window, click the **Hide retries** link.


Restore point details
Weekly Backup
Backed up items: n/a
Backup duration: 0:00:06
Restore point size: n/a
Total backup size: 0 B
Average backup duration: 0:01:51
Free disk space: n/a
Action
Duration
Retry: 3
Initializing
Error: Failed to connect to backup repository Default Backup Repository. It may be offl
Processing finished with errors at 1/12/2023 4:56:41 PM
Retry: 4
Initializing
Error: Failed to connect to backup repository Default Backup Repository. It may be offl
Processing finished with errors at 1/12/2023 5:06:55 PM
Retry: 5
Initializing
Error: Failed to connect to backup repository Default Backup Repository. It may be offl
Processing finished with errors at 1/12/2023 5:17:08 PM
Restore Files
Restore Volumes
Hide retries

Viewing Status of Restore Points in Backup Cache

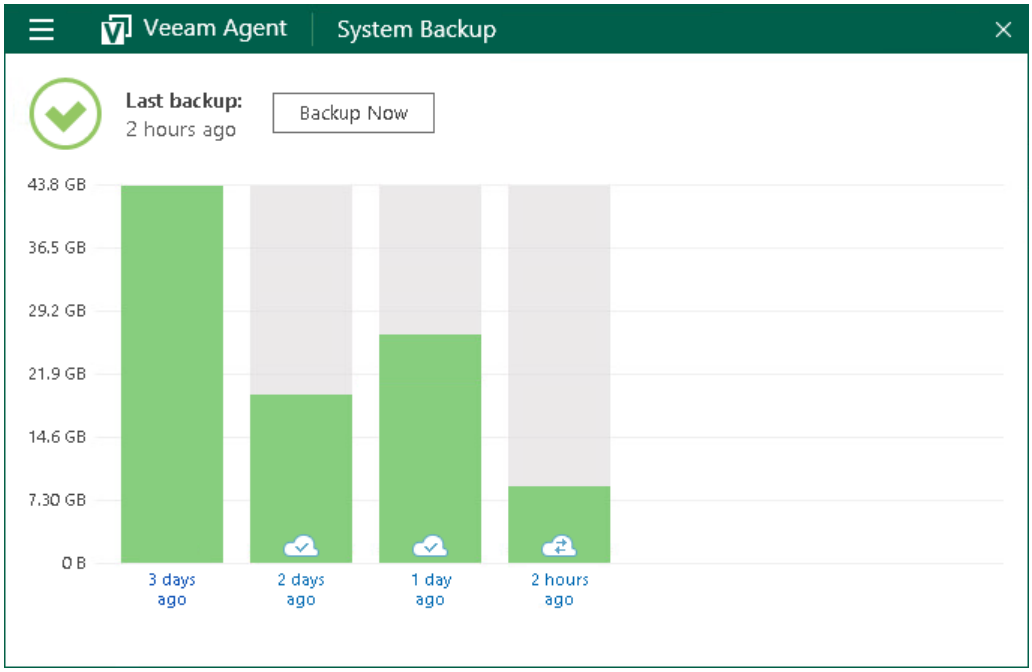
If the backup cache is enabled for the job, you can monitor status of restore points in the backup cache. Veeam Agent for Microsoft Windows displays the restore point status through the icon on a bar in the chart.

The icon can be in one of the following states:

Icon	Description	Backup state
	Check mark over the icon.	The backup file created within the backup session is saved on the target storage.
—	No icon.	The backup file created within the backup session is saved in the backup cache.
	Sync sign over the icon.	The backup file is being uploaded from the backup cache to the target storage.
	Error sign over the icon.	The backup file was not uploaded to the target storage or has been deleted from the backup cache.

TIP

You can also monitor the backup cache activity and view detailed statistics on the restore point upload process. To learn more, see Monitoring Backup Cache Activity.



Monitoring Backup State with Tray Agent

The Veeam Agent for Microsoft Windows icon displayed in the system tray lets you monitor the state of your backups and get informed about the computer protection status.

The icon can be in one of the following states:

Icon	Description	Backup state
	Question mark over the icon	The backup job is not configured.
	Veeam Agent for Microsoft Windows icon	The backup job is set up but scheduling settings for the job are not configured.
	Animated icon	The backup task is being performed. To view the backup task progress, hover the mouse over the icon.
	Clock over the icon	• The backup job has been scheduled; waiting for the first backup job session. • The latest session of the scheduled backup job has completed successfully; waiting for the next backup job session.
	Sync sign over the icon	Veeam Agent is uploading backup files from the backup cache to the target storage.
	Cancel sign over the icon	The latest session of the scheduled backup job has been canceled.
	Error sign over the icon	An error occurred during the latest backup job session, and the session was terminated.
	Minus sign over the icon	The scheduled backup job is disabled.
	Grey icon	The tray agent is not connected to the Veeam Agent for Microsoft Windows service.
	Warning sign over the icon	• The backup job has completed with a warning, for example, the target location is running low on space. • [If you have selected a removable storage device as a target destination in the backup job settings] The target removable storage device is not connected to the computer. In this case, Veeam Agent also displays a warning on the notifications bar in the control panel. You can

Icon	Description	Backup state
		attach the target removable storage device to the computer within 10 minutes, and Veeam Agent will automatically start the scheduled backup job.

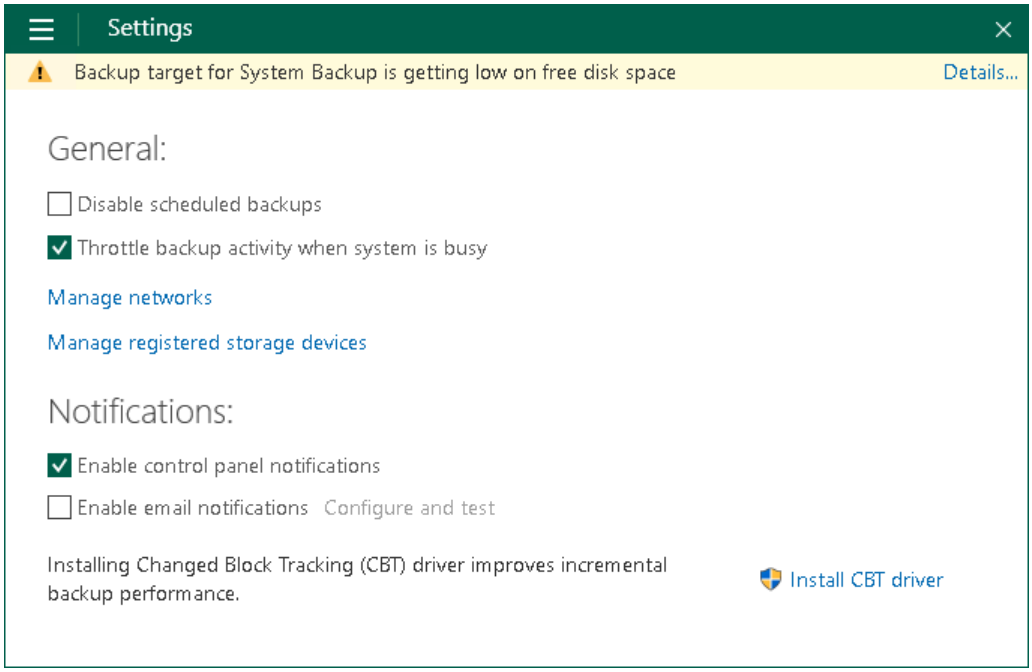
Monitoring Backup Process in Taskbar Button

You can monitor the backup process with the Veeam Agent taskbar button. Veeam Agent displays on the taskbar button a green progress bar that reflects the bar for the currently running job session in the control panel. As a result, you can track the process of the backup file creation while working with another application without having to switch to the control panel.



Viewing and Dismissing Veeam Agent Events

If a warning event occurs, Veeam Agent displays a notification bar with the event description in the control panel window. You can get detailed information about events and dismiss events not to get alerted of them in future. For the full list of notifications, see Control Panel Notifications.



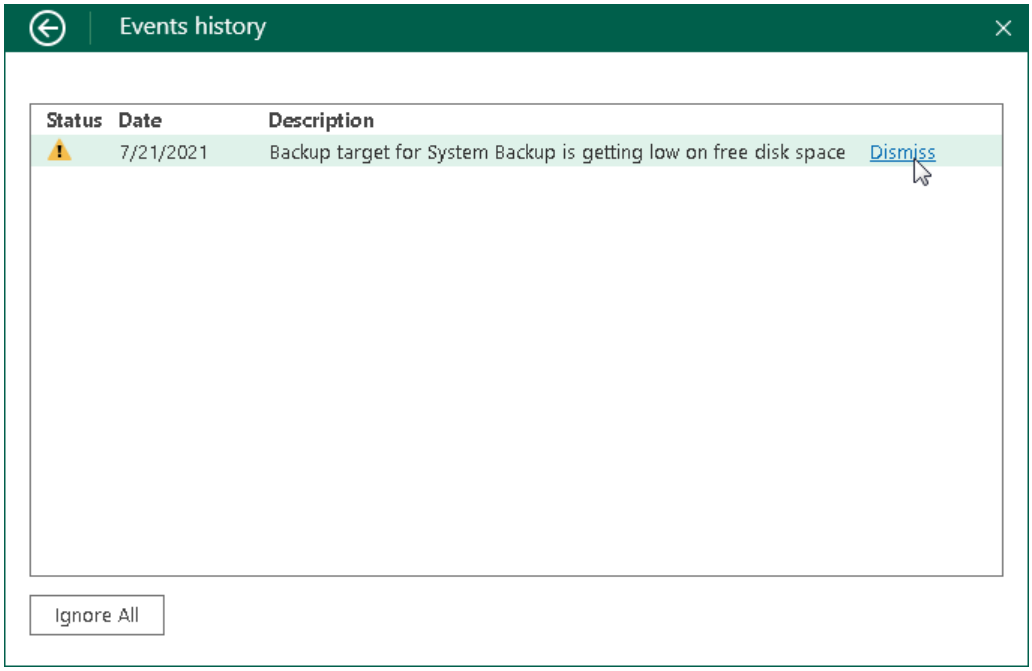
Veeam Agent displays only the latest event in the notification bar. To view detailed information about all events:

1. Double-click the Veeam Agent icon in the system tray, or right-click the Veeam Agent icon in the system tray and select **Control Panel**.
2. Click **Details** on the notification bar at the top of the control panel window.

To dismiss events:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. Click **Details** on the notification bar at the top of the control panel window.
3. Click **Dismiss** next to the necessary event. To dismiss all events at once, click **Ignore All** at the bottom left corner of the window.

> **TIP**
>
> You can disable notifications at all. To learn more, see Disabling Control Panel Notifications.



Control Panel Notifications

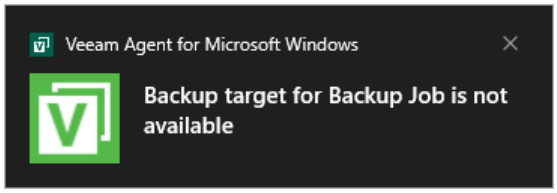
Veeam Agent for Microsoft Windows can inform you about the following events using the notification bar:

Notification	Description
New software update is available	A newer version of Veeam Agent for Microsoft Windows is available for download.
Veeam Recovery Media must be recreated due to a recent Veeam Agent for Microsoft Windows upgrade	You must recreate the Veeam Recovery Media after you have upgraded Veeam Agent for Microsoft Windows to the newer version.
Recovery media OS version is different from the current OS version	You must recreate the Veeam Recovery Media after you have updated the Microsoft Windows OS.
Recovery media has not been created	You have not created the Veeam Recovery Media yet. If the OS on the computer fails to boot, you will not be able to boot the OS using the Veeam Recovery Media to diagnose and fix problems, or restore data from the backup.
Backup target is not available, backup is postponed	Veeam Agent for Microsoft Windows is unable to detect the backup target at the time when the scheduled backup job must start (for example, the backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification during the job retry sessions.
Backup target is not available	Veeam Agent for Microsoft Windows is unable to detect the backup target by the moment when the scheduled backup job

Notification	Description
	must start (for example, backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification after the job has failed.
Backup target has not been seen for N days	The backup target has not been seen for N days. This notification is displayed if scheduled backups have not been created for 2 days or more.
Backup target is getting low on free disk space	Free space on the target storage disk is below 10%. If Veeam Agent for Microsoft Windows does not have enough disk space for backup operation, the job session will fail.
Skipping scheduled backup, because battery level is too low	[For laptops and tablets] The battery level is below 20%. Veeam Agent for Microsoft Windows does not start a new backup session in this case.
This application is managed by your system administrator	This notification is displayed if Veeam Agent for Microsoft Windows is operating in the read-only mode. Veeam Agent for Microsoft Windows operates in the read-only mode if backup operations are managed by Veeam Backup & Replication or Veeam Availability Console.
Your license will expire in N days	The Veeam Agent for Microsoft Windows license will expire, and the grace period will start in N days.
Your license has expired and needs to be renewed	The Veeam Agent for Microsoft Windows license has expired, and the grace period has started. During the grace period, you can perform all types of backup and restore operations. You must obtain a new license before the end of the grace period.
Your license has expired, and your grace period is over	The Veeam Agent for Microsoft Windows license has expired, and the grace period is over. In this case, Veeam Agent for Microsoft Windows does not perform backup operations. However, you are able to restore data from existing backups. To use Veeam Agent for Microsoft Windows in the full functionality mode, you must obtain a new license.

Viewing Events with Windows Notification Center

In addition to displaying notifications about Veeam Agent events in the control panel window, Veeam Agent can inform you about its events using the Windows Notification Center. Once an event occurs, a message notifying about this event will appear on the Microsoft Windows desktop. This lets you view the notification without the need to open the Veeam Agent Control Panel and take the necessary actions immediately. For the full list of notifications that appears on the Microsoft Windows desktop, see Windows Desktop Notifications.



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

To disable desktop notifications, right-click the message and select **Turn off notifications for Veeam Agent for Microsoft Windows**.

Windows Desktop Notifications

Veeam Agent for Microsoft Windows can inform you about the following events using the Windows Notification Center:

Notification	Description
New software update is available	A newer version of Veeam Agent for Microsoft Windows is available for download.
Veeam Recovery Media must be recreated due to a recent Veeam Agent for Microsoft Windows upgrade	You must recreate the Veeam Recovery Media after you have upgraded Veeam Agent for Microsoft Windows to the newer version.
Recovery media OS version is different from the current OS version	You must recreate the Veeam Recovery Media after you have updated the Microsoft Windows OS.
Recovery media has not been created	You have not created the Veeam Recovery Media yet. If the OS on the computer fails to boot, you will not be able to boot the OS using the Veeam Recovery Media to diagnose and fix problems, or restore data from the backup.
Backup target is not available	Veeam Agent for Microsoft Windows is unable to detect the backup target by the moment when the scheduled backup job must start (for example, backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification after the job has failed.

Notification	Description
Your license will expire in N days	The Veeam Agent for Microsoft Windows license will expire, and the grace period will start in N days.
Your license has expired and needs to be renewed	The Veeam Agent for Microsoft Windows license has expired, and the grace period has started. During the grace period, you can perform all types of backup and restore operations. You must obtain a new license before the end of the grace period.
Your license has expired, and your grace period is over	The Veeam Agent for Microsoft Windows license has expired, and the grace period is over. In this case, Veeam Agent for Microsoft Windows does not perform backup operations. However, you are able to restore data from existing backups. To use Veeam Agent for Microsoft Windows in the full functionality mode, you must obtain a new license.

Viewing Job Session Results in Email Reports

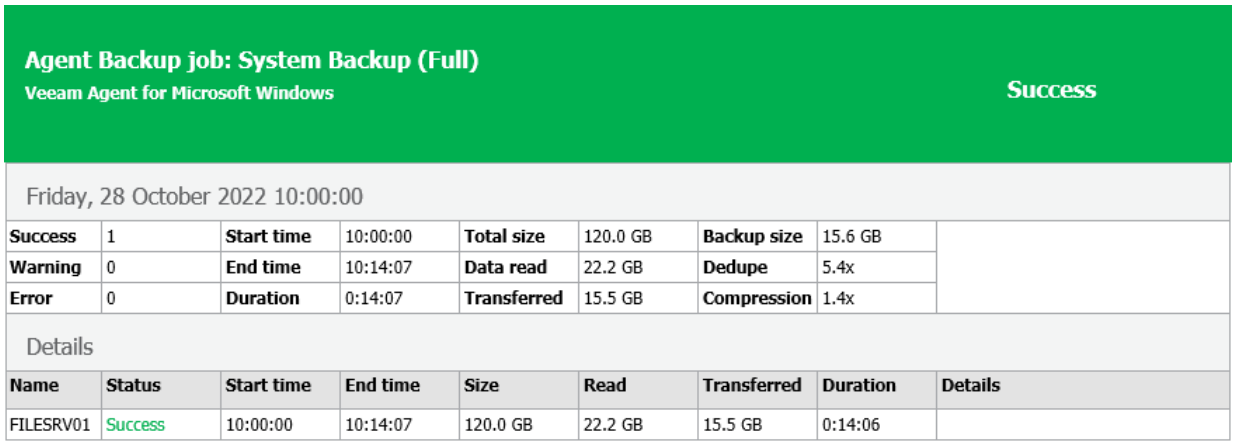
You can receive email notifications with Veeam Agent for Microsoft Windows job results. When the backup job session completes, Veeam Agent for Microsoft Windows will send a report containing data on the job session to the specified email address.

The report contains the following data:

- Cumulative job session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression and deduplication ratios.
- Detailed statistics for the computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).
- If the backup job is set up to create database log backups, the report contains statistics for the database log backup job: a list of databases that were backed up at least once during the last session and information for the latest log processing intervals.
- If you use the backup cache, the report also contains statistics on the backup cache activity: a list of restore points created in the backup cache, their status and upload details. To learn more about the backup cache, see Backup Cache.

To receive email reports, you must enable and configure email notifications in the Veeam Agent for Microsoft Windows Control Panel. To learn more, see Enabling Email Notifications. Once email notifications are configured, Veeam Agent for Microsoft Windows will send email report for every backup job session that is started by schedule, manually or when you perform standalone full or incremental ad-hoc backup.

If the scheduled backup job fails, Veeam Agent for Microsoft Windows does not send a report after every job retry. Instead, Veeam Agent for Microsoft Windows sends one report on the first error within the job session and another report on the last job session result — success or error.



Agent Backup job: System Backup (Full)
Veeam Agent for Microsoft Windows — **Success**

Friday, 28 October 2022 10:00:00

Success	1	**Start time**	10:00:00	**Total size**	120.0 GB	**Backup size**	15.6 GB	
Warning	0	**End time**	10:14:07	**Data read**	22.2 GB	**Dedupe**	5.4x	
Error	0	**Duration**	0:14:07	**Transferred**	15.5 GB	**Compression**	1.4x	

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FILESRV01	Success	10:00:00	10:14:07	120.0 GB	22.2 GB	15.5 GB	0:14:06	

Specifying Settings

You can use global settings of Veeam Agent to accomplish the following tasks:

- Throttle backup activities.
- Restrict network connections usage.
- Manage backup storage devices.
- Disable Control Panel notifications.
- Enable email notifications.
- Check for new product versions and updates.

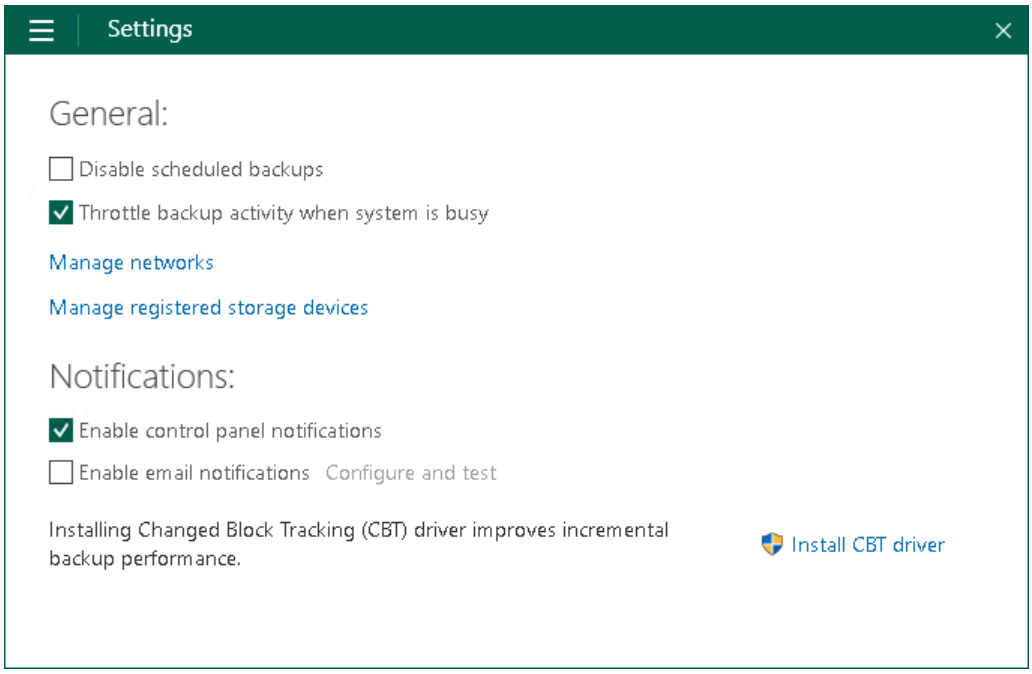
Throttling Backup Activities

You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup. The throttling option can help you avoid situations when backup tasks consume all available hard disk resources and hinder work of other applications and services.

With throttling enabled, Veeam Agent for Microsoft Windows sets low priority for Veeam Agent for Microsoft Windows components engaged in the backup process (in particular, the *VeeamAgent.exe* process). If this option is not enabled, Veeam Agent for Microsoft Windows components have normal priority.

To enable the throttling option for backup activities:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Select the **Throttle backup activity when system is busy** check box.



Restricting Network Connections Usage

You can instruct Veeam Agent for Microsoft Windows to throttle network traffic for backup jobs and disable backup over Internet connections of certain types. This helps limit the impact of Veeam Agent operations on network performance and avoid extra costs.

Network usage settings apply to all types of backups: scheduled and ad-hoc. To restrict network connections usage for Veeam Agent, you can perform the following tasks:

- Limit bandwidth consumption for Veeam Agent.
- Disable backup over metered connections.
- Disable backup over VPN connections.
- Allow Veeam Agent to use specific Wi-Fi networks only.

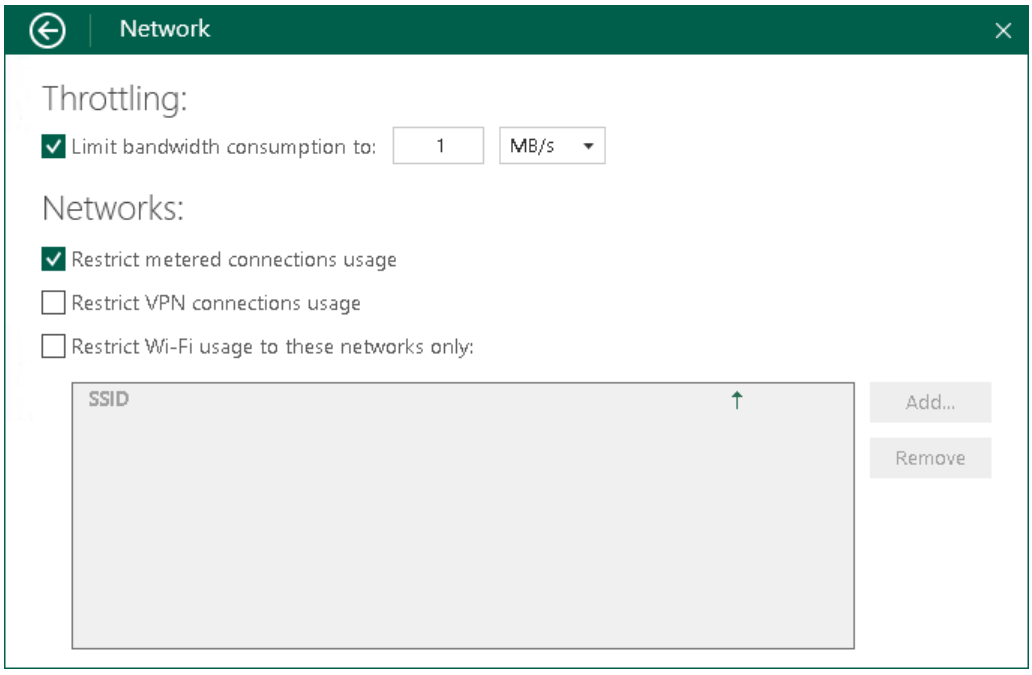
Limiting Bandwidth Consumption

To reduce the impact of Veeam Agent operations on network performance, you can limit bandwidth consumption for Veeam Agent backup jobs. Limiting bandwidth consumption prevents jobs from utilizing the entire bandwidth available in your environment to ensure that enough traffic is provided for other network operations. We strongly recommend to limit bandwidth consumption if you perform backup to a remote location over a slow network connection.

> **NOTE**
>
> Bandwidth consumption limit does not apply to restore operations.

By default, Veeam Agent is set up to use the entire bandwidth available in your environment. To limit bandwidth consumption for Veeam Agent backup jobs:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Throttling** section, select the **Limit bandwidth consumption to** check box and specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.



Disabling Backup over Metered Connections

Veeam Agent can disable backup over metered Internet connections to help you avoid extra costs. If you use a metered Internet connection, your service provider charges you by the amount of data sent and received by your computer. Veeam Agent automatically detects metered connections and will not perform backup when your computer is on such connection.

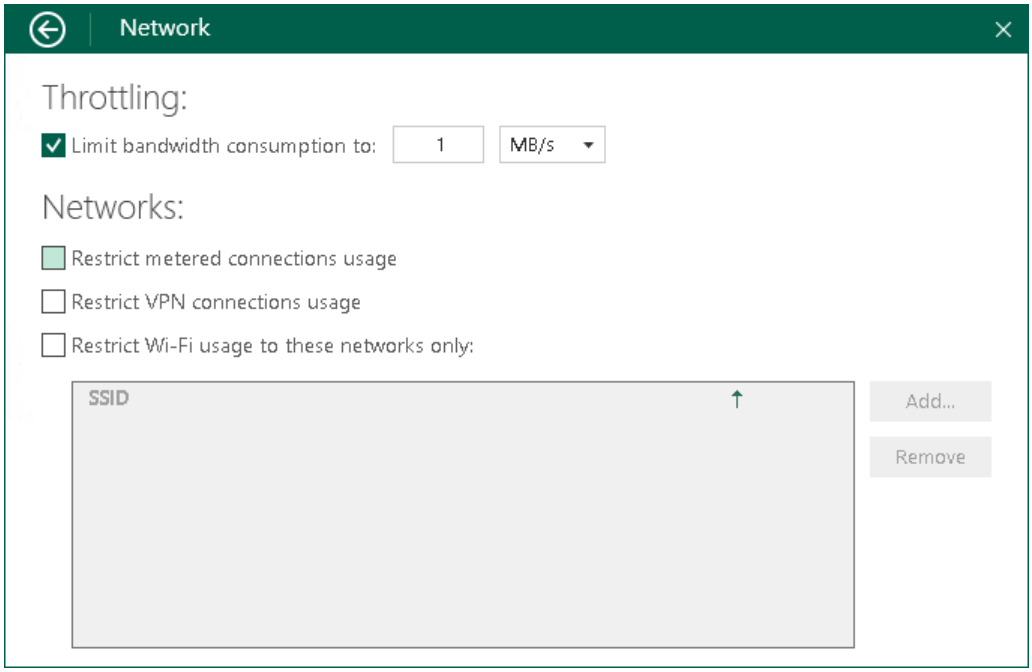
Consider the following limitations and requirements:

- Veeam Agent disables backup over metered Internet connections only on computers that run Microsoft Windows 8.1 and later. If the computer runs an earlier version of Microsoft Windows, this option is not applicable.
- You must specify which connections are metered in Microsoft Windows. To learn more, see this Microsoft article.

By default, backup over metered connections is disabled. To enable backup over metered connections:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Networks** section, clear the **Restrict metered connections usage** check box.

> **NOTE**
>
> For the cases when backup over metered connections is disabled, consider the following:
>
> - If you start the backup job manually when only a metered connection is available, Veeam Agent for Microsoft Windows will display a warning and ask you to confirm that you want to use this connection for backup.
> - If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use metered connections for backup.
> - If you enable the backup cache for the backup job, and this backup job starts upon schedule when only a metered connection is available, Veeam Agent for Microsoft Windows will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.


Network
Throttling:
Limit bandwidth consumption to:
1
MB/s
Networks:
Restrict metered connections usage
Restrict VPN connections usage
Restrict Wi-Fi usage to these networks only:
SSID
Add...
Remove

Disabling Backup over VPN Connections

Veeam Agent can disable backup over VPN connections. This helps you avoid extra costs if your VPN service provider charges you by the amount of data sent and received by your computer. Veeam Agent automatically detects VPN connections and will not perform backup when your computer is on such connection.

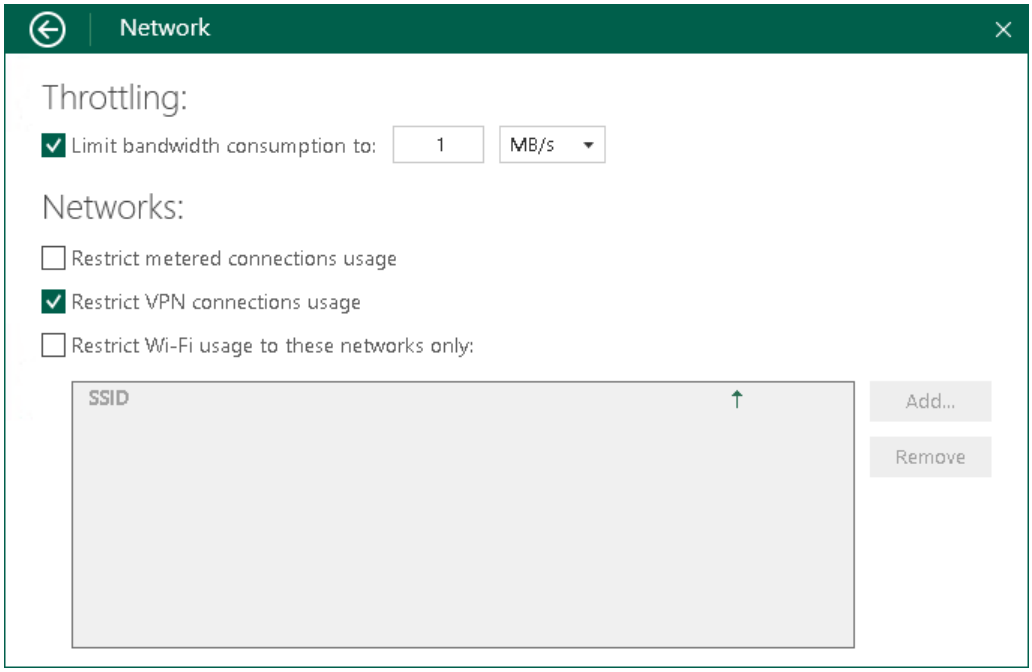
By default, backup over VPN connections is enabled. To disable backup over VPN connections:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Networks** section, select the **Restrict VPN connections usage** check box.

Keep in mind that Veeam Agent detects VPN connections created with Microsoft Windows in-built tools and the following 3rd party VPN providers:

- Cisco AnyConnect
- Fortinet SSL VPN
- Open VPN
- Palo Alto Networks GlobalProtect VPN

> **NOTE**
>
> For the cases when backup over VPN connections is disabled, consider the following:
>
> - If you start the backup job manually when only a VPN connection is available, Veeam Agent will display a warning and ask you to confirm that you want to use this connection for backup.
> - If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use VPN connections for backup.
> - If you enable the backup cache for the backup job, and this backup job starts upon schedule when only a VPN connection is available, Veeam Agent will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.


Network
Throttling:
Limit bandwidth consumption to:
1
MB/s
Networks:
Restrict metered connections usage
Restrict VPN connections usage
Restrict Wi-Fi usage to these networks only:
SSID
Add...
Remove

Selecting Wireless Networks for Backup

You can restrict usage of Wi-Fi networks for Veeam Agent for Microsoft Windows. This may be useful, for example, to avoid transmission of backed-up data over insecure or slow wireless network connections.

By default, Veeam Agent for Microsoft Windows is set up to back up data over any Wi-Fi network to which the Veeam Agent computer is connected. You can select one or more specific Wi-Fi networks and instruct Veeam Agent for Microsoft Windows to perform backup over these networks only. Backup over other wireless networks will be disabled.

To restrict usage of wireless networks:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. Select the **Restrict Wi-Fi usage to these networks only** check box and click **Add.**
5. Select one or more Wi-Fi networks in the list and click **Save**.

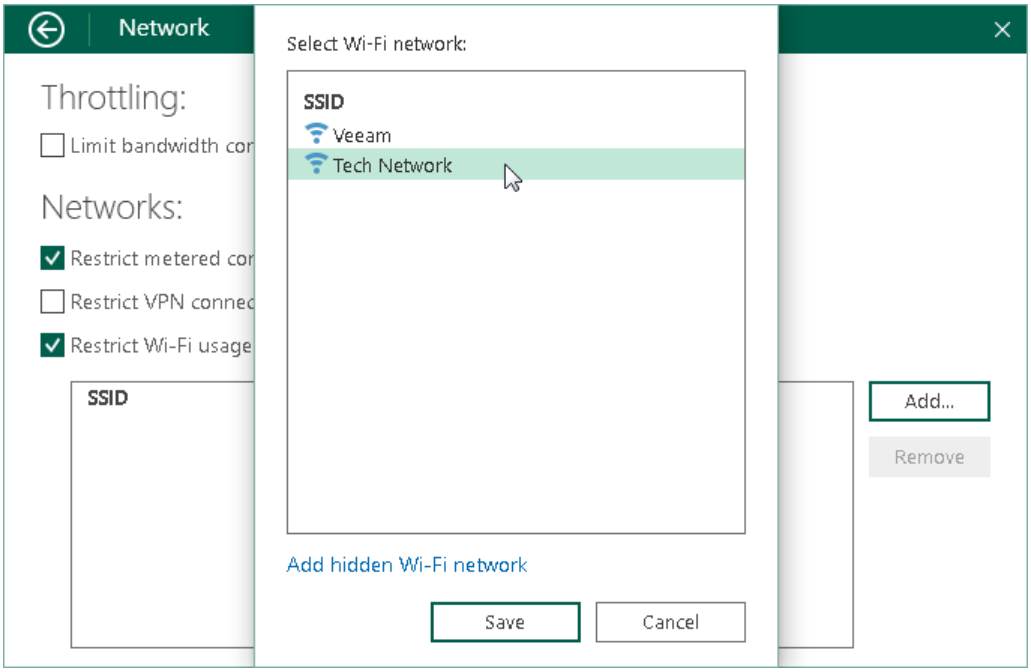
   If you want to allow Veeam Agent to back up data over a hidden wireless network, click the **Add hidden Wi-Fi network** link. In the displayed window, specify the SSID of the necessary network and click **Save**.

   If you want to restrict usage over any wireless networks, select the **Restrict Wi-Fi usage to these networks only** check box and do not add any networks to the list.

NOTE

For the cases when backup over Wi-Fi networks is restricted, consider the following:

- If you start the backup job manually when selected Wi-Fi networks are not available, Veeam Agent for Microsoft Windows will display a warning and ask you to confirm that you want to use this connection for backup.
- If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use all available Wi-Fi networks for backup.
- If you enable the backup cache for the backup job, and this backup job starts upon schedule when selected Wi-Fi networks are not available, Veeam Agent for Microsoft Windows will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.


Network
Throttling:
Limit bandwidth cor
Networks:
Restrict metered cor
Restrict VPN connec
Restrict Wi-Fi usage
SSID
Add...
Remove
Select Wi-Fi network:
SSID
Veeam
Tech Network
Add hidden Wi-Fi network
Save
Cancel

Managing Rotated Drives

You can use a rotated drives scheme for storing backups. To do this, you can create backups on several external drives (for example, USB or FireWire) and swap these drives when needed.

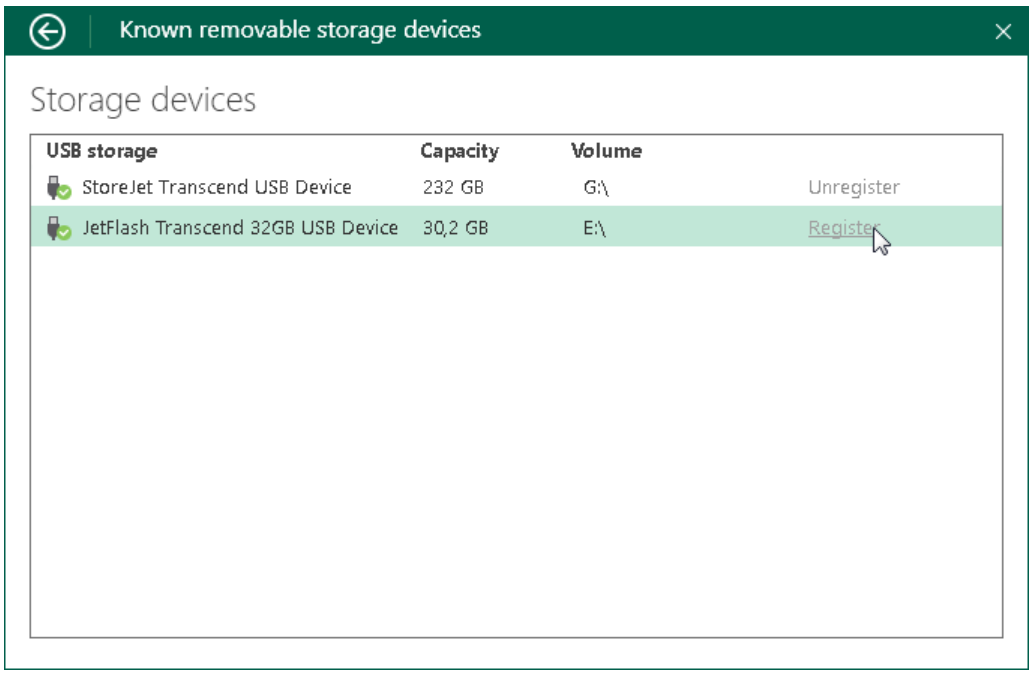
The drive on which you plan to store a backup must be registered in Veeam Agent for Microsoft Windows. If the drive is not registered, Veeam Agent for Microsoft Windows will not be able to detect the drive and store a backup on it.

Consider the following limitations:

- You can register and unregister drives if you have selected to store backups on an external drive connected to the computer. If you have selected to store backups on a local computer drive, in a network shared folder or in a backup repository, registering options will be disabled.
- You cannot unregister all drives at once. At least one drive will remain registered in Veeam Agent for Microsoft Windows.

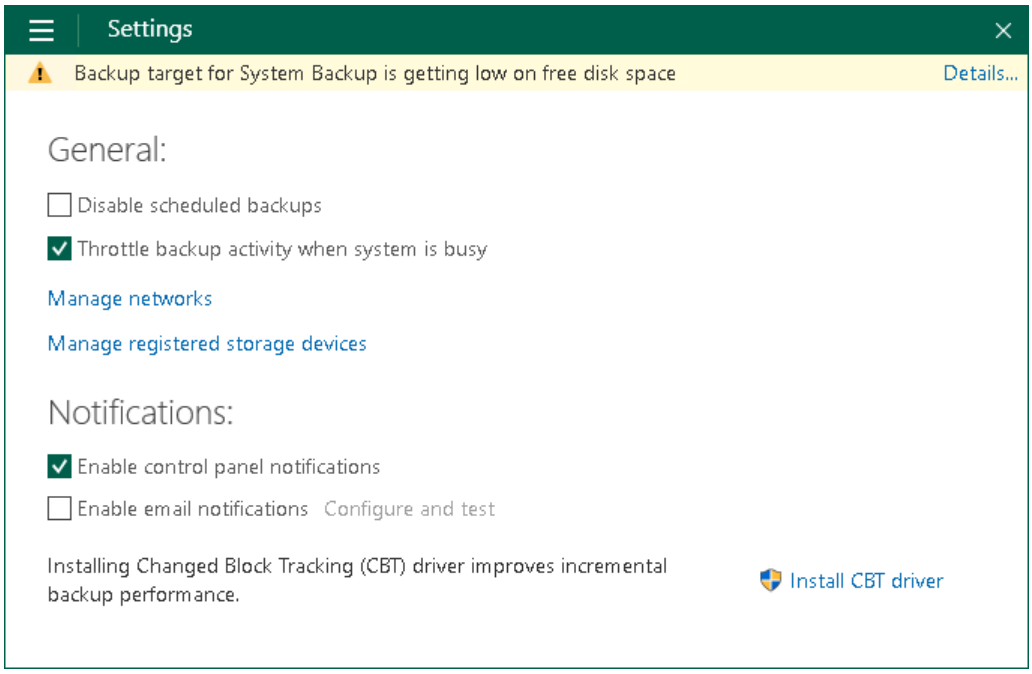
To register and unregister a drive in Veeam Agent for Microsoft Windows:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage registered storage devices** link.
4. In the list of devices, click **Register/Unregister** next to the necessary backup storage device.



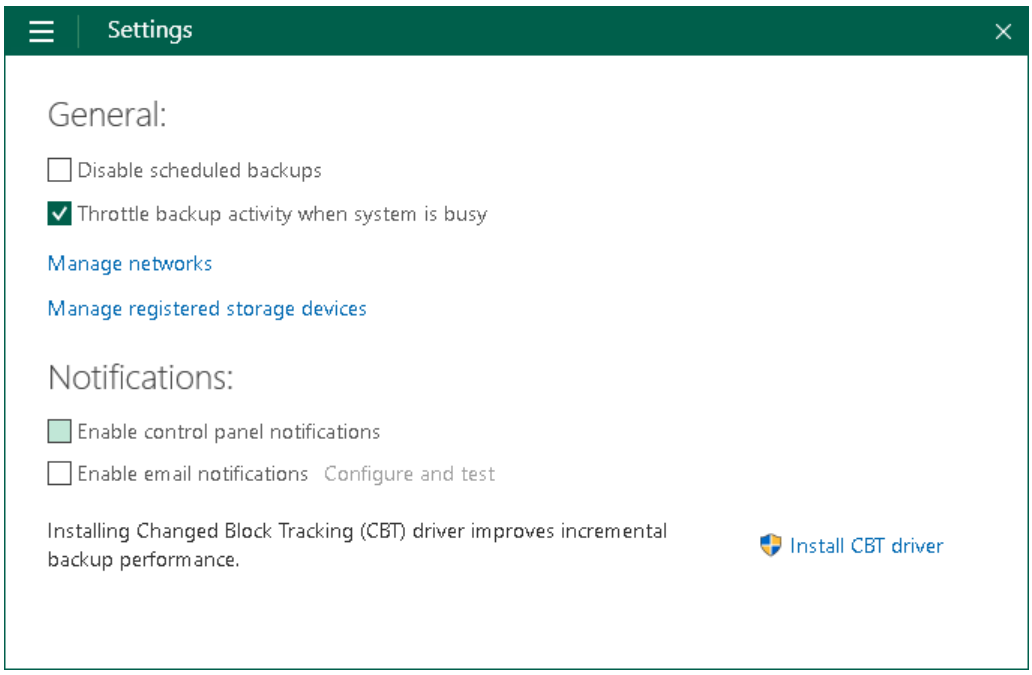
Disabling Control Panel Notifications

Veeam Agent for Microsoft Windows displays warning and information messages on the notification bar in the Control Panel. If necessary, you can disable Veeam Agent notifications.



To disable notifications:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. In the **Notifications** section, clear the **Enable Control Panel notifications** check box.

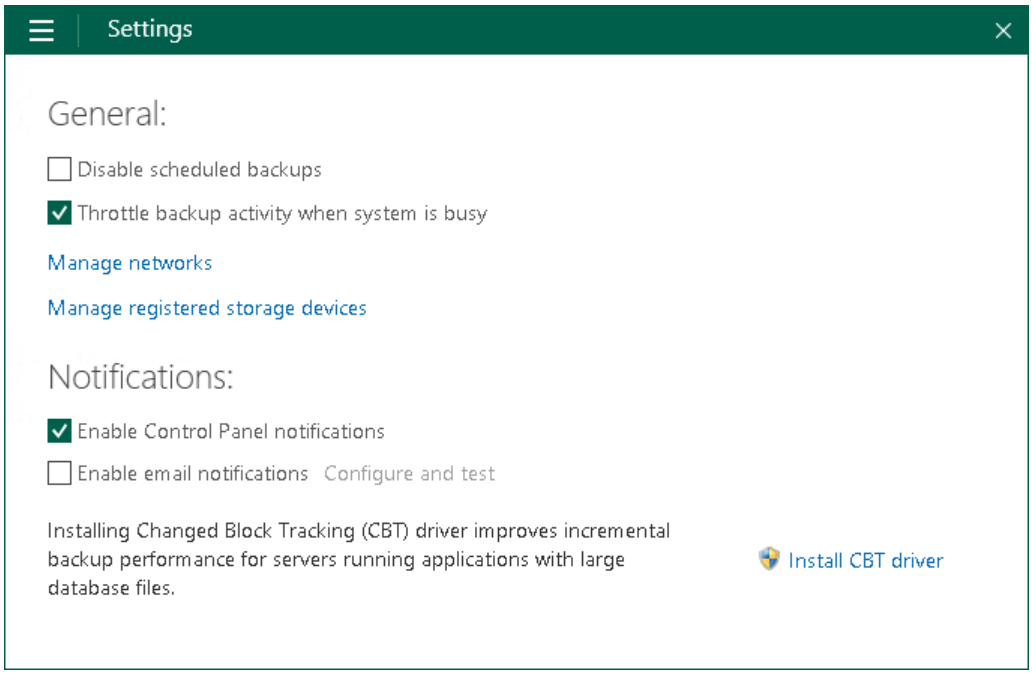


Enabling Email Notifications

You can enable Veeam Agent for Microsoft Windows email notifications to receive reports containing data on the latest backup job session statistics and result.

