Veeam Agent for Microsoft Windows

Version 2.2

User Guide

July, 2018

> **NOTE:**
>
> Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

About This Document

This user guide provides information about main features of Veeam Agent for Microsoft Windows 2.2.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for Microsoft Windows to protect his/her computer.

Document Revision History

Revision #	Date	Change Summary
Revision 2	7/03/2018	Document revised for Veeam Agent for Microsoft Windows 2.2. Updated sections: System Requirements.
Revision 1	12/19/2017	Initial version of the document for Veeam Agent for Microsoft Windows 2.1.

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 any computer that runs the following OSes:

- Microsoft Windows 7 SP1 or later
- Microsoft Windows 2008 R2 SP1 or later

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, on a Veeam backup repository or Veeam Cloud Connect repository, as well as in Microsoft OneDrive.

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: restore files and disks from backups, manage Veeam Agent backup jobs or backups created with these jobs.

Solution Architecture

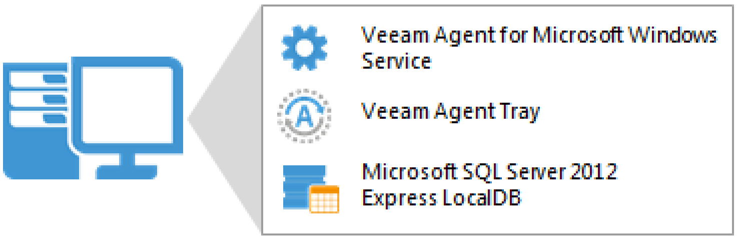
Veeam Agent for Microsoft Windows is set up on a computer whose data you want to protect.

Veeam Agent for Microsoft Windows has a one-service architecture. When you install the product, Veeam Agent for Microsoft Windows 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 for Microsoft Windows uses the Microsoft SQL Server 2012 LocalDB Express. The LocalDB requires only few files to install and takes little resources to run a local on-demand Microsoft SQL Server instance. The LocalDB is executed as a subprocess launched by the Veeam Agent for Microsoft Windows Service. When the Veeam Agent for Microsoft Windows Service is stopped, the LocalDB subprocess is stopped, too.

NOTE:

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


Veeam Agent for Microsoft Windows Service
Veeam Agent Tray
Microsoft SQL Server 2012 Express LocalDB

Data Backup

It is recommended 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.

> **NOTE:**
>
> You cannot currently use Veeam Agent for Microsoft Windows to back up data residing on an external hard drive, USB drive or in a network shared folder.

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
- Backup repository managed by a Veeam backup server
- Cloud repository managed by a Veeam Cloud Connect service provider
- Microsoft OneDrive

Backup Types

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

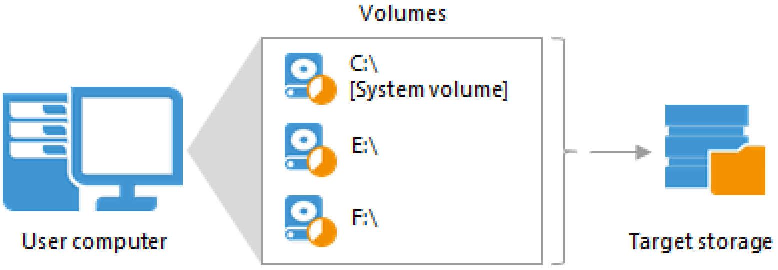
- Volume-level backup
- File-level backup

Volume-Level Backup

You can set up Veeam Agent for Microsoft Windows to create 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.

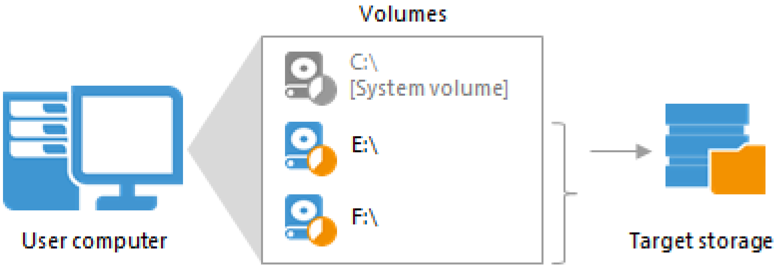
- When you back up the entire computer image, Veeam Agent for Microsoft Windows captures the content of all volumes on your computer. The resulting backup file contains all volume data and Microsoft Windows OS system data: system partition and boot partition. For GPT disks on Microsoft Windows 8, 8.1, 10, 2012 and 2012 R2, Veeam Agent for Microsoft Windows additionally backs up the recovery partition.



- When you back up a specific computer volume, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows will capture only data on the system volume.

  To learn more, see System State Data Backup.

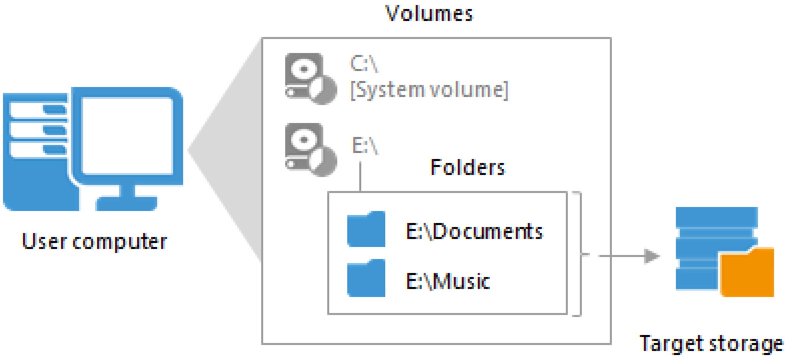


File-Level Backup

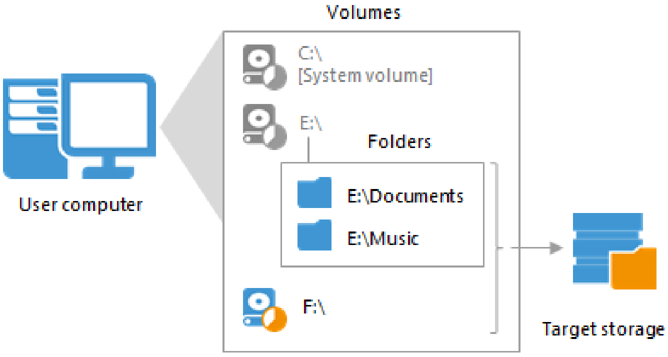
You can set up Veeam Agent for Microsoft Windows to create file-level backup. The file-level backup captures only data of individual folders on the computer. You can use the file-level backup to restore files and folders that you have added to the backup scope.

Veeam Agent for Microsoft Windows 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.

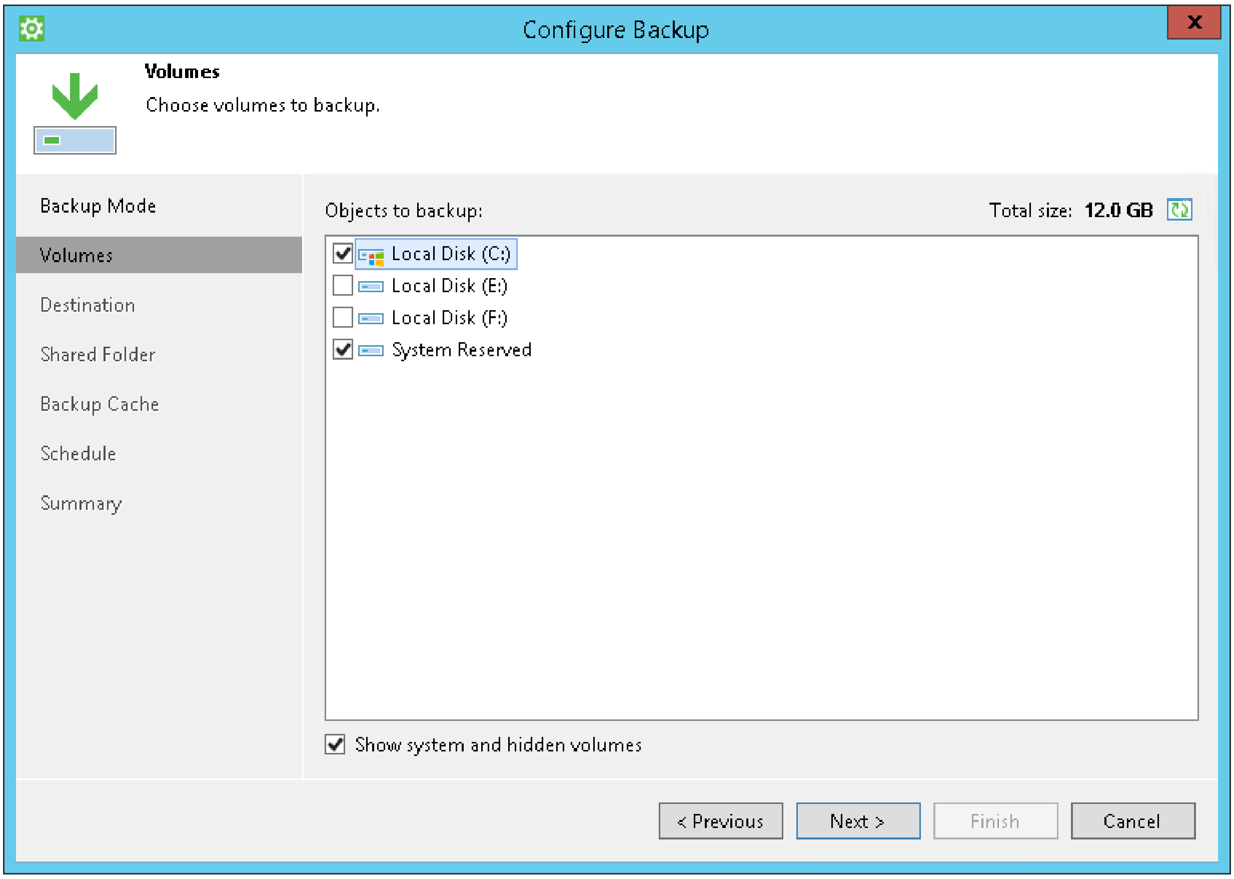


System State Data Backup

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 create such type of backup, you must add the following components to the backup scope:

- Volume-level backup: system volume. When you select to back up the system volume, Veeam Agent for Microsoft Windows automatically includes the System Reserved partition in the backup.



Configure Backup

Volumes

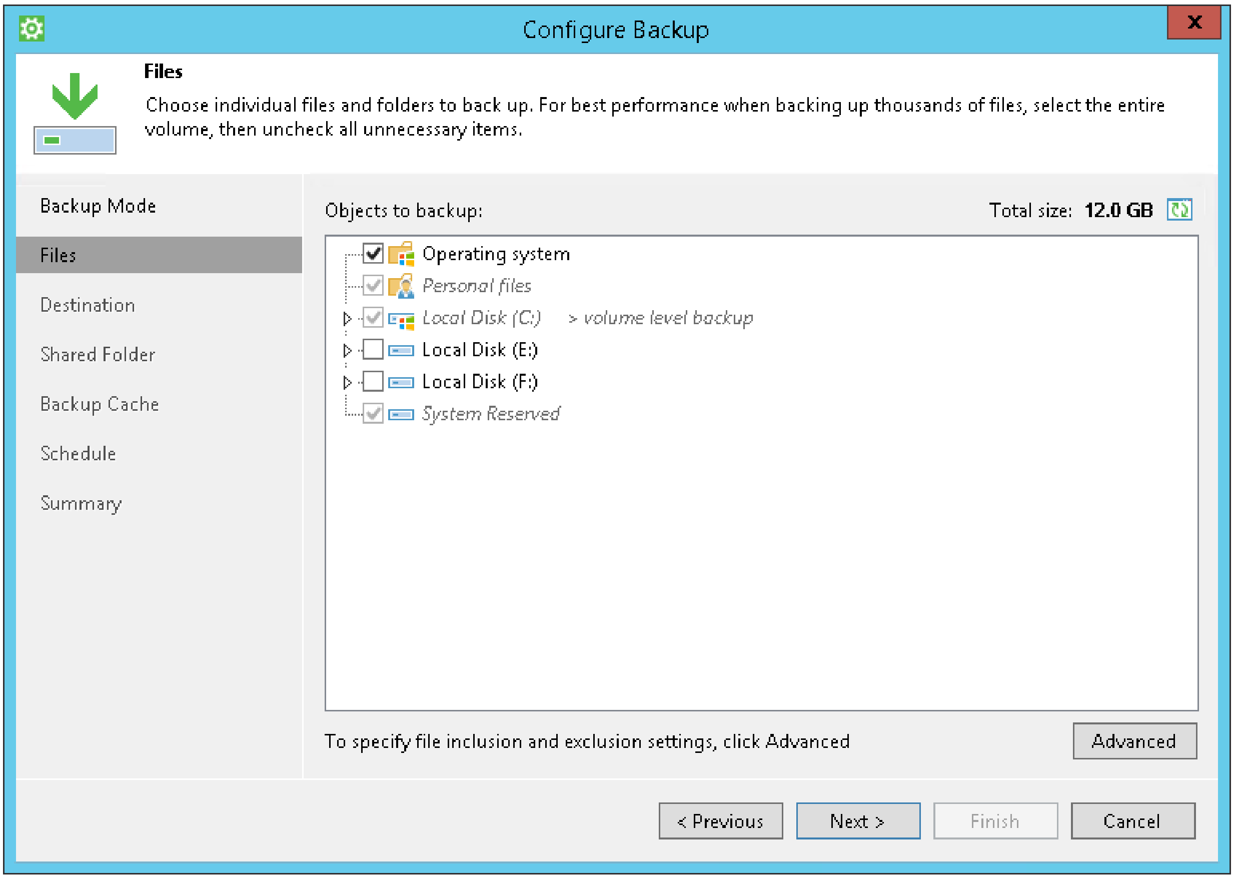
Choose volumes to backup.

Objects to backup: Total size: **12.0 GB**

☑ Local Disk (C:)
☐ Local Disk (E:)
☐ Local Disk (F:)
☑ System Reserved

☑ Show system and hidden volumes

- File-level backup: *Operating system* data. When you select to back up the Operating System data, Veeam Agent for Microsoft Windows automatically includes in the backup all data related to the OS: the system volume, personal files and the System Reserved partition.



Files

Choose individual files and folders to back up. For best performance when backing up thousands of files, select the entire volume, then uncheck all unnecessary items.

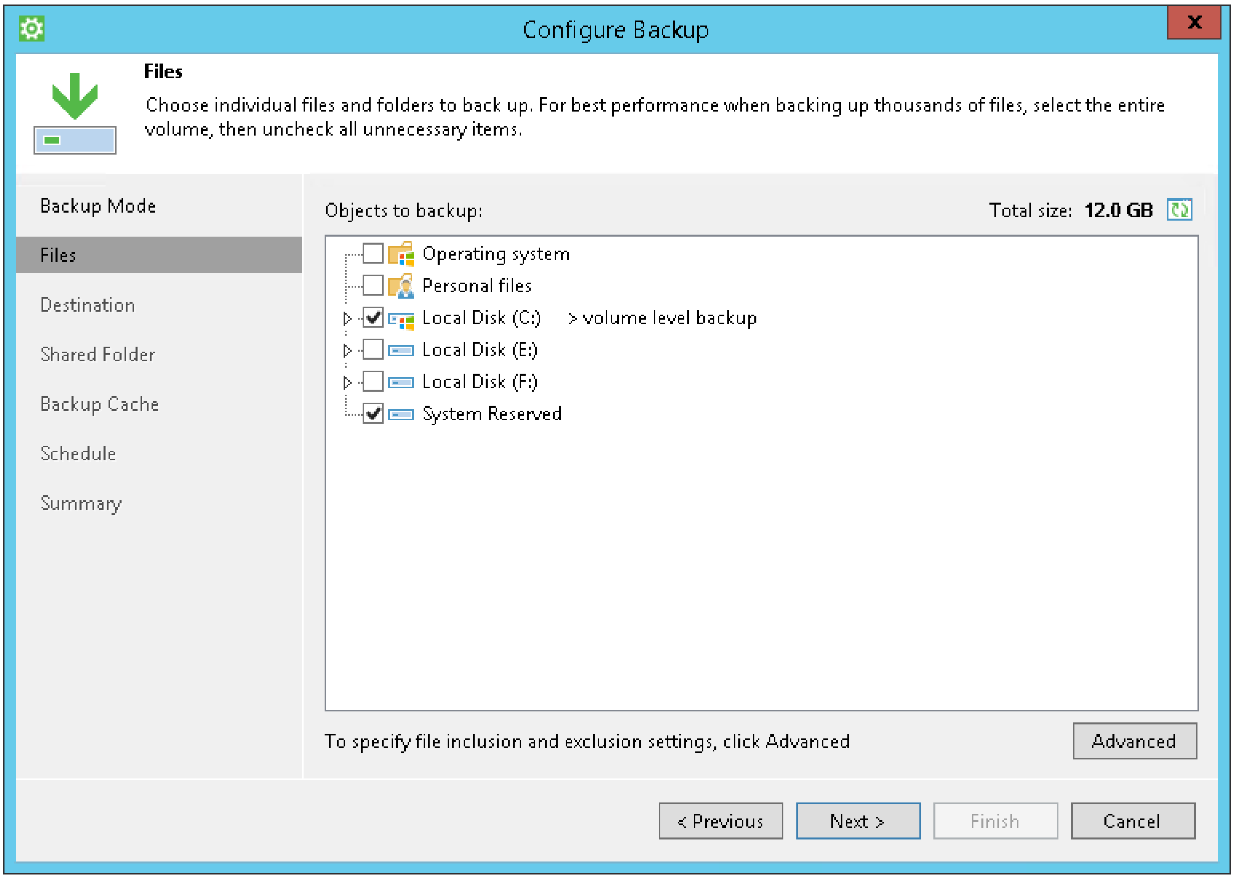
Objects to backup: Total size: **12.0 GB**

- ☑ Operating system
- ☑ *Personal files*
- ☑ *Local Disk (C:)* *> volume level backup*
- □ Local Disk (E:)
- □ Local Disk (F:)
- ☑ *System Reserved*

To specify file inclusion and exclusion settings, click Advanced

Alternatively, you can select to back up the system volume and the System Reserved partition.

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.



Configure Backup

Files

Choose individual files and folders to back up. For best performance when backing up thousands of files, select the entire volume, then uncheck all unnecessary items.

Objects to backup: Total size: **12.0 GB**

- □ Operating system
- □ Personal files
- ☑ Local Disk (C:) > volume level backup
- □ Local Disk (E:)
- □ Local Disk (F:)
- ☑ System Reserved

To specify file inclusion and exclusion settings, click Advanced

How Backup Works

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

1. Veeam Agent for Microsoft Windows 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. On Microsoft Windows Desktop versions, Veeam Agent for Microsoft Windows creates a copy-only VSS snapshot. On Microsoft Windows Server versions, Veeam Agent for Microsoft Windows creates a full VSS snapshot.

   Veeam Agent for Microsoft Windows does not create a VSS snapshot for the EFI system partition on GPT disks as 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:

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.

2. Veeam Agent for Microsoft Windows reads data from the created VSS snapshot, compresses it and copies it to the target location.

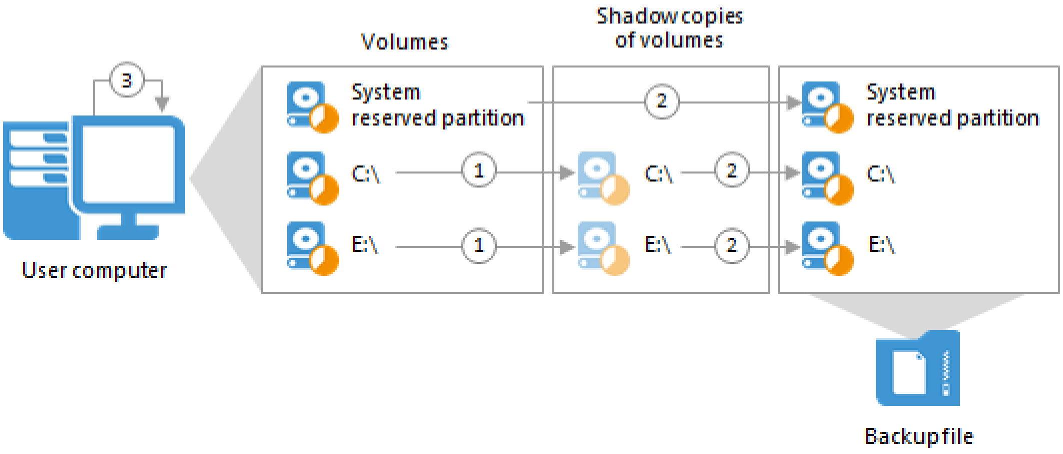
    - For volume-level backup, Veeam Agent for Microsoft Windows copies data blocks of the whole volume.
    - For file-level backup, Veeam Agent for Microsoft Windows creates a volume inside the backup file in the target location. The content of the volume in the backup file is synchronized with the volume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

    During incremental backup, Veeam Agent for Microsoft Windows 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 for Microsoft Windows stores copied data to the backup file.

3. [For Microsoft Windows Server Edition] If an application on the computer uses transaction logs to maintain the database consistency, Veeam Agent for Microsoft Windows automatically truncates transaction logs upon successful backup.

> **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 for Microsoft Windows to automatically truncate transaction logs, you need to manually add the LocalSystem account to a group that has the SQL Server System Administrator rights.



Scheduled 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 and change its settings at any time.

In Veeam Agent for Microsoft Windows, you can configure only one backup job that will process one set of data. For example, if you configure the backup job to perform file-level backup, you will not be able to create volume-level backup in addition to it. Settings of the scheduled backup job apply to ad-hoc backups as well: standalone full backups and incremental backups.

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 Microsoft Windows:

- For 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 for Microsoft Windows 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.

For portable devices, Veeam Agent for Microsoft Windows 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 the backup job fails, Veeam Agent for Microsoft Windows automatically retries the job. In Free and Workstation editions, Veeam Agent for Microsoft Windows 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.

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 for Microsoft Windows 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 for Microsoft Windows will automatically launch the scheduled job to back up your data.

Additionally, you can instruct Veeam Agent for Microsoft Windows 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 for Microsoft Windows will not wait for the next scheduled backup. Instead, Veeam Agent for Microsoft Windows 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 for Microsoft Windows to launch the backup job on specific events. Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows will launch the backup job at the end of the working day, when you lock your computer. In addition, Veeam Agent for Microsoft Windows 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 for Microsoft Windows will perform backup in the following order. At 10:00 PM, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows automatically retries the job every 10 minutes within the next 23 hours.

Veeam Agent for Microsoft Windows does not automatically retry the backup job if the job session is started when the computer is powered on after missed daily backup.

For portable devices, Veeam Agent for Microsoft Windows does not automatically retry the backup job if a device is working on battery.

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.x] 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.

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

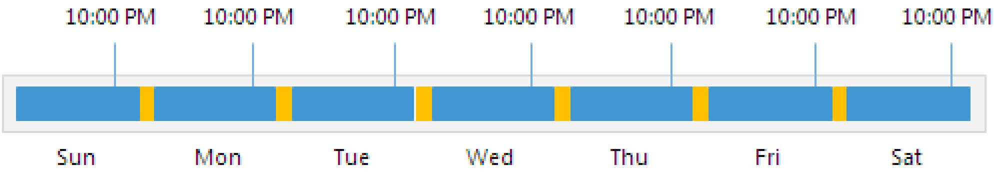
Veeam Agent for Microsoft Windows lets you configure the following scheduling settings for jobs:

- 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.

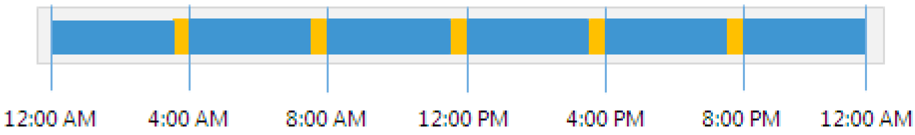
This type of schedule requires that you define the exact time when the job must be started. For example, you can configure the job to start daily at 10:00 PM or every first Sunday of the month at 12:00 AM.



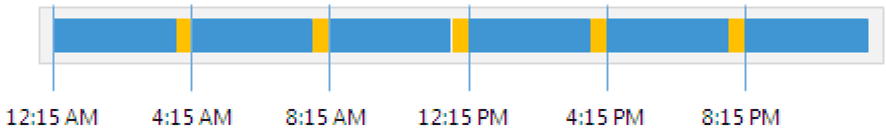
Job Started at Specific Time Intervals

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.

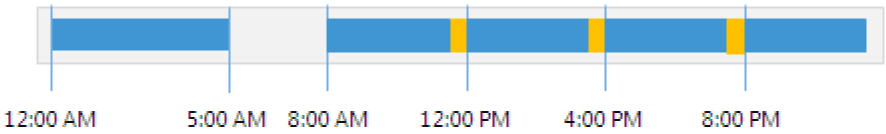
For periodically run jobs, reference time is midnight (12:00 AM). Veeam Agent for Microsoft Windows always starts counting defined intervals from 12:00 AM, and the first job session will start at 12:00 AM. For example, if you configure a job to run with a 4-hour interval, the job will start at 12:00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

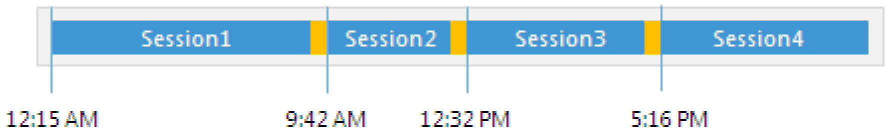


If a session of the periodically run job does not fit into the specified time interval and overlaps the next planned job session, Veeam Agent for Microsoft Windows starts the next backup job session at the nearest scheduled interval. For example, you set up the job to run with a 4-hour interval. The 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 pass 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.

Veeam Agent for Microsoft Windows retries a job only if the previous job session has failed. Veeam Agent for Microsoft Windows does not perform a retry if a job session has finished with the *Success* or *Warning* status.

IMPORTANT!

Veeam Agent for Microsoft Windows does not perform automatic retry for jobs started manually.

Backup Window

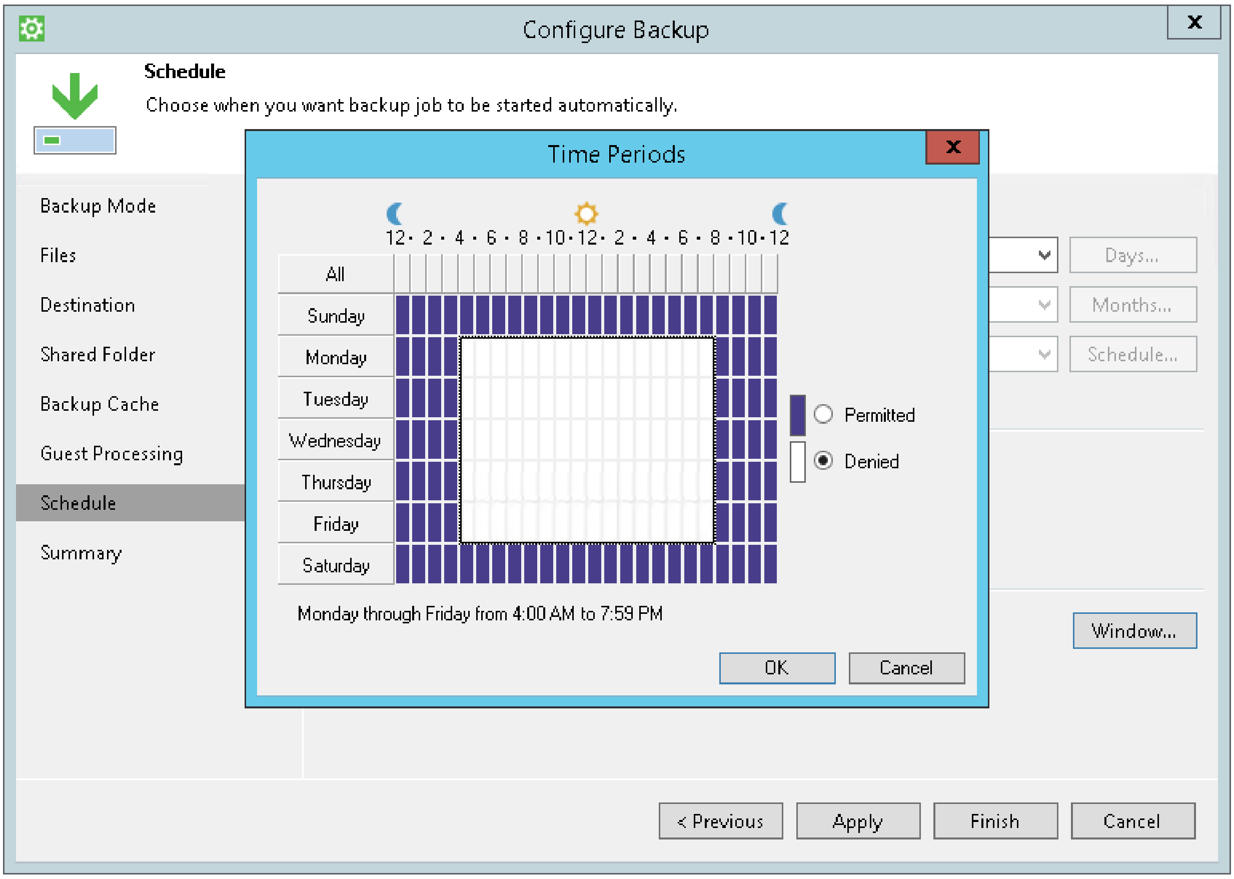
If necessary, you can specify a backup window for the backup job. The backup window is a period of time on week days when the job is permitted to run. If the job exceeds the allowed window, Veeam Agent for Microsoft Windows will automatically terminate it.

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.

IMPORTANT!

Consider the following:

- The backup window affects only the data transport process. Transform operations can be performed on the target location outside the backup window.
- The backup window does not affect the process of uploading backup files from the backup cache to the target storage. If Veeam Agent for Microsoft Windows has created one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent for Microsoft Windows will upload backup files to the target location immediately, regardless of the specified backup window.



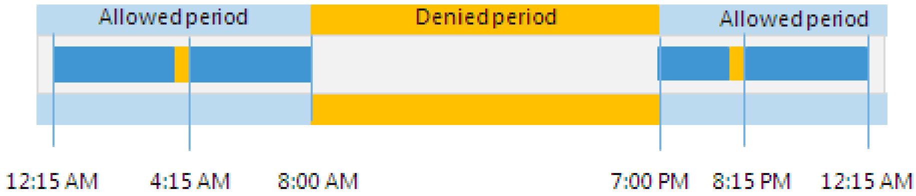
Monday through Friday from 4:00 AM to 7:59 PM

Backup Window for Periodically Run Job

If you define the backup window for the job that runs periodically at specific time intervals, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 as 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.



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.

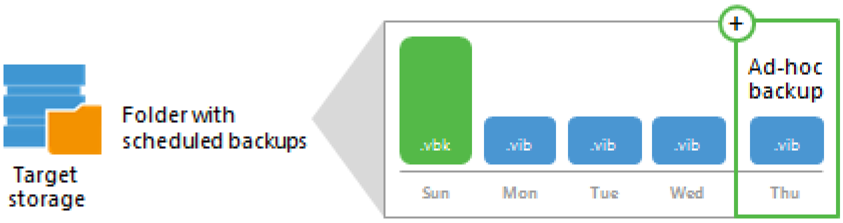
Veeam Agent for Microsoft Windows lets you create the following types of ad-hoc backups:

- 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 scheduled backup job. For example, if you have configured the backup job to perform backup of the 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.



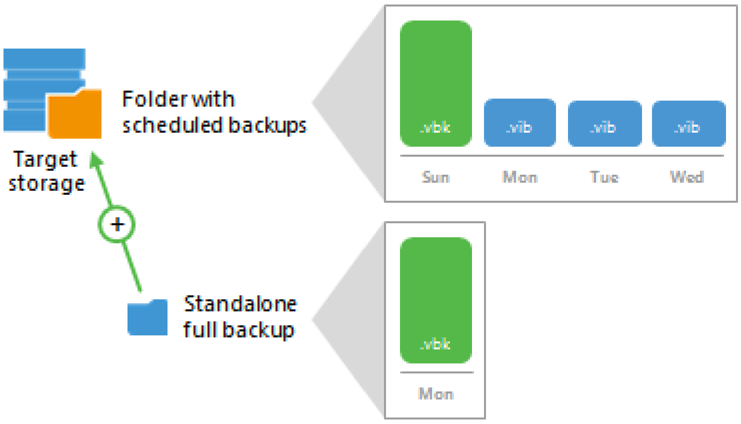
Unlike the scheduled backup job, the ad-hoc incremental backup task is not retried automatically. If the task fails for some reason, you will have to start it manually again.

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, 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 delete it, you must manually remove the full backup file from disk.

NOTE:

You cannot perform standalone full backup if the backup job is targeted at a Veeam Cloud Connect repository or at Microsoft OneDrive.

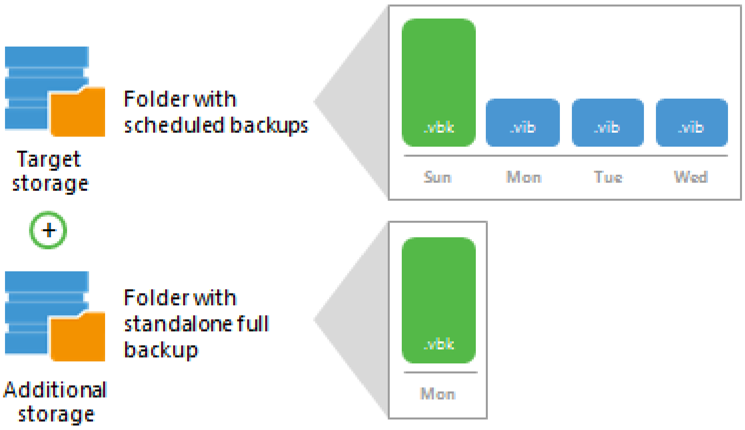
Standalone Full Backup to Another Location

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 one of the following locations:

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

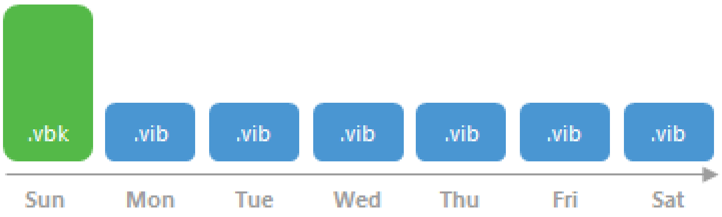
You cannot use a Veeam backup repository, Veeam Cloud Connect repository or Microsoft OneDrive storage as a target for backup to another location.



Backup Chain

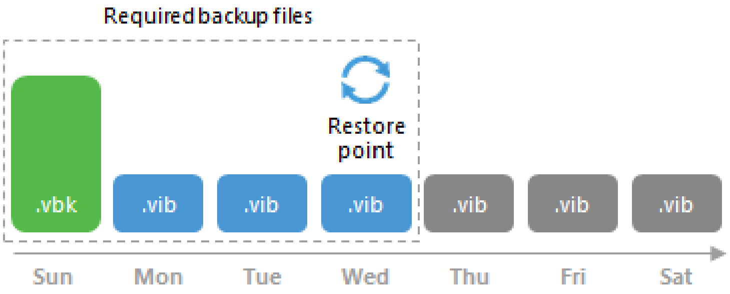
Every backup job session produces a new backup file in the target location. Backup files make up a backup chain. The backup chain can contain files of two types: full backup(s) and incremental backups.

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



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

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



Types of Backup Files

Veeam Agent for Microsoft Windows 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 and VSM files — for Microsoft SQL Server transaction log backups
- VLB and VOM files — for Oracle archived log backups

Backup Retention Policy

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

Backup retention policy depends on the edition of Veeam Agent for Microsoft Windows:

- In 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. To learn more, see Backup Retention Policy in Free and Workstation Editions.

- In the Server edition, Veeam Agent for Microsoft Windows retains the specific number of restore points defined by the user. To learn more, see Backup Retention Policy in Server Edition.

Backup Retention Policy in Free and Workstation Editions

In 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.

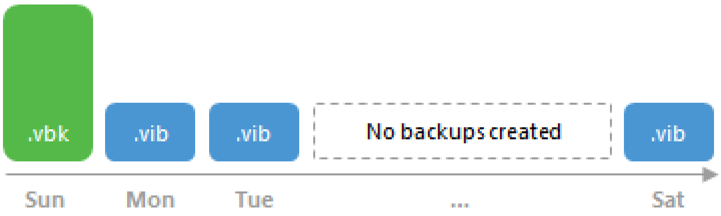
For retention policy settings, Veeam Agent for Microsoft Windows takes into account not calendar days but days on which backup files were successfully created.

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.

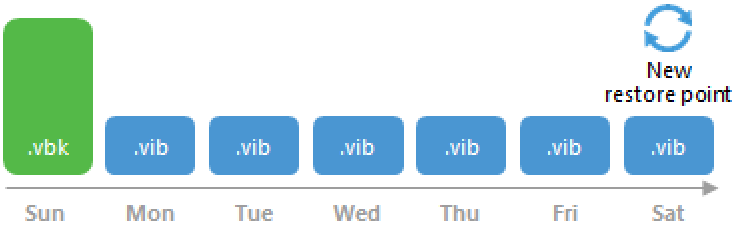
The backup job has successfully run 3 times and created 3 restore points in the backup chain. After that, you have turned off your computer for 10 days. When you turn on your computer, Veeam Agent for Microsoft Windows runs a backup job by schedule and creates a new restore point. The earliest restore 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

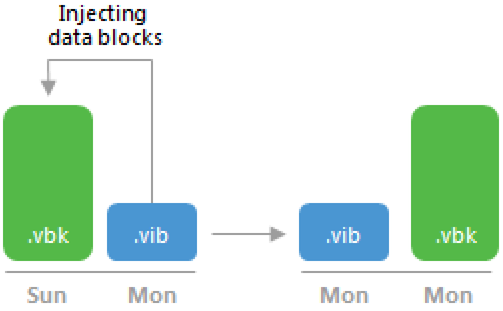
When removing obsolete restore points, Veeam Agent for Microsoft Windows does not simply delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of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

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

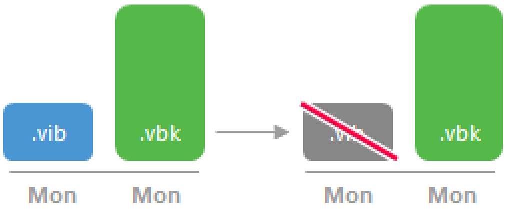


2. If an obsolete restore point exists, Veeam Agent for Microsoft Windows transforms the backup chain. As part of this process, it performs the following operations:

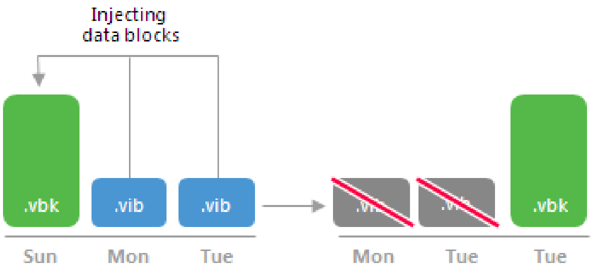
   a. Veeam Agent for Microsoft Windows re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Agent for Microsoft Windows injects into the full backup file data blocks from the earliest incremental backup file in the chain. 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 for Microsoft Windows makes sure that the backup chain is not broken, and you will be able to recover your data to any restore point.

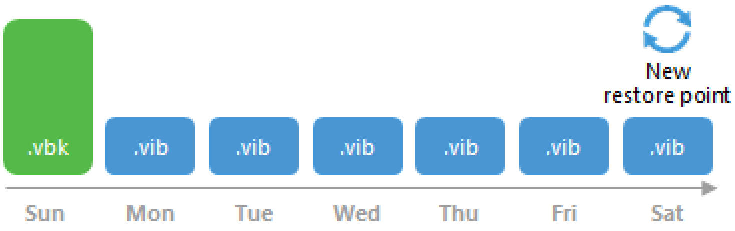


Backup Retention Policy in Server Edition

In the Server edition, Veeam Agent retains the number of latest restore points 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.

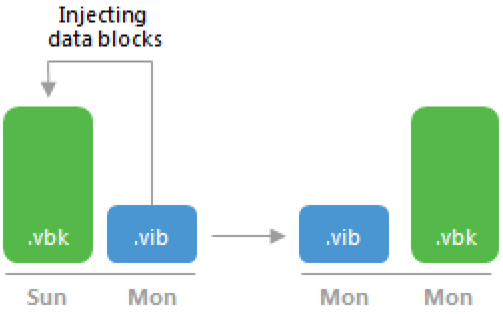
When removing obsolete restore points, Veeam Agent for Microsoft Windows does not simply delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of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

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

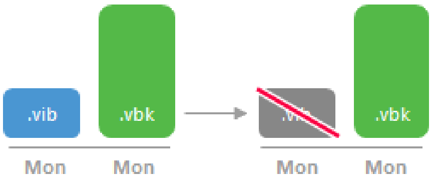


2. If an obsolete restore point exists, Veeam Agent for Microsoft Windows transforms the backup chain. As part of this process, it performs the following operations:

   a. Veeam Agent for Microsoft Windows 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 for Microsoft Windows injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup ‘moves’ forward in the backup chain.



b. The earliest incremental backup file is removed from the chain as redundant: its data has already been injected into the full backup file, and the full backup file includes data of this incremental backup file.

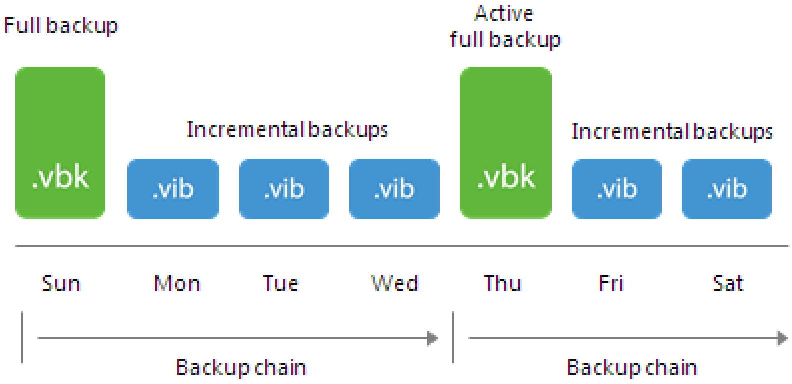


Active Full Backup

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

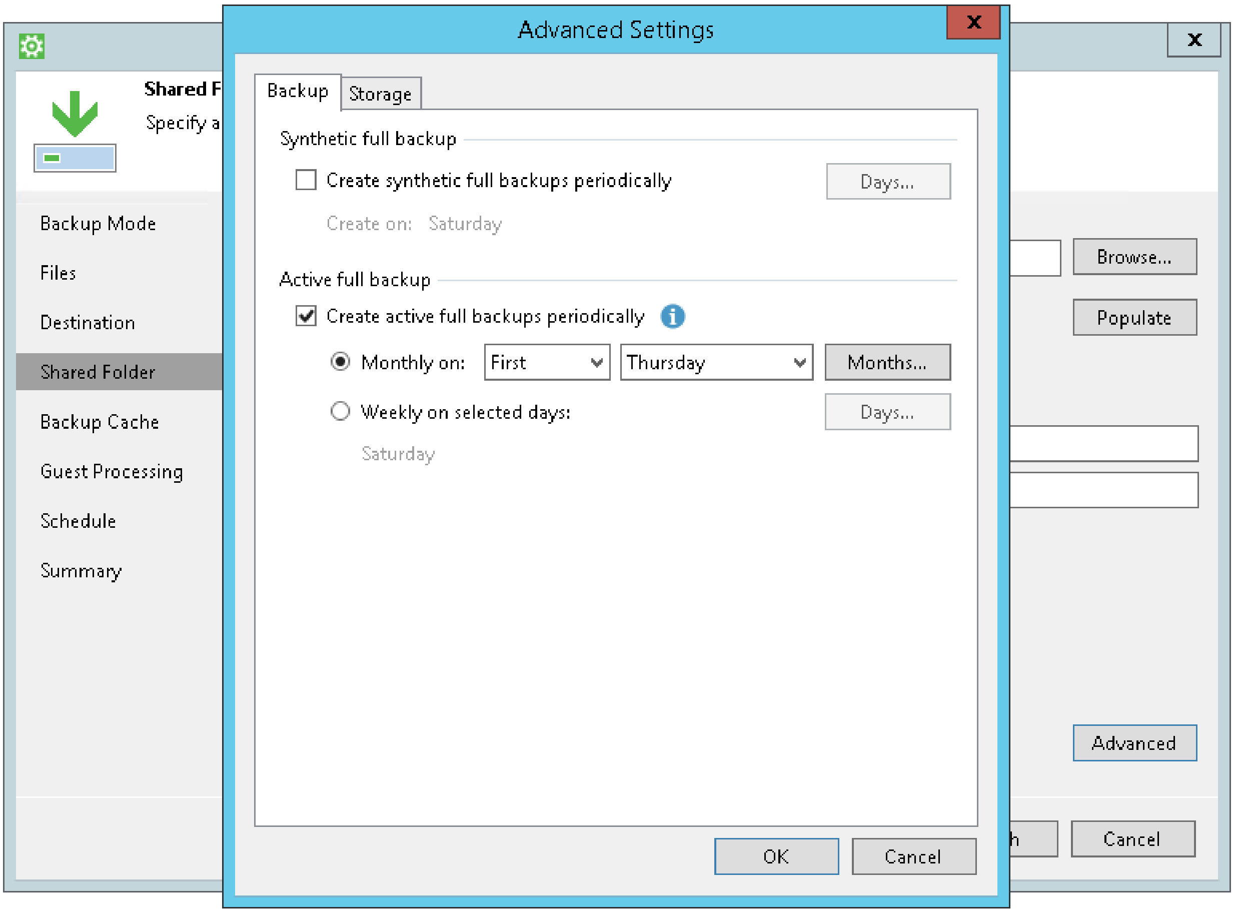
When Veeam Agent for Microsoft Windows performs active full backup, it produces a full backup file and adds this file to the backup chain.

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 for Microsoft Windows automatically deletes the previous backup chain. To learn more, see Retention Policy 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 **Configure Backup** wizard. You can schedule active full backups to run weekly, for example, every Saturday, or monthly, for example, every first Thursday of a month.



Advanced Settings

Backup | Storage

Synthetic full backup

☐ Create synthetic full backups periodically

Create on: Saturday

Active full backup

☑ Create active full backups periodically

● Monthly on: First | Thursday

○ Weekly on selected days:

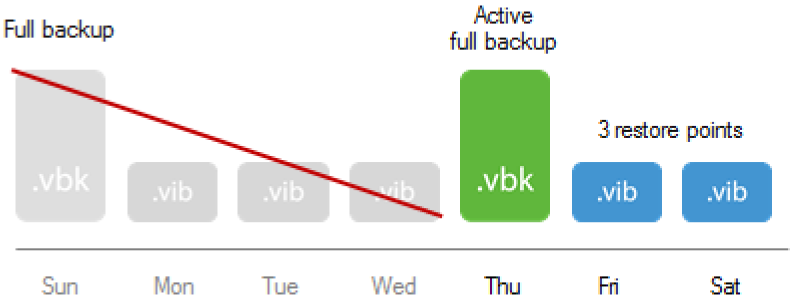
Saturday

Retention Policy for Active Full Backups

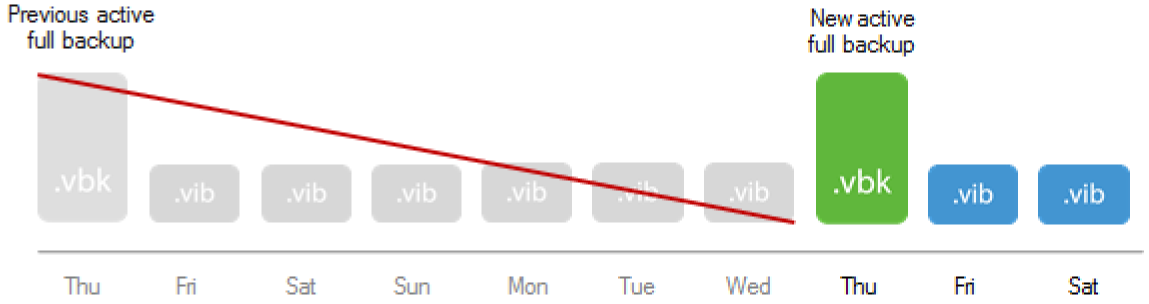
To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental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

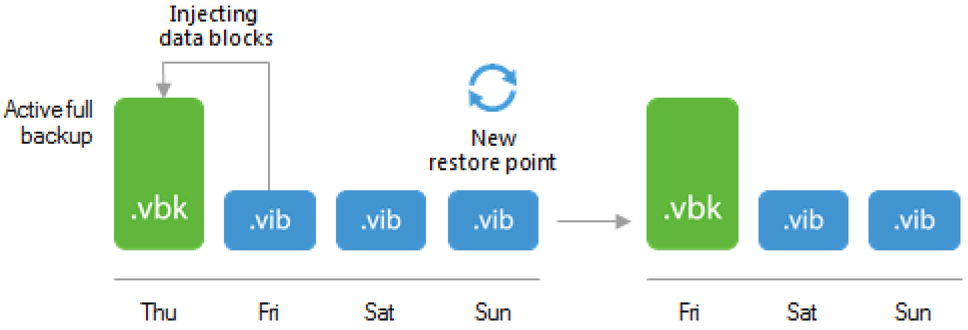
For example, the retention policy is set to 3 restore points. A full backup file is created on Sunday, incremental backup files are created Monday through Saturday, and an active full backup is scheduled on Thursday. Although the retention policy is already breached on Wednesday, the full backup is not deleted. Without the full backup, backup chain would be 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.



Please note that if the backup job is set up to create periodic active 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.



In contrary, in a situation when you manually create a single active full backup, Veeam Agent for Microsoft Windows will treat the active full backup in the same way as a regular full backup. If some restore point becomes obsolete, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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:**
>
> Synthetic full backup functionality is available only in Workstation and Server editions of Veeam Agent for Microsoft Windows.

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 data from the Veeam Agent computer. Instead, it 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, 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 you would have if you created an active full backup.

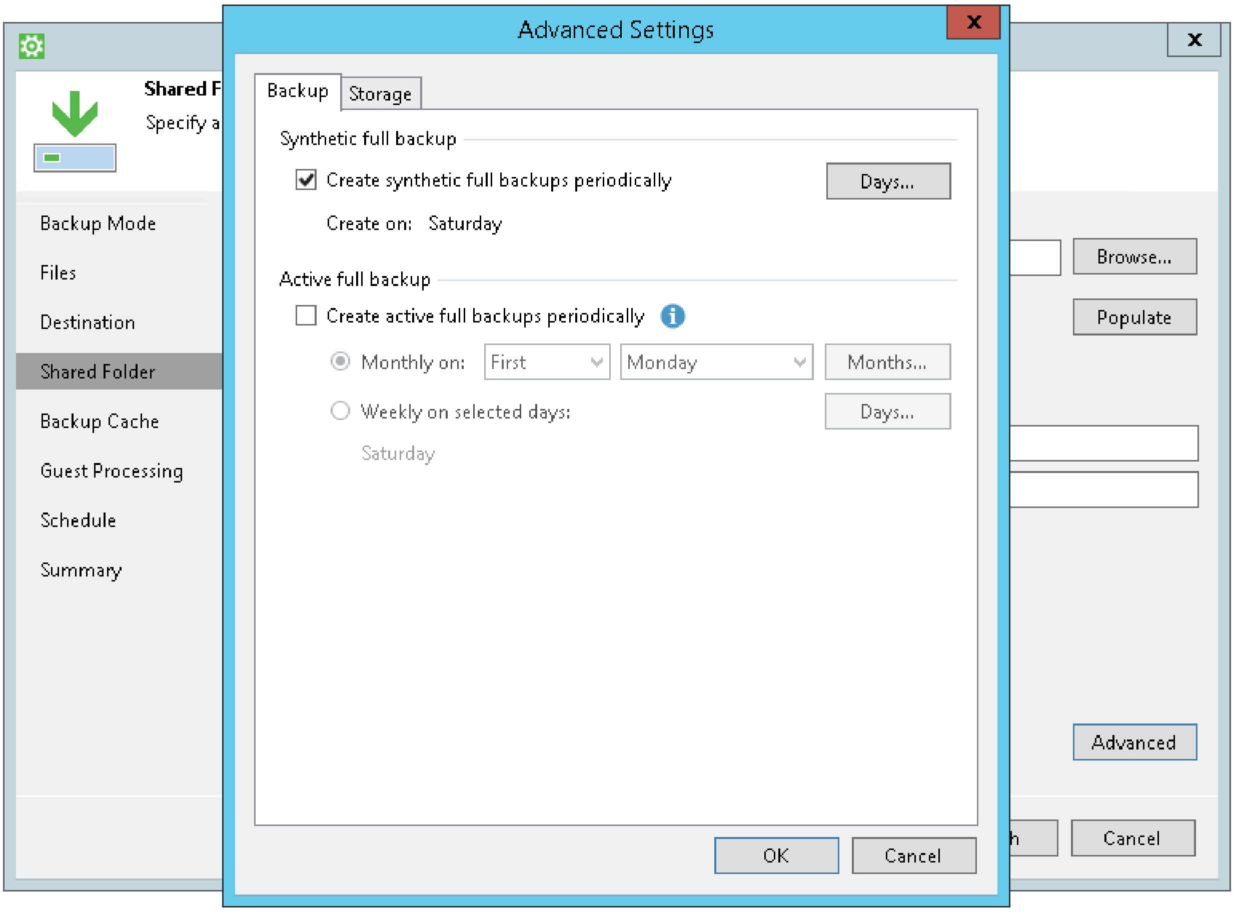
The synthetic full backup has a number of advantages:

- 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.



Advanced Settings

Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

□ Create active full backups periodically

● Monthly on: First Monday

○ Weekly on selected days:

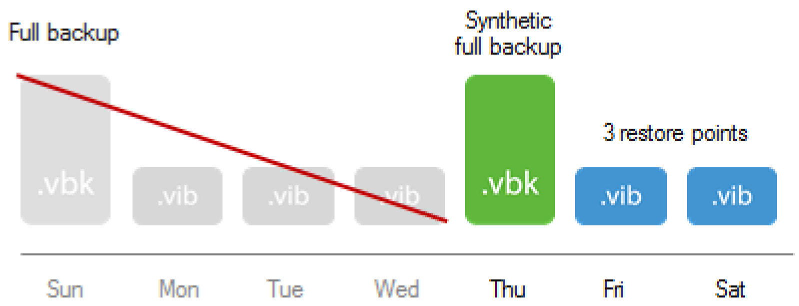
Saturday

Retention Policy for Synthetic Full Backups

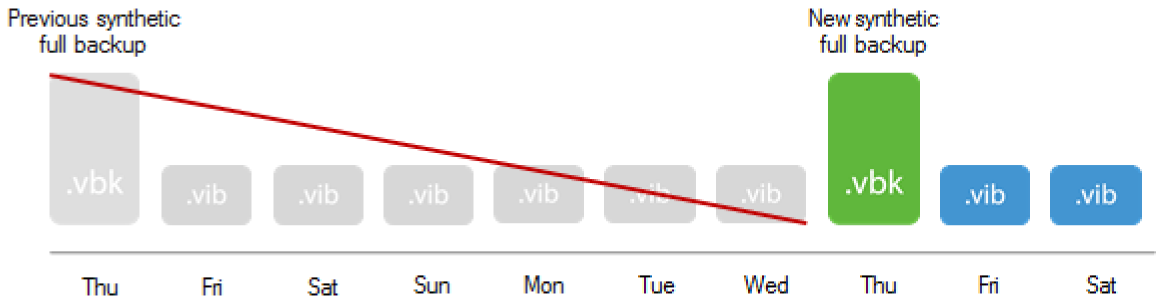
To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental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



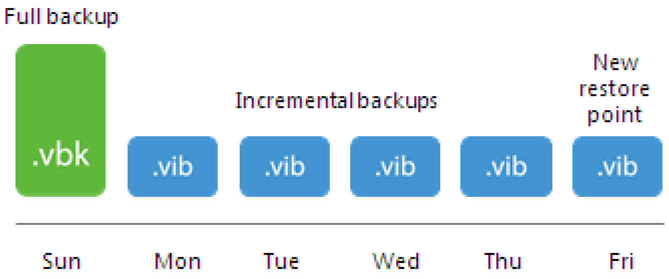
Please note that if the backup job is set up to create synthetic full backups, Veeam Agent for Microsoft Windows will never transform the backup chain. Instead, Veeam Agent for Microsoft Windows will always wait for the next full backup file and the necessary number of incremental backup files to be 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.