To enable email notifications:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. In the **Notifications** section, select the **Enable email notifications** check box and click the **Configure and test** link.
4. In the **Configure and test email notifications** window, select one of the **Mail Server** options and specify the required settings:
   - Custom SMTP server settings.
   - Gmail server settings.
   - Microsoft 365 server settings.



Disabling Email Notifications

To disable email notifications, clear the **Enable email notifications** check box in the **Settings** tab of the Control Panel. Current email notifications configuration will remain saved in the Veeam Agent database.

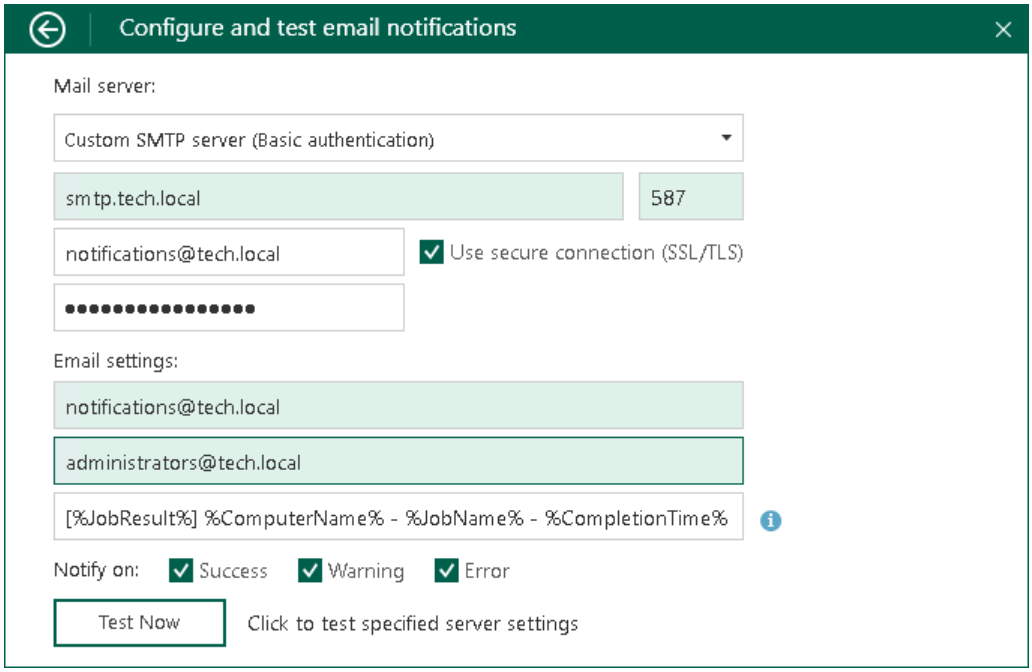
Custom SMTP Server Settings

To connect to the SMTP server, specify the following settings in the **Configure and test email notifications** window:

1. In the **Mail server** section, specify the following:
   a. Select the **Custom SMTP Server (Basic authentication)** option from the drop-down list.
   b. In the **SMTP Server DNS Name or IP address** field, enter a full DNS name or IP address of the SMTP server that will be used for sending email notifications.
   c. In the **Port** field, specify the port number for the SMTP server.

      > **NOTE**
      >
      > Sending email notifications using Implicit TLS (over port 465) is not supported. For more information about Implicit TLS, see this RFC section.

   d. In the **Username** field, specify a user name for the account that has rights to access the SMTP server.
   e. In the **Password** field, enter a password for the account that has rights to access the SMTP server.
   f. To use a secure SSL/TLS connection for email operations, select the **Use secure connection (SSL/TLS)** check box.
2. In the **Email settings** section specify the following:
   a. Specify the sender email address in the **From email address** field. You can specify your account email address or its alias.
   b. Specify the recipient email address in the **To email address** field. You can specify several recipient email addresses separated with a comma or semicolon.
   c. In the **Email subject** filed, specify a subject for the message. You can use the following variables in the subject:
      i. *%JobResult%*
      ii. *%ComputerName%*
      iii. *%JobName%*
      iv. *%CompletionTime%*
3. In the **Notify on** section, select the **Success**, **Warning** or **Error** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
4. [Optional] Click **Test now** to validate the SMTP server settings and send a test email.


Configure and test email notifications
Mail server:
Custom SMTP server (Basic authentication)
smtp.tech.local
587
notifications@tech.local
Use secure connection (SSL/TLS)
Email settings:
notifications@tech.local
administrators@tech.local
[%JobResult%] %ComputerName% - %JobName% - %CompletionTime%
Notify on:
Success
Warning
Error
Test Now
Click to test specified server settings

Gmail Server Settings

To connect to the Gmail server, specify the following settings in the **Configure and test email notifications** window:

1. In the **Mail server** section, specify the following:
   a. Select the **Google Gmail (Modern authentication)** option from the drop-down list.
   b. Click the **Sign in with Google** button, enter your Google account credentials and complete Google authorization process.

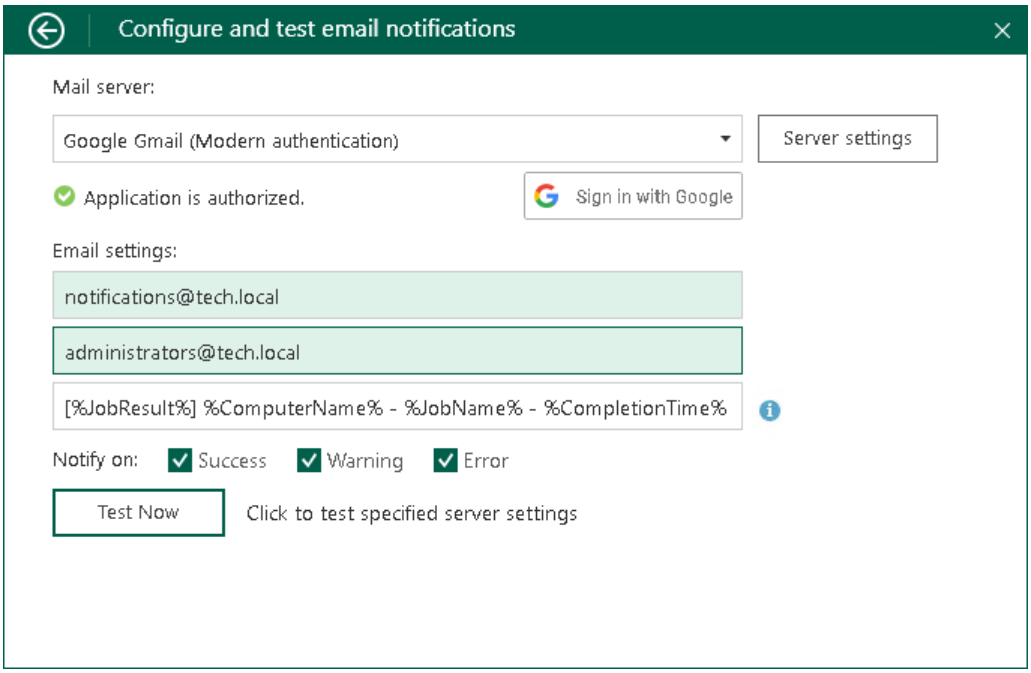
   > **IMPORTANT**
   >
   > When you are prompted to allow Veeam Agent sending emails on behalf of your Google account, grant the permission and click **Continue**.

2. In the **Email settings** section, specify the following:
   a. If necessary, change the email address in the **From email address** field to its alias.
   b. If necessary, change the recipient email address in the **To email address** field. You can specify several recipient email addresses separated with a comma or semicolon.
   c. In the **Email subject** filed, specify a subject for the message. You can use the following variables in the subject:
      i. *%JobResult%*
      ii. *%ComputerName%*
      iii. *%JobName%*
      iv. *%CompletionTime%*
3. In the **Notify on** section, select the **Success**, **Warning** or **Error** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
4. [Optional] Click **Test now** to validate the Gmail server settings and send a test email.

To specify custom authentication options, do the following:

1. Click the **Server settings** button.
2. Select the **Use custom settings** check box.
3. Specify the application client ID and the client secret.

To learn how to register your custom application, see Registering Application in Google Cloud Console.



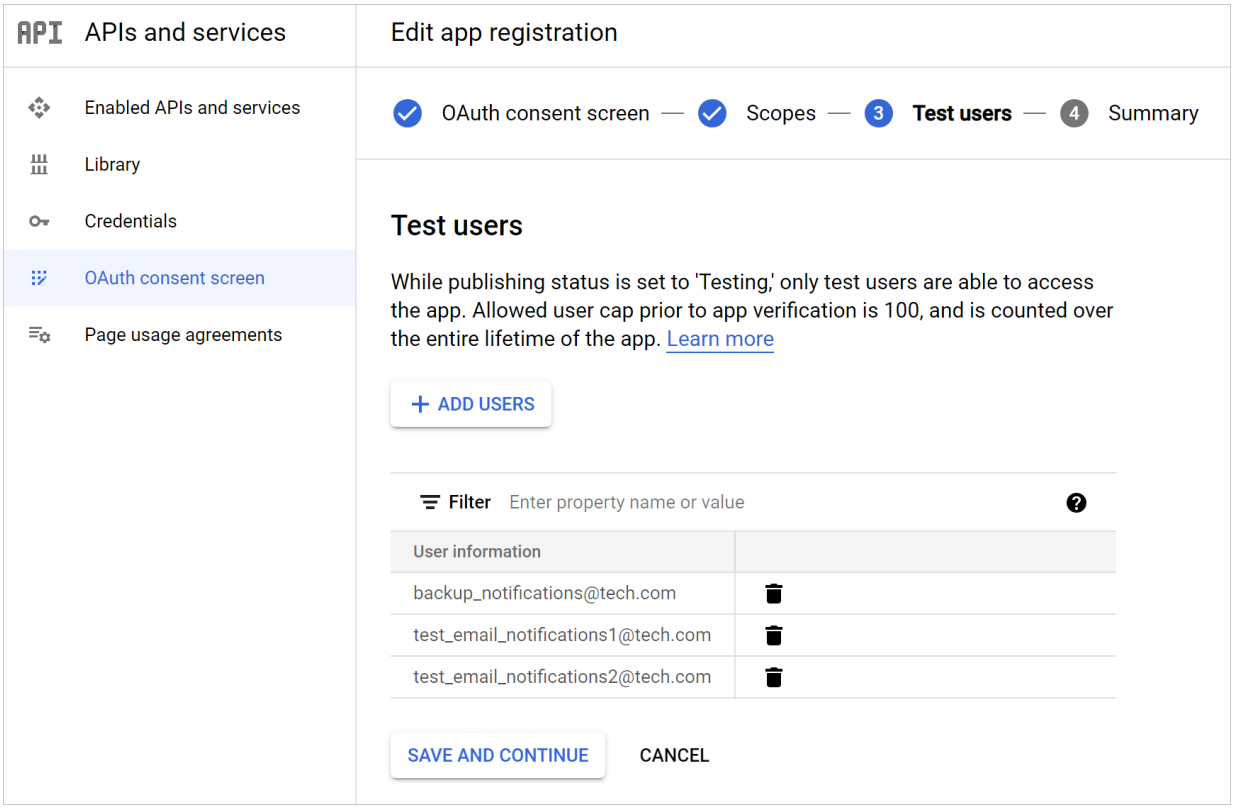
Registering Application in Google Cloud Console

If you want to use your own web application for email notifications, you need to configure it in the Google Cloud console. To do this, perform the following steps:

1. Log in to the Google Cloud console under a Google account that has permissions to create applications.
2. Create a new project and enable Gmail API for the project. To do this, open **APIs and services** > **Library** > **Gmail API** > **Manage** and click **Enable API**.
3. Create OAuth credentials. To do this, perform the following steps:
   a. Open **APIs and services** > **Credentials**. Click **Create credentials** and select **OAuth client ID**.
   b. In the **Application type** field, select **Desktop app**.
   c. In the **Name** field, specify the name of your OAuth 2.0 client.
   d. Click **Create** to generate the application client ID and the client secret. In the opened window, you can copy credentials or download them in the JSON format. You can also find them later in the **APIs and services** > **Credentials** section when editing your OAuth 2.0 client ID.



4. Open **APIs and services > OAuth consent screen** and click **Edit App**. Specify your application name and the user support email and click **Save and continue**.
5. If your application is in the **Testing** status, you must specify test users. To do this, at the **Test users** step of the **Edit App** wizard, click **Add users**. To apply changes, click **Save and continue**. Note that only test users will have access to the app.



After you finish the registration, specify custom application registration settings when configuring the mail server for Google Gmail OAuth 2.0 authentication. For more information, see Gmail Server Settings.

> **NOTE**
>
> You can leave your application in the **Testing** status and do not publish it. In that case, you will receive a warning message *Google hasn't verified this app* when connecting to your application. If you want to verify it, see this Google article.

Microsoft 365 Server Settings

> **NOTE**
>
> Before connecting to the the Microsoft 365 server, check the version of Microsoft .NET Framework installed on your computer. Microsoft 365 server modern authentication requires Microsoft .NET Framework 4.6.2 or later.
>
> If an older version of Microsoft .NET Framework is installed, perform the upgrade before proceeding to authorization.

To connect to the Microsoft 365 server, specify the following settings in the **Configure and test email notifications** window:

1. In the **Mail server** section, specify the following:
   a. Select the **Microsoft 365 (Modern authentication)** option from the drop-down list.
   b. Click the **Authorize now** button and enter your Microsoft 365 account credentials or choose an account from the suggested list.

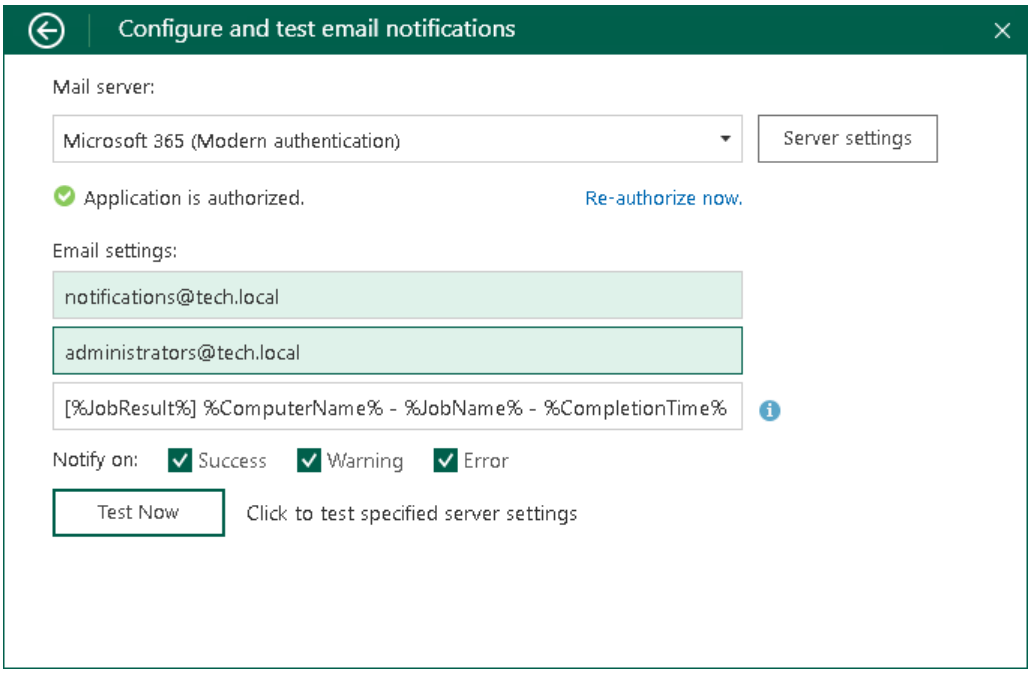
      > **IMPORTANT**
      >
      > When you are prompted to grant Veeam Agent access to your Microsoft 365 profile, accept the permissions listed in the opened window.

2. In the **Email settings** section, specify the following:
   a. If necessary, change the email address in the **From email address** field to its alias.
   b. If necessary, change the recipient email address in the **To email address** field. You can specify several recipient email addresses separated with a comma or semicolon.
   c. In the **Email subject** filed, specify a subject for the message. You can use the following variables in the subject:
      i. *%JobResult%*
      ii. *%ComputerName%*
      iii. *%JobName%*
      iv. *%CompletionTime%*
3. In the **Notify on** section, select the **Success**, **Warning** or **Error** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
4. [Optional] Click **Test now** to validate the Microsoft 365 server settings and send a test email.

To specify custom authentication options, do the following:

1. Click the **Server settings** button.
2. Select the **Use custom settings** check box.
3. Specify the application client ID and the tenant ID.

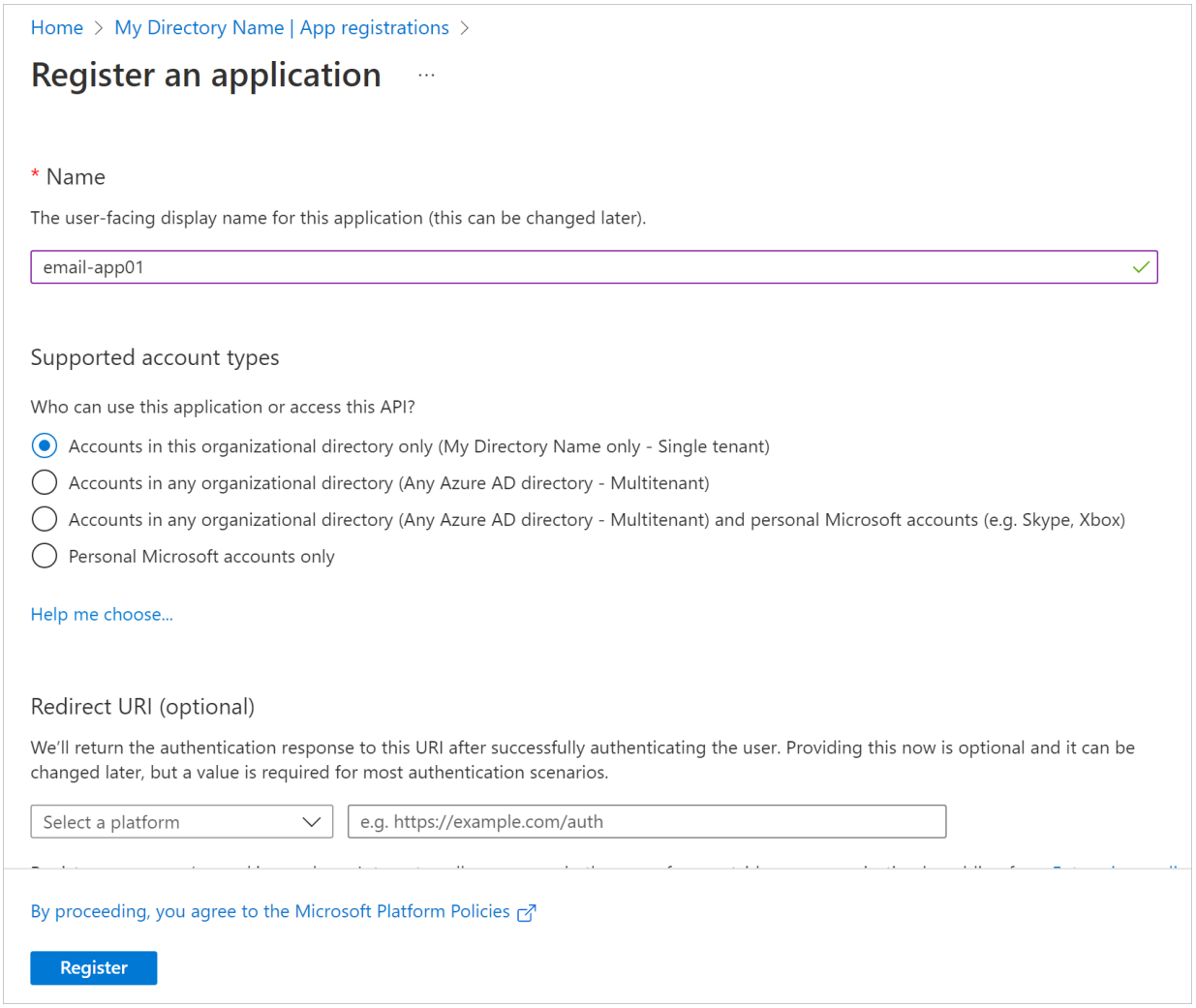
To learn how to register your custom application, see Registering Application in Microsoft Azure Portal.



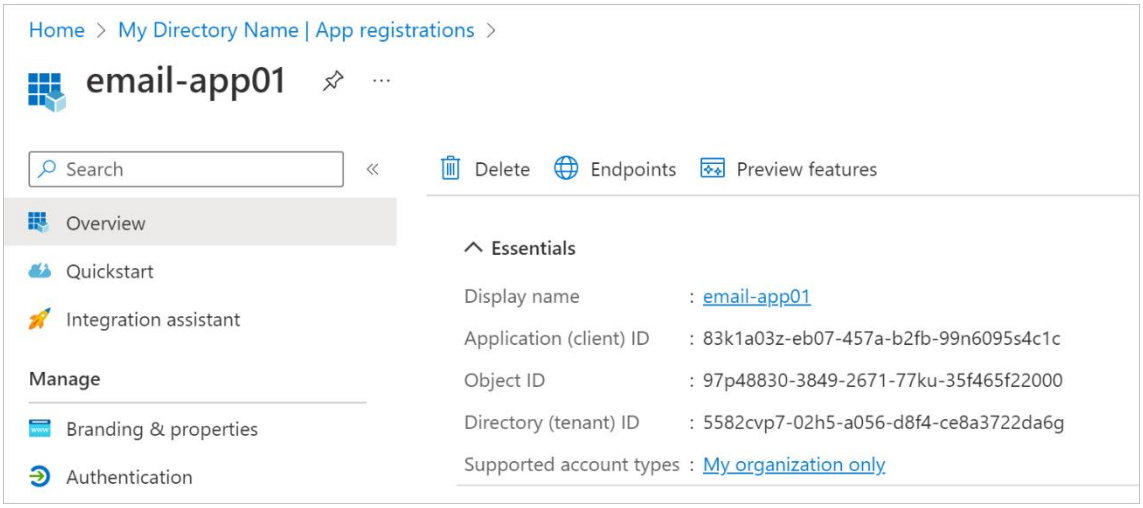
Registering Application in Microsoft Azure Portal

If you want to use your own web application for email notifications, you need to configure it in the Microsoft Azure portal. To do this, perform the following steps:

1. Log in to the Microsoft Azure portal under Exchange Online credentials that has permissions to register Azure AD applications.
2. Register the application. To do this, open **Azure Active Directory** > **App registrations** and click **New registration:**
   a. In the **Name** field, specify the name of your application.
   b. In the **Supported account types** section, select the **Accounts in this organizational directory only** option.
   c. Click **Register**.

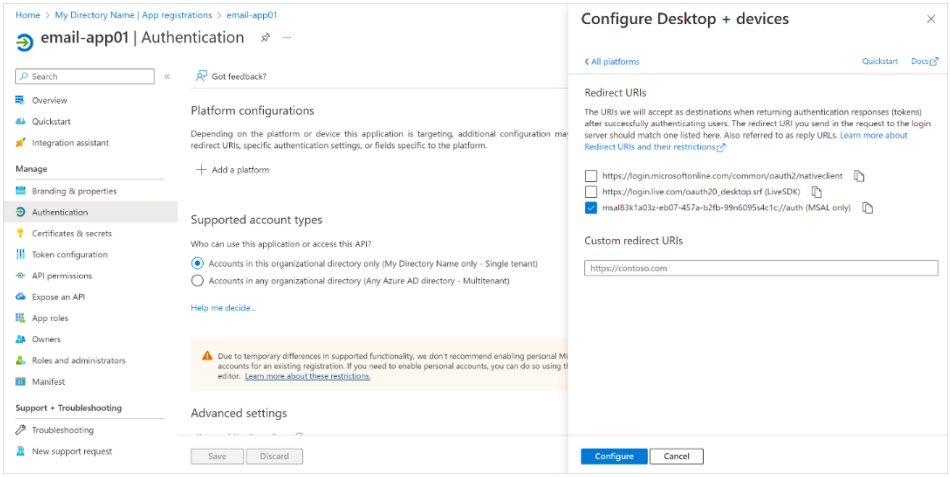


After registration, you can copy application (client) ID and directory (tenant) ID. You can also find these credentials later in the **Overview** section of you application properties.



3. Add a platform configuration for your application. To do this, open **Authentication** > **Platform configurations** and click **Add a platform**:
   a. Select **Mobile and desktop applications**.
   b. Select the MSAL redirect URI generated in the following format: `msal<applicationid>://auth`.

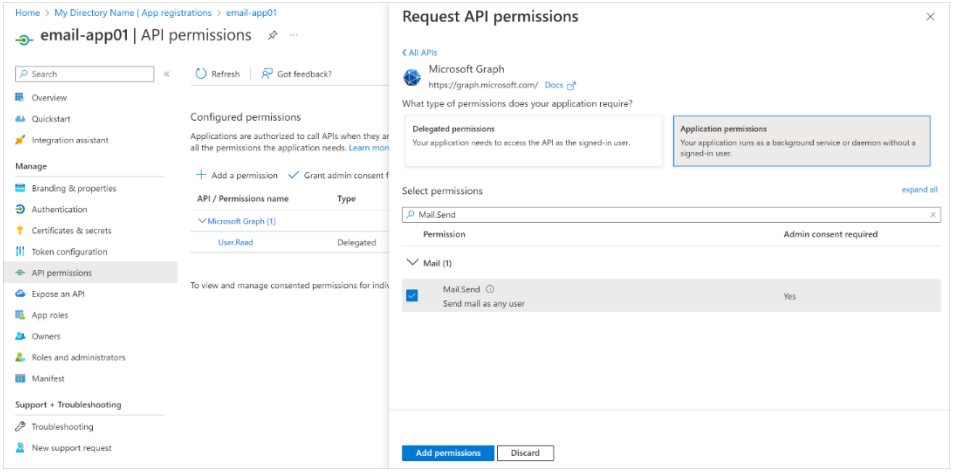
c. Click **Configure**.



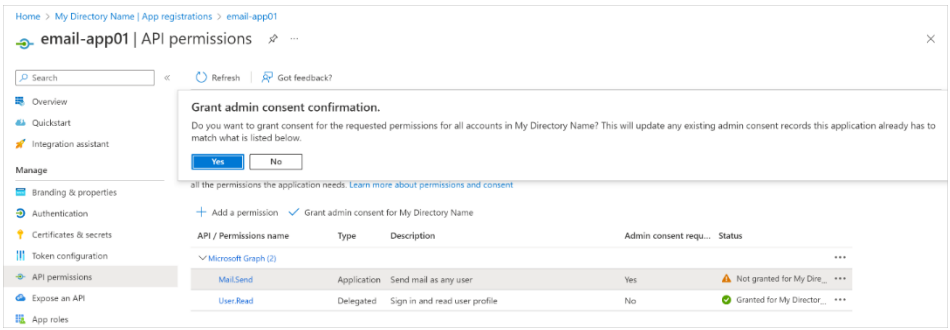
4. Grant the application the *Mail.Send* permission of Microsoft Graph. This will allow Veeam Agent for Microsoft Windows to call the Microsoft Graph API for sending email notifications. To do this, open **API permissions** and click **Add a permission**:

   a. Select **Microsoft Graph** > **Application Permissions**.

   b. Select the *Mail.Send* permission from the list and click **Add permissions**.



5. Click **Grant admin consent for <Your Directory Name>**. In the displayed window, click **Yes** to confirm the operation.



After you finish the registration, specify custom application registration settings when configuring the mail server for Microsoft 365 OAuth 2.0 authentication. For more information, see Microsoft 365 Server Settings.

Checking for New Product Versions and Updates

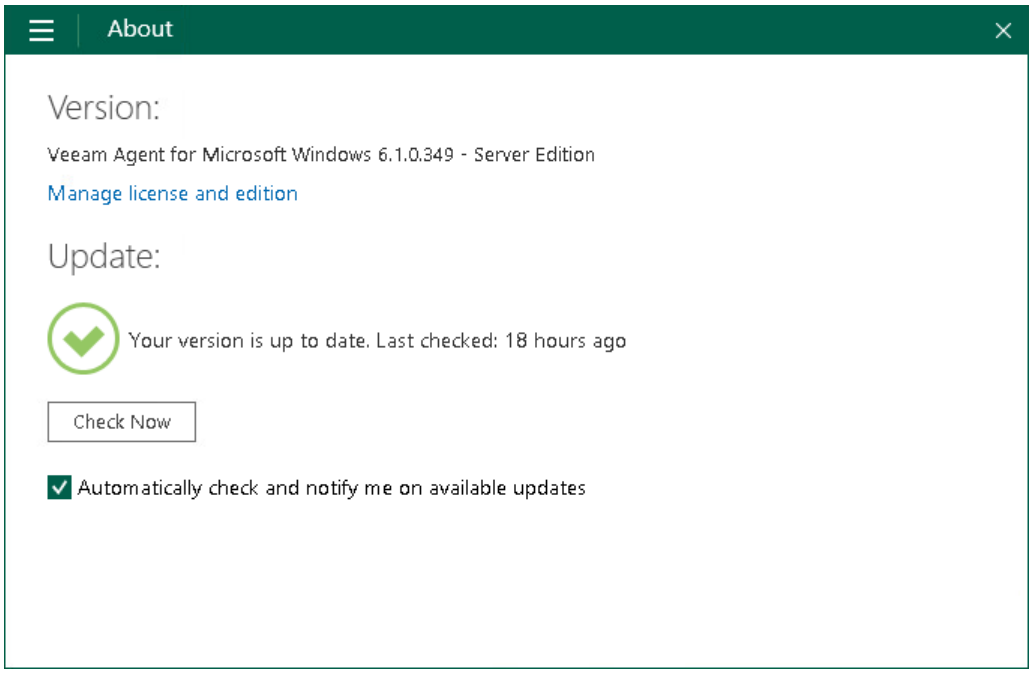
You can set up Veeam Agent for Microsoft Windows to automatically notify you about new product versions and updates. When a new version or patch becomes available, Veeam Agent for Microsoft Windows displays a notification in the notification bar. You can download the setup file and update Veeam Agent for Microsoft Windows. To learn more, see Upgrading Veeam Agent for Microsoft Windows.

By default, automatic notifications are enabled. To disable notifications:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **About**.
3. In the **Update** section, clear the **Automatically check and notify me on available updates** check box.

To manually check if product updates are available, click **Check Now**.

> **NOTE**
>
> Consider the following:
>
> - To get information about available product updates, Veeam Agent for Microsoft Windows sends request to the Veeam Update Notification Server (autolk.veeam.com).
> - For downloading setup files, Veeam Agent uses the Background Intelligent Transfer Service (BITS). If this service is disabled on the Veeam Agent computer, Veeam Agent for Microsoft Windows will not be able to download a setup file.



Managing Veeam CBT Driver

You can set up Veeam Agent to use the Veeam CBT driver instead of the default CBT mechanism. The Veeam CBT driver offers more efficient changed block tracking mechanism that will be useful for machines running applications with large database files. To learn more about how the Veeam CBT driver works, see Veeam Changed Block Tracking Driver.

You can perform the following operations with the Veeam CBT driver in Veeam Agent:

- Install the Veeam CBT driver.
- Remove the Veeam CBT driver.
- Remove the Veeam CBT driver with Veeam Recovery Media.
- Reset the Veeam CBT driver.

Installing Veeam CBT Driver

You can install the Veeam CBT driver at any time you need. To use the Veeam CBT driver, the Veeam Agent computer must meet the following requirements:

- Run a 64-bit version of Microsoft Windows OS.
- Run one of the following OSes:
  - Microsoft Windows 11 (from version 21H2 to version 23H2).
  - Microsoft Windows 10 (from version 1803 to version 22H2).
  - Microsoft Windows Server OS that is supported by Veeam Agent. For more information, see System Requirements.
- Run the Workstation or Server edition of Veeam Agent for Microsoft Windows.

IMPORTANT

Consider the following:

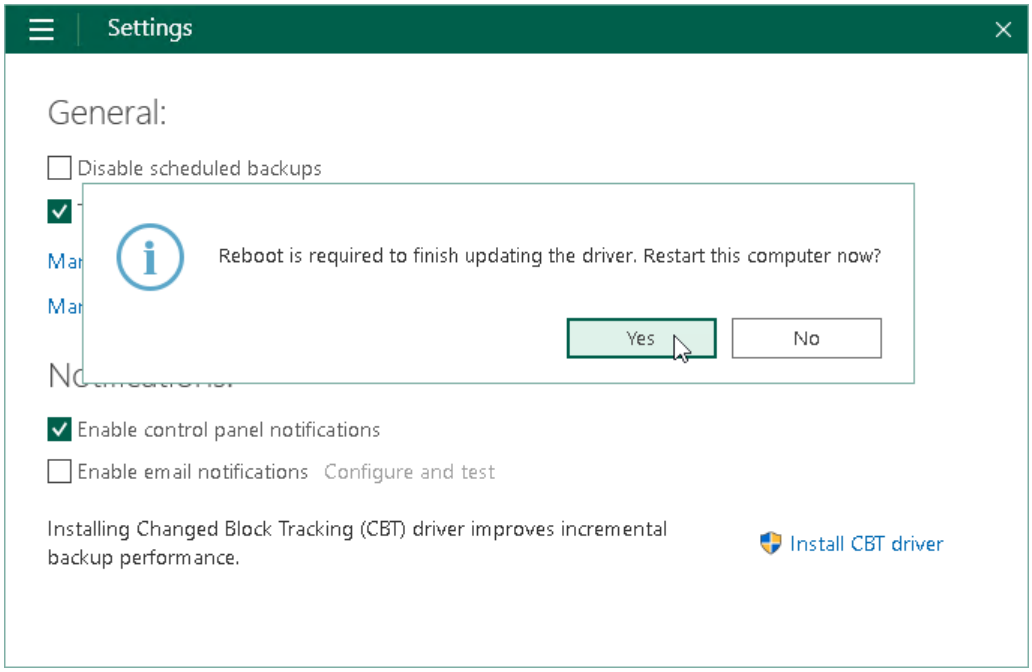
- Prior to installing the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, make sure that update KB3033929 is installed in the OS.

  The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver. To learn more, see this Microsoft KB article.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, 2012 or 2012 R2 if one or more volumes on this computer are encrypted with Microsoft BitLocker (or other encryption tool), or if you plan to use Microsoft BitLocker to encrypt volumes on this computer. Concurrent operation of Microsoft BitLocker and Veeam CBT driver may result in driver failures and may prevent the OS from starting.
- Do not install the Veeam CBT driver on a computer if you plan to use devices with hardware encryption made according to the TCG Opal Security Subsystem Class Specification. Operation of the driver on such devices may lead to a crash of the operating system. To learn more about the TCG Opal Security Subsystem Class Specification, see this Trusted Computing Group webpage.

To install the Veeam CBT driver:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click **Install CBT driver**.
4. To complete the installation process, Veeam Agent for Microsoft Windows needs to reboot the computer. To reboot the computer immediately, in the displayed window, click **Yes**. After Veeam Agent for Microsoft Windows reboots the computer, the driver will start tracking blocks that are changing on the volumes whose data you chose to back up in the backup job settings.

   If you choose not to reboot the computer immediately, Veeam Agent for Microsoft Windows will continue to use the default CBT mechanism until the next computer reboot.


Settings
General:
Disable scheduled backups
Reboot is required to finish updating the driver. Restart this computer now?
Yes
No
Enable control panel notifications
Enable email notifications
Configure and test
Installing Changed Block Tracking (CBT) driver improves incremental backup performance.
Install CBT driver

Removing Veeam CBT Driver

You can quickly remove the Veeam CBT driver, for example, if your Veeam Agent computer does not run applications with large database files any more, and you do not need to perform advanced change block tracking on this computer.

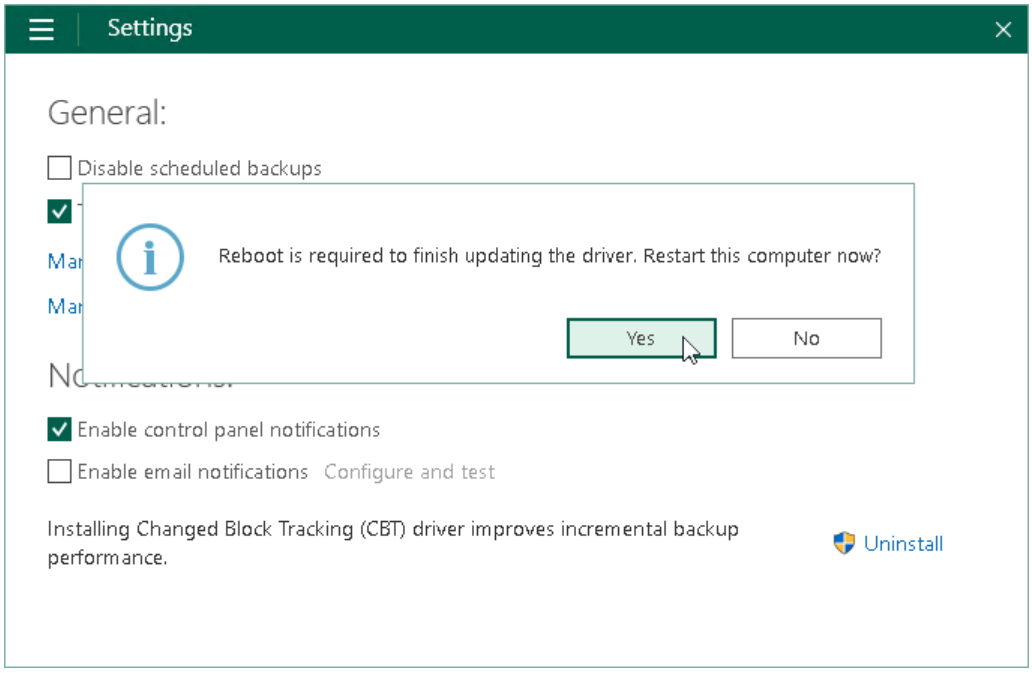
To remove the Veeam CBT driver:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click **Uninstall**.
4. To complete the uninstallation process, Veeam Agent for Microsoft Windows needs to reboot the computer. To reboot the computer immediately, in the displayed window, click **Yes**. After computer reboot, Veeam Agent for Microsoft Windows will use the default CBT mechanism to get the list of changed data blocks.

TIP

You can also uninstall the Veeam CBT driver in the Microsoft Windows control panel:

1. From the **Start** menu, select **Control Panel** > **Programs and Features**.
2. In the programs list, right-click **Veeam CBT Driver** and select **Uninstall**.
3. In the displayed window, click **Yes**.



Removing CBT Driver with Veeam Recovery Media

You can use the Veeam Recovery Media to remove the Veeam CBT driver from your Veeam Agent computer. This operation may be required, for example, if the OS on your computer fails to start after you have installed the Veeam CBT driver in Veeam Agent for Microsoft Windows.

To remove the Veeam CBT driver:

1. Boot from the Veeam Recovery Media.
2. On the Veeam Recovery Media screen, click **Tools** > **Command Prompt** or press **[Shift]** + **[F10]**.
3. Use a command with the following syntax:

```
X:\VeeamRecovery\Veeam.Endpoint.Recovery.exe -RemoveVeeamCBTDriver
```

4. Reboot the Veeam Agent computer.

NOTE

Veeam Agent for Microsoft Windows will remove the Veeam CBT Driver from the Veeam Agent computer. However, a record about the driver will remain in the Microsoft Windows control panel. To remove the record, from the **Start** menu, select **Control Panel** > **Programs and Features**. Then right-click **Veeam CBT Driver** in the programs list and select **Uninstall**.

Resetting CBT

In some cases, it may be required to reset CBT data collected by the Veeam CBT driver. For example, this may be necessary if you want to avoid performing active full backup after a volume was changed in a non-Windows OS.

To reset CBT, run the command line interface with administrative privileges and use one of the following commands:

- To reset CBT for all volumes of the Veeam Agent computer, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT all
```

- To reset CBT for a specific volume, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT %volumeMountPoint%
```

or

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT %volumeUUID%
```

where:

  - `%volumeMountPoint%` — mount point of the volume, for example: `C:\`.
  - `%volumeUUID%` — ID of the volume, for example: `\\?\Volume{1214be80-1165-41e5-8244-8fbf79d85c31}`.

After CBT reset, during the next backup job session, Veeam Agent for Microsoft Windows will create incremental backup. The backup job session will require greater time, because Veeam Agent for Microsoft Windows will need to read all data from the backed-up volumes.

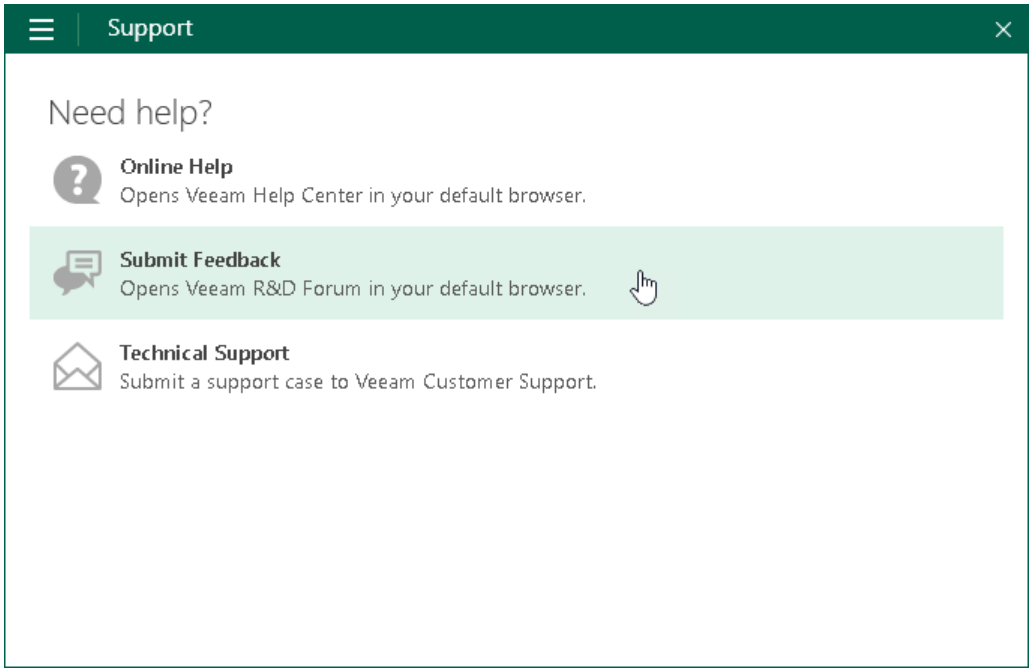
Getting Support

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 Microsoft Windows User Guide.
- You can visit Veeam R&D Forums and share your opinion or ask a question.
- You can submit a support case to the Veeam Customer Support directly from the product. To learn more, see Reporting Issues.

To access help and support options in Veeam Agent:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Support**.
3. Click one of available options to get support on the product.



Reporting Issues

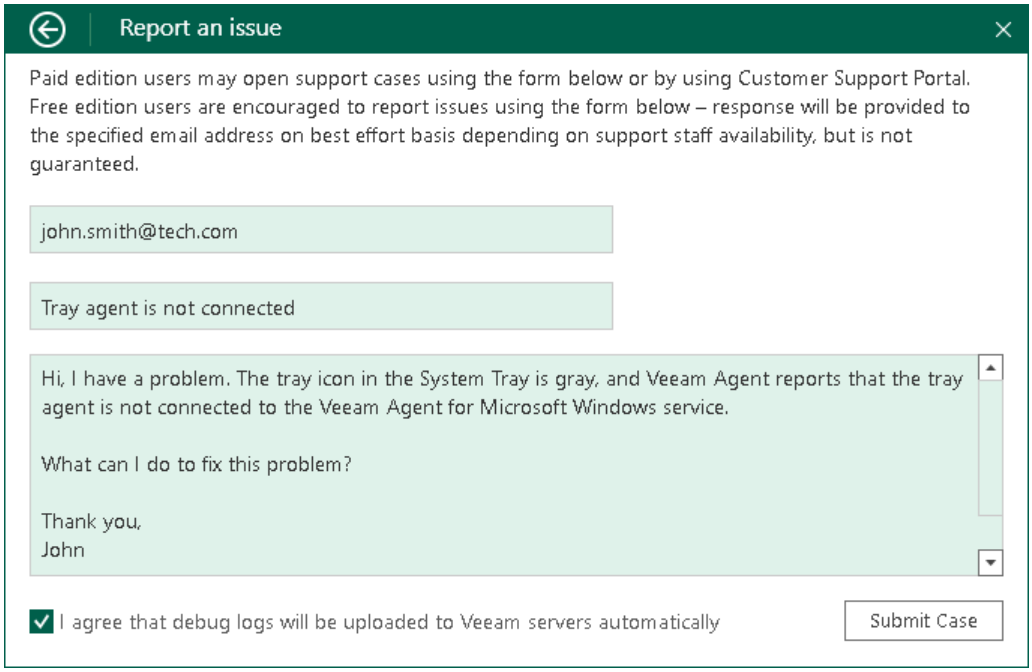
You can submit a support case in the Control Panel. To submit a support case:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Support**.
3. Click **Technical Support**.
4. In the email field of the **Report an issue** window, enter a valid email address.

   If the email address that you have entered in not registered at the Veeam Customer Support Portal, click **Register** on the right of the email field. Veeam Software will register your email address and send you a verification email to the specified address. When you receive a verification email, open it and click a link provided in the email to complete the verification procedure. After the verification procedure is complete, you will be able to submit a support case.
5. In the description fields, enter a short and detailed description of your problem.
6. Select the **I agree that debug logs will be uploaded to Veeam servers automatically** check box and click **Submit Case**.

Veeam Agent will automatically collect logs from your computer (without additional warnings) and open a support case at the Veeam Customer Support Portal.

> **IMPORTANT**
>
> Consider the following:
>
> - If you have any questions about the product functionality, do not submit a support case through the Veeam Customer Support Portal and do not send an email to the Veeam Customer Support directly. To submit a support case, use the Control Panel in Veeam Agent for Microsoft Windows.
> - You can submit a support case only in the Control Panel of the current version of Veeam Agent. If you use an older version of Veeam Agent, upgrade Veeam Agent and check whether the problem still exists in the current version. If the problem exists, use the Control Panel to submit a support case.


Report an issue
Paid edition users may open support cases using the form below or by using Customer Support Portal. Free edition users are encouraged to report issues using the form below – response will be provided to the specified email address on best effort basis depending on support staff availability, but is not guaranteed.
john.smith@tech.com
Tray agent is not connected
Hi, I have a problem. The tray icon in the System Tray is gray, and Veeam Agent reports that the tray agent is not connected to the Veeam Agent for Microsoft Windows service.
What can I do to fix this problem?
Thank you,
John
I agree that debug logs will be uploaded to Veeam servers automatically
Submit Case

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 Microsoft Windows 6.1 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 Microsoft Windows 6.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.0 on the Veeam backup server.

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 Veeam Agent backups to Hyper-V VMs.
- Restore Veeam Agent backups to VMware vSphere VMs.
- Restore Veeam Agent backups to Nutanix VMs.
- Restore volumes from Veeam Agent backups.
- Restore files and folders from Veeam Agent backups..
- Restore application items from Veeam Agent backups.
- Restore disks from Veeam Agent backups.
- Publish disks to analyze backup content.
- Restore data from Veeam Agent backups to Amazon EC2.

- Restore data from Veeam Agent backups to Microsoft Azure.
- Restore data from Veeam Agent backups to Google Compute Engine.
- 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.
- View Veeam Agent backup job statistics.
- Delete Veeam Agent backup jobs.
- View Veeam Agent backup properties.
- Create recovery tokens.
- Copy Veeam Agent backups.
- 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.

> **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.

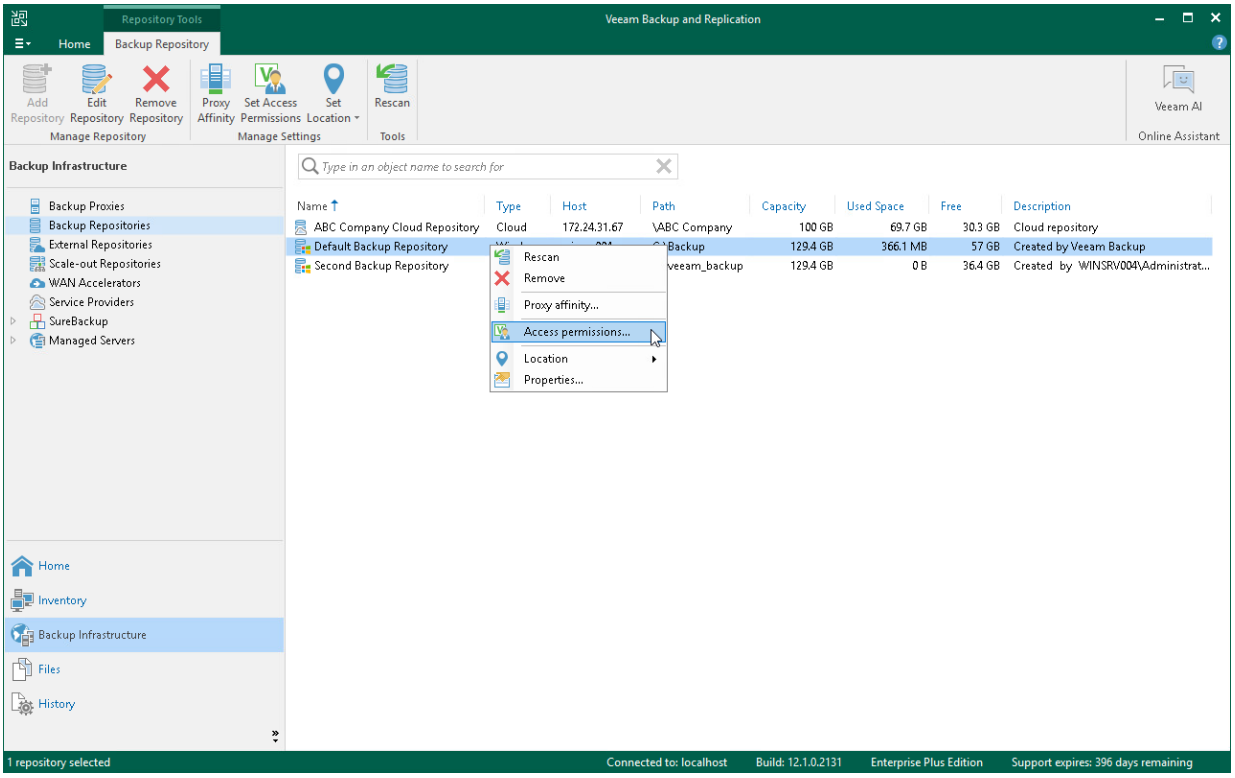
Access permissions are granted to security principals such as users and AD groups by the backup administrator working with Veeam Backup & Replication. Users with granted access permissions can target Veeam Agent backup jobs at this backup repository and perform restore from backups located in this backup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

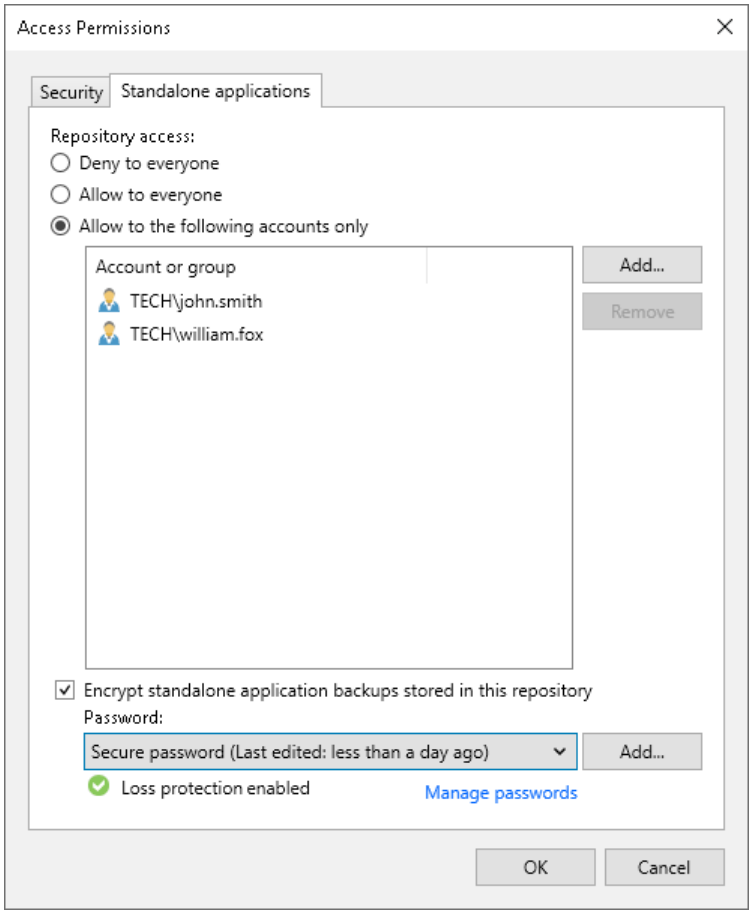
To grant access permissions to a security principal:

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.


Access Permissions
Security
Standalone applications
Repository access:
Deny to everyone
Allow to everyone
Allow to the following accounts only
Account or group
TECH\john.smith
TECH\william.fox
Add...
Remove
Encrypt standalone application backups stored in this repository
Password:
Secure password (Last edited: less than a day ago)
Add...
Loss protection enabled
Manage passwords
OK
Cancel

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.

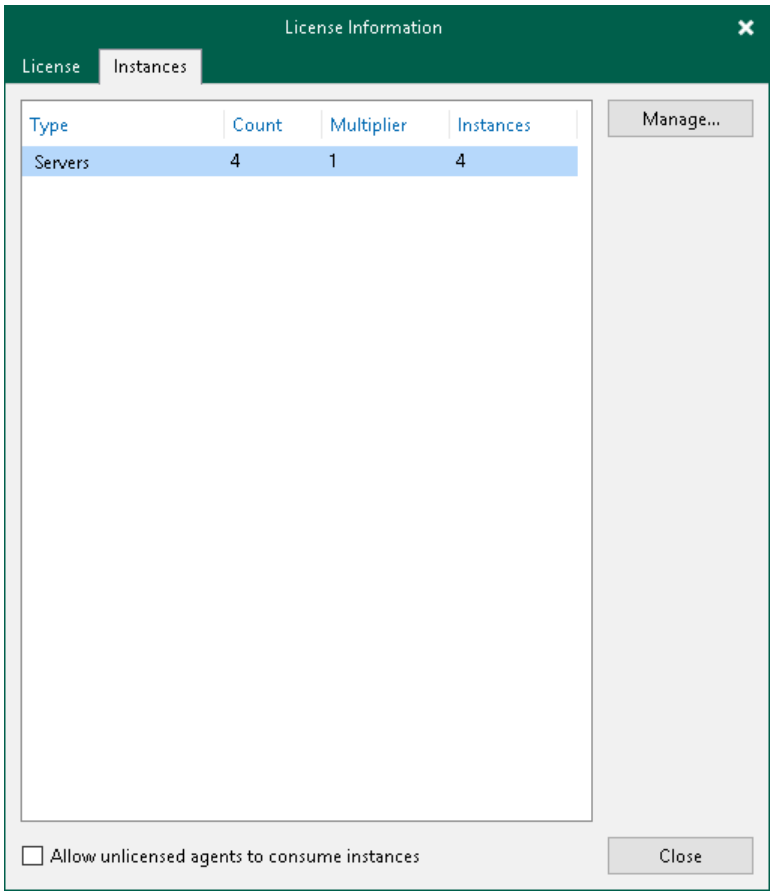
Managing Instance Consumption by Veeam Agents

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**.



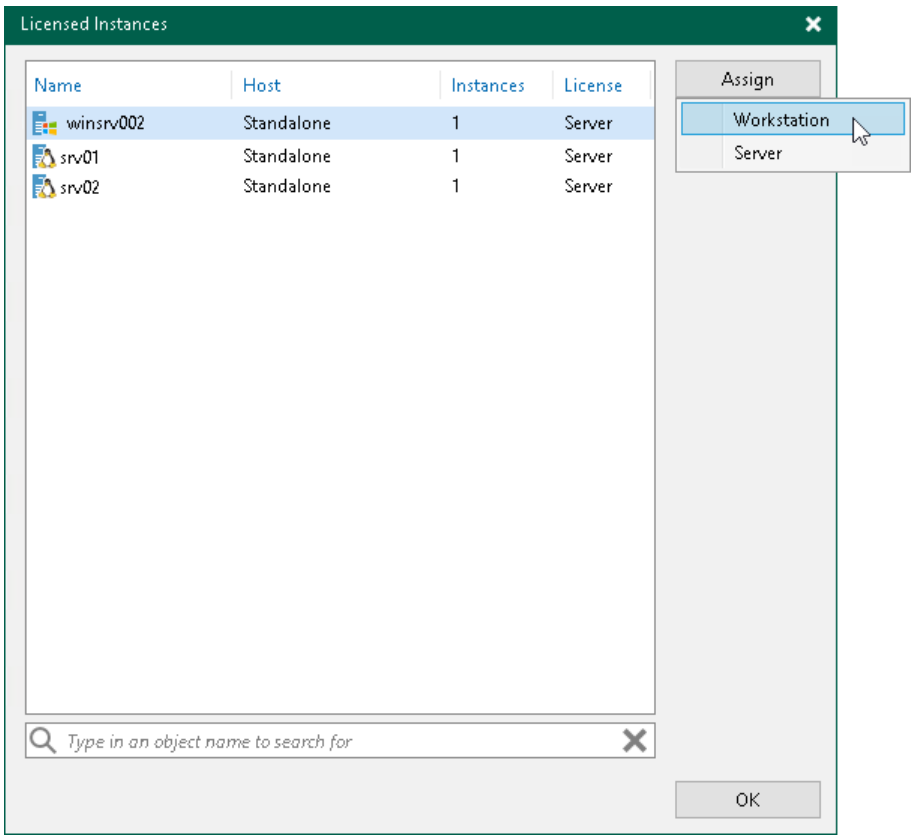
Assigning License to Veeam Agent

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**.

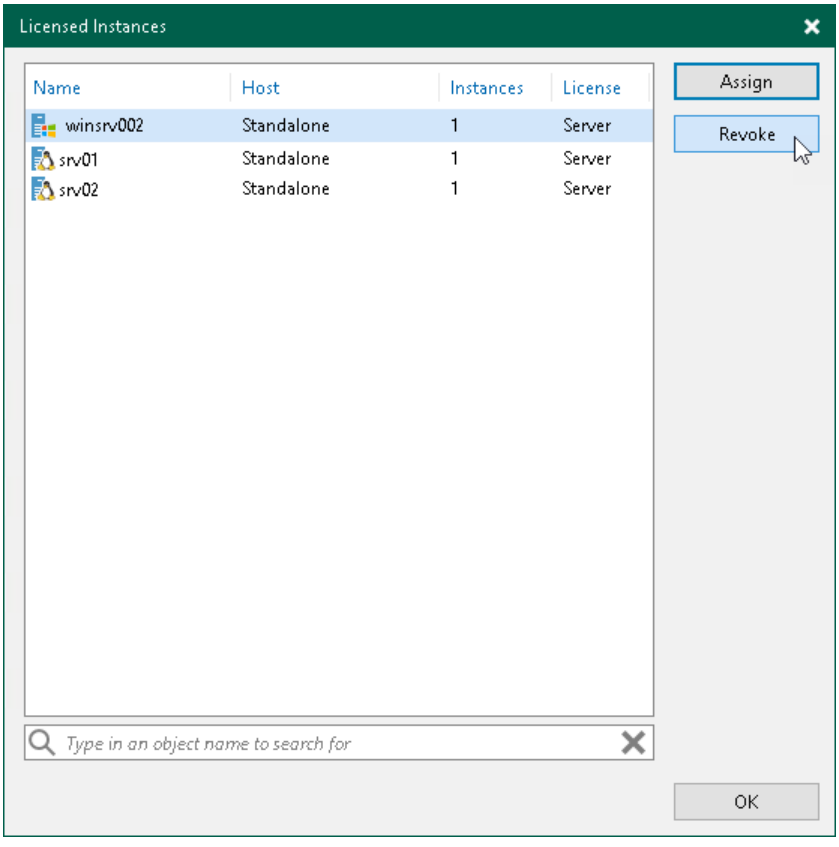
In the list of licensed instances, Veeam Backup & Replication displays Veeam Agents that have established a connection with the backup server when you created the backup job.

Revoking License from Veeam Agents

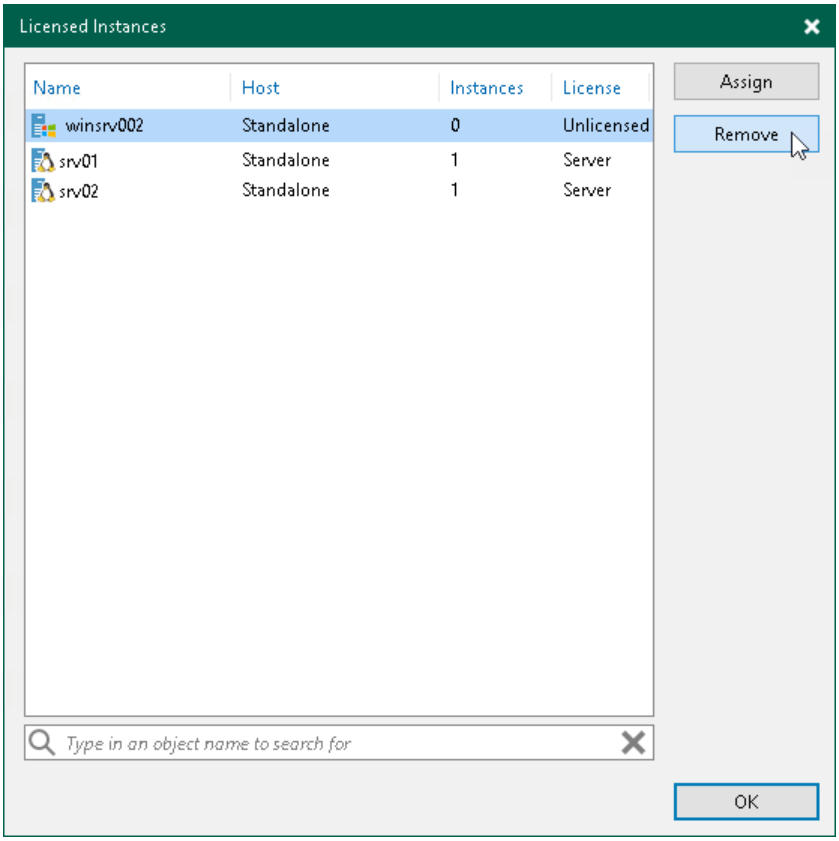
You can revoke the license from some Veeam Agents and re-apply it to other protected workloads. License revoking can be helpful, for example, if you do not want to use some Veeam Agents with Veeam Backup & Replication anymore.

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.

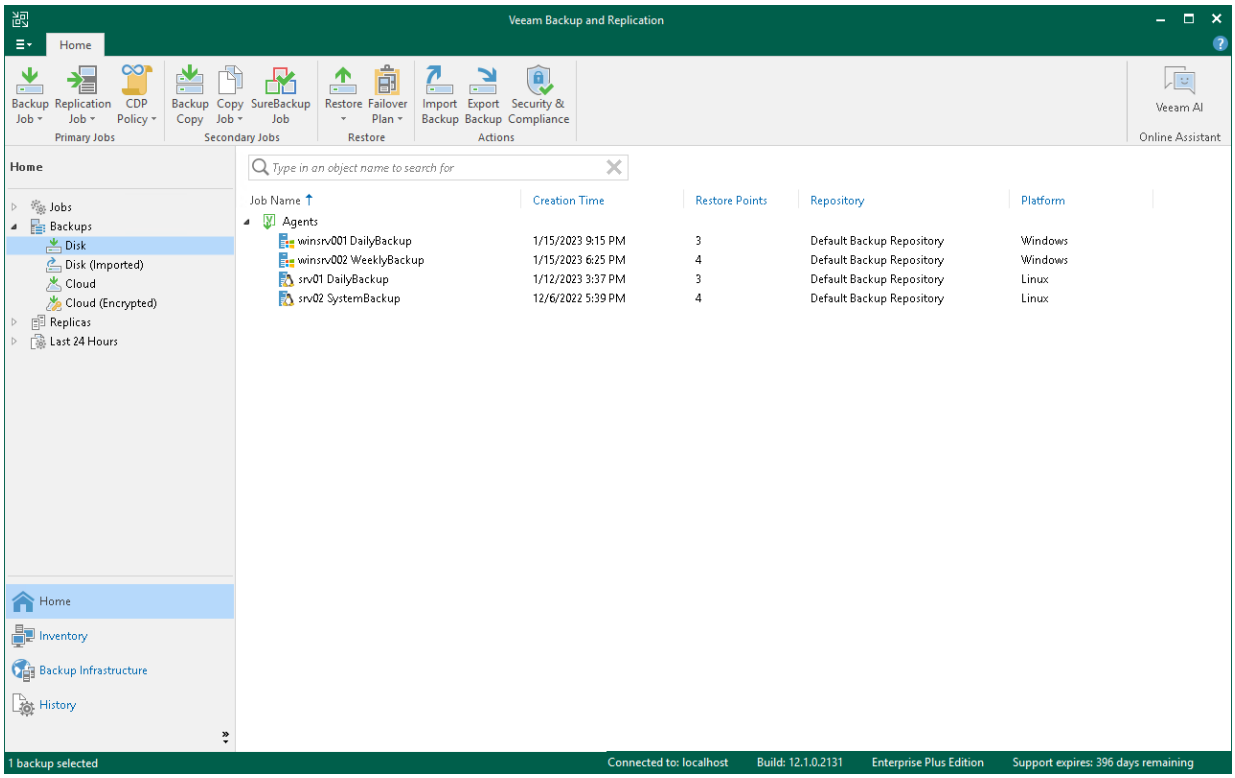
NOTE

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

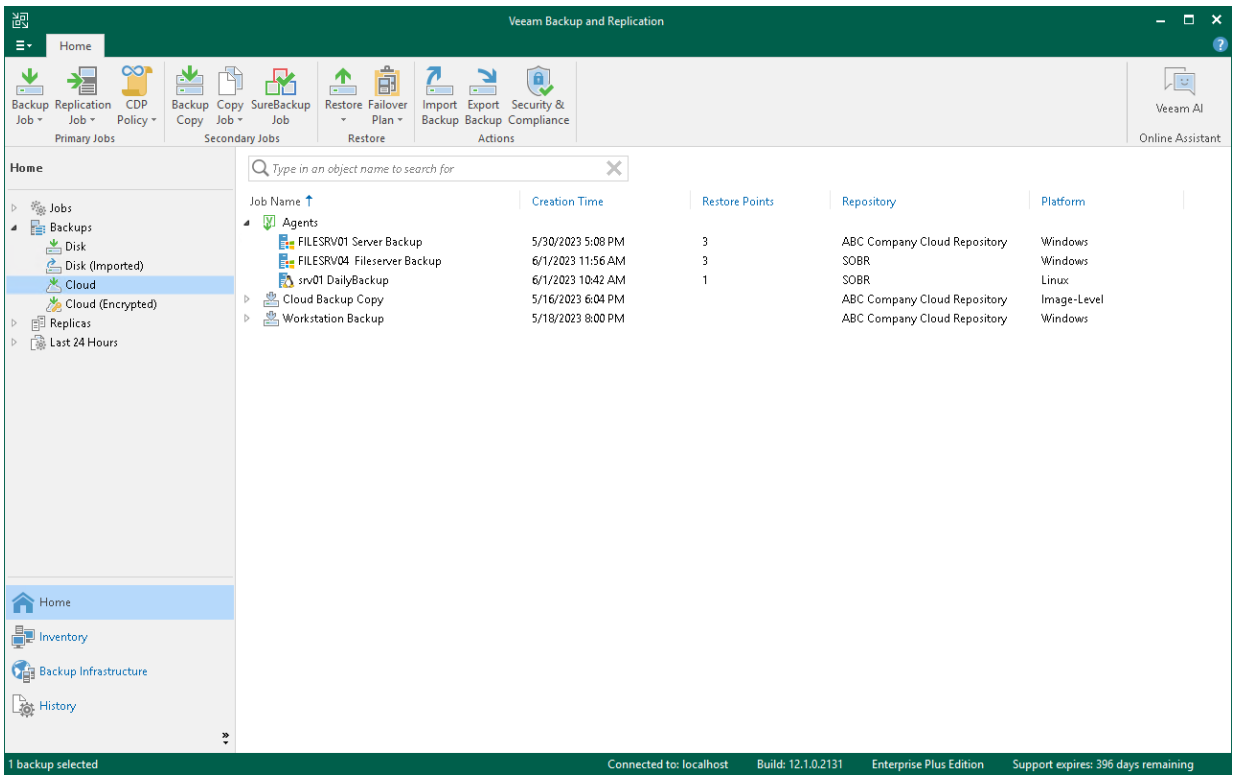
You can store backups created with Veeam Agent in cloud repositories provided to you by a Veeam Cloud Connect service provider. To do this, you must connect to the service provider and point the backup job to the cloud repository. To learn more, see Specify Service Provider Settings.

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:

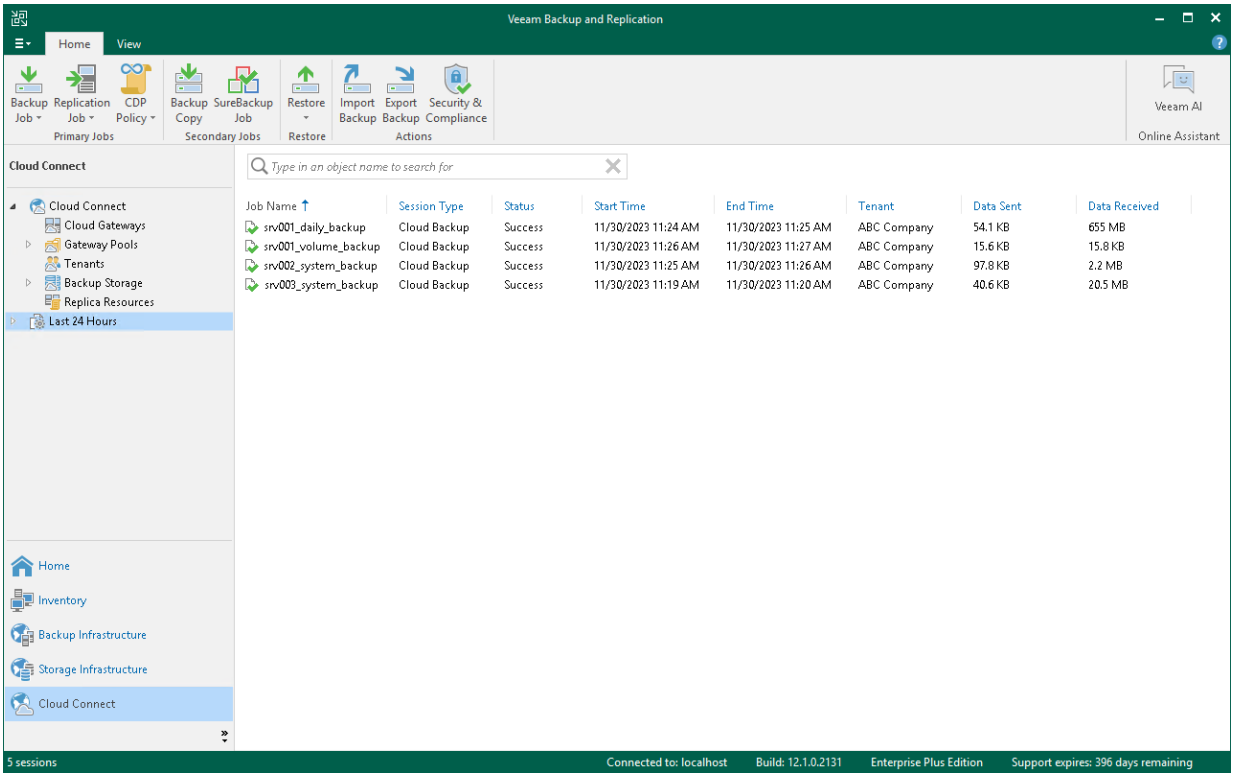
- Export computer disks as virtual disks.
- Restore guest OS files.
- Export restore points to standalone full backup files.



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.

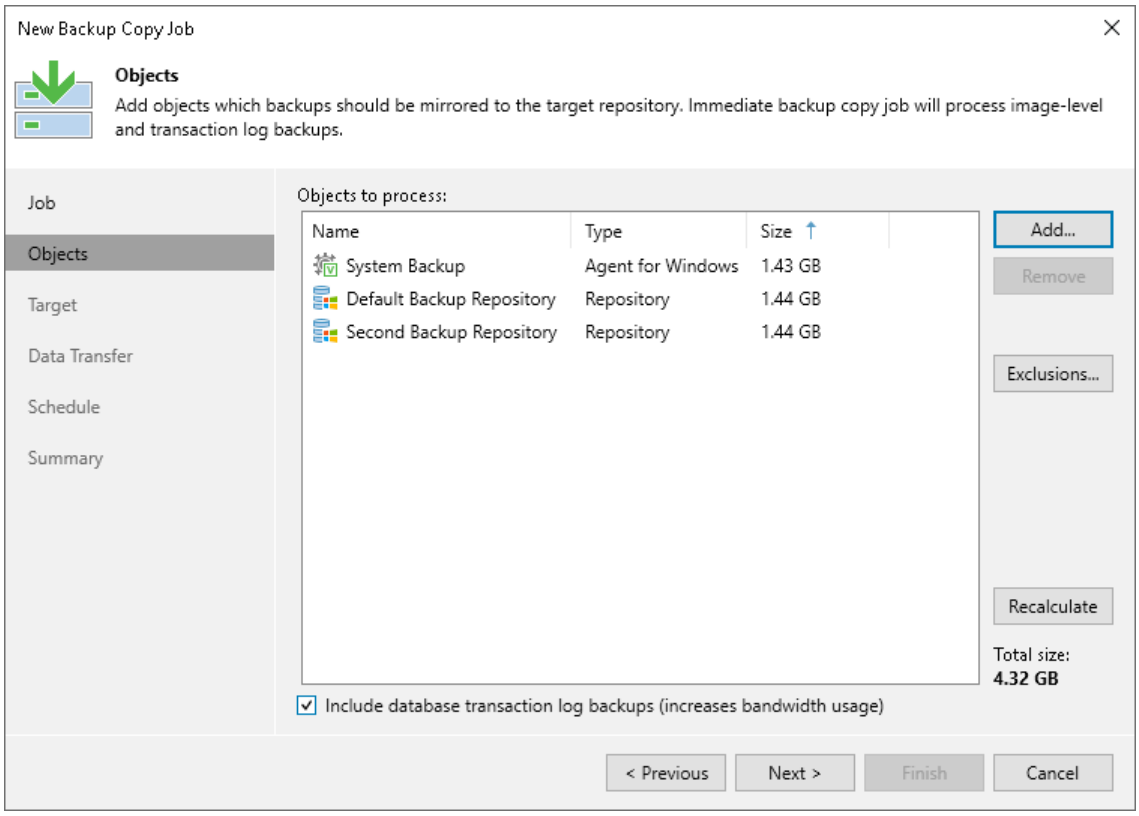

Veeam Backup and Replication
Home
View
Backup Job
Replication Job
CDP Policy
Backup Copy
SureBackup Job
Restore
Import Backup
Export Backup
Security & Compliance
Veeam AI
Primary Jobs
Secondary Jobs
Restore
Actions
Online Assistant
Cloud Connect
Type in an object name to search for
Cloud Connect
Cloud Gateways
Gateway Pools
Tenants
Backup Storage
Replica Resources
Last 24 Hours
Job Name
Session Type
Status
Start Time
End Time
Tenant
Data Sent
Data Received
srv001_daily_backup Cloud Backup Success 11/30/2023 11:24 AM 11/30/2023 11:25 AM ABC Company 54.1 KB 655 MB
srv001_volume_backup Cloud Backup Success 11/30/2023 11:26 AM 11/30/2023 11:27 AM ABC Company 15.6 KB 15.8 KB
srv002_system_backup Cloud Backup Success 11/30/2023 11:25 AM 11/30/2023 11:26 AM ABC Company 97.8 KB 2.2 MB
srv003_system_backup Cloud Backup Success 11/30/2023 11:19 AM 11/30/2023 11:20 AM ABC Company 40.6 KB 20.5 MB
Home
Inventory
Backup Infrastructure
Storage Infrastructure
Cloud Connect
5 sessions
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

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

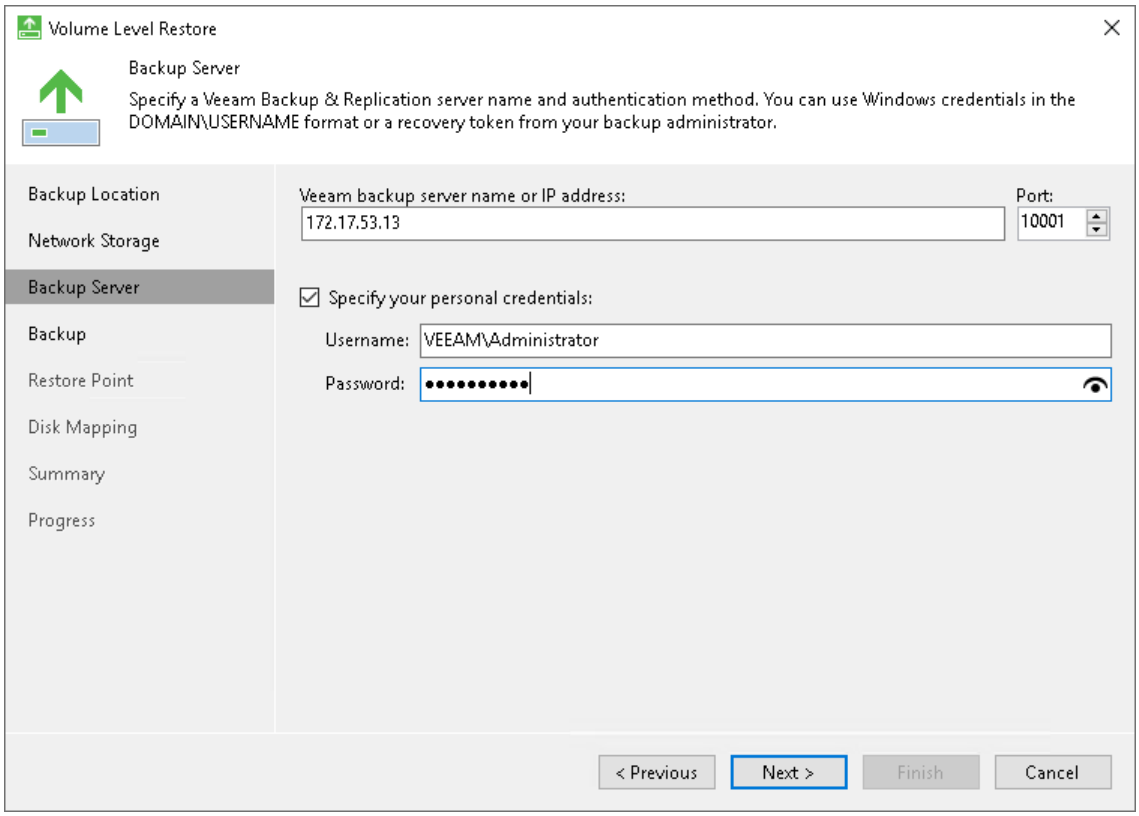
Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

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.

To do this:

1. In Veeam Agent, launch the **Volume Level Restore** wizard to restore volumes or **File Level Restore** wizard to restore files and folders. You can also boot from the Veeam Recovery Media and launch the **Veeam Recovery Media** wizard for data restore.
2. At the **Backup Location** step of the wizard, select **Network storage**.
3. At the **Network Storage** step of the wizard, select to restore data from the backup repository.
4. At the **Backup Server** wizard, specify settings for the Veeam backup server that manages the target backup repository where the copied backup is located.
5. Select the **Specify your personal credentials** check box and provide credentials for the user who has the *Veeam Backup Administrator* or *Veeam Restore Operator* role on the Veeam backup server.
6. Pass through the next steps of the wizard and select a backup and restore point from which you want to restore data.

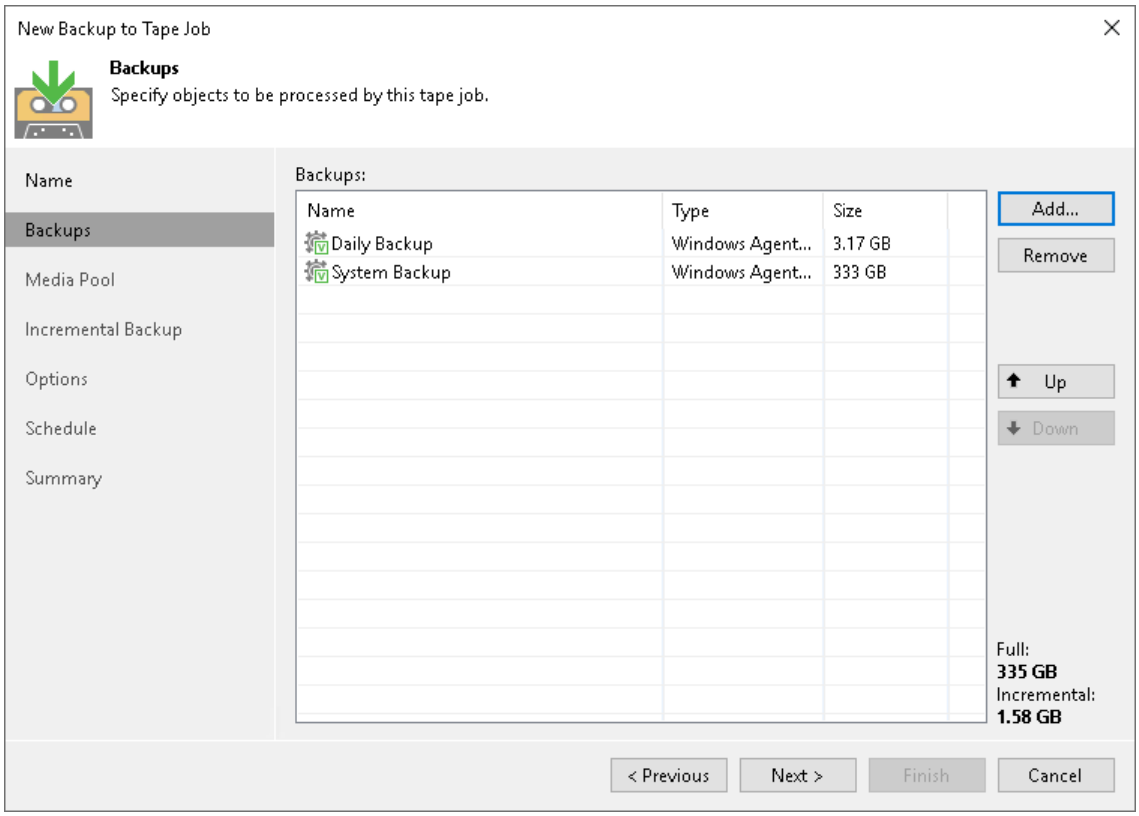


Archiving Veeam Agent Backups to Tape

You can configure backup to tape jobs to archive Veeam Agent backups to tape.

Backup to tape jobs treat Veeam Agent backups as usual backup files. The archiving job setup and processing procedures practically do not differ from the regular ones. To learn more about backup to tape jobs, see the Backup to Tape section in the Veeam Backup & Replication User Guide.

> **NOTE**
>
> Note that in backup to tape job schedule, you cannot select the **After this job** option for a Veeam Agent job that was configured directly on a Veeam Agent computer.



Restoring Data from Veeam Agent Backups

You can perform the following restore operations:

- Restore Veeam Agent backups to VMware vSphere VMs
- Restore Veeam Agent backups to Hyper-V VMs
- Restore Veeam Agent backups to Nutanix AHV VMs
- Restore data from Veeam Agent backups to Microsoft Azure
- Restore data from Veeam Agent backups to Amazon EC2
- Restore data from Veeam Agent backups to Google Compute Engine
- Restore computer volumes from Veeam Agent backups
- Restore individual files and folders from Veeam Agent backups
- Restore application items from Veeam Agent backups with Veeam Explorers
- 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 Veeam Agent Backup to vSphere VM

In the Veeam Backup & Replication console, you can use Instant Recovery to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment.

A restored VMware vSphere VM will have the same settings as the backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves the settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

- Amount of RAM.
- Number of CPU cores.
- Number of network adapters.
- Network adapter settings.
- BIOS UUID.

  If you do not want to preserve the backed-up machine UUID for a VMware vSphere VM, you can create a new UUID during the Instant Recovery configuration process.
- Number of disks and volumes.
- Size of volumes.

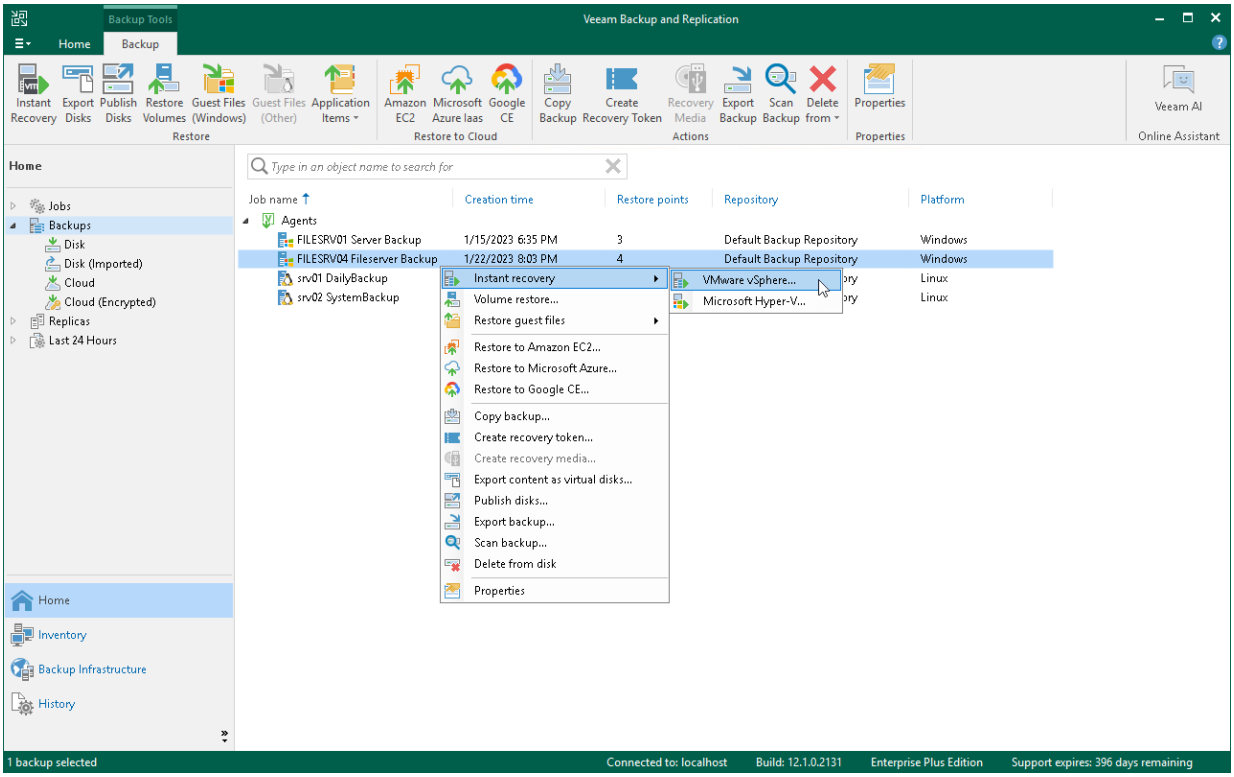
Considerations and Limitations

If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- If you restore a workload to the production network, make sure that the original workload is powered off.

Restore to vSphere VM

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to VMware vSphere section in the Veeam Backup & Replication User Guide.


Backup Tools
Veeam Backup and Replication
Home
Backup
Instant Recovery
Export Disks
Publish Disks
Restore Volumes
Guest Files (Windows)
Guest Files (Other)
Application Items
Amazon EC2
Microsoft Azure Iaas
Google CE
Copy Backup
Create Recovery Token
Recovery Media
Export Backup
Scan Backup
Delete from
Properties
Veeam AI
Restore
Restore to Cloud
Actions
Properties
Online Assistant
Home
Type in an object name to search for
Job name
Creation time
Restore points
Repository
Platform
Jobs
Backups
Disk
Disk (Imported)
Cloud
Cloud (Encrypted)
Replicas
Last 24 Hours
Agents
FILESRV01 Server Backup
1/15/2023 6:35 PM
3
Default Backup Repository
Windows
FILESRV04 Fileserver Backup
1/22/2023 8:03 PM
4
Default Backup Repository
Windows
srv01 DailyBackup
Linux
srv02 SystemBackup
Linux
Instant recovery
Volume restore...
Restore guest files
Restore to Amazon EC2...
Restore to Microsoft Azure...
Restore to Google CE...
Copy backup...
Create recovery token...
Create recovery media...
Export content as virtual disks...
Publish disks...
Export backup...
Scan backup...
Delete from disk
Properties
VMware vSphere...
Microsoft Hyper-V...
Home
Inventory
Backup Infrastructure
History
1 backup selected
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

Restoring Veeam Agent Backup to Hyper-V VM

In the Veeam Backup & Replication console, you can use Instant Recovery to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment.

A restored Hyper-V VM will have the same settings as the backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM.

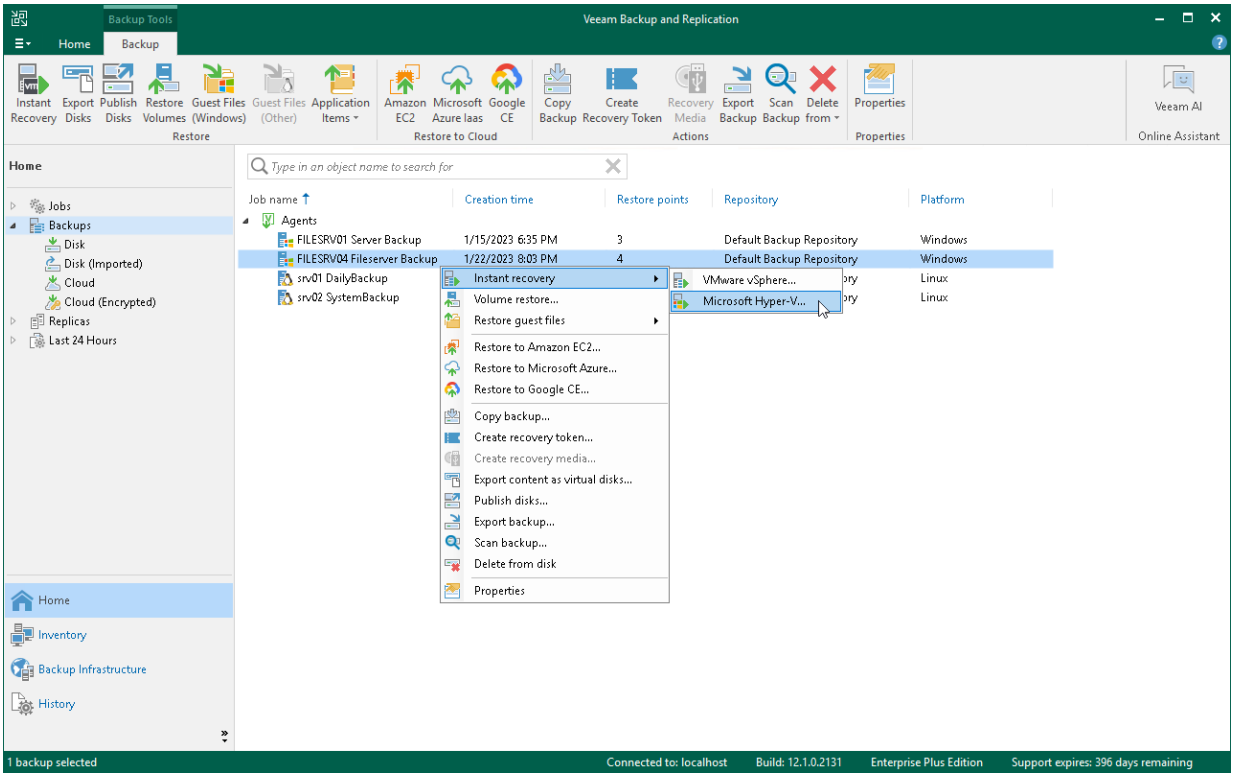
Considerations and Limitations

If you restore a Veeam Agent computer to a Hyper-V VM, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository only. You cannot use backups stored in a Veeam Cloud Connect repository for this operation.
- You cannot recover an EFI-based Veeam Agent computer that runs Windows 7, Windows Server 2008 or Windows Server 2008 R2 to a Hyper-V VM. These OSes can be restored only to a Generation 1 VM that does not support EFI. To learn more, see this Microsoft article.
- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- Veeam Agent computer disks are recovered as dynamically expanding virtual disks.
- By default, Veeam Backup & Replication automatically powers on a VM after restore. If you do not want to power on a VM after restore, you can change this setting during the Instant Recovery configuration process.