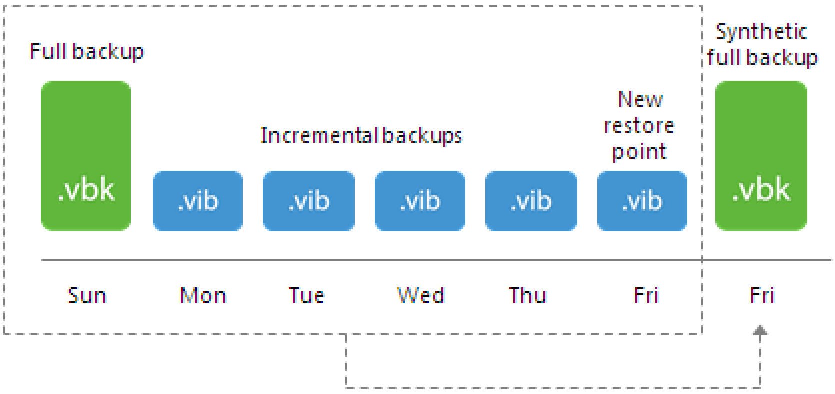
How Synthetic Full Backup Works

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

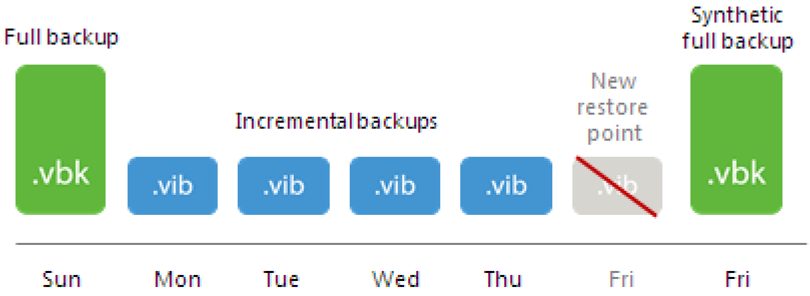
1. On a day when synthetic full backup is scheduled, Veeam Agent for Microsoft Windows triggers a new backup job session. During this session, Veeam Agent for Microsoft Windows first performs incremental backup in a regular manner and adds a new incremental backup file to the backup chain. Incremental 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.

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 functionality is available if the Veeam Agent computer runs a Microsoft Windows Server OS and the Server edition of Veeam Agent for Microsoft Windows. To learn more, see Veeam Changed Block Tracking Driver.

Default Changed Block Tracking Mechanism

By default, Veeam Agent for Microsoft Windows performs changed block tracking in the following way:

1. During the full backup job session, Veeam Agent for Microsoft Windows reads the Master File Table (MFT) of the backed-up volume. Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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.

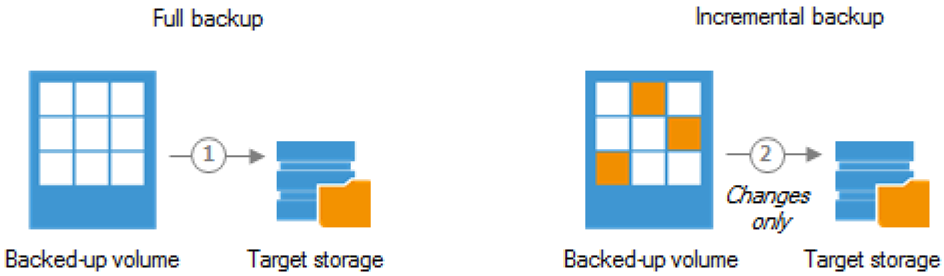
    b. Interacts with the target backup location to obtain digests from the backup file that was created during the previous job session.

    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 for Microsoft Windows cannot calculate information about the changed files, for example, if it fails to retrieve digests from the backup file, Veeam Agent for Microsoft Windows will need to read all data blocks from the VSS snapshot. As a result, the backup window may increase significantly.

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.



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 for Microsoft Windows keep track of changed data blocks in a more efficient way. The driver is intended for servers running applications with large database files.

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

- Run a Microsoft Windows Server OS
- Run the 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, make sure that update KB3033929 is installed in the OS. To learn more, see https://www.microsoft.com/en-us/download/details.aspx?id=46083.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2, 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.

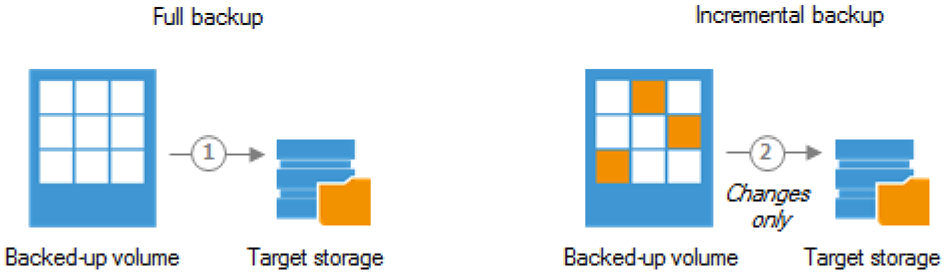
To enable the advanced CBT mechanism provided by the Veeam CBT driver, you need to install the driver in the Veeam Agent for Microsoft Windows control panel. You can perform this operation at any time you need. To activate the driver after installation, Veeam Agent for Microsoft Windows needs to reboot 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:

- NTFS
- FAT
- 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.

> **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 disc. 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 for Microsoft Windows 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 for Microsoft Windows allows you to select one of the following compression levels:

- **None** compression level is recommended if you plan to store backup files on storage devices that support hardware compression and deduplication.
- **Dedupe-friendly** is an 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** is the recommended compression level. It provides the best ratio between size of the backup file and time of the backup procedure.
- **High** compression level provides additional 10% compression ratio over the **Optimal** level at the cost of about 10x higher CPU usage.
- **Extreme** compression 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 for Microsoft Windows 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 **Local target (16 TB + backup files)** 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. Note, however, that this storage optimization option will provide the largest size of incremental backup files.

- The **Local target** option is recommended for backup to SAN, DAS or local storage. With this option selected, Veeam Agent for Microsoft Windows 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 **LAN target** option is recommended for backup to NAS and onsite backup. With this option selected, Veeam Agent for Microsoft Windows uses data block size of 512 KB. This option reduces the size of an incremental backup file because of reduced data block sizes.
- The **WAN target** option is recommended if you are planning to use WAN for offsite backup. With this option selected, Veeam Agent for Microsoft Windows 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:**
>
> Because of Microsoft OneDrive limitations, a larger number of backed-up data blocks results in lower write speed on a Microsoft OneDrive storage. As a result, it is not recommended to use data block size of less than 1024 KB for the backup job targeted at Microsoft OneDrive (as long as your network connection bandwidth allows you to transfer larger amounts of incremental backup data over the internet).

To apply new storage optimization settings, you must create an active full backup after you change storage optimization settings. Veeam Agent for Microsoft Windows will use the new block size for the active full backup and subsequent backup files in the backup chain.

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 logs 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, refer to the Veeam Backup Enterprise Manager User Guide at: https://www.veeam.com/documentation-guides-datasheets.html.

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 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 2003.
Microsoft Exchange	The following versions of Microsoft Exchange are supported: ▪ Microsoft Exchange 2016 ▪ Microsoft Exchange 2013 SP1 ▪ Microsoft Exchange 2013 ▪ Microsoft Exchange 2010 SP1, SP2, or SP3
Microsoft SharePoint	The following versions of Microsoft SharePoint are supported: ▪ Microsoft SharePoint 2016 ▪ Microsoft SharePoint 2013 ▪ Microsoft SharePoint 2010 All editions are supported (Foundation, Standard, Enterprise
Microsoft SQL Server	The following versions of Microsoft SQL Server are supported: ▪ 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 ▪ Microsoft SQL Server 2005 SP4 All editions of Microsoft SQL Server except LocalDB are supported.

Oracle	Oracle Database 11g and 12c are supported for the following operating systems (32-bit and 64-bit architecture): • 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. ▪ Current version does not support creating transactionally-consistent backups of a standby database in case you are using Oracle Active Data Guard; only crash-consistent backups can be created in this case. However, a primary database can be backed up in a transactionally-consistent way. ▪ 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 for Microsoft Windows creates a Microsoft VSS snapshot and starts copying backed up data to the target location. For more information about Microsoft VSS, see https://technet.microsoft.com/en-us/library/cc785914(v=ws.10).aspx.

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

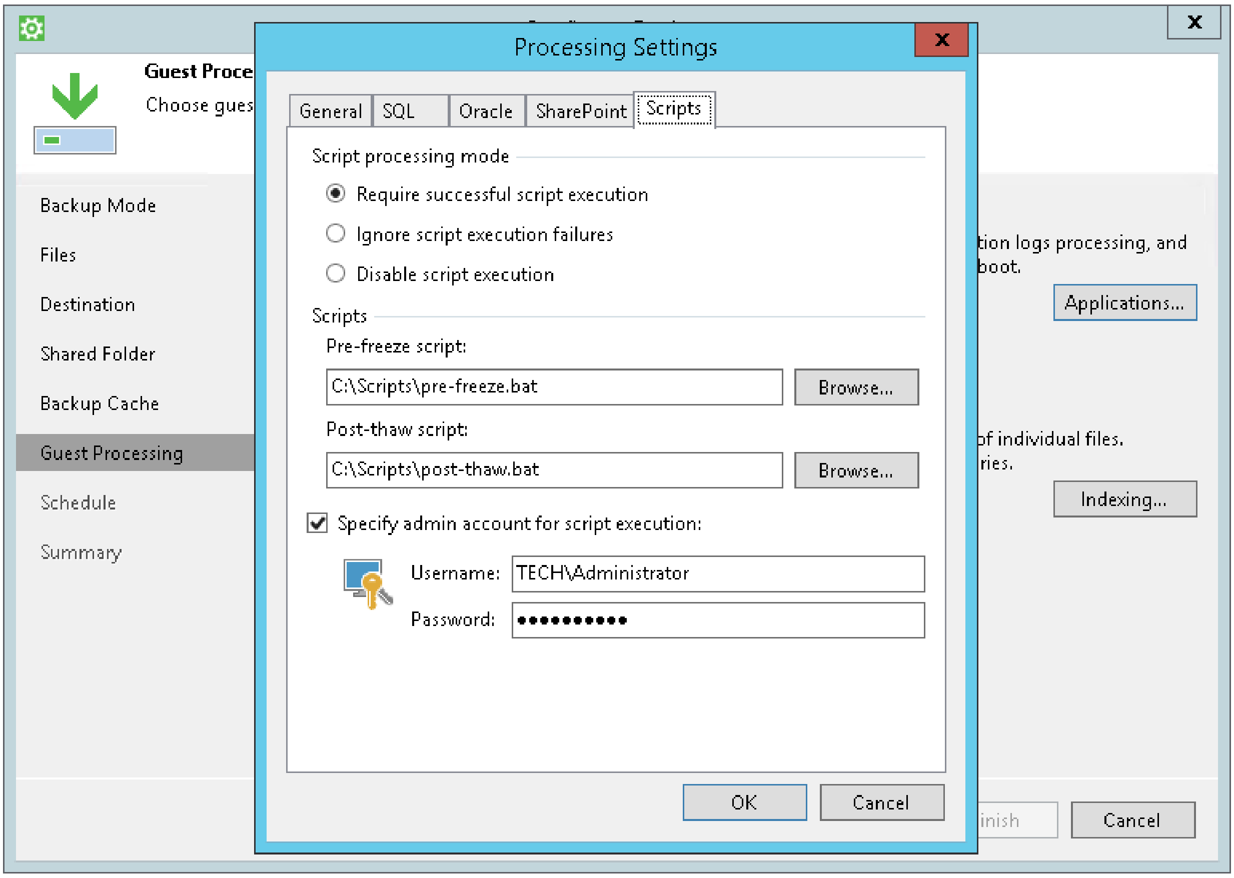
If Veeam Agent computer runs applications that do not support Microsoft VSS, you can instruct Veeam Agent for Microsoft Windows to run custom scripts during the backup job session. For example, the pre-freeze script may quiesce the file system and application data to bring the computer OS to a consistent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



Script processing mode

● Require successful script execution

○ Ignore script execution failures

○ Disable script execution

Scripts

Pre-freeze script: C:\Scripts\pre-freeze.bat

Post-thaw script: C:\Scripts\post-thaw.bat

☑ Specify admin account for script execution:

Username: TECH\Administrator

Password: ●●●●●●●●●●●

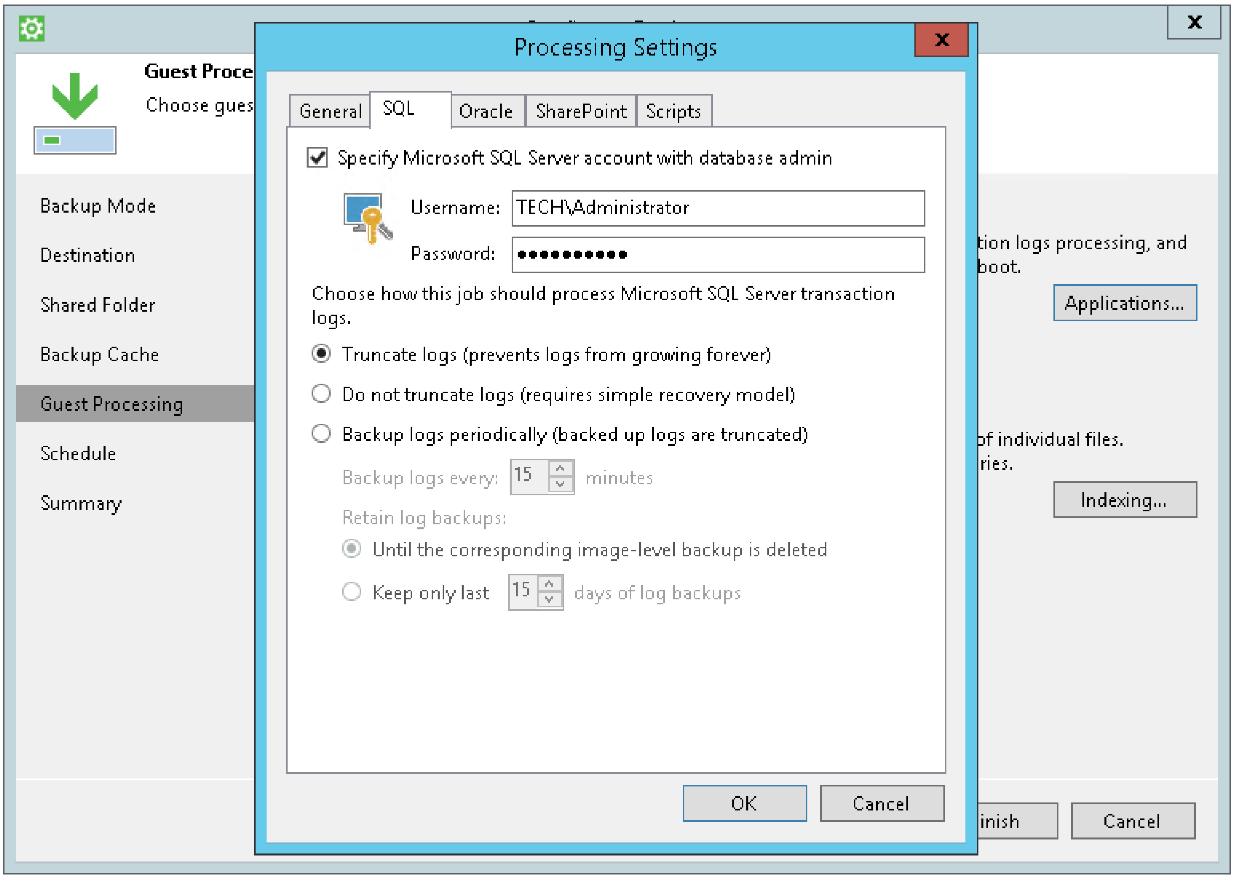
Limitations for Pre-Freeze and Post-Thaw Scripts

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 terminates the job.

Transaction Log Truncation

If you back up or replicate 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



Processing Settings

General | SQL | Oracle | SharePoint | Scripts

☑ Specify Microsoft SQL Server account with database admin

Username: TECH\Administrator

Password: ●●●●●●●●●●●

Choose how this job should process Microsoft SQL Server transaction logs.

● Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

○ Backup logs periodically (backed up logs are truncated)

Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

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. This option is recommended if together with Veeam Agent for Microsoft Windows you use another backup tool.

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

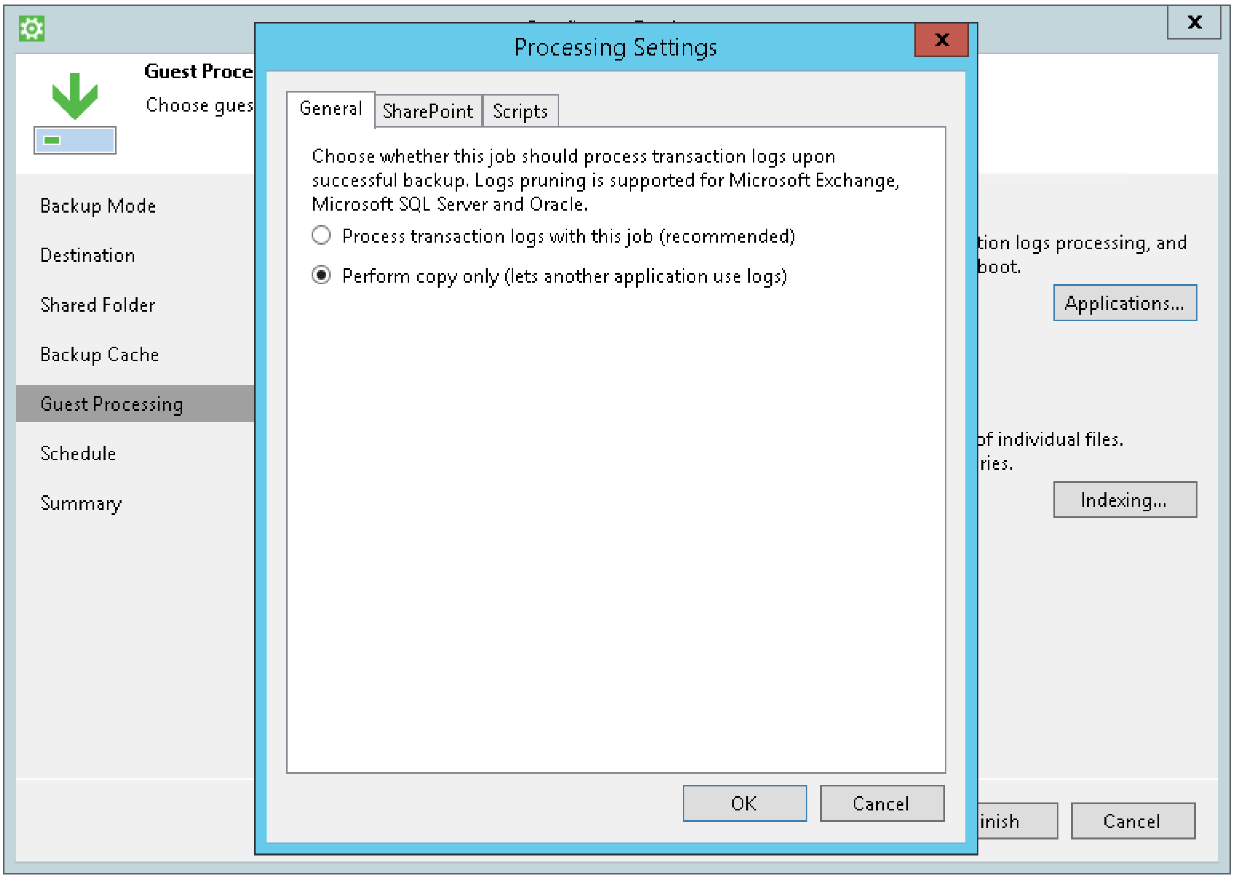
Some organizations prefer to back up Microsoft SQL Server databases and transaction logs with native Microsoft SQL Server tools or 3rd party backup tools. To restore database systems in a proper way, database administrators must be sure that they have database backups and a sequence of transaction log 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). Veeam Agent for Microsoft Windows backs up data on a machine that runs Microsoft SQL Server using the *VSS_BT_COPY* method for VSS snapshot creation. The *VSS_BT_COPY* method produces a copy-only backup — the backup that is independent of the existing chain of database backups. The copy-only backup does not influence the backup history — it does not change the last database modification date and time for the database (unlike non-copy only backups).

IMPORTANT!

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.



Processing Settings

General | SharePoint | Scripts

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server and Oracle.

○ Process transaction logs with this job (recommended)

● Perform copy only (lets another application use logs)

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, refer to the Veeam Backup & Replication documentation at: https://www.veeam.com/documentation-guides-datasheets.html.

Microsoft SQL Server Logs 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 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 http://msdn.microsoft.com/en-us/library/ms189275.aspx.

Oracle Logs 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. This mode is not recommended as it does not provide for proper disaster recovery.

With ARCHIVELOG turned on, the Oracle system stores database archived logs to 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 **Configure Backup** wizard — you can specify how logs should be backed up and/or truncated for Oracle databases.

Requirements for Oracle Archived Log Backup

- Veeam Agent for Microsoft Windows supports archived logs 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 logs 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 **Configure Backup** 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 for Microsoft Windows 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.

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, and/or when this parent backup job is disabled.

How Microsoft SQL Server Logs Backup Works

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

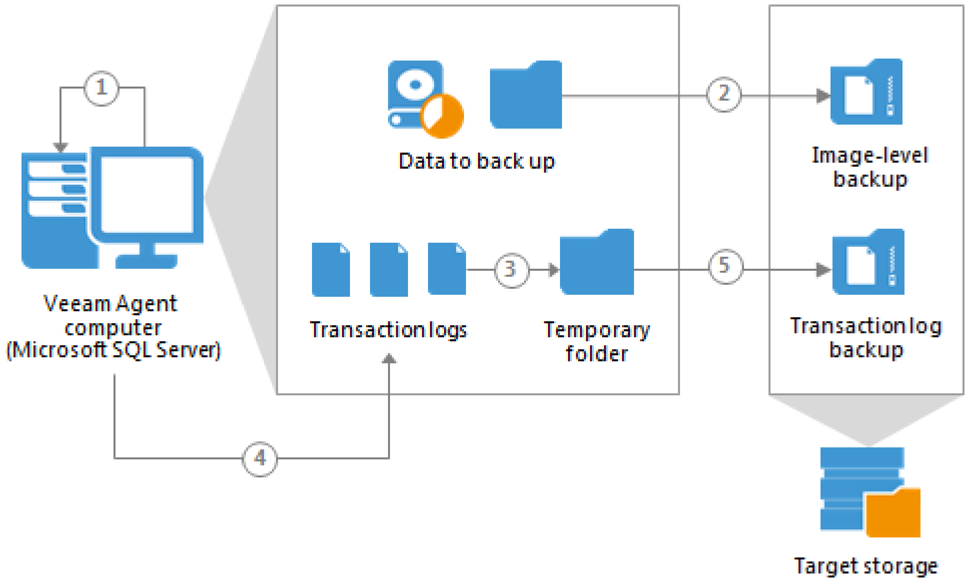
1. Veeam Agent for Microsoft Windows launches the parent backup job by schedule.
2. The parent backup job creates a volume-level or file-level backup and stores it to the backup location.
3. A new session of the transaction log backup job starts. Veeam Agent for Microsoft Windows copies transaction log 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.

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

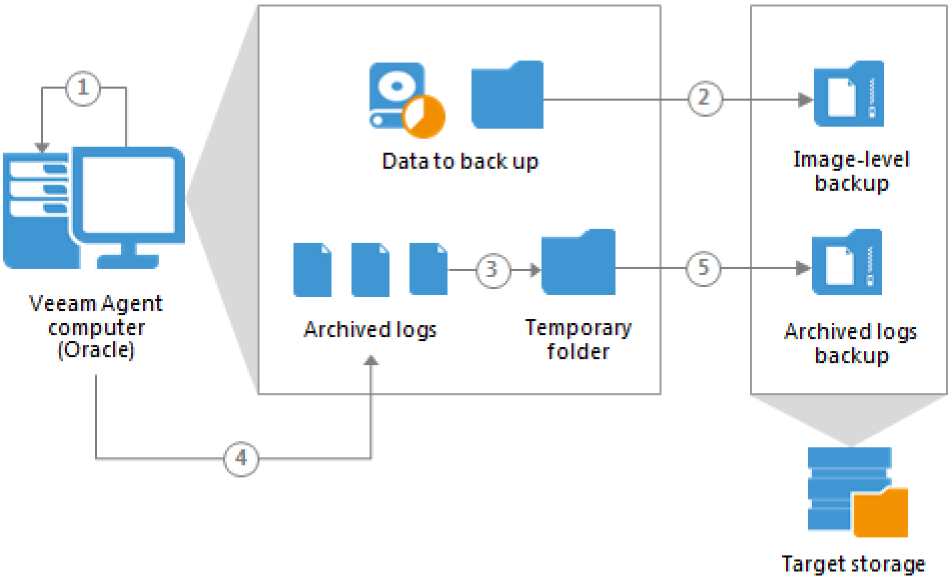
The archived logs backup for Oracle is performed in the following way:

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.

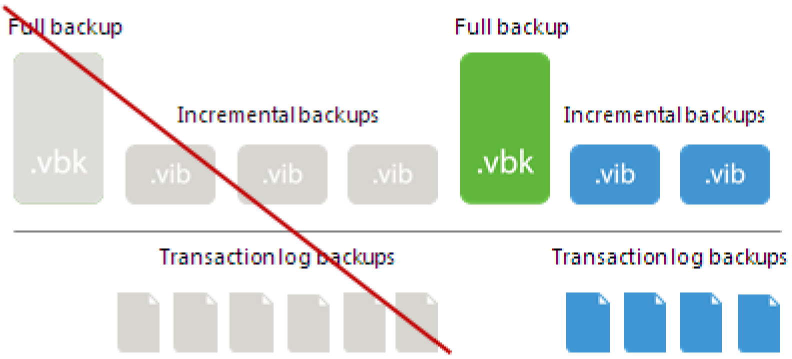
Veeam Agent for Microsoft Windows removes transaction log backups by retention. You can choose one of the following retention methods:

- 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.

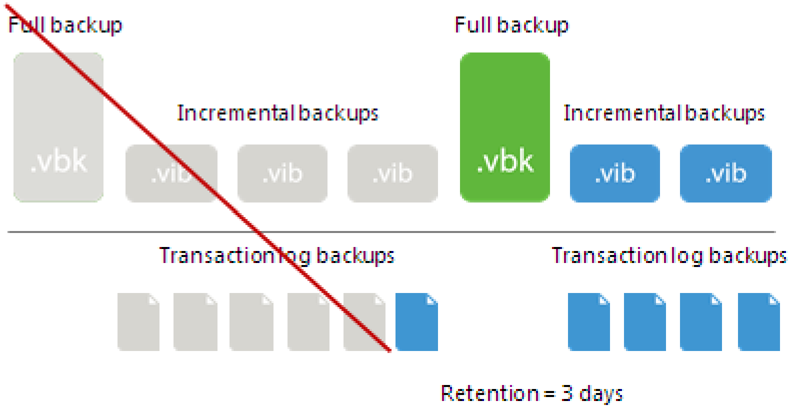
This method allows you to have both the file-level or volume-level backup and necessary transaction log backups at hand. If you need to recover a database to some state, you can restore a machine running Microsoft SQL Server or Oracle from the necessary restore point and perform transaction log replay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

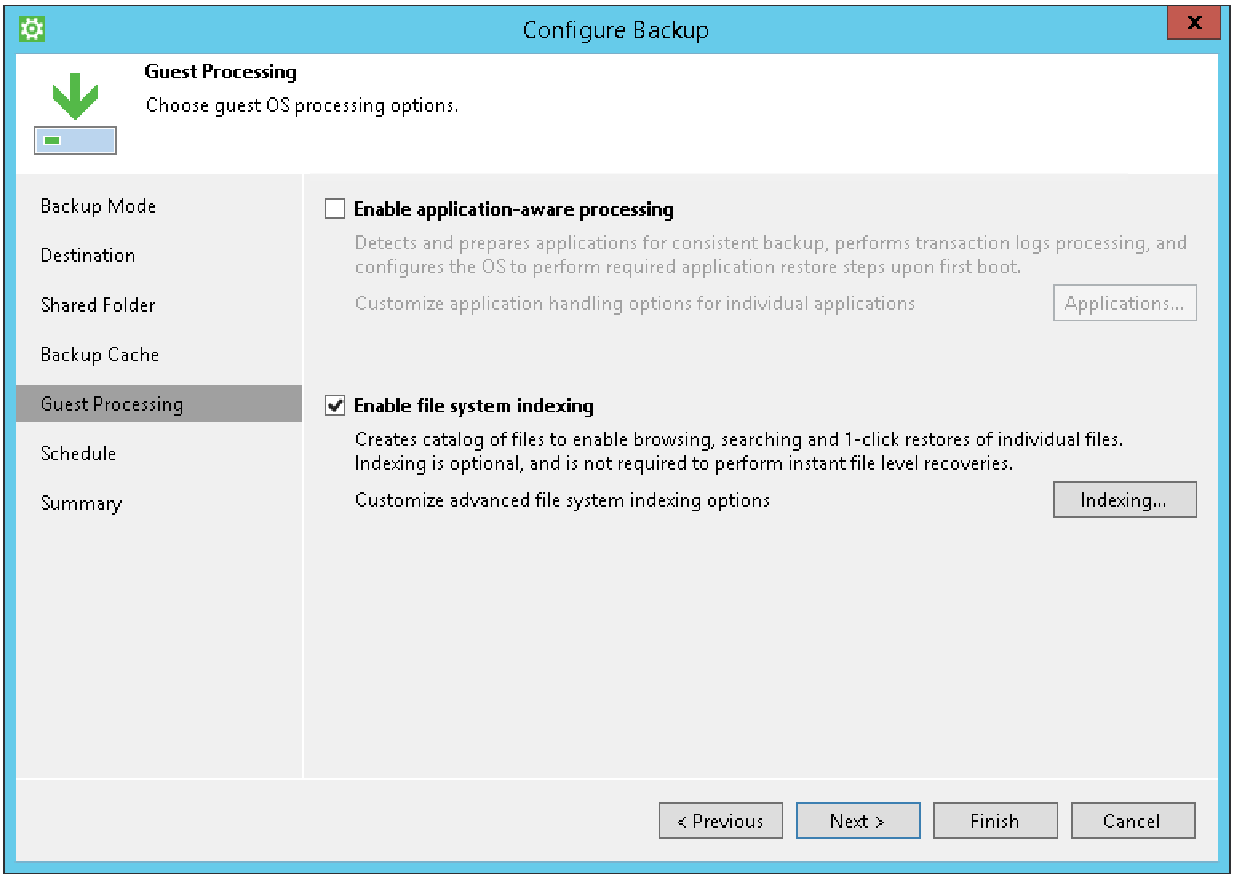
If you select this retention method, you must make sure that retention policies for the Veeam Agent backup and transaction log backup are consistent. The restore point of the volume-level or file-level backup must always be preserved. If a backup of the database itself is missing, you will not be able 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 at: https://www.veeam.com/documentation-guides-datasheets.html.



Guest Processing

Choose guest OS processing options.

□ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual applications

☑ **Enable file system indexing**

Creates catalog of files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced file system indexing options

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.

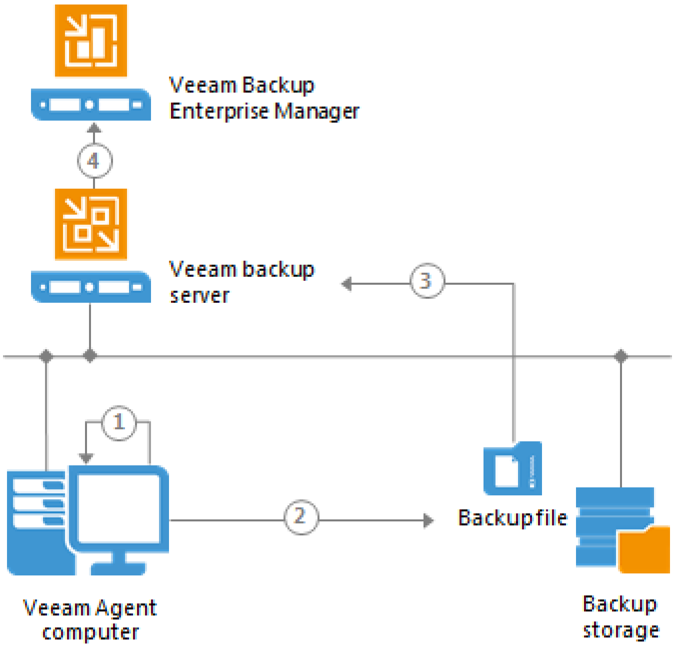
2. When file indexing is complete, Veeam Agent for Microsoft Windows collects indexing data, writes it to an archive file and stores this archive file to the backup file along with the backed-up data.

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 at: https://www.veeam.com/documentation-guides-datasheets.html.

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:**
>
> 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.



Data Encryption

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

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

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

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

To create encrypted backups, you must enable the **Enable backup file encryption** option and specify a password that will be used for data encryption.

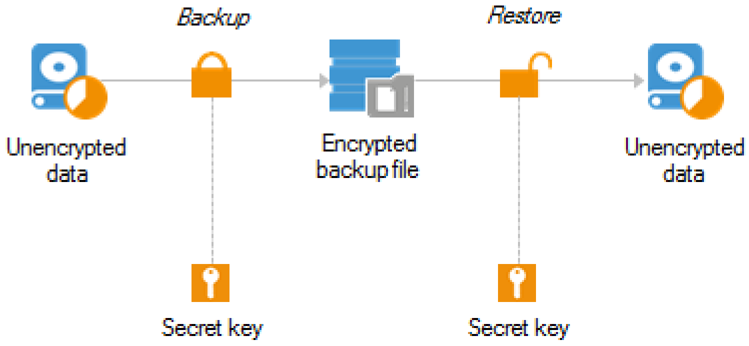
NOTE:

You cannot enable encryption options in the properties of the Veeam Agent backup job if you have chosen to create Veeam Agent backups on 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 at https://www.veeam.com/documentation-guides-datasheets.html.

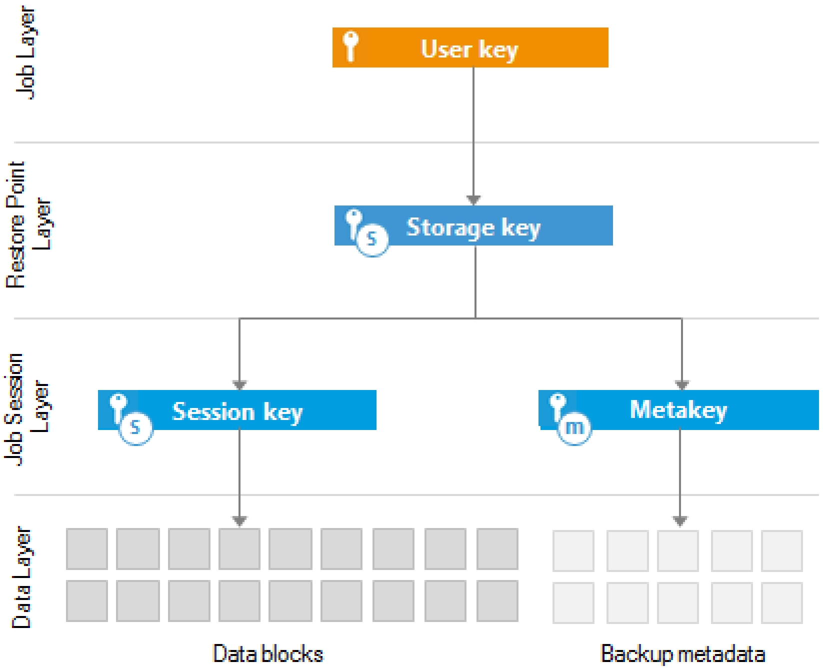
Encryption Algorithms

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

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



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



Encryption Keys

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

Veeam Agent for Microsoft Windows uses 4 types of keys:

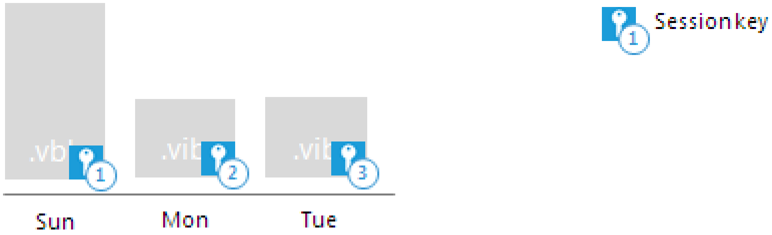
- 3 service keys generated by Veeam Agent for Microsoft Windows:
    - Session key
    - Metakey
    - Storage key
- 1 key generated based on a user password: a user key.

Session Keys and Metakeys

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

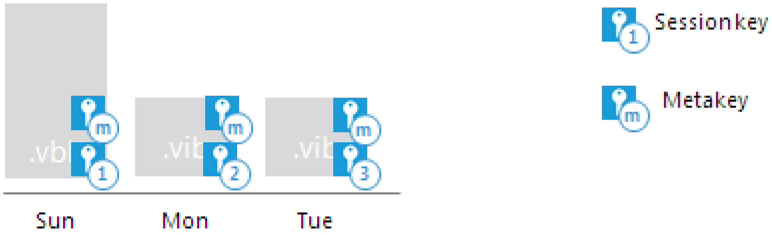
Veeam Agent for Microsoft Windows generates a new session key for every backup job session. For example, if you have created an encrypted backup job and run 3 job sessions, Veeam Agent for Microsoft Windows will produce 3 backup files that will be encrypted with 3 different session keys:

- 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 for Microsoft Windows applies a separate key — metakey. Use of a metakey for metadata raises the security level of encrypted backups.

For every job session, Veeam Agent for Microsoft Windows generates a new metakey. For example, if you have run 3 job sessions, Veeam Agent for Microsoft Windows will encrypt metadata with 3 metakeys.

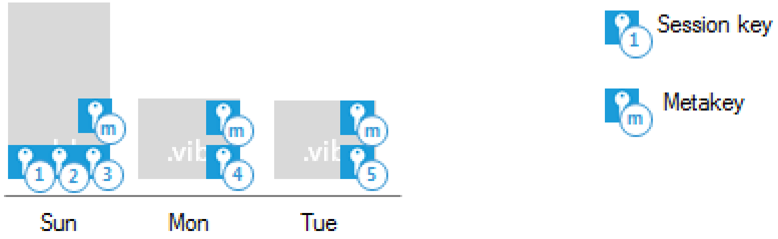


In the encryption process, session keys and metakeys are encrypted with keys of a higher layer — storage keys. Cryptograms of session keys and metakeys are stored to the resulting file next to encrypted data blocks. Metakeys are additionally kept in the Veeam Agent for Microsoft Windows database.

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 for Microsoft Windows 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.

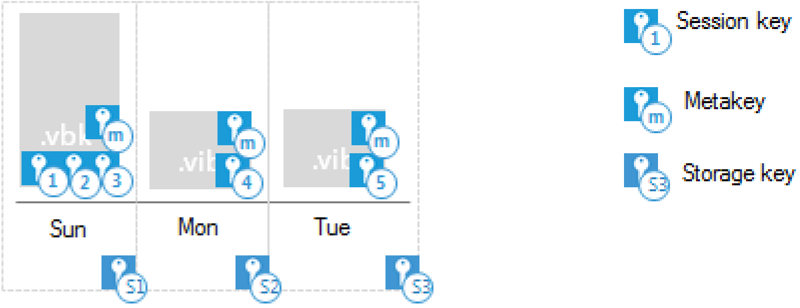
To restore data from such “composed” backup file, Veeam Agent for Microsoft Windows would require a bunch of session keys. For example, if the backup chain contains restore points for 2 months, Veeam Agent for Microsoft Windows would have to keep session keys for a 2-month period.



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

For storage keys, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows does not need to keep the session keys history in the Veeam Agent for Microsoft Windows database. Instead, it requires only one storage key to restore data from one file.

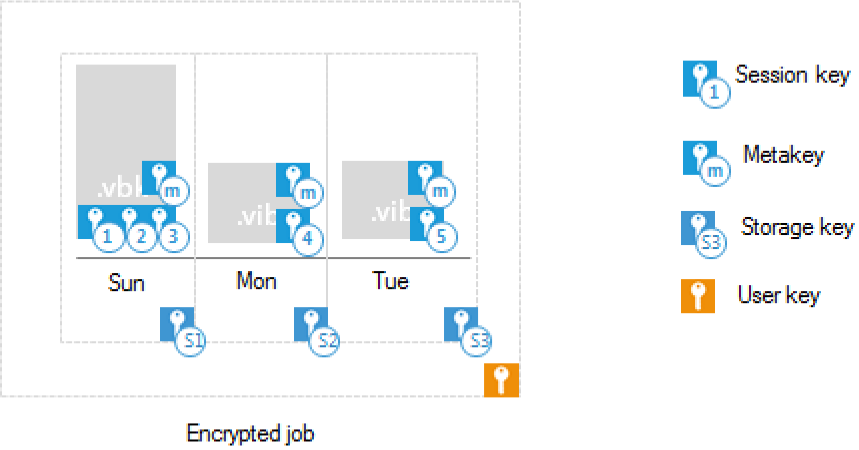
In the encryption process, storage keys are encrypted with a key of a higher layer — a user key. Cryptograms of storage keys are stored to the resulting file next to encrypted data blocks, and cryptograms of session keys and metakeys.

Storage keys are also kept in the Veeam Agent for Microsoft Windows database. To maintain a set of valid storage keys in the database, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows saves a hint for the password to its database and to the backup metadata file (VBM). When you decrypt a file, Veeam Agent for Microsoft Windows displays a hint for the password that you must provide. After you enter a password, Veeam Agent for Microsoft Windows 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 for Microsoft Windows creates a new user key and uses it to encrypt new restore points in the backup chain. If you lose a password that was specified for encryption, you can change the password in the encryption settings. You can use the new password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.

How Data Encryption Works

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

The encryption process includes the following steps:

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

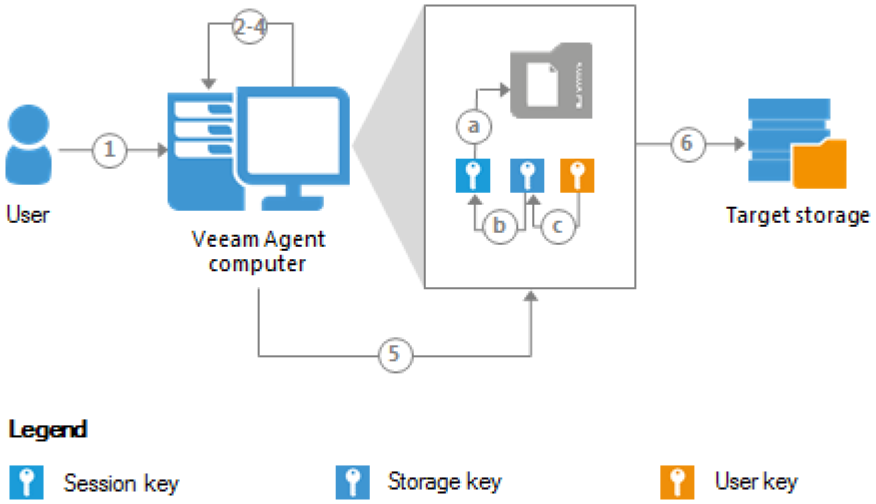
5. Veeam Agent for Microsoft Windows processes job data in the following way:

   a. The session key encrypts data blocks in the backup file. The metakey encrypts backup metadata.

   b. The storage key encrypts the session key and the metakey.

   c. The user key encrypts the storage key.

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



How Data Decryption Works

When you restore data from an encrypted backup file, Veeam Agent for Microsoft Windows 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 for Microsoft Windows database, you do not need to enter 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 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.

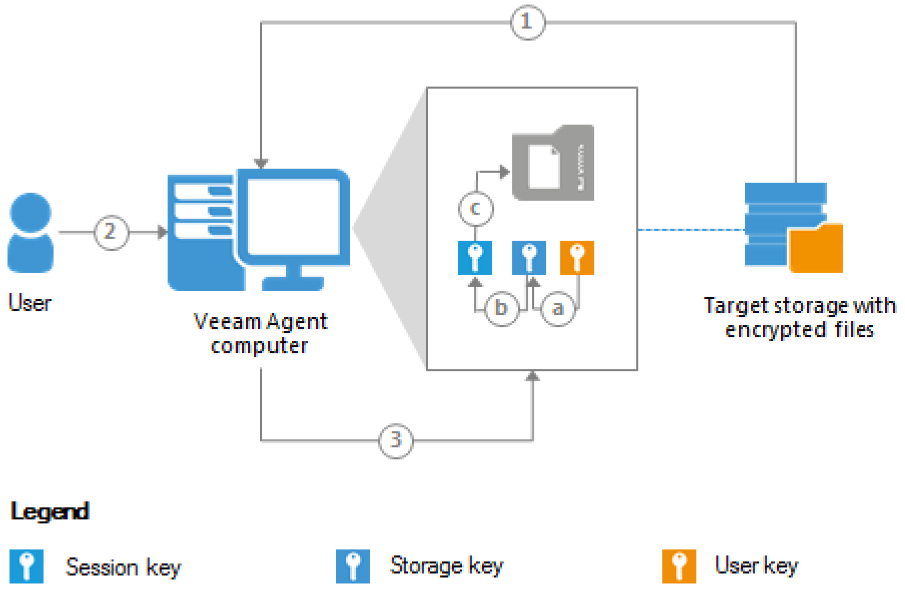
- If encryption keys are not available in the Veeam Agent for Microsoft Windows database, you need to provide a password to unlock the encrypted file.

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

The decryption process includes the following steps. Note 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 for Microsoft Windows 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 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.
3. Veeam Agent for Microsoft Windows reads the entered password and generates the user key based on this password. With the user key available, Veeam Agent for Microsoft Windows performs decryption in the following way:
    a. Veeam Agent for Microsoft Windows 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.

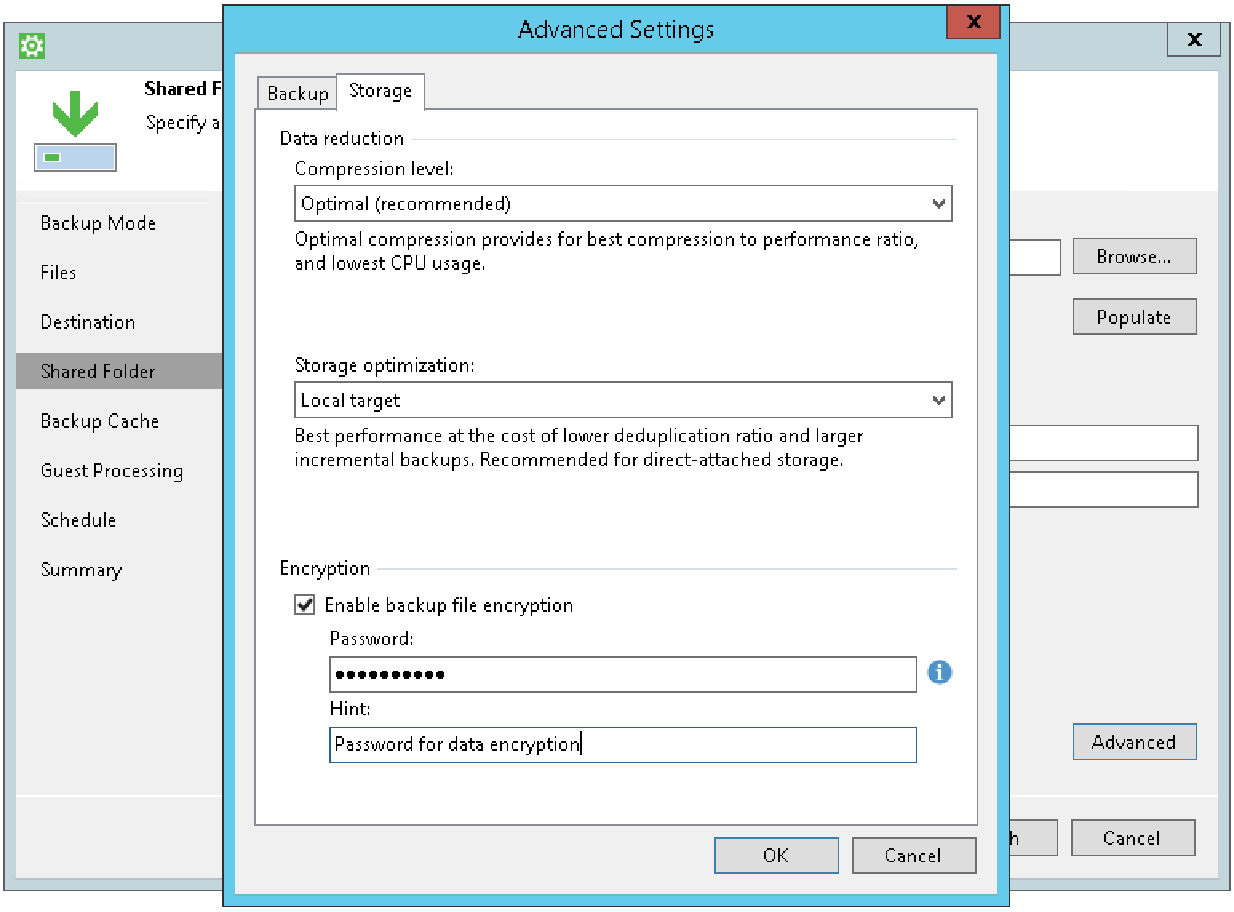


Backup Job Encryption

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, refer to the Veeam Backup & Replication documentation at https://www.veeam.com/documentation-guides-datasheets.html.



Advanced Settings

Backup | Storage

Data reduction

Compression level: Optimal (recommended)

Optimal compression provides for best compression to performance ratio, and lowest CPU usage.

Storage optimization: Local target

Best performance at the cost of lower deduplication ratio and larger incremental backups. Recommended for direct-attached storage.

Encryption

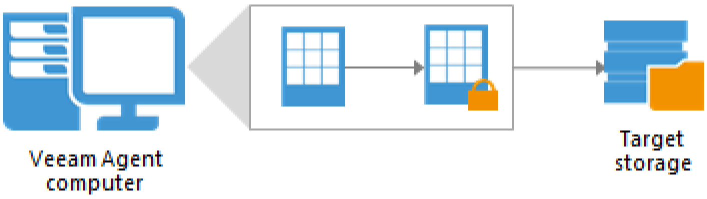
☑ Enable backup file encryption

Password: ●●●●●●●●●●●

Hint: Password for data encryption

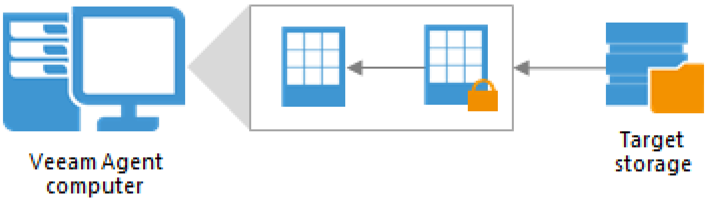
The backup job processing with encryption enabled includes the following steps:

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



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 for Microsoft Windows uses the provided password to generate user key and unlock the subsequent keys for backup file decryption.
3. Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows Control Panel.

When the backup job is started (either manually or upon the defined schedule), Veeam Agent for Microsoft Windows detects the latest encrypted backup created by this job in the target location and displays a window in the 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 for Microsoft Windows will use this password to decrypt backup metadata on the target location and update information about backup in its database. After that, Veeam Agent for Microsoft Windows will create the new incremental backup file in the existing encrypted backup chain. To encrypt this backup file and subsequent backup files, Veeam Agent for Microsoft Windows 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.

- If you do not remember the password or do not want to continue the existing backup chain for some reason, you can click **Start New** immediately without providing a password.

  When you start a new backup chain, Veeam Agent for Microsoft Windows creates the active full backup file. All incremental backup files use this full backup file as a new starting point. Depending on the defined encryption settings, Veeam Agent for Microsoft Windows creates a full backup file according to the following rules:

  - If the encryption option is disabled in Veeam Agent for Microsoft Windows at the time when you start a new backup chain, Veeam Agent for Microsoft Windows creates an unencrypted full backup file. Subsequent incremental backup files will be unencrypted, too.

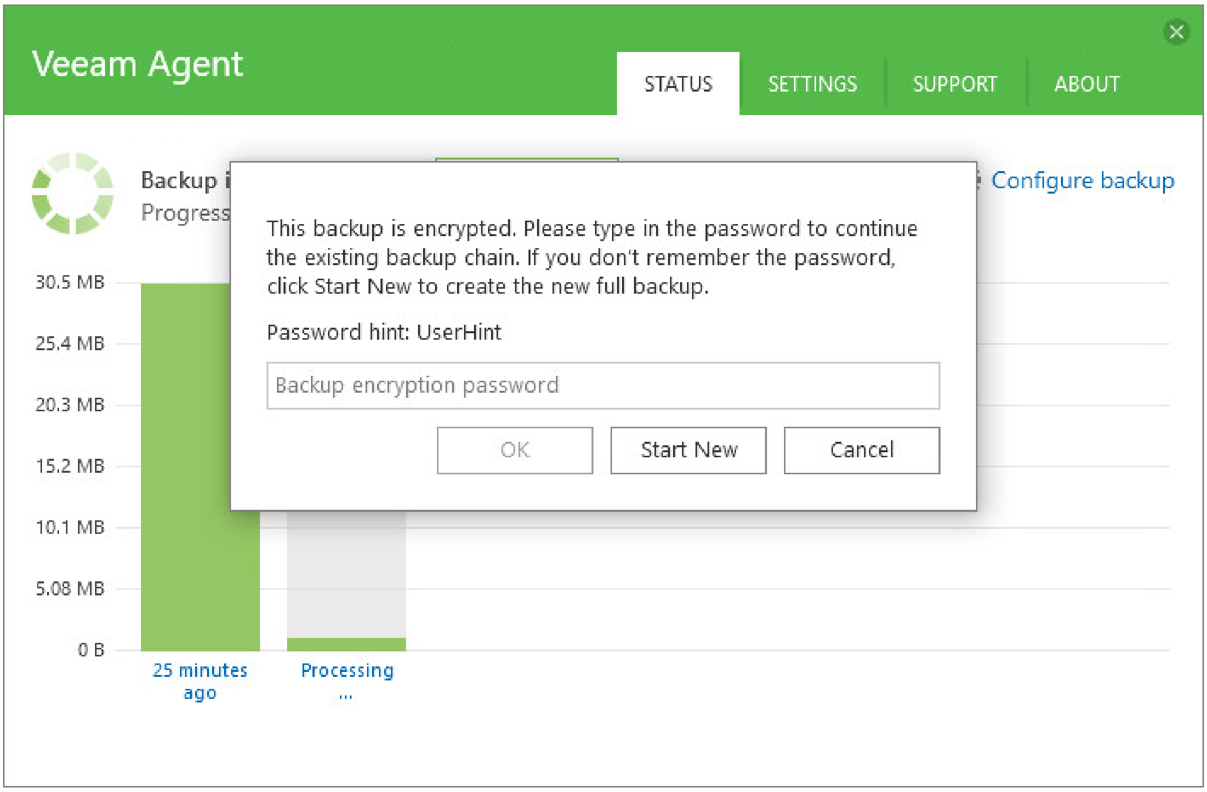
  - If the encryption option is enabled in Veeam Agent for Microsoft Windows at the time when you start a new backup chain, Veeam Agent for Microsoft Windows creates an encrypted full backup file. To encrypt this backup file, Veeam Agent for Microsoft Windows uses the password that exists in its database at the time when you start a new backup chain.

- 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 for Microsoft Windows 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 to continue the existing backup chain, start a new backup chain or cancel the backup job, after this time period expires, Veeam Agent for Microsoft Windows will automatically close the window and cancel the job. If email notification settings are enabled for the backup job, Veeam Agent for Microsoft Windows will also send an email report informing that the job was canceled.

Veeam Agent for Microsoft Windows will display this window every time the backup job is started (manually or upon schedule) until you choose to continue the existing backup chain or start a new backup chain.



This backup is encrypted. Please type in the password to continue the existing backup chain. If you don't remember the password, click Start New to create the new full backup.

Password hint: UserHint

Backup encryption password

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 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 an existing backup job, Veeam Agent for Microsoft Windows does not encrypt the previous backup chain created with this job. However, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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 for Microsoft Windows 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
- Microsoft OneDrive 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 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.
   - [For Microsoft OneDrive] Veeam Agent for Microsoft Windows Service cannot connect to Microsoft OneDrive API.

   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:

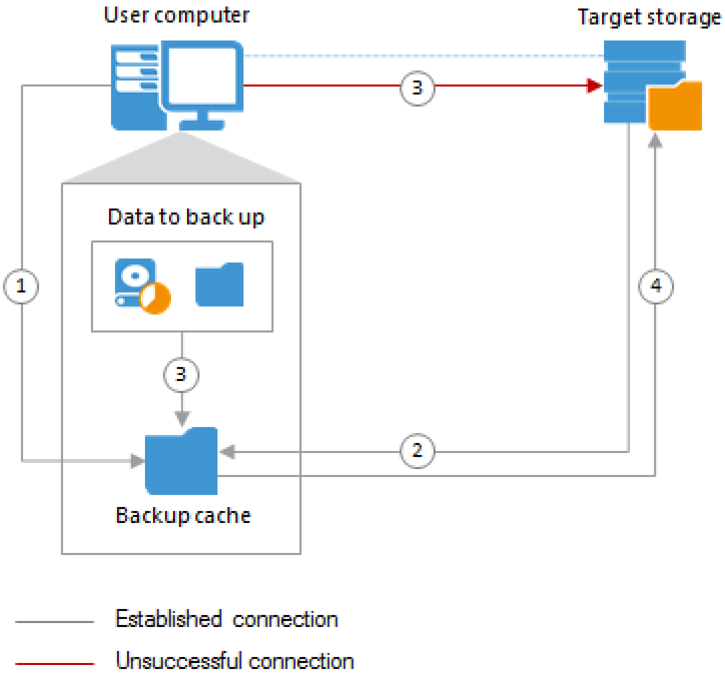
   - [For network shared folder] Veeam Agent for Microsoft Windows immediately switches to the backup cache and writes to the backup cache all data that must be backed up within the current backup job session. If some data has already been transferred to the target location, Veeam Agent for Microsoft Windows starts the data transfer operation from the beginning and transfers all backed up data to the backup cache.
   - [For Veeam backup repository, Veeam Cloud Connect repository and Microsoft OneDrive] 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 on 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 were 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 functionality is available only in Workstation and Server editions of Veeam Agent for Microsoft Windows.
- You cannot use the backup cache for the 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 logs 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:

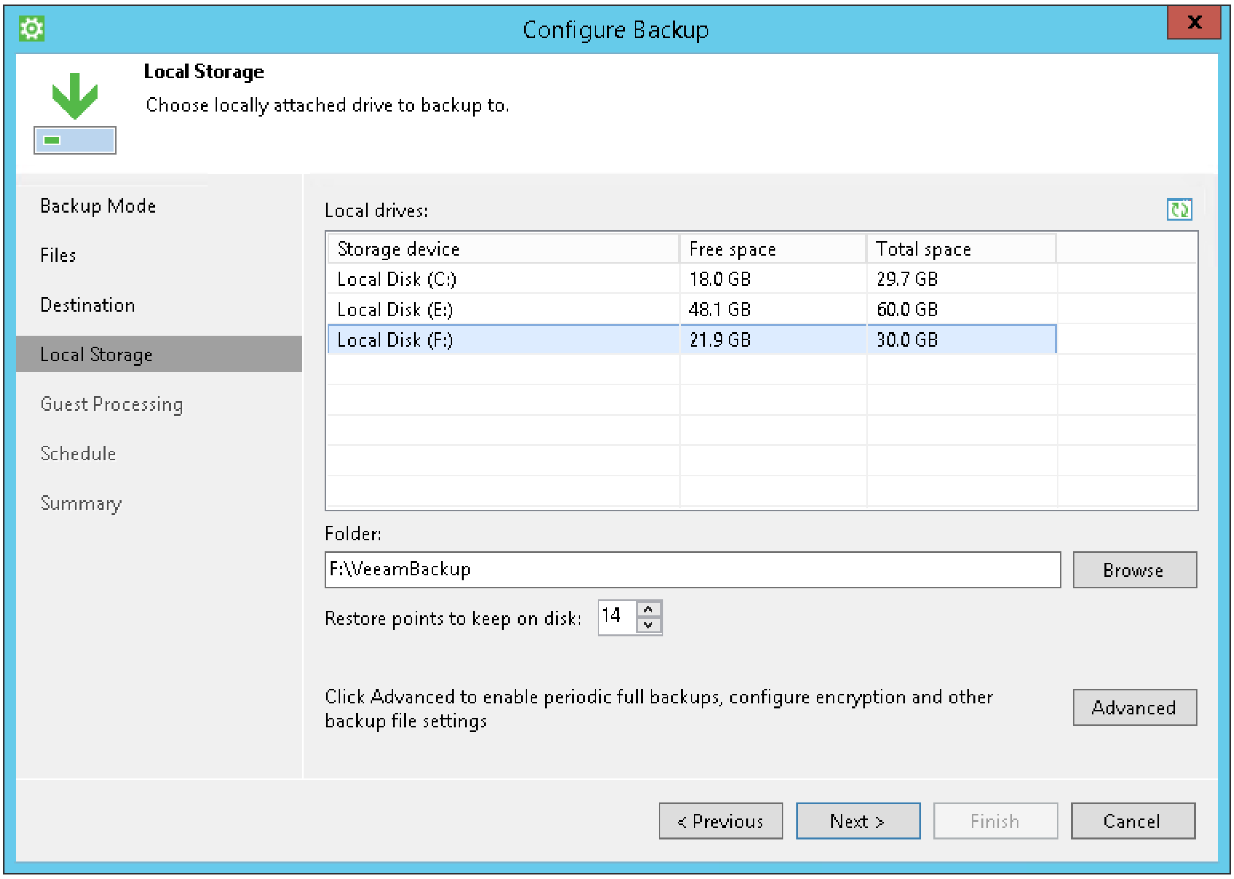
1. Veeam Agent for Microsoft Windows creates a backup chain on an external drive that you use as a backup target. The backup chain consists of the first full backup and a set of subsequent incremental backups.

2. When you swap drives and attach a new external drive, Veeam Agent for Microsoft Windows creates a separate backup chain on the new drive.

3. After you swap drives again, Veeam Agent for Microsoft Windows detects if there is a backup chain on the currently attached drive. If the backup chain exists, Veeam Agent for Microsoft Windows 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.



Configure Backup

Local Storage

Choose locally attached drive to backup to.

Local drives:

Storage device	Free space	Total space
Local Disk (C:)	18.0 GB	29.7 GB
Local Disk (E:)	48.1 GB	60.0 GB
Local Disk (F:)	21.9 GB	30.0 GB

Folder: F:\VeeamBackup

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

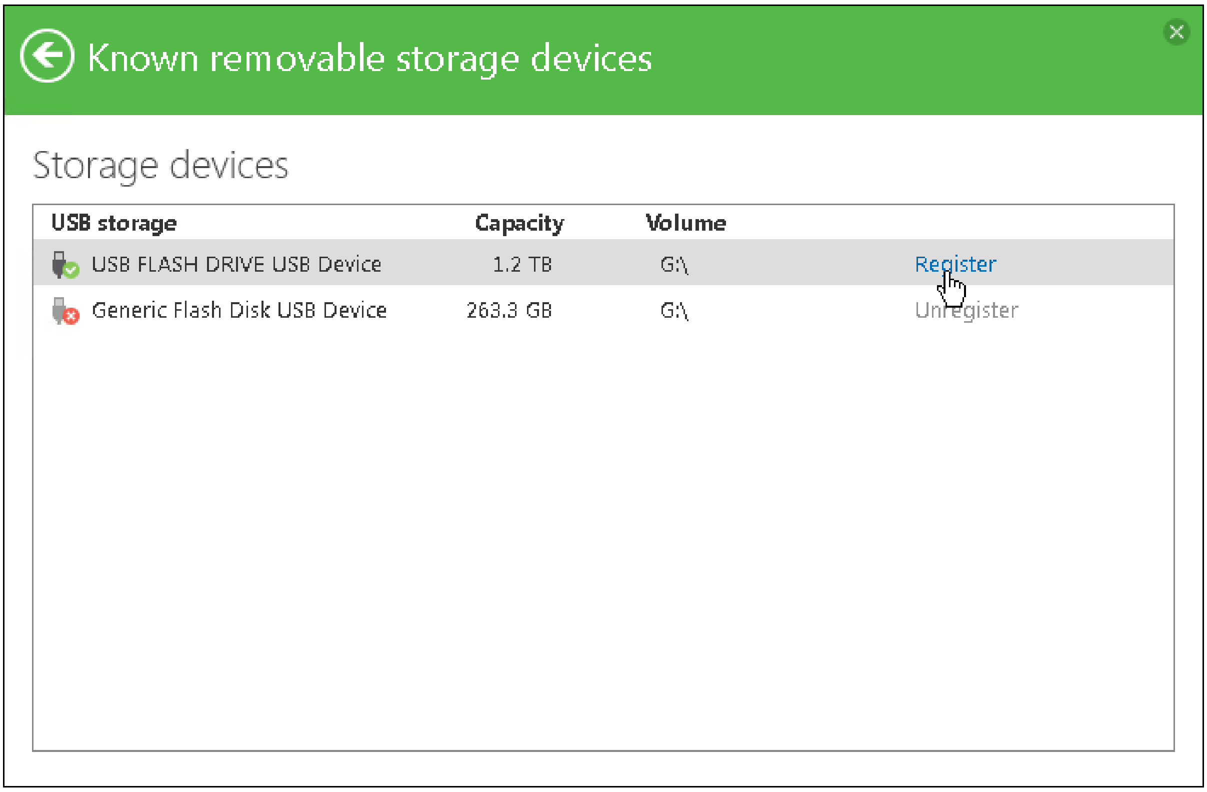
3. When you need to swap files, disconnect the drive that was used previously and attach a new drive to your computer.

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 for Microsoft Windows icon in the system tray to open the Control Panel.

    b. Click the **Settings** tab, then click the **Manage registered storage devices** link.

    c. Click **Register** next to the newly connected drive.



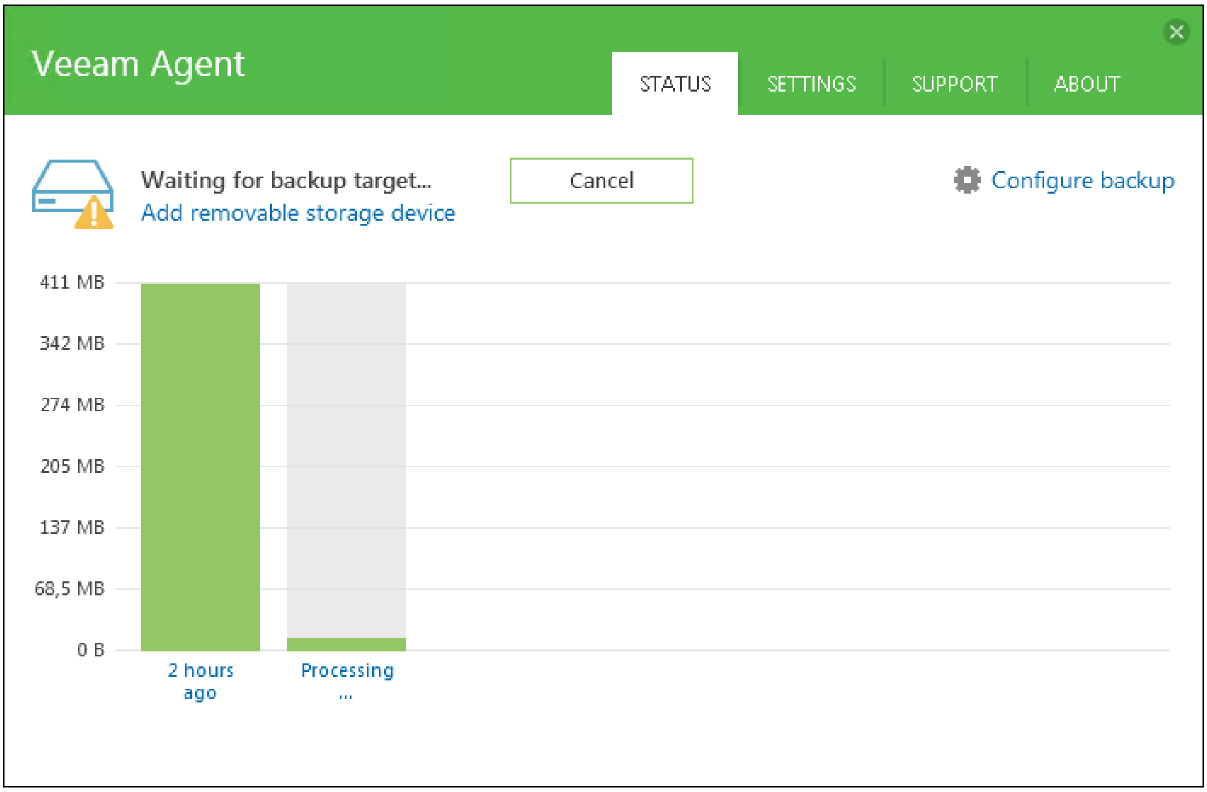
Known removable storage devices

Storage devices

USB storage	Capacity	Volume	
USB FLASH DRIVE USB Device	1.2 TB	G:\	Register
Generic Flash Disk USB Device	263.3 GB	G:\	Unregister

If you do not register the newly connected drive before the backup job starts, Veeam Agent for Microsoft Windows will be unable to detect the backup target and launch the backup job. Veeam Agent for Microsoft Windows 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 for Microsoft Windows to start a new session.

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.

Note 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.

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 simply 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 Restoring Volumes under Microsoft Windows system.
- With the **Veeam Bare Metal Recovery** wizard when 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.

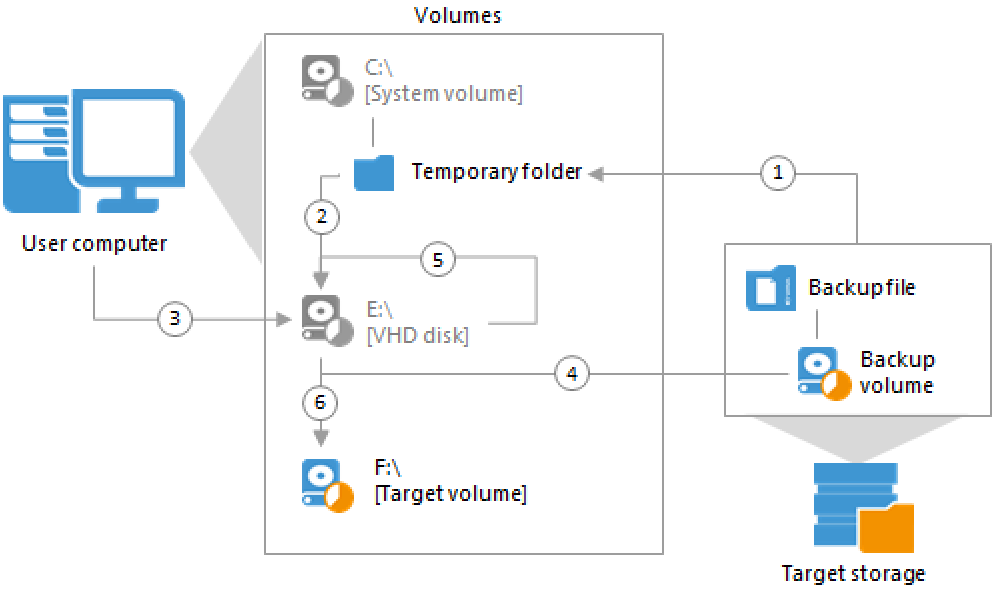
   This step may take some time depending on the size of the backup volume and its data fragmentation ratio.

   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.

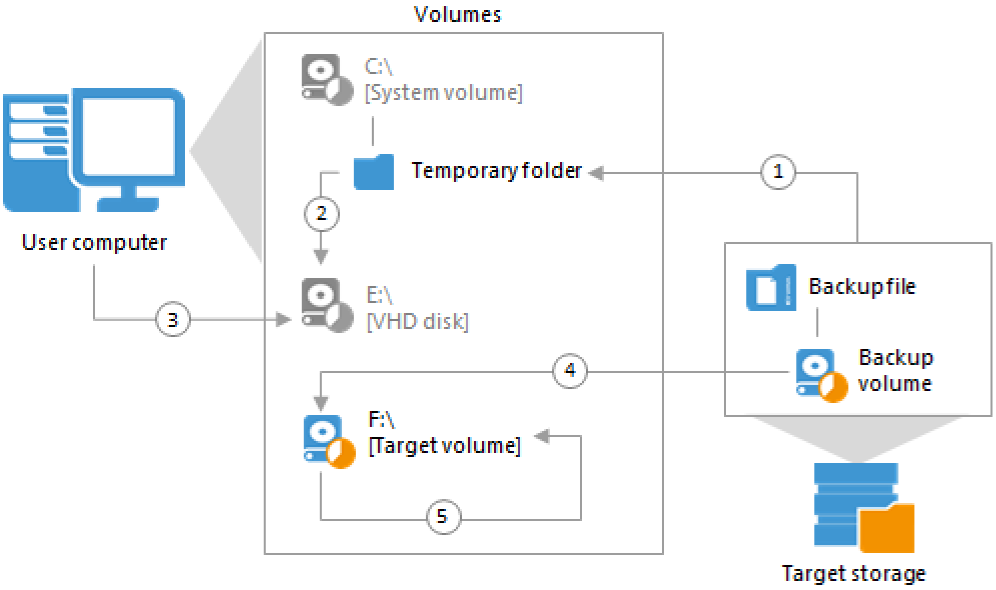
3. Veeam Agent for Microsoft Windows sends a query request to the mounted VHD disk to calculate its size, amount of stored data and free disk space by which the volume can be extended.

   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:

1. Set of files required to start your computer OS from the recovery media.
2. Diagnostic tools from Microsoft and Veeam.
3. 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.
4. 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.
5. 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.
6. Web browser required to log in to a Microsoft OneDrive account. If your backed-up data resides in Microsoft OneDrive, you can boot your computer from the Veeam Recovery Media and recover the necessary data from Microsoft OneDrive. To learn more, see Microsoft OneDrive Support.

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

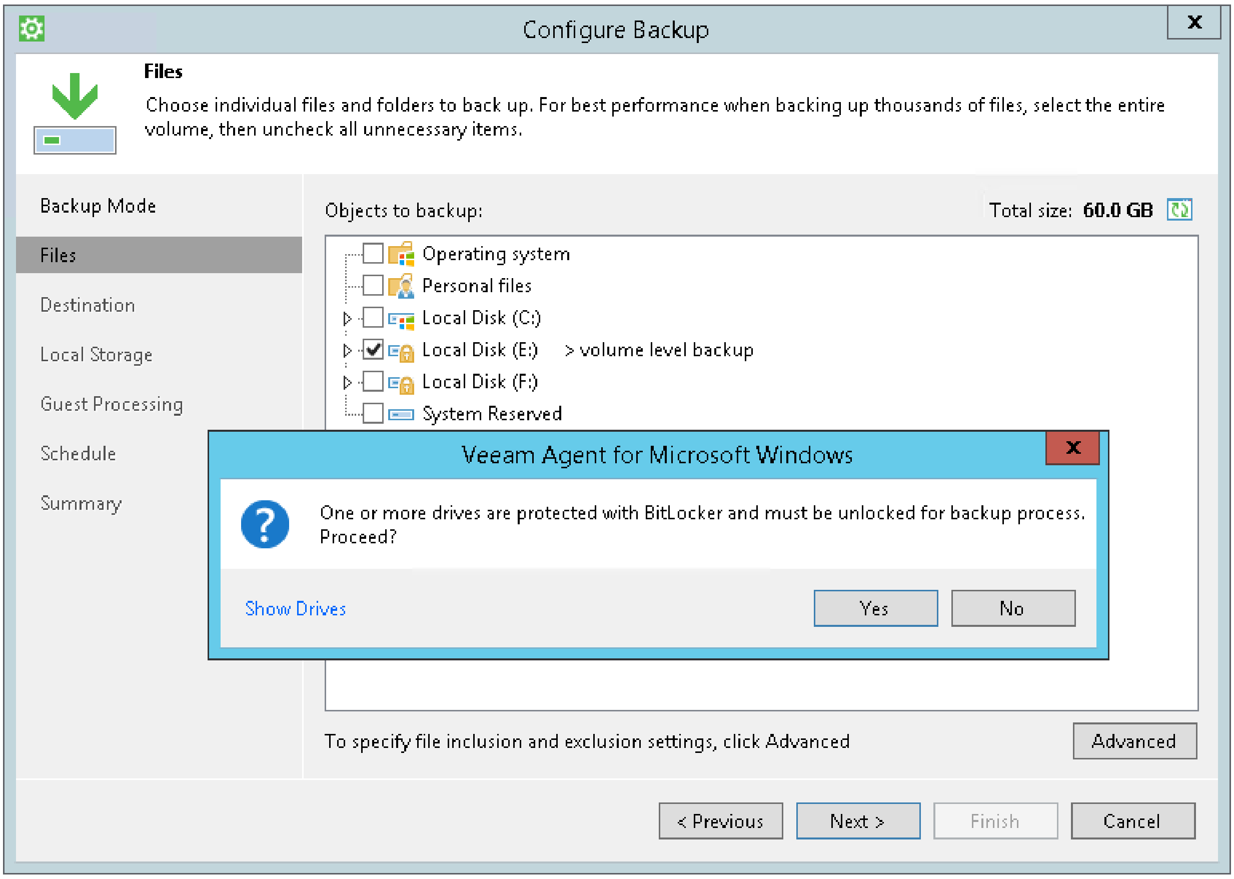
Veeam Agent for Microsoft Windows supports scenarios of data backup and restore to/from volumes encrypted with Microsoft Windows BitLocker.

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 to 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.



Choose individual files and folders to back up. For best performance when backing up thousands of files, select the entire volume, then uncheck all unnecessary items.

□ Operating system
□ Personal files
□ Local Disk (C:)
☑ Local Disk (E:) > volume level backup
□ Local Disk (F:)
□ System Reserved

One or more drives are protected with BitLocker and must be unlocked for backup process. Proceed?

To specify file inclusion and exclusion settings, click Advanced

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:

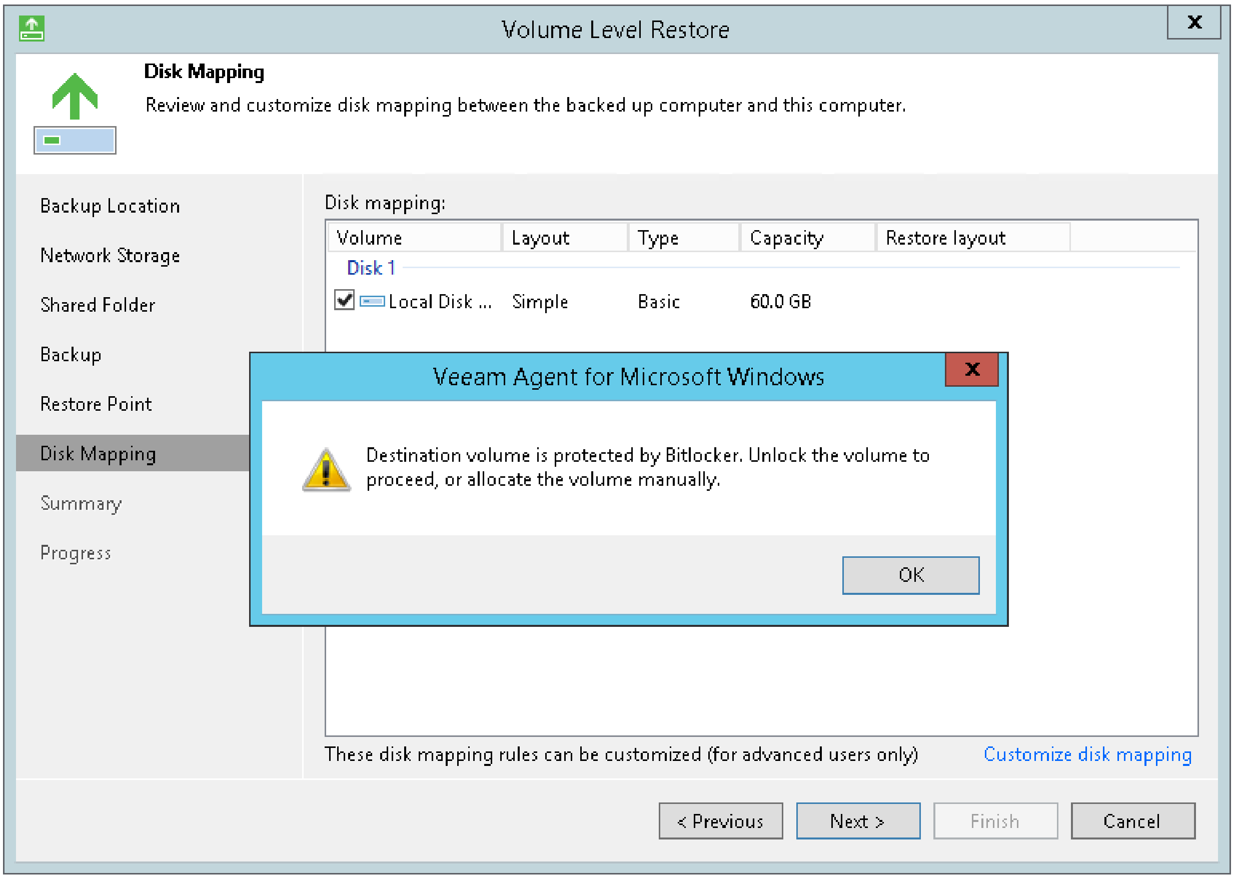
- If you restore an encrypted volume to its original location, the restored volume will be encrypted.
- If you restore an unencrypted volume to an encrypted volume, the restored volume will be unencrypted.

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.



Volume Level Restore

Disk Mapping

Review and customize disk mapping between the backed up computer and this computer.

Disk mapping:

Volume	Layout	Type	Capacity	Restore layout
Disk 1				
☑ Local Disk ...	Simple	Basic	60.0 GB	

Veeam Agent for Microsoft Windows

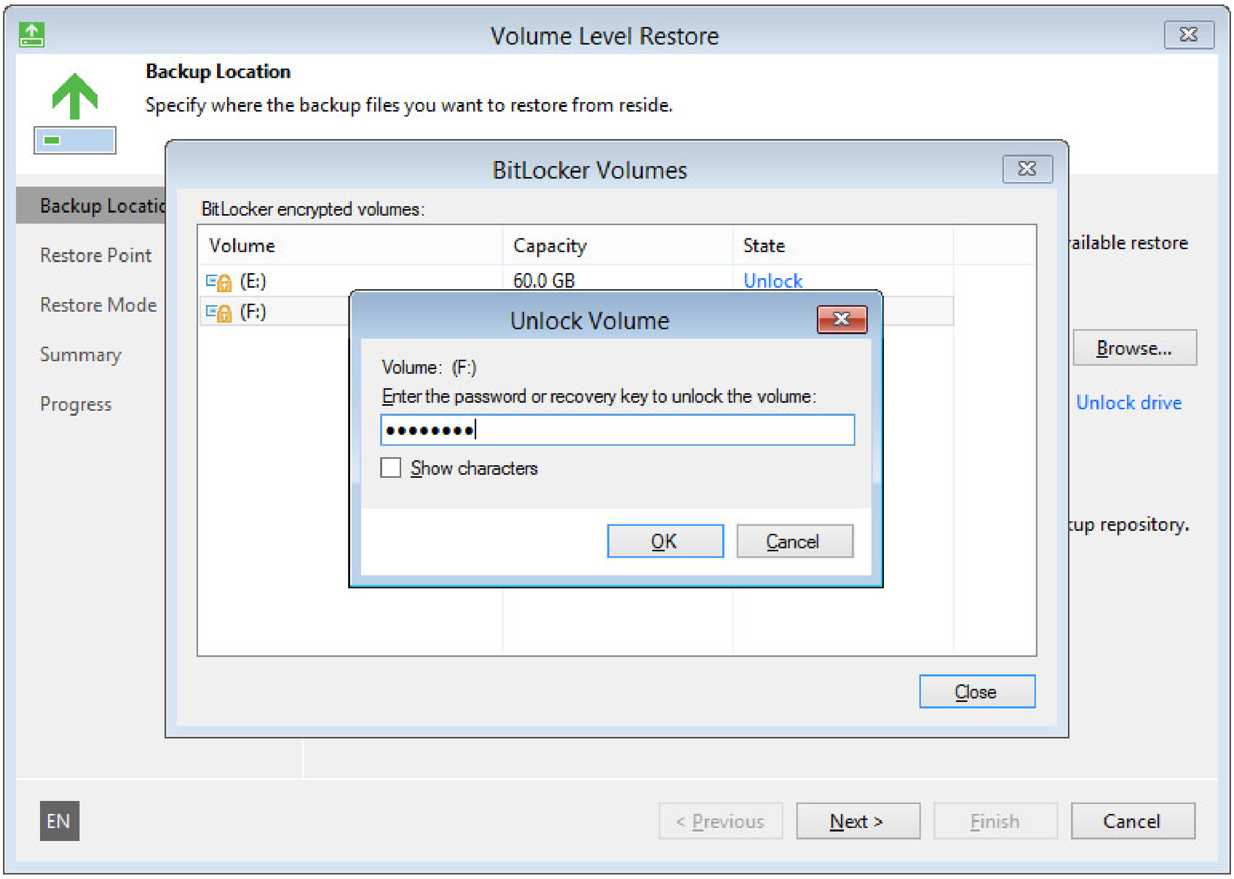
Destination volume is protected by Bitlocker. Unlock the volume to proceed, or allocate the volume manually.

These disk mapping rules can be customized (for advanced users only)

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.



Volume Level Restore

Backup Location

Specify where the backup files you want to restore from reside.

BitLocker Volumes

BitLocker encrypted volumes:

Volume	Capacity	State
(E:)	60.0 GB	Unlock
(F:)		

Unlock Volume

Volume: (F:)

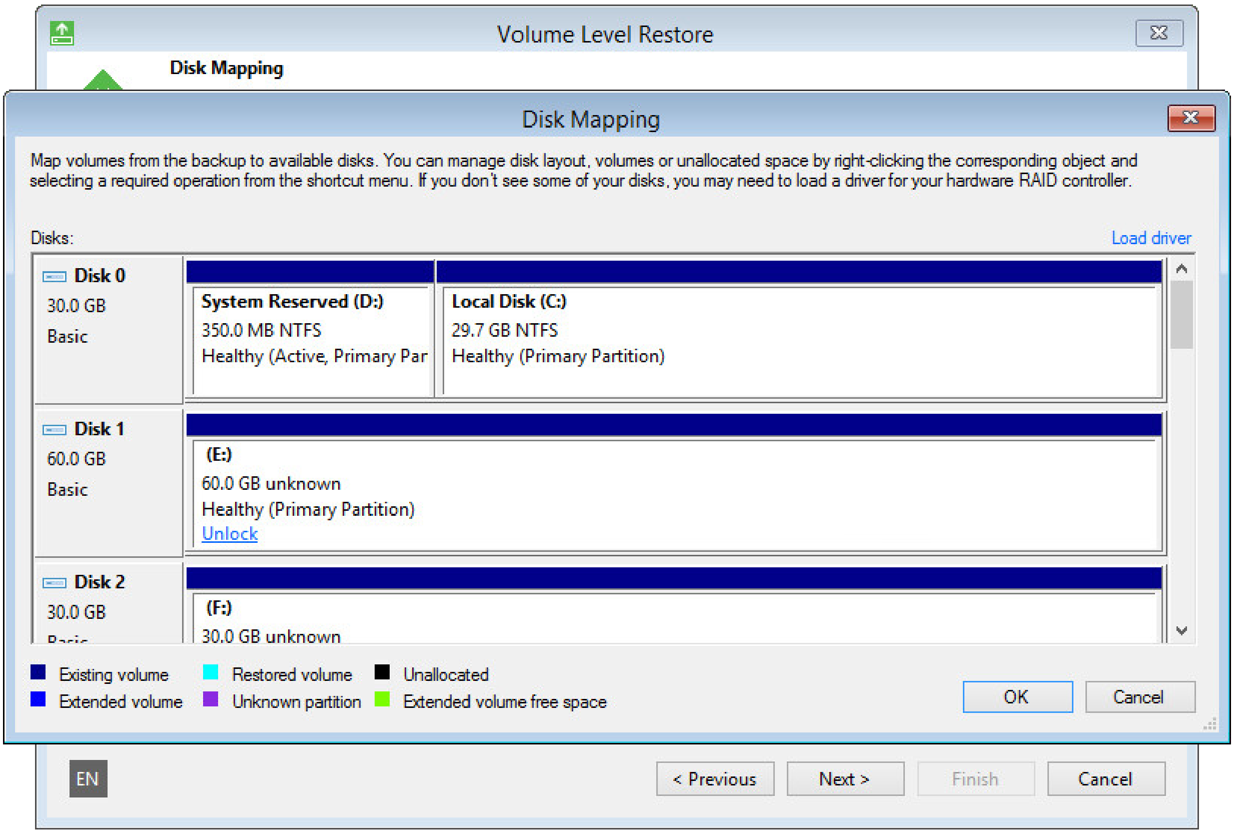
Enter the password or recovery key to unlock the volume:

••••••••

□ Show characters

- 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.



Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

Disk 0
30.0 GB
Basic

System Reserved (D:)
350.0 MB NTFS
Healthy (Active, Primary Par

Local Disk (C:)
29.7 GB NTFS
Healthy (Primary Partition)

Disk 1
60.0 GB
Basic

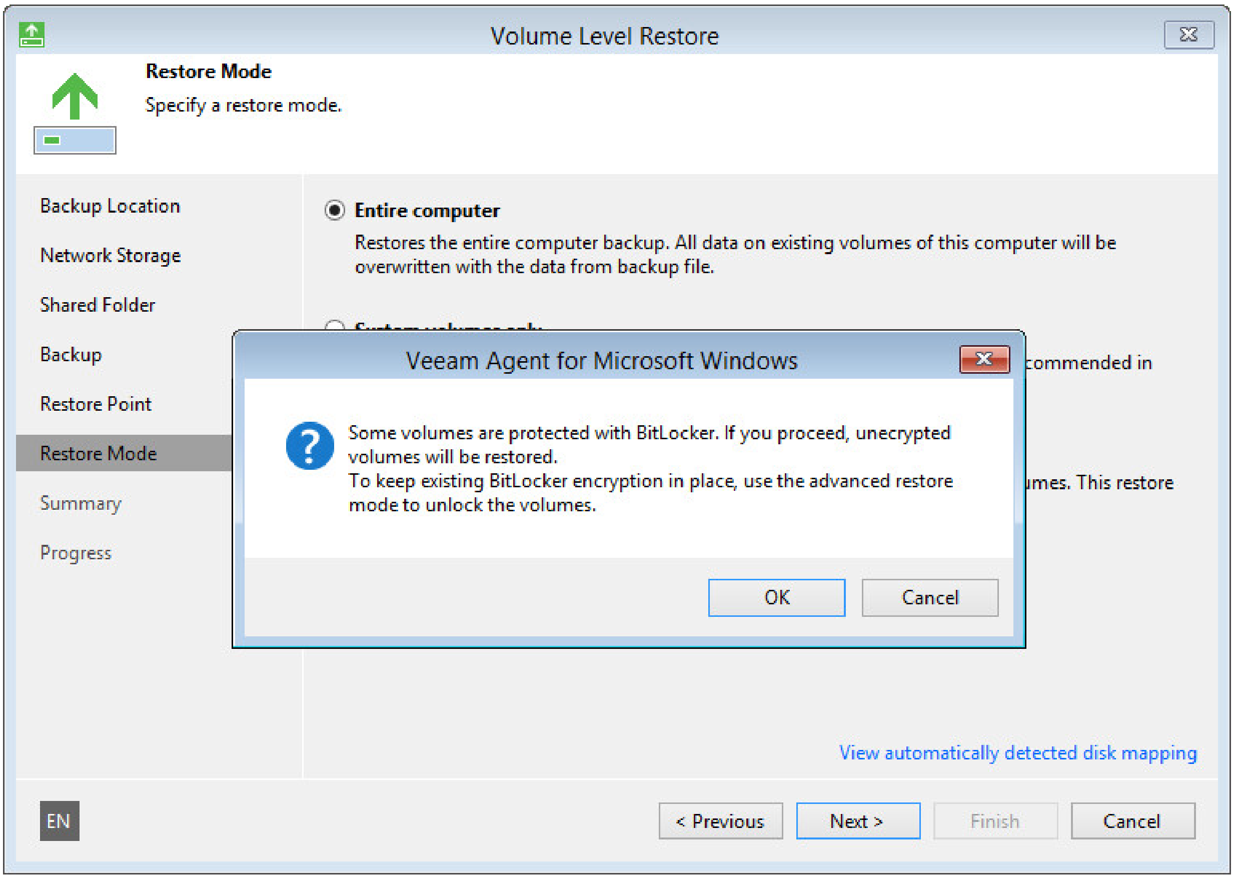
(E:)
60.0 GB unknown
Healthy (Primary Partition)
Unlock

Disk 2
30.0 GB
Basic

(F:)
30.0 GB unknown

🟦 Existing volume 🟦 Restored volume ⬛ Unallocated
🟦 Extended volume 🟪 Unknown partition 🟩 Extended volume free space

- 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.



Veeam Agent for Microsoft Windows

Some volumes are protected with BitLocker. If you proceed, unecrypted volumes will be restored.
To keep existing BitLocker encryption in place, use the advanced restore mode to unlock the volumes.

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.

Microsoft OneDrive Support

Veeam Agent for Microsoft Windows lets you back up your data to Microsoft OneDrive. This functionality is intended for users of home PCs, workstations and laptops who want to keep backups off-site without the need to set up the backup infrastructure.

Backup to Microsoft OneDrive is supported for Veeam Agent computers running the following operating systems:

- Microsoft Windows 7 SP1
- Microsoft Windows 8.x
- Microsoft Windows 10

To create backups in Microsoft OneDrive, you need to select Microsoft OneDrive as a target for backup files in the properties of the Veeam Agent backup job. When you configure the backup job, you must provide credentials of the Microsoft OneDrive account that has access to the Microsoft OneDrive storage. You can use the following types of Microsoft OneDrive accounts to back up your data:

- OneDrive (personal)
- OneDrive for Business

When the backup job session starts, Veeam Agent for Microsoft Windows copies the backed-up data directly to Microsoft OneDrive. In contrast to other types of backup location, during backup to Microsoft OneDrive, Veeam Agent for Microsoft Windows does not store copied data blocks to backups files of the VBK or VIB type. Instead, Veeam Agent for Microsoft Windows stores the entire data blocks 'as is'. This helps Veeam Agent for Microsoft Windows upload backed-up data, perform transform operations with restore points in the backup chain and delete obsolete restore points by retention in a more efficient way.

For backups residing in Microsoft OneDrive, backup metadata is stored alongside the backed-up data itself. In addition, Veeam Agent for Microsoft Windows saves a copy of backup metadata to the *C:\ProgramData\Veeam\OneDriveBackup* folder on the Veeam Agent computer.

You can use backups that reside in Microsoft OneDrive to perform the same data recovery operations that are available for Veeam Agent backups in other types of target location. You can restore entire computer volumes or individual files and folders. In case your computer fails to start, you can also boot your computer from the Veeam Recovery Media and restore data from a volume-level backup residing in Microsoft OneDrive.

> **NOTE:**
>
> You can use Microsoft OneDrive as a target for Veeam Agent backup jobs configured directly on a Veeam Agent computer only. Backup to Microsoft OneDrive for Veeam Agent for Microsoft Windows managed within the Veeam Agent management scenario is not supported.

Authorization in Microsoft OneDrive

Veeam Agent for Microsoft Windows communicates with Microsoft OneDrive over the OneDrive API. To let Veeam Agent for Microsoft Windows access the API, you need to sign in to Microsoft OneDrive in the **Configure Backup** wizard. When you sign in to Microsoft OneDrive, Veeam Agent for Microsoft Windows obtains from Microsoft OneDrive authorization tokens that provide access to the OneDrive API.

To work with the OneDrive API, Veeam Agent for Microsoft Windows uses the following types of tokens:

- **Access token.** Veeam Agent for Microsoft Windows uses this token to send requests to the OneDrive API. The access token is valid for 2 hours. To obtain a new access token after this period expires without the need to sign in to Microsoft OneDrive once again, Veeam Agent for Microsoft Windows uses the refresh token.
- **Refresh token.** Veeam Agent for Microsoft Windows uses this token to request a new access token from Microsoft OneDrive after the initial access token expires. In contrast to the access token, the refresh token is saved to Veeam Agent for Microsoft Windows database. The refresh token can be valid for 14 to 180 days depending on the type of account used to connect to Microsoft OneDrive:
    - 180 days — for a personal OneDrive account.
    - 14 to 90 days — for a OneDrive for Business account. Veeam Agent for Microsoft Windows can use the refresh token for more that 14 days if one of the following operations is performed within a 14-day period:
        - Sign-in to Microsoft OneDrive in the **Configure Backup** wizard
        - Backup to Microsoft OneDrive
        - Backup chain transform in Microsoft OneDrive
        - Backup cache synchronization with Microsoft OneDrive
        - Data restore from Microsoft OneDrive

      After a 90-day period expires, you need to sign in to your OneDrive for Business account once again in the **Configure Backup** wizard. Otherwise, the backup job will be failing.

Limitations for Backup to Microsoft OneDrive

Backup to Microsoft OneDrive has the following limitations:

- You cannot create a standalone full backup in Microsoft OneDrive.
- Veeam Agent for Microsoft Windows does not support creating Microsoft SQL Server transaction log backups and Oracle archived log backups in Microsoft OneDrive.
- In the Free edition of Veeam Agent for Microsoft Windows you can create in Microsoft OneDrive only file-level backups that contain operating system data.
- You cannot move backup files residing in Microsoft OneDrive to a backup storage of a different type and continue the Veeam Agent backup chain in another target location.
- If you use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you cannot import a backup residing in Microsoft OneDrive in the Veeam Backup & Replication console.
- Due to limitations set in Microsoft OneDrive for third-party applications, backup to Microsoft OneDrive and data restore from Microsoft OneDrive requires longer time even in fast networks.
- Backup to Microsoft OneDrive is not supported for the following OneDrive storage plan regions:
  - US Government
  - China
  - Germany

Integration with Veeam Backup & Replication

If you plan to use Veeam Agent for Microsoft Windows 2.2 with Veeam Backup & Replication, you must install Veeam Backup & Replication 9.5 Update 3 or later on the Veeam backup server.

> **NOTE:**
>
> Starting from version 9.5 Update 3, you can 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 at: https://www.veeam.com/documentation-guides-datasheets.html.

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.

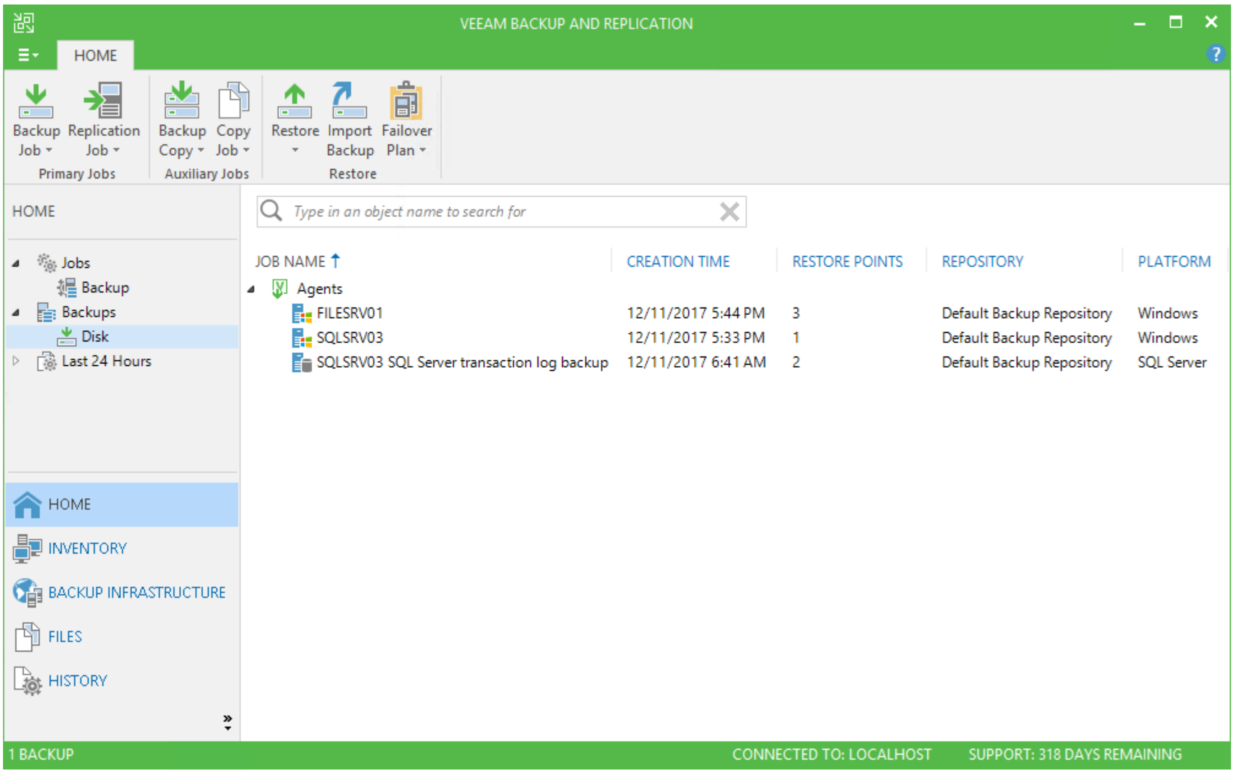
Veeam Agent for Microsoft Windows works with the backup repository as with any other target location. Backup files are stored to a separate folder; you can perform standard restore operations using these files.

Information about Veeam Agent backups stored on 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** 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 from Veeam Agent backups; restore computer disks and convert them to the VMDK, VHD or VHDX format; restore Veeam Agent backups to Microsoft Azure or to Hyper-V VMs.
- Perform administrative tasks: disable and delete Veeam Agent backup jobs, remove Veeam Agent backups and so on.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01	12/11/2017 5:44 PM	3	Default Backup Repository	Windows
SQLSRV03	12/11/2017 5:33 PM	1	Default Backup Repository	Windows
SQLSRV03 SQL Server transaction log backup	12/11/2017 6:41 AM	2	Default Backup Repository	SQL Server

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:

1. You cannot use a Veeam Cloud Connect repository as a target for standalone full backup.
2. 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.

Veeam Agent Management in Veeam Backup & Replication

Veeam Backup & Replication lets you automate management of Veeam Agent for Microsoft Windows on multiple computes 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 9.5 Update 3 or later on the Veeam backup server.

To learn more, see Veeam Agent Management User Guide at:
https://helpcenter.veeam.com/docs/backup/agents/.

Requirements

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 endpoint must meet the following requirements:

Specification	Requirement
Hardware	CPU: x86-64 processor. Memory: 2 GB RAM. Disk Space: 150 MB for product installation. Network: 1 Mbps or faster*. System firmware: BIOS or UEFI. Drive encryption: Microsoft BitLocker (optional)**. * High latency and reasonably unstable WAN links are supported. ** 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*: • Microsoft Windows 7 SP1 • Microsoft Windows 8.x • Microsoft Windows 10 (including version 1803)** • Microsoft Windows Server 2008 R2 SP1*** • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 * Consider the following: ▪ Small Business Server and Server Essentials editions of Microsoft Windows Server OSs are supported. ▪ Server Core installations of Microsoft Windows Server OSs are not supported. ▪ Windows Embedded / Windows IoT OSs are not supported. ▪ Microsoft Failover Clusters are supported for Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication. Veeam Agent for Microsoft Windows operating in the standalone mode does not support Microsoft Failover Clusters. ** Microsoft Windows 10 Education is supported starting from build 10586 and higher. *** Veeam CBT driver is supported only if update KB3033929 is installed on the Veeam Agent computer.

File System	Microsoft Windows FAT, NTFS, ReFS file systems are supported.
Software	The following required 3rd party software is included in the setup program: • Microsoft .NET Framework 4.5.2 • Microsoft SQL Server 2012 Management Objects • Microsoft SQL Server System CLR Types 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 9.5 Update 3 or later on the Veeam backup server.
Microsoft SQL Database	Microsoft SQL Server 2012 Express LocalDB Edition (installed with the product).

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.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share.
- Veeam Backup & Replication 9.5 Update 3 or later backup repository*.

Cloud storage

- Veeam Cloud Connect 9.5 Update 3 or later cloud repository.
- Microsoft OneDrive storage

* Advanced integration with HPE StoreOnce storage appliances via the HPE StoreOnce Catalyst technology is not supported. If you want to use an HPE StoreOnce storage appliance as a backup repository, please use it as a CIFS share.

* Veeam Agent for Microsoft Windows should be able to establish a direct IP connection to the Veeam Backup & Replication repository server. Thus, Veeam Agent for Microsoft Windows cannot work with Veeam Backup & Replication that is located behind the NAT gateway.

Used Ports

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

From	To	Protocol	Port	Notes
Veeam Agent Computer	Veeam Backup Server	TCP	10001	Default port used for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.
	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 (dev.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				
Veeam Agent Computer	Linux server performing the role of a backup repository	TCP	22	Port used as a control channel from the Veeam Agent computer to the target Linux host.
		TCP	2500 to 5000	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	1025 to 5000 (for Microsoft Windows 2003) 49152-65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see https://support.microsoft.com/kb/929851/en-us.
		TCP	2500 to 5000	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	135, 137 to 139, 445	Ports used as a transmission channel from the Veeam Agent computer to the target CIFS (SMB) share.

	Gateway Microsoft Windows server	TCP UDP	135, 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.
		TCP	1025 to 5000 (for Microsoft Windows 2003) 49152-65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see https://support.microsoft.com/kb/929851/en-us.
		TCP	2500 to 5000	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				
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.

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.

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 Veeam Agent license in the Veeam Backup & Replication console or in Veeam Backup Enterprise Manager. To learn more, see Managing Veeam Agent 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 Microsoft Windows OS. To use the Server edition of Veeam Agent for Microsoft Windows, you must obtain and install on the protected computer a paid license that supports this product edition.
- *Workstation* — a commercial edition that offers capabilities for performing data protection tasks on desktop computers and laptops that run Microsoft Windows OS. To use the Workstation edition of Veeam Agent for Microsoft Windows, you must obtain and install on the protected computer a paid license that supports this product edition.
- *Free* — a free edition that offers limited capabilities sufficient for personal use of the product. In contrast to 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 the Veeam Agent for Microsoft Windows product page on the Veeam web site at https://www.veeam.com/.

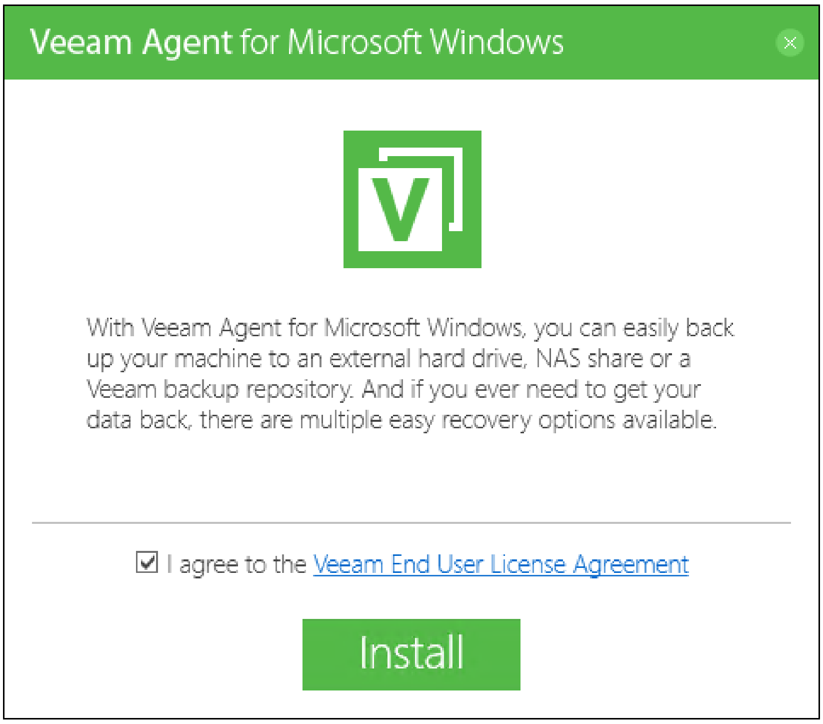
When you install a license on the protected computer, you can select the product edition of Veeam Agent for Microsoft Windows: Workstation or Server (if both editions are supported by the license). To learn more, see Selecting Product Edition.

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 with Veeam Backup & Replication.

After the license expires, Veeam Agent for Microsoft Windows automatically switches to the free edition. If you have used backup job options available for Workstation and Server editions, you must disable these options in the properties of the backup job. Otherwise, the backup job will be failing.

License Agreement

When you install Veeam Agent for Microsoft Windows, you must accept the terms of the product license agreement. To view the license agreement, click the **Veeam End User License Agreement** link in the installation window or visit the Veeam website at: www.veeam.com/eula.html.



Veeam Agent for Microsoft Windows

With Veeam Agent for Microsoft Windows, you can easily back up your machine to an external hard drive, NAS share or a Veeam backup repository. And if you ever need to get your data back, there are multiple easy recovery options available.

☑ I agree to the Veeam End User License Agreement

Installing License

When you launch the Veeam Agent for Microsoft Windows control panel for the first time, Veeam Agent for Microsoft Windows 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 and manage the Veeam Agent for Microsoft Windows license in Veeam Backup & Replication. To learn more, see Managing Veeam Agent License.

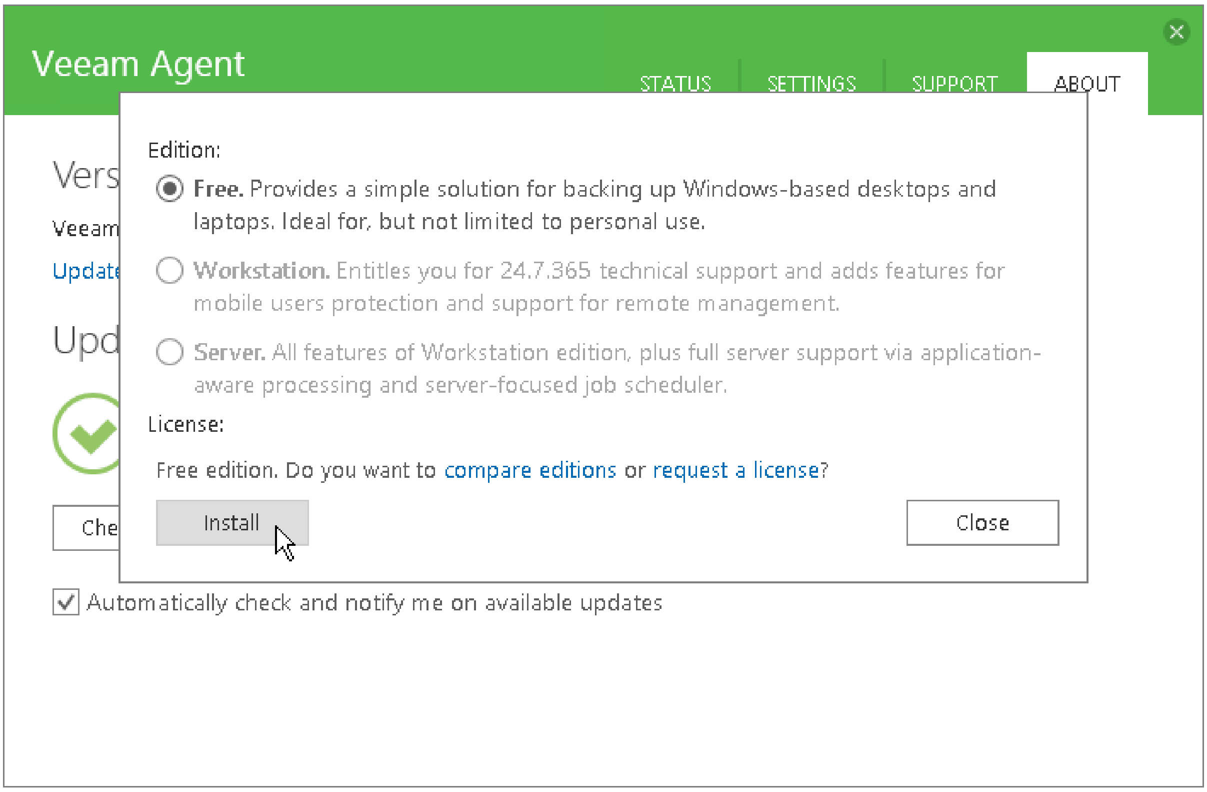
To install a license:

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. At the top of the window, click the **About** tab.
3. In the **Version** section, click the following link:
   - **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.
   - **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 to 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.



Edition:

● **Free.** Provides a simple solution for backing up Windows-based desktops and laptops. Ideal for, but not limited to personal use.

○ **Workstation.** Entitles you for 24.7.365 technical support and adds features for mobile users protection and support for remote management.

○ **Server.** All features of Workstation edition, plus full server support via application-aware processing and server-focused job scheduler.

License:

Free edition. Do you want to compare editions or request a license?

☑ Automatically check and notify me on available updates

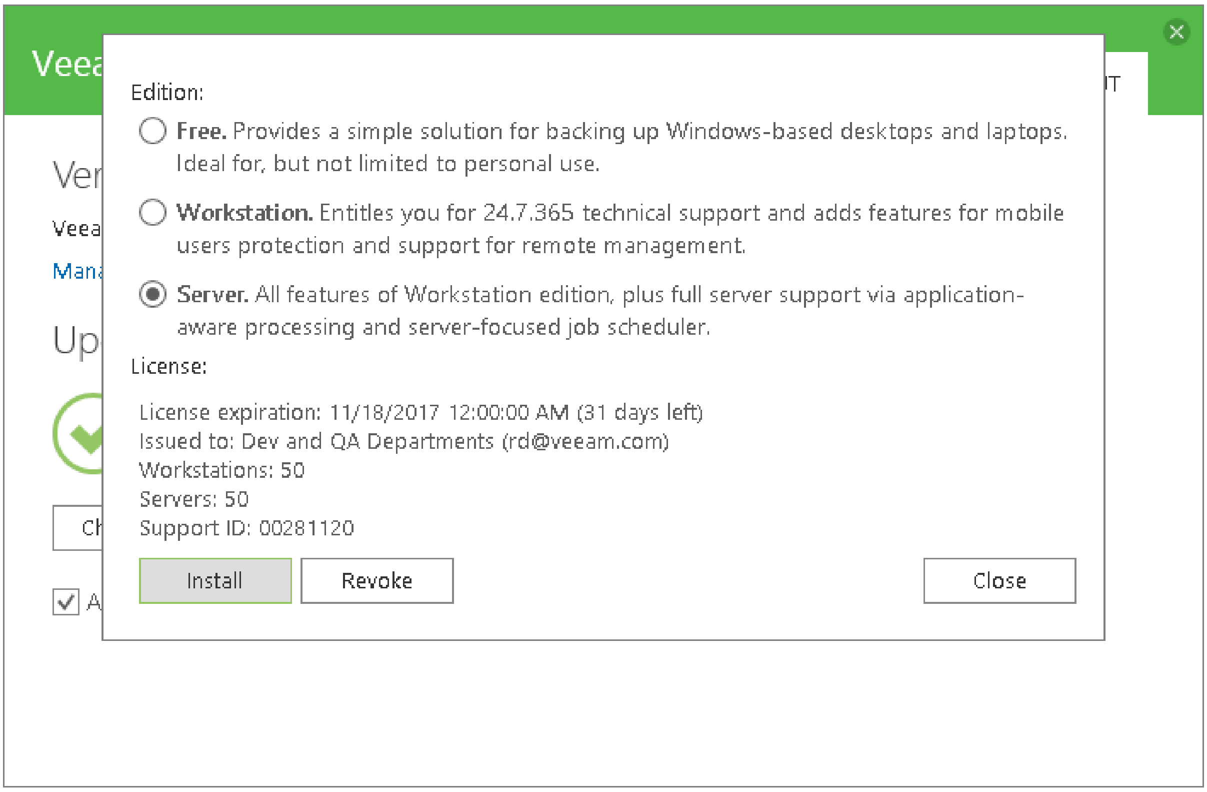
Selecting Product Edition

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. At the top of the window, click the **About** tab.
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.