-

Restore to Hyper-V VM

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to Hyper-V section in the Veeam Backup & Replication User Guide.


Backup Tools
Veeam Backup and Replication
Home
Backup
Instant Recovery
Export Disks
Publish Disks
Restore Volumes
Guest Files (Windows)
Guest Files (Other)
Application Items
Amazon EC2
Microsoft Azure Iaas
Google CE
Copy Backup
Create Recovery Token
Recovery Media
Export Backup
Scan Backup
Delete from
Properties
Veeam AI
Restore
Restore to Cloud
Actions
Properties
Online Assistant
Home
Jobs
Backups
Disk
Disk (Imported)
Cloud
Cloud (Encrypted)
Replicas
Last 24 Hours
Type in an object name to search for
Job name
Creation time
Restore points
Repository
Platform
Agents
FILESRV01 Server Backup
1/15/2023 6:35 PM
3
Default Backup Repository
Windows
FILESRV04 Fileserver Backup
1/22/2023 8:03 PM
4
Default Backup Repository
Windows
srv01 DailyBackup
Linux
srv02 SystemBackup
Linux
Instant recovery
Volume restore...
Restore guest files
Restore to Amazon EC2...
Restore to Microsoft Azure...
Restore to Google CE...
Copy backup...
Create recovery token...
Create recovery media...
Export content as virtual disks...
Publish disks...
Export backup...
Scan backup...
Delete from disk
Properties
VMware vSphere...
Microsoft Hyper-V...
Home
Inventory
Backup Infrastructure
History
1 backup selected
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

Restoring Veeam Agent Backup to Nutanix VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Nutanix AHV VM in your virtualization environment.

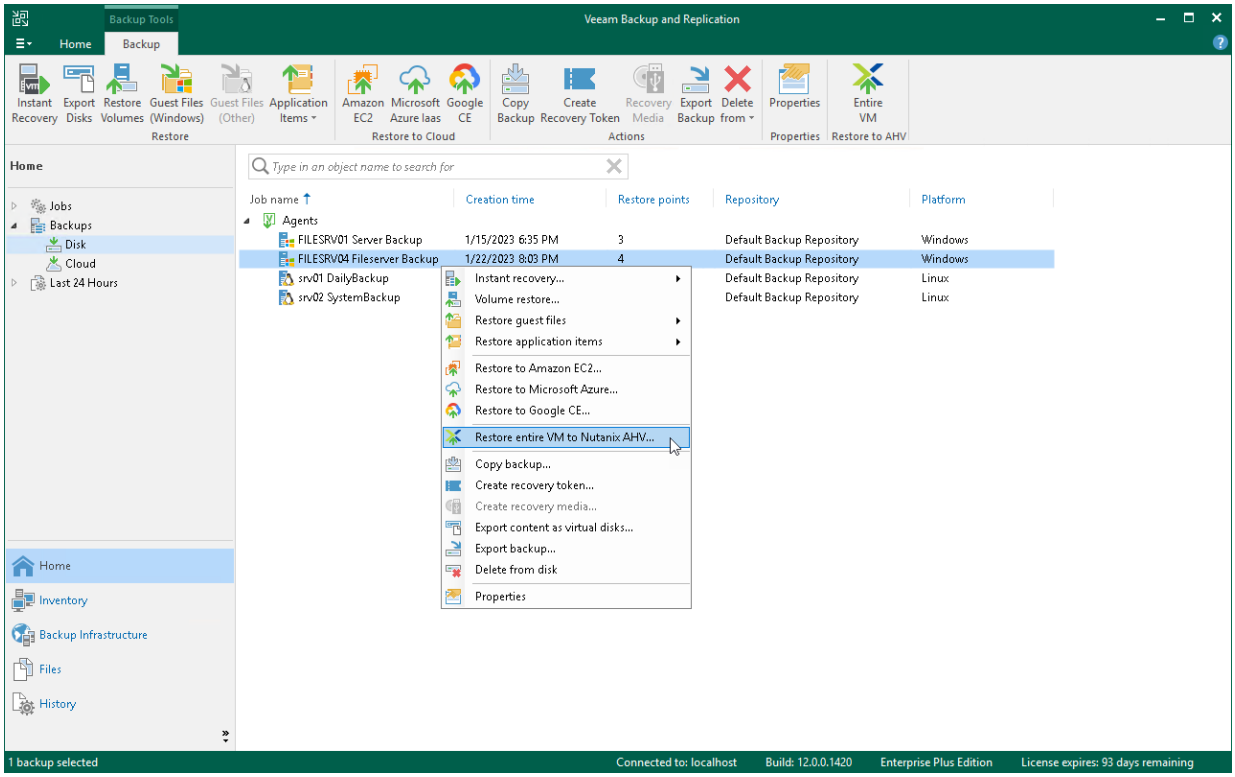
Considerations and Limitations

If you restore a Veeam Agent computer to a Nutanix AHV VM, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- To restore to Nutanix AHV, you must install Nutanix AHV Plug-in on the Veeam Backup & Replication server. To learn more, see the Installation section in the Veeam Backup for Nutanix AHV User Guide.

Restore to Nutanix AHV

The procedure of restore to Nutanix AHV for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Nutanix AHV, see the Restoring VMs Using Veeam Backup & Replication Console section in the Veeam Backup for Nutanix AHV User Guide.



Restoring to Microsoft Azure

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Microsoft Azure.

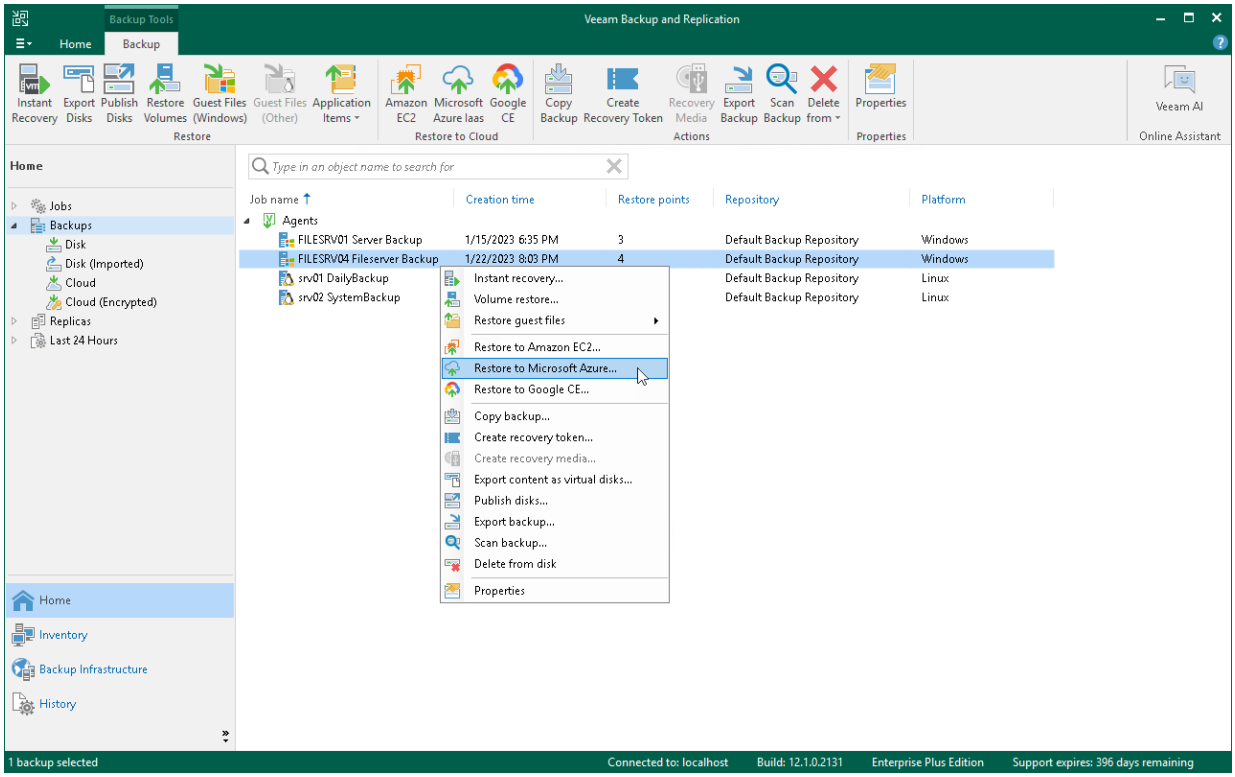
Considerations and Limitations

If you restore a Veeam Agent computer to Microsoft Azure, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.
- If you recover an EFI-based system to Microsoft Azure, Veeam Agent will restore a BIOS-based Generation 1 VM.
- Veeam Backup & Replication offers experimental support for generation 2 VMs within restore to Microsoft Azure feature. To learn more, see the Generation 2 VM Support section in the Veeam Backup & Replication User Guide.

Restore to Microsoft Azure

The procedure of restore to Microsoft Azure from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Microsoft Azure, see the Restoring to Microsoft Azure section in the Veeam Backup & Replication User Guide.



Restoring to Amazon EC2

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Amazon EC2.

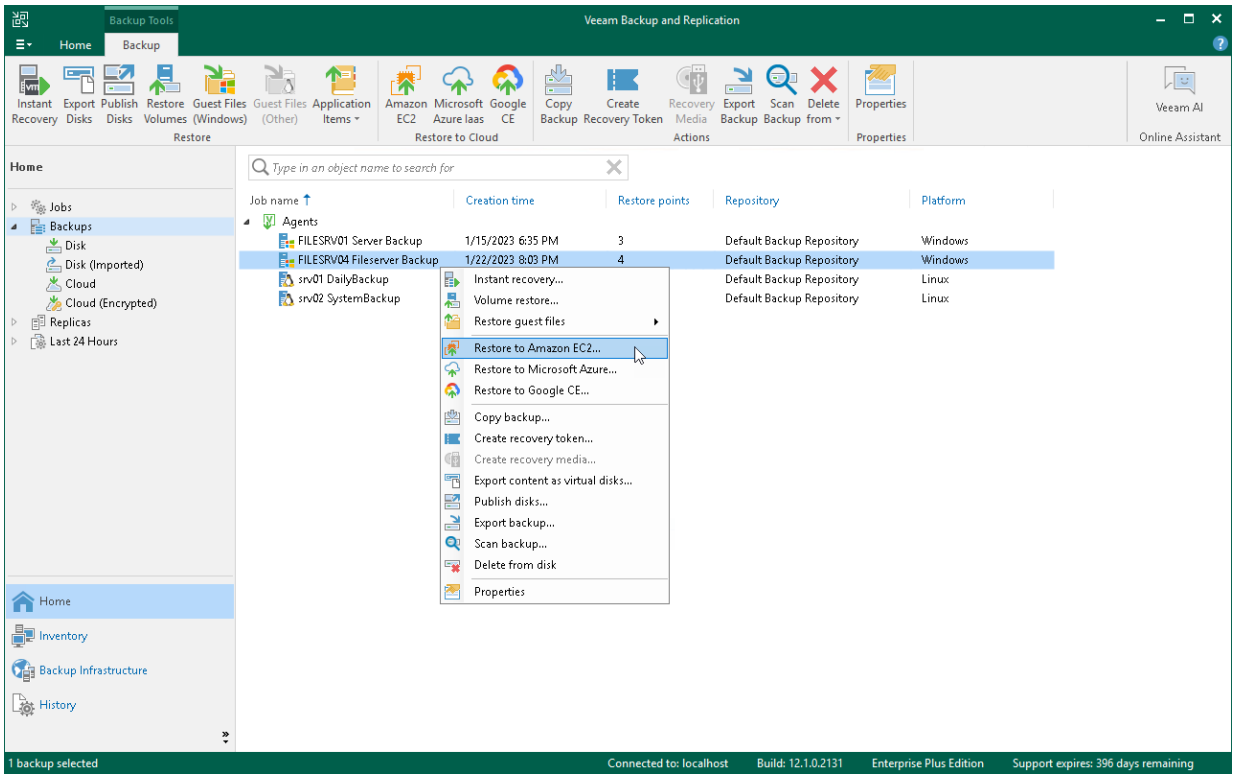
Considerations and Limitations

If you restore a Veeam Agent computer to Amazon EC2, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.

Restore to Amazon EC2

The procedure of restore to Amazon EC2 from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Amazon EC2, see the Restoring to Amazon EC2 section in the Veeam Backup & Replication User Guide.



Restoring to Google Compute Engine

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Google Compute Engine.

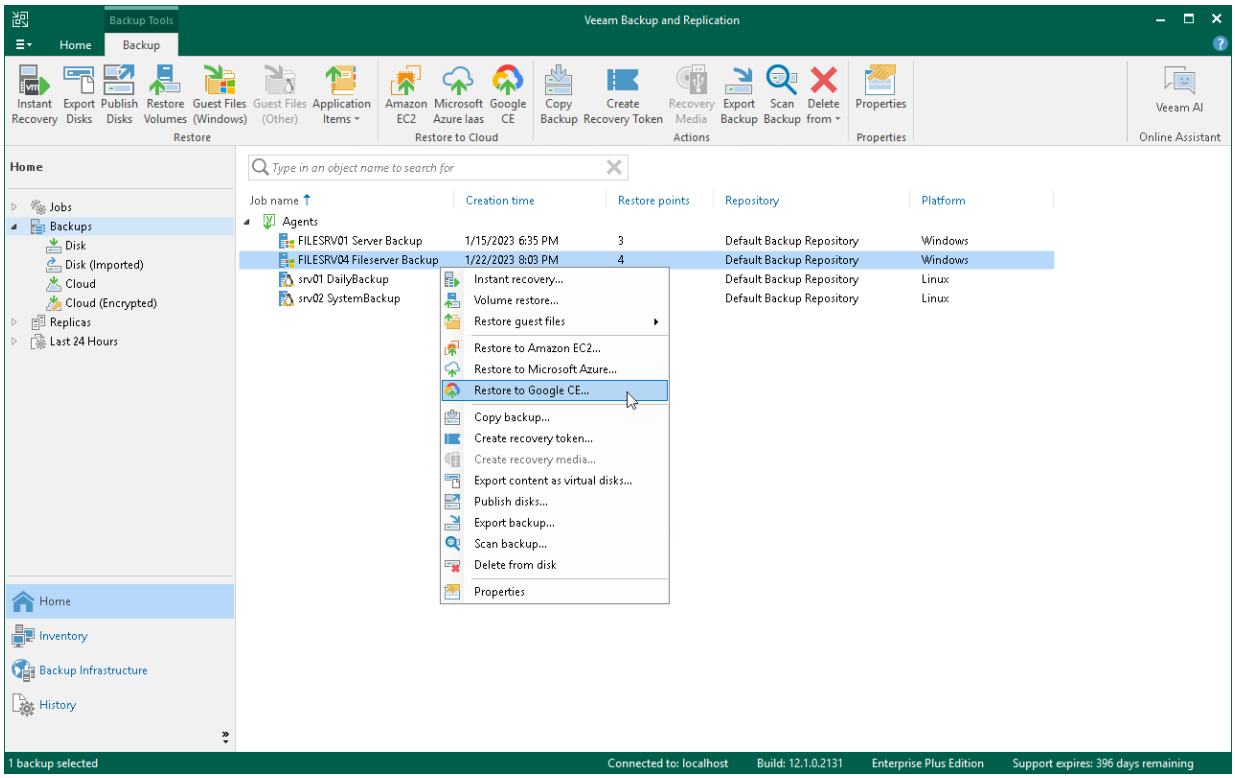
Considerations and Limitations

If you restore a Veeam Agent computer to Google Compute Engine, consider the following:

- You can use backups of Microsoft Windows computers stored in a Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.

Restore to Google Compute Engine

The procedure of restore to Google Compute Engine from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Google Compute Engine, see the Restoring to Google Compute Engine section in the Veeam Backup & Replication User Guide.



Restoring Volumes

You can use Veeam Backup & Replication to restore a specific computer volume or all volumes from a volume-level backup created with Veeam Agent for Microsoft Windows.

If data on a computer volume gets corrupted, you can restore this volume from the backup. For volume-level restore, you can use backups that were created at the volume level. File-level backups cannot be used for volume restore.

When you perform volume-level restore, Veeam Backup & Replication restores the entire content of the volume. It retrieves from the backup data blocks pertaining to a specific volume and copies them to the necessary location. Keep in mind that you cannot browse the volume in the backup and select individual application items, files and folders for restore. For granular file-level restore, you can use the restore guest files option.

A volume can be restored to its original location or a new location. If you restore the volume to its original location, Veeam Backup & Replication overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Backup & Replication overwrites data in the target location with data retrieved from the backup.

A volume can be restored to a new location that has greater or less space than the size of the volume in the backup. Depending on the amount of free disk space on target location, you can select either to shrink or to extend the volume during restore. To learn more, see Volume Resize.

- Complete the restore process.

Before You Begin

Before you begin the volume-level restore process, check the following prerequisites:

- The volume-level backup from which you plan to restore data must be successfully created at least once.
- A computer on which you want to restore a volume must be added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows operating in the standalone mode.

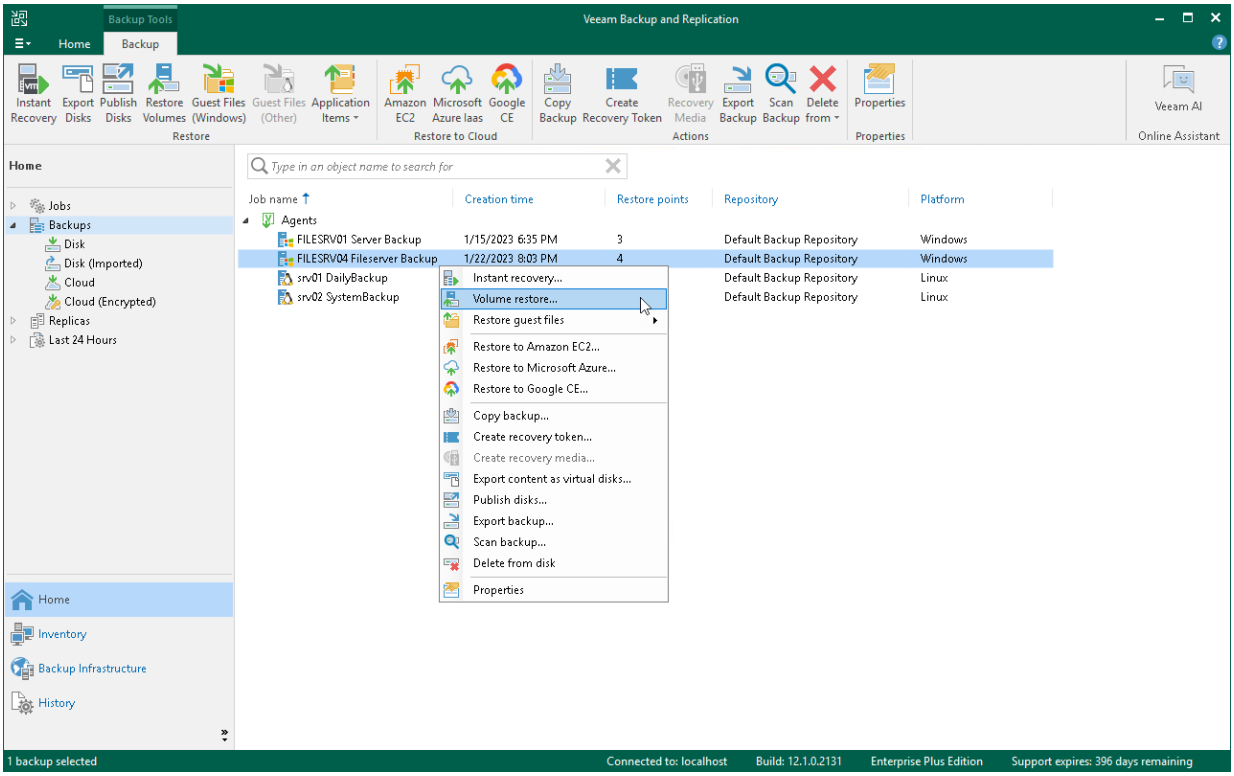
Volume-level restore has the following limitations:

- You cannot restore a system volume to a system volume of the original Veeam Agent computer or another computer with the running OS. To perform such restore, you need to boot the OS from the recovery image. To learn more, see Restoring Data with Veeam Recovery Media. You can also restore a system volume to a non-system volume that has enough free space.
- You cannot restore a volume to a volume on which the Microsoft Windows swap file is hosted.

Step 1. Launch Volume Level Restore Wizard

To launch the **Volume Level Restore** wizard, do either of the following:

- Open the **Home** tab and click **Restore** > **Agent** > **Disk restore** > **Volume restore**. 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 **Restore Volumes** on the ribbon or right-click the computer and select **Volume restore**. In this case, you will proceed immediately to the Restore Point step of the wizard.

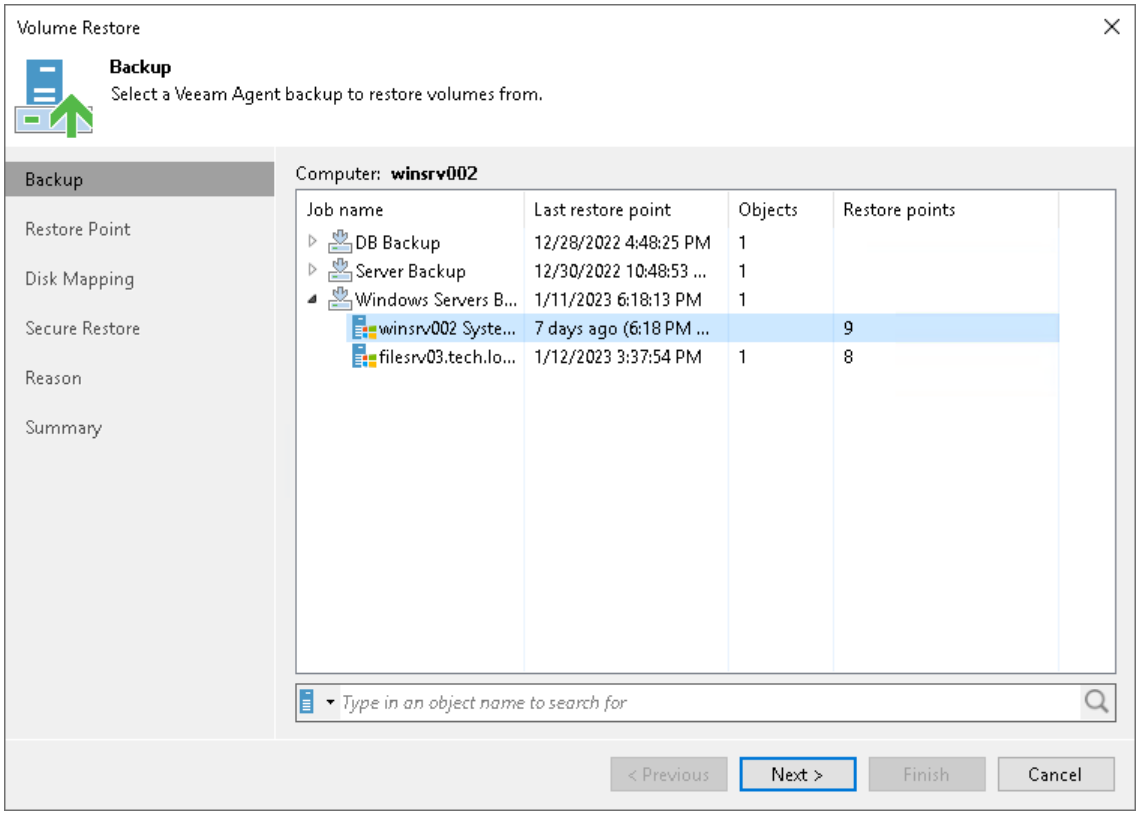


Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to recover data.

To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

In the list of backups, Veeam Backup & Replication displays only volume-level backups created with Veeam Agent for Microsoft Windows. File-level backups are not displayed.

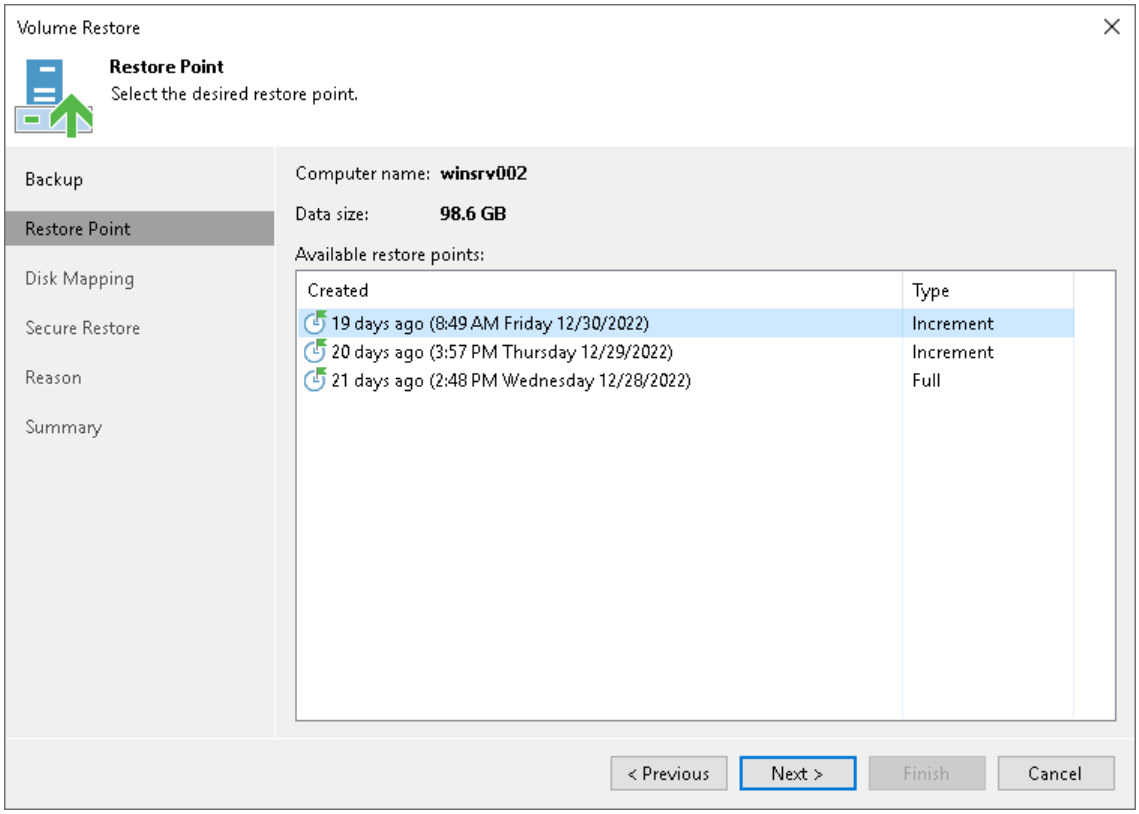


Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Backup & Replication uses the latest restore point. However, you can select any valid restore point to recover volumes to a specific point in time.

Veeam Backup & Replication displays restore points for volume-level backups only. For example, if you have run 3 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Backup & Replication will display only 3 restore points in the list.



Step 4. Map Restored Disks

At the **Disk Mapping** step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on the target computer.

> **IMPORTANT**
>
> It is strongly recommended that you change disk mapping settings only if you have experience in working with Microsoft Windows disks and partitions. If you make a mistake, your computer data may get corrupted.

To select volumes for restore:

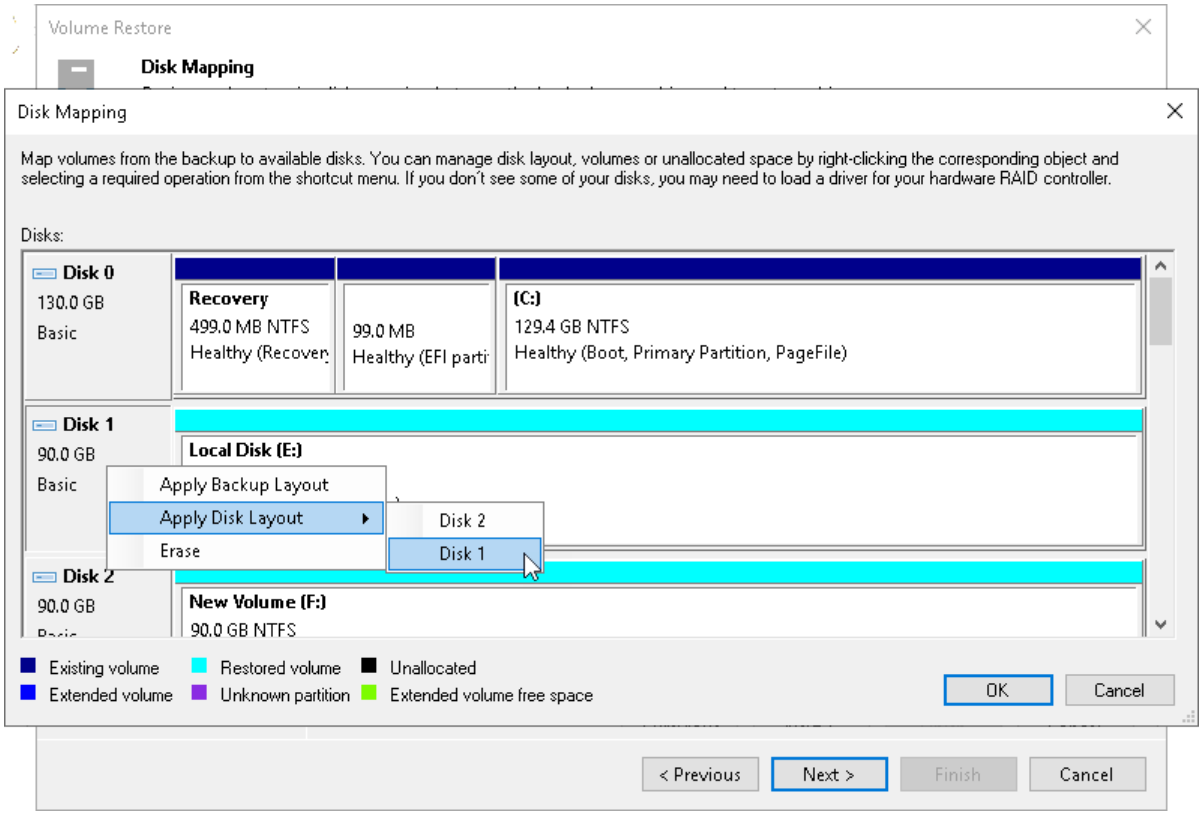
1. In the **Destination host** field, specify the target computer where you want to restore volumes. Click **Choose** and select the necessary computer. You can restore volumes only to computers that are added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows.

   If you select a computer included in a protection group for pre-installed Veeam Agents, you must provide credentials of the account that has administrator permissions on the target computer. Keep in mind that Veeam Backup & Replication will keep these credentials only during the restore process and delete them after the restore process completion. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

2. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. If you want to map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**.

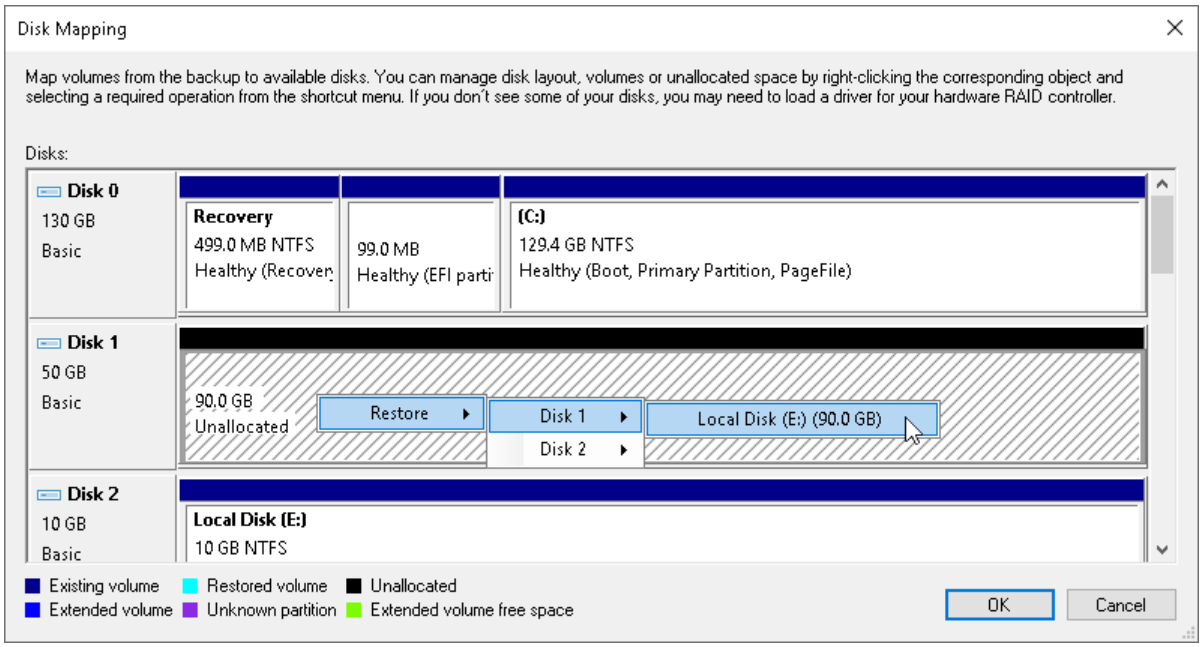
   > **NOTE**
   >
   > If Veeam Backup & Replication cannot map a volume automatically, Veeam Backup & Replication will prompt you to perform disk mapping manually. To proceed to the **Disk Mapping** window, click **Yes**.

3. In the **Disk Mapping** window, specify how volumes must be restored:
   - Right-click the target disk on the left and select the necessary disk layout:
     - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.
     - **Apply Disk Layout** — select this option if you want to apply to the current disk settings of another disk.
     - **Erase** — select this option if you want to discard the current disk settings.



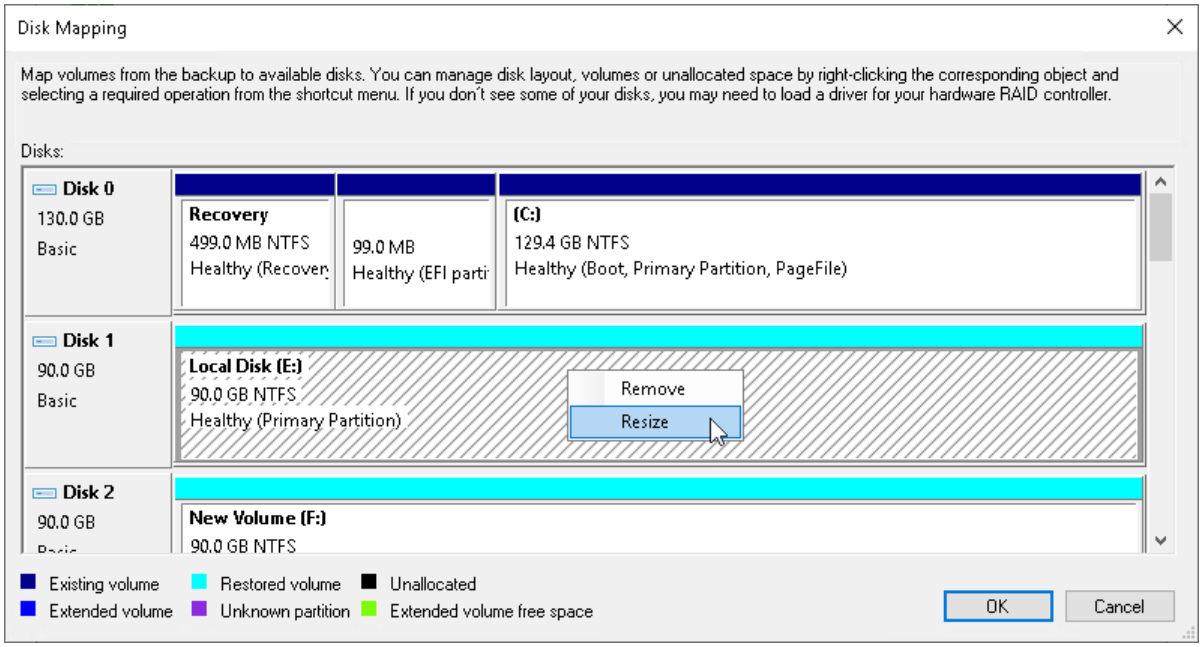
- Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

  If you want to change disk layout configured by Veeam Backup & Replication, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



4. [For restore with volume resize] You can resize a volume mapped by Veeam Backup & Replication to a target computer disk. To resize a volume, right-click it in the **Disk Mapping** window and select **Resize**. With this option selected, you will pass to the Volume Resize window.

> **NOTE**
>
> If you map a backup volume that is larger than the amount of available space on the target disk, Veeam Backup & Replication will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Backup & Replication will prepare to shrink the volume to the size of available disk space.



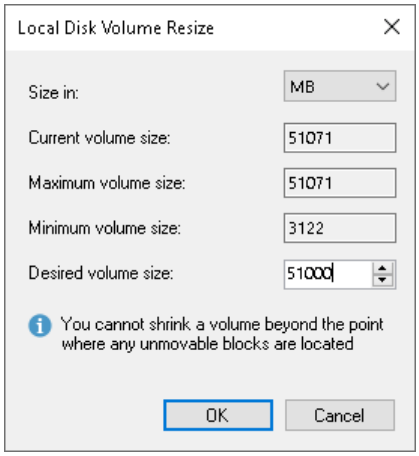
Step 5. Resize Restored Volumes

At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. A volume will be shrunk or extended to the specified size during the process of data restore.

> **NOTE**
>
> By default, Veeam Agent for Microsoft Windows displays volume size in megabytes (MB). This allows you to specify the desired size for the volume precisely. You can also choose to display volume size in gigabytes (GB). This may be helpful when you need to resize volumes on larger computer disks and want to simplify disk size calculations.
>
> When you use GB as a volume size unit, you can specify volume size with integral numbers, for example, 1 GB, 60 GB or 200 GB, but not 0,8 GB, 60,5 GB or 200,7 GB. However, if the maximum volume size is in fact greater than the displayed value for less than 1 GB, Veeam Agent for Microsoft Windows will automatically add the exceeding amount of disk space to the extended volume. For example, if the maximum volume size is 60,2 GB, Veeam Agent for Microsoft Windows will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Agent for Microsoft Windows will extend the volume to 60,2 GB.

To resize a volume:

1. Specify a volume you want to resize:
   a. Right-click a restored volume mapped to a target disk and select **Resize**.
   b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Backup & Replication will prompt you to shrink the restored volume.
2. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.

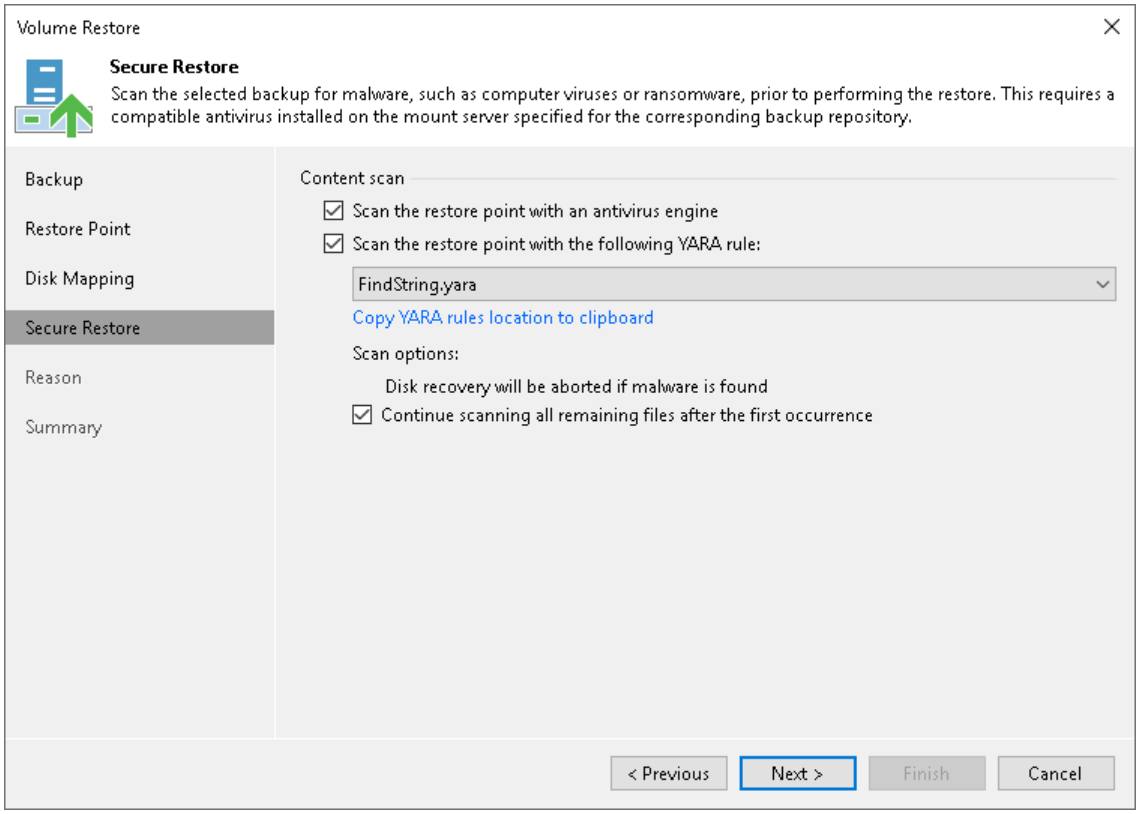


Step 6. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

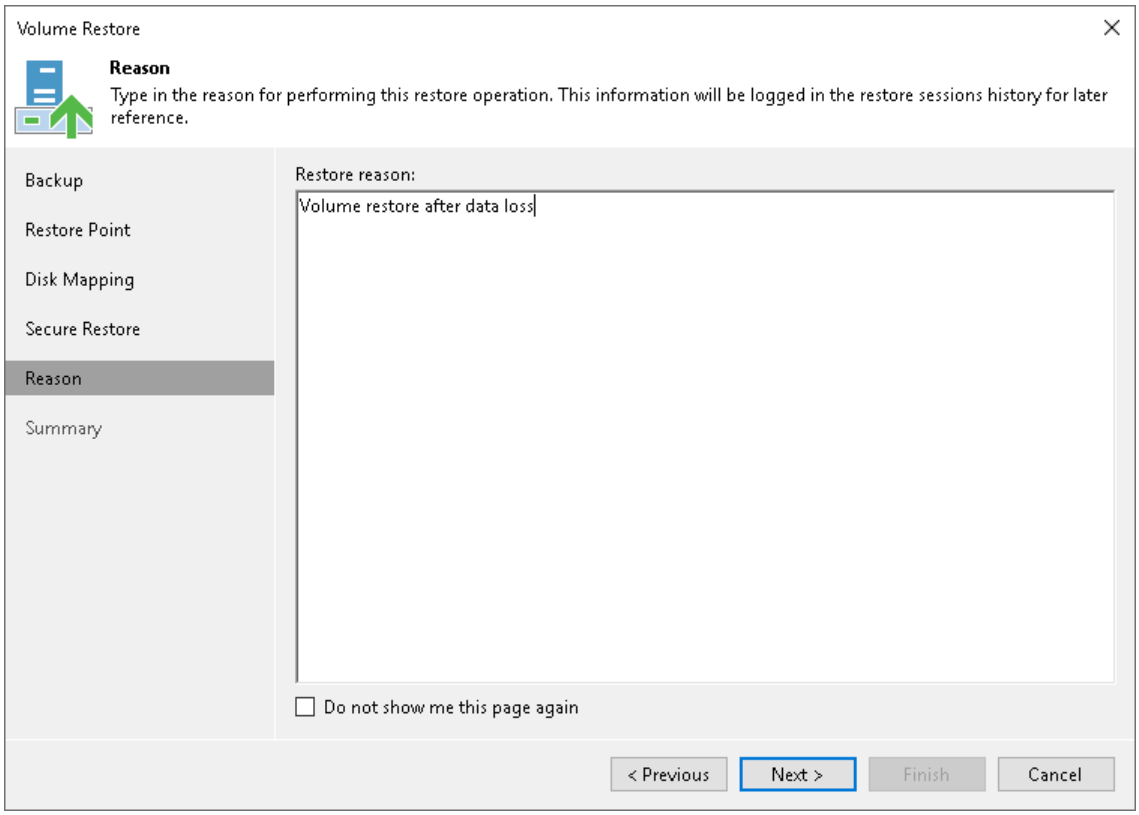
1. In the **Content scan** section, specify the following:
   - For Veeam Backup & Replication version 12.1:
     i. If you want to scan the restored volume with antivirus software, select the **Scan the restore point with an antivirus engine** check box. For more information on antivirus scan, see the Antivirus Scan (Secure Restore) section in the Veeam Backup & Replication.
     ii. If you want to scan the restored volume with a YARA rule, select the **Scan backup content with the following YARA** rule check box and select a YARA rule from the drop-down list. By default, the YARA rules are located in the folder by the following path: `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`.
   - For Veeam Backup & Replication version 12.0, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. In the **Scan options** section, select the **Continue scanning all remaining files after the first occurence** (**Scan the entire image** — for Veeam Backup & Replication version 12.0) check box if you want to continue volume scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Malware Scan Results section in the Veeam Backup & Replication User Guide.



Step 6. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

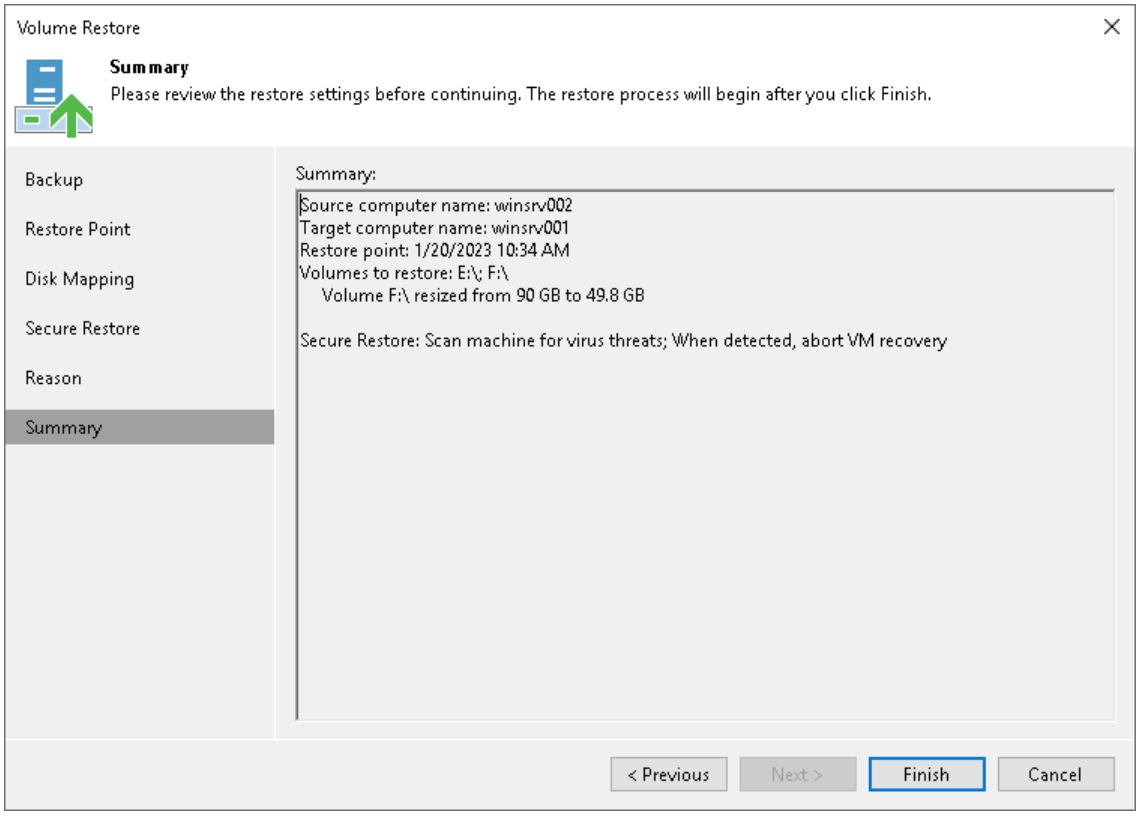
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of volume-level restore.

1. Review settings of the restore process.
2. Click **Finish** to start the recovery process. Veeam Backup & Replication will perform partition re-allocation operations if necessary, restore the necessary volume data from the backup and overwrite volume data on the target computer with the restored data.



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.

> **NOTE**
>
> Before you start file-level restore from a backup of a failover cluster, make sure that the cluster is added to a protection group in the Veeam Backup & Replication inventory. The failover cluster may be not present in the inventory, for example, in the following cases:
>
> - The original protection group that contained the cluster was removed from Veeam Backup & Replication.
> - You want to restore cluster data from a backup created on another backup server and imported in the Veeam backup console.
>
> In this case, add the failover cluster whose data you want to restore to a protection group.

Before you perform file-level restore, check prerequisites. Then use the **File Level Restore** wizard to restore the necessary files and folders.

1. Launch the File Level Restore wizard.
2. Select a machine.
3. Select a restore point.
4. Specify a restore reason.
5. Verify restore settings.
6. Finalize restore.

Before You Begin

Before you begin the file-level restore process, check the following requirements and limitations:

Requirements

Consider the following general requirements:

- You can restore files from the file systems listed in the Guest OS File Restore section in the Veeam Backup & Replication User Guide.
- The account that you use to start the Veeam Backup & Replication console and to connect to the backup server must have permissions and privileges described in the Installing and Using Veeam Backup & Replication section in the Veeam Backup & Replication User Guide.
- You can restore files from a backup that has at least one successfully created restore point.
- [For restore to original location] The mount server must have access to the Veeam Agent computer.

- [For restore changes functionality] This functionality is included in the Veeam Universal License. When using a legacy socket-based license, the Enterprise or Enterprise Plus editions of Veeam Backup & Replication are required.

Requirements for ReFS

> **NOTE**
>
> The information in this subsection is only applicable to restore from volume-level backups.

If you plan to restore files from a computer running Microsoft Windows ReFS, consider the following requirements for the Veeam Backup & Replication components involved in the restore process:

- The machine on which a mount point is created (for example, the mount server) must run Microsoft Windows Server 2012 OS or later.
- [For ReFS 3.x] If you plan to restore files from a computer running Microsoft Windows ReFS 3.x, the machine on which mount point is created must run Microsoft Windows Server 2016 OS or later and the ReFS version must be supported on it.
- The machine on which a mount point is created must run Microsoft Windows Server OS of the same version or newer than the Veeam Agent computer from which you plan to restore files.

To learn more about mount points creation, see the Mount Points and Restore Scenarios section in the Veeam Backup & Replication User Guide.

Requirements for Data Deduplication

> **NOTE**
>
> The information in this subsection is only applicable to restore from volume-level backups.

If you plan to restore files from a computer running Microsoft Windows Server 2012 OS or later and data deduplication is enabled for some volumes, consider the following for the Veeam Backup & Replication components involved in the restore process:

- The machine on which a mount point is created (for example, the mount server) must run Microsoft Windows Server 2012 OS or later.
- The machine on which a mount point is created must run Microsoft Windows Server OS of the same version or newer than the Veeam Agent computer from which you plan to restore files.
- Data deduplication must be enabled on the machine on which a mount point is created.

To learn in which scenarios on which machines mount points can be created, see the Mount Points and Restore Scenarios section in the Veeam Backup & Replication User Guide.

Limitations

Consider the following limitations:

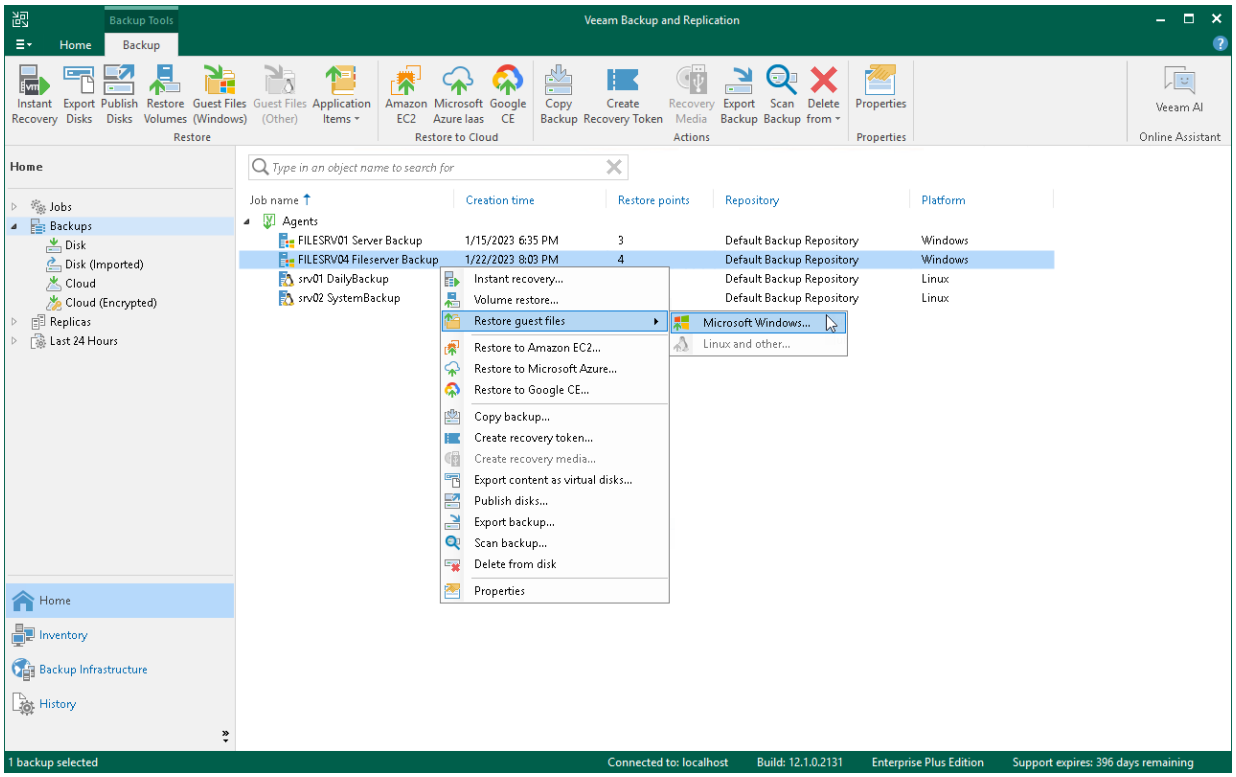
- You cannot restore pipes and other file system objects. File-level restore supports recovery of files and folders only.
- You can restore files from basic disks and dynamic disks (including simple, mirrored and striped volumes).

- [For restore from volume-level backups] Processing of reparse points is supported only for NTFS. Note that reparse points with reparse tag values other than IO_REPARSE_TAG_MOUNT_POINT, IO_REPARSE_TAG_SYMLINK and IO_REPARSE_TAG_DEDUP may be processed and restored incorrectly.
- The comparison functionality uses Veeam Deployer Service. This service is a 32-bit service. During the comparison, the service converts some 64-bit objects in 32-bit objects. That is why such objects are shown as deleted in the Veeam Backup browser, for example, some objects in the `Windows` folder.
- [For permission restore] Veeam Backup & Replication restores only permissions. Attributes such as Read-only, Encrypted and so on are not restored.
- [For permission restore] Permissions can be restored only for files and folders that are still present on the Veeam Agent computer. If files and folders are missing, restore fails.
- You cannot restore files encrypted with Windows EFS.

Step 1. Launch File Level Restore Wizard

To launch the **File Level Restore** wizard, do either of the following:

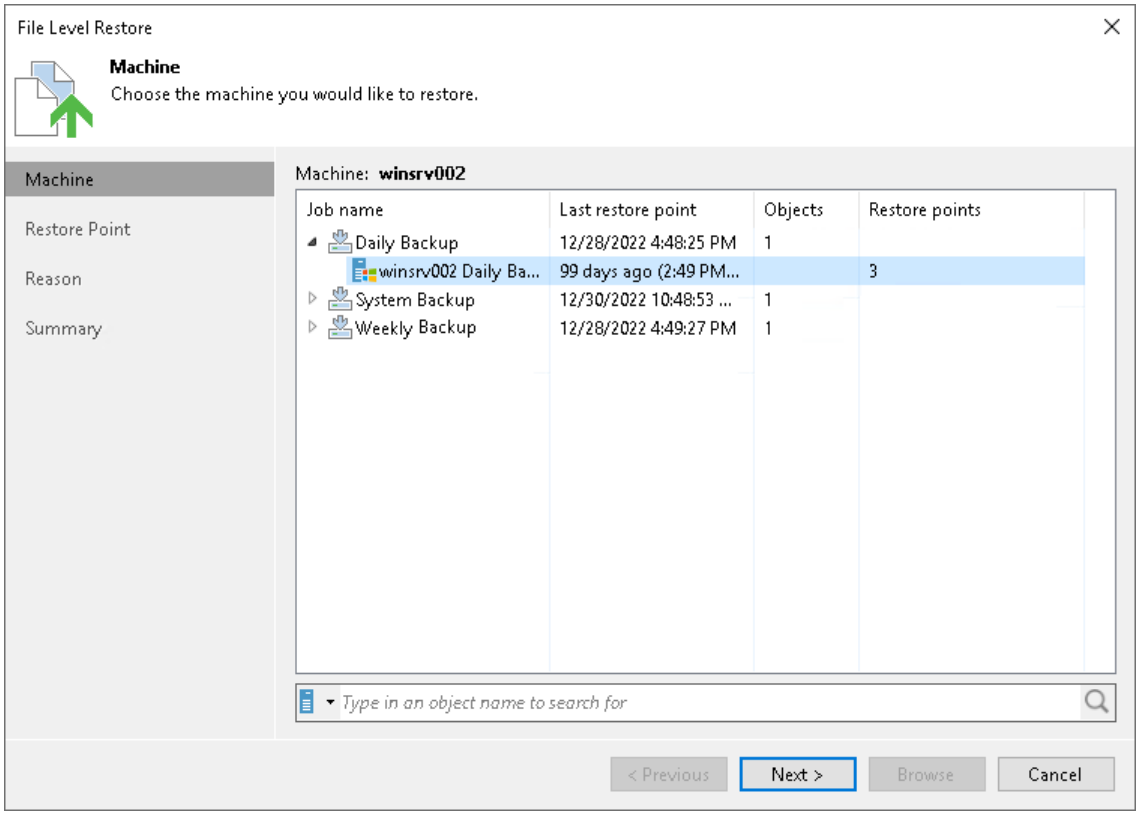
- Open the **Home** tab and click **Restore** > **Agent** > **Guest files restore** > **Microsoft Windows**. In this case, you will be able to select a Veeam Agent computer whose files and folders you want to restore at the Machine step of the wizard.
- Open the **Home** view. In the inventory pane, click the **Backups** node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click **Guest Files (Windows)** on the ribbon. Alternatively, right-click the computer and select **Restore guest files** > **Microsoft Windows**. In this case, you will proceed immediately to the Restore Point step of the wizard.



Step 2. Select Machine

At the **Machine** step of the wizard, select a backup from which you want to recover data.

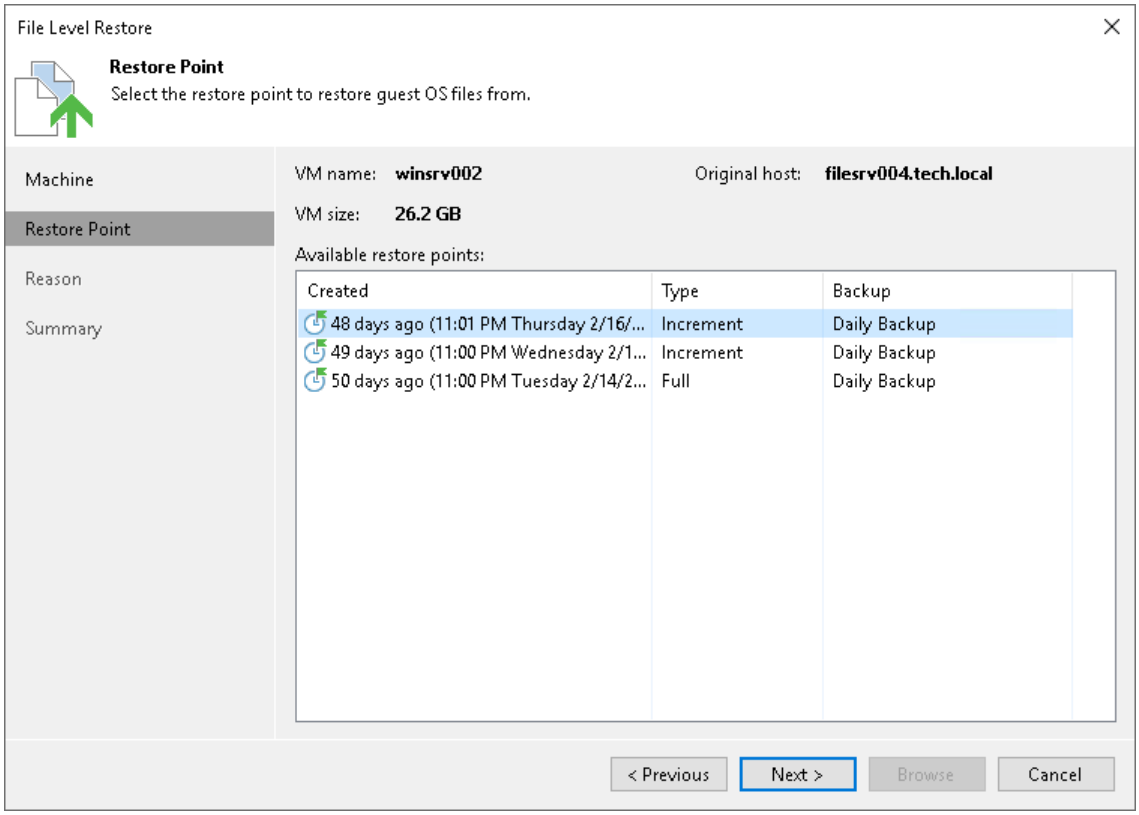
To quickly find the necessary backup, use the search field at the bottom of the window: enter a Veeam Agent computer name or a part of it in the search field and click the **Start search** button on the right or press [Enter].



Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

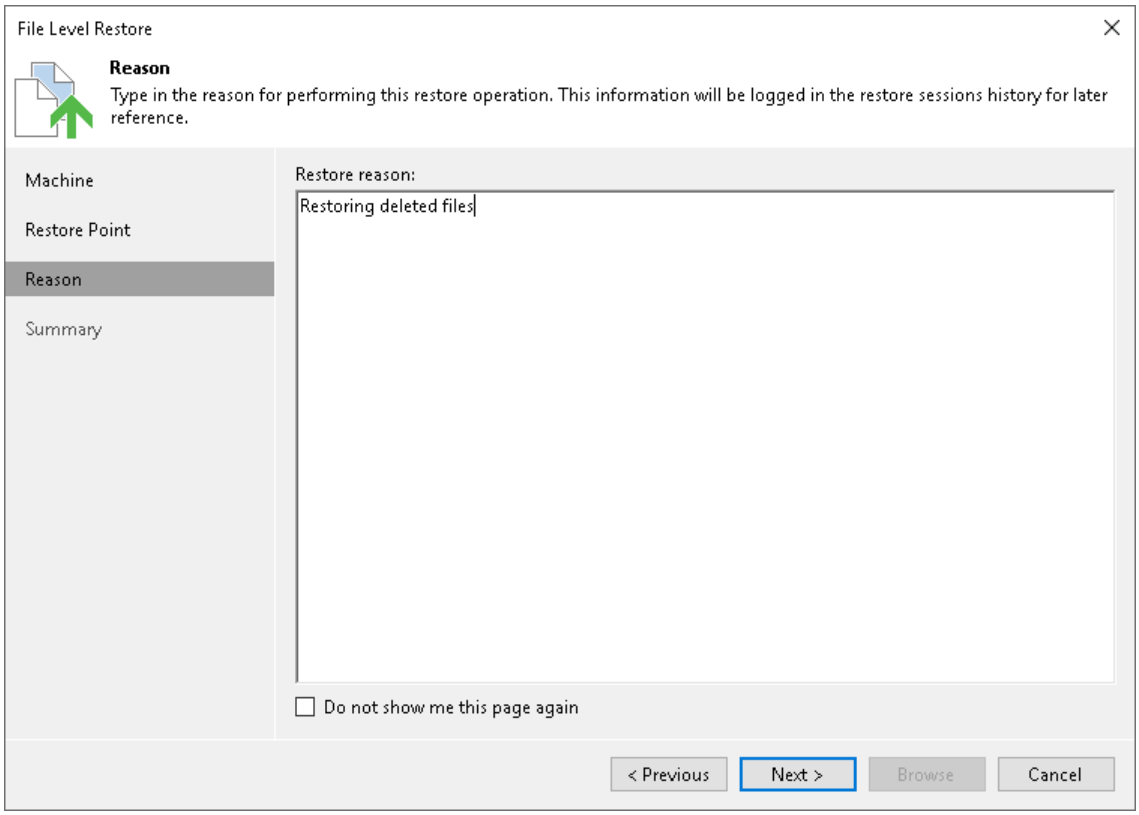
By default, Veeam Backup & Replication uses the latest restore point. However, you can select any valid restore point to recover data from.



Step 4. Specify Restore Reason

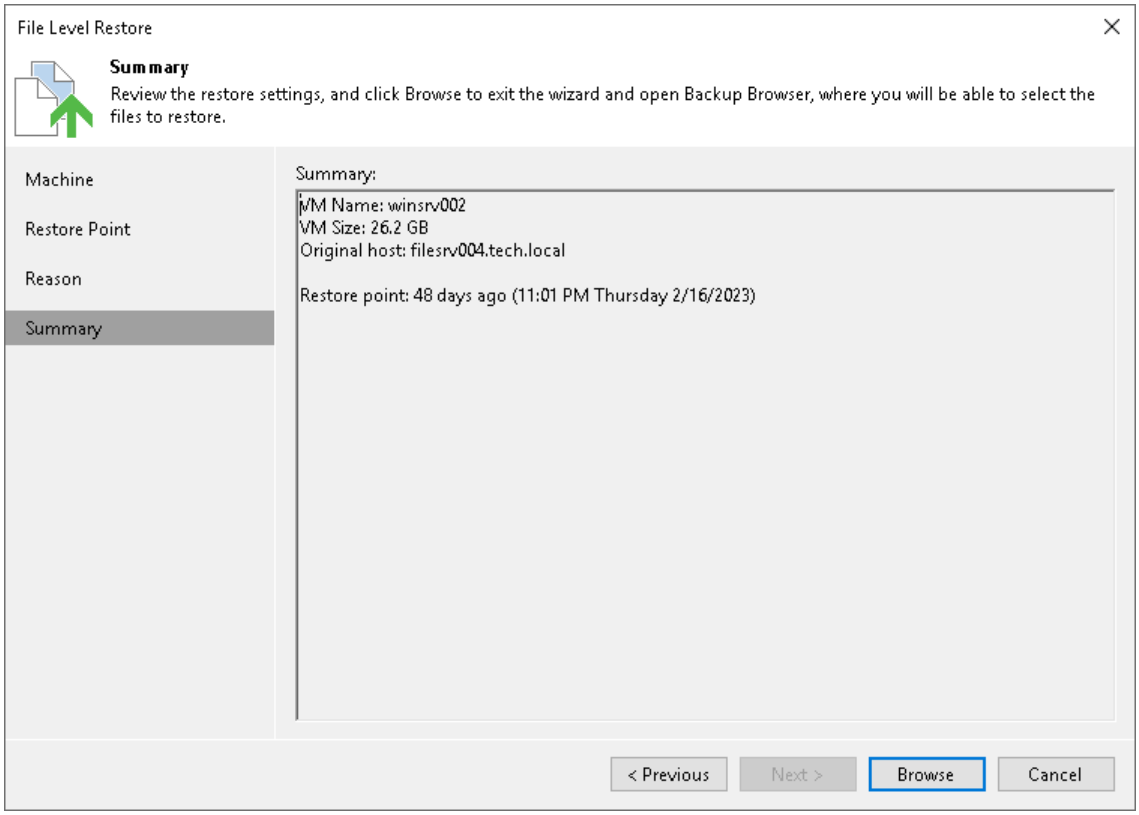
At the **Reason** step of the wizard, enter a reason for restoring data.

> **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.



Step 5. Verify Restore Settings

At the **Summary** step of the wizard, check details of the restore task and click **Browse** to close the wizard and open the Veeam Backup browser.



Step 6. Finalize Restore

After you close the wizard, Veeam Backup & Replication opens the Veeam Backup browser with the file system tree of the restored Veeam Agent computer.

You can perform the following operations in the Veeam Backup browser:

- Compare files and folders from a backup with the original files and folders.
- Restore only changed files and folders to the original location.
- Copy files and folders to the Veeam Backup & Replication console or network shared folder.
- Restore files and folders to the original location.
- Restore permissions only.
- Launch application item restore.
- Open files in Microsoft Windows File Explorer.

After you finish restoring files, close the Veeam Backup browser.

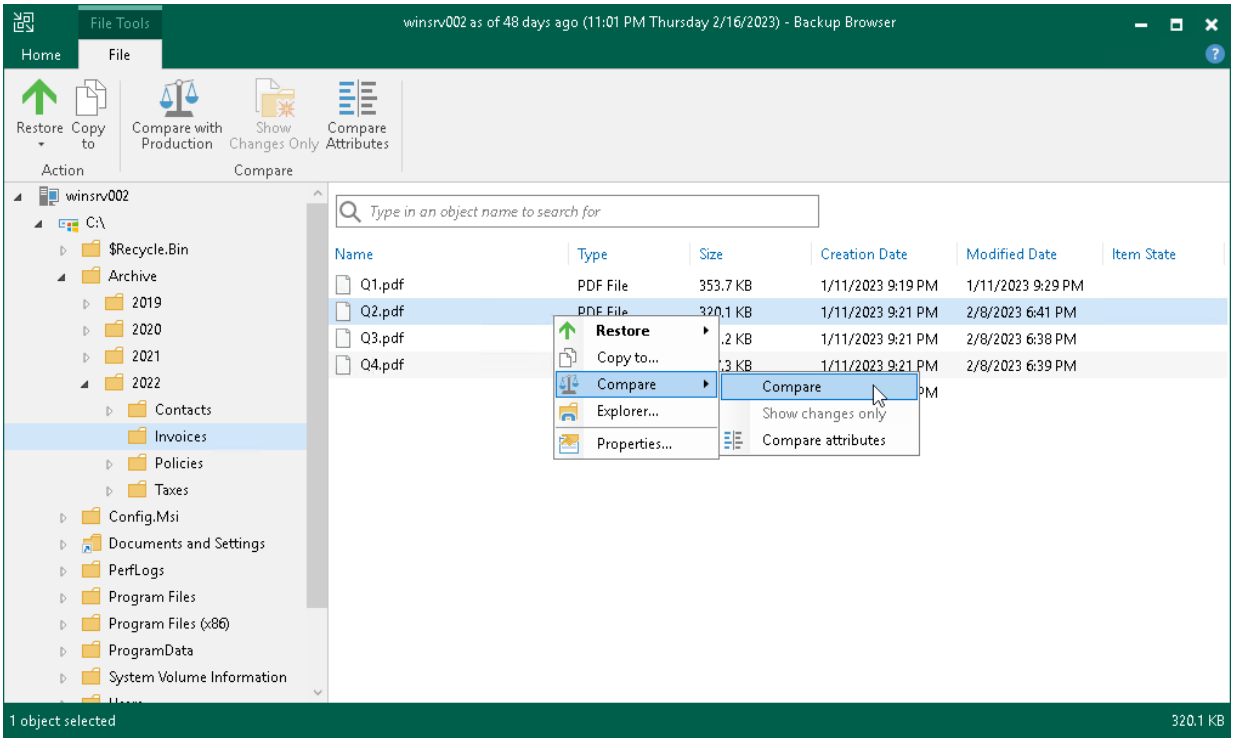
> **NOTE**
>
> Consider the following:
>
> - Folder symbolic links are displayed under the  icon.
> - When restoring symbolic links, Veeam Backup & Replication restores only links, not the content they point to.
> - Hard links are displayed and restored as files.

Comparing Files and Folders

When Veeam Backup & Replication compares files, it compares their attributes. When Veeam Backup & Replication compares folders, it compares folder attributes, and also folder and file attributes inside the folder recursively. Once a file or folder with changed attributes is found, Veeam Backup & Replication stops comparing items and marks the folder as changed. If you further browse the folder in the compared state, Veeam Backup & Replication continues comparing non-compared files and folders. Veeam Backup & Replication compares the following attributes: Date Created, Date Modified, Size (only for files), Read-Only, Hidden, Archive, NTFS Encryption.

To compare files and folders from a backup with the files and folders stored in the original location:

1. Select the necessary files and folders in the file system tree or in the details pane on the right. You can also select disks. In this case, Veeam Backup & Replication will compare files and folders stored on the disks.
2. Right-click one of the selected items and select **Compare** > **Compare** or click **Compare with Production** on the ribbon.
3. If prompted, in the **Credentials** window, specify user credentials to access the original location.



After the comparison, files and folders will have the following comparison states in the **Item State** column: *changed*, *unchanged*, *deleted*, *pending*, or *failed to compare*. The states are updated when you turn off and then turn on the comparison mode, and when you start restoring changes of files and folders. Note that when comparing symbolic links, Veeam Backup & Replication compares attributes of the links, not the attributes of files and folders which the symbolic link points to.

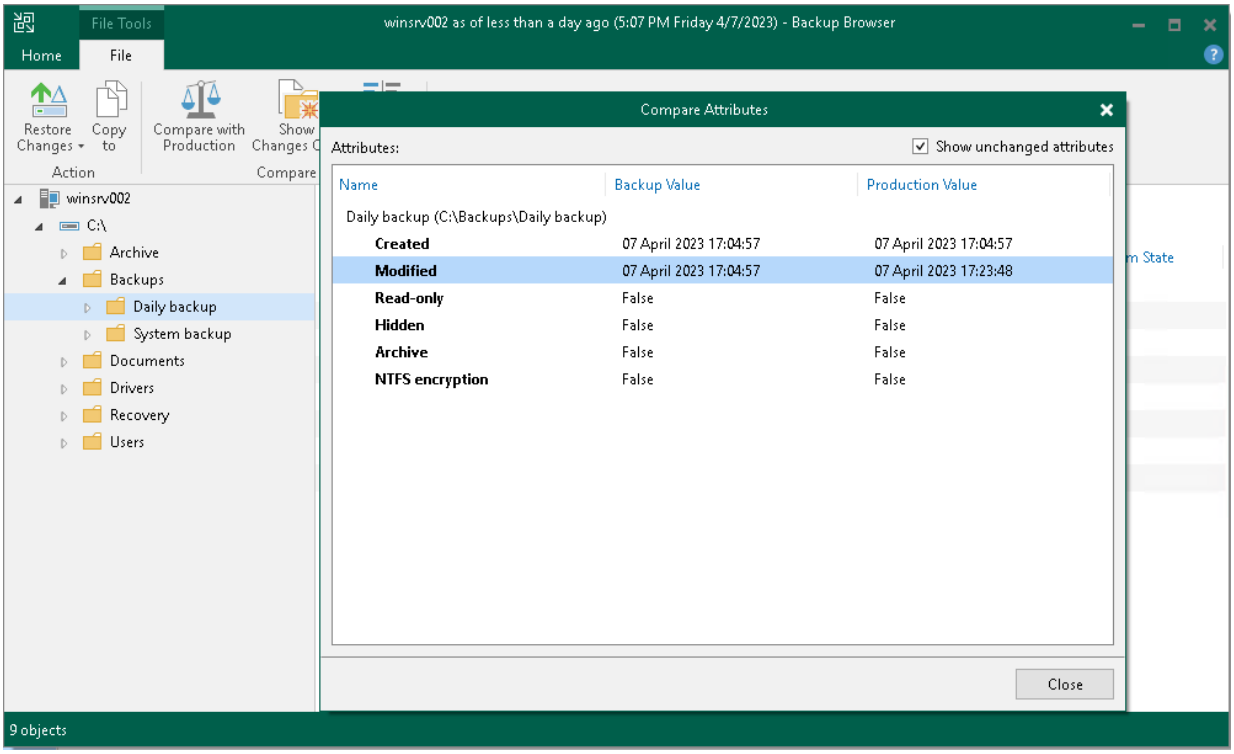
For files and folders in the comparison states, Veeam Backup & Replication provides other restore operations than for files and folders in the non-comparison state. For example, you can restore only changed files and folders. For more information, see Restoring Changed Files and Folders.

> **TIP**
>
> To show only changed files and folders (in the *changed* and *deleted* states), perform the compare operation, right-click any area in the Veeam Backup browser and select **Compare** > **Show changes only** or click **Show Changes Only** on the ribbon. Note that in this case the search field becomes unavailable. To show all files and folders, click the **Show changes only** option once again.
>
> To switch off the comparison states, select an item in the comparison state and click **Compare** > **Compare** or click **Compare with Production** on the ribbon. Note that if you switch off comparison for child files and folders, comparison for parent folders will also be switched off.

You can view which attributes were changed for files and folders:

1. Select the necessary files and folders in the file system tree or in the details pane on the right.
2. Right-click one of the selected items and select **Compare > Compare attributes** or click **Compare Attributes** on the ribbon.

In the **Compare Attributes** window, Veeam Backup & Replication shows changed attributes. If you want to show all attributes, click the **Show unchanged attributes** check box at the top right corner. Note that Veeam Backup & Replication shows attributes maximum for 500 files and folders and shows attributes for the selected files and folders, not for the nested files.



Restoring Changed Files and Folders

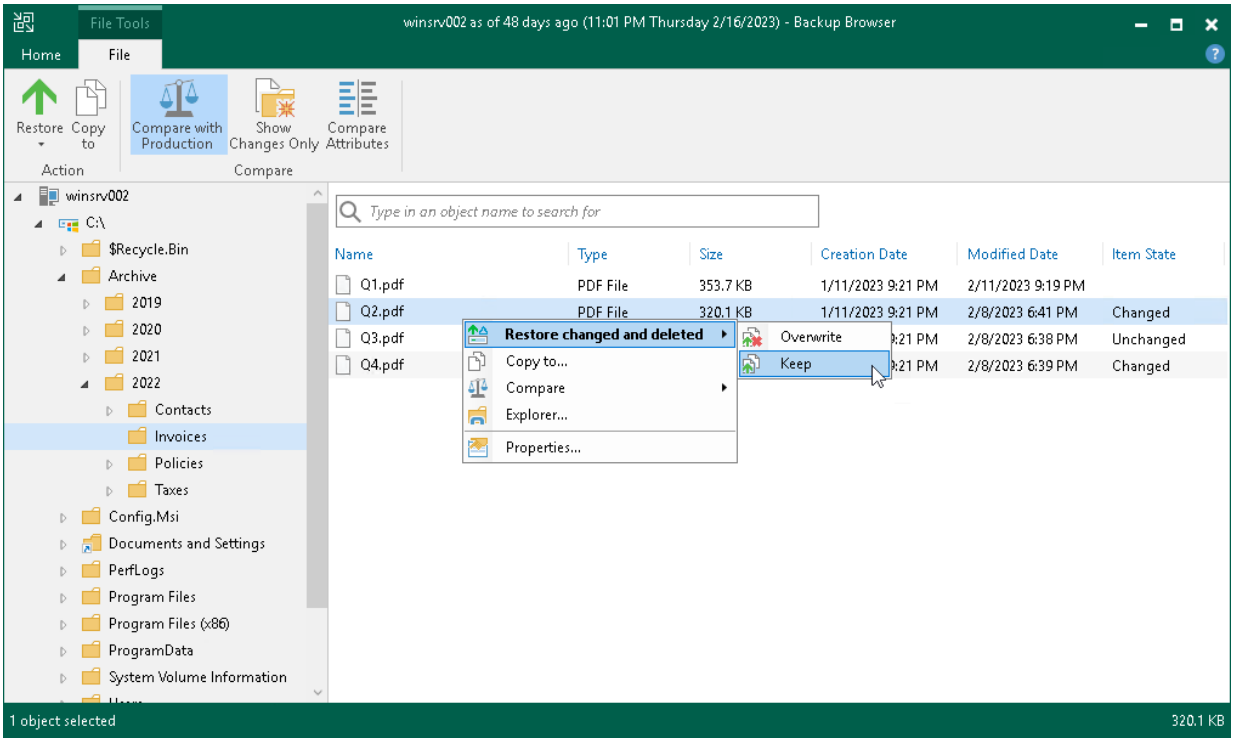
To restore only changed files and folders to the original location, do the following:

1. Select the necessary files and folders in the file system tree or in the details pane on the right. Note that at least one file or folder must be in a comparison state. Files and folders in the non-comparison state, Veeam Backup & Replication will compare automatically.
2. Right-click one of the selected items and select one of the following:
   - To overwrite the original files and folders with the ones restored from the backup, select **Restore changed and deleted** (**Restore changed only** — for Veeam Backup & Replication version 12.1) > **Overwrite**.
   - To save the files and folders restored from the backup next to the original ones, select **Restore changed and deleted** (**Restore changed only** — for Veeam Backup & Replication version 12.0)> **Keep**.

     Veeam Backup & Replication will add the *RESTORED_YYYYMMDD_HHMMSS* postfix to the original names and store the restored items in the same folder where the original items reside.

   Alternatively, you can select the same commands on the ribbon.

If you want to restore entire files and folders to the original location, see Restoring to Original Location.



Copying Files and Folders to Console or Shared Folder

To copy files and folders to the machine where the Veeam Backup & Replication console is installed or to a network shared folder:

1. Select the necessary files and folders in the file system tree or in the details pane on the right.
2. Right-click one of the selected items and click **Copy to** or click **Copy to** on the ribbon.
3. In the **Choose Folder** window, select the necessary destination:
   - To recover files and folders to a folder on the machine where the Veeam Backup & Replication console is installed, click **Browse** to find the necessary folder.
   - To recover files and folders to a network shared folder, enter a path to the destination folder in the **Choose folder** field.
4. In the **Choose Folder** window, choose whether to preserve original NTFS permissions or not:
   - To keep the original ownership and security permissions for the restored items, select the **Preserve permissions and ownership** check box.

     Veeam Backup & Replication will copy selected files and folders along with associated Access Control Lists, preserving granular access settings.

     > **IMPORTANT**
     >
     > To preserve permissions and ownership for the selected files and folders, you must run the Veeam Backup & Replication console under the Administrator account.
     >
     > If you run the Veeam Backup & Replication console under any other account, you will see a warning message after you click **Copy to** at the step 2. In this case, close the **Choose Folder** window and click the **Click here to run as administrator** link in the warning window to elevate access rights.

- If you do not want to preserve the original ownership and access settings for the restored items, leave the **Preserve permissions and ownership** check box not selected.

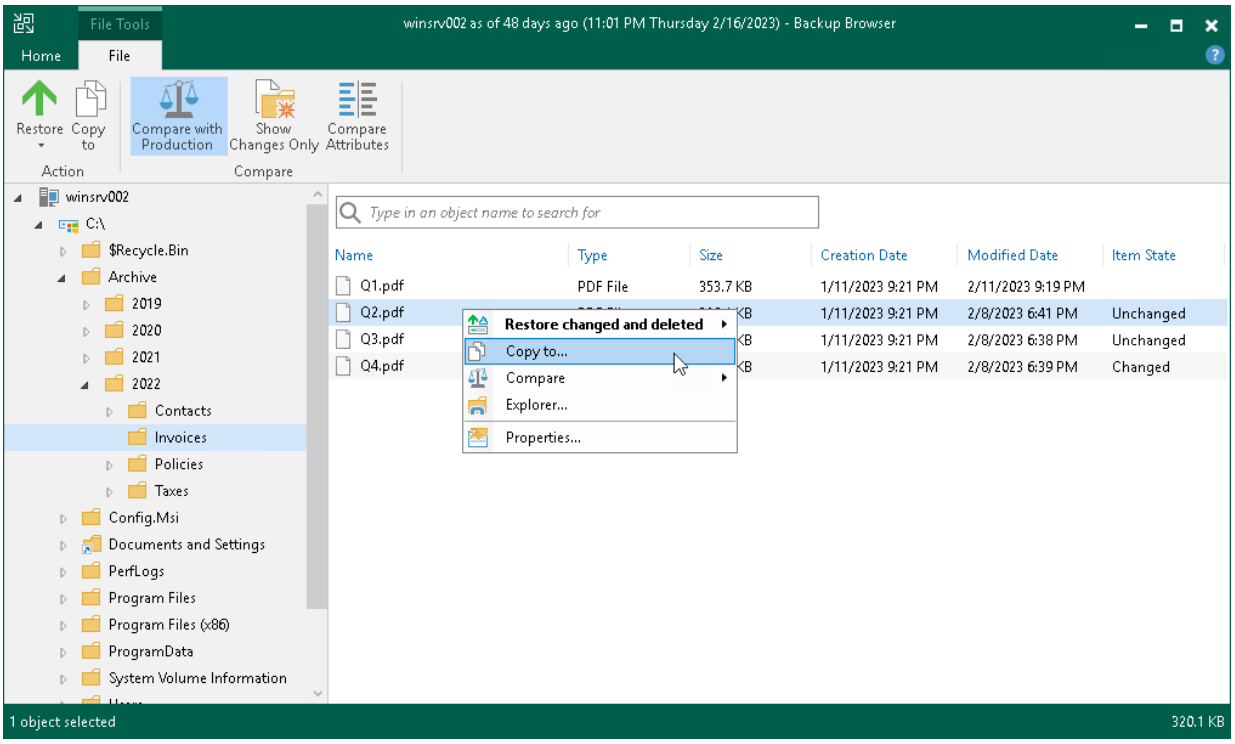
  Veeam Backup & Replication will change security settings: the user who launched the Veeam Backup & Replication console will be set as the owner of the restored item, while access permissions will be inherited from the folder to which the restored item is copied.

5. If prompted, in the **Credentials** window, specify user credentials to access the destination location.

NOTE

Consider the following:

- The copy to operation does not use the comparison states and copies all selected files and folders.
- When copying symbolic links, Veeam Backup & Replication copies the content which the links point to.



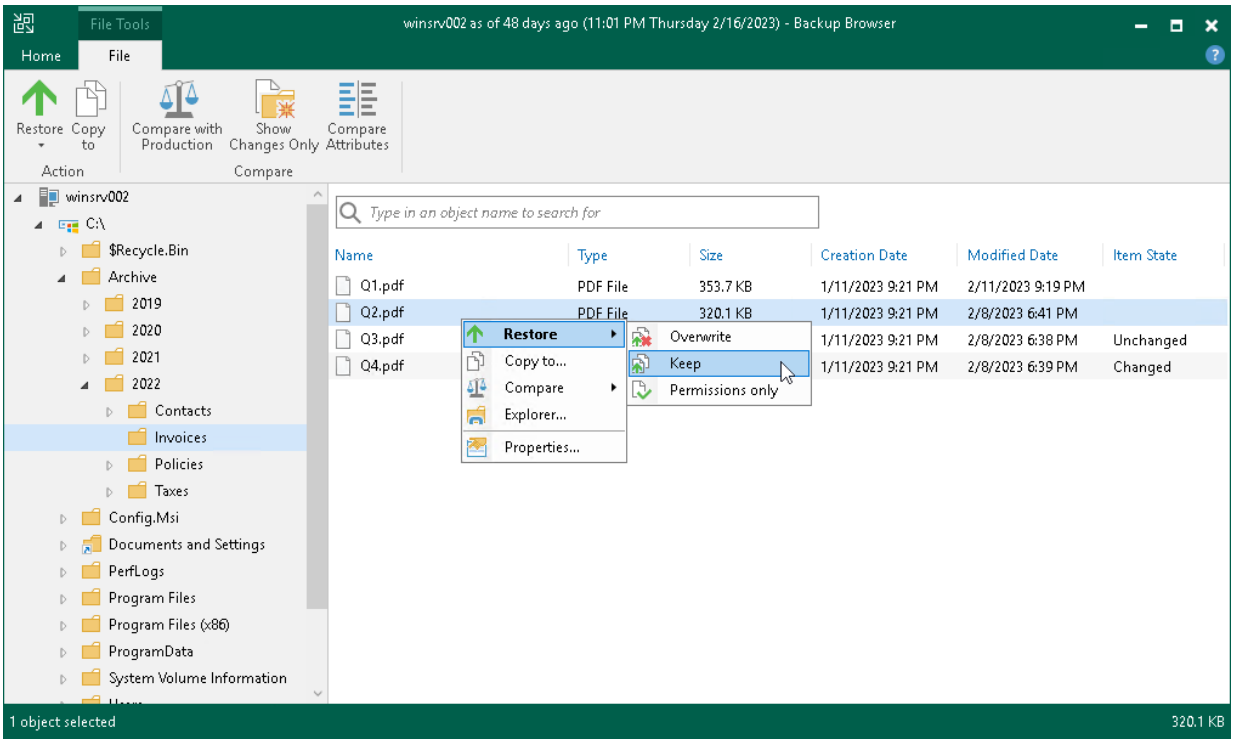