Edition:

○ **Free.** Provides a simple solution for backing up Windows-based desktops and laptops. Ideal for, but not limited to personal use.

○ **Workstation.** Entitles you for 24.7.365 technical support and adds features for mobile users protection and support for remote management.

● **Server.** All features of Workstation edition, plus full server support via application-aware processing and server-focused job scheduler.

License:

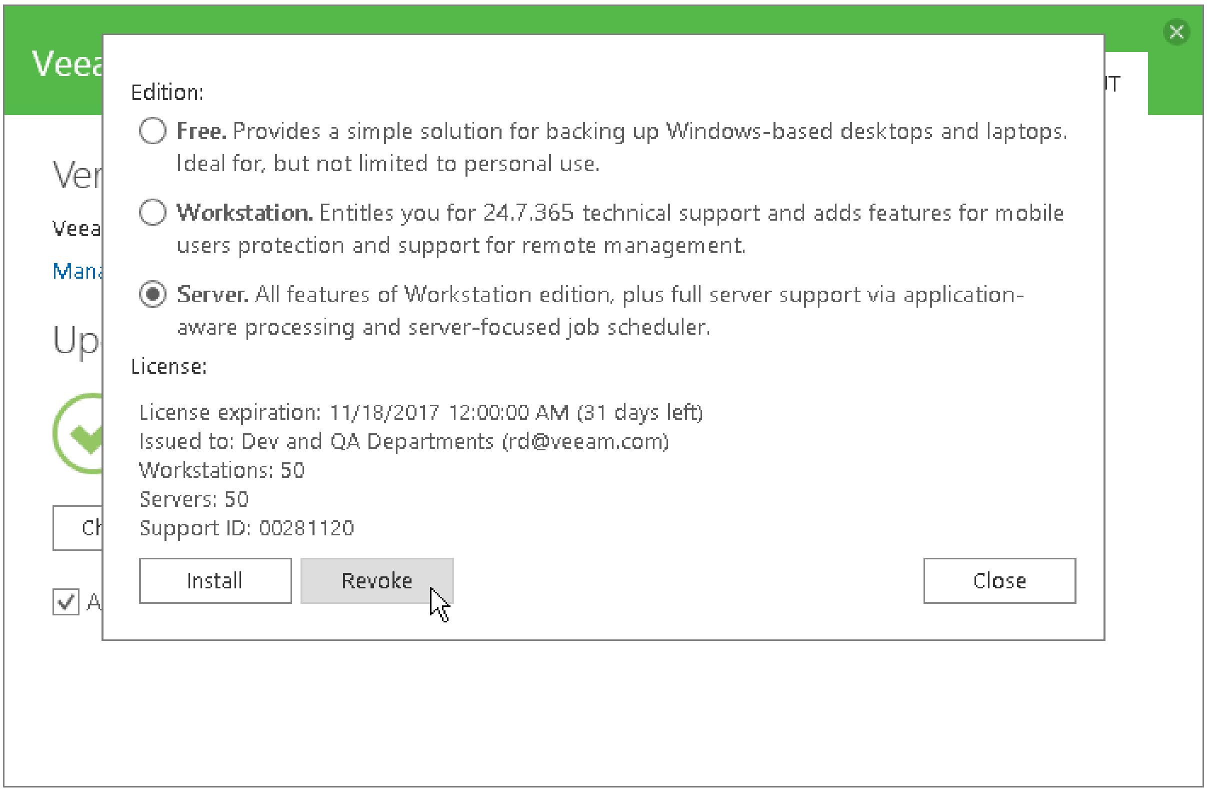
License expiration: 11/18/2017 12:00:00 AM (31 days left)
Issued to: Dev and QA Departments (rd@veeam.com)
Workstations: 50
Servers: 50
Support ID: 00281120

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. At the top of the window, click the **About** tab.
3. In the **Version** section, click **Manage license and edition**.
4. In the dialog window, click **Revoke**.



Edition:

○ **Free.** Provides a simple solution for backing up Windows-based desktops and laptops. Ideal for, but not limited to personal use.

○ **Workstation.** Entitles you for 24.7.365 technical support and adds features for mobile users protection and support for remote management.

● **Server.** All features of Workstation edition, plus full server support via application-aware processing and server-focused job scheduler.

License:

License expiration: 11/18/2017 12:00:00 AM (31 days left)
Issued to: Dev and QA Departments (rd@veeam.com)
Workstations: 50
Servers: 50
Support ID: 00281120

Installation and Configuration

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

Before You Begin

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

1. The computer on which you plan to install Veeam Agent for Microsoft Windows must satisfy system requirements specified in this document. To learn more, see System Requirements.

2. You must run the Veeam Agent for Microsoft Windows setup file under the Administrator account or any user account that has Administrator privileges on the computer where you plan to install the product.

3. Veeam Agent for Microsoft Windows requires the following components:

   - Microsoft SQL Server System CLR Types
   - Microsoft SQL Server 2012 Management Objects
   - Microsoft SQL Server 2012 (LocalDB)
   - Microsoft .NET Framework 4.5.2

   If these components are not pre-installed on the computer, the setup will install them during the product installation process.

4. The product program files are placed to the `%Program Files%\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 for Microsoft Windows requires at least 150 MB.

5. [Recommended] If you want to configure a scheduled backup job with default settings after the installation, you must prepare a USB storage device.

6. [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 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.

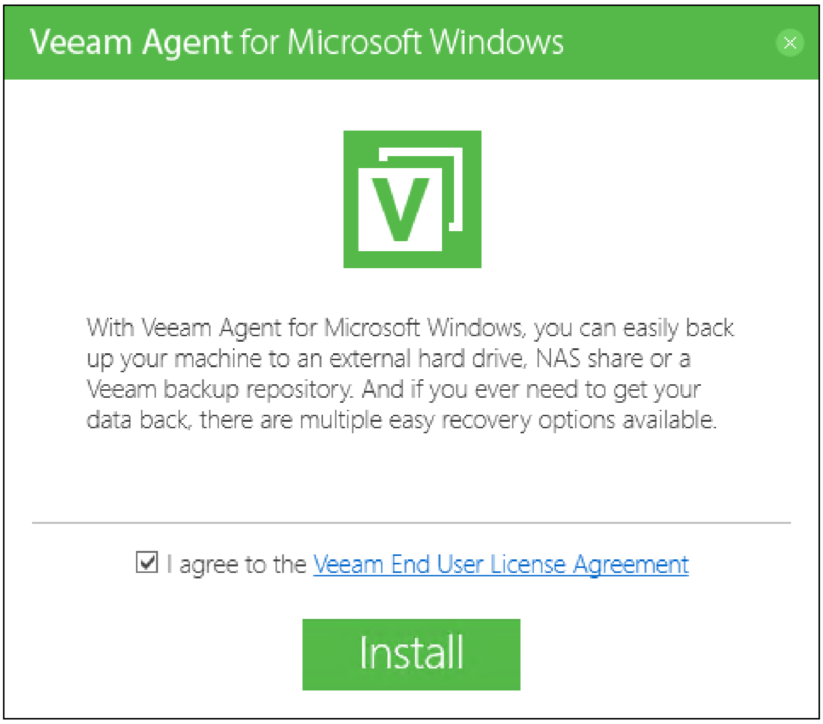
Installing Veeam Agent for Microsoft Windows

To install Veeam Agent for Microsoft Windows:

1. Download the Veeam Agent for Microsoft Windows setup archive from the Veeam Download page at https://www.veeam.com/downloads.html, and save the downloaded archive on the computer where you plan to install the product.

2. Double-click the downloaded setup archive.

3. To install Veeam Agent for Microsoft Windows, you must accept the license agreement. Read the license agreement, select the **I agree to the Veeam End User License Agreement** check box and click **Install**.



Veeam Agent for Microsoft Windows

With Veeam Agent for Microsoft Windows, you can easily back up your machine to an external hard drive, NAS share or a Veeam backup repository. And if you ever need to get your data back, there are multiple easy recovery options available.

☑ I agree to the Veeam End User License Agreement

4. After the installation process is complete, you can instruct Veeam Agent for Microsoft Windows to perform the following advanced actions:

   - Auto-configure settings for the backup job. To learn more, see Auto-Configuring Scheduled Backup Job.

   - 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 for Microsoft Windows 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:

- Microsoft SQL Server System CLR Types for SQL Server 2012
- Microsoft SQL Server 2012 Management Objects
- Microsoft SQL Server 2012 Express LocalDB Edition

Veeam Agent for Microsoft Windows will also set 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 Syntax

To install Veeam Agent for Microsoft Windows in the unattended mode, use a command with the following syntax:

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

where `<path_to_exe>` is a 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.
- 1101 — Veeam Agent for Microsoft Windows has been installed. The machine needs to be rebooted.

Using Sysprep and Veeam Agent for Microsoft Windows

You can pre-install Veeam Agent for Microsoft Windows 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 for Microsoft Windows:

1. Install Veeam Agent for Microsoft Windows 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 for Microsoft Windows. To learn more, see Configuring Backup Job.

> **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 key value: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Endpoint Backup\SysprepMode (DWORD)=1`.

   This registry key value is used to regenerate the job ID when Veeam Agent for Microsoft Windows starts for the first time on the new computer. If you do not create the registry key 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 key 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 https://technet.microsoft.com/en-us/library/dd349343.aspx.

When you deploy the created image on the computer, Veeam Agent for Microsoft Windows will re-generate its internal ID of the backup job. As a result, the backup job will be fully functional.

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 for Microsoft Windows Control Panel when the new version becomes available. To learn how to check for product updates, see Checking for New Product Versions and Updates.

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

To upgrade 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. Open the **About** tab.
3. If the new version of Veeam Agent for Microsoft Windows is available, click **Download**.
4. When the download is complete, click **Install** to run the setup archive.
5. To upgrade Veeam Agent for Microsoft Windows, you must accept the license agreement. Read the license agreement, select the **I agree to the Veeam End User License Agreement** check box and click **Update**.

> **NOTE:**
>
> Consider the following:
>
> - In some cases, upgrade to the new version of Veeam Agent for Microsoft Windows may require computer reboot.
> - You can also download the Veeam Agent for Microsoft Windows setup archive from the Veeam Download page at https://www.veeam.com/downloads.html. 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.

Unattended Upgrade

You can upgrade Veeam Agent for Microsoft Windows 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.

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 for Microsoft Windows and select **Uninstall**. Wait for the process to complete.

The LocalDB and other prerequisite components installed and used by Veeam Agent for Microsoft Windows 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

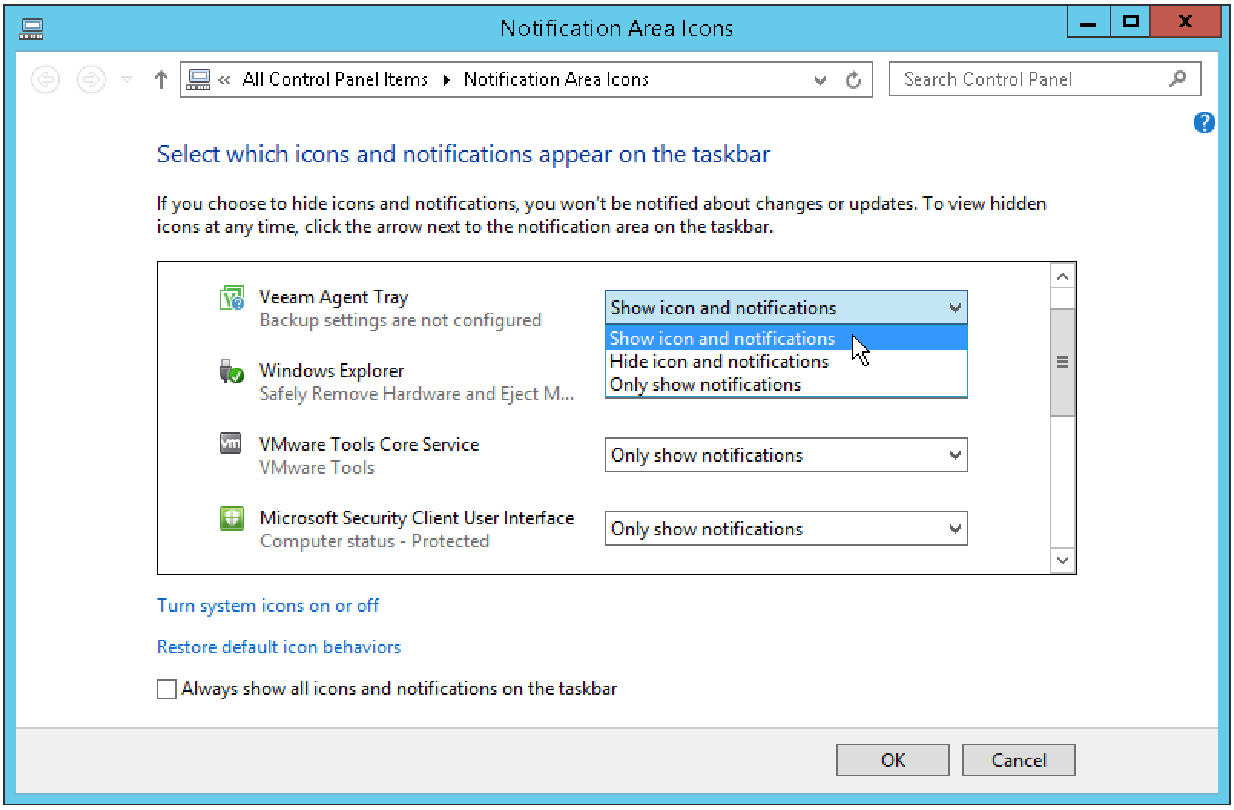
After the product installation, Veeam Agent for Microsoft Windows displays its icon in the system tray. You can use the system tray icon to perform main operations in Veeam Agent for Microsoft Windows:

- Configure the backup job and start ad-hoc backup operations
- Launch restore wizards
- Open the Veeam Agent for Microsoft Windows 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 Icons** view. To do this, do either of the following:
    - Click the arrow in the system tray and click the **Customize** link.
    - From the Microsoft Windows main menu, select **Control Panel** and navigate to **Appearance and Personalization**. In the **Taskbar** section, select **Customize icons on the taskbar**.
2. In the **Notification Area Icons** window, find Veeam Agent Tray.
3. In the **Behaviors** column, set the **Show icon and notification** setting for it.
4. Click **OK**.



Select which icons and notifications appear on the taskbar

If you choose to hide icons and notifications, you won't be notified about changes or updates. To view hidden icons at any time, click the arrow next to the notification area on the taskbar.

Veeam Agent Tray Backup settings are not configured	Show icon and notifications Show icon and notifications Hide icon and notifications Only show notifications
Windows Explorer Safely Remove Hardware and Eject M...	
VMware Tools Core Service VMware Tools	Only show notifications
Microsoft Security Client User Interface Computer status - Protected	Only show notifications

☐ Always show all icons and notifications on the taskbar

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 the 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 scheduled 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 Performing Backup.

3. **Specify Veeam Agent for Microsoft Windows settings**.

   You can define resource usage settings during backup, instruct Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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.

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.
- Back up your data. 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 Performing Backup.

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).

Note 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 process, 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, 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 https://technet.microsoft.com/en-us/library/hh994698.aspx.

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 https://technet.microsoft.com/en-us/library/hh994698.aspx.

Local Target and Shared Folder Scenario (ISO)

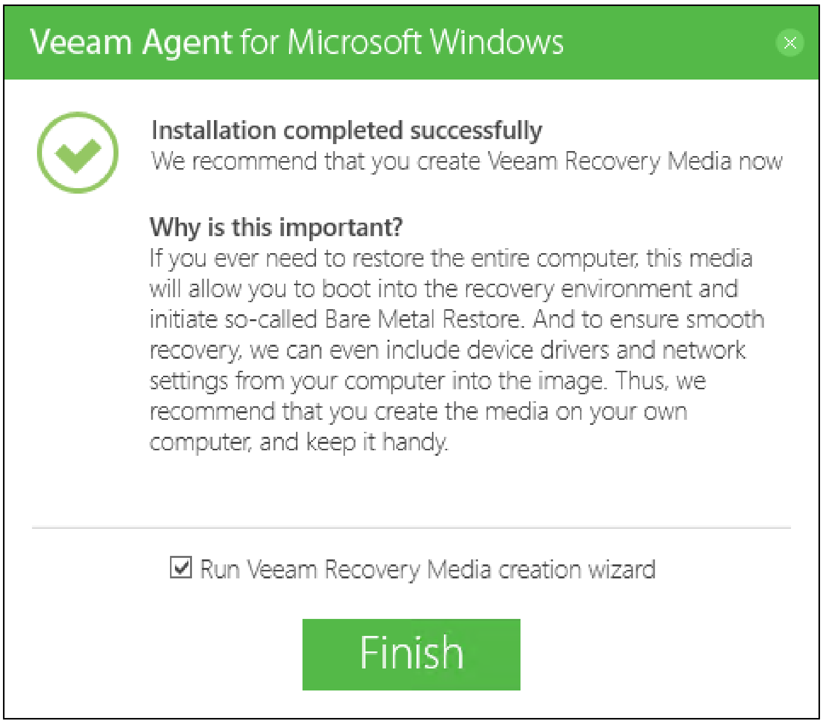
- If you want to include specific storage and network drivers into the recovery image, place them to a local folder on your computer or in a network shared folder on which you have read permissions. During the recovery image creation, you will be able to define a path to this folder, and Veeam Agent 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 https://technet.microsoft.com/en-us/library/hh994698.aspx.

Step 1. Launch Create Recovery Media Wizard

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

To launch the **Create Veeam 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 Veeam Recovery Media** wizard.



Veeam Agent for Microsoft Windows

Installation completed successfully

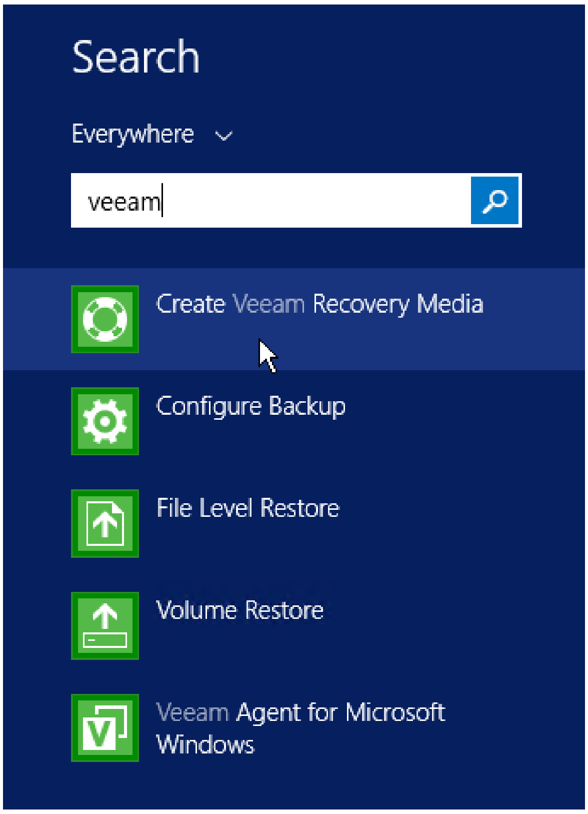
We recommend that you create Veeam Recovery Media now

Why is this important?

If you ever need to restore the entire computer, this media will allow you to boot into the recovery environment and initiate so-called Bare Metal Restore. And to ensure smooth recovery, we can even include device drivers and network settings from your computer into the image. Thus, we recommend that you create the media on your own computer, and keep it handy.

☑ Run Veeam Recovery Media creation wizard

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



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.

   This option is unavailable in the following cases:

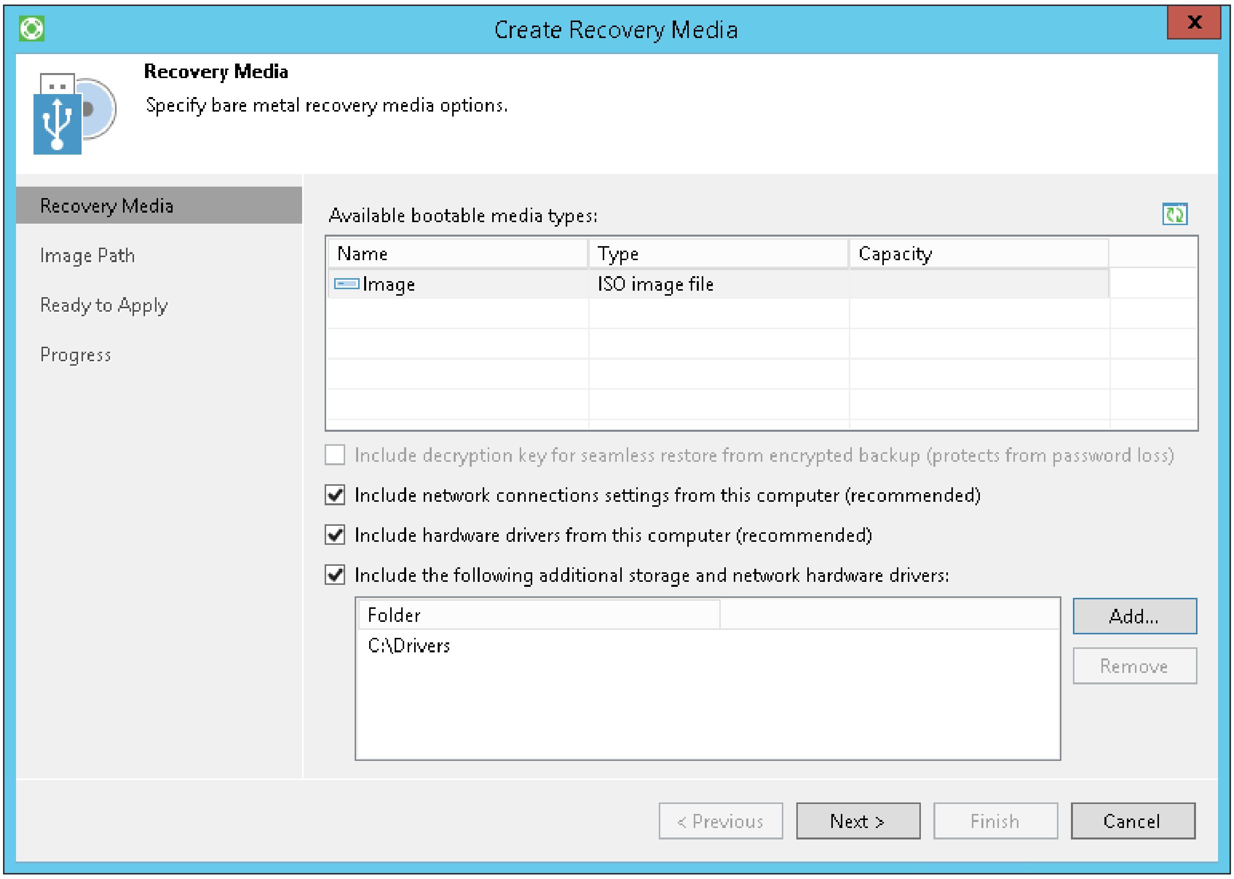
   - If data encryption options are not enabled for the backup job in Veeam Agent for Microsoft Windows at the time when you start the **Create Recovery Media** wizard.
   - If the backup job is targeted at a Veeam backup repository with data encryption options enabled in Veeam Backup & Replication.

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).

   It is strongly recommended 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.



Recovery Media

Specify bare metal recovery media options.

Available bootable media types:

Name	Type	Capacity
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

IMPORTANT!

Mind 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.
- It is not recommended that you 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.

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.

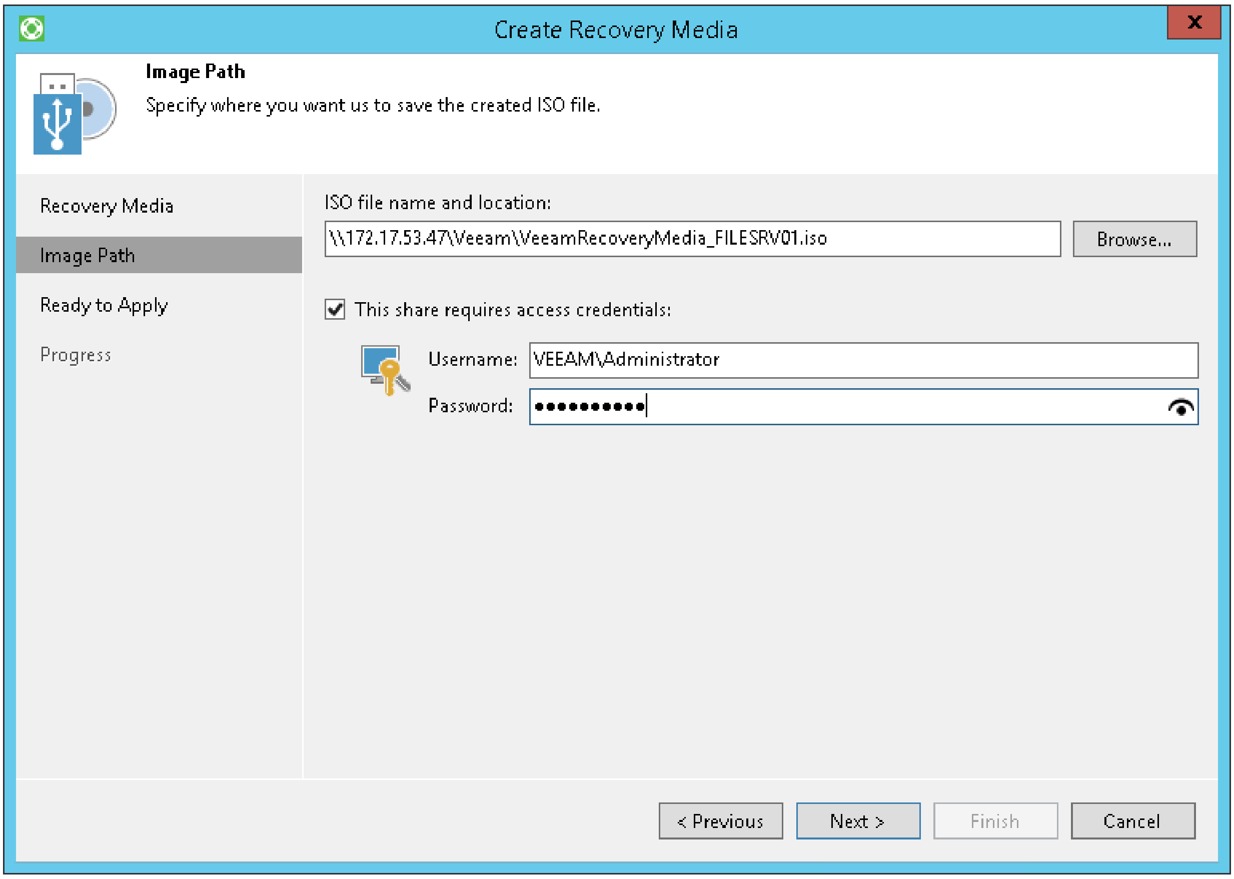
1. In the **ISO file name and location** field, specify a real path to the folder where you want to save the created recovery image and the ISO file name. You can save the ISO file in the following locations:

    - 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 (\\).

    It is strongly recommended 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.



Create Recovery Media

Image Path

Specify where you want us to save the created ISO file.

ISO file name and location: \\172.17.53.47\Veeam\VeeamRecoveryMedia_FILESRV01.iso

☑ This share requires access credentials:

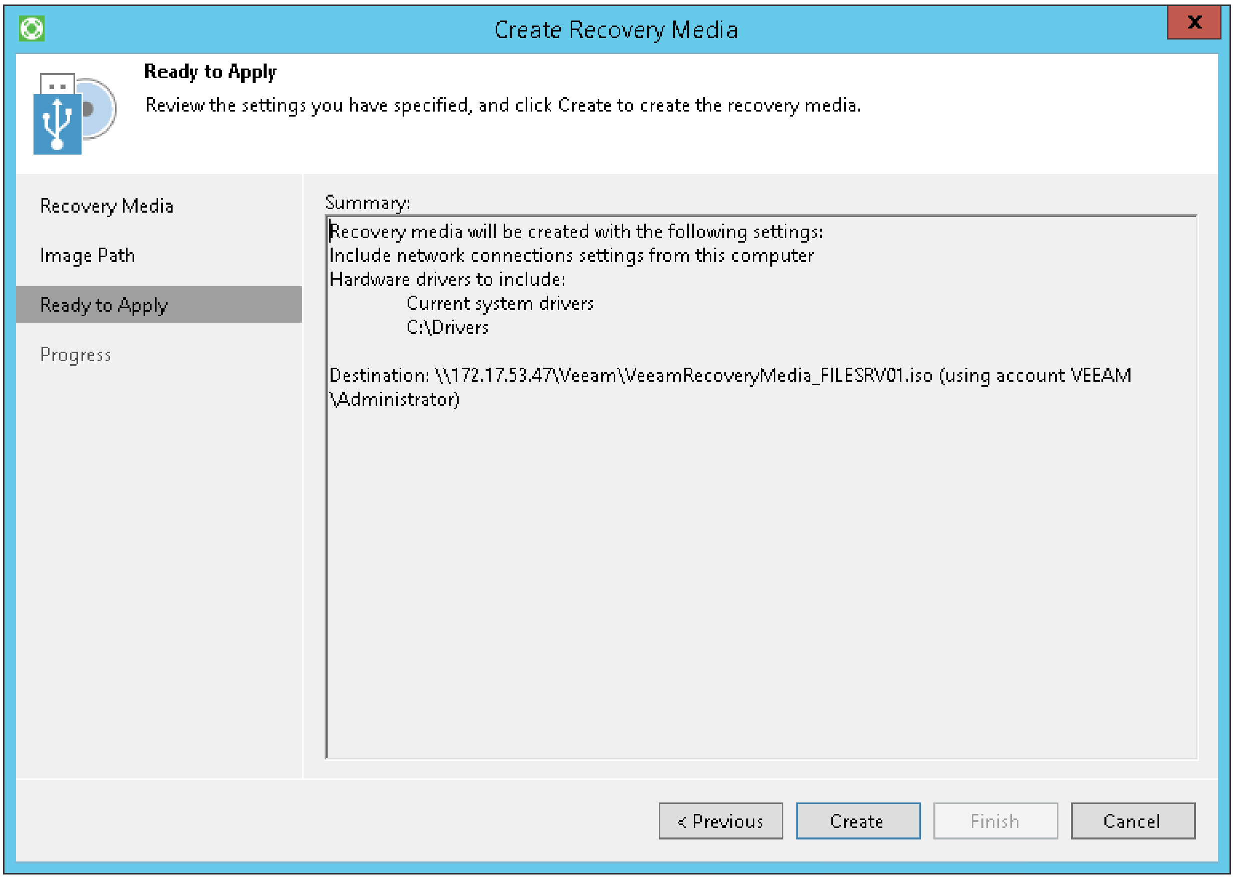
Username: VEEAM\Administrator

Password: ●●●●●●●●●●●

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.



Ready to Apply

Review the settings you have specified, and click Create to create the recovery media.

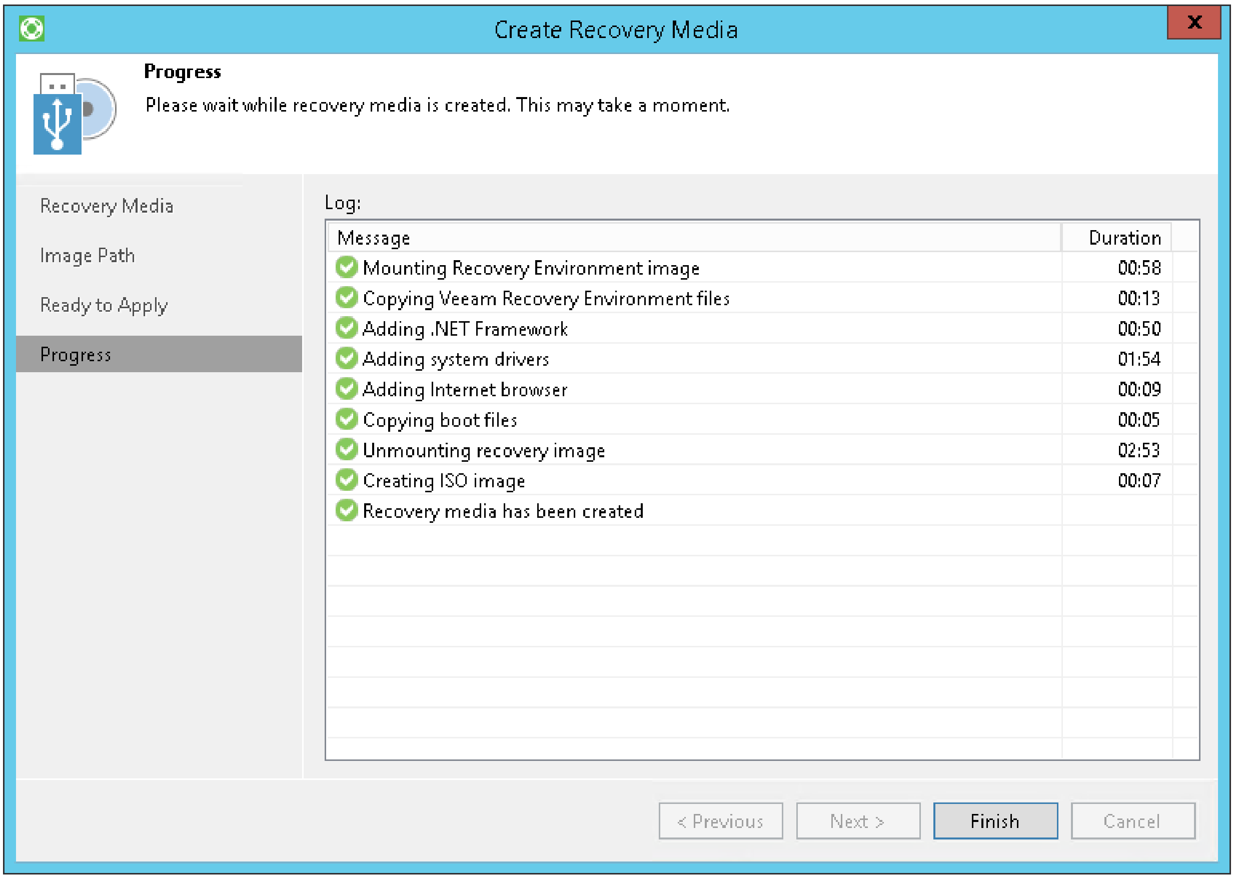
Summary:

```
Recovery media will be created with the following settings:
Include network connections settings from this computer
Hardware drivers to include:
          Current system drivers
          C:\Drivers

Destination: \\172.17.53.47\Veeam\VeeamRecoveryMedia_FILESRV01.iso (using account VEEAM
\Administrator)
```

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.



Message	Duration
✓ Mounting Recovery Environment image	00:58
✓ Copying Veeam Recovery Environment files	00:13
✓ Adding .NET Framework	00:50
✓ Adding system drivers	01:54
✓ Adding Internet browser	00:09
✓ Copying boot files	00:05
✓ Unmounting recovery image	02:53
✓ Creating ISO image	00:07
✓ Recovery media has been created	

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.

Performing Backup

You can back up your data to protect the entire computer image, individual volumes or folders on your computer. Veeam Agent for Microsoft Windows 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.

Auto-Configuring Scheduled Backup Jobs

After the product installation, you can instruct Veeam Agent for Microsoft Windows to auto-configure the scheduled backup job with the default settings. The backup job will have the following settings:

- Backup scope: entire computer
- Target destination: USB drive connected to the computer
- Schedule: 12:30 AM nightly

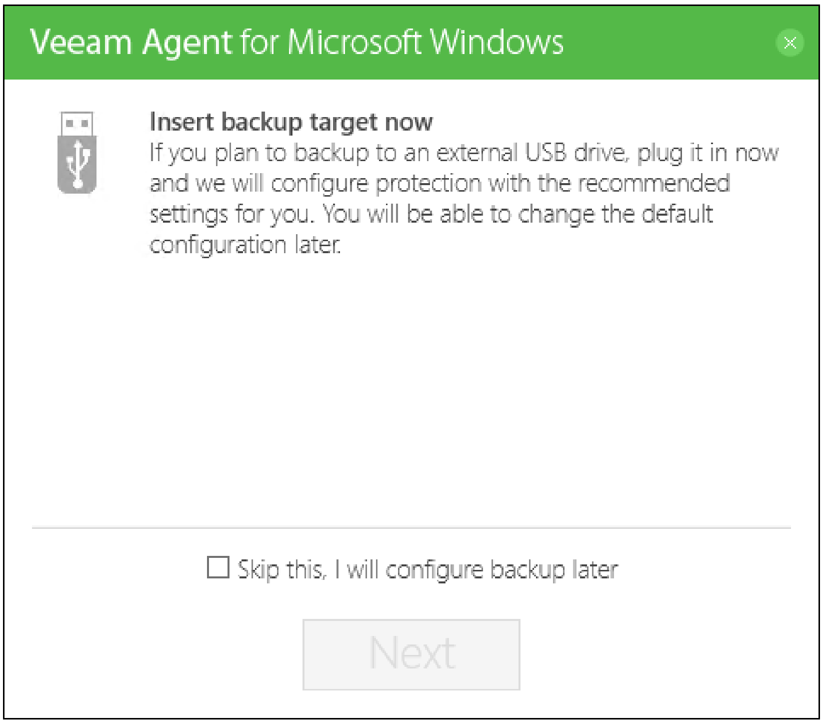
That is, the scheduled backup job will run regularly to create an entire computer backup at 12:30 AM and save this backup on the USB drive.

To auto-configure the scheduled backup job:

1. At the **Insert backup target now** step of the setup wizard, make sure that the **Skip this, I will configure backup later** check box is not selected.
2. Insert a USB drive to a USB slot on your computer.
3. Follow the steps of the installation wizard. At the last step of the wizard, click **Finish**.

IMPORTANT!

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



Insert backup target now

If you plan to backup to an external USB drive, plug it in now and we will configure protection with the recommended settings for you. You will be able to change the default configuration later.

□ Skip this, I will configure backup later

Configuring Backup Job

To back up your data, you must configure the 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.
- 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 support the desired product functionality. 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 9.5 Update 3 or later. If you plan to use a commercial version of Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install the Veeam Agent license in Veeam Backup & Replication in advance.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. 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.
- [For Microsoft OneDrive targets] To log in to Microsoft OneDrive, Veeam Agent for Microsoft Windows uses the Internet Explorer web browser. ActiveX and JavaScript must be enabled in the web browser settings.
- A user account under which you launch the **Configure Backup** 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.

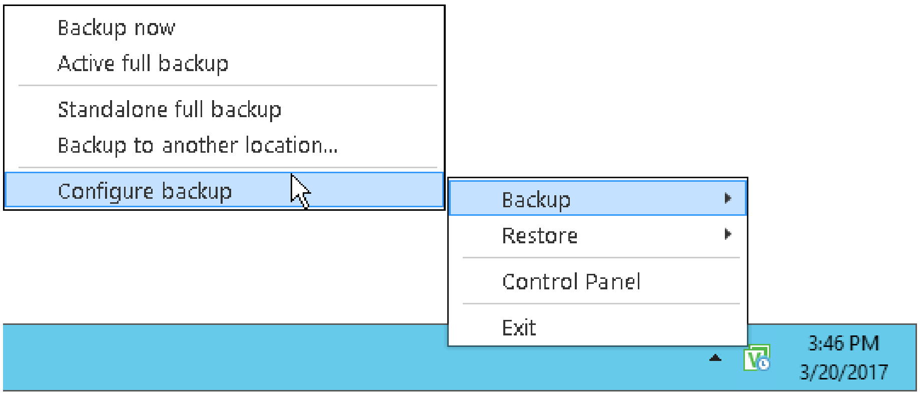
Backup has the following limitations:

- 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.

Step 1. Launch Configure Backup Wizard

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

- [If the backup job is not 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**.
- From the main 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. Select Backup Mode

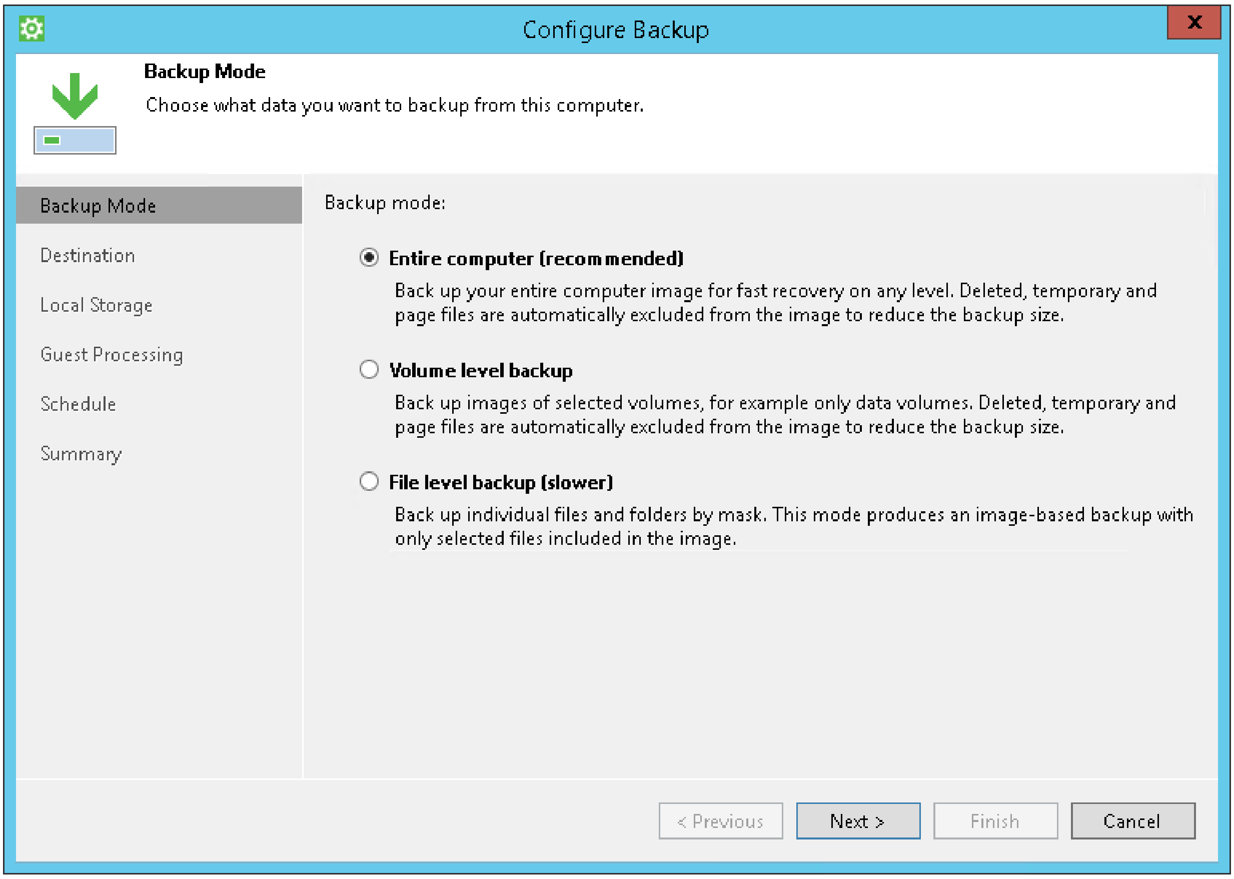
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup.

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. With this option selected, you will pass to the Files step of the wizard.

TIP:

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



Backup Mode

Choose what data you want to backup from this computer.

Backup mode:

● **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.

○ **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.

Step 3. 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. In the **Objects to backup** list, choose volumes and items that you want to include in the backup.

You can back up the following data:

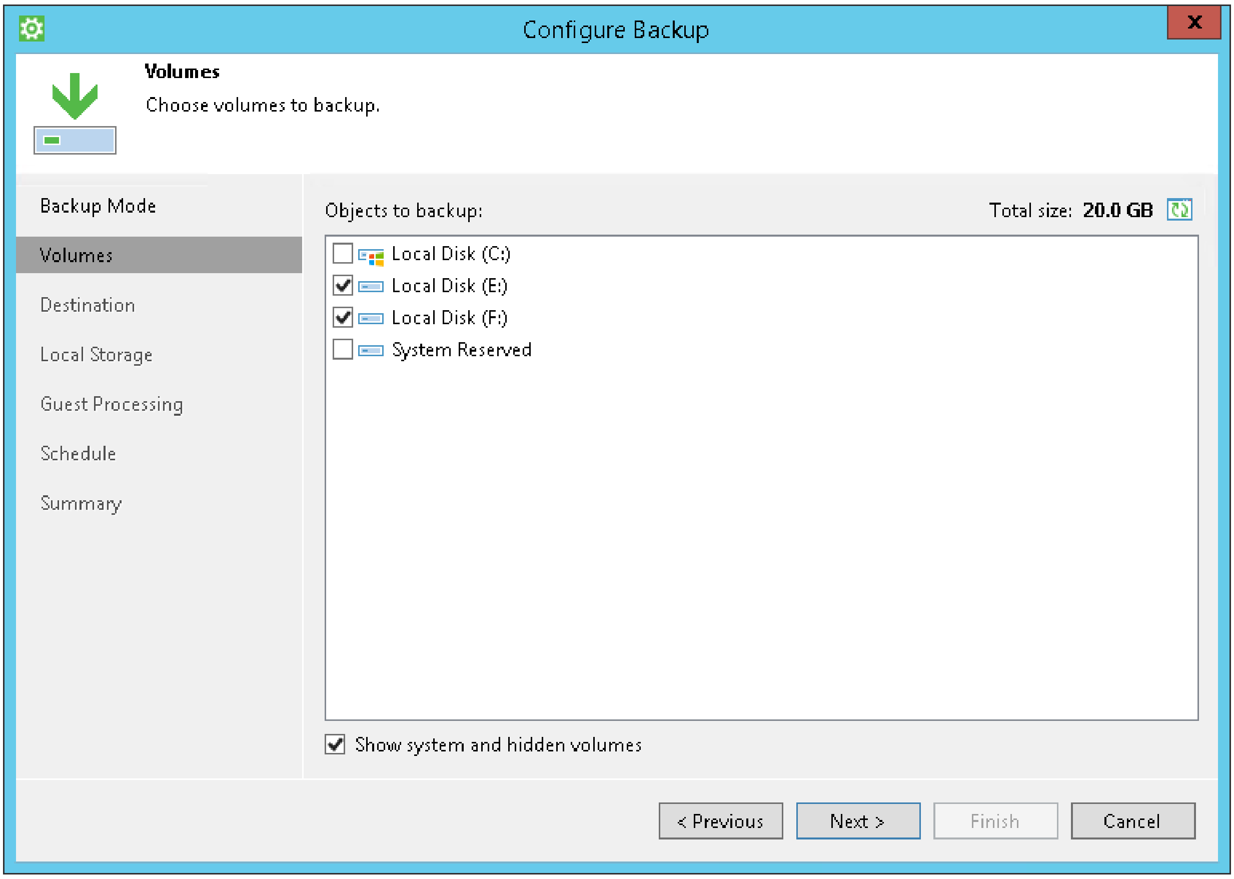
- Computer volumes. To include individual volumes of your computer to the backup scope, select check boxes next to necessary volumes.
- System state data. To include system state data into the backup, select the **Show system and hidden volumes** check box at the bottom of the window. In the **Objects to backup** list, select the **System Reserved** check box.

  With this option enabled, 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, 8.1, 10, 2012 and 2012 R2, Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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** check box. However, in this case Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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.



Objects to backup:

Total size: **20.0 GB**

- □ Local Disk (C:)
- ☑ Local Disk (E:)
- ☑ Local Disk (F:)
- □ System Reserved

☑ Show system and hidden volumes

Selecting Folders to Back Up

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

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

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

- Operating system data — data pertaining to the OS installed on your computer.
- Personal files — user profile folder including all user settings and data. Typically, the user profile data is located in the *Users* folder on the system disk, for example, `C:\Users`.
- 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, 8.1, 10,

2012 and 2012 R2, Veeam Agent for Microsoft Windows will additionally back up the recovery partition. To learn more, see System State Data Backup.

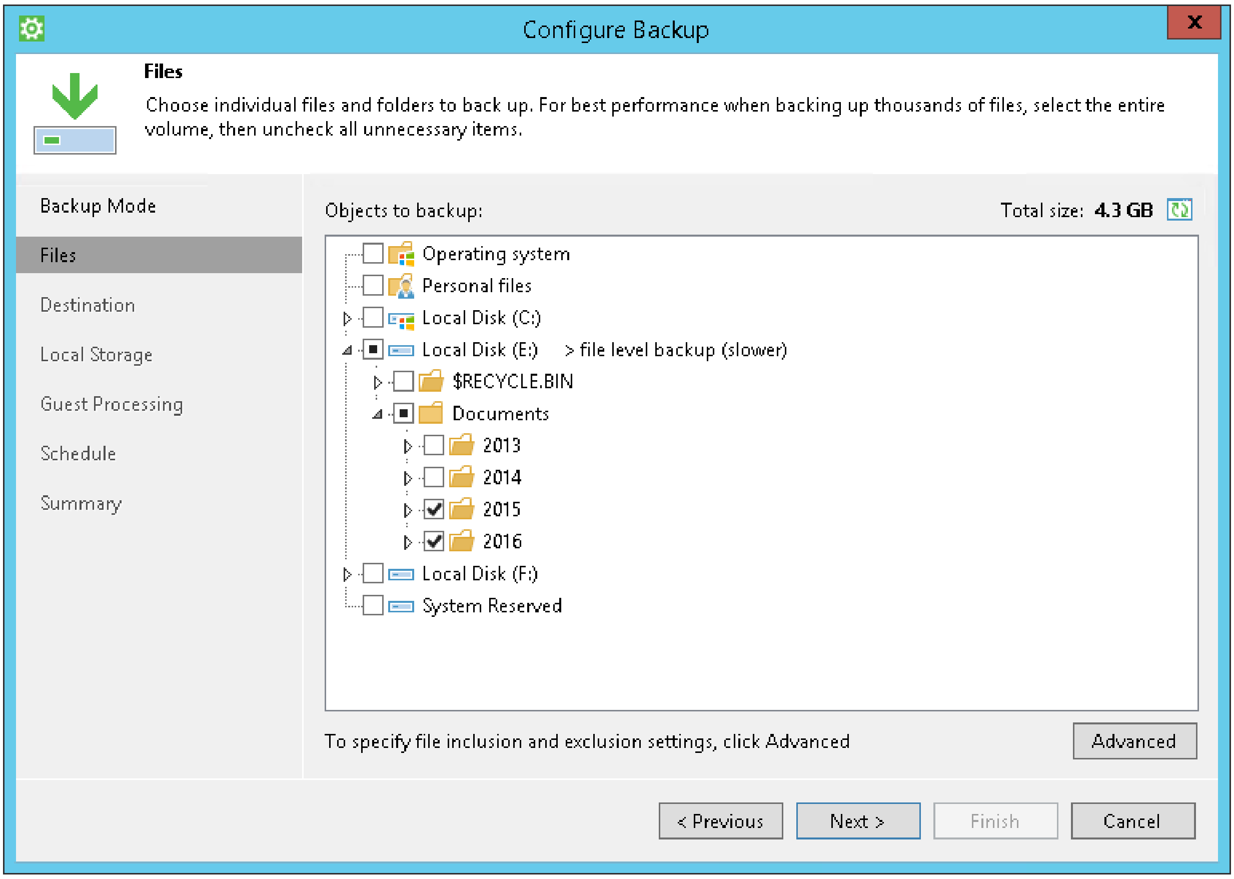
- Individual folders. To include
- Individual computer volumes.

If you include a specific computer volume in the backup, you can exclude one or more folders that reside on this volume from the backup. To exclude a folder, in the **Objects to backup** list expand the volume that you have selected for backup and clear the check box next to the necessary folder.

If you choose to back up personal files or include one or more individual folders in the backup, you can configure filters to include or exclude files of a specific type in/from the backup. To learn more, see Configuring Filters.

NOTE:

Veeam Agent for Microsoft Windows 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.



Files

Choose individual files and folders to back up. For best performance when backing up thousands of files, select the entire volume, then uncheck all unnecessary items.

Objects to backup: Total size: **4.3 GB**

- □ Operating system
- □ Personal files
- □ Local Disk (C:)
- ■ Local Disk (E:) > file level backup (slower)
  - □ $RECYCLE.BIN
  - ■ Documents
    - □ 2013
    - □ 2014
    - ☑ 2015
    - ☑ 2016
- □ Local Disk (F:)
- □ System Reserved

To specify file inclusion and exclusion settings, click Advanced [Advanced]

Configuring Filters

To include or exclude files of a specific type in/from the file-level backup, you can configure filters. Veeam Agent for Microsoft Windows applies filters to specific folders that you include in the backup. Filters are not applied to computer volumes selected for backup.

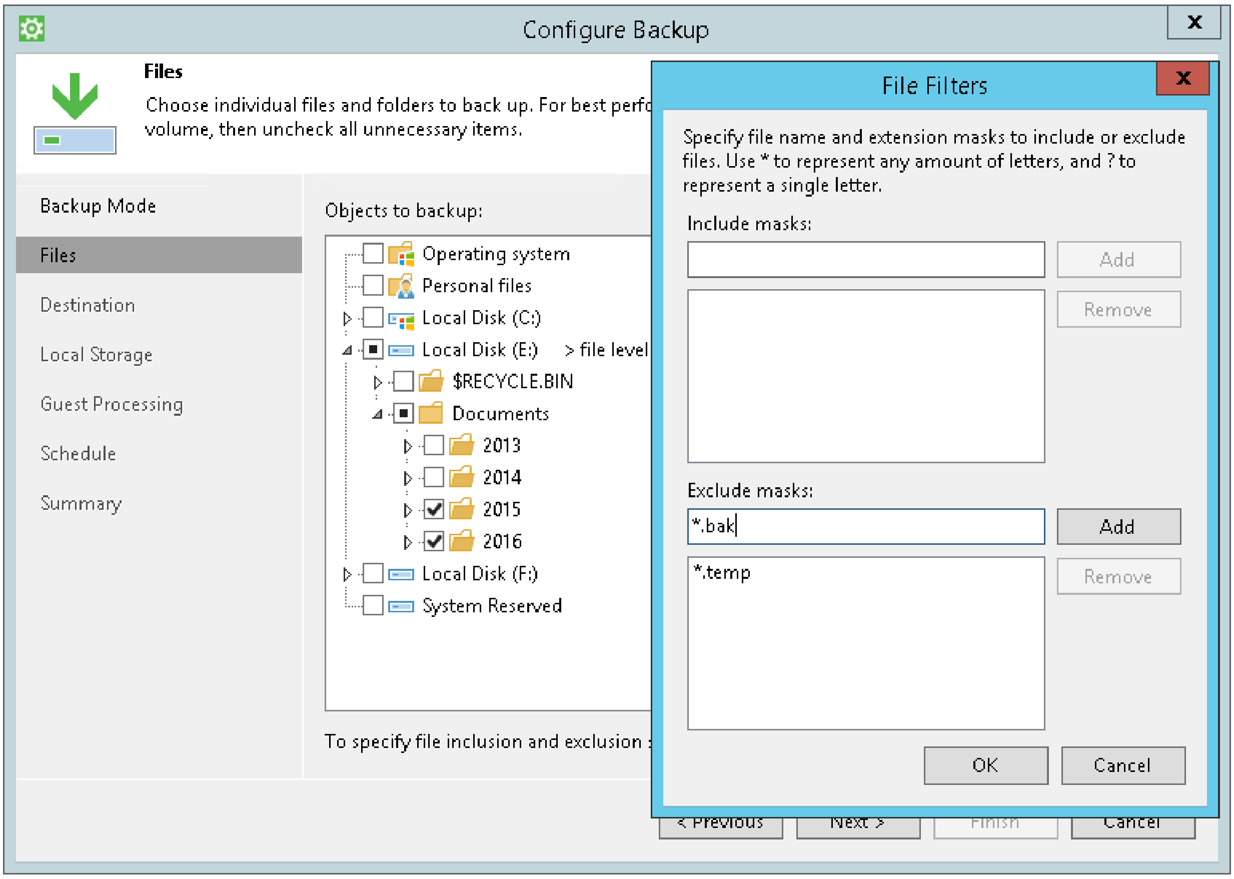
To configure a filter:

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

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

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

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



Configure Backup

Files

Choose individual files and folders to back up. For best perfo
volume, then uncheck all unnecessary items.