Restoring Files and Folders to Original Location

To restore files and folders to the original location, do the following:

1. Select the necessary files and folders in the file system tree or in the details pane on the right.
2. Right-click one of the selected items and select one of the following:
   - To overwrite the original files and folders with the ones restored from the backup, select **Restore** > **Overwrite**.
   - To save the restored files and folders next to the original ones, select **Restore** > **Keep**.

     Veeam Backup & Replication will add the *RESTORED_YYYYMMDD_HHMMSS* postfix to the original names and store the restored items in the same folder where the original items reside.

Alternatively, you can select the same commands on the ribbon.

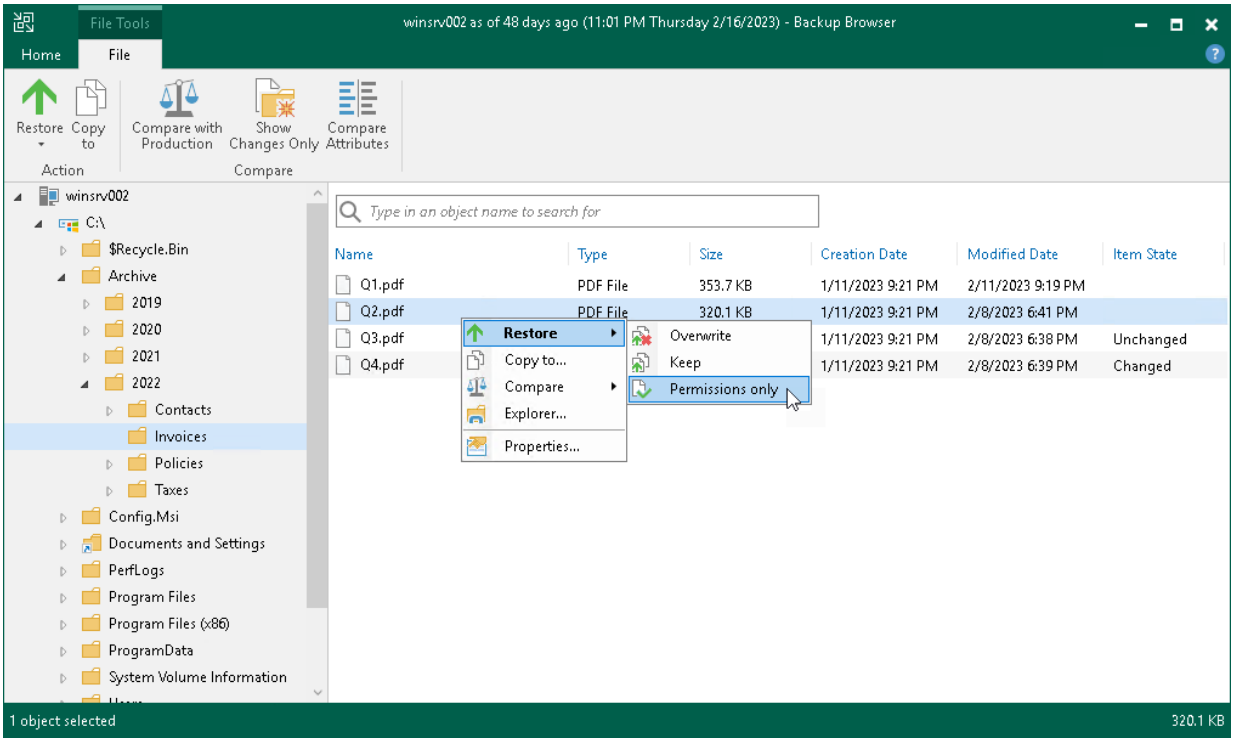


Restoring Permissions

This functionality is available for files and folders in the non-comparison state.

To restore permissions for files and folders, do the following:

1. Select the necessary files and folders in the file system tree or in the details pane on the right.
2. Right-click one of the selected items and select **Restore** > **Permissions only** or select **Restore** > **Permissions only** on the ribbon.



Launching Application Item Restore

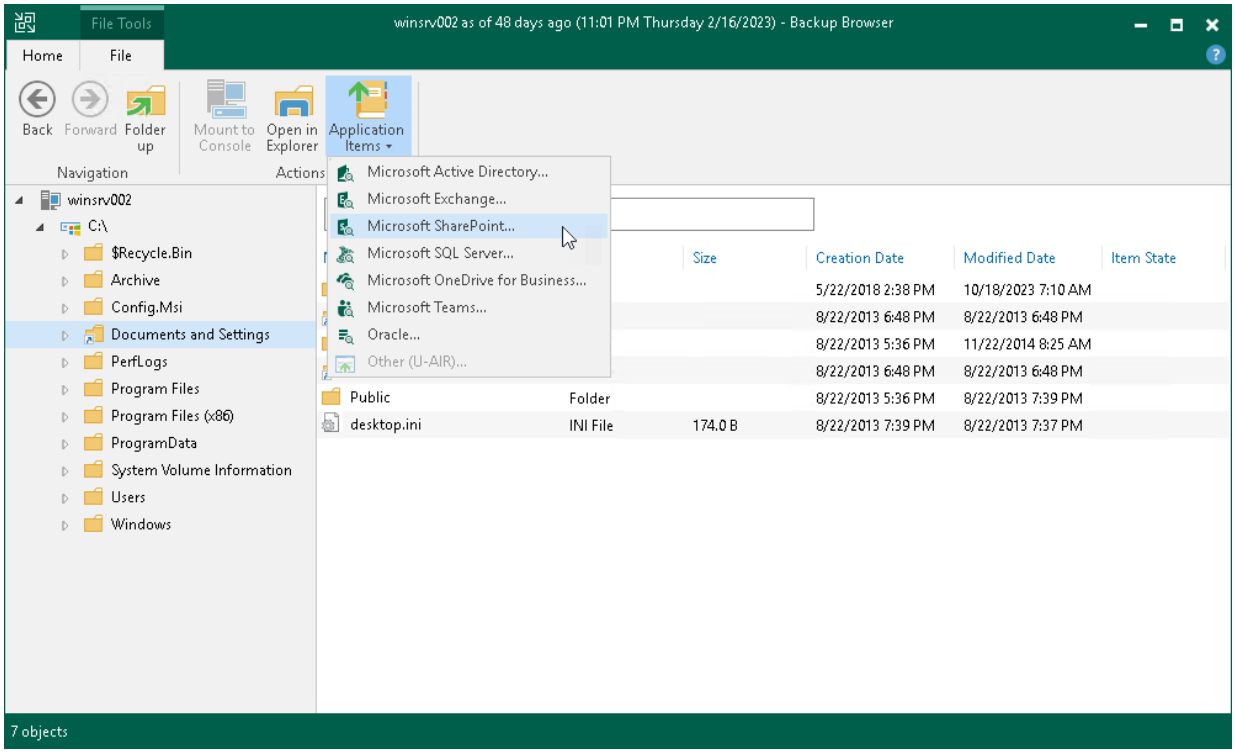
If you are restoring files from a Veeam Agent computer where the supported applications are installed, you can also launch application item restore directly from the Veeam Backup browser. Veeam Backup & Replication lets you restore items and objects from the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle

To restore application items, Veeam Backup & Replication uses special tools called Veeam Explorers.

To launch application item restore, do the following:

1. On the ribbon, switch to the **Home** tab.
2. Click **Application Items** and select the required application.
3. In the opened Veeam Explorer, perform the necessary operations. For more information on Veeam Explorers, see the Veeam Explorers User Guide.



Working with Microsoft Windows File Explorer

You can use Microsoft Windows File Explorer to work with restored files and folders:

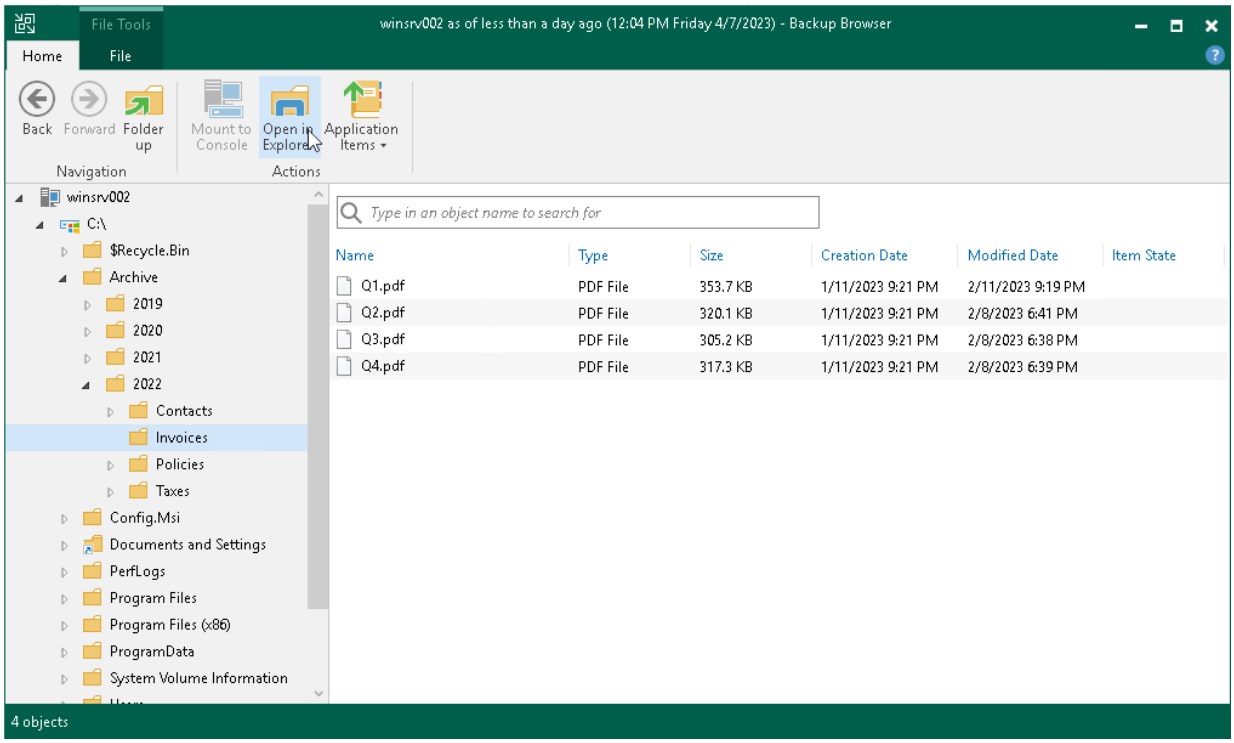
1. On the ribbon of the Veeam Backup browser, switch to the **Home** tab and click **Mount to Console** to mount the Veeam Agent computer disks to the Veeam Backup & Replication console.
2. To open Microsoft Windows File Explorer, do the following:
   - Click **Open in Explorer** on the Veeam Backup browser ribbon or right-click the necessary folder and select **Explorer**.
   - Click **File Explorer** in the **Start** menu of the machine where Veeam Backup & Replication console is installed. Browse to the `C:\VeeamFLR\<machinename>\<volume n>` folder where the disks of the machine are mounted and find the necessary files.

> **NOTE**
>
> The **Mount to Console** button is not available if the mount point is already created on the Veeam Backup & Replication console.

It is recommended that you use Microsoft Windows File Explorer only to view file content, not to restore files. For file restore, use Veeam Backup browser. This browser has the following advantages:

1. You can browse the Veeam Agent computer file system ignoring the file system ACL settings.
2. You can preserve permissions and ownership during file-level restore.

If you open the Veeam Agent computer file system in Microsoft Windows Explorer, these capabilities are not available. For more information, see Microsoft Docs.



Closing Veeam Backup Browser

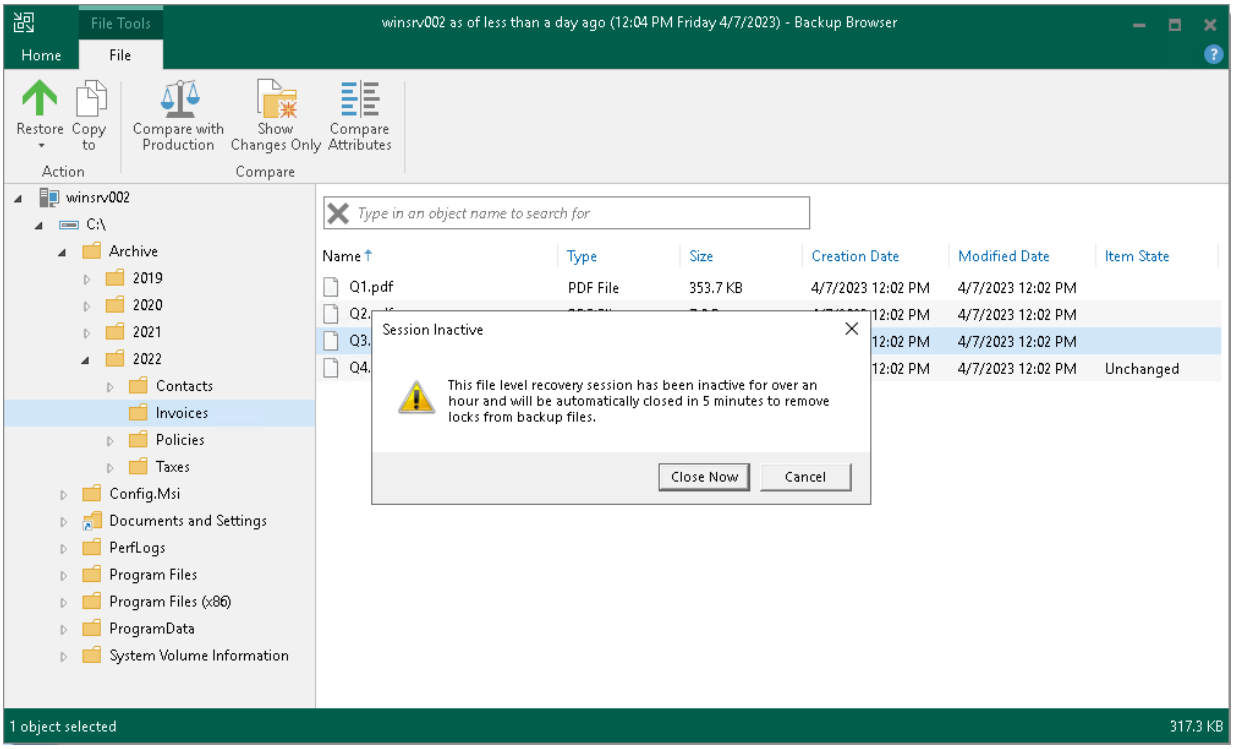
You can browse Veeam Agent computer files only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup & Replication unmounts Veeam Agent computer disks from the machine where the Veeam Backup & Replication console is installed and from the mount server (if you have restored Veeam Agent computer files to the original location).

It is recommended that you close the Veeam Backup browser after you have finished restoring Veeam Agent computer files. When the Veeam Backup browser is open, the backup file whose computer file system is displayed in the browser is locked in the backup repository. As a result, some scheduled operations that use this backup file may fail.

Veeam Backup & Replication checks if there is any activity in the Veeam Backup browser with an interval of 5 minutes. If the user or Veeam Backup & Replication components and services do not perform any actions for 30 minutes, Veeam Backup & Replication displays a warning that the Veeam Backup browser is to be closed in 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 5 minutes. After this period expires, Veeam Backup & Replication will display the warning again.
- You can perform no action at all. In this case, the Veeam Backup browser will close automatically in 5 minutes.

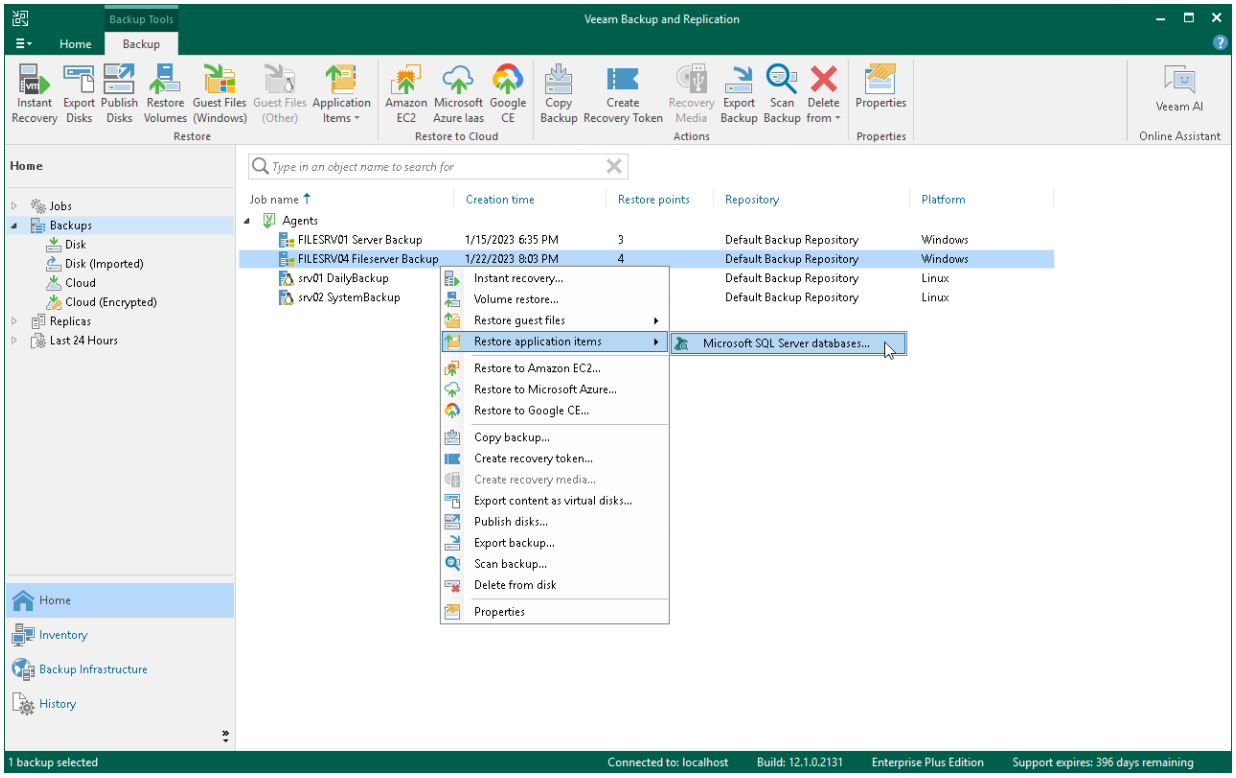

File Tools
winsrv002 as of less than a day ago (12:04 PM Friday 4/7/2023) - Backup Browser
Home
File
Restore
Copy to
Compare with Production
Show Changes Only
Compare Attributes
Action
Compare
winsrv002
C:\
Archive
2019
2020
2021
2022
Contacts
Invoices
Policies
Taxes
Config.Msi
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
System Volume Information
Type in an object name to search for
Name
Type
Size
Creation Date
Modified Date
Item State
Q1.pdf
PDF File
353.7 KB
4/7/2023 12:02 PM
4/7/2023 12:02 PM
4/7/2023 12:02 PM
Unchanged
Session Inactive
This file level recovery session has been inactive for over an hour and will be automatically closed in 5 minutes to remove locks from backup files.
Close Now
Cancel
1 object selected
317.3 KB

Restoring Application Items

You can use Veeam Explorers to restore application items from backups created using Veeam Agent for Microsoft Windows. Veeam Backup & Replication lets you restore items and objects from the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle

The procedure of application item restore from a Veeam Agent backup does not differ from the same procedure for a VM backup. To learn more, see the Application Item Restore section in the Veeam Backup & Replication User Guide.



Exporting Disks

You can restore computer disks from Veeam Agent backups created using Veeam Agent for Microsoft Windows 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 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.

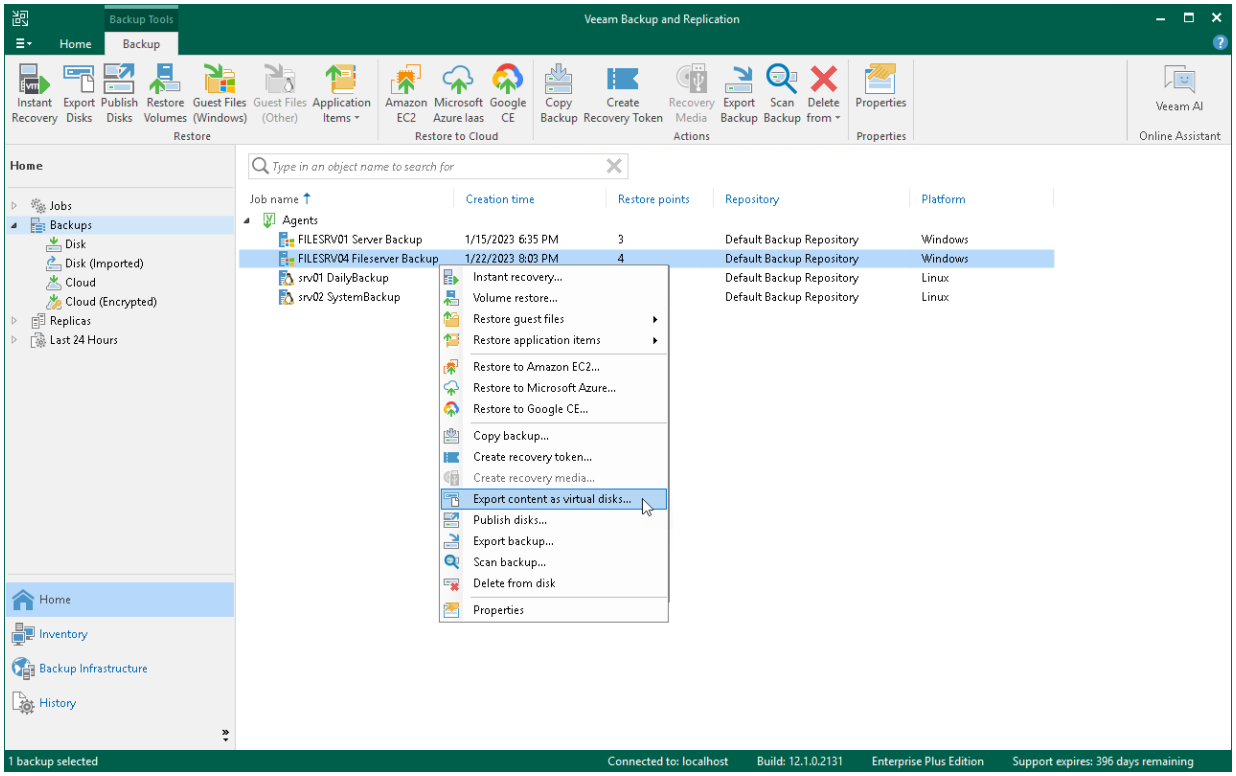
To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

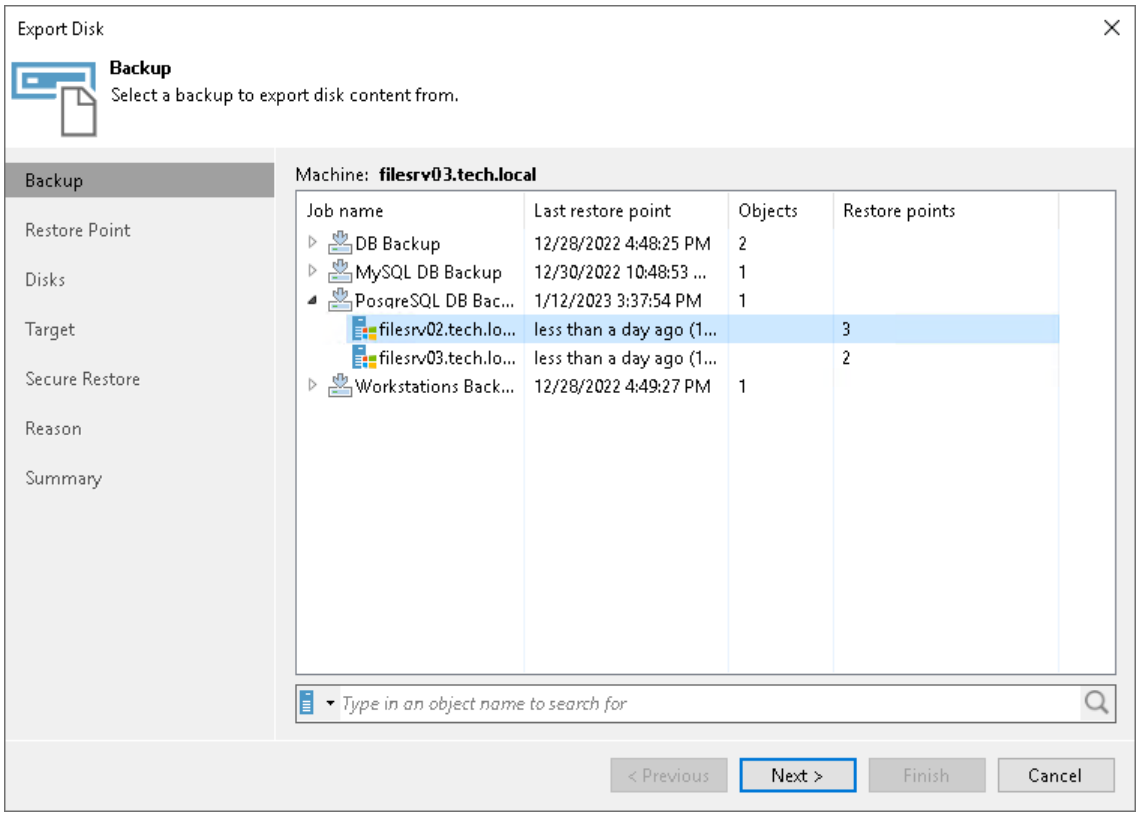
- Open the **Home** tab and click **Restore** > **Agent** > **Disk restore** > **Export disk**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the Backup step of the wizard.
- Open the **Home** view. In the inventory pane, click the Backups node. In the working 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.



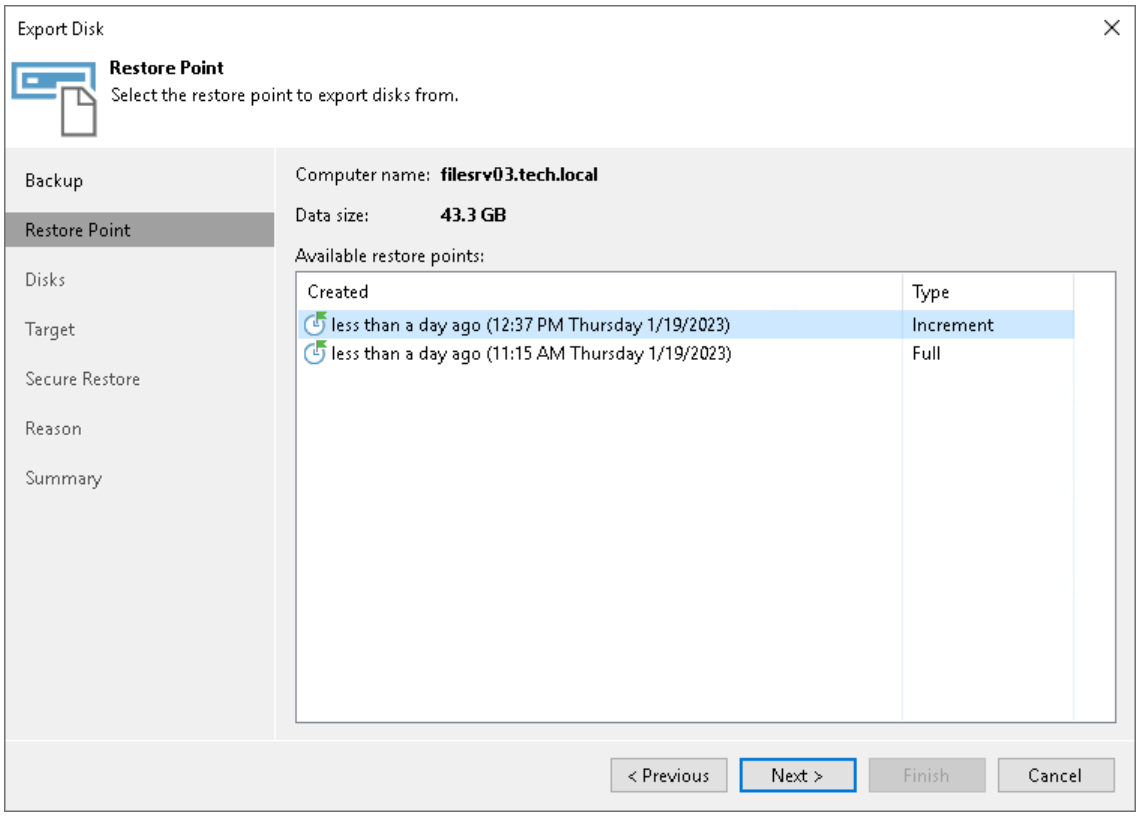
Step 2. Select Backup

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.



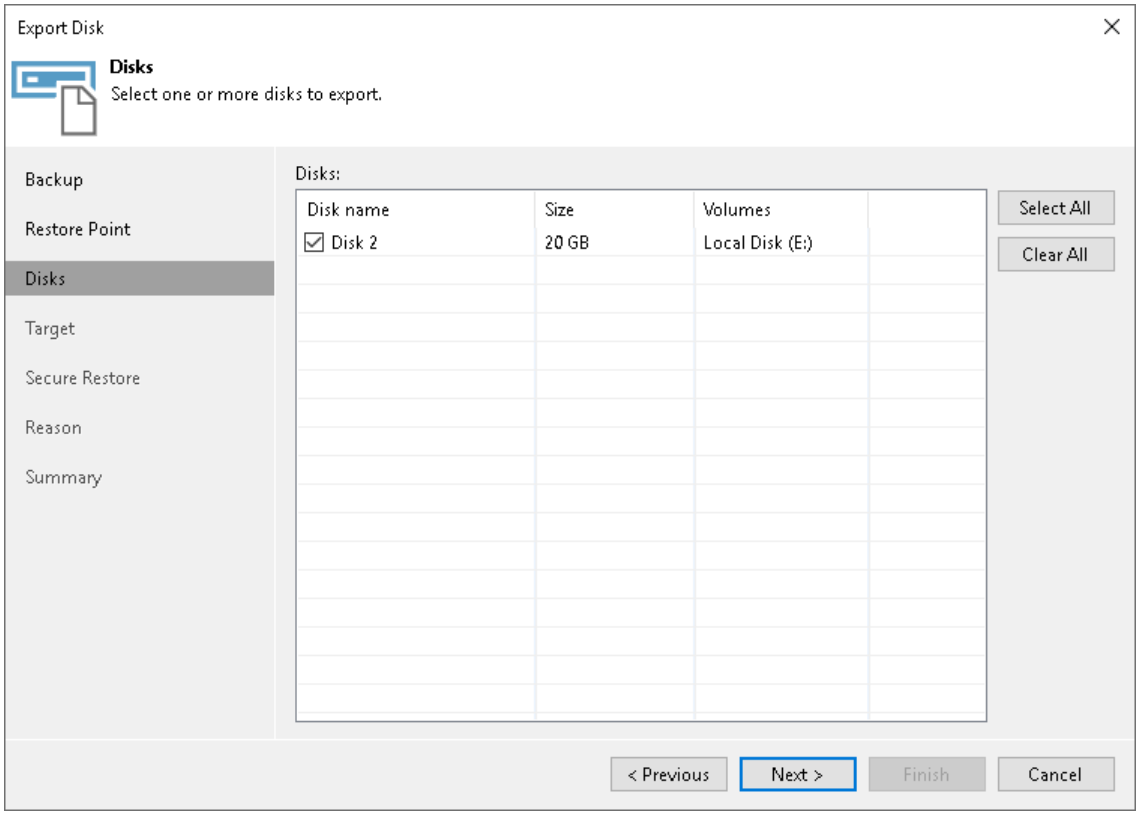
Step 3. Select Restore Point

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 4. Select Disks

At the **Disks** step of the wizard, select check boxes next to those disks that you want to export.

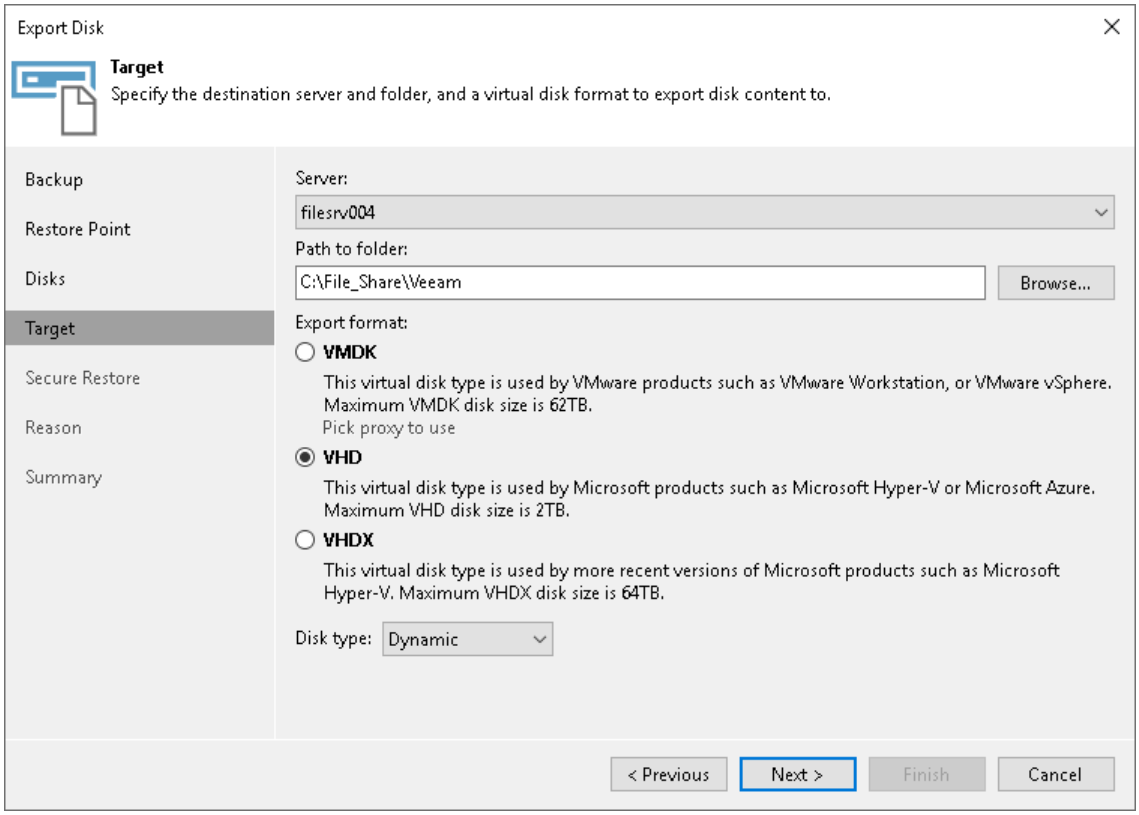


Step 5. Select Destination and Disk Format

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 VMDX 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.

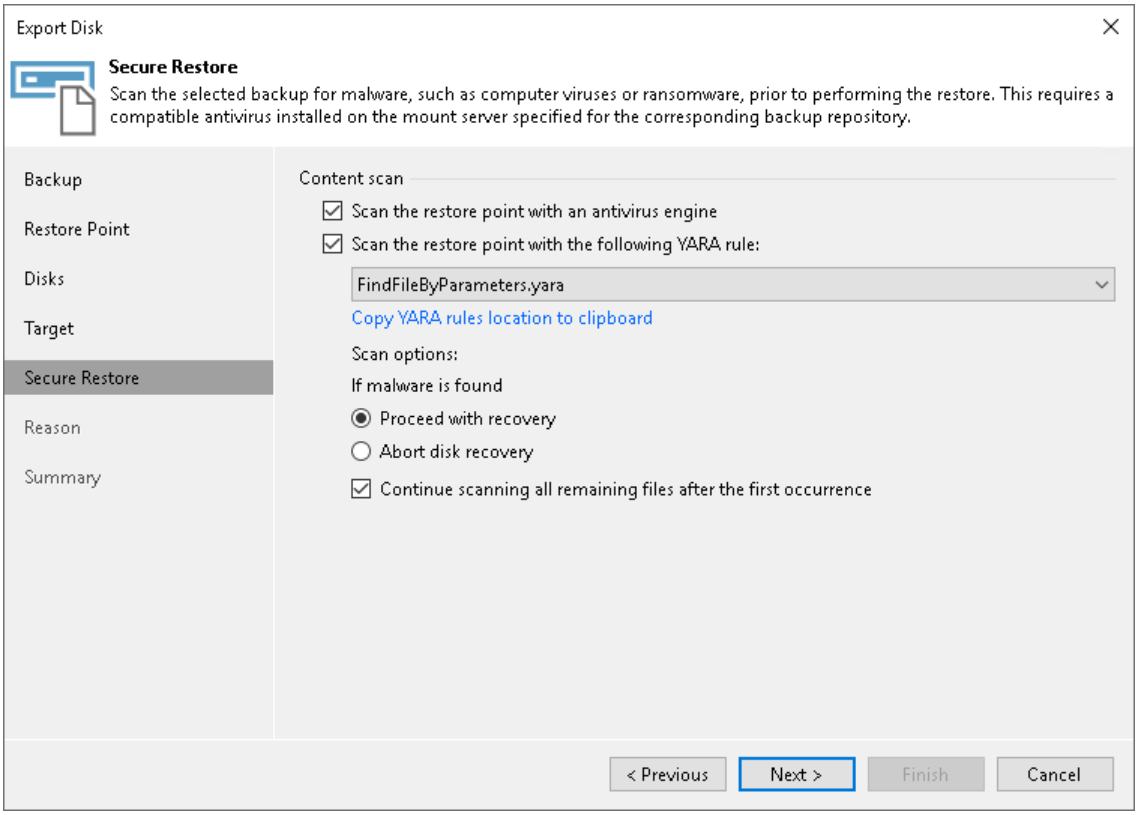

Export Disk
Target
Specify the destination server and folder, and a virtual disk format to export disk content to.
Backup
Restore Point
Disks
Target
Secure Restore
Reason
Summary
Server:
filesrv004
Path to folder:
C:\File_Share\Veeam
Browse...
Export format:
VMDK
This virtual disk type is used by VMware 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:
Dynamic
< Previous
Next >
Finish
Cancel

Step 6. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan restored disk data with antivirus software before restoring the disk. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

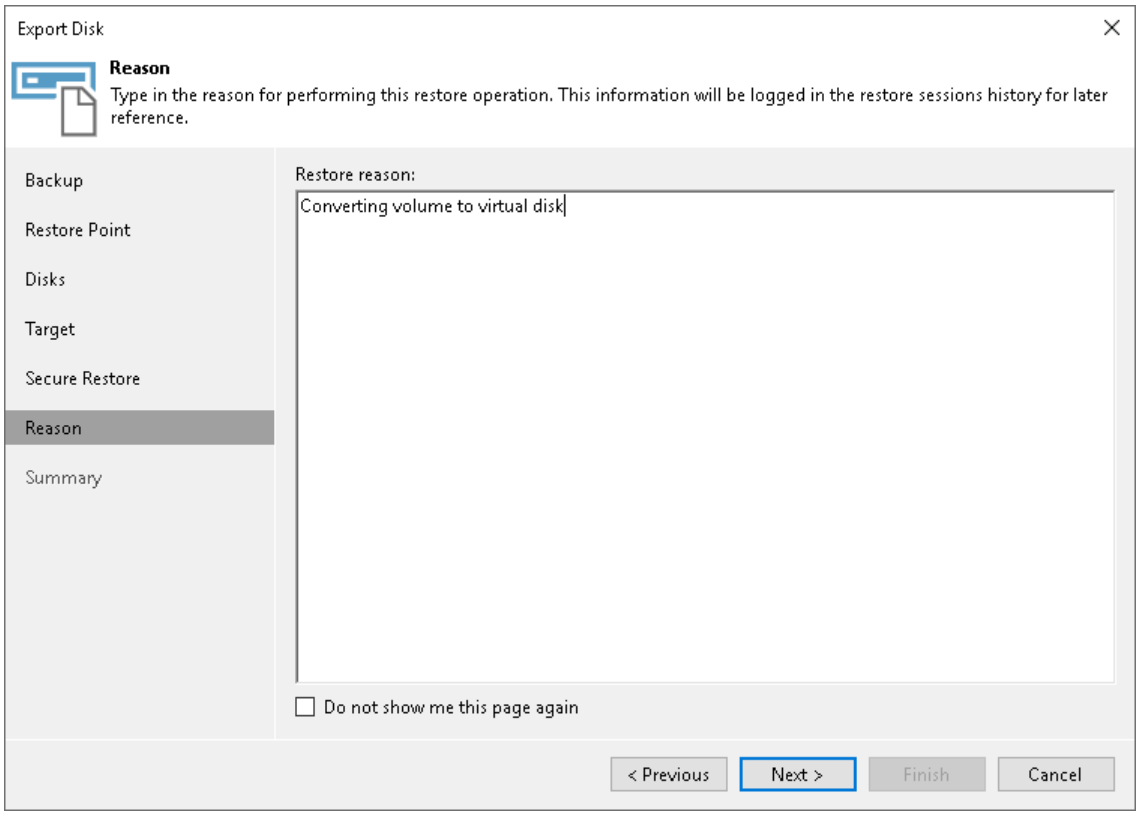
1. In the **Content scan** section, specify the following:
   - For Veeam Backup & Replication version 12.1:
     i. To use antivirus software as a scan engine, select the **Scan the restore point with an antivirus engine** check box. For more information on antivirus scan, see the Antivirus Scan (Secure Restore) section in the Veeam Backup & Replication User Guide.
     ii. To use a YARA rule as a scan engine, select the **Scan the restore point with the following YARA** rule check box and choose a YARA rule from the drop-down list. By default, the YARA rules are located in the folder by the following path: `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`.
   - For Veeam Backup & Replication version 12.0, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. Instruct Veeam Backup & Replication what to perform in case malware is found:
   - Select **Proceed with recovery** if you want to continue the recover process, despite the found malware threat.
   - Select **Abort disk recovery** if you want to stop the recovery process after the first malware threat is found.
3. In the **Scan options** section, select the **Continue scanning all remaining files after the first occurrence** (**Scan the entire image** — for Veeam Backup & Replication version 12.0) check box if you want the antivirus software to continue volume scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Malware Scan Results section in the Veeam Backup & Replication User Guide.


Export Disk
Secure Restore
Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.
Backup
Restore Point
Disks
Target
Secure Restore
Reason
Summary
Content scan
Scan the restore point with an antivirus engine
Scan the restore point with the following YARA rule:
FindFileByParameters.yara
Copy YARA rules location to clipboard
Scan options:
If malware is found
Proceed with recovery
Abort disk recovery
Continue scanning all remaining files after the first occurrence
< Previous
Next >
Finish
Cancel

Step 7. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

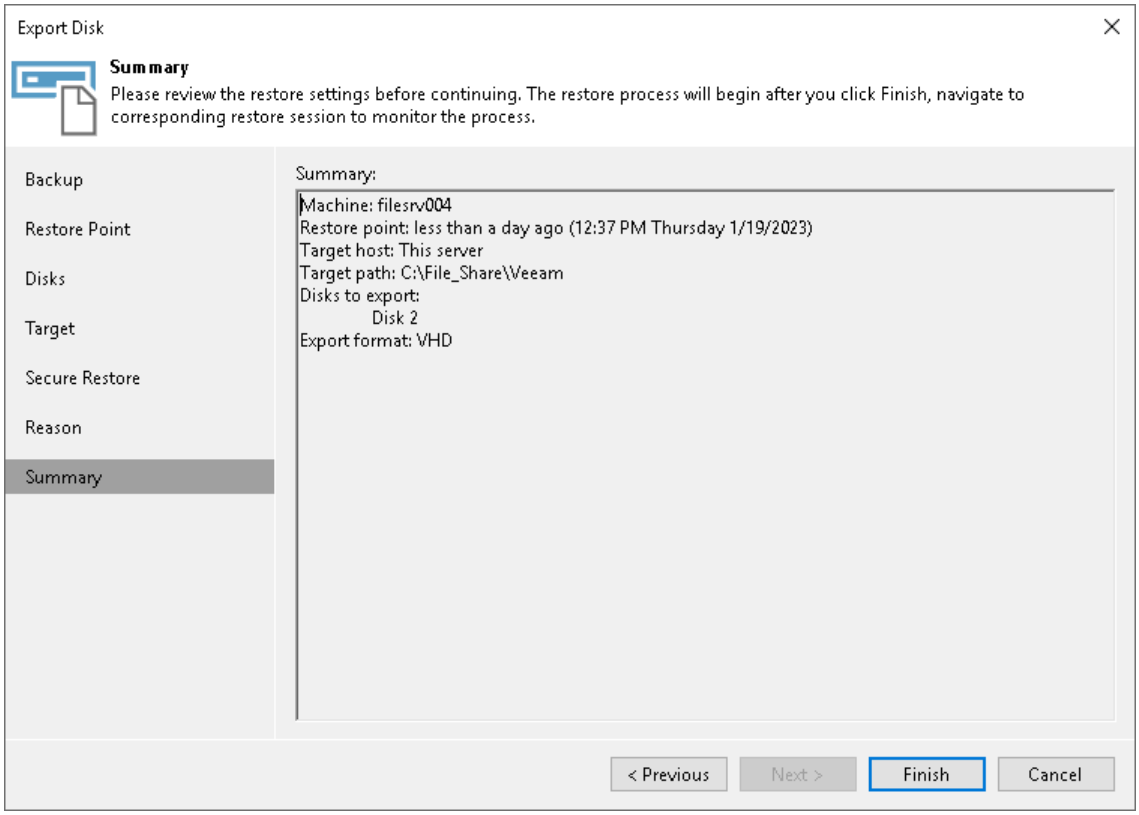
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. 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 Veeam 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 Microsoft Windows-based Veeam Agent computers, disk publishing uses the iSCSI protocol. After the publishing, the target server can access the backup content using the iSCSI initiator 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

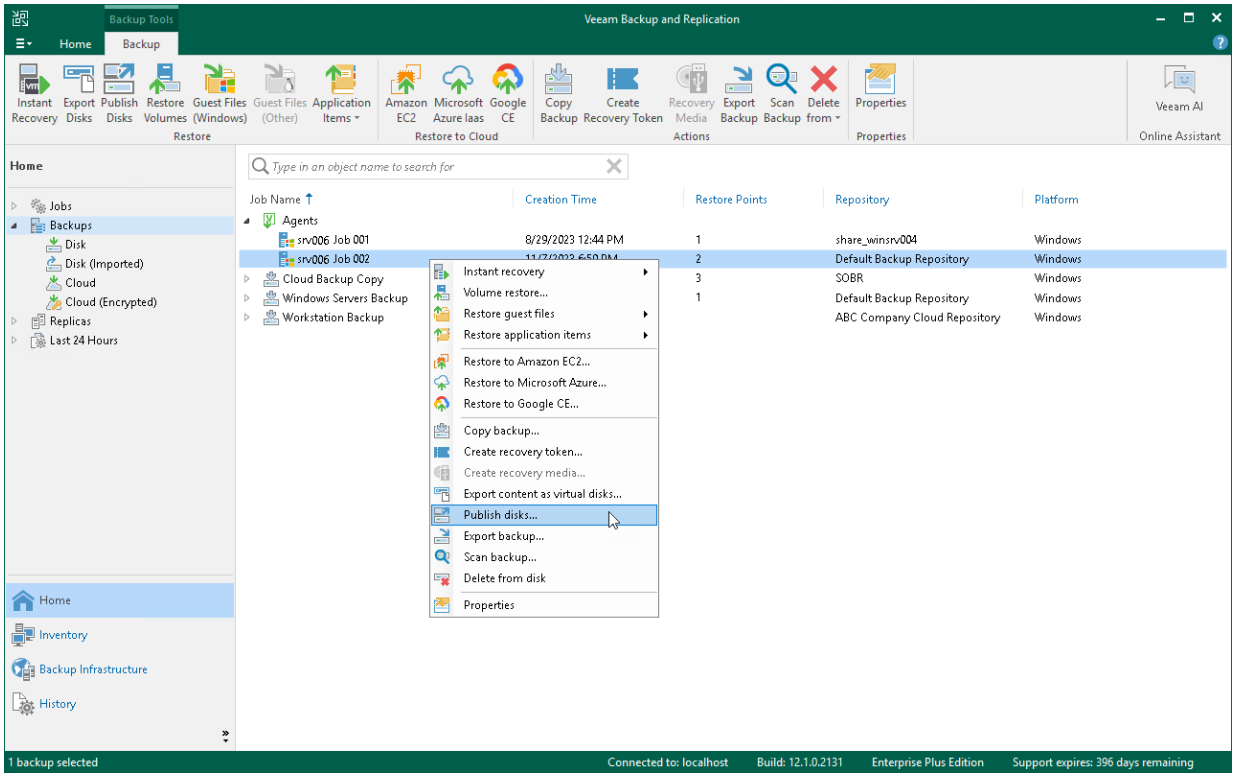
Before you publish disks, check the following requirements and limitations:

- 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 target Microsoft Windows server must support the same ReFS version or later than the version used on the Veeam Agent computer from which you plan to publish disks. For more information on which OSes support which ReFS, see the ReFS versions and compatibility matrix.

Step 1. Launch Publish Disks Wizard

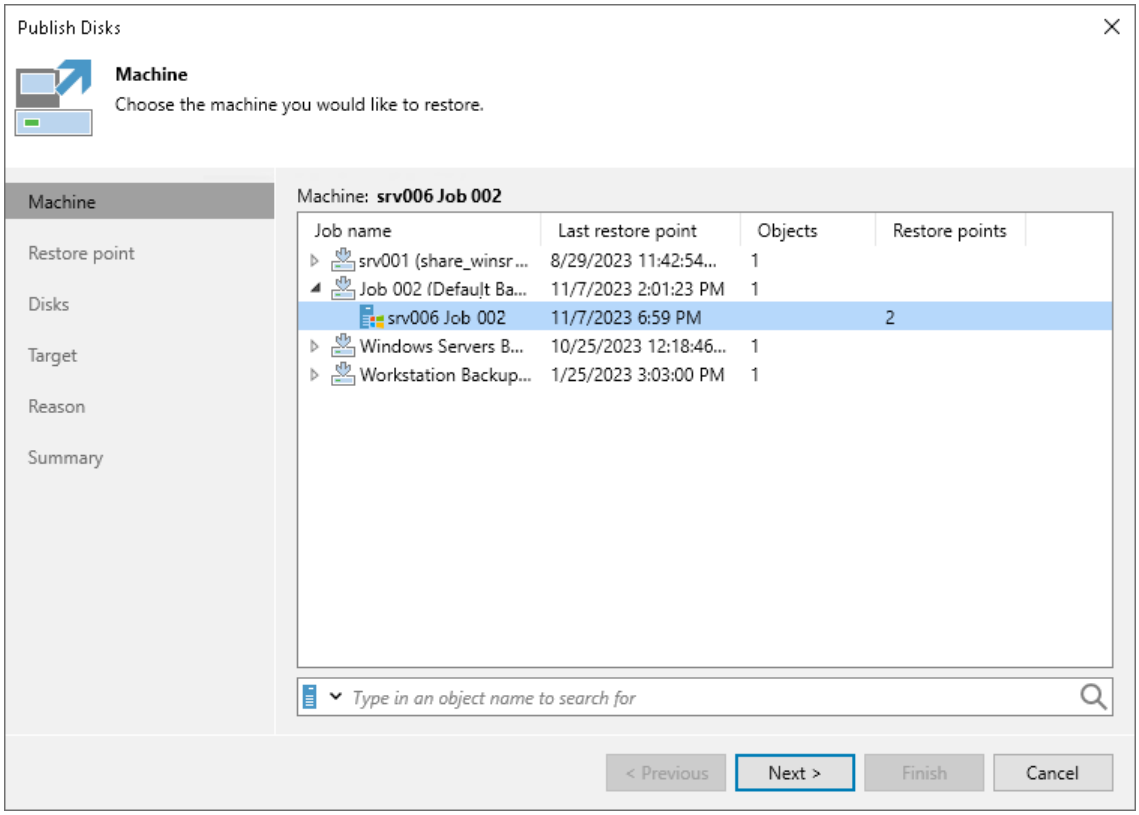
To launch the **Publish Disks** wizard, do either of the following:

- 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.



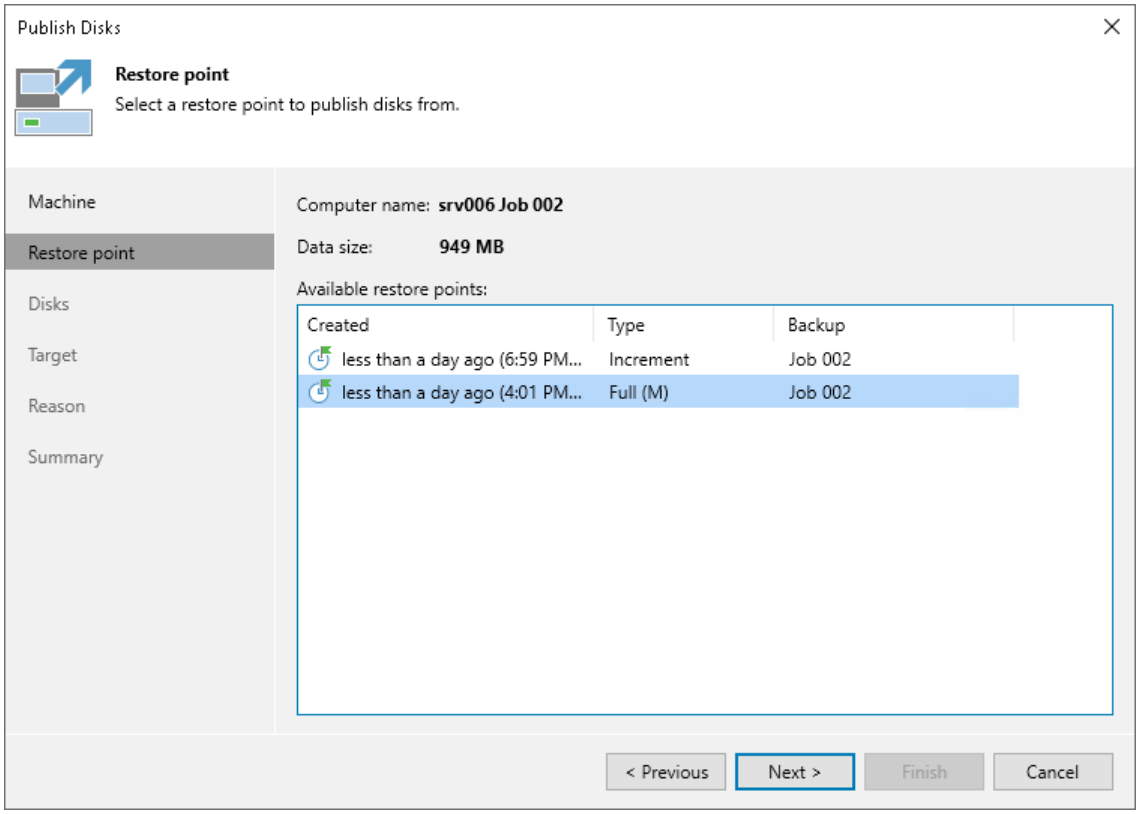
Step 2. Select Computer

At the **Machine** step of the wizard, expand a backup and select a Veeam Agent computer whose disks you want to publish.



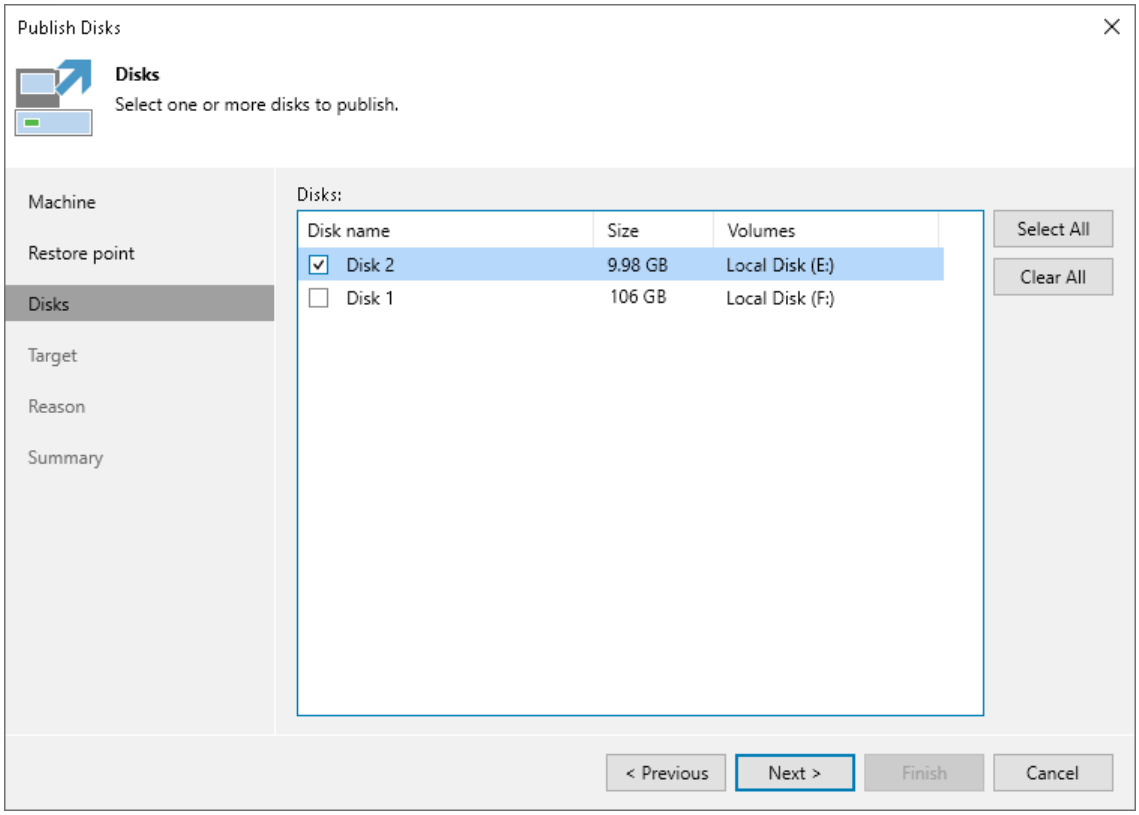
Step 3. Select Restore Point

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 Microsoft Windows server that will have access to the 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 Microsoft Windows server. To learn more, see the Adding Microsoft Windows Servers section in the Veeam Backup & Replication User Guide.

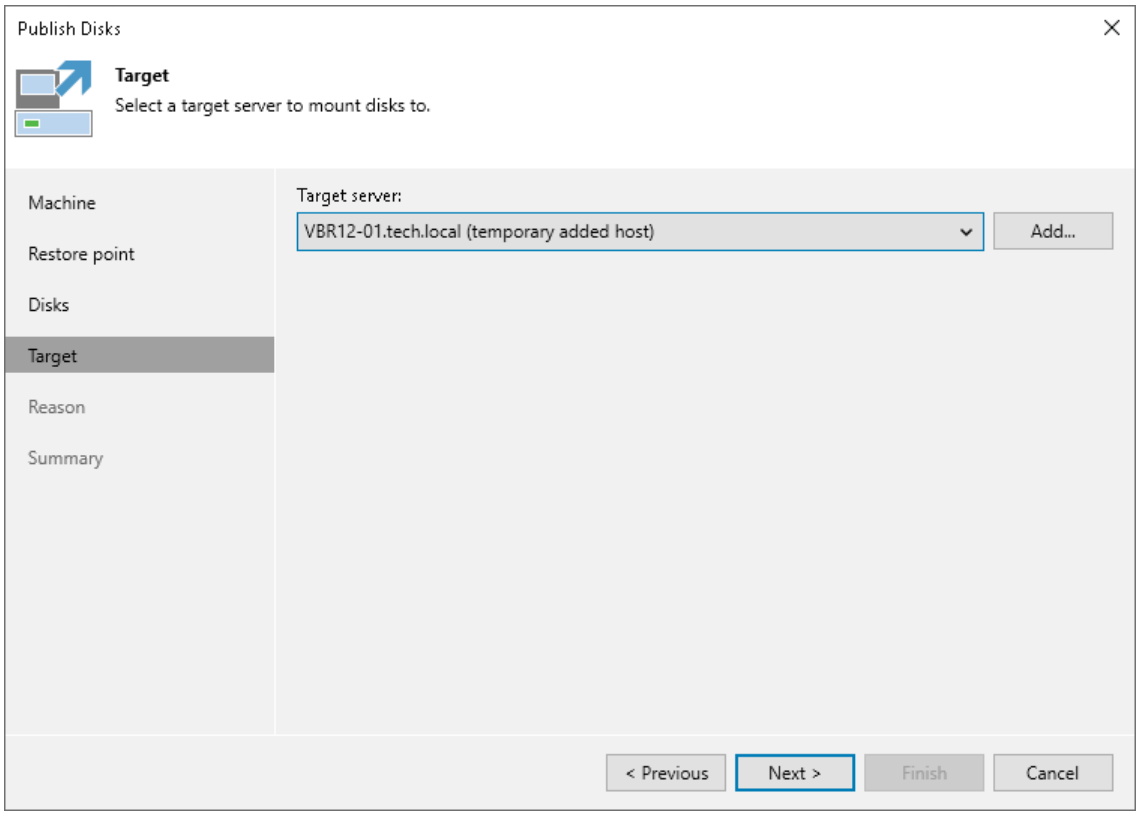
- A temporary server. In this case, select *Specify a different host* from the drop-down list. In the **Target Server** window, specify the following settings:

  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.

- The original server. In this case, select *Original server* from the drop-down list.

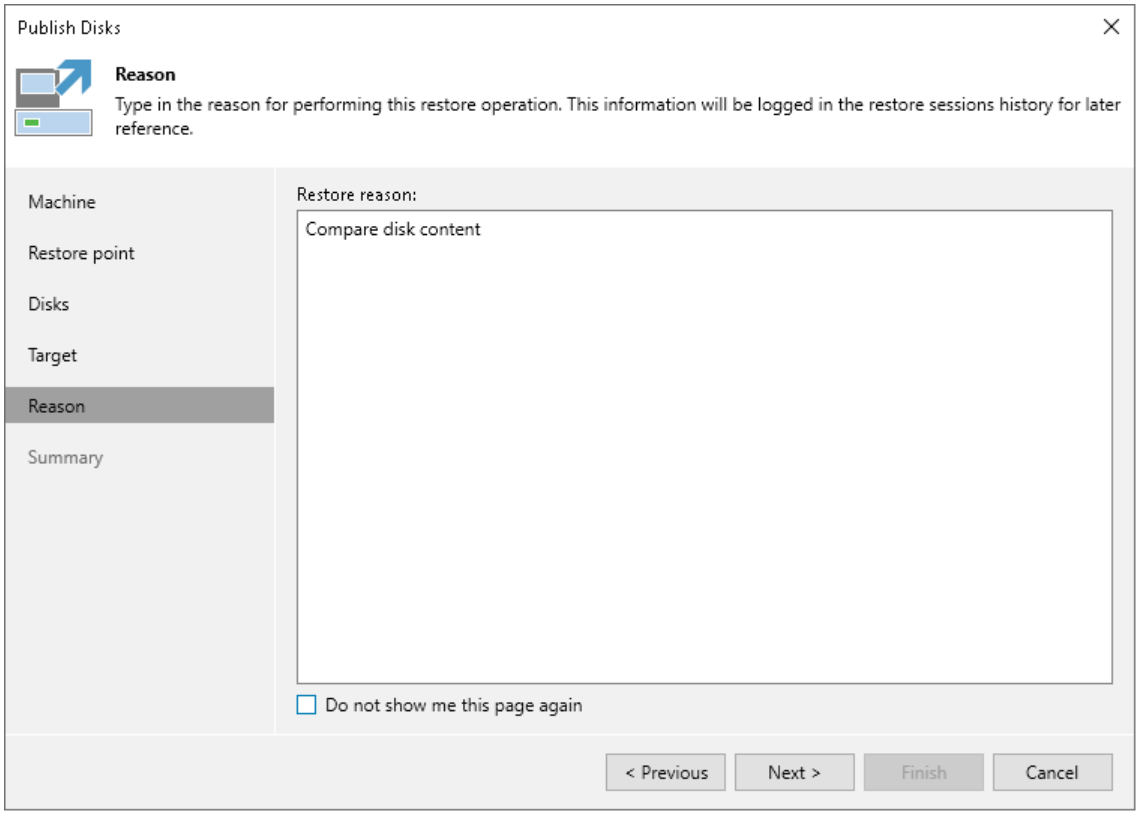
If prompted, specify credentials for the target server.



Step 6. Specify Restore Reason

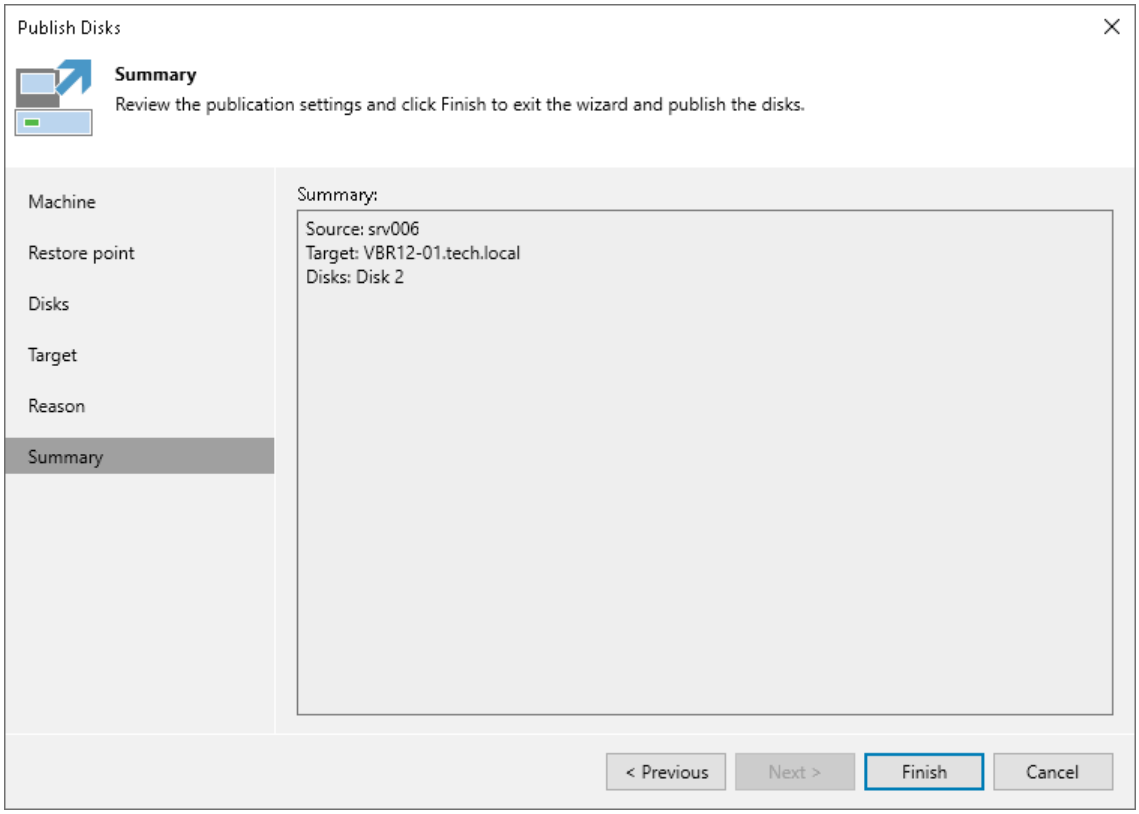
At the **Reason** step of the wizard, enter a reason for publishing disks.

> **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.



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 `C:\VeeamFLR\` folder on the target server 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.

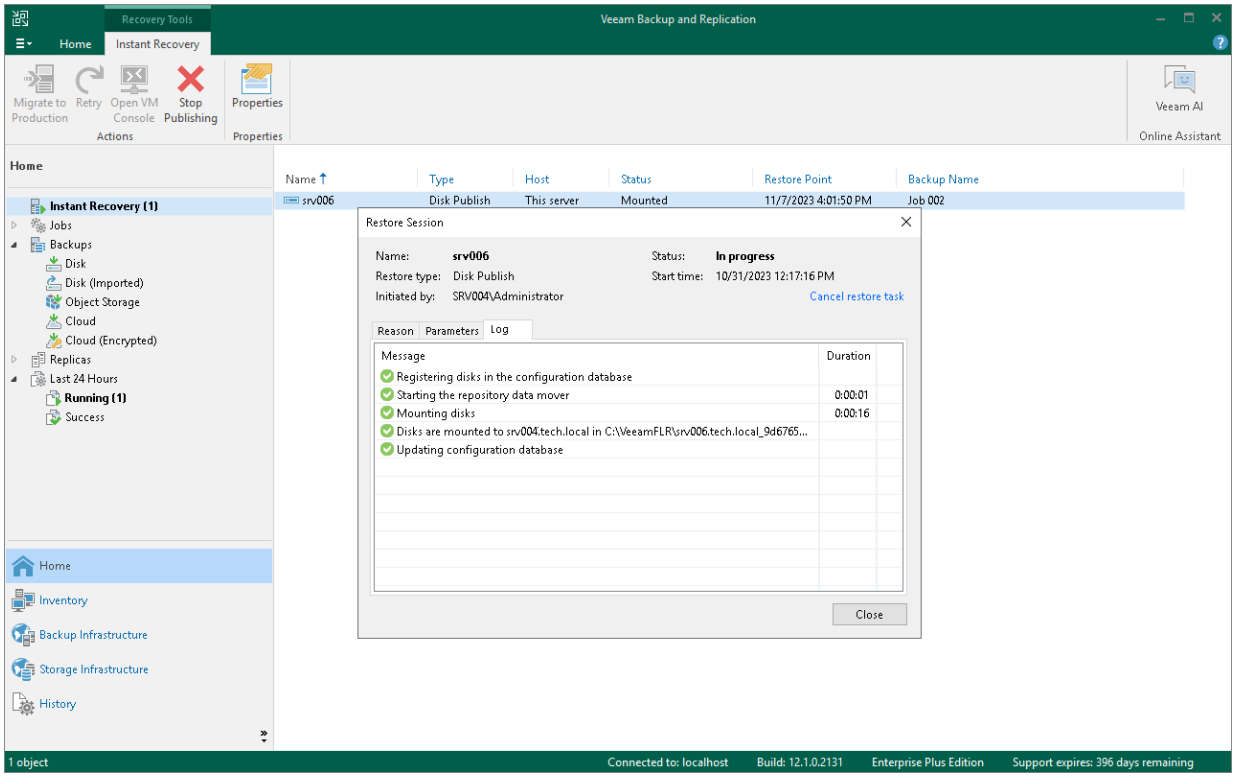
Viewing Statistics on Publishing Session

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:

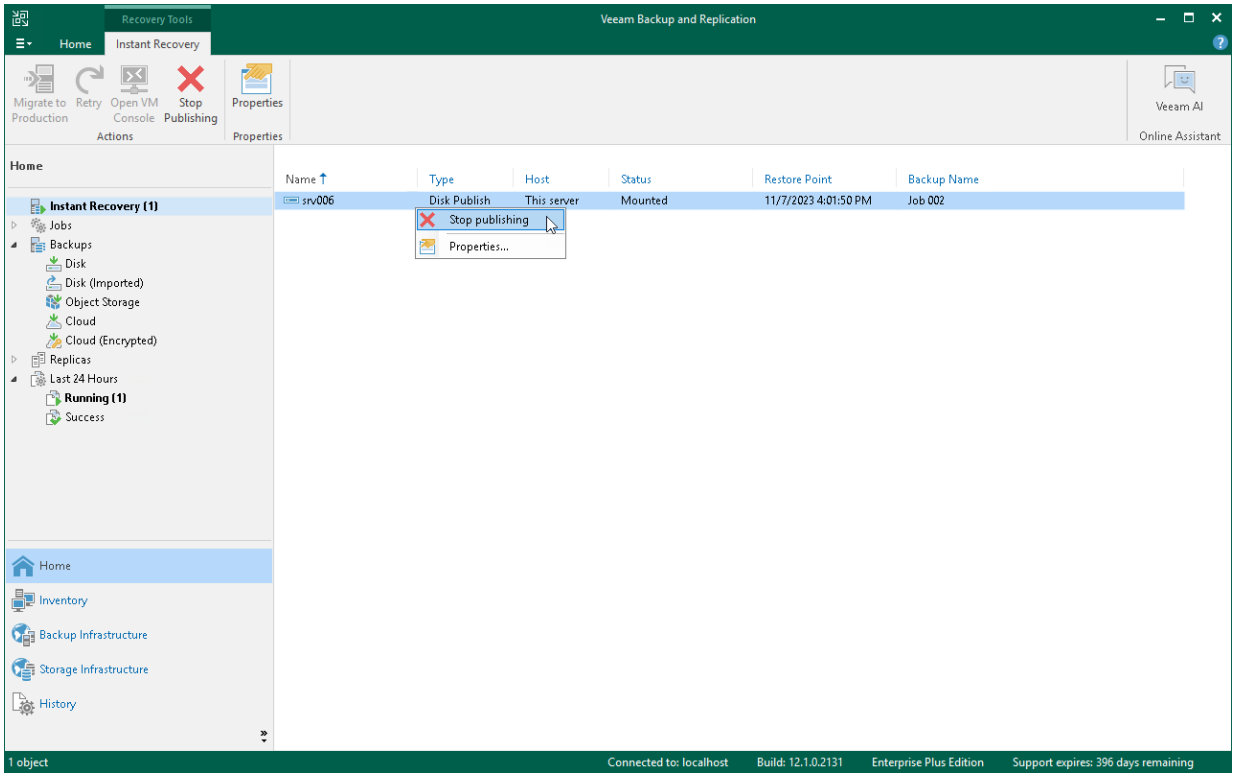
- At the top of the **Restore Session** window, Veeam Backup & Replication shows general session statistics. It includes a name of the Veeam Agent computer whose disk you want to publish, a name of the backup server which initiated the publishing session, a user name of the account under which the session 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

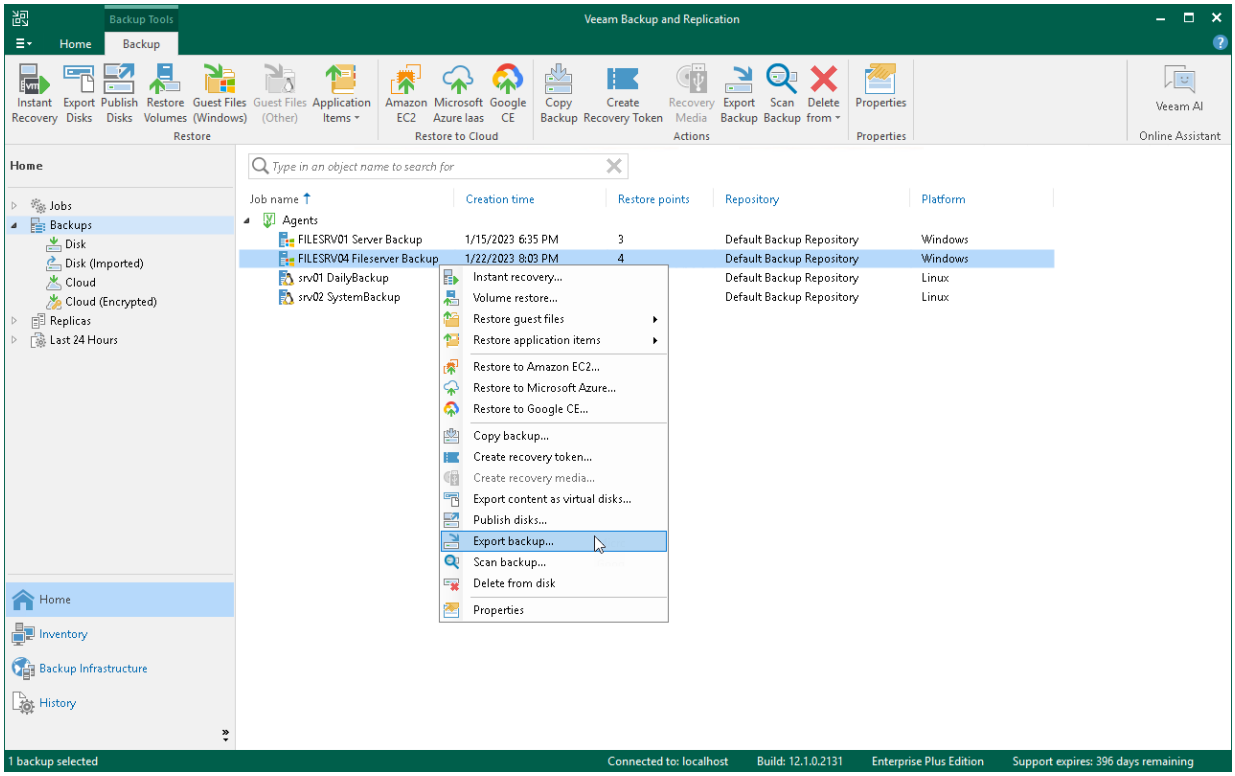
To stop a publishing session, do one of the following:

- 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**.


Recovery Tools
Veeam Backup and Replication
Home
Instant Recovery
Migrate to Production
Retry
Open VM Console
Stop Publishing
Actions
Properties
Properties
Veeam AI
Online Assistant
Home
Instant Recovery (1)
Jobs
Backups
Disk
Disk (Imported)
Object Storage
Cloud
Cloud (Encrypted)
Replicas
Last 24 Hours
Running (1)
Success
Name
Type
Host
Status
Restore Point
Backup Name
srv006
Disk Publish
This server
Mounted
11/7/2023 4:01:50 PM
Job 002
Stop publishing
Properties...
Home
Inventory
Backup Infrastructure
Storage Infrastructure
History
1 object
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

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.
- View Veeam Agent backup job statistics.
- Delete Veeam Agent backup jobs.
- View Veeam Agent backup properties.
- Create recovery token.
- Copy Veeam Agent backups.
- 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.

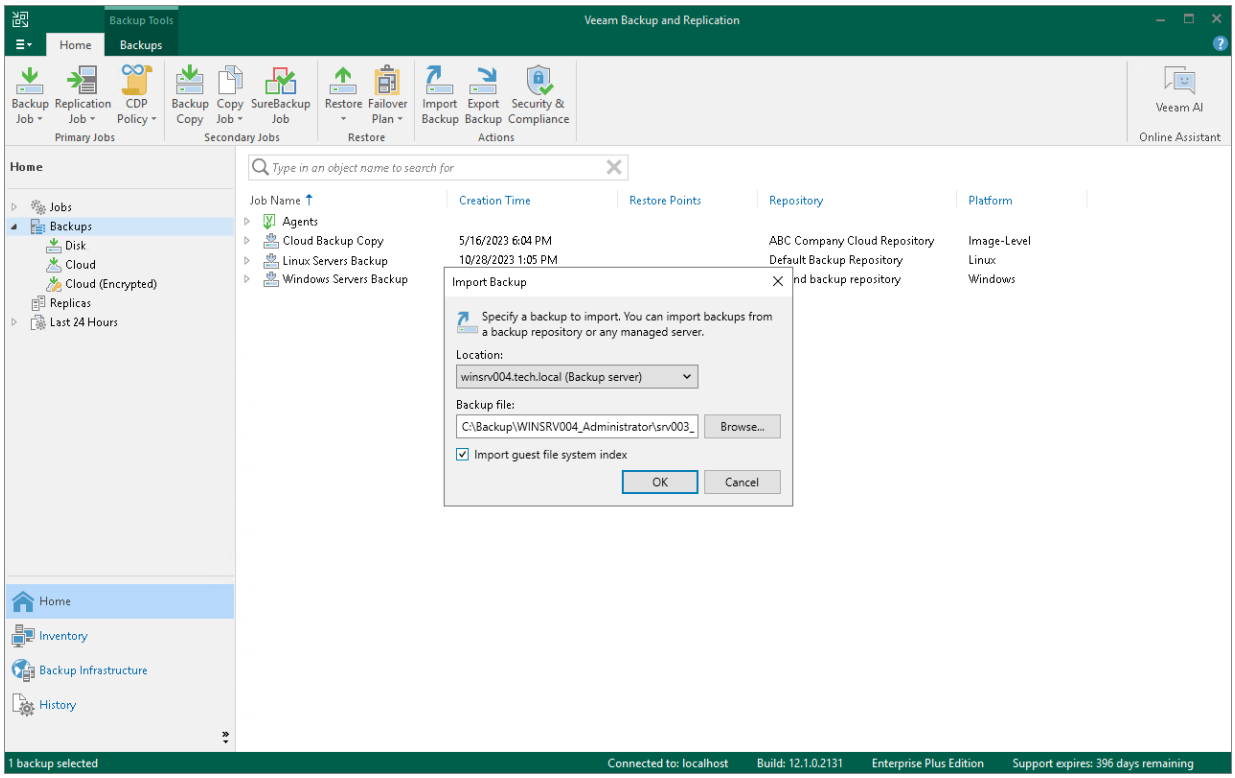
After importing, the Veeam Agent backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

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.



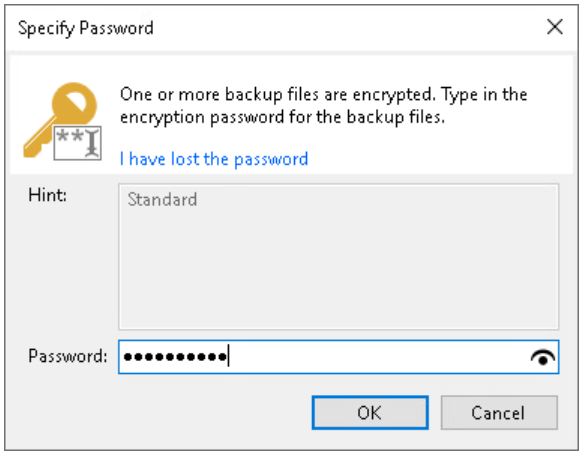
Importing Encrypted Backups

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 form all restore points in the backup chain, including those restore points that were encrypted with an old password.

If you enter correct password, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups** > **Disk (imported)** node in the inventory pane.



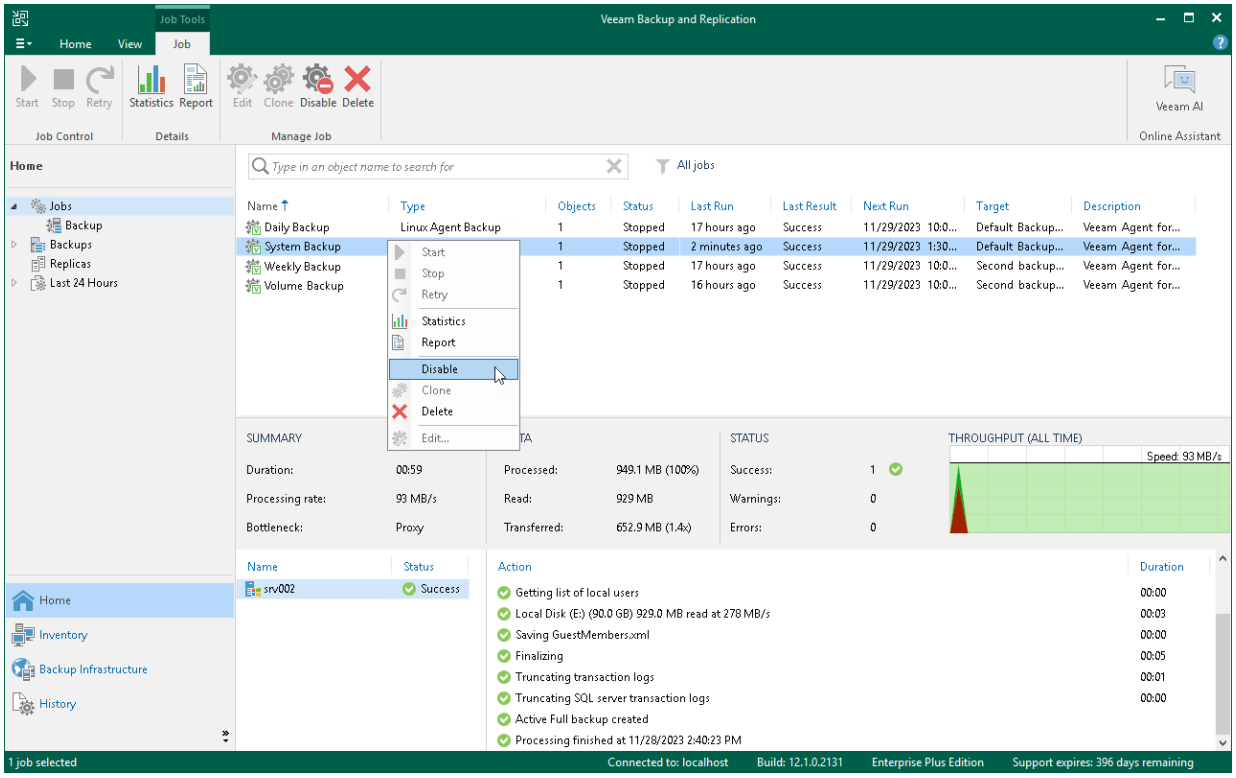
Enabling and Disabling Veeam Agent Backup Jobs

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 "*The job has been disabled by the Veeam Backup & Replication administrator*" 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.

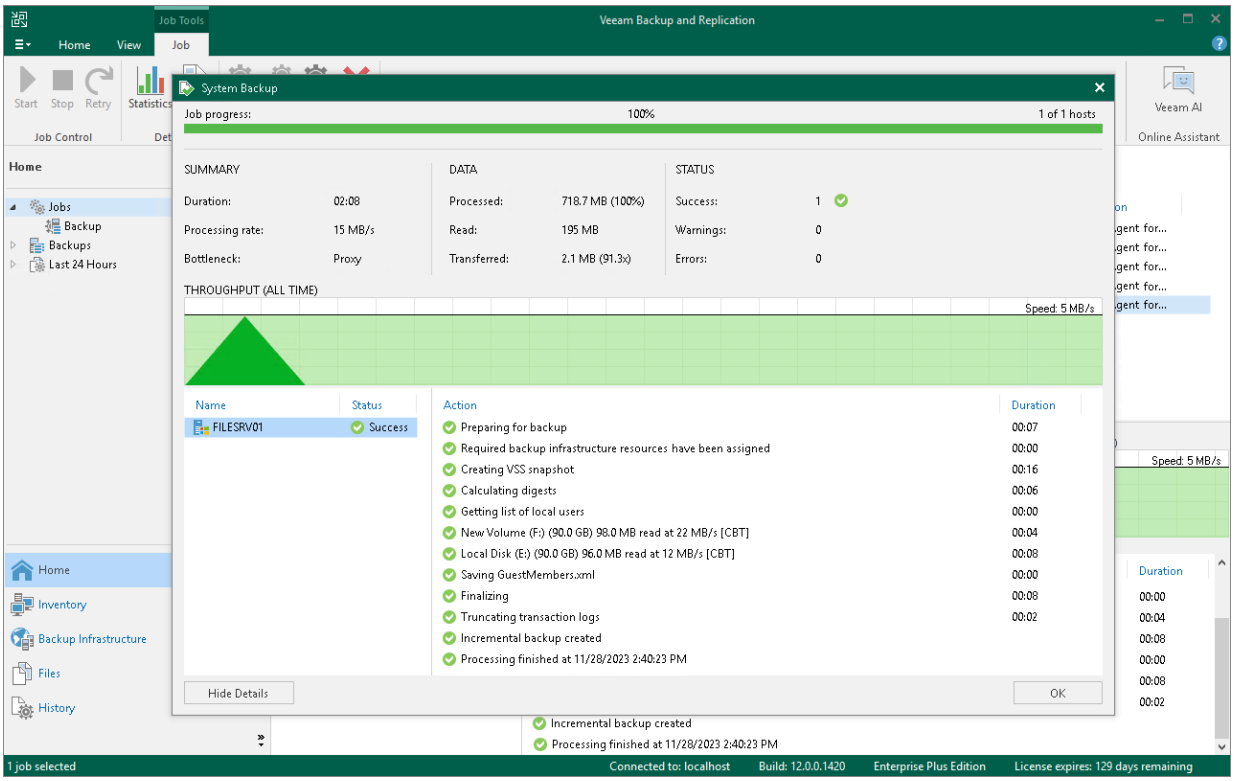


Viewing Veeam Agent Backup Job Statistics

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**.



Deleting Veeam Agent Backup Jobs

You can delete Veeam Agent backup jobs.

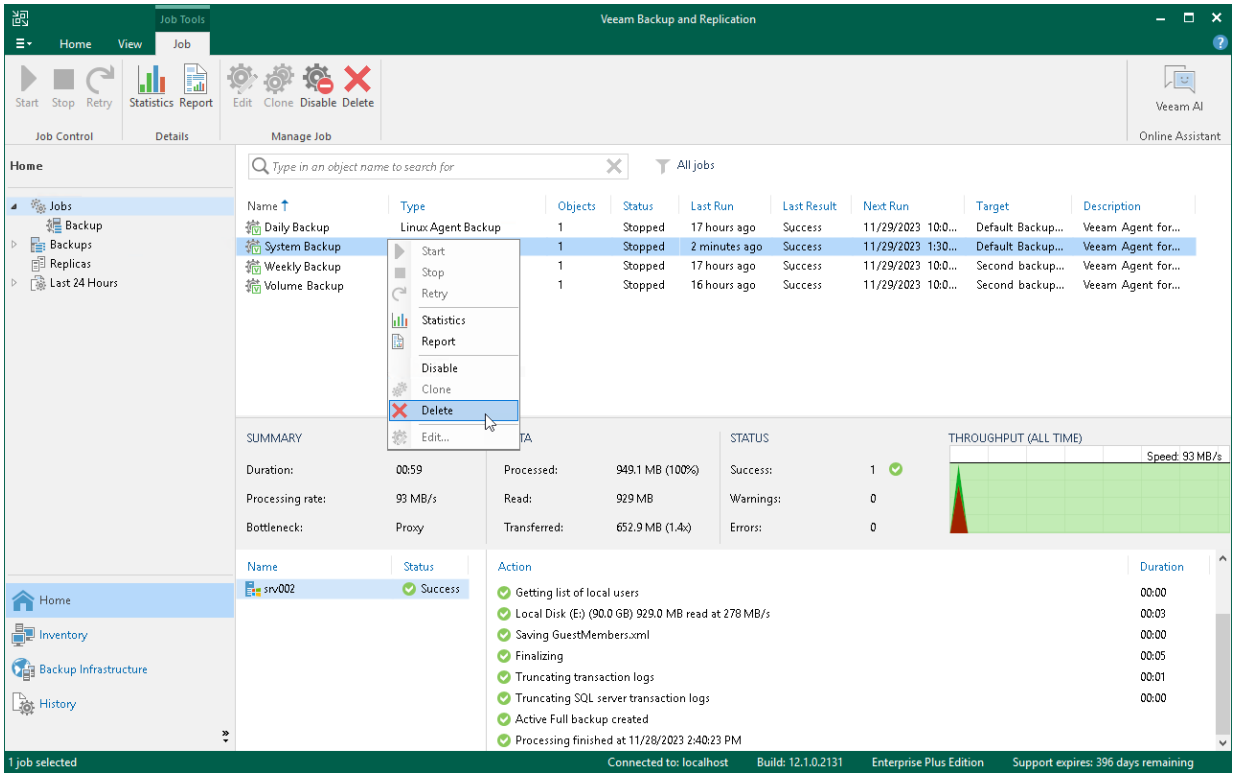
When you delete a Veeam Agent backup job, Veeam Backup & Replication removes all records about the job from its database and console. When the user starts a new Veeam Agent backup job session manually or the job starts automatically by schedule, the job will appear in the Veeam Backup & Replication console 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 computer.

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**.

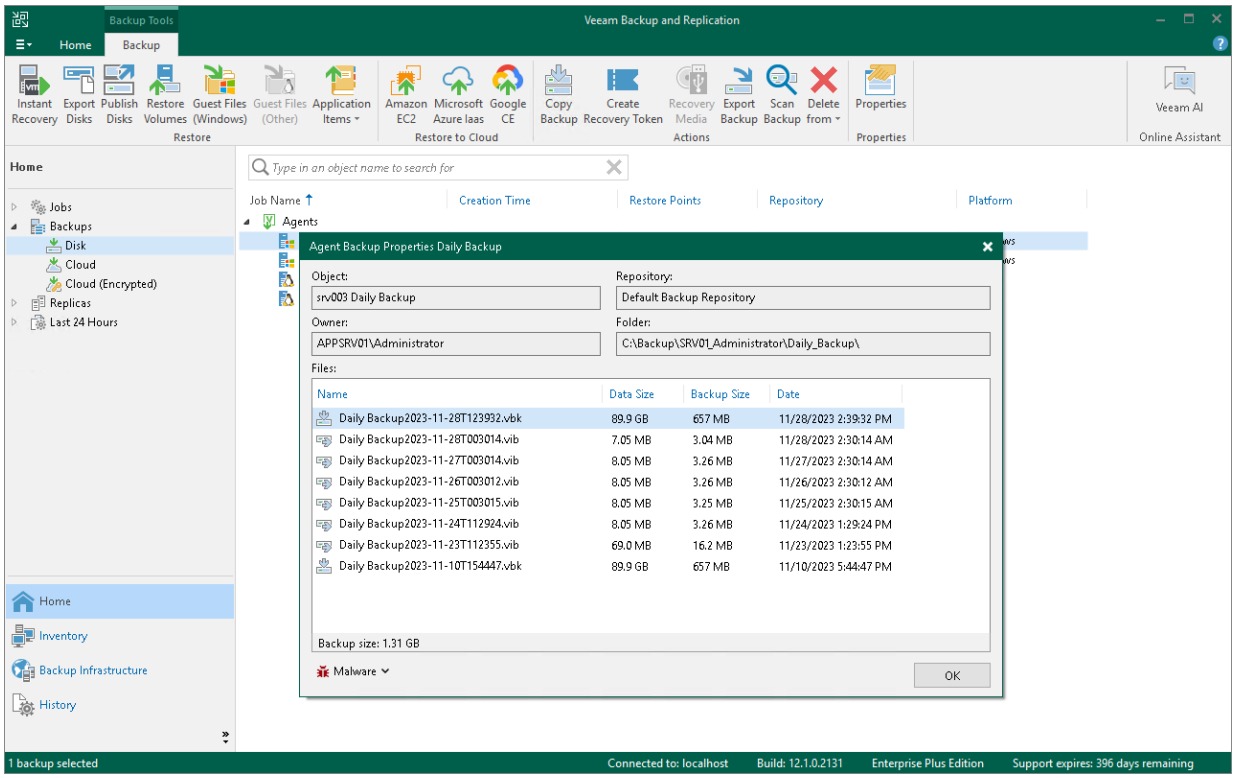


Viewing Veeam Agent Backup Properties

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**.



Creating Recovery Token

If you want to recover volumes or an entire computer protected with Veeam Agent, you can use the **Create recovery token** operation.

You can generate the recovery token on the Veeam Backup & Replication side. Then, on the computer side, with this recovery token get access to the backup and recover data that are stored in the backup.

To learn more, see Backup Server Settings.

Limitations

Before creating a recovery token, consider the following prerequisites and limitations:

- Recovery tokens stay valid for 24 hours.
- You can recover files and folders from the selected backup only.
- During recovery, Veeam Backup & Replication does not stop backup operations.
- You cannot create a recovery token for backups stored in Veeam Cloud Connect repository.

Generating Recovery Token

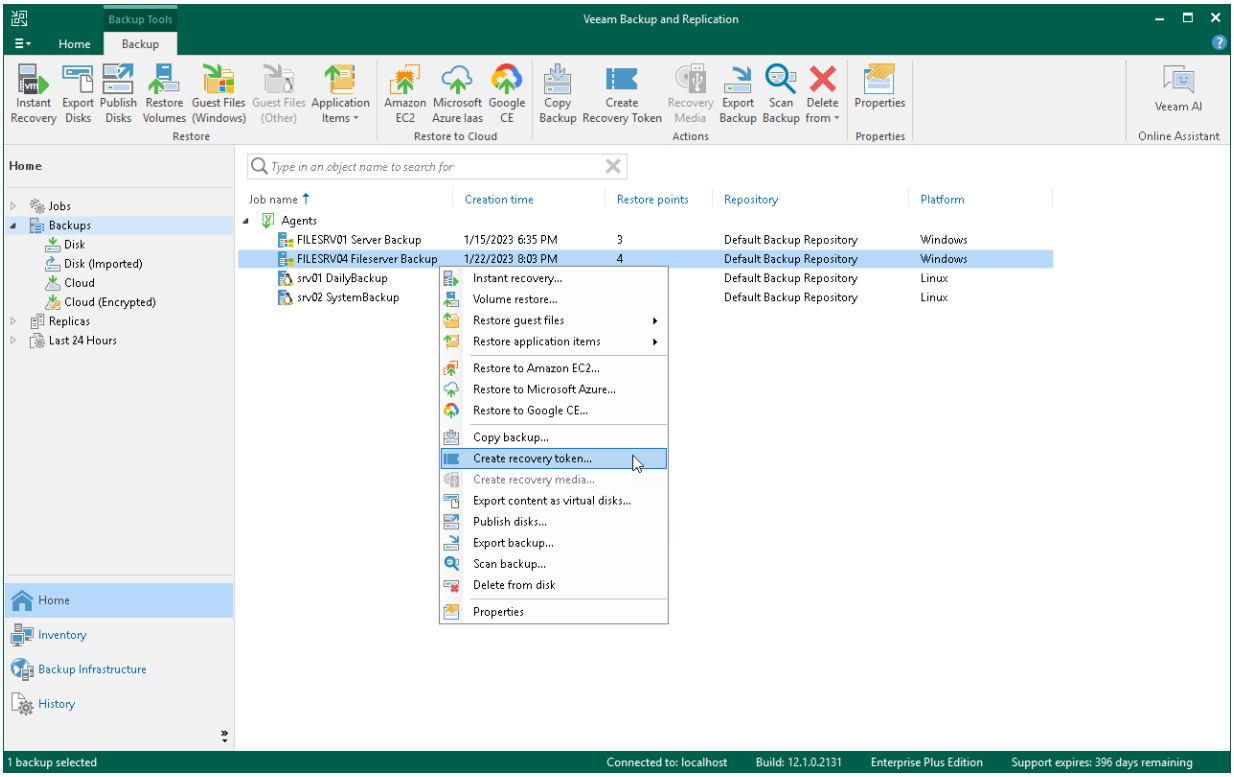
To create a recovery token on the Veeam Backup & Replication side:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Create recovery token**.

   You can create a recovery token for several backups. To do this, press and hold **[CTRL]**, select multiple backups, right-click one of the selected backups and select **Create recovery token**.
4. In the **Create Recovery Token** window, click **Create**.

You can modify the existing recovery token using the PowerShell console. To learn more, see the Working with Tokens section in the Veeam PowerShell Reference.

> **TIP**
>
> Alternatively, you can get access to the backup using user credentials. To learn more, see Backup Server Settings.


Backup Tools
Veeam Backup and Replication
Home
Backup
Instant Recovery
Export Disks
Publish Disks
Restore Volumes
Guest Files (Windows)
Guest Files (Other)
Application Items
Amazon EC2
Microsoft Azure Iaas
Google CE
Copy Backup
Create Recovery Token
Recovery Media
Export Backup
Scan Backup
Delete from
Properties
Veeam AI
Restore
Restore to Cloud
Actions
Properties
Online Assistant
Home
Type in an object name to search for
Job name
Creation time
Restore points
Repository
Platform
Jobs
Backups
Disk
Disk (Imported)
Cloud
Cloud (Encrypted)
Replicas
Last 24 Hours
Agents
FILESRV01 Server Backup
1/15/2023 6:35 PM
3
Default Backup Repository
Windows
FILESRV04 Fileserver Backup
1/22/2023 8:03 PM
4
Default Backup Repository
Windows
srv01 DailyBackup
Default Backup Repository
Linux
srv02 SystemBackup
Default Backup Repository
Linux
Instant recovery...
Volume restore...
Restore guest files
Restore application items
Restore to Amazon EC2...
Restore to Microsoft Azure...
Restore to Google CE...
Copy backup...
Create recovery token...
Create recovery media...
Export content as virtual disks...
Publish disks...
Export backup...
Scan backup...
Delete from disk
Properties
Home
Inventory
Backup Infrastructure
History
1 backup selected
Connected to: localhost
Build: 12.1.0.2131
Enterprise Plus Edition
Support expires: 396 days remaining

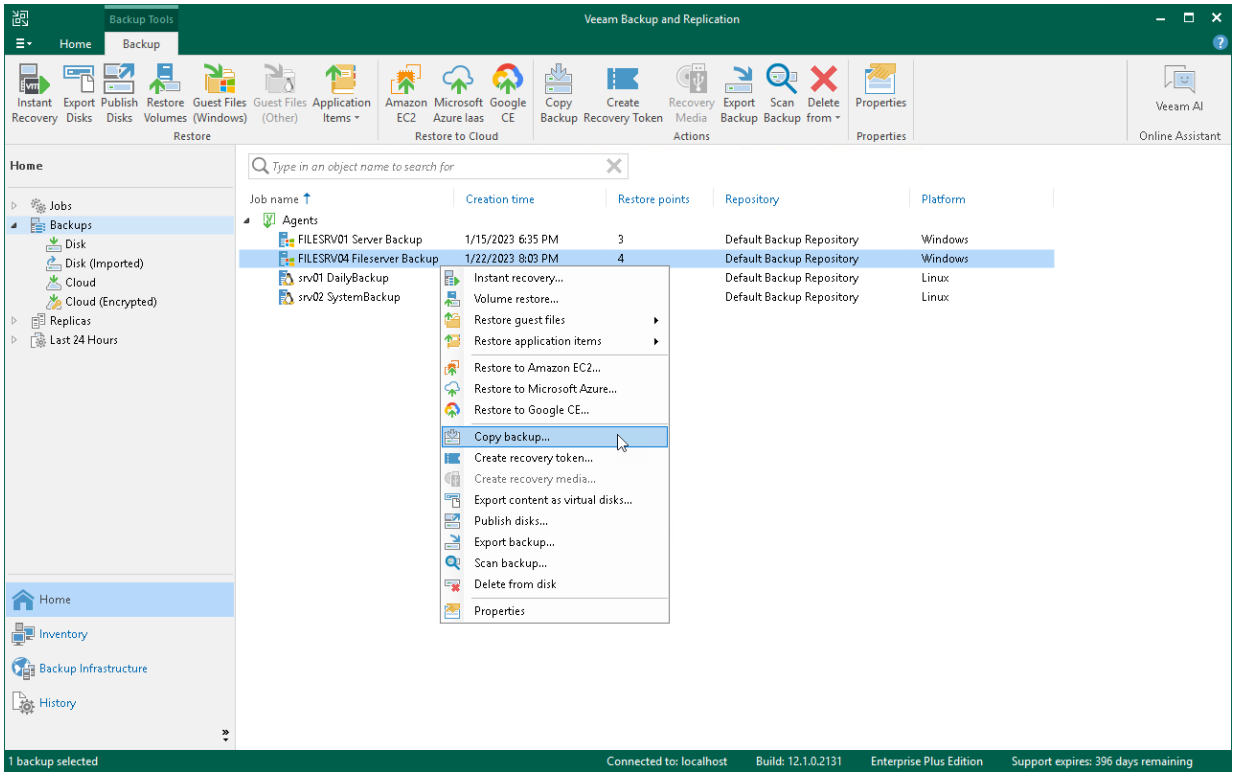
Copying Veeam Agent Backups

Veeam Backup & Replication offers the copying backup functionality that can be helpful if you want to copy backups of a backup job to another repository, local or shared folder.

When Veeam Backup & Replication performs the copy operation, it disables the job, copies files to the target location and then enables the job. After the copy operation finishes, the copied backups are shown in a node with the **(Exported)** postfix in the inventory pane.

To copy a backup, do the following:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Copy backup**.



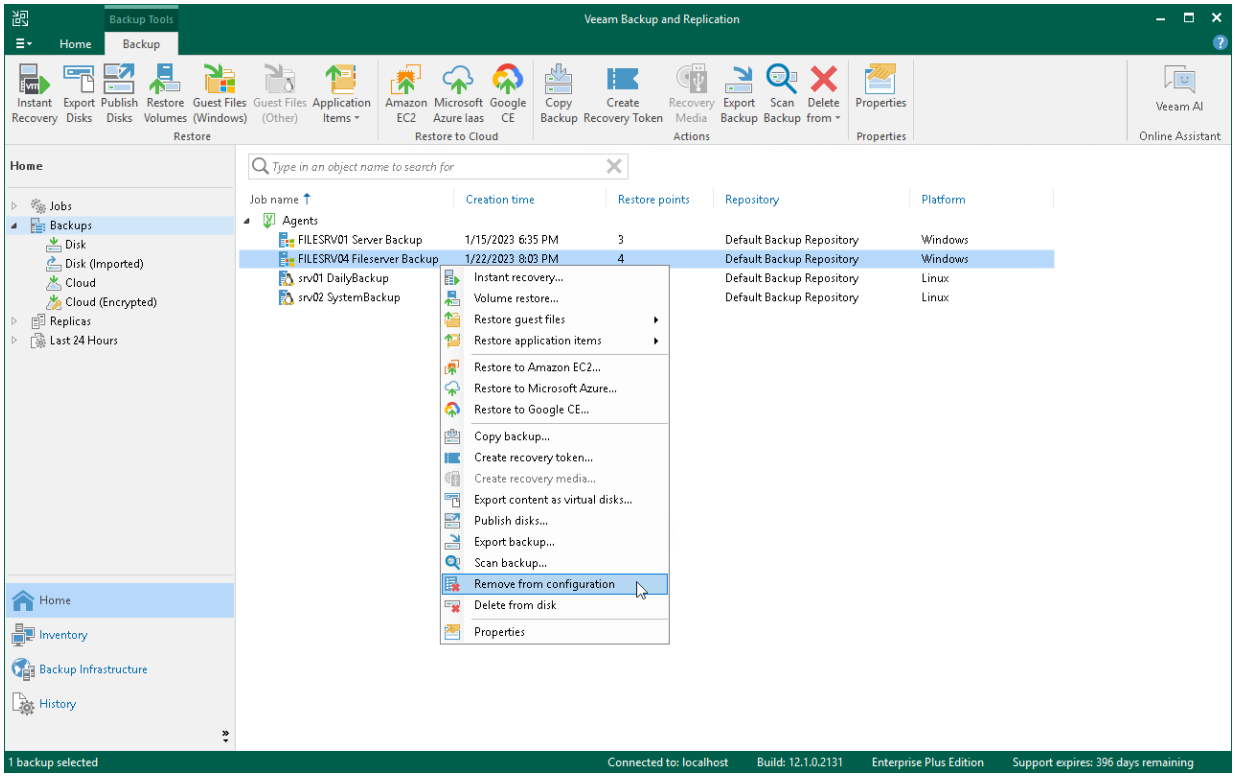
Removing Veeam Agent Backups

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.

To remove a Veeam Agent backup from configuration:

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**.

> **IMPORTANT**
>
> You should not remove a Veeam Agent backup from configuration if Veeam Agent is set up to use the backup cache and the backup cache contains one or several restore points that are not uploaded to the target location yet. If you remove such backup and then import it in the Veeam Backup & Replication console, the backup will receive the new ID in the configuration database. As a result, Veeam Agent will become unable to upload restore points from the backup cache to the target location and to create new restore points in the backup cache. To continue creating backups in the Veeam backup repository, you will need to delete restore points from the backup cache and run the backup job to create a new restore point in the backup repository.

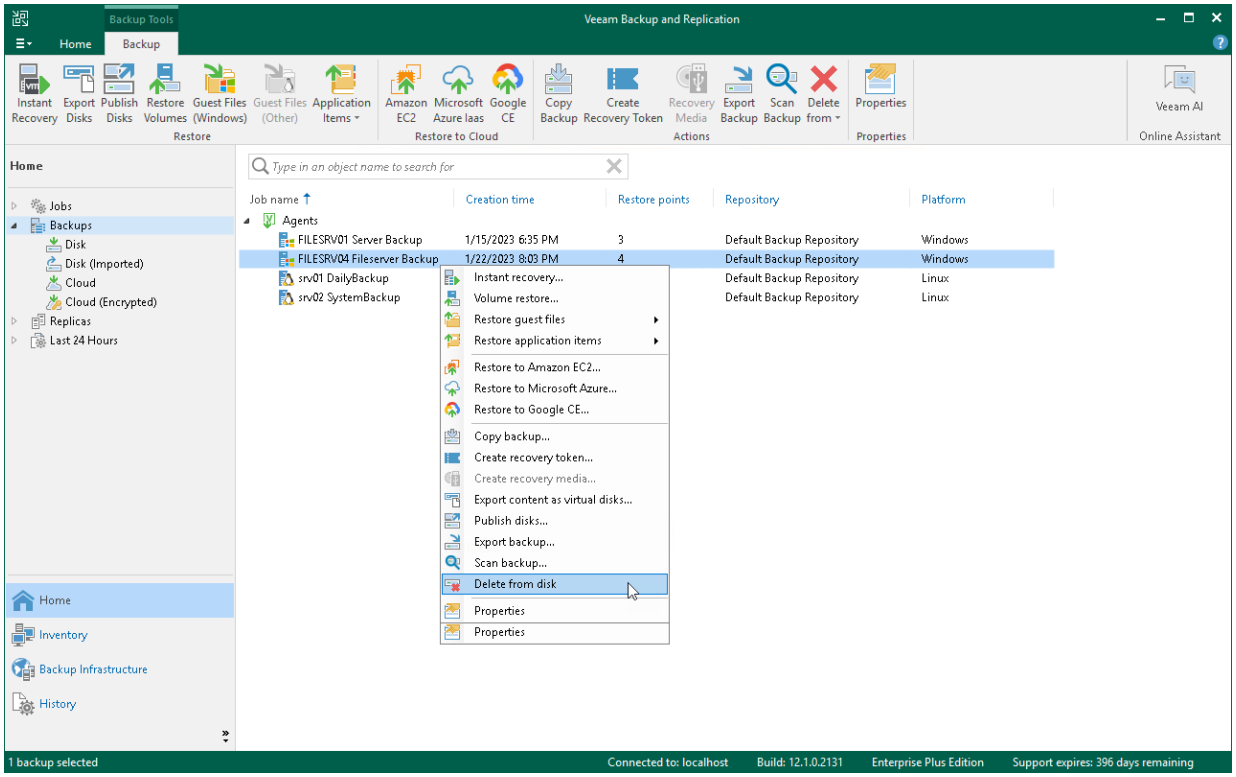


Deleting Agent Backups from Disk

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 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. Veeam Agent for Microsoft Windows sends email notifications on every type of backup tasks, such as backup job sessions started automatically by schedule, backup job sessions started from the command line and ad-hoc backup tasks. 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.

Automating Veeam Agent for Windows Operations

You can automate Veeam Agent for Microsoft Windows operations with Veeam Agent Configurator.

Veeam Agent Configurator is a tool that provides a command-line interface for Veeam Agent for Microsoft Windows. With Veeam Agent Configurator, you can perform data protection and administrative operations for Veeam Agent for Microsoft Windows from the command line, create custom scripts or integrate Veeam Agent for Microsoft Windows with third-party applications.

Veeam Agent Configurator is available in the Workstation and Server editions of Veeam Agent for Microsoft Windows.

Veeam Agent Configurator comes with Veeam Agent for Microsoft Windows. The `Veeam.Agent.Configurator.exe` file is placed in the product folder on the computer protected with Veeam Agent for Microsoft Windows, by default, `C:\Program Files\Veeam\Endpoint Backup`.

For more information, see the Veeam Agent Configurator Reference.

Appendix A. Veeam Agent Events

Veeam Agent for Microsoft Windows logs its events to event logs on the computer where the product is installed. Events can be used for monitoring the backup job activity and alerting about the backup status.

The table below lists all events logged by Veeam Agent for Microsoft Windows.

Event ID	Name	Description	Event Log	Source	Severity
110	Backup Job Started	Veeam Agent <jobname> has been started [by user <username>].	Veeam Agent	Veeam Agent	Information
115	Backup Job Resumed	Backup Job <jobname> has been resumed.	Veeam Agent	Veeam Agent	Information
190	Backup Job Finished	Veeam Agent <jobname> finished with <job status>. Job details: <additional information about the job results>[1].	Veeam Agent	Veeam Agent	Information Warning Error
191	Backup Job Retry	Veeam Agent <jobname> finished with Error and will be retried. Job details: <additional information about the job results>[1].	Veeam Agent	Veeam Agent	Warning
195	Synchronization Finished	Synchronization for cached restore points finished with <job status>. <Additional information about synchronized restore points>.	Veeam Agent	Veeam Agent	Information Warning Error
196	Destination Changed	Backup job destination has been switched from <target> to Backup Cache.	Veeam Agent	Veeam Agent	Information
197	Backup Cache Deleted	Backup cache has been deleted by <username>.	Veeam Agent	Veeam Agent	Information

Event ID	Name	Description	Event Log	Source	Severity
1074	Computer shut down[2]	The process C:\Windows\system32\Shutdown.exe (<jobname>) has initiated the shutdown of computer <jobname> on behalf of user NT AUTHORITY\SYSTEM for the following reason: No title for this reason could be found Reason Code: 0x800000ff Shutdown Type: shutdown Comment: Computer was shut down after successful backup by Veeam Agent for Microsoft Windows.	System	User32	Information
4010	License Installed	License key for Veeam Agent for Windows has been installed.	Veeam Agent	Veeam Agent	Information
4020	License Expiring	License key for Veeam Agent is about to expire in <number of days> of Days.	Veeam Agent	Veeam Agent	Warning
4030	License Expired	License key for Veeam Agent has expired.	Veeam Agent	Veeam Agent	Error
4025	License in Grace Period	Your license has expired and needs to be renewed. Veeam Agent will continue to operate for the duration of the grace period.	Veeam Agent	Veeam Agent	Error
4040	License Support Expiring	Support contract for Veeam Agent is about to expire in <number of days> of Days.	Veeam Agent	Veeam Agent	Warning
4050	License Support Expired	Support contract for Veeam Agent has expired. Contact Veeam sales representative to renew your support contract.	Veeam Agent	Veeam Agent	Error
4060	Product Edition Changed	Veeam Agent for Windows edition has been changed from <previousedition> to <currentedition>.	Veeam Agent	Veeam Agent	Information
10010	Restore Point Created	'<computername>' restore point has been created.	Veeam Agent	Veeam Agent	Information

Event ID	Name	Description	Event Log	Source	Severity
10050	Restore Point Removed	Restore point for '<computername>' has been removed according to the configured retention policy.	Veeam Agent	Veeam Agent	Information
23010	Backup Job Created	The <jobname> backup job has been created.	Veeam Agent	Veeam Agent	Information
23050	Backup Job Modified	The <jobname> backup job has been modified.	Veeam Agent	Veeam Agent	Information
23090	Backup Job Deleted	EndpointBackup <jobname> has been deleted.	Veeam Agent	Veeam Agent	Information
23051	Agent Modified	Veeam Agent option <optionname> has been changed.[3]	Veeam Agent	Veeam Agent	Information
23501	Agent Updated	Veeam Agent has been successfully updated.	Veeam Agent	Veeam Agent	Information
		Failed to update Veeam Agent.			Error
23110	Backup Mode Changed	The <jobname> backup mode has been changed from <previousmode> to <currentmode>.	Veeam Agent	Veeam Agent	Information
23120	Backup Source Updated	The <jobname> backup job source objects have been updated.	Veeam Agent	Veeam Agent	Information
26010	USB Device Ejected	Target USB device has been successfully ejected.	Veeam Agent	Veeam Agent	Information
178	Managed mode Enabled	Veeam Agent has been switched to managed mode.[4]	Veeam Agent	Veeam Agent	Information
179	Managed mode Disabled	Veeam Agent has been switched to free mode.[4]	Veeam Agent	Veeam Agent	Information
201	Read-only mode Enabled	Read only UI access has been enabled.[4]	Veeam Agent	Veeam Agent	Information
202	Read-only mode Disabled	Read only UI access has been disabled.[4]	Veeam Agent	Veeam Agent	Information

[1] Job details contain information about the reason for completing the job with the Warning or Error status.

[2] The event is triggered if the user has instructed Veeam Agent for Microsoft Windows to shut down the computer on successful backup.

[3] The event is triggered if the user has changed any Veeam Agent for Microsoft Windows setting other than backup job settings.

[4] The event can be triggered if Veeam Agent for Microsoft Windows is managed by a Remote Monitoring and Management platform, for example, LabTech.

Appendix B. Moving Veeam Agent Backups

A Veeam Agent backup job starts a new backup chain when you change a target location in the backup job settings. If you do not want the backup job to start a new backup chain, you can map a backup job to the previously made backups and continue the existing backup chain. For more information about backup chains, see Backup Chain.

This appendix describes the following cases of moving Veeam Agent backups:

- Move a Veeam Agent backup to the Veeam backup repository.

  In this section, scenarios describe how to move a locally stored backup to a Veeam backup repository and how to move a backup from one Veeam backup repository to another and continue the existing backup chain.

- Move a Veeam Agent backup to the Veeam Cloud Connect repository.

  In this section, scenarios describe how to move a locally stored backup to a simple backup repository or scale-out backup repository used as a cloud repository and continue the existing backup chain.

> **TIP**
>
> This appendix describes how to move backups created by Veeam Agent operating in the standalone mode. To learn how to move backups created by Veeam Agent operating in the managed mode, see the following topics:
>
> - If Veeam Agent is managed by Veeam Backup & Replication, see the Moving Backup section in the Veeam Agent Management Guide.
> - If Veeam Agent is managed by Veeam Service Provider Console, see the Moving Veeam Agent Backups section in the Guide for Service Providers.
>
> For more information about Veeam Agent operation modes, see Standalone and Managed Operation Modes.

Moving Veeam Agent Backups to Veeam Backup Repository

This topic describes how to place existing Veeam Agent backups in a Veeam backup repository so that the Veeam Agent backup job continues the existing backup chain.

This topic covers the following scenarios:

- Move a backup stored locally to the Veeam backup repository.
- Replace the initial Veeam backup repository with another Veeam backup repository.

> **NOTE**
>
> Keep in mind that the following users participate in implementation of both scenarios:
>
> - Veeam Agent user performs all actions in the Veeam Agent control panel.
> - Veeam Backup Administrator performs all actions in the Veeam Backup & Replication console.

Moving Locally Stored Backup to Veeam Backup Repository

In this scenario, a backup job is targeted at a local folder. The backup job ran at least once.