Objects to backup:

- □ Operating system
- □ Personal files
- □ Local Disk (C:)
- ■ Local Disk (E:) > file level
  - □ $RECYCLE.BIN
  - ■ Documents
    - □ 2013
    - □ 2014
    - ☑ 2015
    - ☑ 2016
- □ Local Disk (F:)
- □ System Reserved

To specify file inclusion and exclusion

File Filters

Specify file name and extension masks to include or exclude files. Use * to represent any amount of letters, and ? to represent a single letter.

Include masks:

Exclude masks: *.bak

*.temp

Step 4. 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:

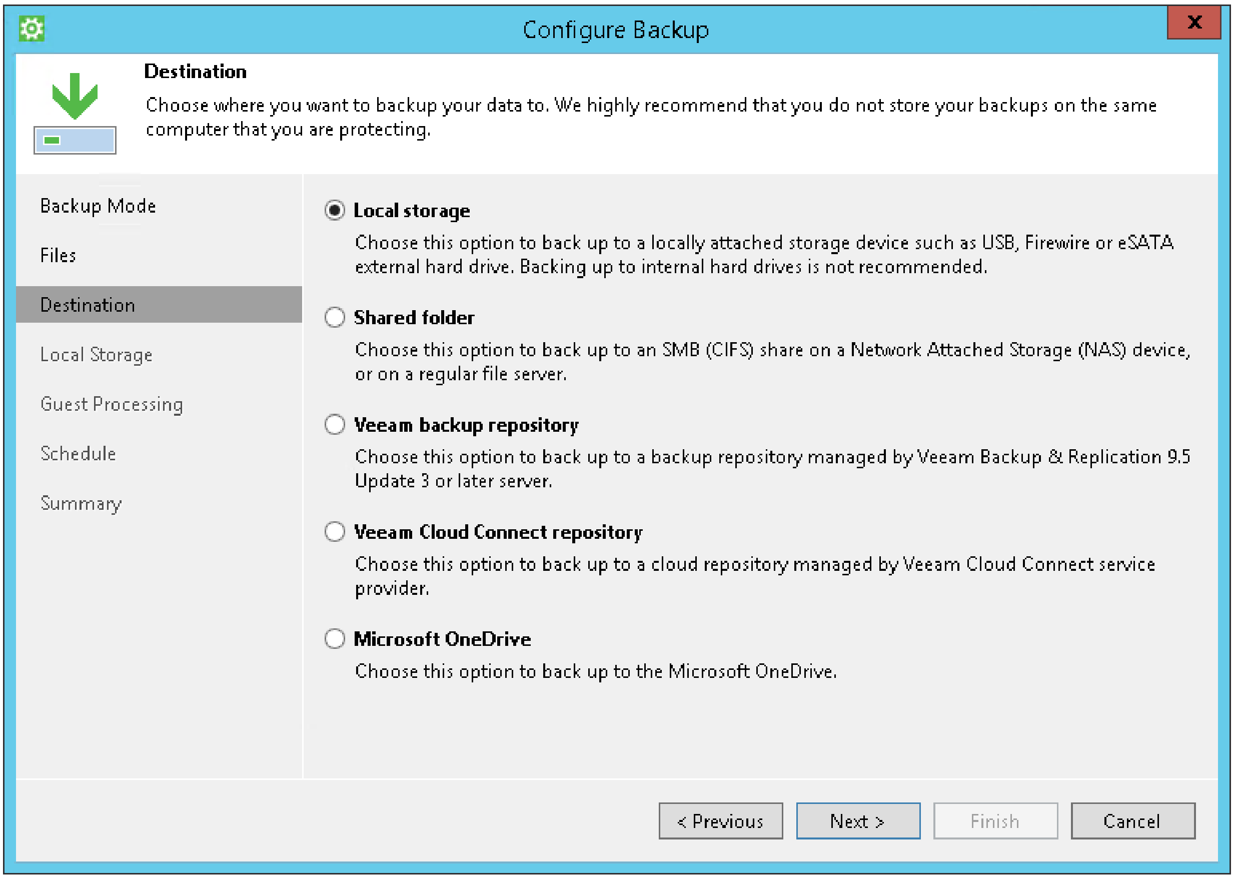
- **Local storage** — select this option if you want to save the backup on a removable storage device attached to the computer or on a local computer drive. With this option selected, you will pass to the Local Storage step of the wizard.

- **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 on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the Backup Server step of the wizard.

- **Veeam Cloud Connect repository** — select this option if you want to save the backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the Service Provider step of the wizard.

- **Microsoft OneDrive** — select this option if you want to save the backup in the Microsoft OneDrive cloud storage. With this option selected, you will pass to the Microsoft OneDrive step of the wizard.



Destination

Choose where you want to backup your data to. We highly recommend that you do not store your backups on the same computer that you are protecting.

● **Local storage**
Choose this option to 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.

○ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

○ **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication 9.5 Update 3 or later server.

○ **Veeam Cloud Connect repository**
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

○ **Microsoft OneDrive**
Choose this option to back up to the Microsoft OneDrive.

IMPORTANT!

Consider the following:

- It is strongly recommended 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 on a local folder included in the backup scope, Veeam Agent for Microsoft Windows will automatically exclude this folder from the backup.
- The **Veeam Cloud Connect repository** option is available in Workstation and Server editions of Veeam Agent for Microsoft Windows if the license is installed locally on the protected computer. To learn more, see Licensing.
- The **Microsoft OneDrive** option is not available if the Veeam Agent computer runs a Microsoft Windows Server OS.

Step 5. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- Local storage settings — if you have selected the **Local storage** option at the Destination step of the wizard.
- 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.
- Microsoft OneDrive settings — if you have selected the **Microsoft OneDrive** option at the Destination step of the wizard.

Local Storage Settings

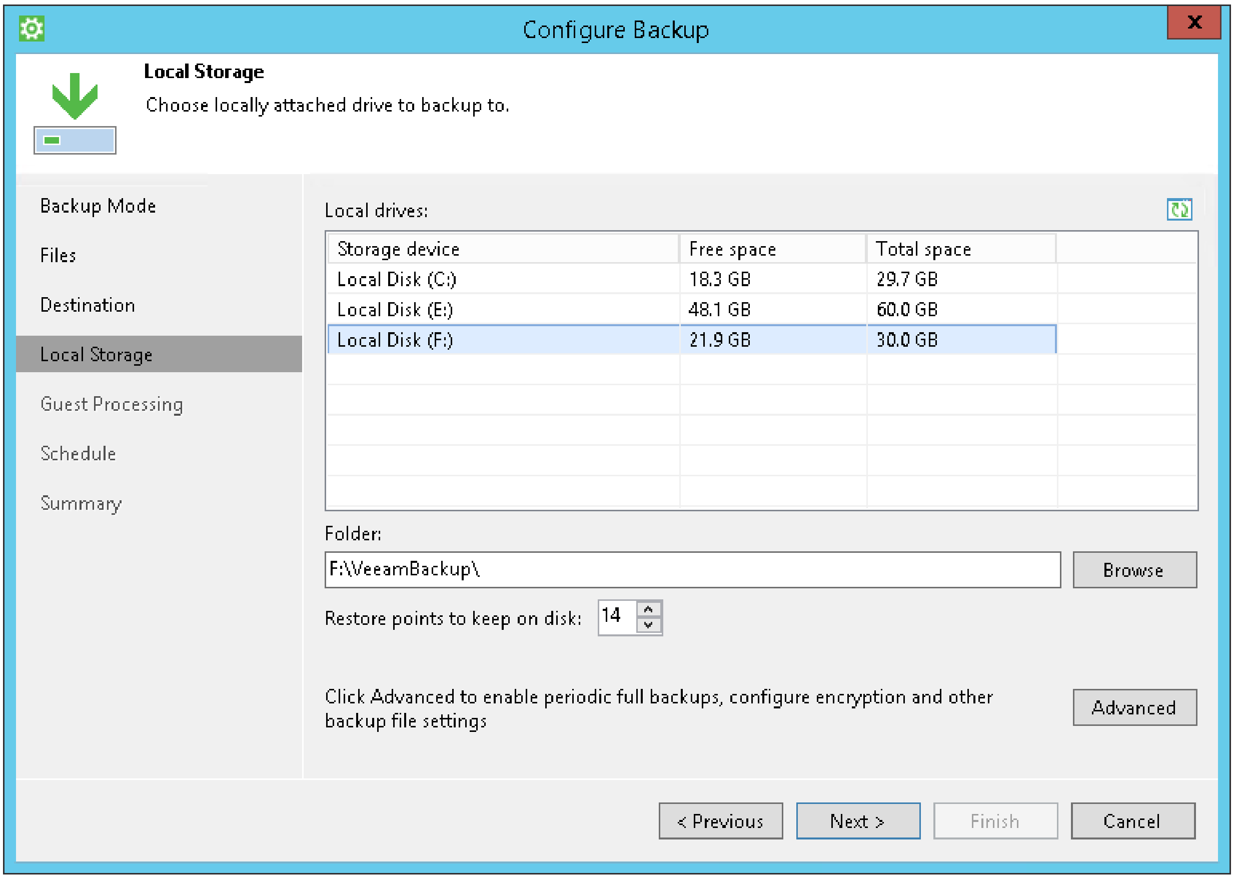
The **Local Storage** step of the wizard is available if you have chosen to save the backup on a local drive of your computer.

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 for Microsoft Windows saves files in the `VeeamBackup` folder.
3. Specify 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 14 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 **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 14 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

     To learn more, see Backup Retention Policy in Server Edition.
4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



Local Storage

Choose locally attached drive to backup to.

Local drives:

Storage device	Free space	Total space
Local Disk (C:)	18.3 GB	29.7 GB
Local Disk (E:)	48.1 GB	60.0 GB
Local Disk (F:)	21.9 GB	30.0 GB

Folder:

F:\VeeamBackup\

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

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

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 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 access permissions on this shared folder. The user name must be specified in the *DOMAIN\USERNAME* format.

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

   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 simply grant *Full Control* access on the shared folder and underlying file system to the computer account *(DOMAIN\COMPUTERNAME$*).

3. To view how much free space is available in the selected shared folder, click **Populate**.

4. Specify backup retention policy settings:

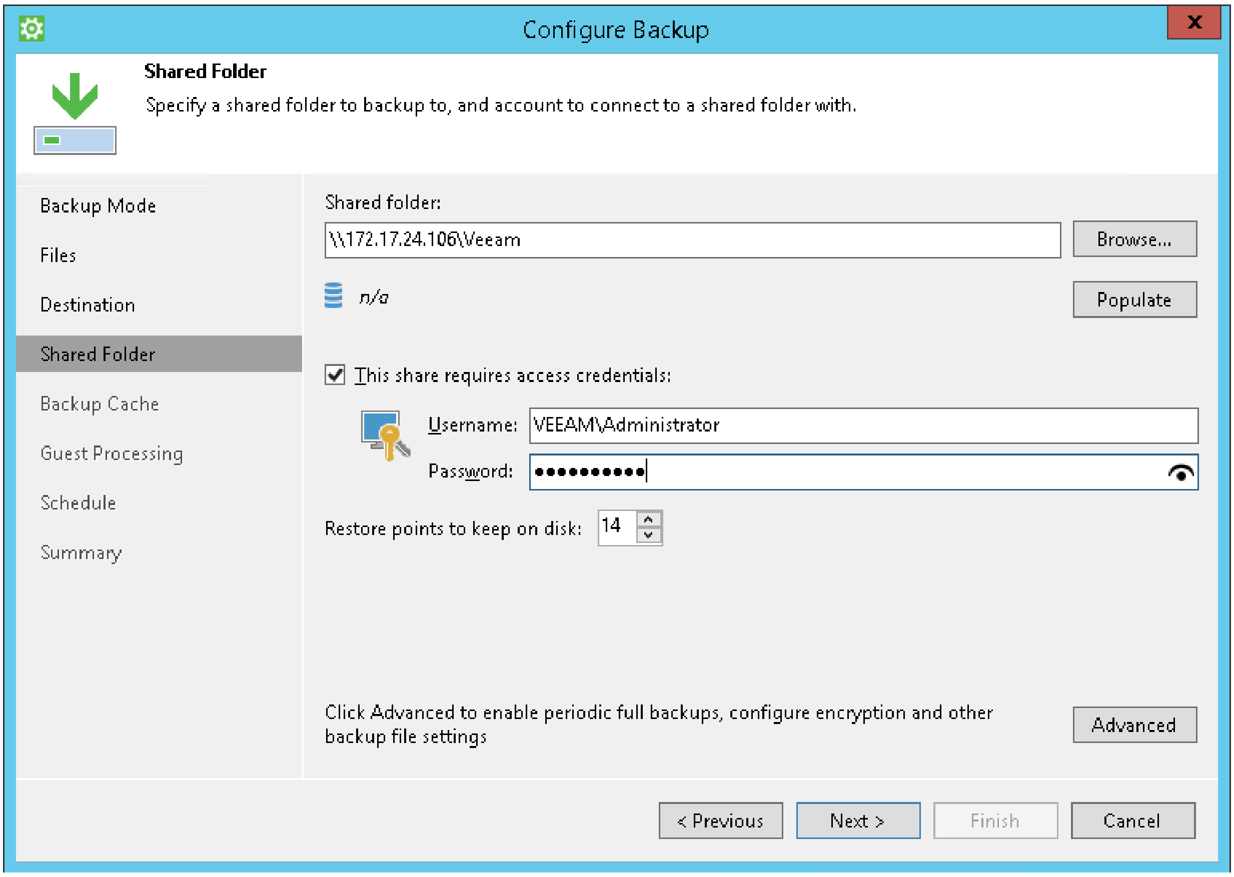
   - [For Free and Workstation product editions] In the **Keep restore points for the last <N> days when computer was used** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files for 14 days. After 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 **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 14 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

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

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



Shared Folder

Specify a shared folder to backup to, and account to connect to a shared folder with.

Shared folder: \\172.17.24.106\Veeam

n/a

☑ This share requires access credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

Veeam Backup Repository Settings

If you have selected to store backup files on 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 on 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. 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 simply add the computer account (*DOMAIN\COMPUTERNAME$*) to an AD group and grant access rights on the backup repository to this group.

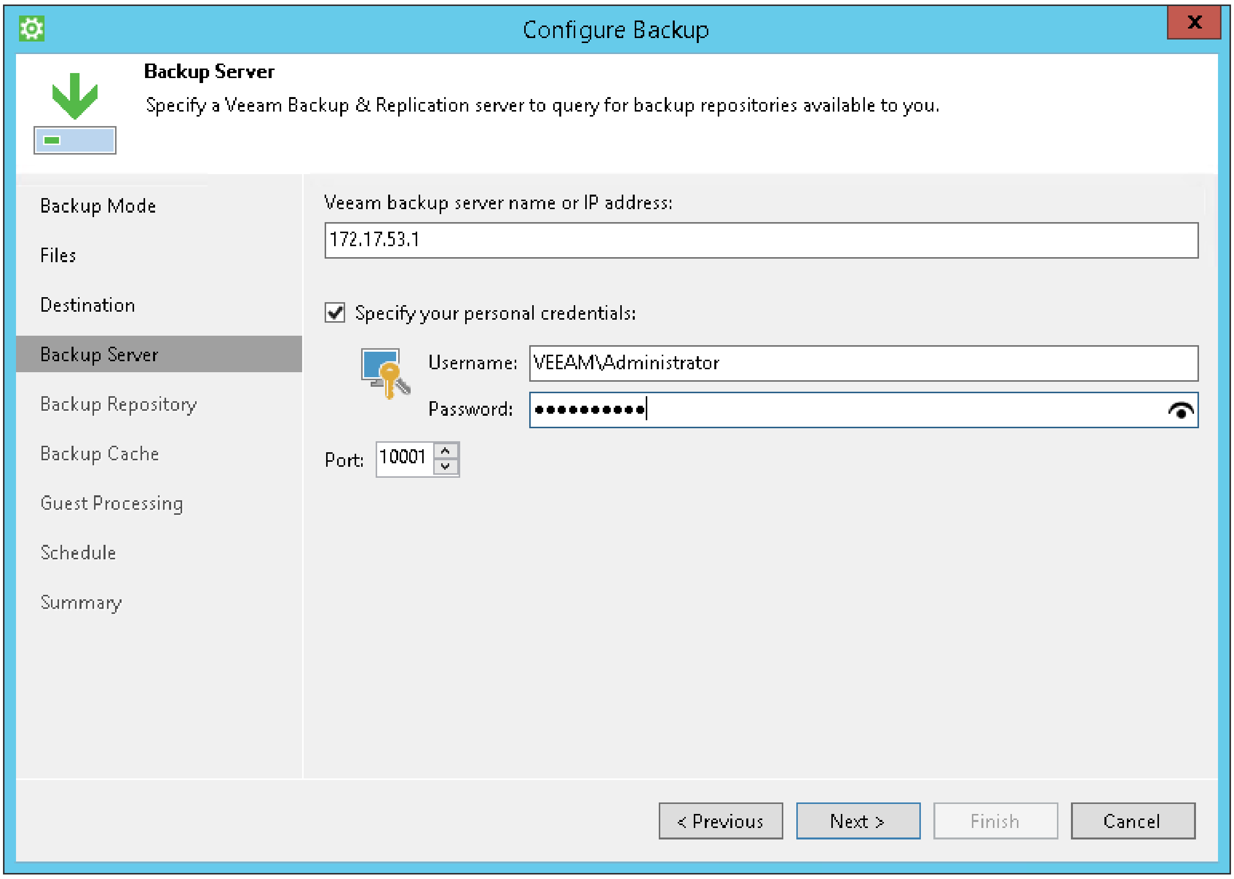
Setting access permissions on the backup repository to *Everyone* is equal to granting access rights to the *Everyone* Microsoft Windows group (*Anonymous* users are excluded). If you have set such permissions on the backup repository, you can omit specifying credentials. However, this scenario is recommended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

3. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup repository. By default, Veeam Agent for Microsoft Windows uses port 10001.

IMPORTANT!

Mind the following:

- If you plan to use a commercial version of Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install the Veeam Agent license in Veeam Backup & Replication in advance, before connecting to the backup server.
- If you specify a DNS name of the Veeam backup server, make sure that the Veeam backup server name is resolved into IPv4 address on the machine where Veeam Agent for Microsoft Windows is installed. The Veeam Backup Service in Veeam Backup & Replication listens on IPv4 addresses only. If the Veeam backup server name is resolved into IPv6 address, Veeam Agent for Microsoft Windows will fail to connect to the Veeam backup server.



Veeam backup server name or IP address: 172.17.53.1

☑ Specify your personal credentials:

Username: VEEAM\Administrator

Password: ••••••••••

Port: 10001

Selecting Backup Repository

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

Specify settings for the target backup repository:

1. From the **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 **Configure Backup** wizard. To learn more, see Setting Up User Permissions on Backup Repositories.

2. Specify backup retention policy settings:

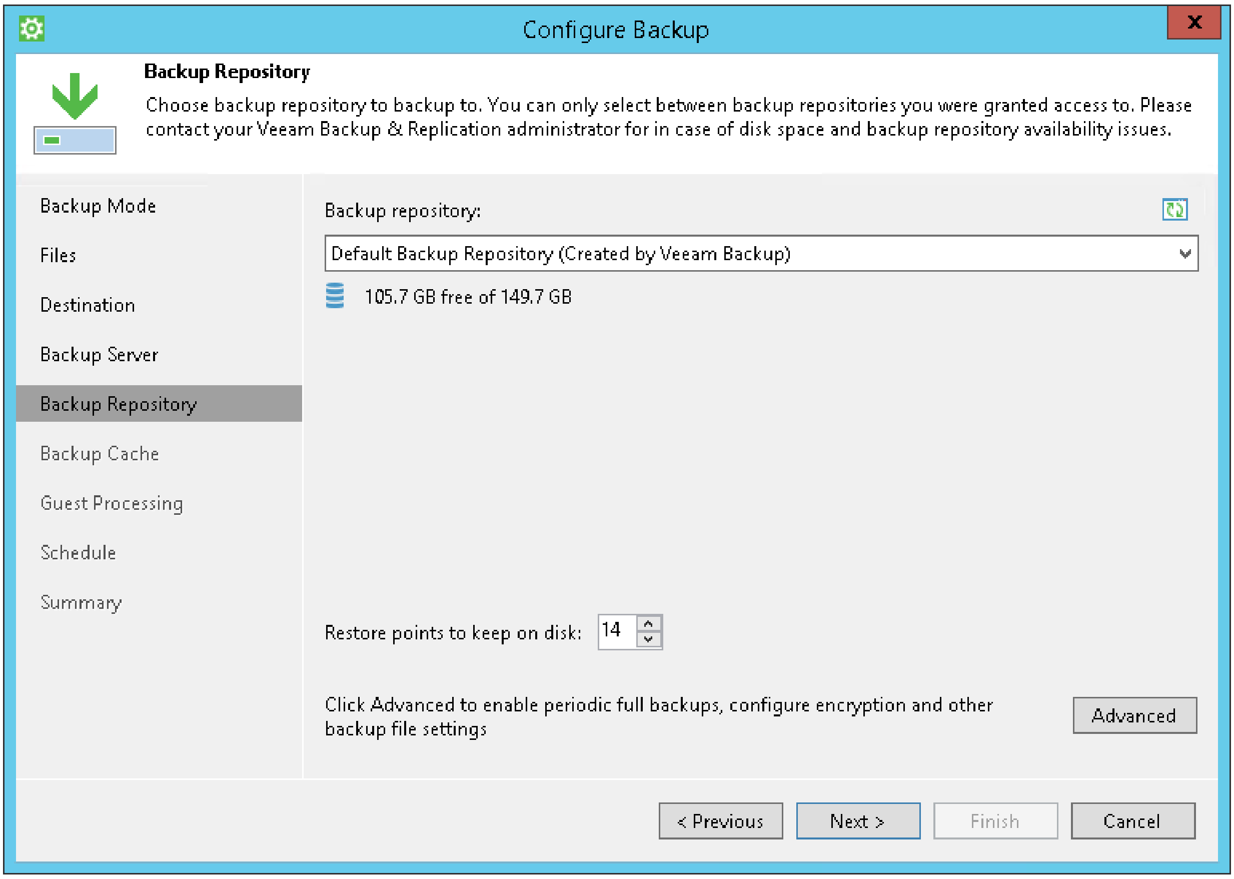
   - [For Free and Workstation product editions] In the **Keep restore points for the last <N> days when computer was used** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files for 14 days. After 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 **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 14 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

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

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



Configure Backup

Backup Repository

Choose backup repository to backup to. You can only select between backup repositories you were granted access to. Please contact your Veeam Backup & Replication administrator for in case of disk space and backup repository availability issues.

Backup repository: Default Backup Repository (Created by Veeam Backup)

105.7 GB free of 149.7 GB

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

Veeam Cloud Connect Repository Settings

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

1. Specify service provider settings.
2. 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 on a Veeam Cloud Connect repository.

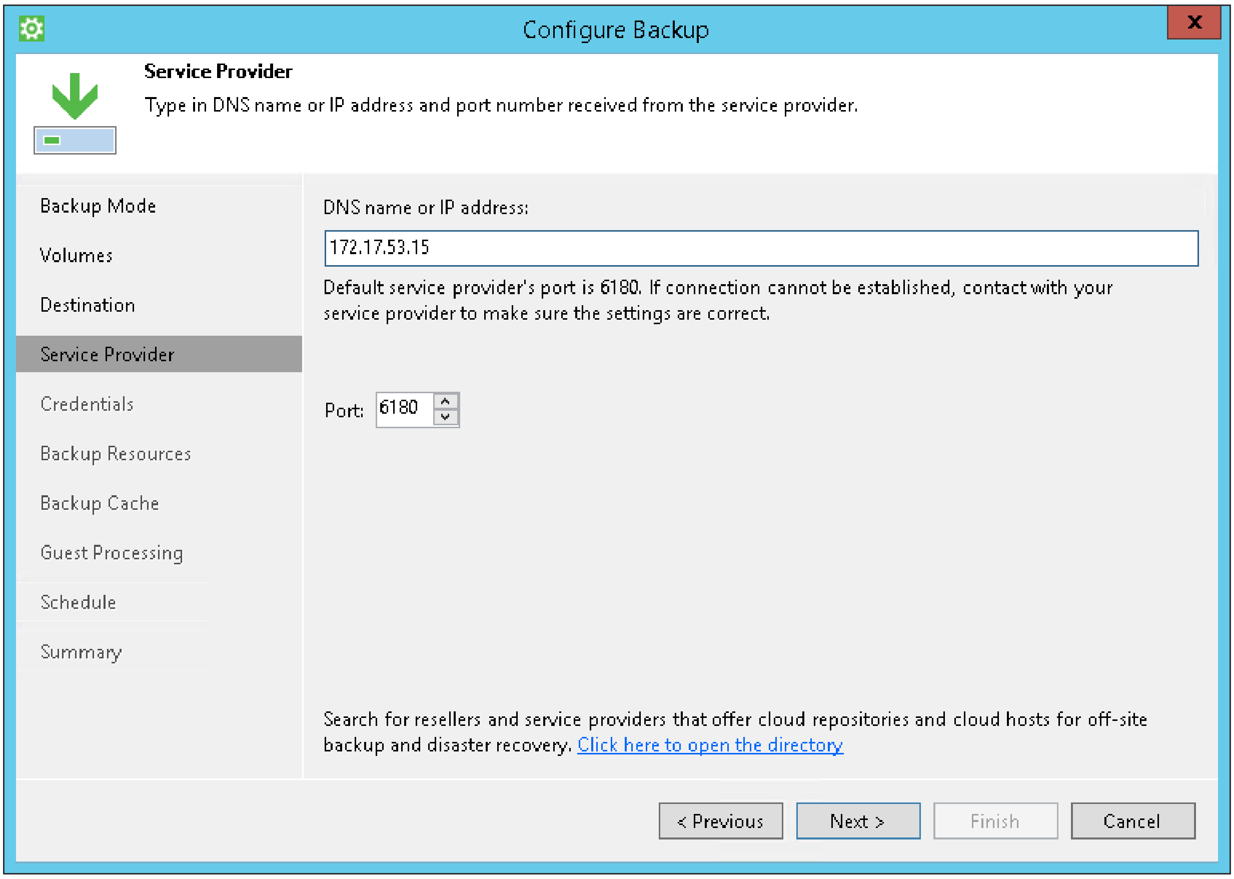
Specify settings for the cloud gateway that the SP or your backup administrator has provided to you:

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 web page on the Veeam website. Use the filter on the web page to find the necessary service provider by the type of provided cloud services, service provider datacenter location or service area.



Configure Backup

Service Provider

Type in DNS name or IP address and port number received from the service provider.

DNS name or IP address: 172.17.53.15

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

Port: 6180

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

Specifying User Account Settings

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

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.

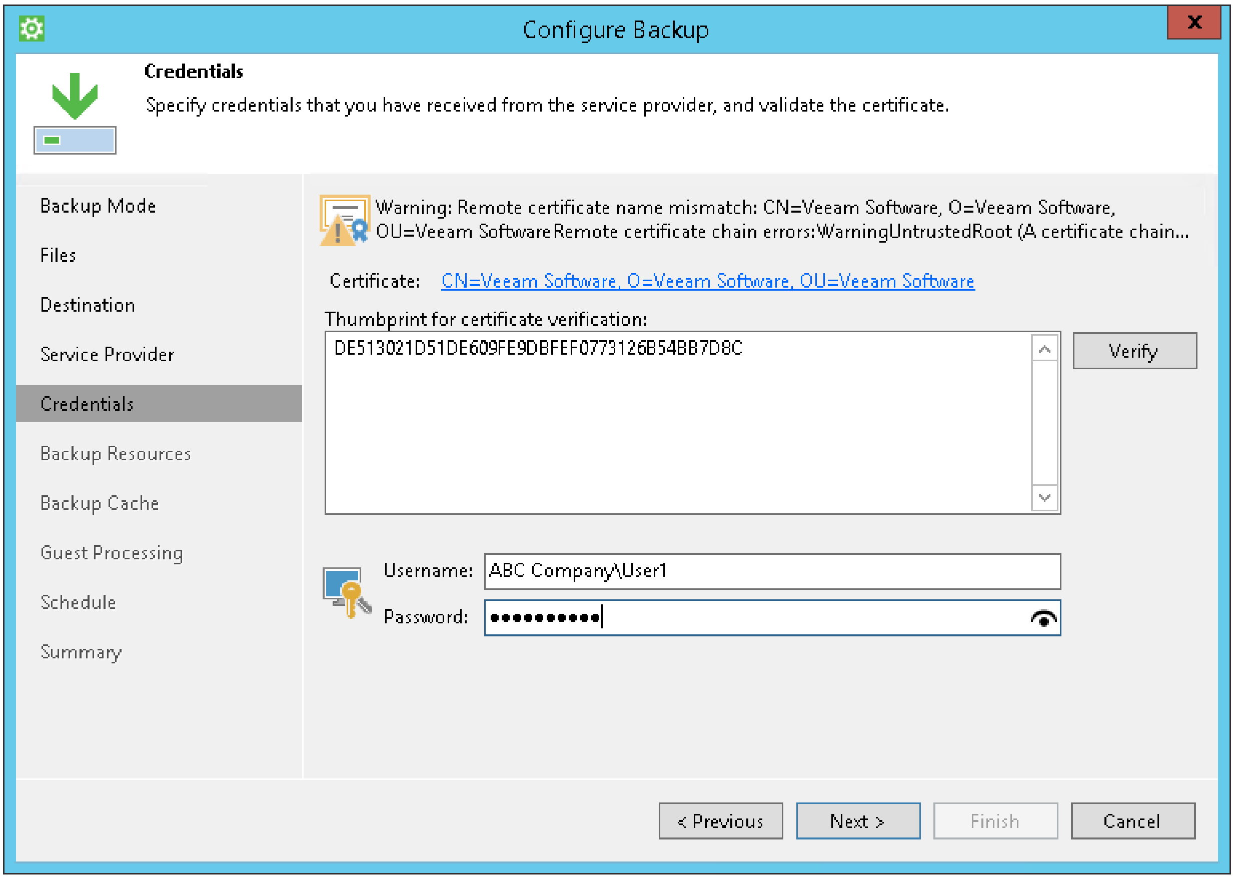
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   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.



Warning: Remote certificate name mismatch: CN=Veeam Software, O=Veeam Software, OU=Veeam Software Remote certificate chain errors:WarningUntrustedRoot (A certificate chain...

Certificate: CN=Veeam Software, O=Veeam Software, OU=Veeam Software

Thumbprint for certificate verification: DE513021D51DE609FE9DBFEF0773126B54BB7D8C

Username: ABC Company\User1

Password: ●●●●●●●●●●

Selecting Cloud Repository

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

Specify settings for the cloud repository:

1. From the **Available cloud repositories** list, select a cloud repository where you want to store created backups. The **Available cloud repositories** list displays only those 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 **Configure Backup** wizard.

2. Specify backup retention policy settings:

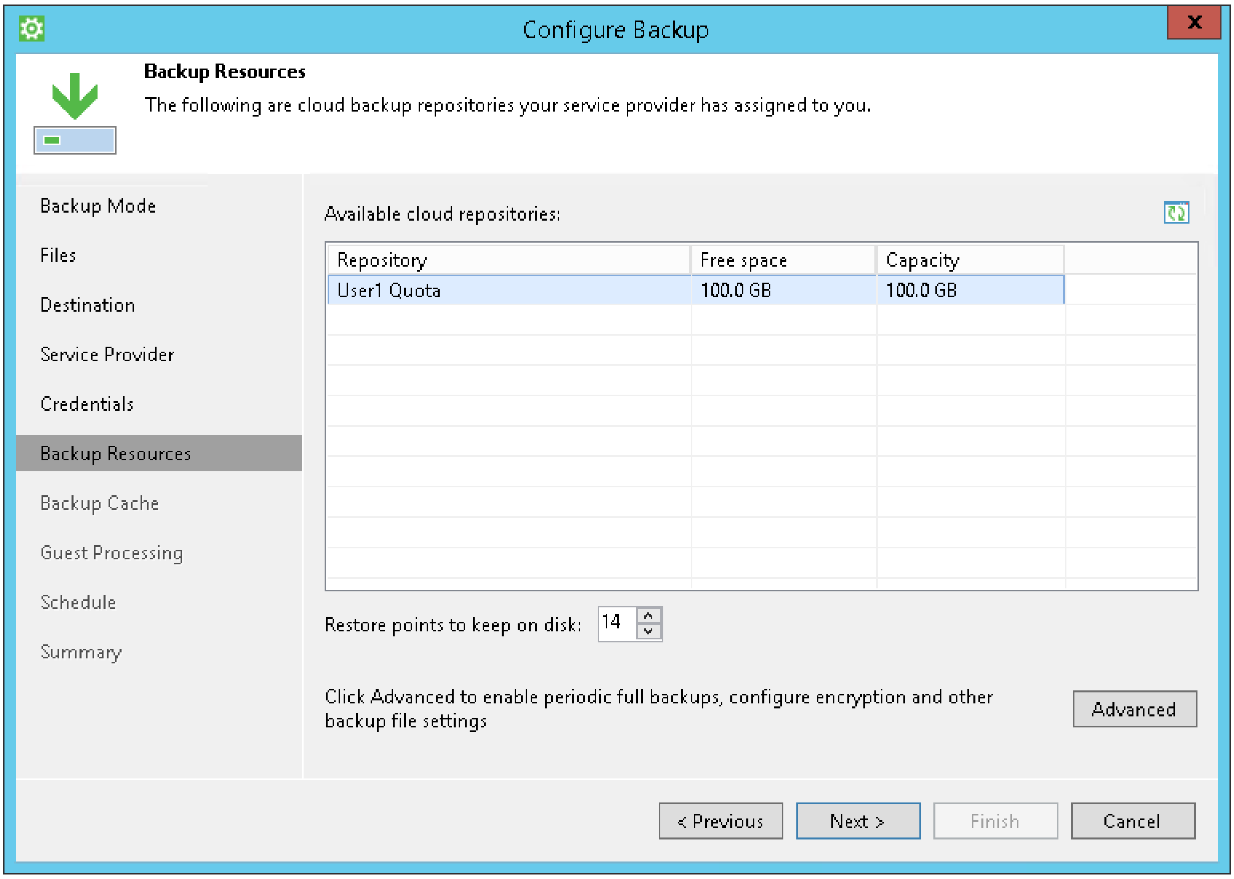
   - [For Free and Workstation product editions] In the **Keep restore points for the last <N> days when computer was used** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files for 14 days. After 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 **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 14 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

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

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



Backup Resources

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

Available cloud repositories:

Repository	Free space	Capacity
User1 Quota	100.0 GB	100.0 GB

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

Microsoft OneDrive Settings

The **Microsoft OneDrive** step of the wizard is available if you have chosen to save the backup in the Microsoft OneDrive cloud storage.

Specify settings to connect to Microsoft OneDrive:

1. Click **Click to sign in to Microsoft OneDrive**.
2. In the **Microsoft OneDrive** web browser window, follow instructions to specify credentials of the Microsoft OneDrive account and click **Sign in**.

> **NOTE:**
>
> You need to sign in to Microsoft OneDrive in the Configure Backup wizard once in every 90 days. If no Veeam Agent backup job sessions are performed for 14 days within a 90-day period, you also need to sign in to Microsoft OneDrive in the Configure Backup wizard after the 14-day period expires. To learn more, see Authorization in Microsoft OneDrive.

3. Specify 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 14 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 **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 14 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

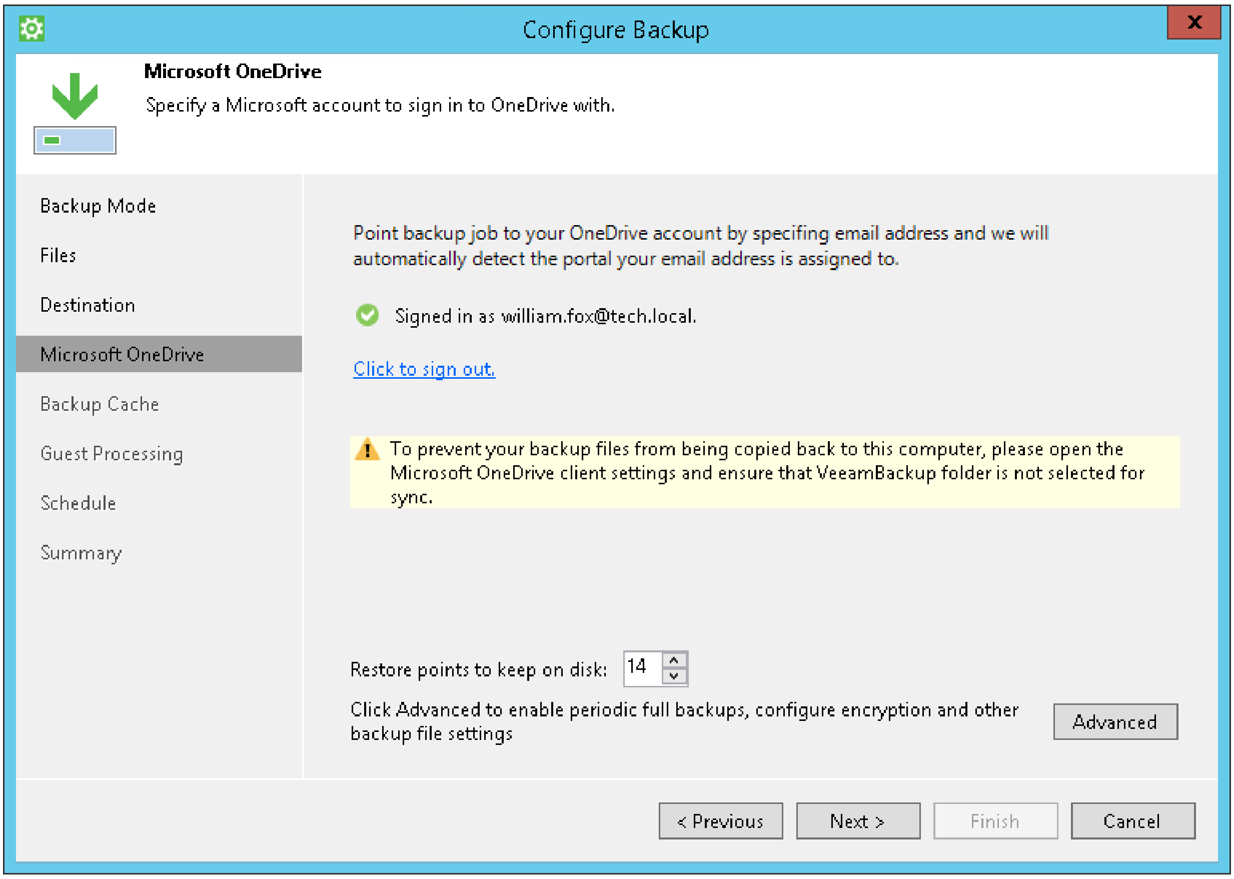
     To learn more, see Backup Retention Policy in Server Edition.

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

TIP:

Consider the following:

- If you want to change settings to connect to Microsoft OneDrive, click the **Click to sign out** link and repeat steps 1-2 to specify another account.
- If you use the Microsoft OneDrive client to sync your OneDrive storage and a local folder on your Veeam Agent computer, you should disable synchronization for the *VeeamBackup* folder in the client settings. Otherwise, Veeam Agent backups created on the Microsoft OneDrive storage will also appear on a computer whose data you back up consuming space on a local disk of this computer.



Microsoft OneDrive

Specify a Microsoft account to sign in to OneDrive with.

Point backup job to your OneDrive account by specifing email address and we will automatically detect the portal your email address is assigned to.

Signed in as william.fox@tech.local.

Click to sign out.

To prevent your backup files from being copied back to this computer, please open the Microsoft OneDrive client settings and ensure that VeeamBackup folder is not selected for sync.

Restore points to keep on disk: 14

Click Advanced to enable periodic full backups, configure encryption and other backup file settings

Step 6. Specify Advanced Backup Settings

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

- Backup settings
- Storage settings

You can access the **Advanced Settings** window from the following steps of the **Configure Backup** 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.
- 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.
- Microsoft OneDrive — if you have selected the **Microsoft OneDrive** option at the Destination step of the wizard.

Backup Settings

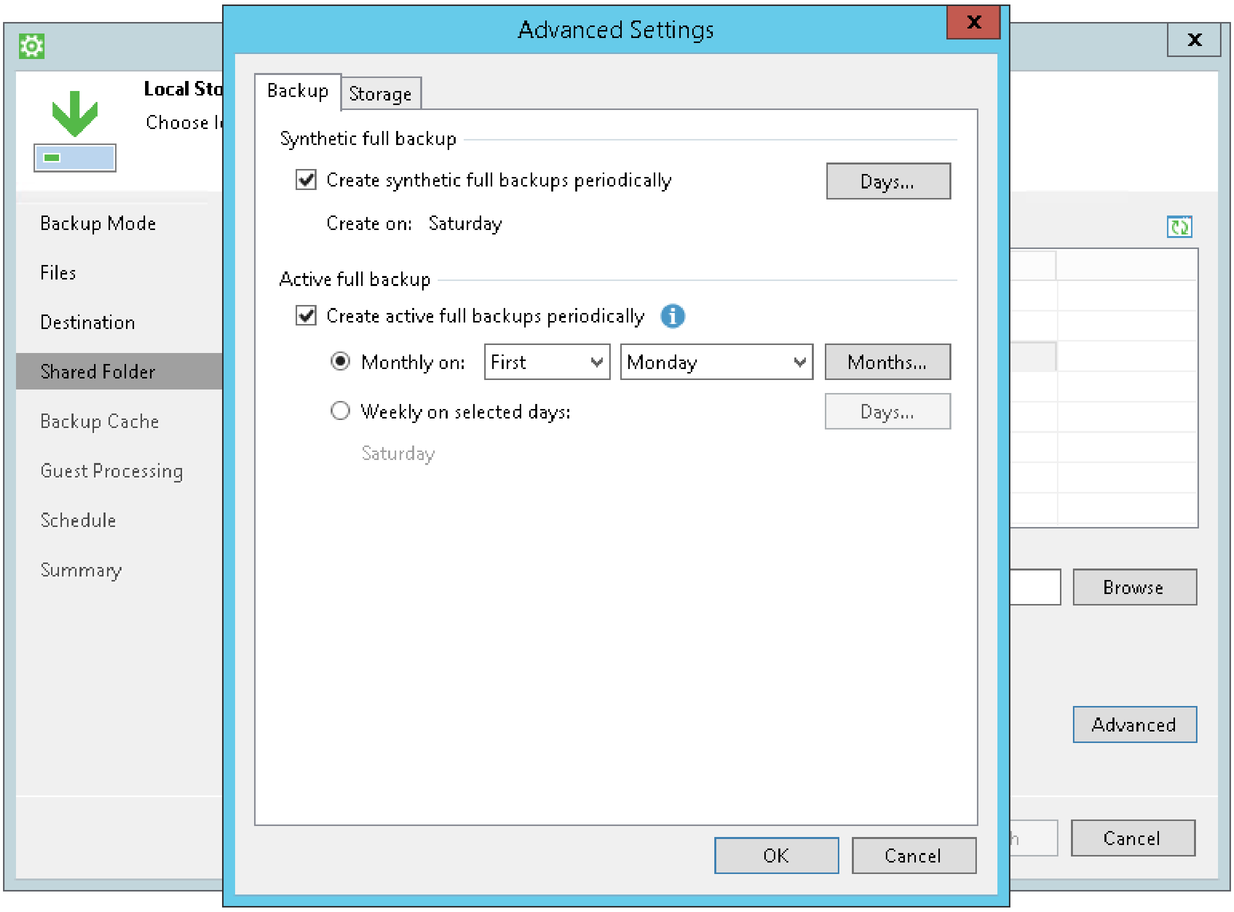
To specify settings for a backup chain created with the backup job:

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.
    - 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.

NOTE:

Consider the following:

- Synthetic full backup functionality is available only in Workstation and Server editions of Veeam Agent for Microsoft Windows.
- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location. As an alternative, you can create active full backups manually when needed. 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.



Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

☑ Create active full backups periodically

● Monthly on: First Monday

○ Weekly on selected days:

Saturday

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.
   - 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 type of backup target you plan to use: *Local target (16 TB + backup files)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Agent for Microsoft Windows will use data blocks of different 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.

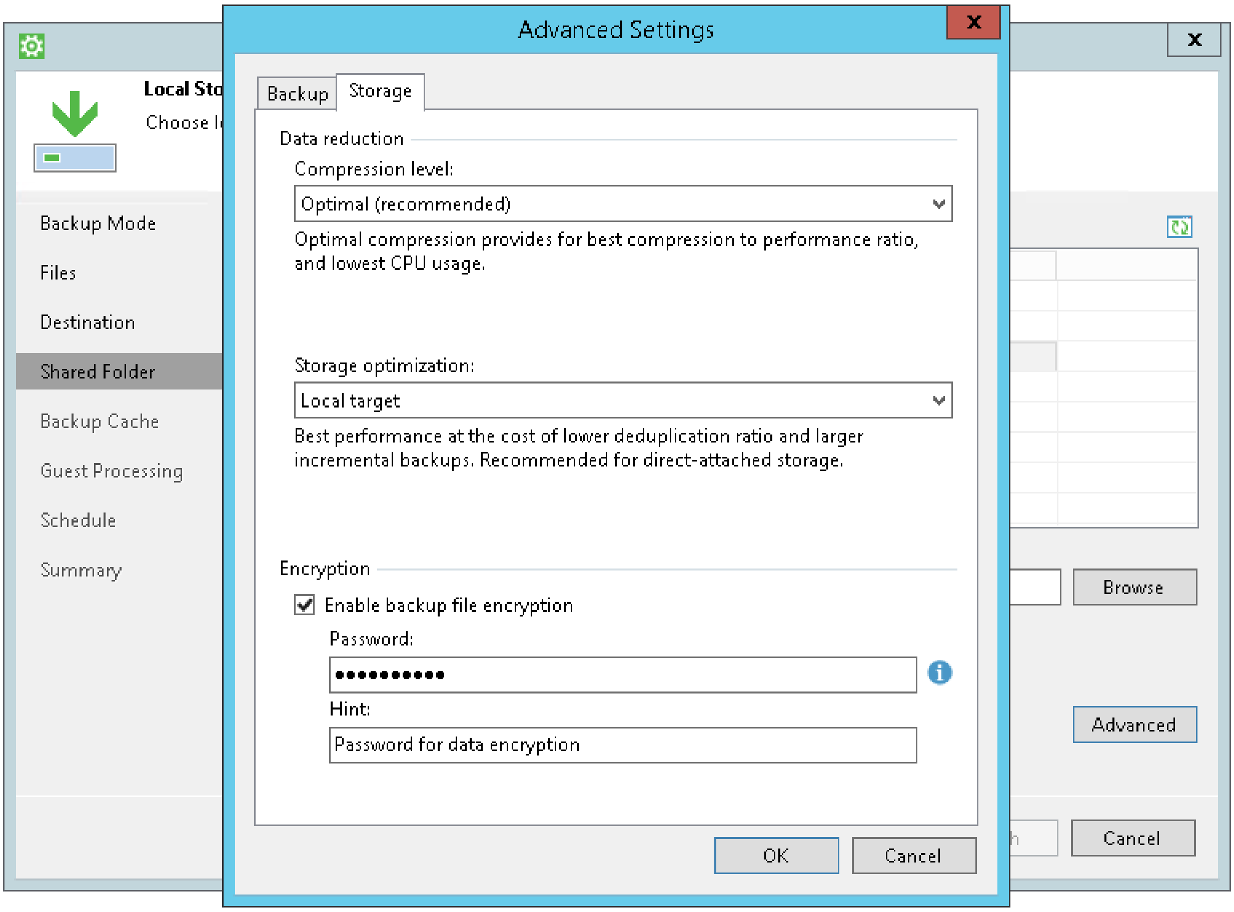
   b. In the **Password** field, type a password that you want to use for encryption.

   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 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, refer to the Veeam Backup & Replication documentation at https://www.veeam.com/documentation-guides-datasheets.html.
- If you lose a password that was specified for encryption, you can change the password in the encryption settings. After the backup job creates a new restore point encrypted with the new password, you will be able to use this password to restore data form 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.



Advanced Settings

Backup | Storage

Data reduction

Compression level: Optimal (recommended)

Optimal compression provides for best compression to performance ratio, and lowest CPU usage.

Storage optimization: Local target

Best performance at the cost of lower deduplication ratio and larger incremental backups. Recommended for direct-attached storage.

Encryption

☑ Enable backup file encryption

Password: ●●●●●●●●●●●

Hint: Password for data encryption

Step 7. Specify Backup Cache Settings

The **Backup Cache** step of the wizard is available if you have chosen to save backup files on a remote storage: in a network shared folder, on a Veeam backup repository, on a Veeam Cloud Connect repository or in Microsoft OneDrive.

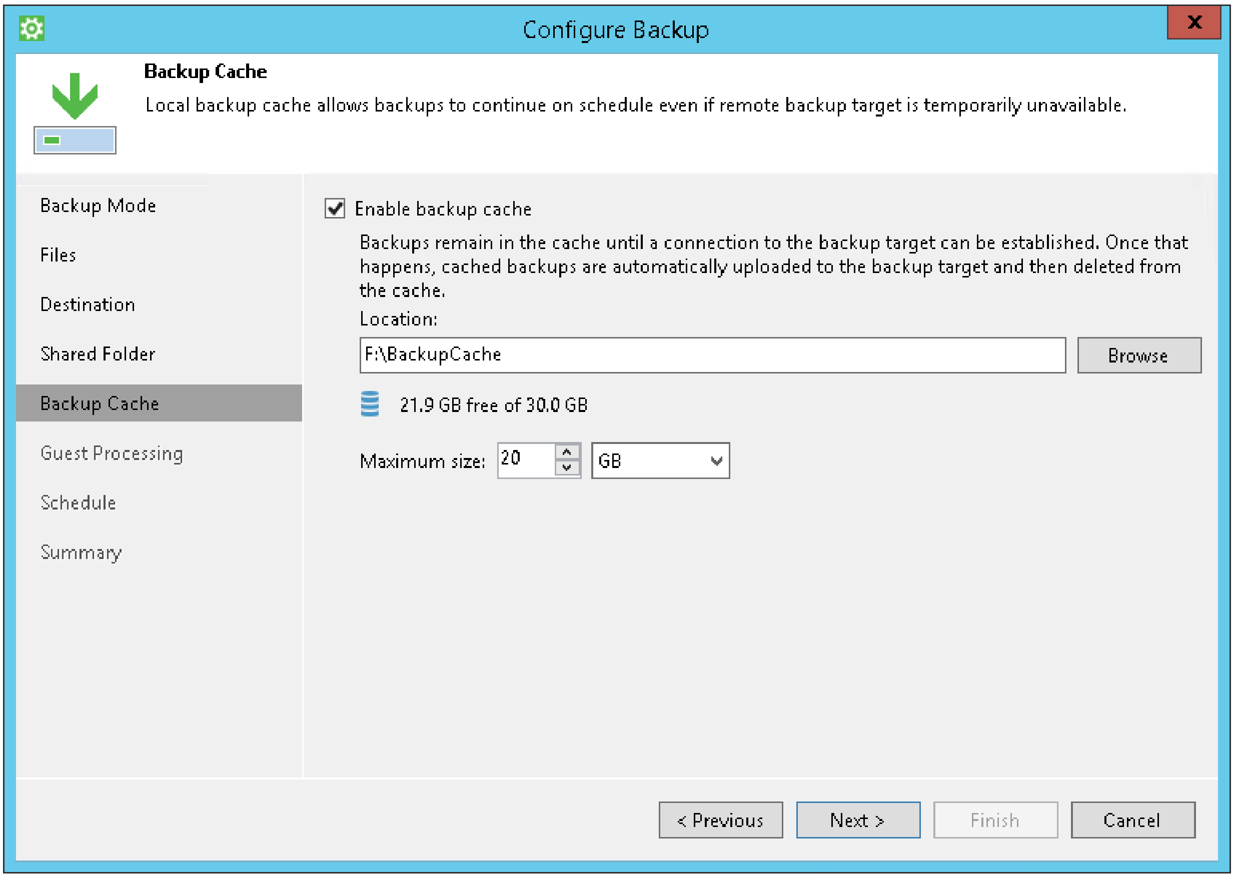
Specify backup cache settings:

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.



Backup Cache

Local backup cache allows backups to continue on schedule even if remote backup target is temporarily unavailable.

☑ Enable backup cache

Backups remain in the cache until a connection to the backup target can be established. Once that happens, cached backups are automatically uploaded to the backup target and then deleted from the cache.

Location: F:\BackupCache

21.9 GB free of 30.0 GB

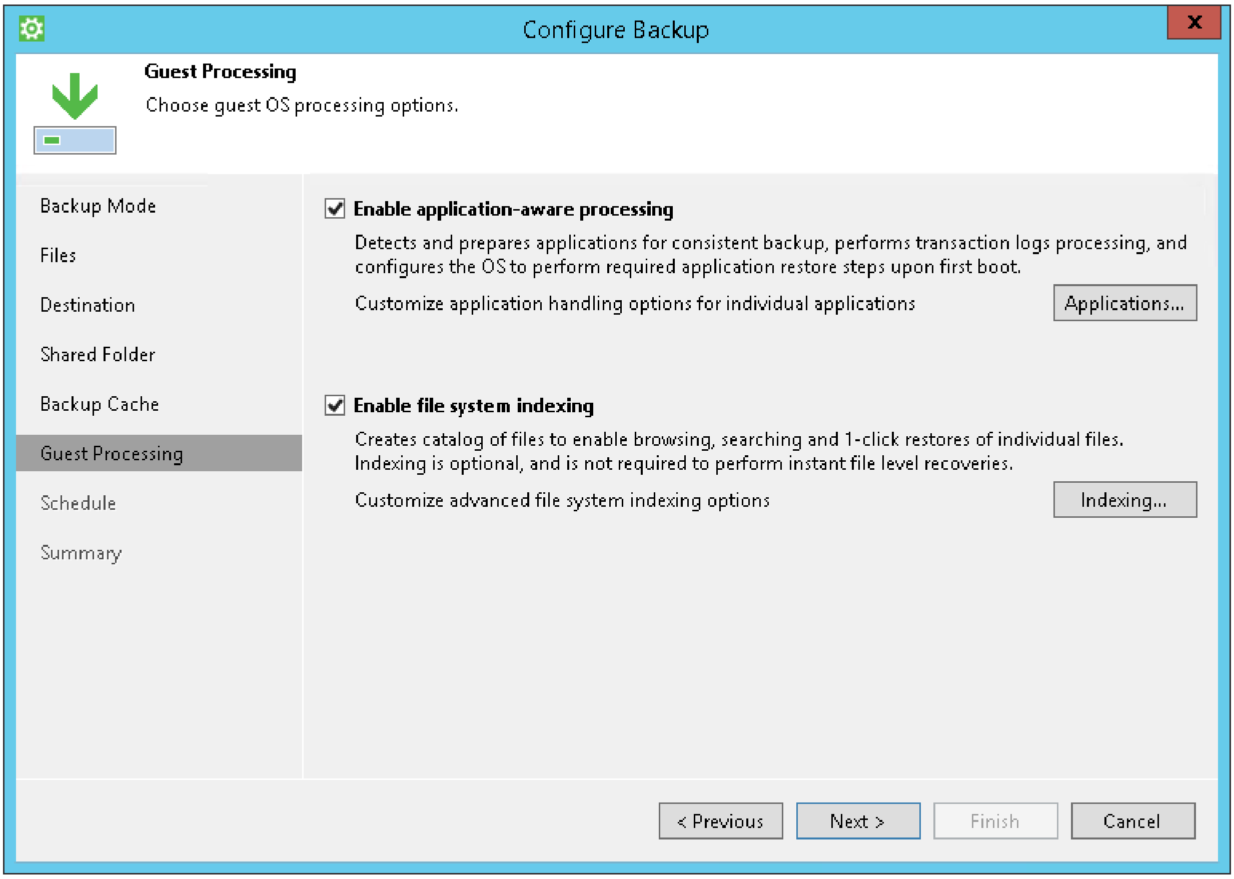
Maximum size: 20 GB

Step 8. 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
- Transaction log handling for Oracle databases
- SharePoint account settings
- Use of pre-freeze and post-thaw scripts
- File indexing



Configure Backup

Guest Processing

Choose guest OS processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual applications

☑ **Enable file system indexing**

Creates catalog of files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced file system indexing options

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**.

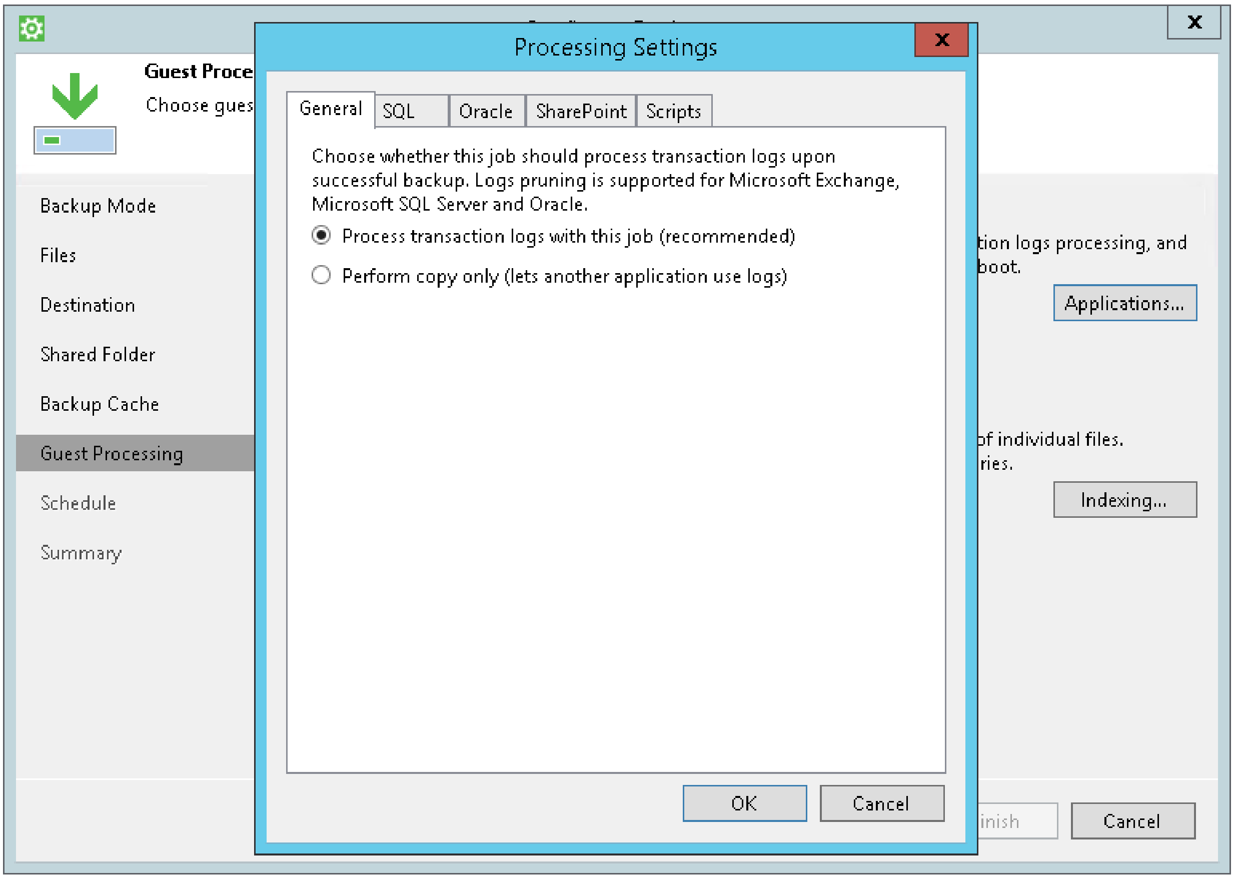
3. In the **Processing Settings** window, on the **General** tab, specify if Veeam Agent for Microsoft Windows must process transaction logs [For Microsoft Exchange, Microsoft SQL and Oracle] or copy-only backups must be created.

   a. Select **Process transaction logs with this job** if you want Veeam Agent for Microsoft Windows to process transaction logs.

      [For Microsoft Exchange] With this option selected, Veeam Agent for Microsoft Windows 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 Transaction Log Settings: Microsoft SQL and Transaction Log Settings: Oracle.

   b. Select **Perform copy only** if you use another tool to maintain consistency of the database state. Veeam Agent for Microsoft Windows will create a copy-only backup. The copy only backup preserves the chain of full/differential backup files and transaction logs. For more information, see http://msdn.microsoft.com/en-us/library/ms191495.aspx.



Processing Settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server and Oracle.

● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

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 the Microsoft Exchange database 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, and log backup is enabled for both applications, Veeam Agent for Microsoft Windows will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.

Transaction Log Settings: Microsoft SQL Server

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 for Microsoft Windows will use to connect to the Microsoft SQL Server, select the **Specify Microsoft SQL Server account with database admin privileges** check box and enter a user name and password for the user account. To connect to the Microsoft SQL Server, you must use a Microsoft Windows user account that has sysadmin privileges on the Microsoft SQL Server. You cannot use Microsoft SQL Server accounts (for example, the SA account) to connect to the database.
6. Specify how transaction logs must be processed. You can select one of the following options:

   - Select **Truncate logs** to truncate transaction logs after successful backup. Veeam Agent for Microsoft Windows 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 for Microsoft Windows will not truncate transaction logs.

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

   - Select **Backup logs periodically** to back up transaction logs with Veeam Agent for Microsoft Windows. Veeam Agent for Microsoft Windows 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.

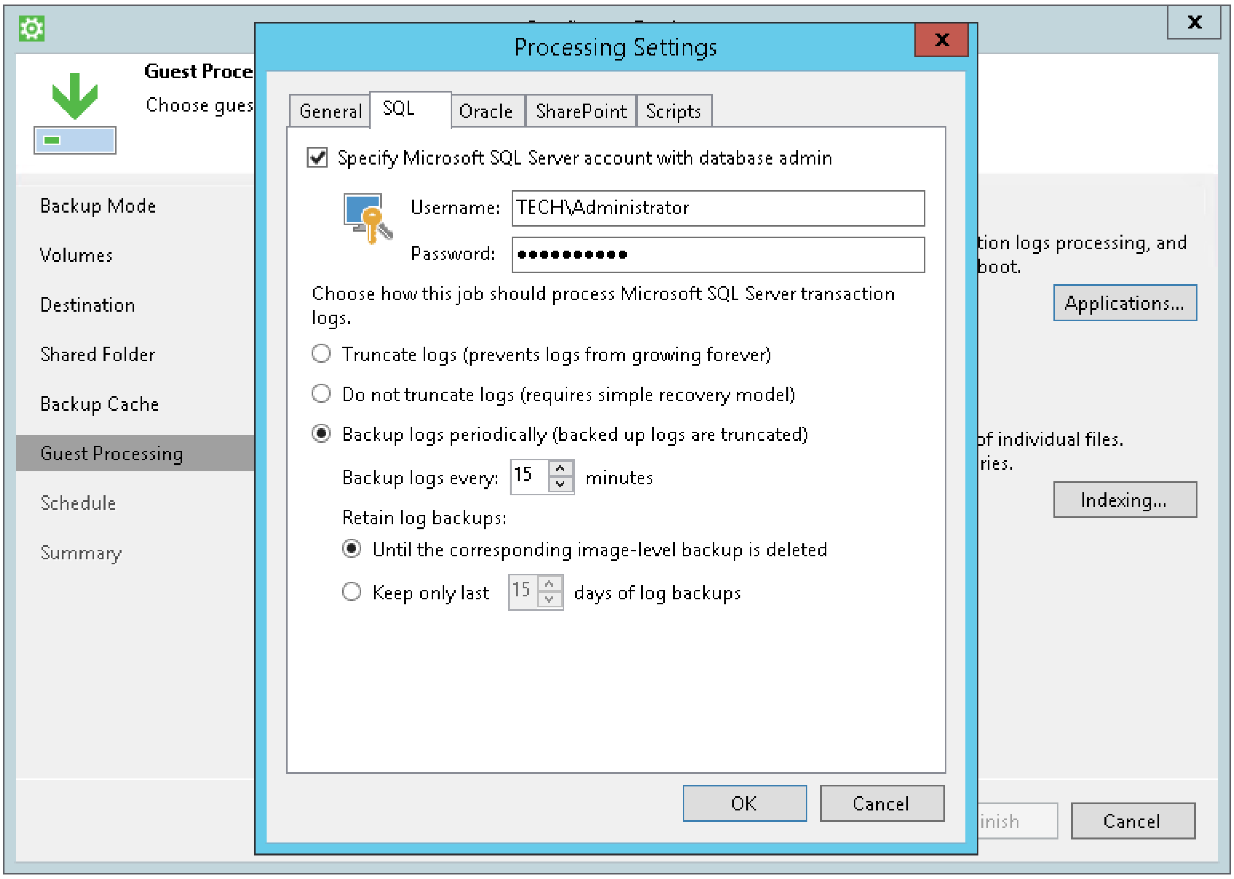
     For more information, see Microsoft SQL Server and Oracle Logs Backup and Restore.

If you have selected to back up transaction logs with Veeam Agent for Microsoft Windows, you must specify settings for transaction logs backup:

1. In the **Backup logs every <N> minutes** field, specify the frequency for transaction logs backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
2. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup location.
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
   - Select **Keep only last <N> days of log backups** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backup. For 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.



☑ Specify Microsoft SQL Server account with database admin

Username: TECH\Administrator

Password: ●●●●●●●●●●●

Choose how this job should process Microsoft SQL Server transaction logs.

○ Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

● Backup logs periodically (backed up logs are truncated)

Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

Archived Log Settings: Oracle

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.

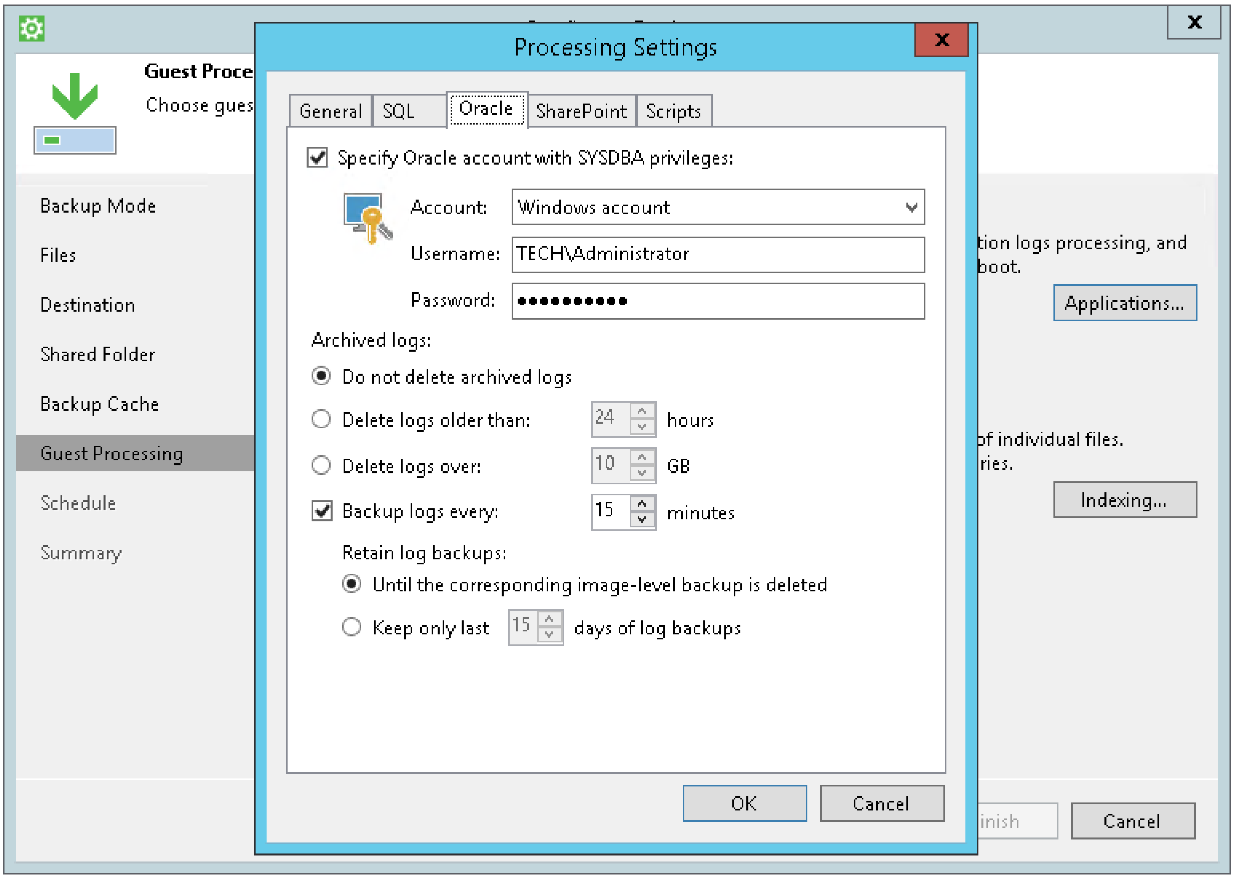
      It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.

    - 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 truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next 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 logs backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

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

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



☑ Specify Oracle account with SYSDBA privileges:

Account: Windows account

Username: TECH\Administrator

Password: ●●●●●●●●●●●

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

☑ Backup logs every: 15 minutes

Retain log backups:

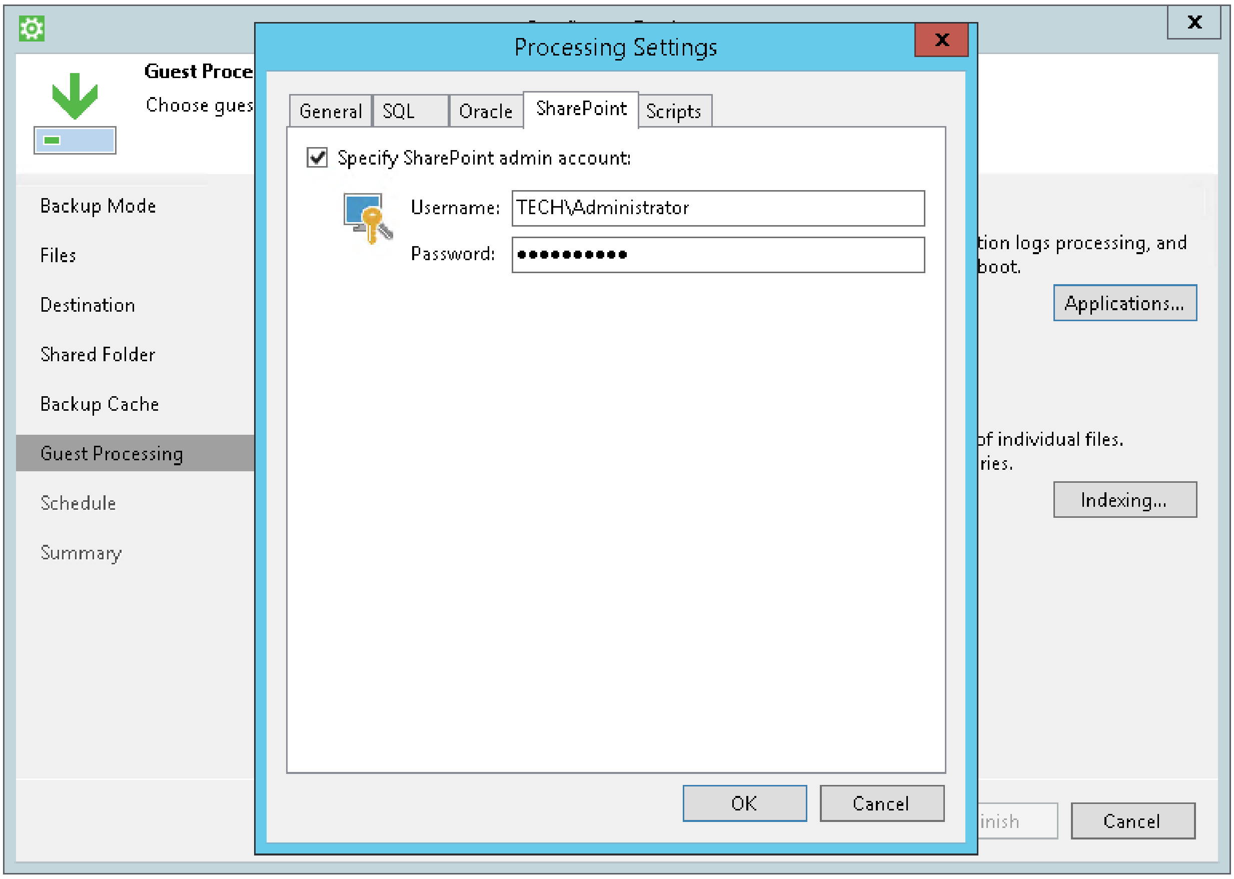
● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of 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 SharePoint admin account** check box and enter a user name and password for the user account.



Processing Settings

☑ Specify SharePoint admin account:

Username: TECH\Administrator

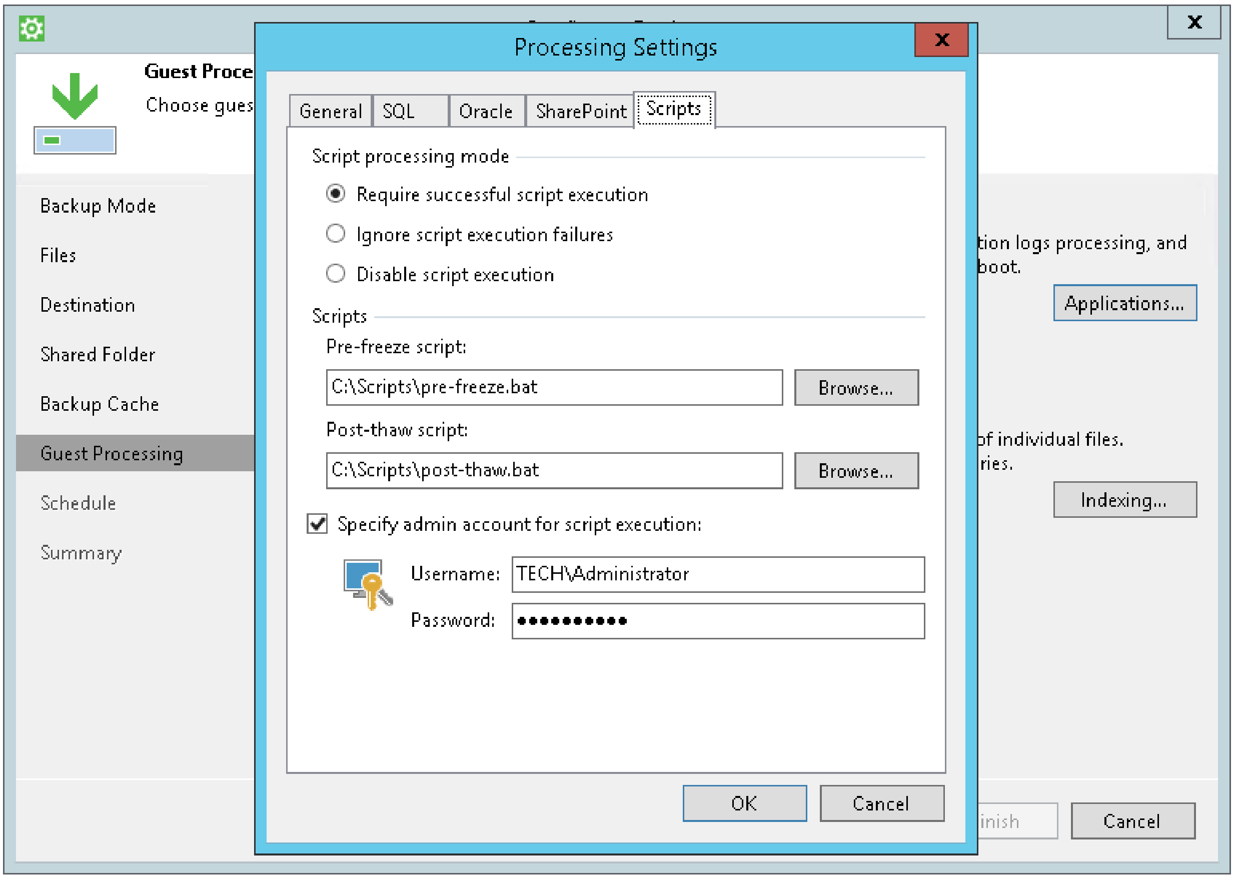
Password: ●●●●●●●●●●●

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 scripts in the EXE, BAT and CMD format.
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.



Processing Settings

Script processing mode

● Require successful script execution

○ Ignore script execution failures

○ Disable script execution

Scripts

Pre-freeze script: C:\Scripts\pre-freeze.bat

Post-thaw script: C:\Scripts\post-thaw.bat

☑ Specify admin account for script execution:

Username: TECH\Administrator

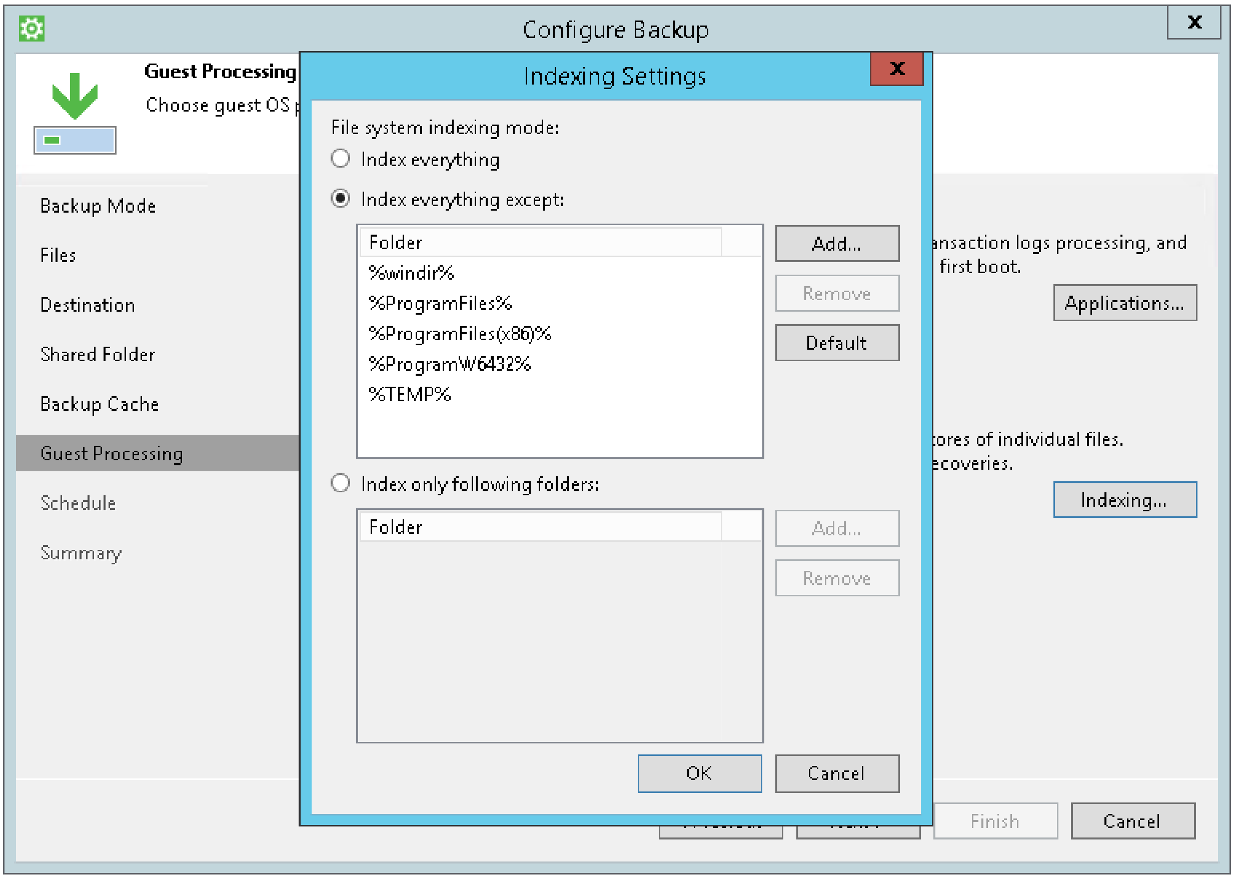
Password: ●●●●●●●●●●●

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%*, *%Program Files%* 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%*, *%Program Files%* and *%Temp%*.



File system indexing mode:

○ Index everything

● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%
%ProgramW6432%
%TEMP%

○ Index only following folders:

Folder

Step 9. 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, specify the schedule according to which you want to perform backup.

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 https://support.microsoft.com/en-us/kb/920730.

    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.

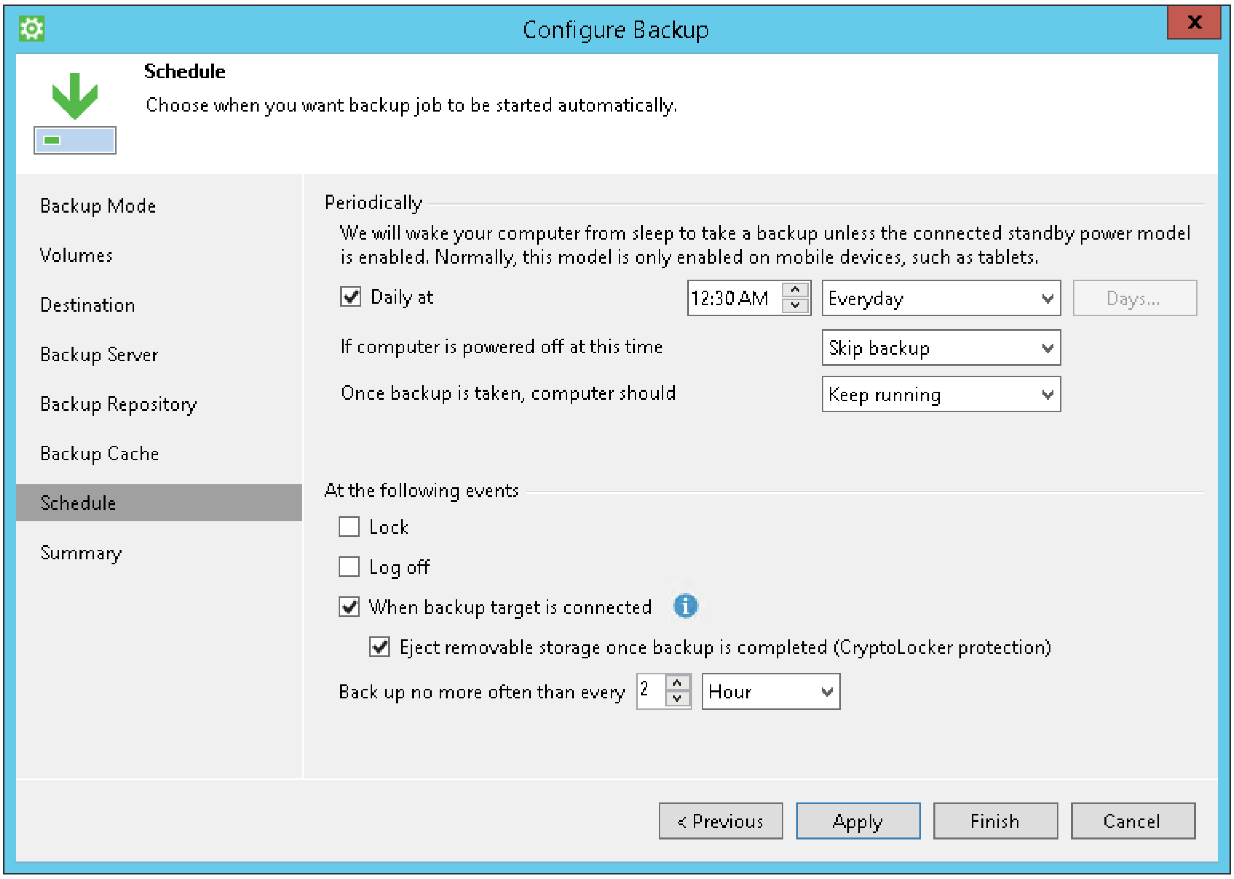
When the backup job completes, Veeam Agent for Microsoft Windows will prompt a dialog with a countdown to the selected post-job action. You can select to proceed to the action immediately or to cancel the action. To learn more, see Controlling Backup Post-Job Action.

5. In the **At the following events** section, specify settings for 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.
   - 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 (for example, when the computer connects to a local network and the target shared folder is accessible).
   - Select the **Eject removable storage once backup is completed** check box if 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.
   - 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.

6. Click **Save**.



Configure Backup

Schedule

Choose when you want backup job to be started automatically.

Periodically

We will wake your computer from sleep to take a backup unless the connected standby power model is enabled. Normally, this model is only enabled on mobile devices, such as tablets.

☑ Daily at 12:30 AM Everyday Days...

If computer is powered off at this time: Skip backup

Once backup is taken, computer should: Keep running

At the following events

☐ Lock

☐ Log off

☑ When backup target is connected

☑ Eject removable storage once backup is completed (CryptoLocker protection)

Back up no more often than every 2 Hour

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**.

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.

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.

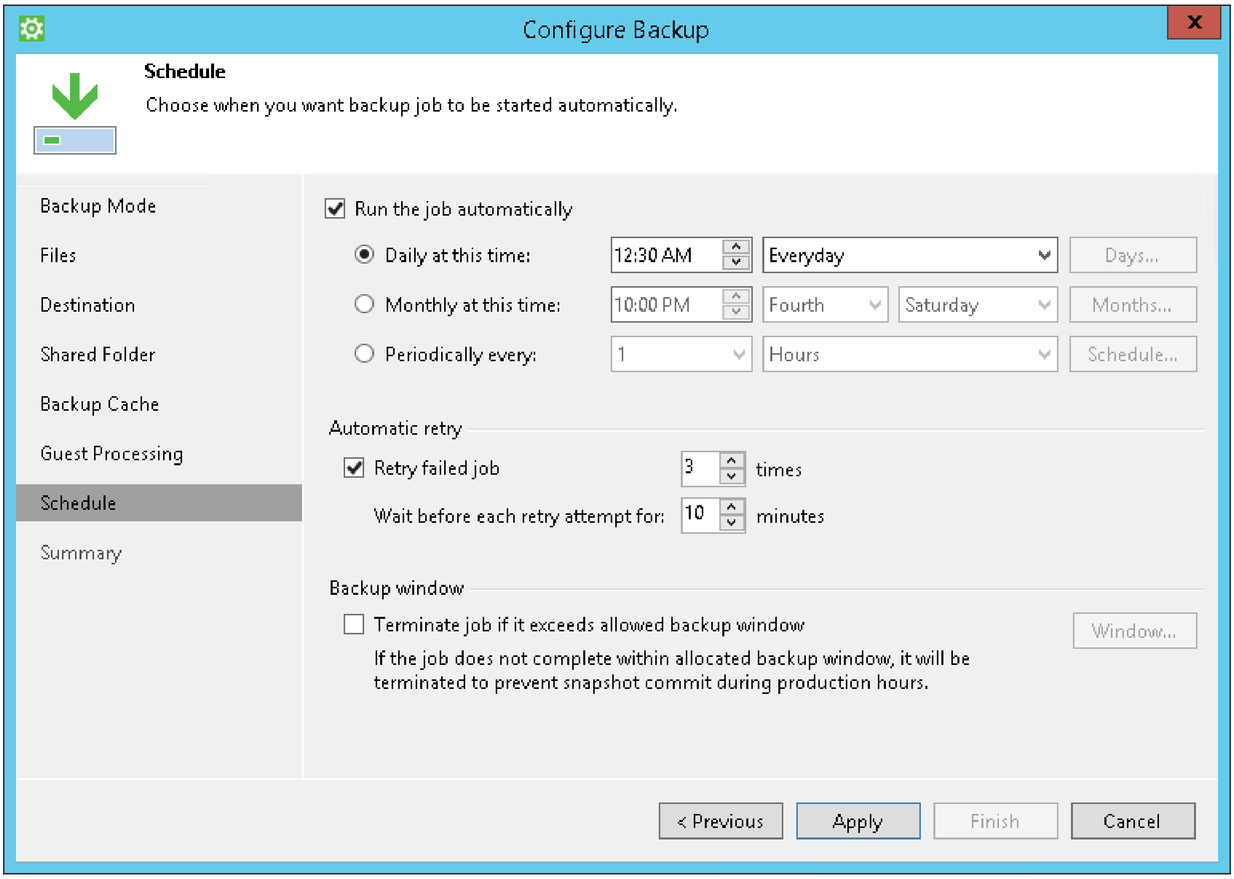
   - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.

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.



Configure Backup

Schedule

Choose when you want backup job to be started automatically.

☑ Run the job automatically

● Daily at this time: 12:30 AM, Everyday

○ Monthly at this time: 10:00 PM, Fourth, Saturday

○ Periodically every: 1, Hours

Automatic retry

☑ Retry failed job 3 times

Wait before each retry attempt for: 10 minutes

Backup window

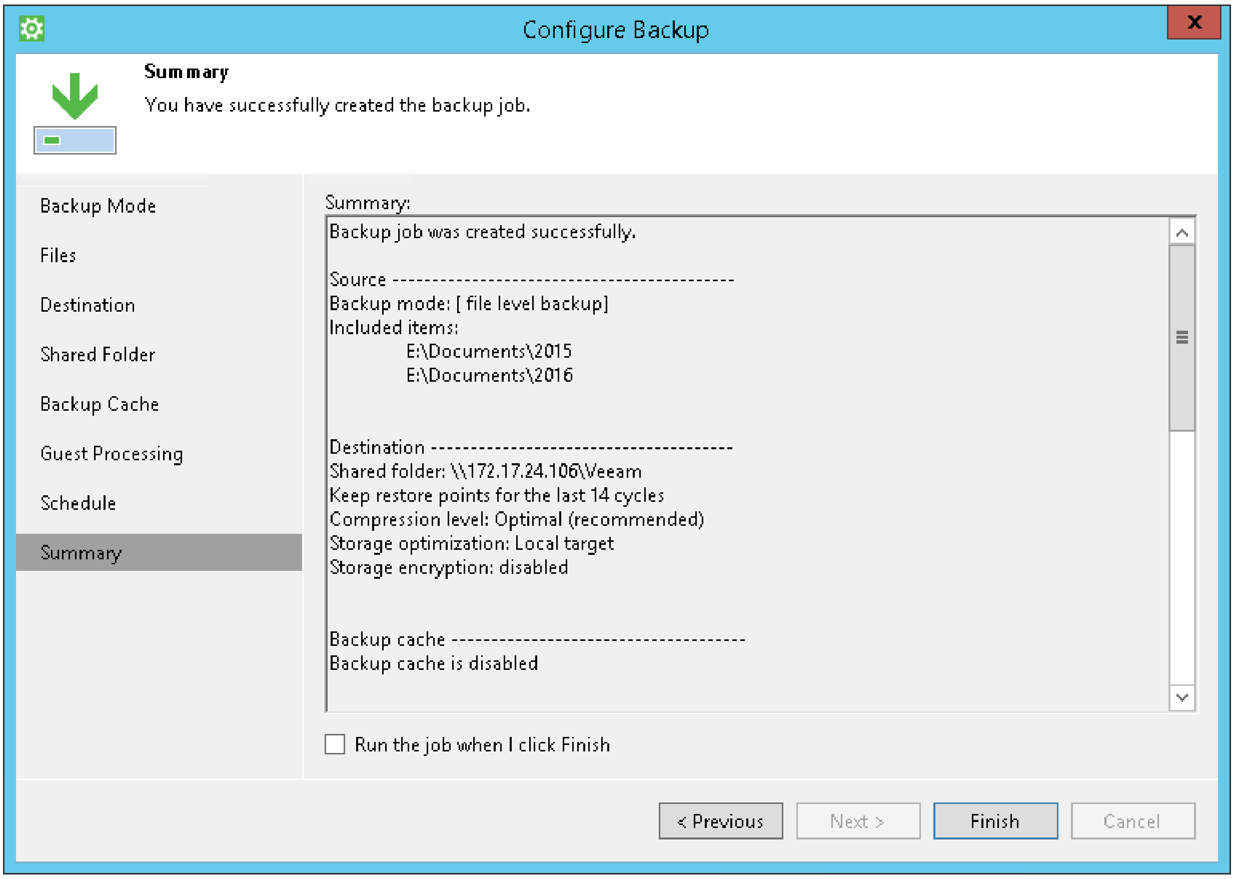
□ Terminate job if it exceeds allowed backup window

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

Step 10. 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.
2. To start the job after you close the wizard, select the **Run the job when I click Finish** check box.
3. Click **Finish**.



```
Backup job was created successfully.

Source ------------------------------------------
Backup mode: [ file level backup]
Included items:
          E:\Documents\2015
          E:\Documents\2016


Destination ------------------------------------
Shared folder: \\172.17.24.106\Veeam
Keep restore points for the last 14 cycles
Compression level: Optimal (recommended)
Storage optimization: Local target
Storage encryption: disabled


Backup cache ----------------------------------
Backup cache is disabled
```

☐ Run the job when I 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 Job

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

Editing Backup Job Settings

If you want to change settings of the scheduled 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:

- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Backup** > **Configure backup**.
- From the main menu, select **All Programs** > **Veeam** > **Tools** > **Configure Backup** or use the Microsoft Windows search to find the **Configure Backup** option on your computer.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**. At the top left corner of the **Status** view, click **Configure backup**.

Then edit the job settings as required. To learn more about available job settings, see Configuring Scheduled Backup Job.

If you change the target location in 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 in the backup job, during the next backup job session Veeam Agent for Microsoft Windows will create a new incremental backup that will contain a full copy of all data that you have selected to back up.

> **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 the scheduled backup job 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 the backup job again.

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

If the scheduled backup job is set up to create database log backups, and you disable this job, the database log backup job will be disabled, too.

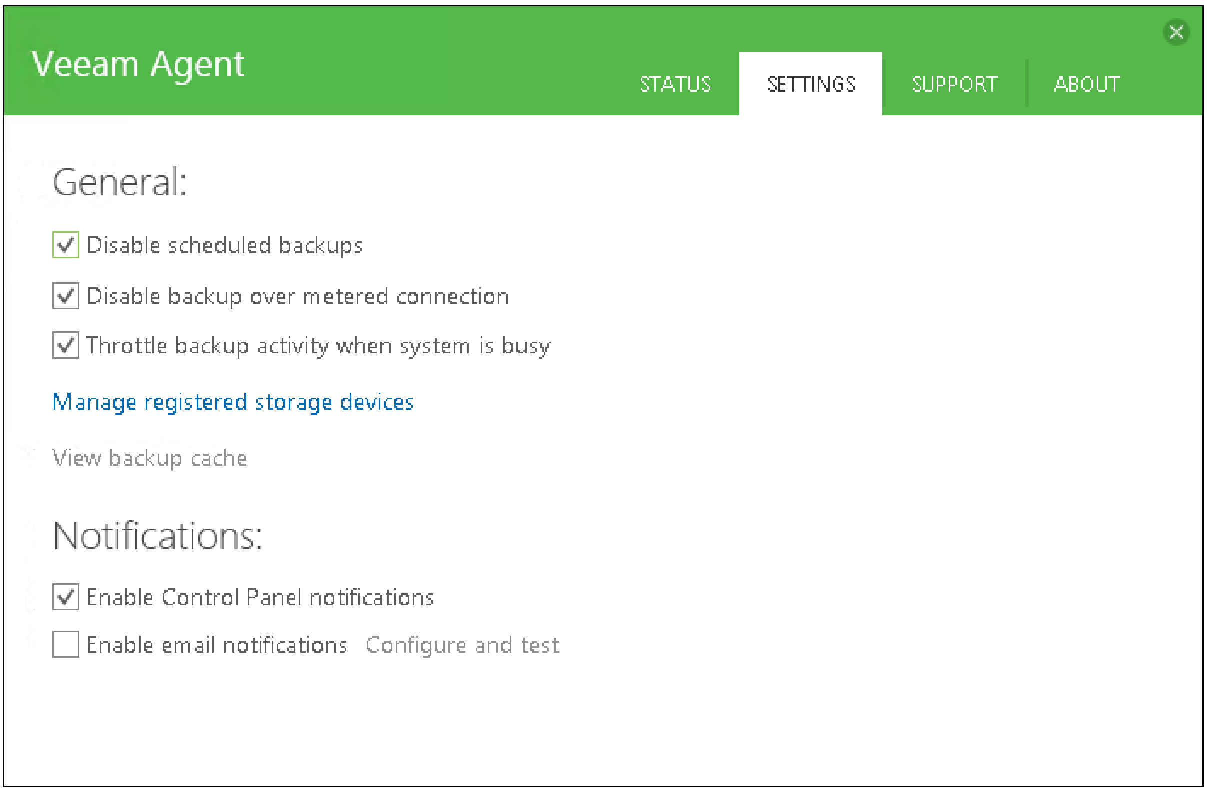
The disabling option does not put on hold the backup cache synchronization process. If Veeam Agent for Microsoft Windows has created one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent for Microsoft Windows will immediately upload backup files to the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

To disable the scheduled backup job:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. Click the **Settings** tab at the top of the window.
3. Select the **Disable scheduled backups** check box.

To enable a disabled backup job:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click it and select **Control Panel**.
2. Click the **Settings** tab at the top of the window.
3. Clear the **Disable scheduled backups** check box.



General:

☑ Disable scheduled backups

☑ Disable backup over metered connection

☑ Throttle backup activity when system is busy

Manage registered storage devices

View backup cache

Notifications:

☑ Enable Control Panel notifications

□ Enable email notifications Configure and test

Controlling Backup Post-Job Action

You can set up Veeam Agent for Microsoft Windows to perform a finalizing action after the backup job completes successfully:

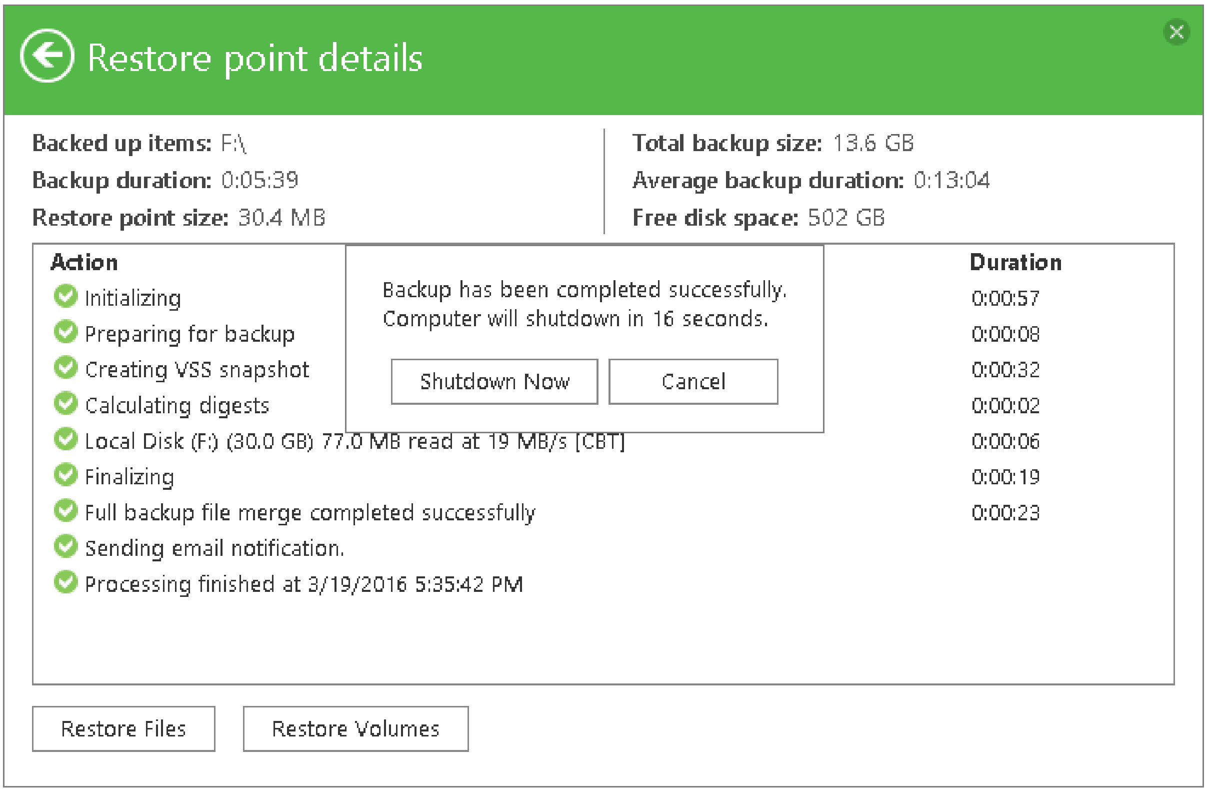
- *Sleep* — bring your computer to the standby mode.
- *Hibernate* — bring your computer to the hibernate mode.
- *Shutdown* — shut down your computer.

To learn more, see Specify Backup Schedule.

When the backup job completes, Veeam Agent for Microsoft Windows opens the 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 for Microsoft Windows will perform the specified action when timeout expires.



Restore point details

Backed up items: F:\
Backup duration: 0:05:39
Restore point size: 30.4 MB

Total backup size: 13.6 GB
Average backup duration: 0:13:04
Free disk space: 502 GB

Action	Duration
✓ Initializing	0:00:57
✓ Preparing for backup	0:00:08
✓ Creating VSS snapshot	0:00:32
✓ Calculating digests	0:00:02
✓ Local Disk (F:) (30.0 GB) 77.0 MB read at 19 MB/s [CBT]	0:00:06
✓ Finalizing	0:00:19
✓ Full backup file merge completed successfully	0:00:23
✓ Sending email notification.	
✓ Processing finished at 3/19/2016 5:35:42 PM	

Backup has been completed successfully.
Computer will shutdown in 16 seconds.

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.

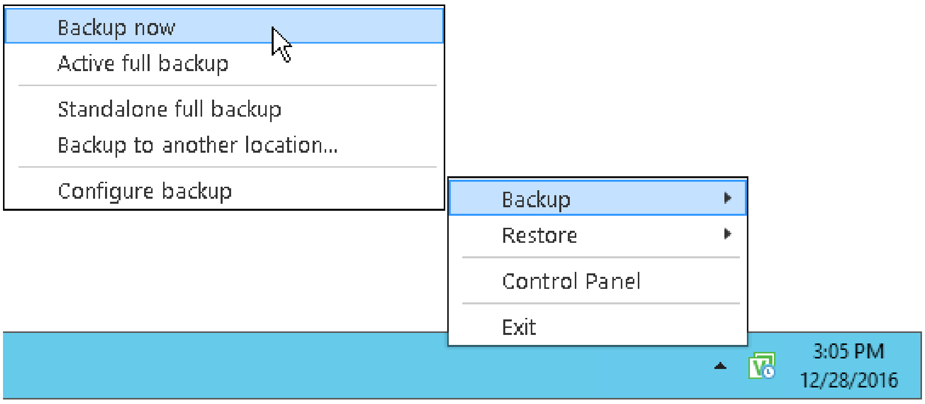
Before you perform ad-hoc incremental backup, check the following prerequisites:

- The backup job 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, do one of the following:

- Double-click the Veeam Agent for Microsoft Windows icon in the system tray and click **Backup Now** in the Control Panel.
- Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Backup** > **Backup now**.

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.



Creating Active Full Backups

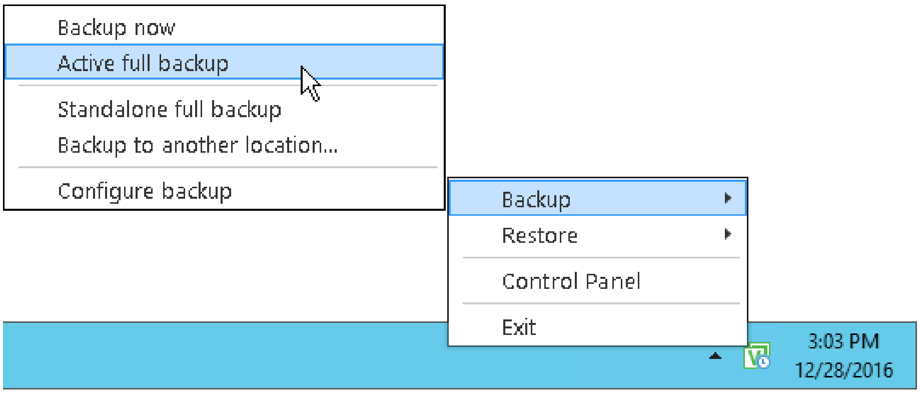
You can create an ad-hoc full backup — active full backup, and add it to the backup chain on the target storage. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the target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

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. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **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.



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:

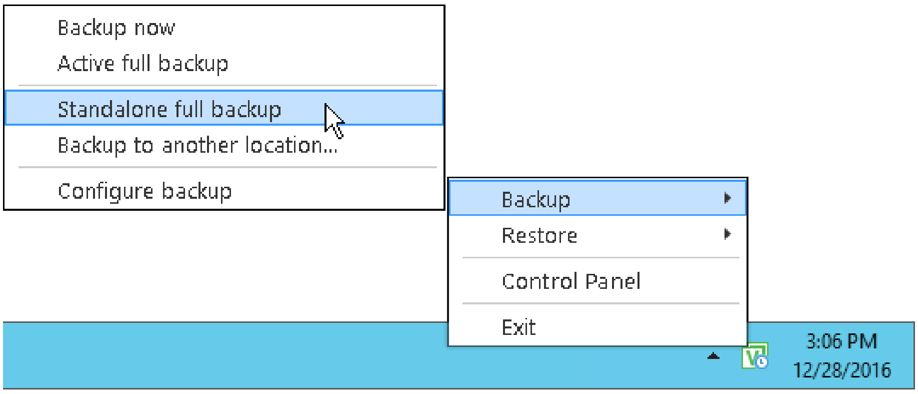
- The backup job must be configured.
- You cannot create a standalone full backup if a backup task of any type is currently running. This includes a scheduled backup, standalone full backup, active full backup or ad-hoc incremental backup.
- You cannot create a standalone full backup if the backup job is targeted at the cloud repository. 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 lean more, see Performing Backup to Another Location.
- 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.

To create a standalone full backup:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **Standalone full backup**. Veeam Agent for Microsoft Windows will create a full backup file using settings of the scheduled 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:

   `Backup Job <ComputerName>.adhoc.<DateandTime>`.

   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.



Performing Backup to Another Location

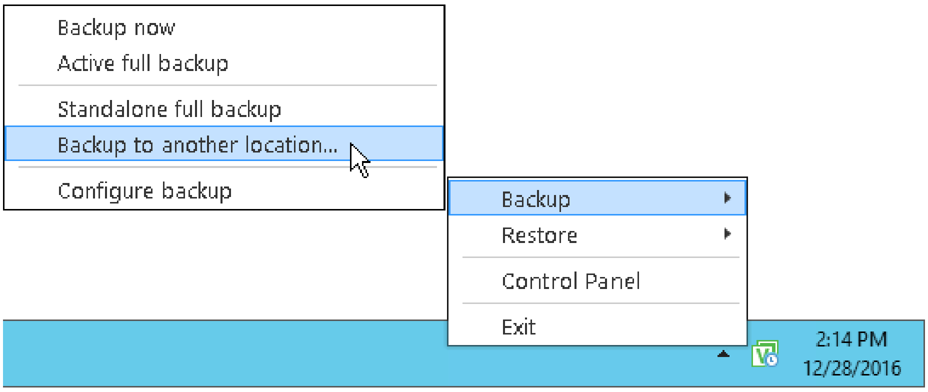
You can create a standalone full backup in a separate location that is not specified as a target location in the backup job settings. Performing backup to another location is similar to creating regular standalone full backups. The main difference is that you must manually select a target location in 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. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **Backup** > **Backup to another location**.

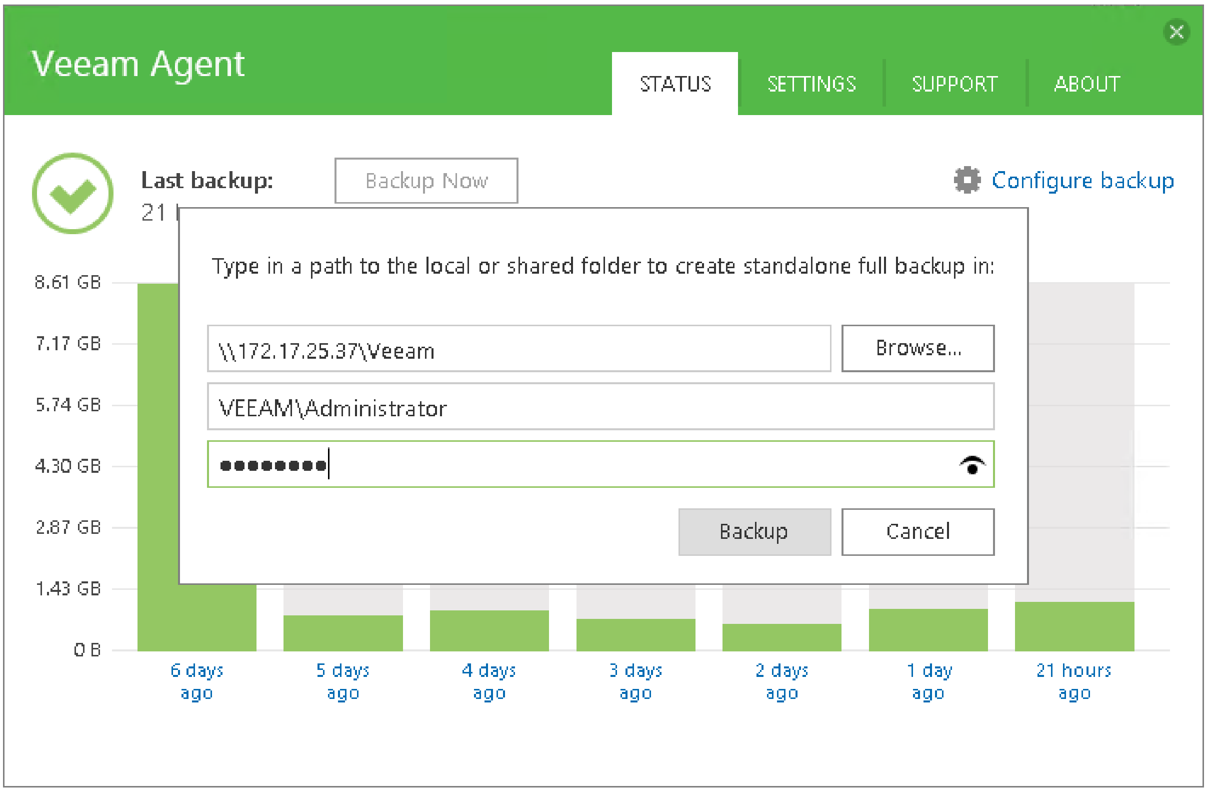


3. In the standalone full backup dialog window, specify the target location for the backup file:
   - If you want to save the backup file in a folder on a local drive or a removable storage device, click **Browse** and select the necessary folder or type a path to the folder where backup file must be 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 scheduled 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:

   `Backup Job <ComputerName>.adhoc.<DateandTime>.`



Type in a path to the local or shared folder to create standalone full backup in:

\\172.17.25.37\Veeam

VEEAM\Administrator

●●●●●●●●

Performing Backup with Command Line Interface

In addition to running scheduled backup jobs and performing ad-hoc backups from the Veeam Agent for Microsoft Windows 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)
- Standalone full backup
- Backup to another location

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 of any type is currently running. This includes a scheduled backup, standalone full backup or ad-hoc incremental backup.
- To create a standalone full backup or backup to another location, you must run the command line interface with administrative privileges.

Creating Backups

To perform backup, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /backup
```

Creating Standalone Full Backups

To create a standalone full backup, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone
```

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:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /standalone
<location>
```

where `<location>` is a path to a folder in which the backup should be created.

> **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. However, you can also remove backup files manually if necessary.

Always delete the whole backup chain from the target location. If you delete a full backup file or individual incremental backup file from the backup chain, the chain will be broken, and Veeam Agent for Microsoft Windows will fail to perform the scheduled backup next time.

If 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.

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 Microsoft OneDrive storage.

When you delete a backup from a cloud repository, Veeam Agent for Microsoft Windows deletes actual backup files from the cloud 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.

When you delete a backup from Microsoft OneDrive, Veeam Agent for Microsoft Windows deletes actual backup files from the target location and removes records about the backup from the Veeam Agent for Microsoft Windows database.

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.
- [For Veeam Cloud Connect repository] The cloud repository from which you want to delete a backup must be specified as a target location for backup files in the backup job settings. To learn more, see Selecting Cloud Repository.
- [For Veeam Cloud Connect repository] Credentials of the user account (tenant account or subtenant account) whose backup you want to delete must be specified in the backup job settings. To learn more, see Specifying User Account Settings.
- [For Microsoft OneDrive] You must be signed in to the Microsoft OneDrive account whose backup you want to delete in the Configure Backup wizard. To learn more, see Microsoft OneDrive Settings.

To delete a Veeam Agent backup, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" /deletebackup
```

Veeam Agent for Microsoft Windows can provide the following exit codes:

- 0 — backup was successfully deleted
- -1 — the delete backup 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

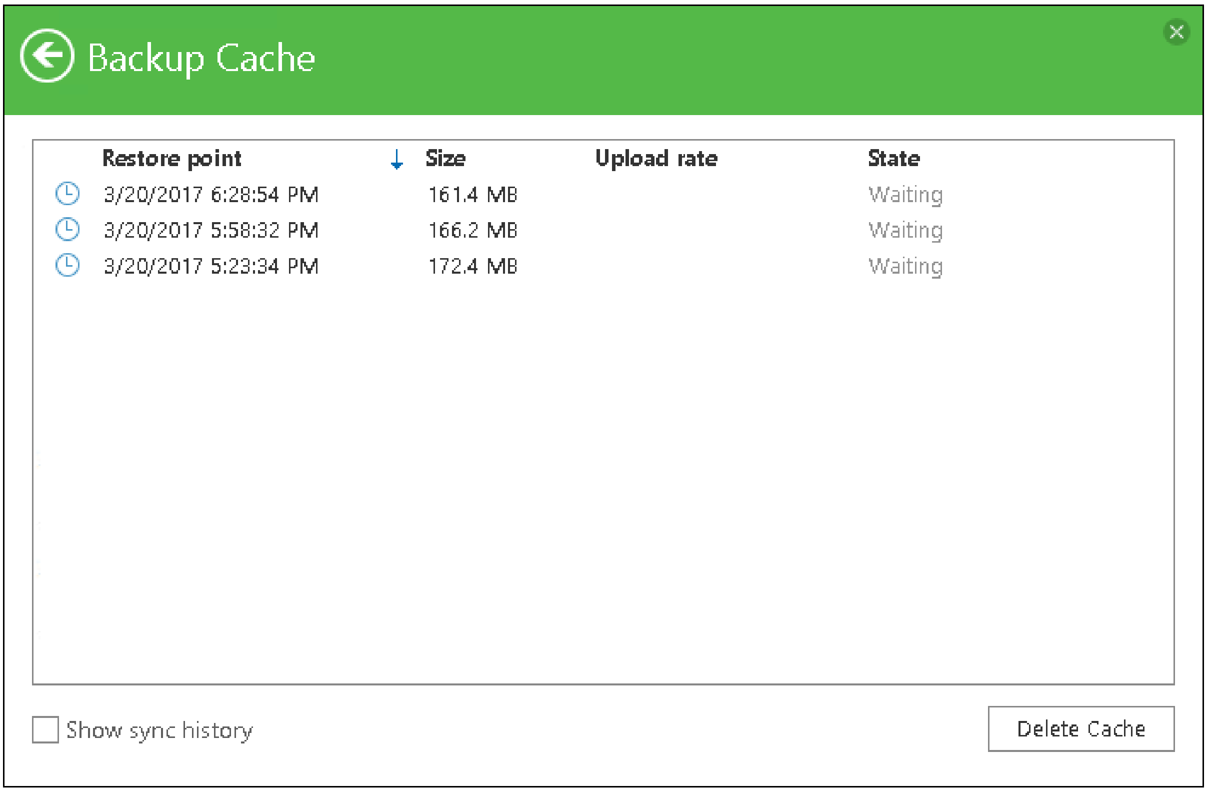
Monitoring Backup Cache Activity

You can use the Veeam Agent for Microsoft Windows Control Panel to view information about backup cache activity. In the **Backup Cache** window, 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:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. Select **View cache**. The Veeam Agent for Microsoft Windows control panel will open, and you will pass immediately to the **Backup Cache** window.