This scenario can be helpful when you need to back up a large amount of data to the Veeam backup repository but the network connection is slow. In this case, you can create a backup locally and move it to the Veeam backup repository.

To move locally stored backup files to the Veeam backup repository, the Veeam Backup Administrator must perform the following steps:

1. Browse to the folder where Veeam backup repository stores backup files. For example, `C:\Backup`.

   For more information, see the Configure Backup Repository Settings section in the Veeam Backup & Replication User Guide.

2. In the `C:\Backup` folder, create a new folder in the following format: `C:\Backup\<domain_name>_<user_name>\<folder_name>`, where:

   - `<domain_name>` — domain name that Veeam Agent uses to connect to the Veeam backup repository.
   - `<user_name>` — user name that Veeam Agent uses to connect to the Veeam backup repository.
   - `<folder_name>` — name of the target folder to store backups. You can use the name of the original backup job or specify a new name for the folder.

   For example: `C:\Backup\TECH_Administrator\System_Backup`.

3. Using external tools, move all backup files to the folder created at the step 2.

4. Rescan the Veeam backup repository. To learn how to rescan the Veeam backup repository, see the Rescanning Backup Repositories section in the Veeam Backup & Replication User Guide.

   As a result, the moved backup will appear under the **Backups** > **Disk (Imported)** node in the inventory pane.

> **NOTE**
>
> If the backup file is encrypted, you must decrypt the backup before proceeding to the next step. To learn more, see the Decrypting Data with Password section in the Veeam Backup & Replication User Guide.

After the Veeam Backup Administrator moved the backup files to the target folder, the Veeam Agent user must perform the following steps:

1. Edit the Veeam Agent backup job:
   a. At the **Name** step of the wizard, make sure that the name of the backup job is the same as the name of the folder you created at the step 2.
   b. At the **Destination** step of the wizard, target the backup job at the Veeam backup repository.
   c. At the **Backup Server** step of the wizard, select a backup repository where you want to store backups and specify settings for the Veeam backup server that manages the target backup repository. For more information, see Veeam Backup Repository Settings.
   d. At the **Backup Repository** step of the wizard, click the **Map backup** link and select the moved backup file.
   e. At the **Summary** step of the wizard, make sure that the *Run the job when I click Finish* check box is cleared and click **Finish** to save changes. As a result, the backup will be moved from the **Backups** > **Disk (Imported)** node to the **Backups** > **Disk** node in the inventory pane.
2. Run the Veeam Agent backup job. The backup job will continue the backup chain for the full backup that was moved to the Veeam backup repository.

Replacing Initial Veeam Backup Repository with Another Veeam Backup Repository

In this scenario, the backup job is targeted at a Veeam backup repository and you want to replace the initial repository with another Veeam backup repository.

This scenario can be helpful if you want to move backed up data to a repository that has more storage capacity.

To replace the Veeam Backup & Replication repository, the Veeam Backup Administrator must perform the following steps:

1. Delete the existing Veeam Agent backup job from the Veeam Backup & Replication console. For more information, see Deleting Veeam Agent Backup Jobs.

   > **NOTE**
   >
   > Deleting the job from the Veeam Backup & Replication console does not remove the backup job from the Veeam Agent control panel.

2. Delete configuration database records about backups created by the Veeam Agent backup job. For more information, see Removing Veeam Agent Backups.
3. Browse to the folder where the target Veeam backup repository stores backup files. For example, `C:\Backup`.

   For more information, see the Configure Backup Repository Settings section in the Veeam Backup & Replication User Guide.

4. In the `C:\Backup` folder, create a new folder in the following format: `C:\Backup\<domain_name>_<user_name>\<folder_name>`, where:
   - `<domain_name>` — domain name that Veeam Agent uses to connect to the Veeam backup repository.
   - `<user_name>` — user name that Veeam Agent uses to connect to the Veeam backup repository.
   - `<folder_name>` — name of the target folder to store backups. You can use the name of the original backup job or specify a new name for the folder.

   For example: `C:\Backup\TECH_Administrator\System Backup`
5. Using external tools, move all backup files to the folder created at the step 4.
6. Rescan the Veeam backup repository. To learn more, see the Rescanning Backup Repositories section in the Veeam Backup & Replication User Guide.

   As a result, the moved backup will appear under the **Backups** > **Disk (Imported)** node in the inventory pane.

   > **NOTE**
   >
   > If the backup file is encrypted, you must decrypt the backup before proceeding to the next step. To learn more, see the Decrypting Data with Password section in the Veeam Backup & Replication User Guide.

After the Veeam Backup Administrator moved the backup files to the target folder, the Veeam Agent user must perform the following steps:

1. Edit the Veeam Agent backup job:
   a. At the **Name** step of the wizard, make sure that the name of the backup job is the same as the name of the folder you created at the step 4.
   b. At the **Backup Server** step of the wizard, select a new backup repository and specify settings for the Veeam backup server that manages the target backup repository. For more information, see Veeam Backup Repository Settings.
   c. At the **Backup Repository** step of the wizard, click the **Map backup** link and select the moved backup file.
   d. At the **Summary** step of the wizard, make sure that the *Run the job when I click Finish* check box is cleared and click **Finish** to save changes. As a result, the backup will be moved from the **Backups** > **Disk (Imported)** node to the **Backups** > **Disk** node in the inventory pane.
2. Run the Veeam Agent backup job.

Moving Veeam Agent Backups to Veeam Cloud Connect Repository

This topic describes how to place existing Veeam Agent backups in a cloud repository in the Veeam Cloud Connect infrastructure so that the Veeam Agent backup job continues the existing backup chain. For more information about Veeam Cloud Connect, see the Veeam Cloud Connect Guide.

The scenarios described in this section can be helpful when you need to back up a large amount of data to the Veeam Cloud Connect repository but the network connection is slow. In this case, you can create a backup locally and move it to the Veeam Cloud Connect repository.

This topic covers the following scenarios:

- Move a backup to a simple backup repository used as a cloud repository
- Move a backup to a scale-out backup repository used as a cloud repository

> **NOTE**
>
> Keep in mind that the following users participate in implementation of both scenarios:
>
> - Service provider moves backup files to the target repository.
> - Veeam Backup Administrator rescans the target repository in the Veeam Backup & Replication console.
> - Veeam Agent user performs actions in the Veeam Agent control panel.

Moving Backup to Simple Backup Repository

Use this scenario if you want to move a locally stored backup to a simple backup repository used as a cloud repository. For information about simple backup repositories, see the Backup Repositories section in the Veeam Backup & Replication User Guide.

To move locally stored backup files to the cloud repository, the service provider must perform the following steps:

1. Browse to the folder where the cloud repository stores backup files. For example, `C:\Backup`.

   For more information, see the Configure Backup Repository Settings section in the Veeam Backup & Replication User Guide.

2. In the `C:\Backup` folder, create a new folder in the following format:

   - [If you work with tenant accounts] `C:\Backup\<tenant_name>\<folder_name>`
   - [If you work with subtenant accounts] `C:\Backup\<tenant_name>\Users\<subtenant_name>\<folder_name>`,

   where:

   - `<tenant_name>` — name of the tenant account that you use to connect to the service provider. For more information, see the Tenant Account Credentials section in the Veeam Cloud Connect Guide.
   - `<subtenant_name>` — name of the subtenant account that you use to connect to the service provider. For more information, see the Managing Subtenant Accounts on SP Side section in the Veeam Cloud Connect Guide.

- <folder_name> — name of the target folder to store backups. You can use the name of the original backup job or specify a new name for the folder.

For example, C:\Backup\ABC_Company\System_Backup or C:\Backup\ABC_Company\Users\John_Smith\System_Backup.

3. Using external tools, move all backup files to the folder created at the step 2.

After the service provider moved the backup files to the backup folder, the Veeam Backup Administrator must rescan the cloud repository. To learn how to rescan a repository, see the Rescanning Backup Repositories section in the Veeam Backup & Replication User Guide.

The information about the added backup will be displayed in the rescan job session window.

After the Veeam Backup Administrator rescanned the backup repository, the Veeam Agent user must perform the following steps:

1. Edit the Veeam Agent backup job:
   a. At the **Destination** step of the wizard, target the backup job at the Veeam Cloud Connect Repository.
   b. At the **Service Provider** step of the wizard, specify settings for the cloud gateway to connect to the service provider. For more information, see Specifying Service Provider Settings.
   c. At the **Credentials** step of the wizard, specify settings for the tenant or subtenant account that you want to use to connect to the service provider. For more information, see Specifying User Account Settings.
   d. At the **Backup Resources** step of the wizard, click the **Map backup** link and select the moved backup.
   e. At the **Summary** step of the wizard, click **Finish** to save changes.
2. Run the Veeam Agent backup job. The backup job will continue the backup chain for the full backup that was moved to the cloud repository.

Moving Backup to Scale-Out Backup Repository

Use this scenario if you want to move a locally stored backup to a scale-out backup repository used as a cloud repository. For information about scale-out backup repositories, see the Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> Before you perform the move, make sure that the backup job name, the target backup folder name, the VBM filename, names of VBM files and paths to VBM files meet the following requirements:
>
> - The names contain only allowed alphanumeric characters: a-z, A-Z, 0-9.
> - The names contain only allowed special characters: _ - . + = @ ^.
> - The names of VBM files and paths to VBM files do not contain spaces. If the names or the paths contain spaces, replace them with underscores.

To move locally stored backup files to the cloud repository, the service provider must perform the following steps:

1. Browse to the folder where the cloud repository stores backup files. For example, C:\Backup.

   For more information, see the Configure Backup Repository Settings section in the Veeam Backup & Replication User Guide.

2. In the `C:\Backup` folder, create new folders for each extent of the scale-out backup repository. The folders must be in the following format:
   - [If you work with tenant accounts]
     `C:\Backup\<extent_name>\<tenant_name>\<folder_name>`
   - [If you work with subtenant accounts]
     `C:\Backup\<extent_name>\<tenant_name>\Users\<subtenant_name>\<folder_name>`,

   where:
   - `<extent_name>` — name of the backup repository you use as an extent. For more information, see the Add Performance Extents section in the Veeam Backup & Replication User Guide.
   - `<tenant_name>` — name of the tenant account that you use to connect to the service provider. For more information, see the Tenant Account Credentials section in the Veeam Cloud Connect Guide.
   - `<subtenant_name>` — name of the subtenant account that you use to connect to the service provider. For more information, see the Managing Subtenant Accounts on SP Side section in the Veeam Cloud Connect Guide.
   - `<folder_name>` — name of the target folder to store backups. You can use the name of the original backup job or specify a new name for the folder.

   For example, `C:\Backup\Extent_1\ABC_Company\System_Backup` or `C:\Backup\Extent_1\ABC_Company\Users\John_Smith\System_Backup`.
3. Using external tools, copy the VBM file to both folders created at the step 2.
4. Using external tools, copy the VBK and VIB files to the folders created at the step 2 according to the placement policy specified for the backup repository. For more information, see the Backup File Placement for Performance Tier section in the Veeam Backup & Replication User Guide.

After the service provider moved the backup files to the backup folder, the Veeam Backup Administrator must rescan the cloud repository. To learn how to rescan the repository, see the Rescanning Backup Repositories section in the Veeam Backup & Replication User Guide.

The information about the added backup will be displayed in the rescan job session window.

After the Veeam Backup Administrator rescanned the backup repository, the Veeam Agent user must perform the following steps:

1. Edit the Veeam Agent backup job:
   a. At the **Destination** step of the wizard, target the backup job at the Veeam Cloud Connect Repository.
   b. At the **Service Provider** step of the wizard, specify settings for the cloud gateway to connect to the service provider. For more information, see Specifying Service Provider Settings.
   c. At the **Credentials** step of the wizard, specify settings for the tenant or subtenant account that you want to use to connect to the service provider. For more information, see Specifying User Account Settings.
   d. At the **Backup Resources** step of the wizard, click the **Map backup** link and select the moved backup.
   e. At the **Summary** step of the wizard, click **Finish** to save changes.
2. Run the Veeam Agent backup job. The backup job will continue the backup chain for the full backup that was moved to the cloud repository.