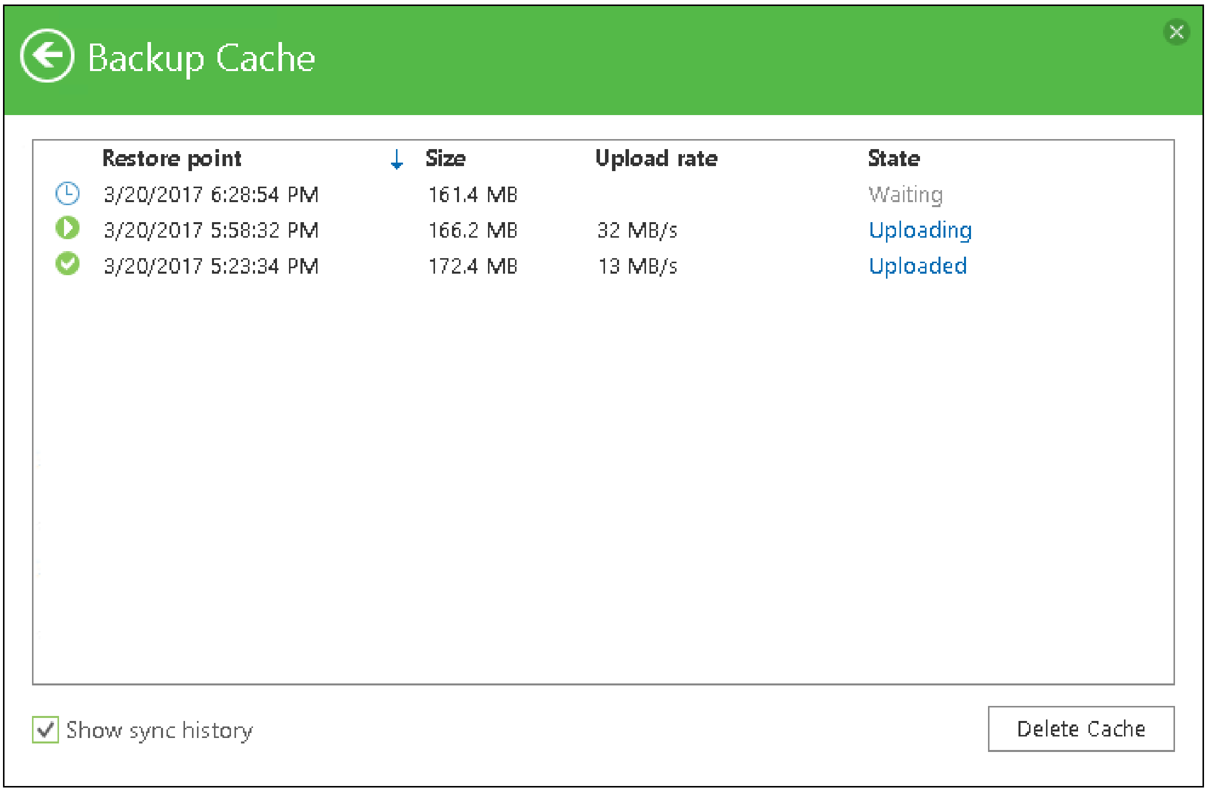


Restore point	Size	Upload rate	State
3/20/2017 6:28:54 PM	161.4 MB		Waiting
3/20/2017 5:58:32 PM	166.2 MB		Waiting
3/20/2017 5:23:34 PM	172.4 MB		Waiting

□ Show sync history

Viewing Backup Cache History

By default, the **Backup Cache** window 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, select the **Show sync history** option in the **Backup Cache** window.



Restore point	Size	Upload rate	State
3/20/2017 6:28:54 PM	161.4 MB		Waiting
3/20/2017 5:58:32 PM	166.2 MB	32 MB/s	Uploading
3/20/2017 5:23:34 PM	172.4 MB	13 MB/s	Uploaded

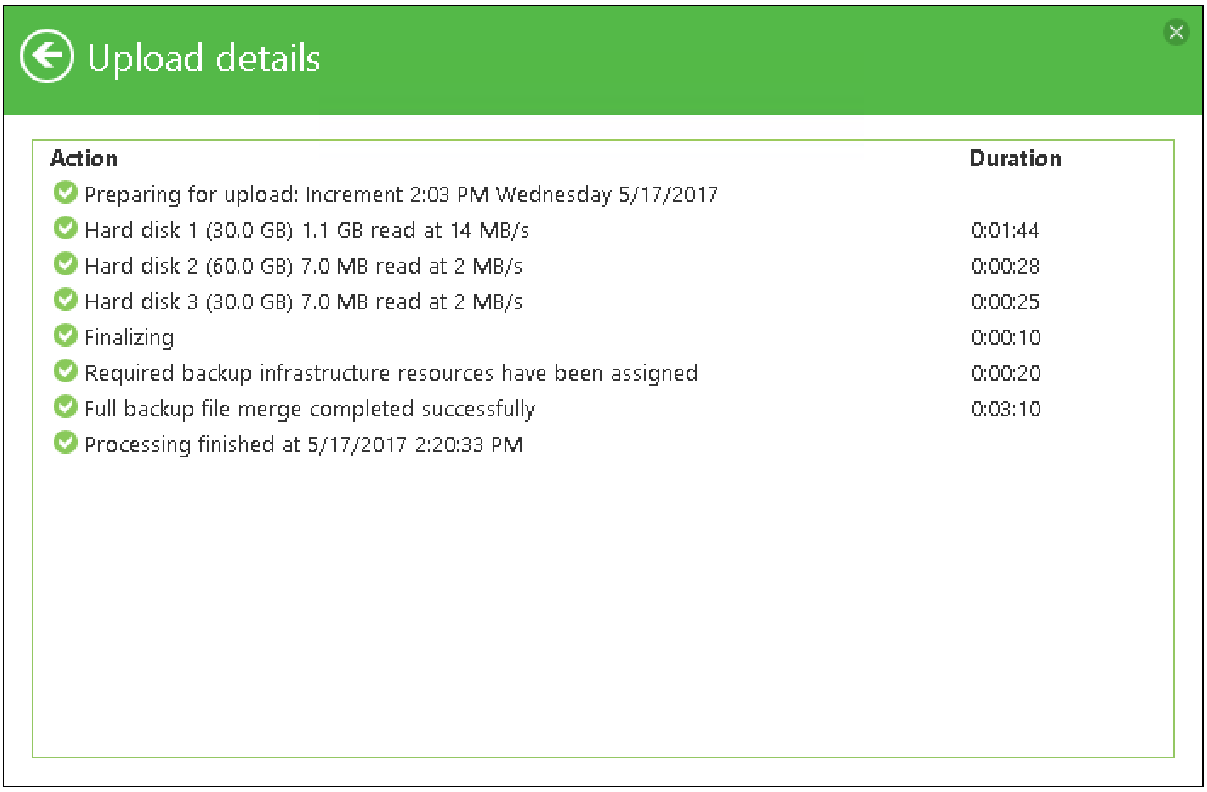
☑ Show sync history

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. Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **View cache**.
2. In the **Backup Cache** window, 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** window, Veeam Agent for Microsoft Windows will provide detailed information about operations performed as part of the restore point upload process.



Upload details

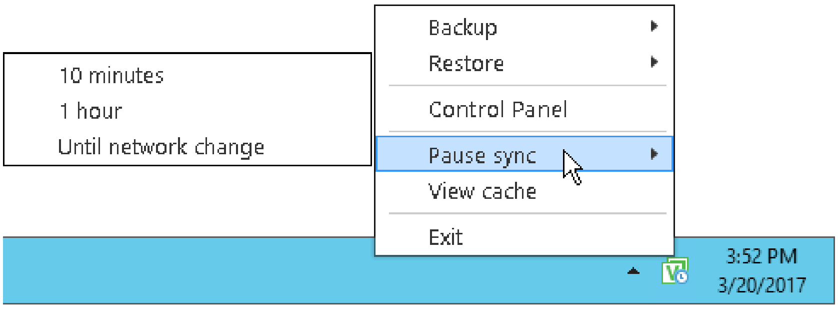
Action	Duration
✓ Preparing for upload: Increment 2:03 PM Wednesday 5/17/2017	
✓ Hard disk 1 (30.0 GB) 1.1 GB read at 14 MB/s	0:01:44
✓ Hard disk 2 (60.0 GB) 7.0 MB read at 2 MB/s	0:00:28
✓ Hard disk 3 (30.0 GB) 7.0 MB read at 2 MB/s	0:00:25
✓ Finalizing	0:00:10
✓ Required backup infrastructure resources have been assigned	0:00:20
✓ Full backup file merge completed successfully	0:03:10
✓ Processing finished at 5/17/2017 2:20:33 PM	

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. 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:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray.
2. 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.



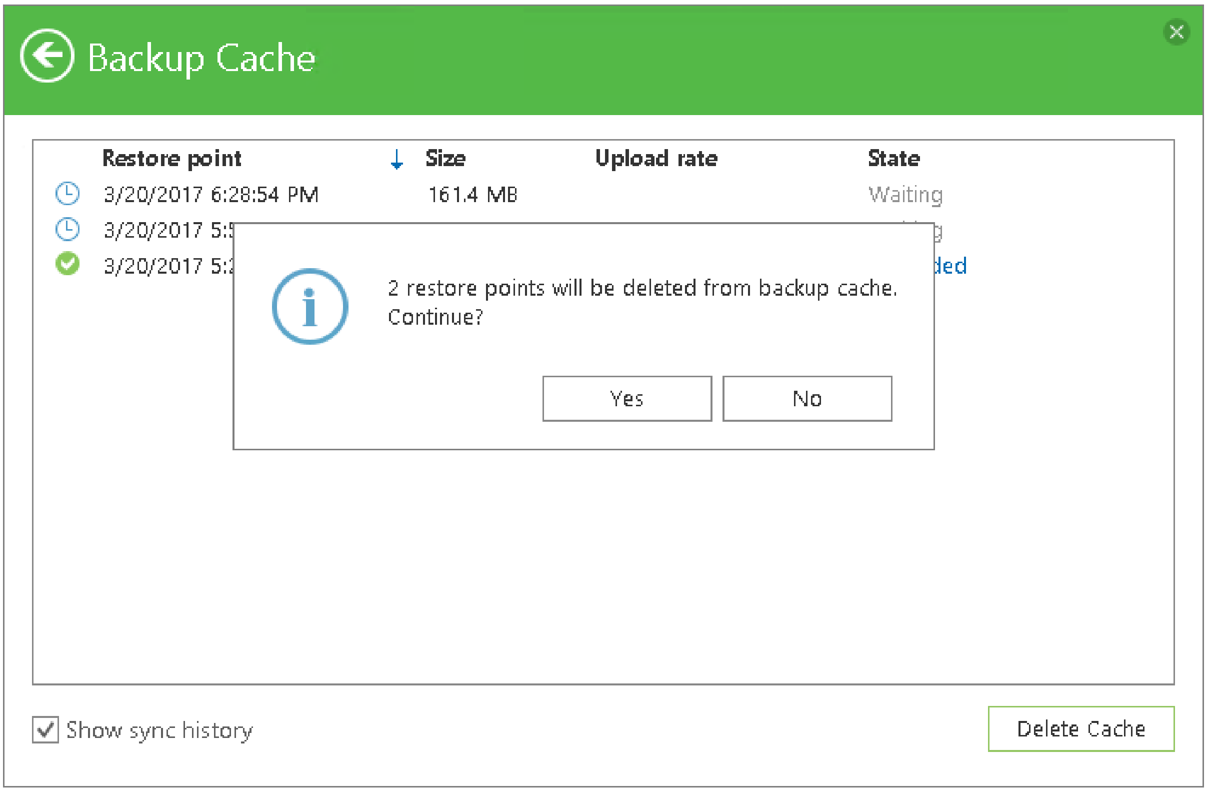
Deleting Restore Points from Backup Cache

You can delete restore points from the backup cache manually if needed. To delete restore points:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **View cache**.
2. In the **Backup Cache** window, 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.



Backup Cache

Restore point	Size	Upload rate	State
3/20/2017 6:28:54 PM	161.4 MB		Waiting
3/20/2017 5:5			g
3/20/2017 5:2			ded

2 restore points will be deleted from backup cache. Continue?

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 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 a network shared folder, on the backup repository managed by a Veeam backup server or on the cloud repository.
- 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.

Mind 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]**.
- 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.

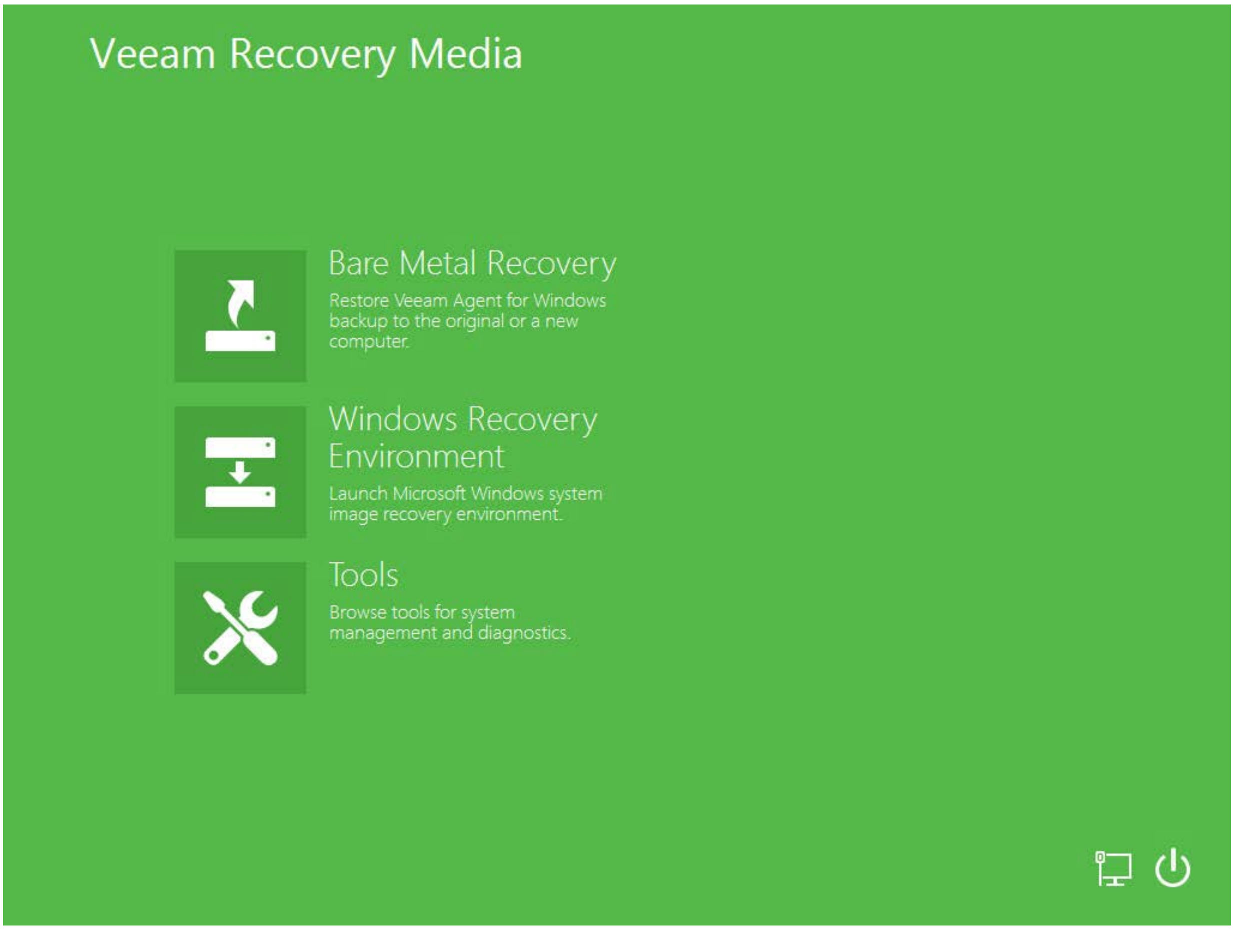
Step 1. Boot from Veeam Recovery Media

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.



Veeam Recovery Media

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.

TIP:

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**.

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:

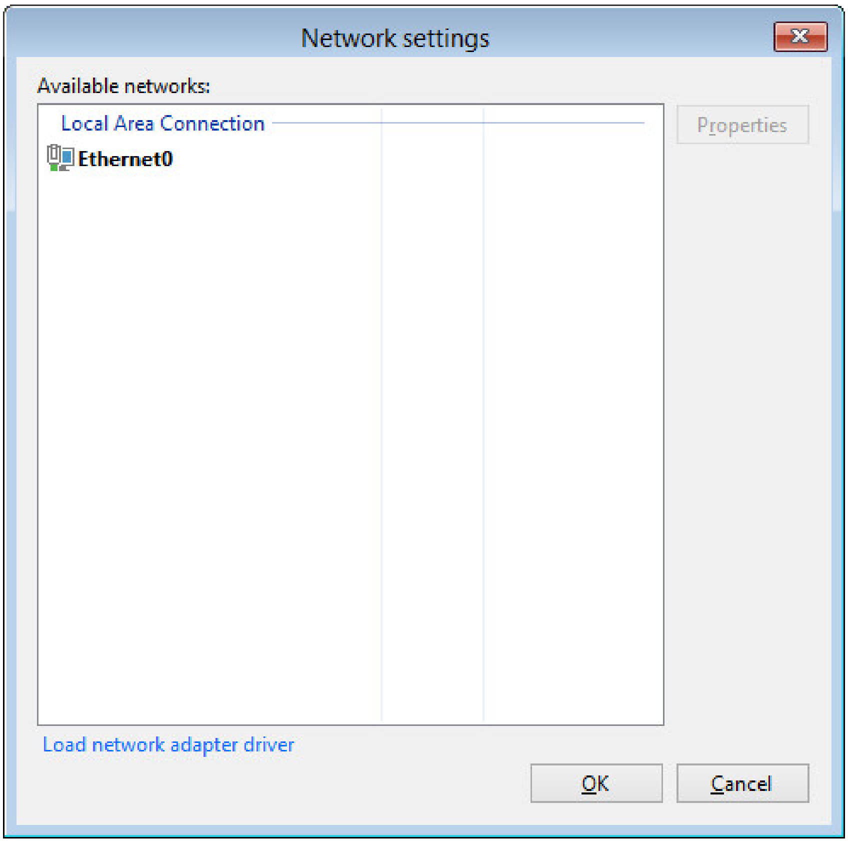
The *Network Settings* button appearance may vary depending on the detected network connection: Ethernet or wireless. If your computer is connected to a wireless network, the *Network Settings* button will indicate Wi-Fi signal strength.

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.


Network settings

Available networks:

Local Area Connection

Ethernet0

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.

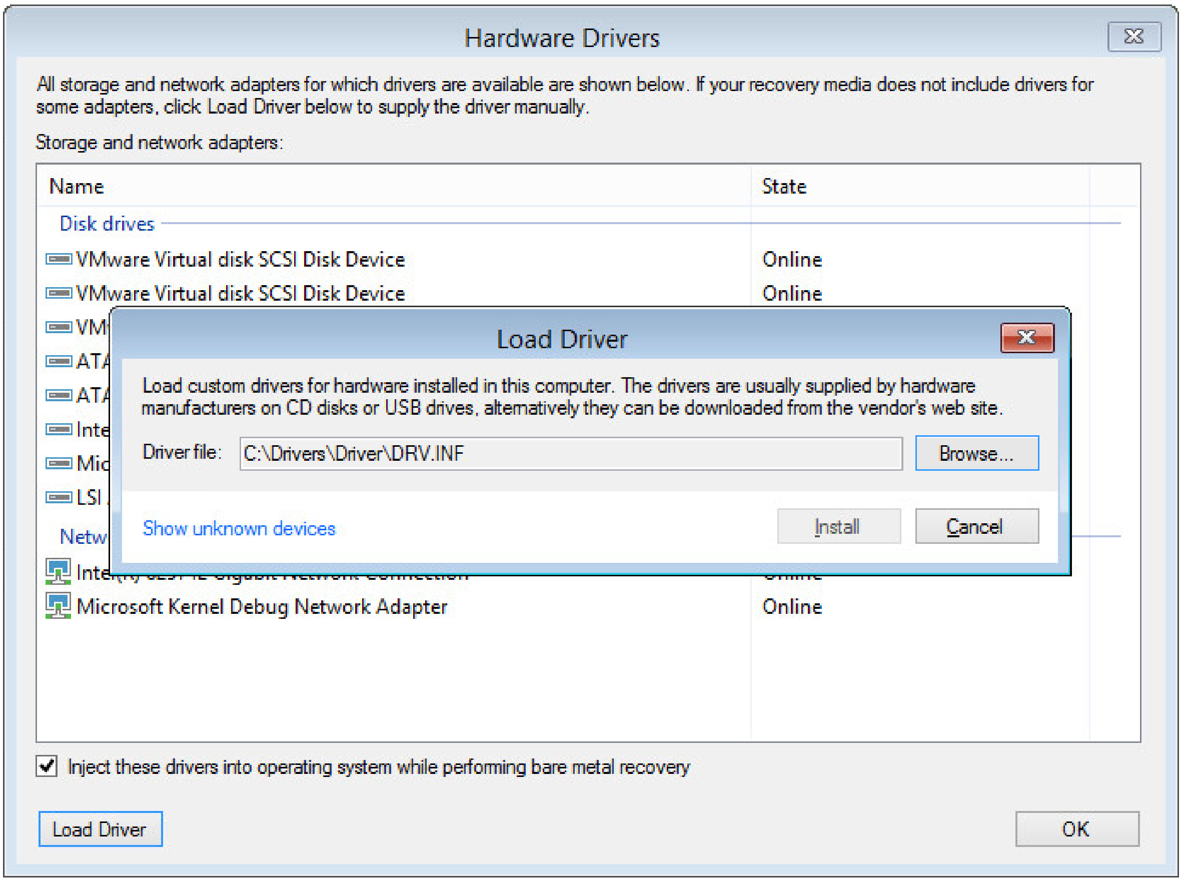
To install drivers that were included in the Veeam Recovery Media:

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**.



Hardware Drivers

All storage and network adapters for which drivers are available are shown below. If your recovery media does not include drivers for some adapters, click Load Driver below to supply the driver manually.

Storage and network adapters:

Name	State
Disk drives	
VMware Virtual disk SCSI Disk Device	Online
VMware Virtual disk SCSI Disk Device	Online
VM	
ATA	
ATA	
Inte	
Mic	
LSI	
Netw	
Inte	
Microsoft Kernel Debug Network Adapter	Online

Load Driver

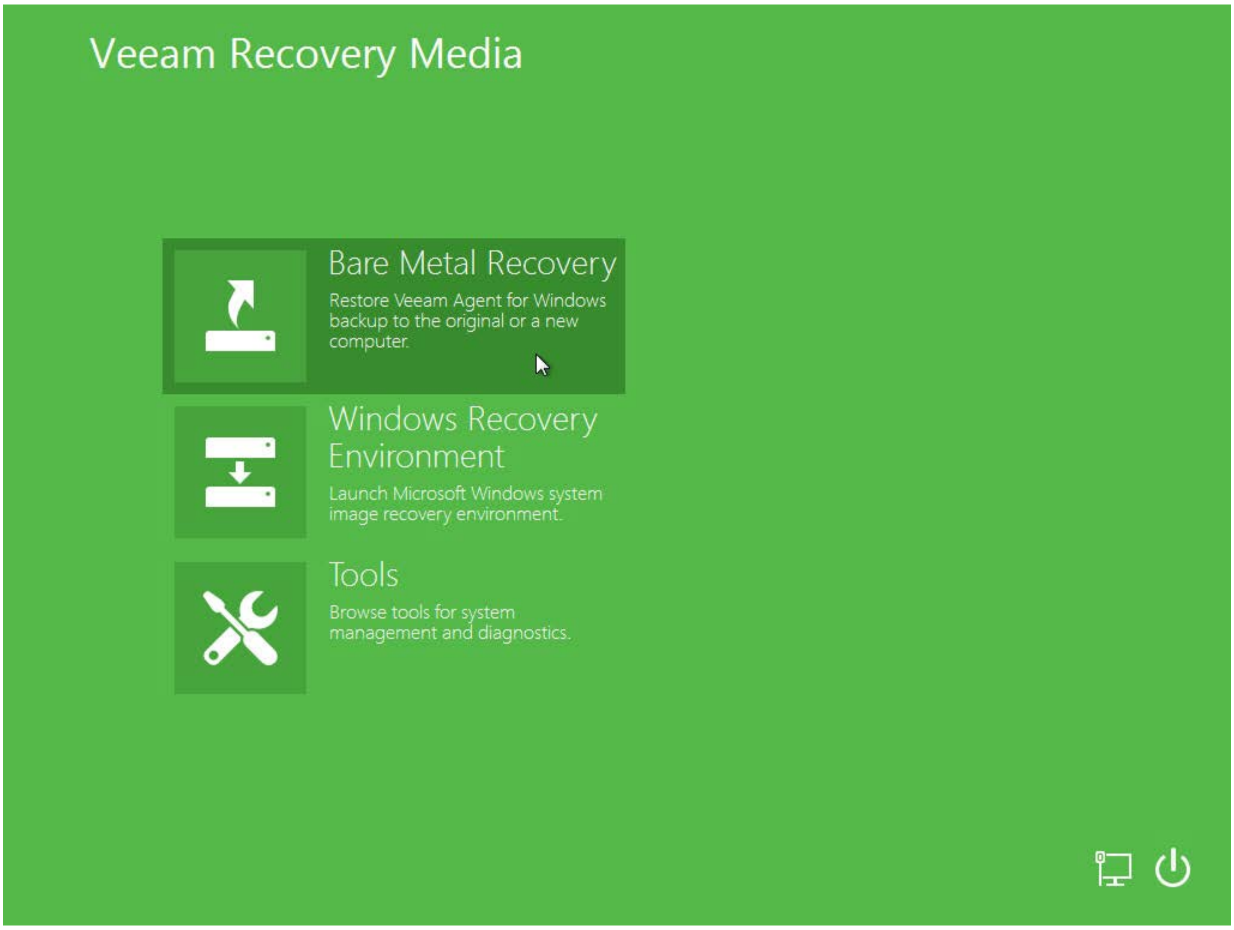
Load custom drivers for hardware installed in this computer. The drivers are usually supplied by hardware manufacturers on CD disks or USB drives, alternatively they can be downloaded from the vendor's web site.

Driver file: C:\Drivers\Driver\DRV.INF

☑ Inject these drivers into operating system while performing bare metal recovery

Step 3. Launch Veeam Recovery Media Wizard

To launch the **Veeam Recovery Media** wizard, on the **Veeam Recovery Media** screen, click **Bare Metal Recovery**.

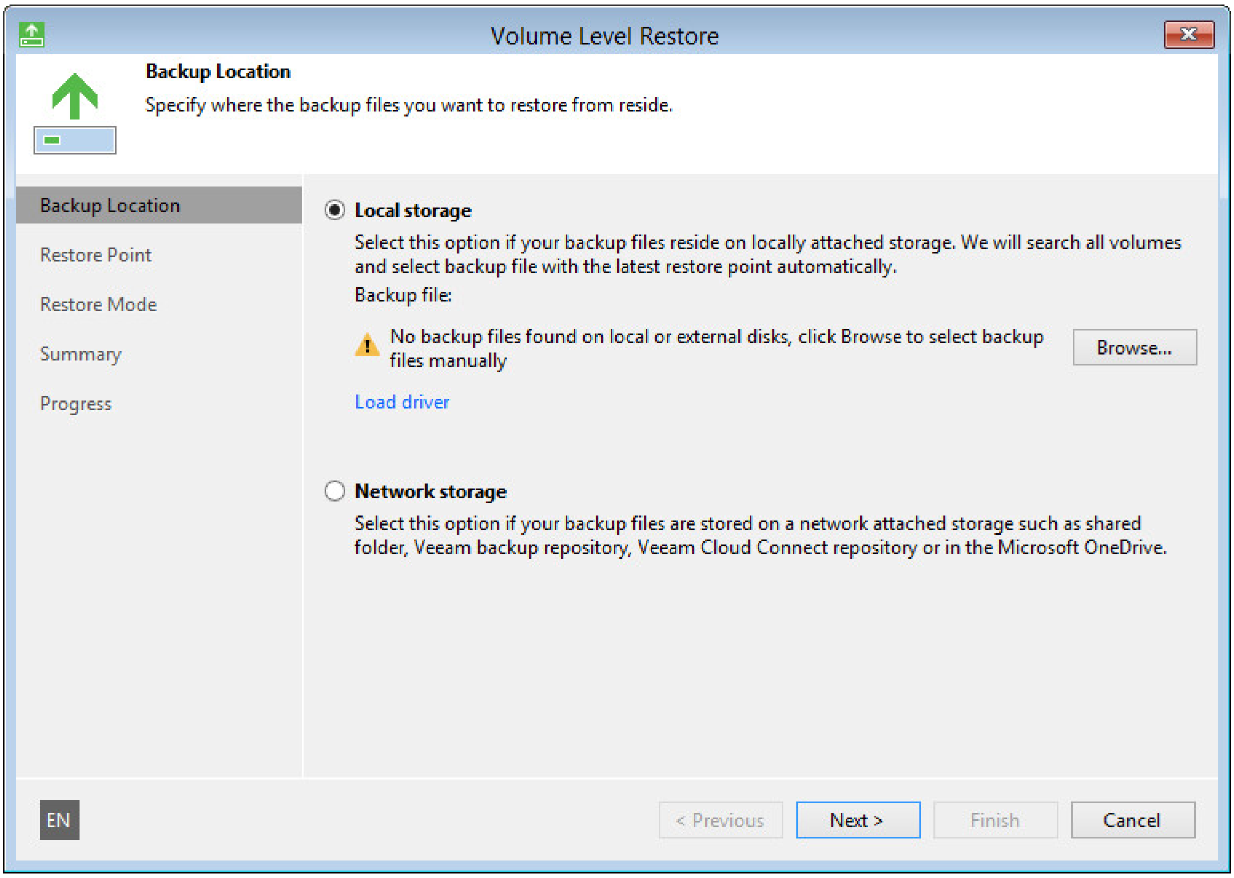

Veeam Recovery Media
Bare Metal Recovery
Restore Veeam Agent for Windows backup to the original or a new computer.
Windows Recovery Environment
Launch Microsoft Windows system image recovery environment.
Tools
Browse tools for system management and diagnostics.

Step 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 a network shared folder, on 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 a network shared folder, in a Microsoft OneDrive cloud storage, on a backup repository managed by a Veeam backup server or on 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.



Volume Level Restore

Backup Location

Specify where the backup files you want to restore from reside.

● **Local storage**

Select this option if your backup files reside on locally attached storage. We will search all volumes and select backup file with the latest restore point automatically.

Backup file:

⚠ No backup files found on local or external disks, click Browse to select backup files manually

○ **Network storage**

Select this option if your backup files are stored on a network attached storage such as shared folder, Veeam backup repository, Veeam Cloud Connect repository or in the Microsoft OneDrive.

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.

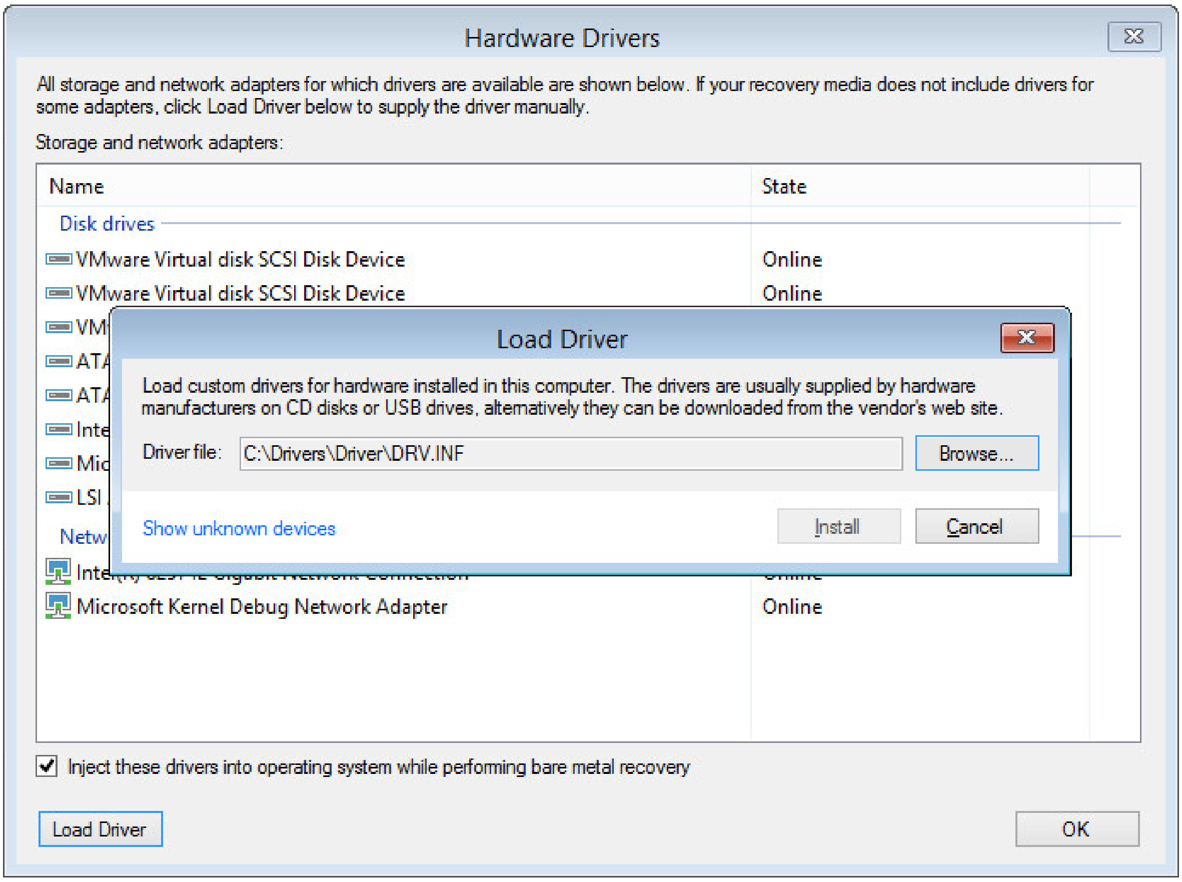
To install drivers that were included in the Veeam Recovery Media:

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**.



All storage and network adapters for which drivers are available are shown below. If your recovery media does not include drivers for some adapters, click Load Driver below to supply the driver manually.

Storage and network adapters:

Name	State
Disk drives	
VMware Virtual disk SCSI Disk Device	Online
VMware Virtual disk SCSI Disk Device	Online
VM	
ATA	
ATA	
Inte	
Mic	
LSI	
Netw	
Inte	
Microsoft Kernel Debug Network Adapter	Online

Load custom drivers for hardware installed in this computer. The drivers are usually supplied by hardware manufacturers on CD disks or USB drives, alternatively they can be downloaded from the vendor's web site.

Driver file: C:\Drivers\Driver\DRV.INF

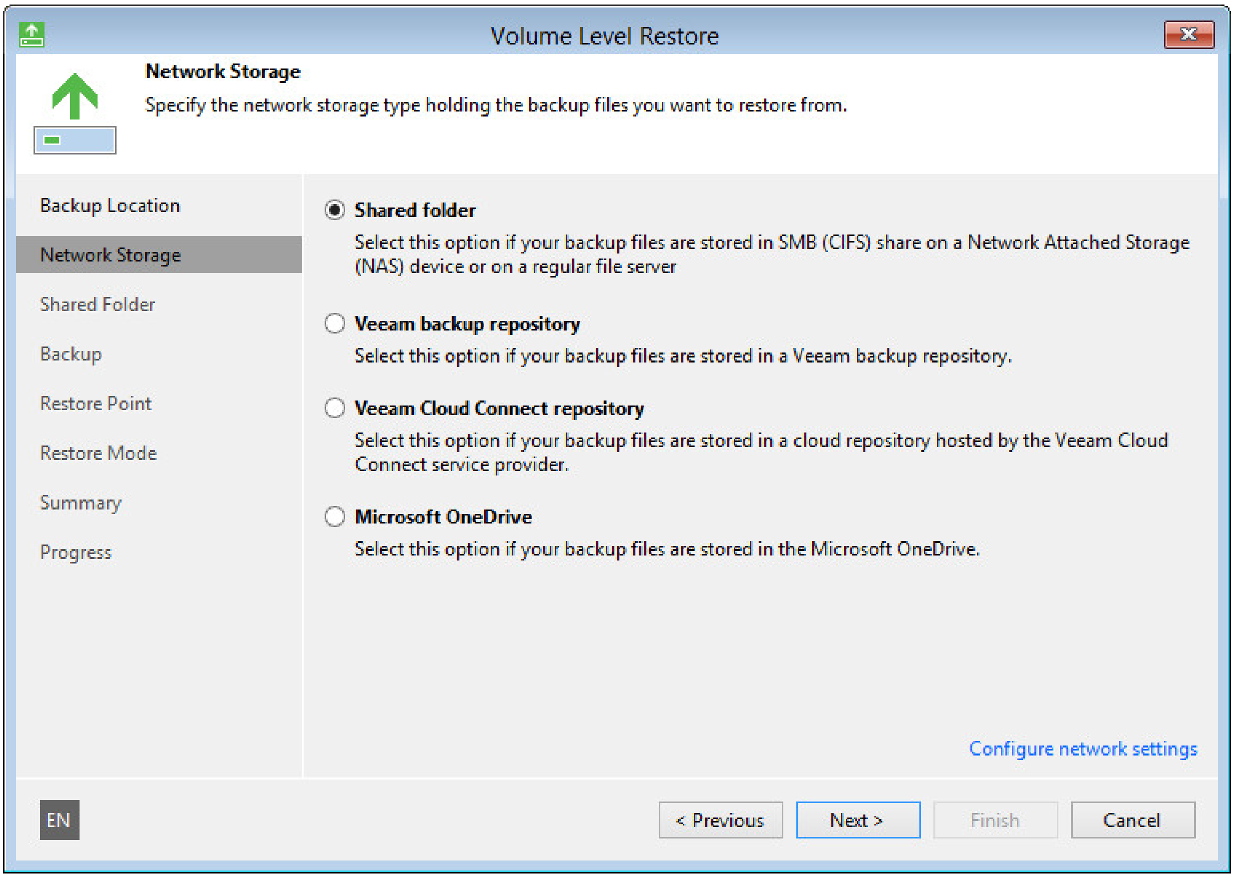
☑ Inject these drivers into operating system while performing bare metal recovery

Step 5. Select Remote 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 a network shared folder, on a backup repository or a cloud repository.

Select where the backup file resides:

- **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 on 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 on 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.
- **Microsoft OneDrive** — select this option if the backup file resides in a Microsoft OneDrive cloud storage. With this option selected, you will pass to the Microsoft OneDrive step of the wizard.



Volume Level Restore

Network Storage

Specify the network storage type holding the backup files you want to restore from.

● **Shared folder**
Select this option if your backup files are stored in SMB (CIFS) share on a Network Attached Storage (NAS) device or on a regular file server

○ **Veeam backup repository**
Select this option if your backup files are stored in a Veeam backup repository.

○ **Veeam Cloud Connect repository**
Select this option if your backup files are stored in a cloud repository hosted by the Veeam Cloud Connect service provider.

○ **Microsoft OneDrive**
Select this option if your backup files are stored in the Microsoft OneDrive.

Step 6. Specify Remote 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.
- Microsoft OneDrive settings — if you have selected the **Microsoft OneDrive** option at the Network Storage step of the wizard.

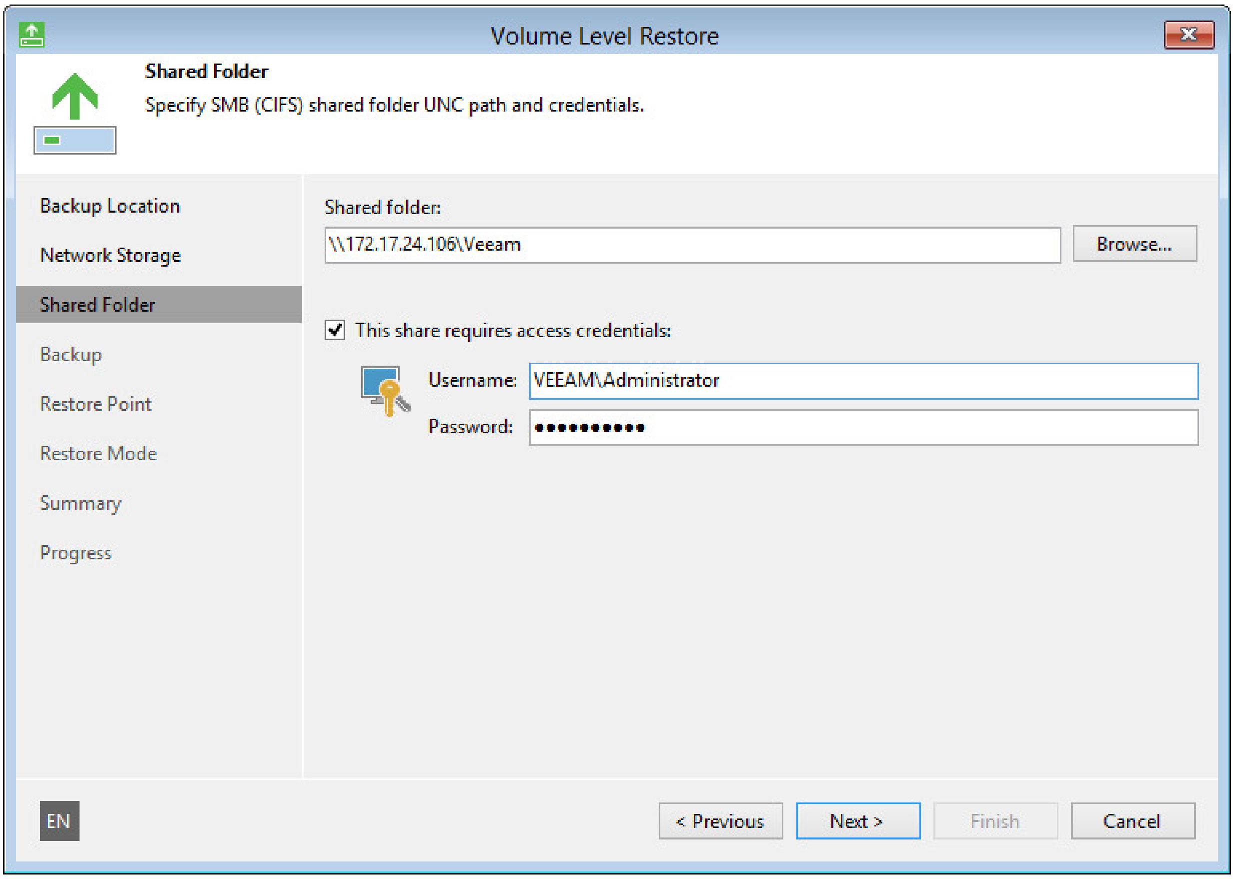
Shared Folder Settings

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 access permissions on this shared folder. The user name must be specified in the *DOMAIN\USERN*AME format.

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



Volume Level Restore

Shared Folder

Specify SMB (CIFS) shared folder UNC path and credentials.

Shared folder: \\172.17.24.106\Veeam

☑ This share requires access credentials:

Username: VEEAM\Administrator

Password: ••••••••••

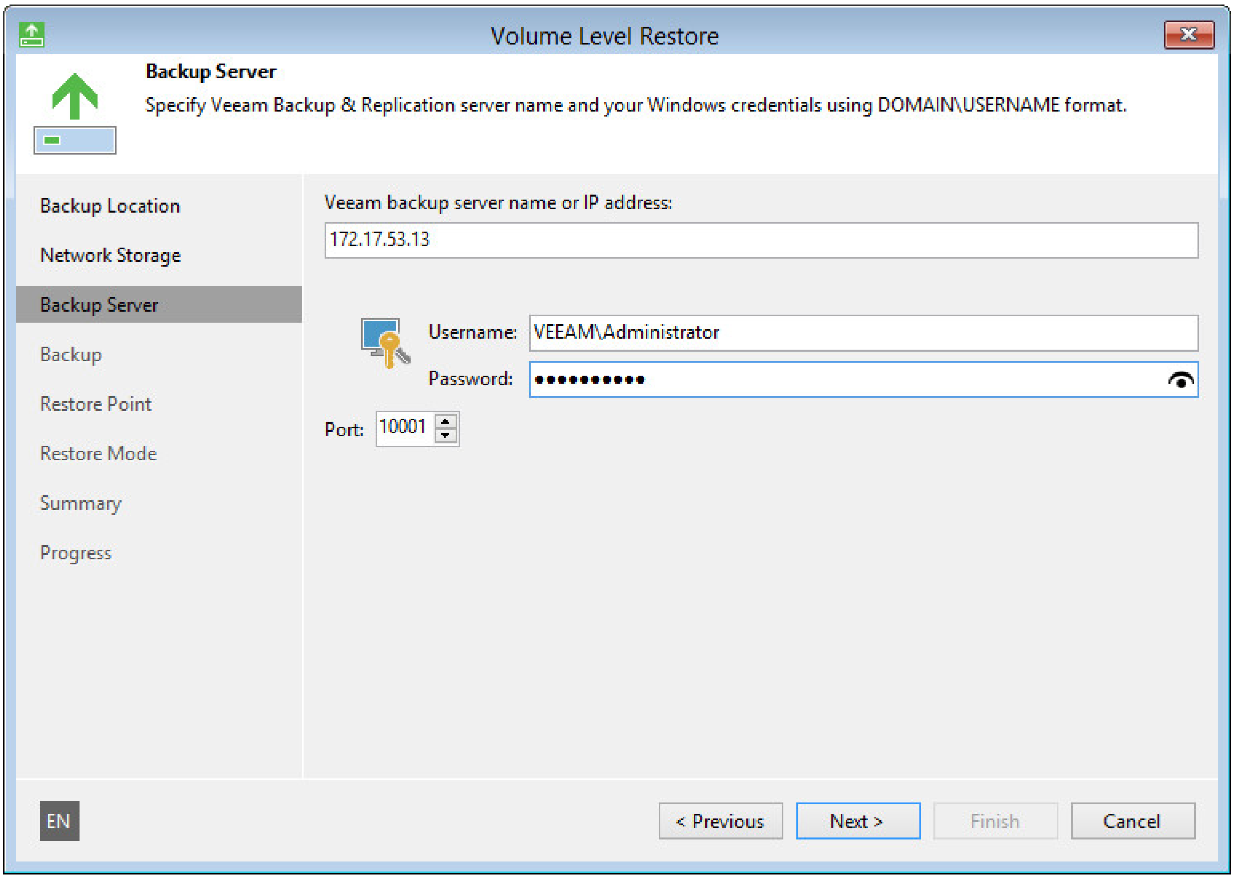
Backup Server Settings

The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located on 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 **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.
3. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup repository. By default, Veeam Agent for Microsoft Windows uses port 10001.

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



Volume Level Restore

Backup Server

Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.

Veeam backup server name or IP address: 172.17.53.13

Username: VEEAM\Administrator

Password: ••••••••••

Port: 10001

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:

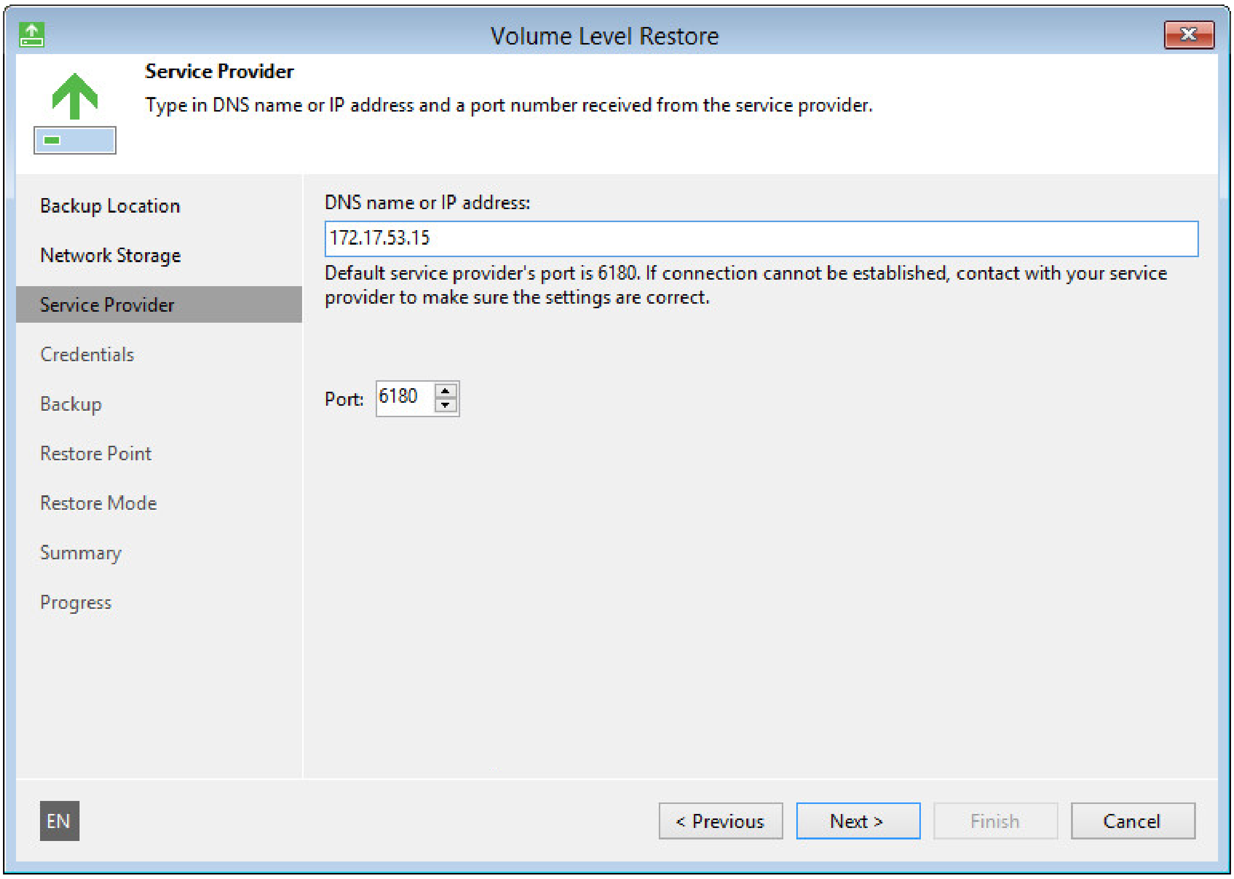
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

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.



Service Provider

Type in DNS name or IP address and a port number received from the service provider.

DNS name or IP address: 172.17.53.15

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

Port: 6180

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.

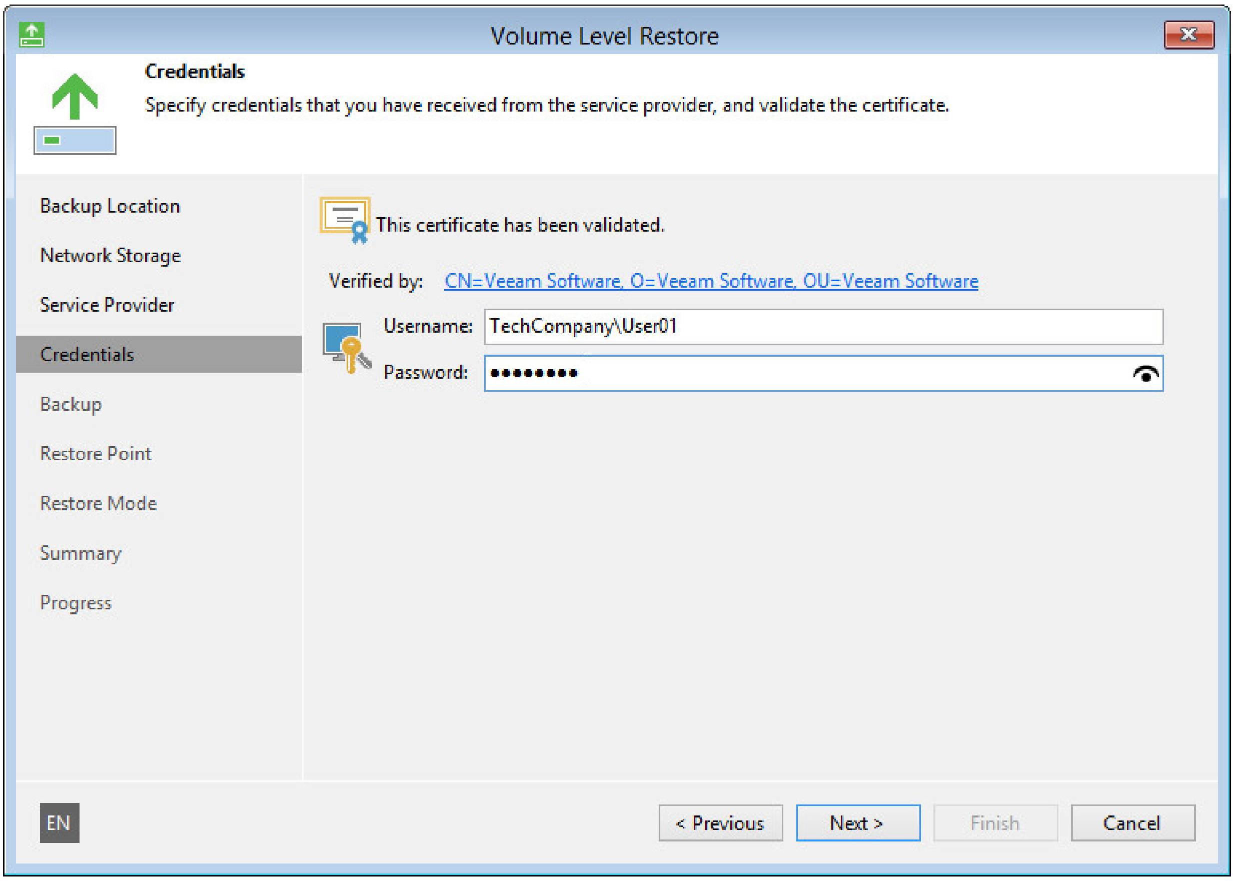
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   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.



Credentials

Specify credentials that you have received from the service provider, and validate the certificate.

This certificate has been validated.

Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software

Username: TechCompany\User01

Password: ••••••••

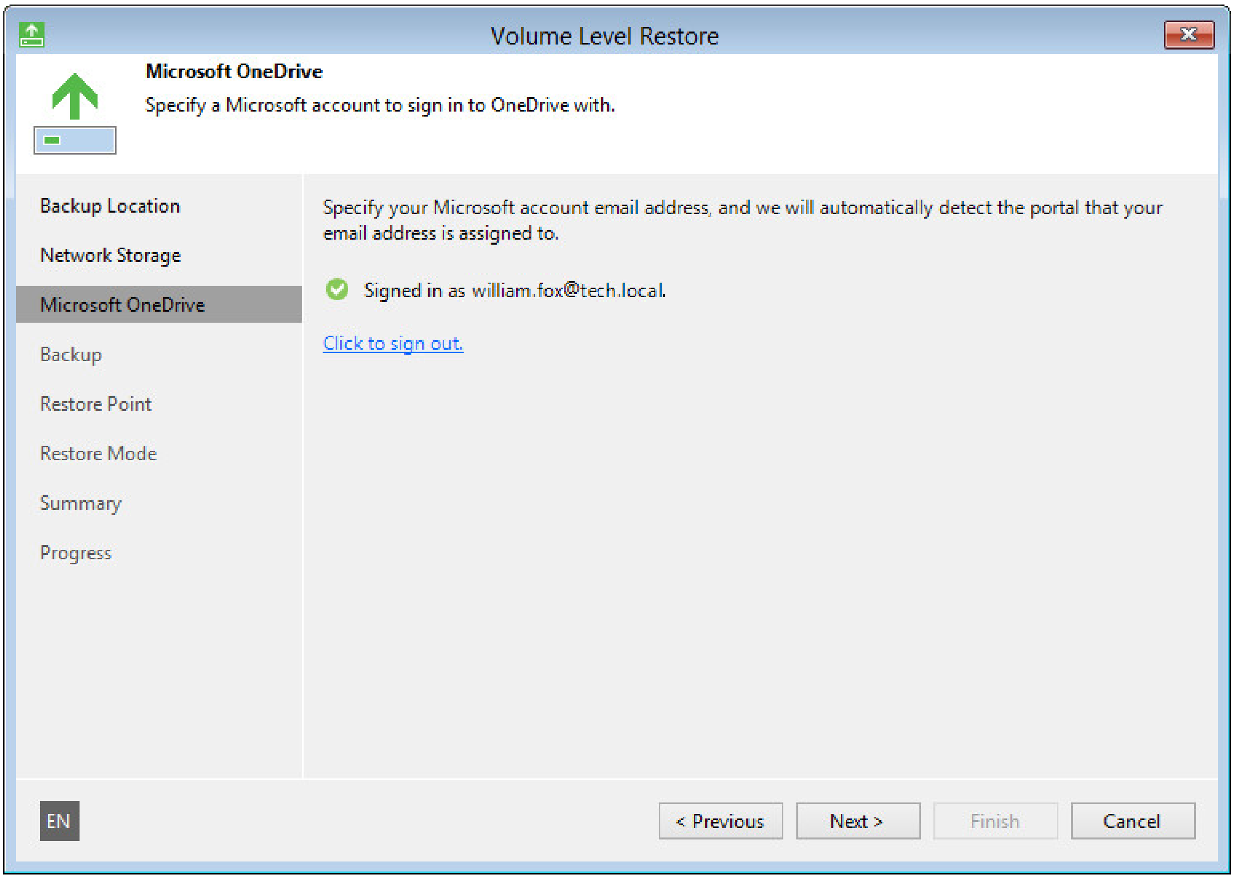
Microsoft OneDrive Settings

The **Microsoft OneDrive** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft OneDrive cloud storage.

Specify settings to connect to Microsoft OneDrive:

1. Click **Click to sign in to Microsoft OneDrive**.
2. In the **Sign in to your account** window, follow instructions to specify credentials of the Microsoft OneDrive account that has access to the storage where the backup file resides and click **Sign in**.

If you want to change settings to connect to Microsoft OneDrive, click the **Click to sign out** link and repeat steps 1–2 to specify another account.



Microsoft OneDrive

Specify a Microsoft account to sign in to OneDrive with.

Specify your Microsoft account email address, and we will automatically detect the portal that your email address is assigned to.

✓ Signed in as william.fox@tech.local.

Click to sign out.

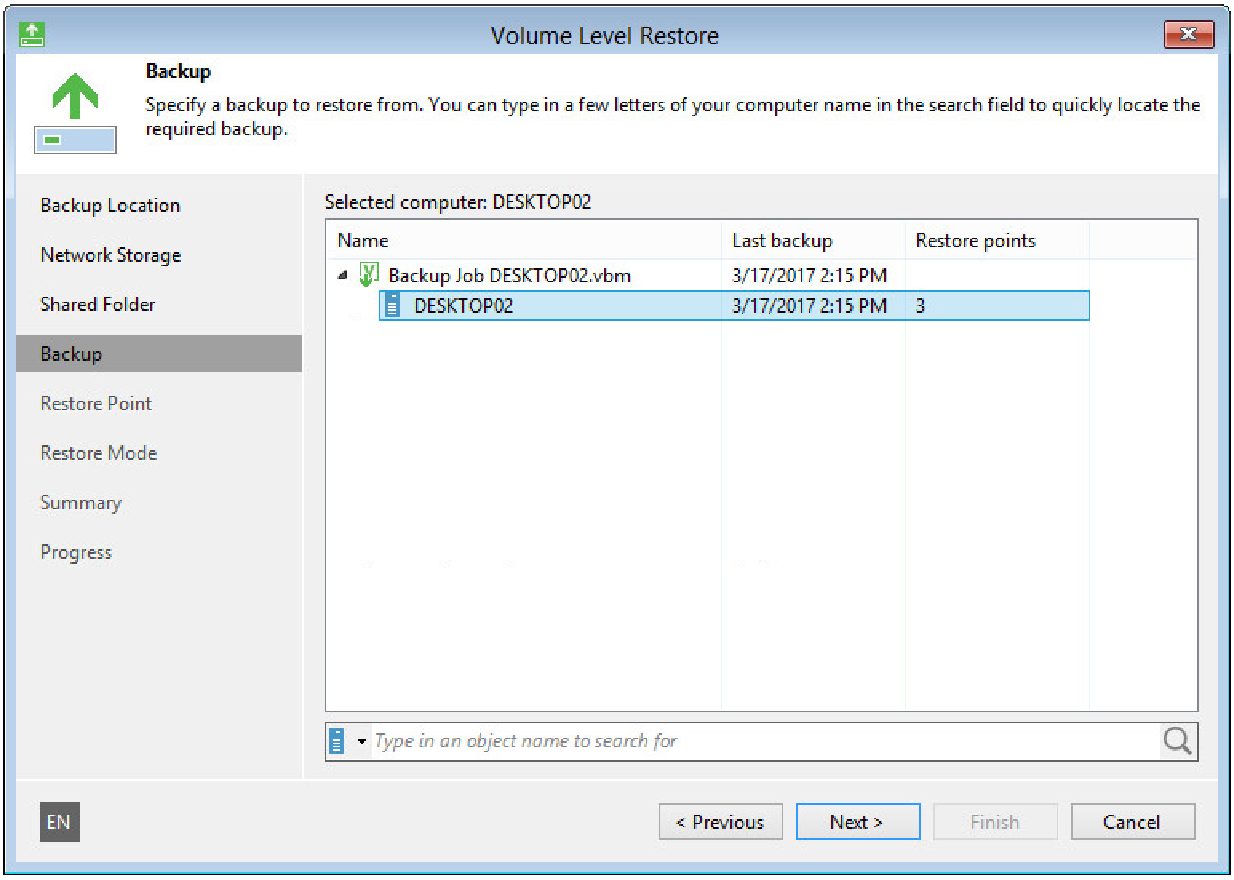
Step 7. Select Backup

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 a network shared folder, on 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 on 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.



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.

Selected computer: DESKTOP02

Name	Last backup	Restore points
Backup Job DESKTOP02.vbm	3/17/2017 2:15 PM	
DESKTOP02	3/17/2017 2:15 PM	3

Type in an object name to search for

NOTE:

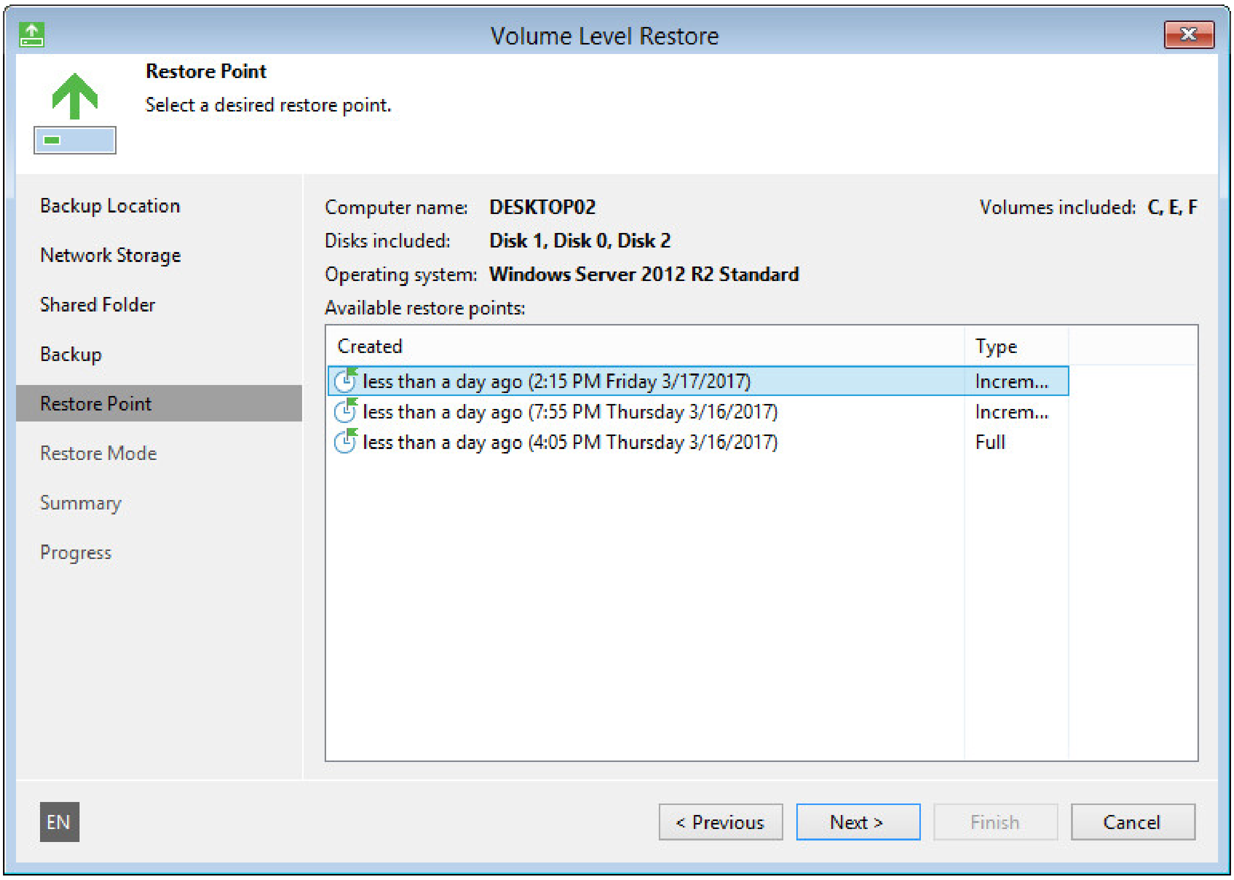
If you want to restore data from an encrypted backup, and the Veeam Recovery Media from which you have booted your computer does not contain encryption keys required to unlock the backup file, you need to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.

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 for Microsoft Windows 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 for Microsoft Windows will display only 2 restore points in the list.



Computer name: **DESKTOP02**

Volumes included: **C, E, F**

Disks included: **Disk 1, Disk 0, Disk 2**

Operating system: **Windows Server 2012 R2 Standard**

Available restore points:

Created	Type
less than a day ago (2:15 PM Friday 3/17/2017)	Increm...
less than a day ago (7:55 PM Thursday 3/16/2017)	Increm...
less than a day ago (4:05 PM Thursday 3/16/2017)	Full

Step 9. Select Data Restore Mode

At the **Restore Mode** step of the wizard, select the data restore mode:

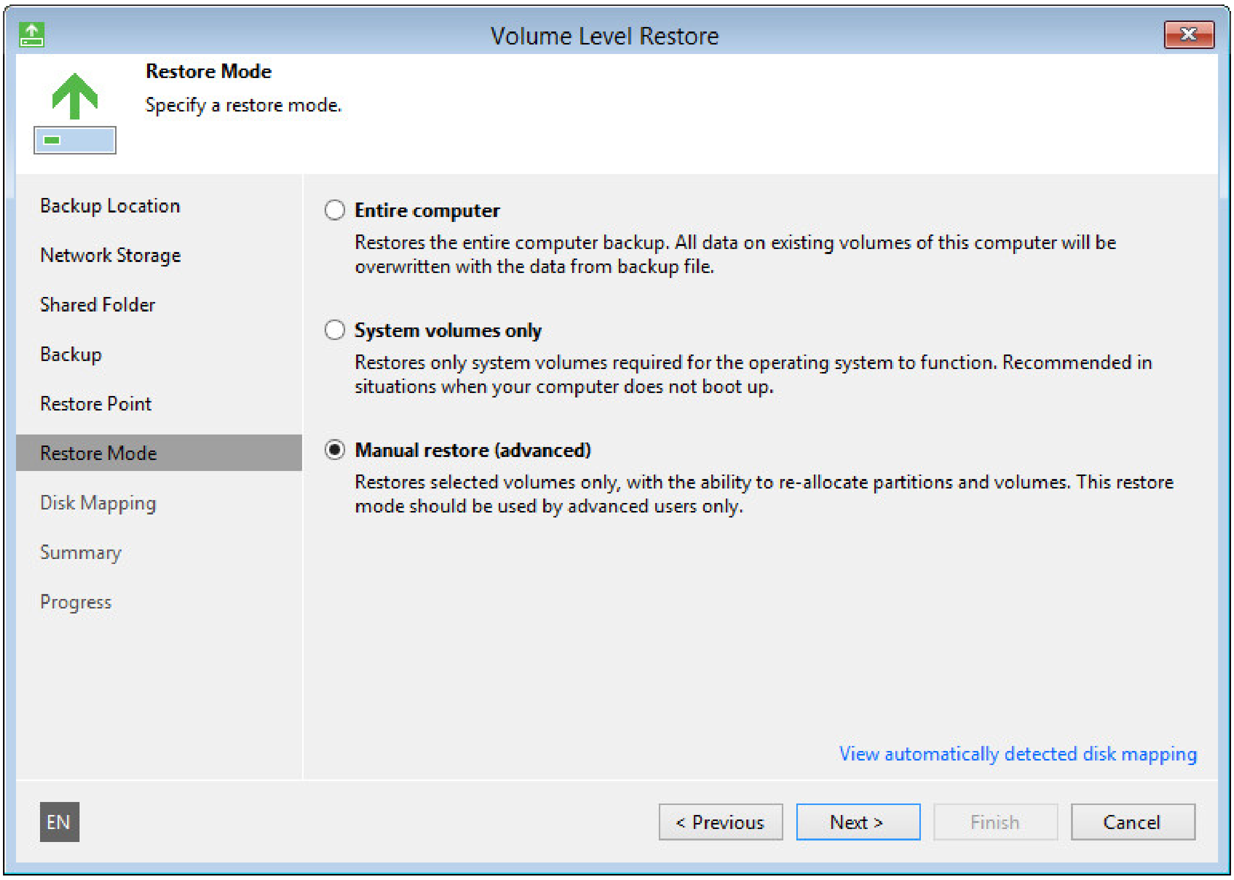
- **Entire computer** — select this option if you want to restore the whole system image of your computer. In this case, Veeam Agent for Microsoft Windows will attempt to map volumes from the backup to existing computer volumes and will overwrite existing data with data restored from the backup.
- **System 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, 8.1, 10, 2012 and 2012 R2, Veeam Agent for Microsoft Windows will additionally restore the recovery partition.

- **Manual restore (advanced)** — 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.



○ **Entire computer**
Restores the entire computer backup. All data on existing volumes of this computer will be overwritten with the data from backup file.

○ **System volumes only**
Restores only system volumes required for the operating system to function. Recommended in situations when your computer does not boot up.

● **Manual restore (advanced)**
Restores selected volumes only, with the ability to re-allocate partitions and volumes. This restore mode should be used by advanced users only.

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.

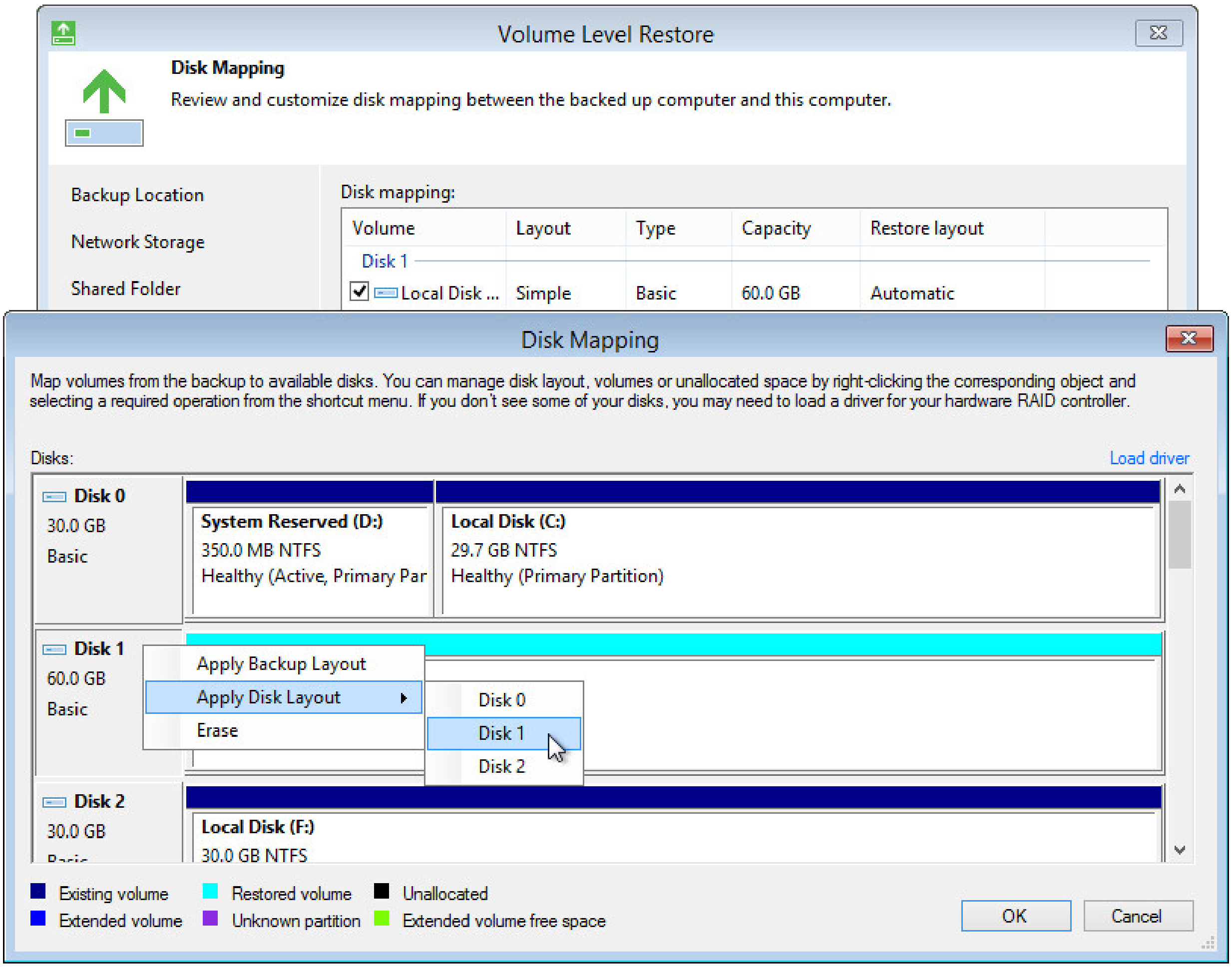
You can map volumes that you want to restore from the backup to disks on the target computer.

IMPORTANT!

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 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.



Volume Level Restore

Disk Mapping

Review and customize disk mapping between the backed up computer and this computer.

Disk mapping:

Volume	Layout	Type	Capacity	Restore layout
Disk 1				
☑ Local Disk ...	Simple	Basic	60.0 GB	Automatic

Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

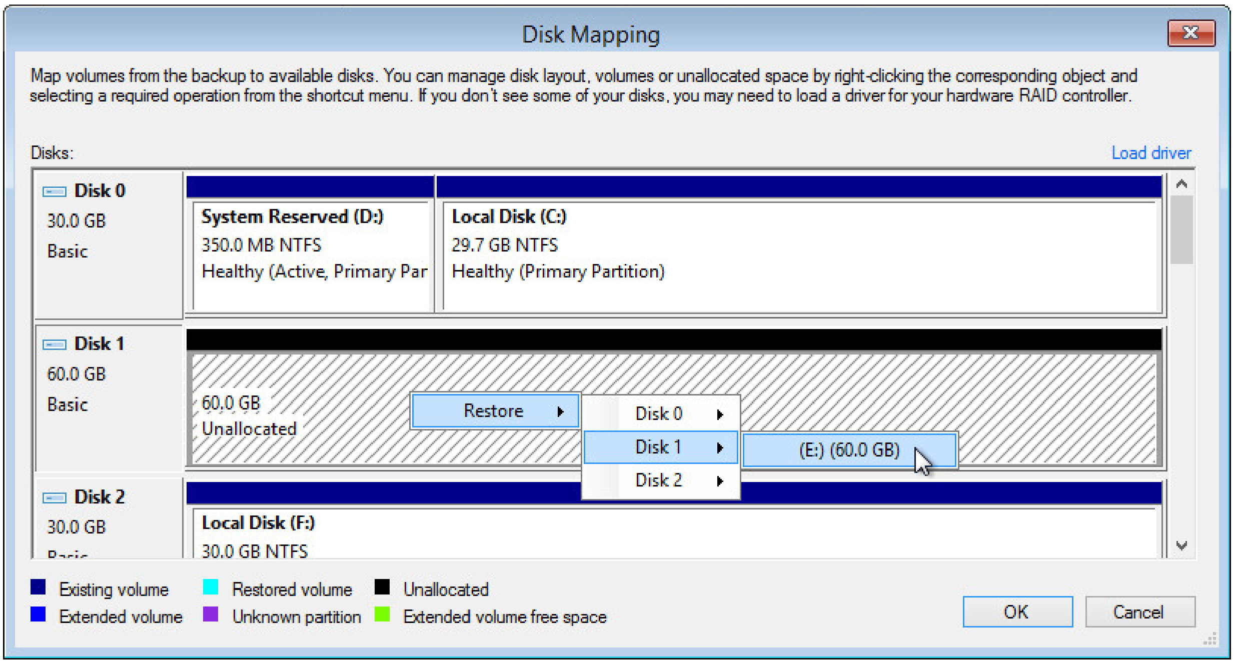
Disk 0 30.0 GB Basic — **System Reserved (D:)** 350.0 MB NTFS Healthy (Active, Primary Par — **Local Disk (C:)** 29.7 GB NTFS Healthy (Primary Partition)

Disk 1 60.0 GB Basic

Disk 2 30.0 GB Basic — **Local Disk (F:)** 30.0 GB NTFS

- 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 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.



Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

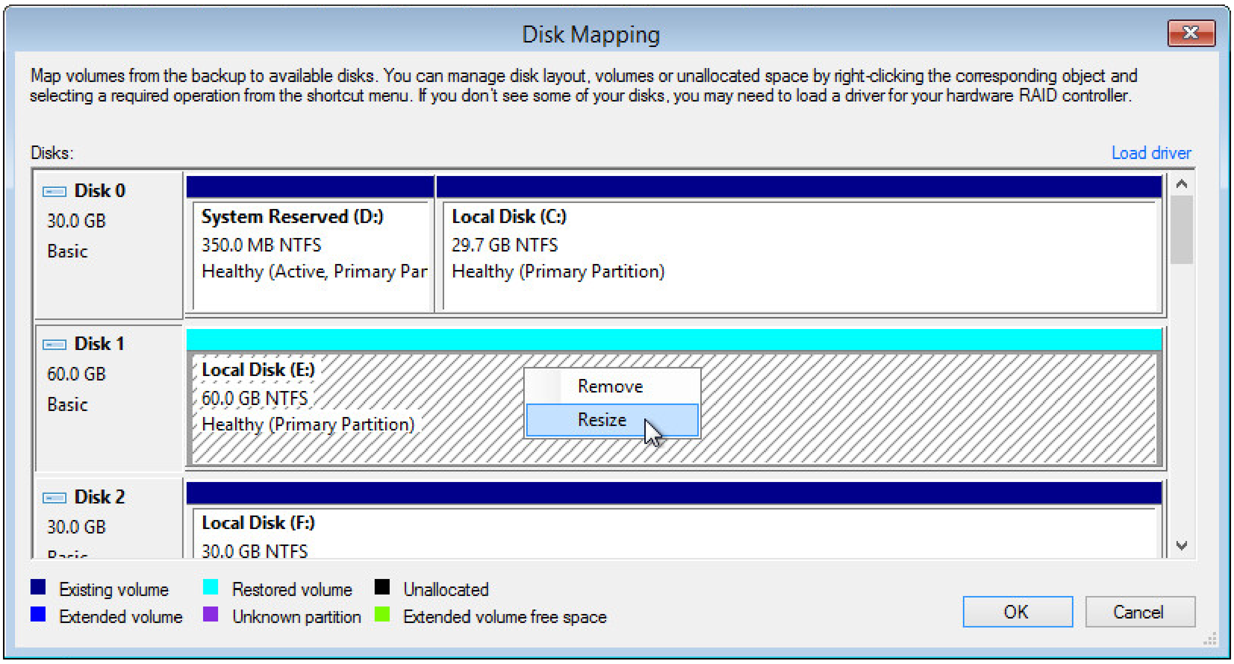
Disks:

Disk 0 30.0 GB Basic	System Reserved (D:) 350.0 MB NTFS Healthy (Active, Primary Par	Local Disk (C:) 29.7 GB NTFS Healthy (Primary Partition)
Disk 1 60.0 GB Basic	60.0 GB Unallocated	
Disk 2 30.0 GB Basic	Local Disk (F:) 30.0 GB NTFS	

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.



Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

Disk 0 30.0 GB Basic	System Reserved (D:) 350.0 MB NTFS Healthy (Active, Primary Par	Local Disk (C:) 29.7 GB NTFS Healthy (Primary Partition)
Disk 1 60.0 GB Basic	Local Disk (E:) 60.0 GB NTFS Healthy (Primary Partition)	
Disk 2 30.0 GB Basic	Local Disk (F:) 30.0 GB NTFS	

Installing Storage Adapters 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.

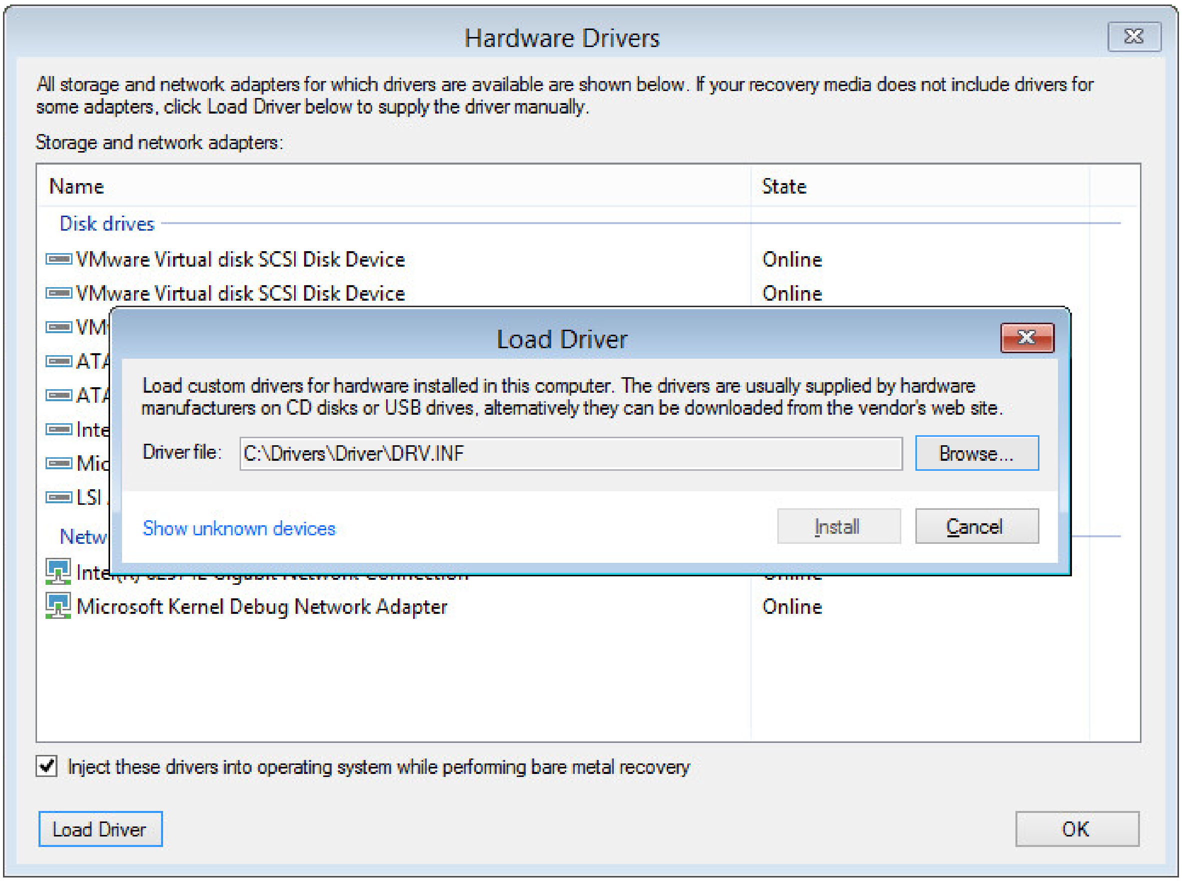
To install drivers that were included in the Veeam Recovery Media:

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**.



Hardware Drivers

All storage and network adapters for which drivers are available are shown below. If your recovery media does not include drivers for some adapters, click Load Driver below to supply the driver manually.

Storage and network adapters:

Name	State
Disk drives	
VMware Virtual disk SCSI Disk Device	Online
VMware Virtual disk SCSI Disk Device	Online
VM	
ATA	
ATA	
Inte	
Mic	
LSI	
Netw	
Inte	
Microsoft Kernel Debug Network Adapter	Online

☑ Inject these drivers into operating system while performing bare metal recovery

Load Driver

Load custom drivers for hardware installed in this computer. The drivers are usually supplied by hardware manufacturers on CD disks or USB drives, alternatively they can be downloaded from the vendor's web site.

Driver file: C:\Drivers\Driver\DRV.INF

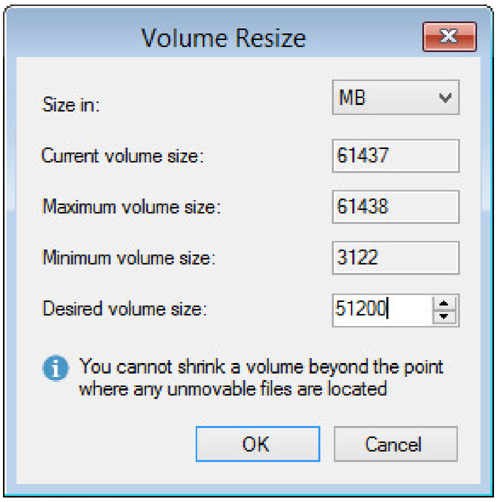
Step 11. Resize Restored Volumes

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.



Volume Resize

Size in: MB

Current volume size: 61437

Maximum volume size: 61438

Minimum volume size: 3122

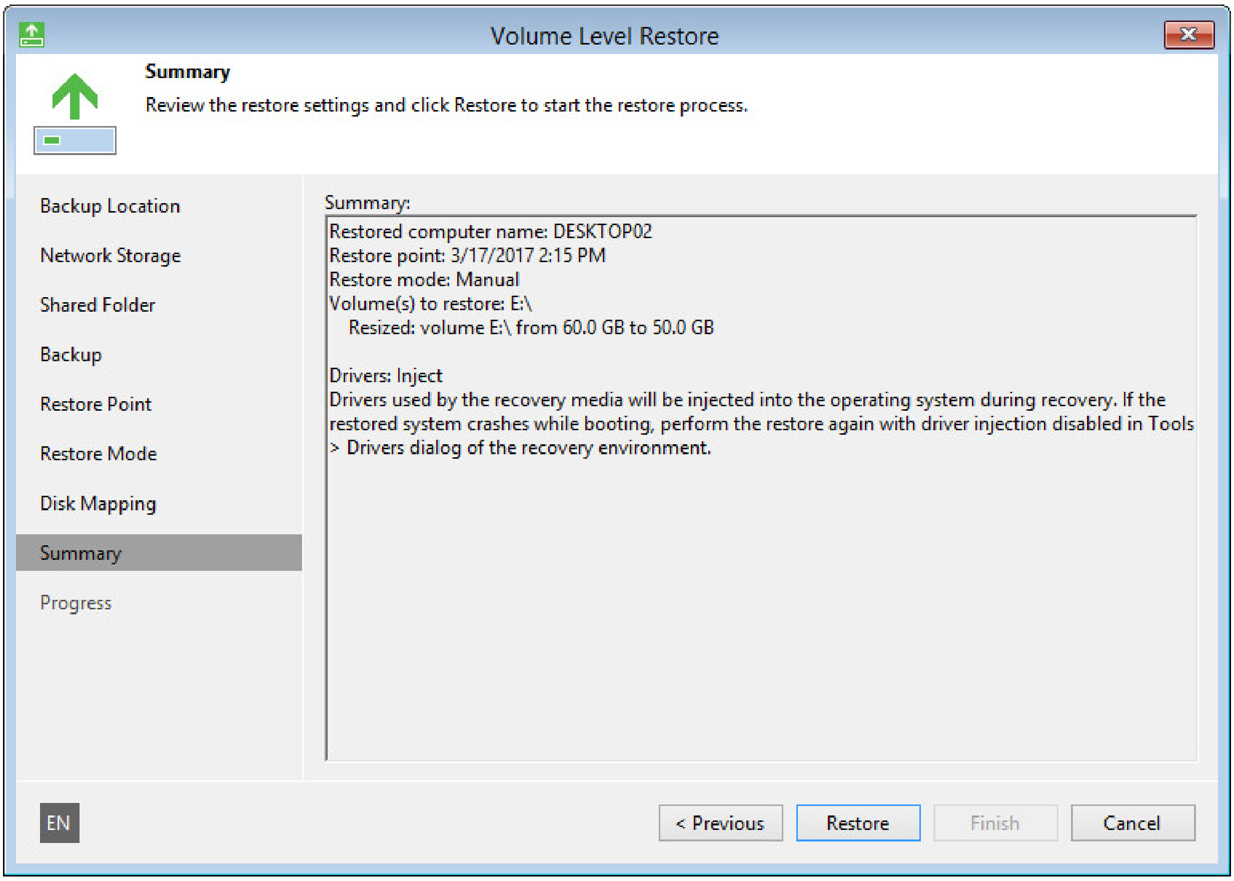
Desired volume size: 51200

You cannot shrink a volume beyond the point where any unmovable files are located

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.



Summary:

Restored computer name: DESKTOP02
Restore point: 3/17/2017 2:15 PM
Restore mode: Manual
Volume(s) to restore: E:\
Resized: volume E:\ from 60.0 GB to 50.0 GB

Drivers: Inject
Drivers used by the recovery media will be injected into the operating system during recovery. If the restored system crashes while booting, perform the restore again with driver injection disabled in Tools > Drivers dialog of the recovery environment.

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.

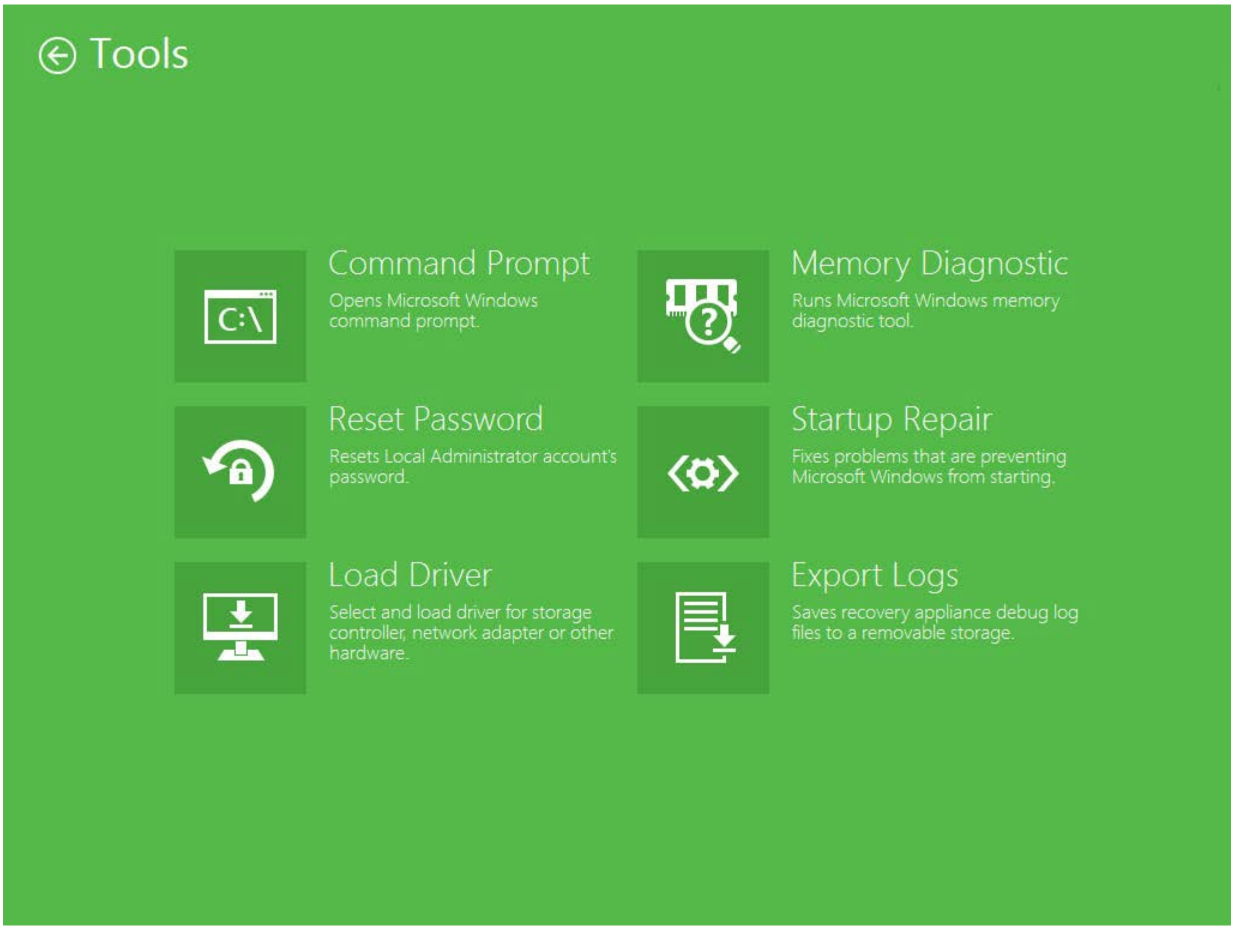
> **IMPORTANT!**
>
> Veeam Agent for Microsoft Windows includes Microsoft Windows Tools in the Veeam Recovery Media. If some of Microsoft Windows Tools components are missing on the computer, some of Microsoft Windows Tools may not be available when you boot from the Veeam Recovery Media.

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. Mind 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 http://technet.microsoft.com/en-us/magazine/2008.09.utilityspotlight.aspx.
- **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 http://windows.microsoft.com/en-us/windows/startup-repair-faq#1TC=windows-7.
- **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.



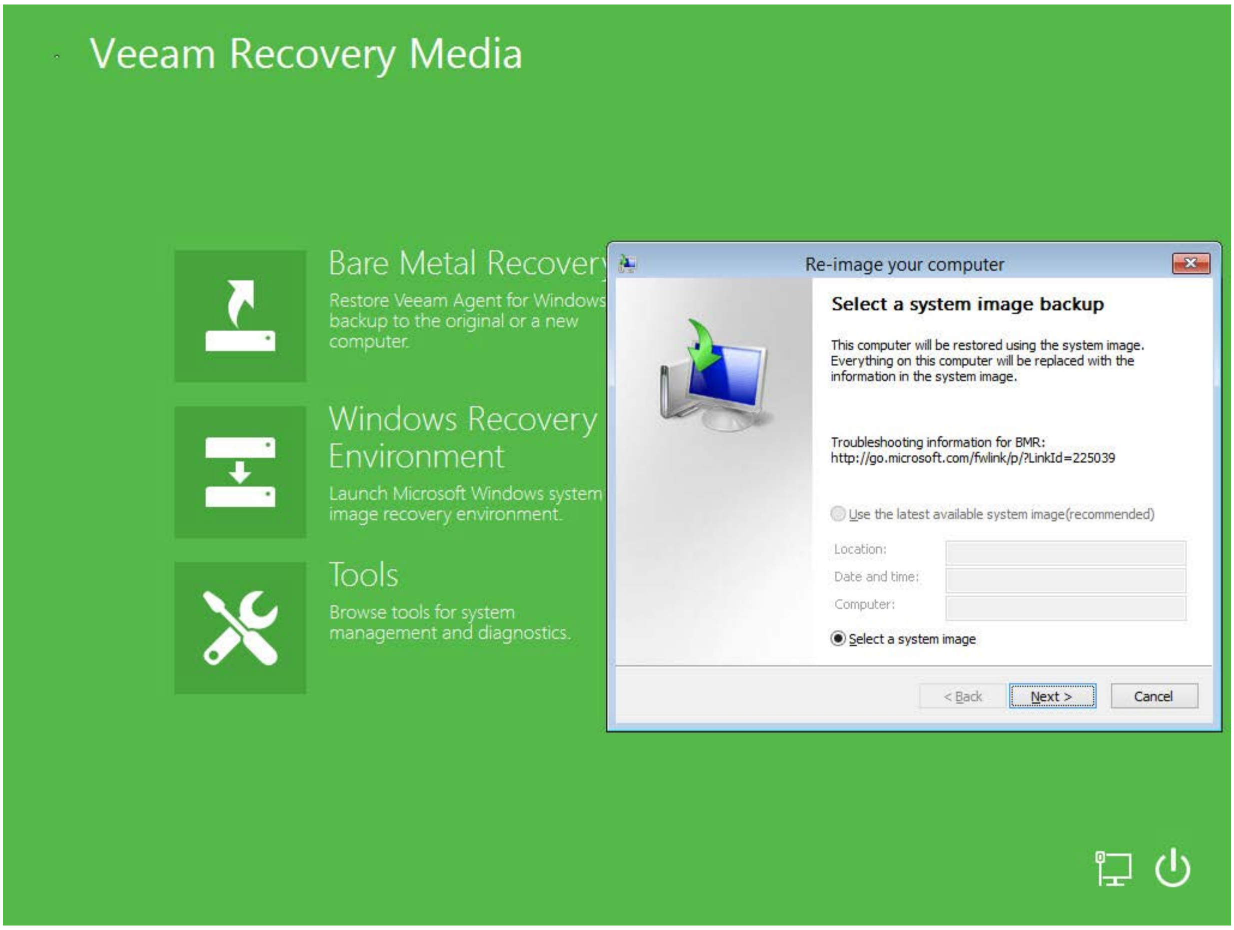
Tools
Command Prompt
Opens Microsoft Windows command prompt.
Memory Diagnostic
Runs Microsoft Windows memory diagnostic tool.
Reset Password
Resets Local Administrator account's password.
Startup Repair
Fixes problems that are preventing Microsoft Windows from starting.
Load Driver
Select and load driver 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 http://windows.microsoft.com/en-us/windows/restore-computer-from-system-image-backup.



Restore Veeam Agent for Windows backup to the original or a new computer.

Launch Microsoft Windows system image recovery environment.

Browse tools for system management and diagnostics.

Select a system image backup

This computer will be restored using the system image. Everything on this computer will be replaced with the information in the system image.

Troubleshooting information for BMR:
http://go.microsoft.com/fwlink/p/?LinkId=225039

○ Use the latest available system image(recommended)

Location:

Date and time:

Computer:

● Select a system image

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:

- 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 on 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.

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.

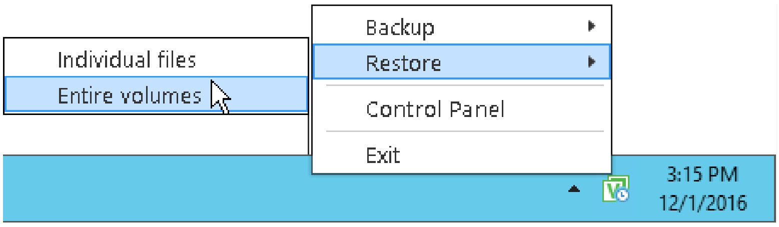
To overcome the first two limitations, you can boot from the recovery image and use the **Volume Level Restore** wizard for volume-level restore. To learn more, see Restoring from Veeam Recovery Media.

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 **Status** view, click a bar of the necessary backup job session. Click **Restore Volumes** at the bottom of the window.
- 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.

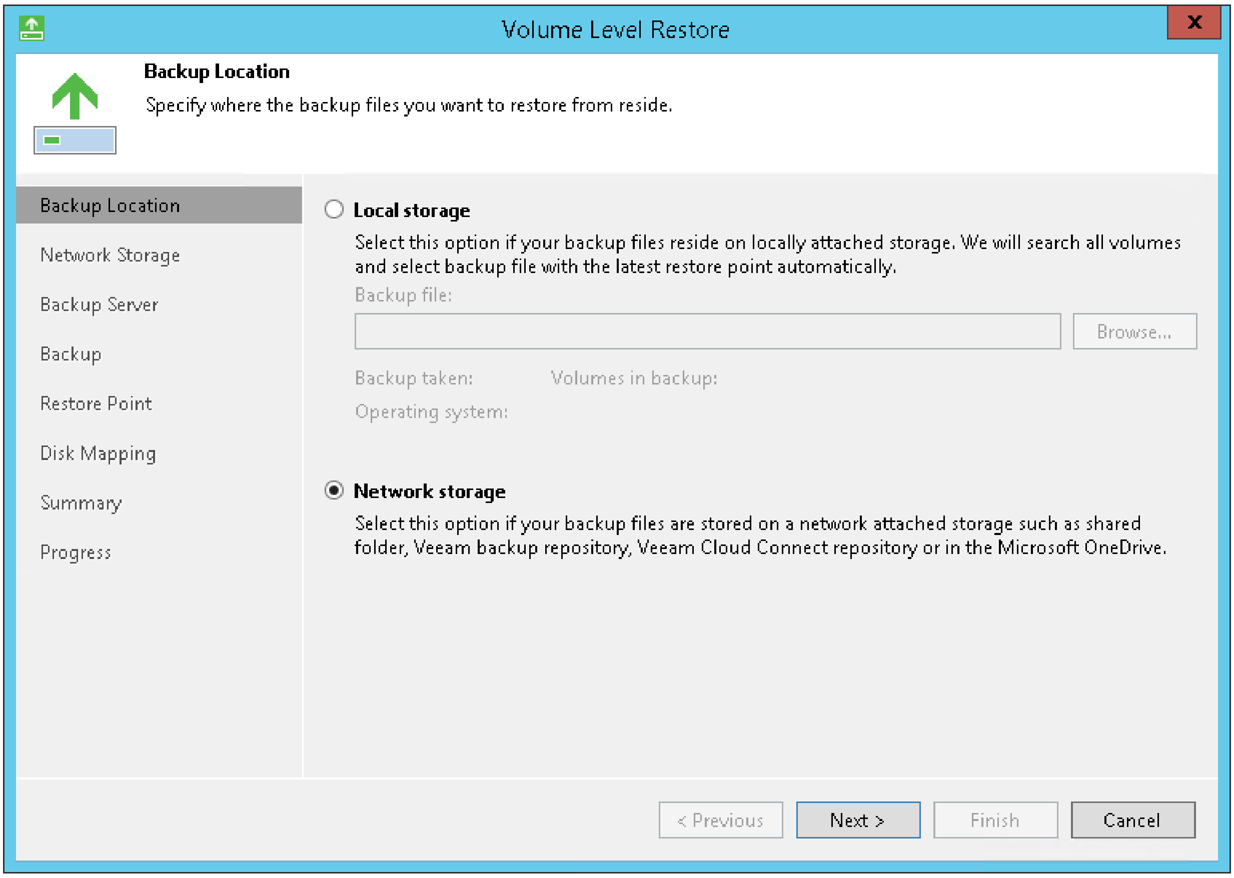


Step 2. Specify Backup File Location

At the **Backup Location** step of the wizard, specify where the backup file that you plan to use for restore resides.

By default, Veeam Agent for Microsoft Windows automatically locates the latest backup on the target location, and you pass immediately to the Restore Point step of the wizard. If Veeam Agent for Microsoft Windows fails to locate the backup for some reason or you want to use another backup for recovery, 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 a network shared folder, in a Microsoft OneDrive cloud storage, on a backup repository managed by a Veeam backup server or on 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.



Backup Location

Specify where the backup files you want to restore from reside.

○ **Local storage**

Select this option if your backup files reside on locally attached storage. We will search all volumes and select backup file with the latest restore point automatically.

Backup file:

Backup taken: Volumes in backup:

Operating system:

● **Network storage**

Select this option if your backup files are stored on a network attached storage such as shared folder, Veeam backup repository, Veeam Cloud Connect repository or in the Microsoft OneDrive.

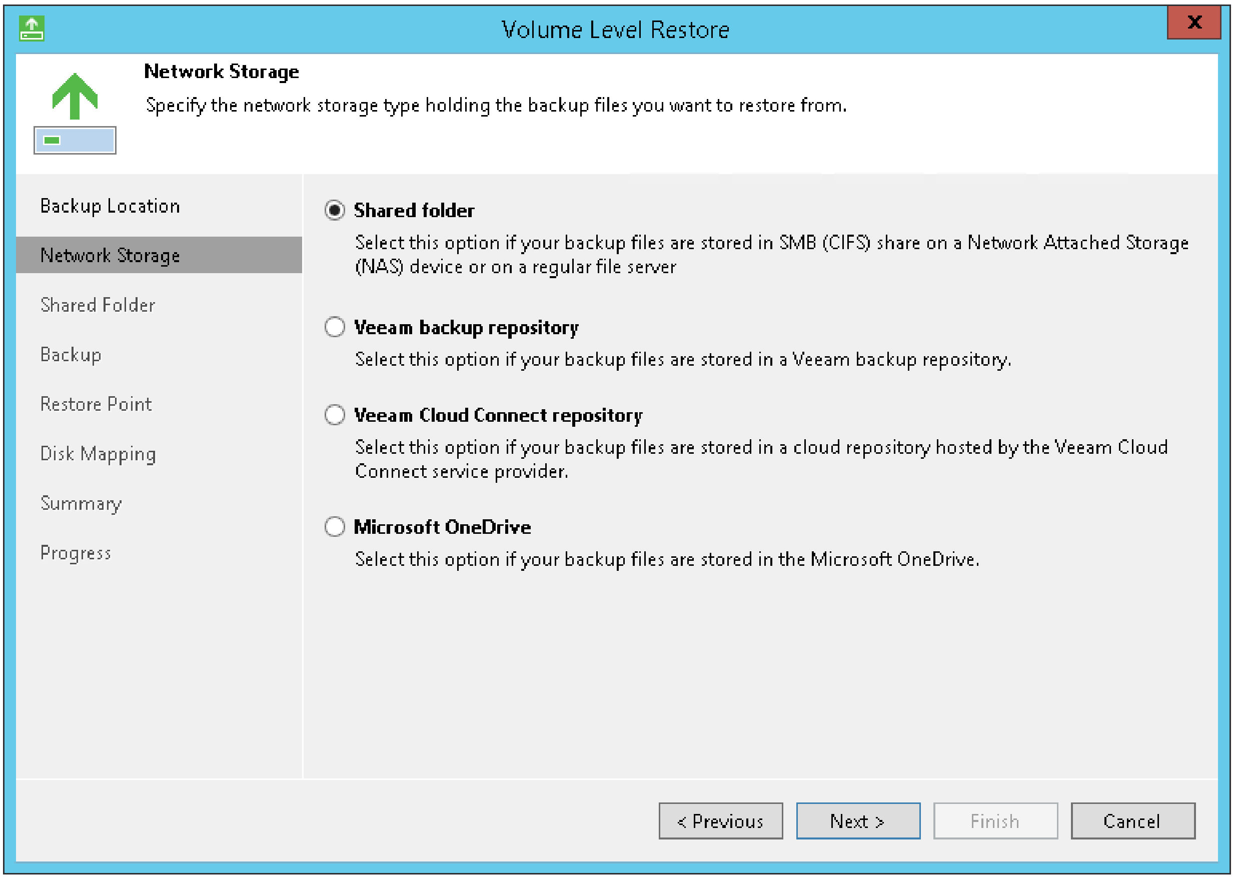
Step 3. Select Remote Storage Type

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 a network shared folder, on a backup repository or a cloud repository.

Select where the backup file is located:

- **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 on 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 on 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.
- **Microsoft OneDrive** — select this option if the backup file resides in the Microsoft OneDrive cloud storage. With this option selected, you will pass to the Microsoft OneDrive step of the wizard.

> **NOTE:**
>
> The **Microsoft OneDrive** option is not available if the Veeam Agent computer runs a Microsoft Windows Server OS.



Volume Level Restore

Network Storage

Specify the network storage type holding the backup files you want to restore from.

● **Shared folder**
Select this option if your backup files are stored in SMB (CIFS) share on a Network Attached Storage (NAS) device or on a regular file server

○ **Veeam backup repository**
Select this option if your backup files are stored in a Veeam backup repository.

○ **Veeam Cloud Connect repository**
Select this option if your backup files are stored in a cloud repository hosted by the Veeam Cloud Connect service provider.

○ **Microsoft OneDrive**
Select this option if your backup files are stored in the Microsoft OneDrive.

Step 4. Specify Remote 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.
- Microsoft OneDrive settings — if you have selected the **Microsoft OneDrive** option at the Network Storage step of the wizard.

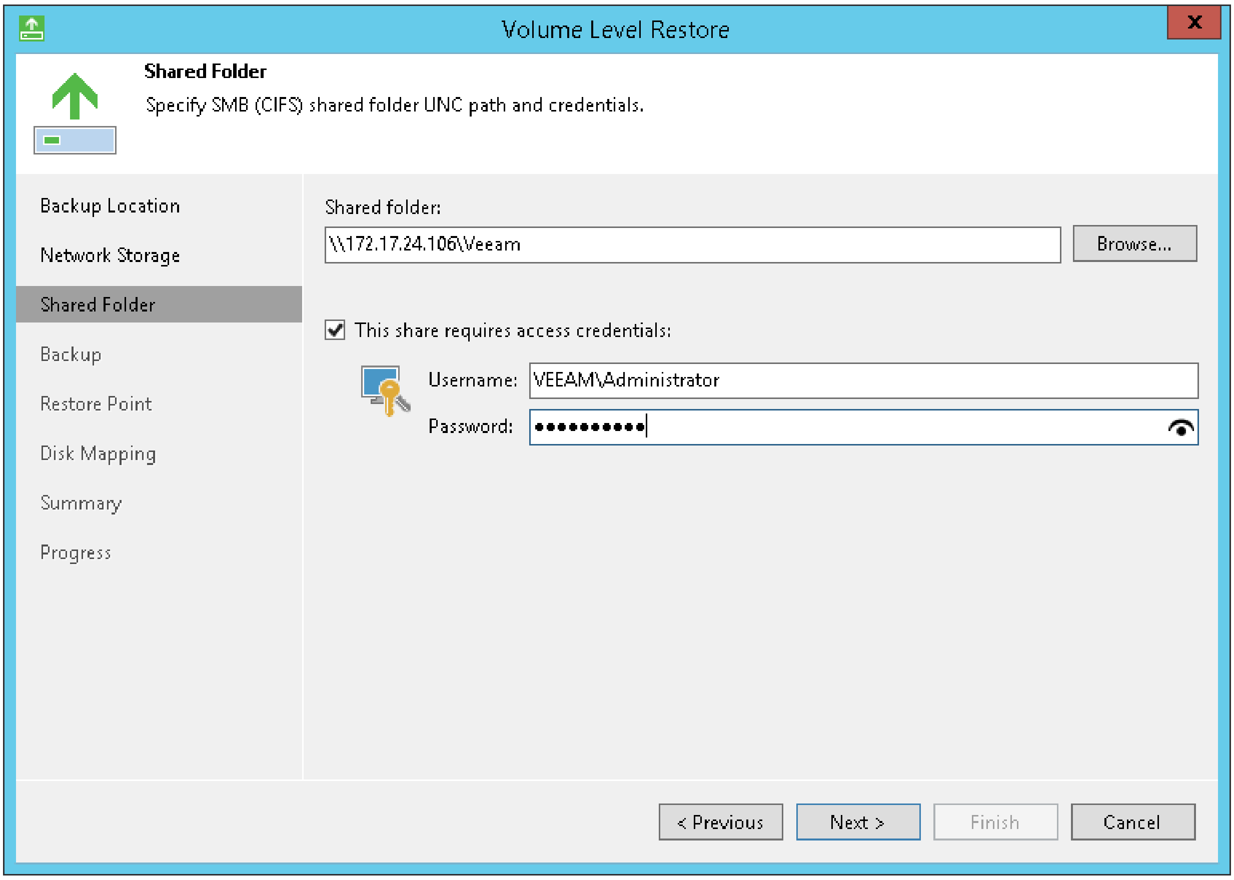
Shared Folder Settings

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 access permissions on this shared folder. The user name must be specified in the *DOMAIN\USERNAME* format.

   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.



Shared folder: \\172.17.24.106\Veeam

☑ This share requires access credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●

Backup Server Settings

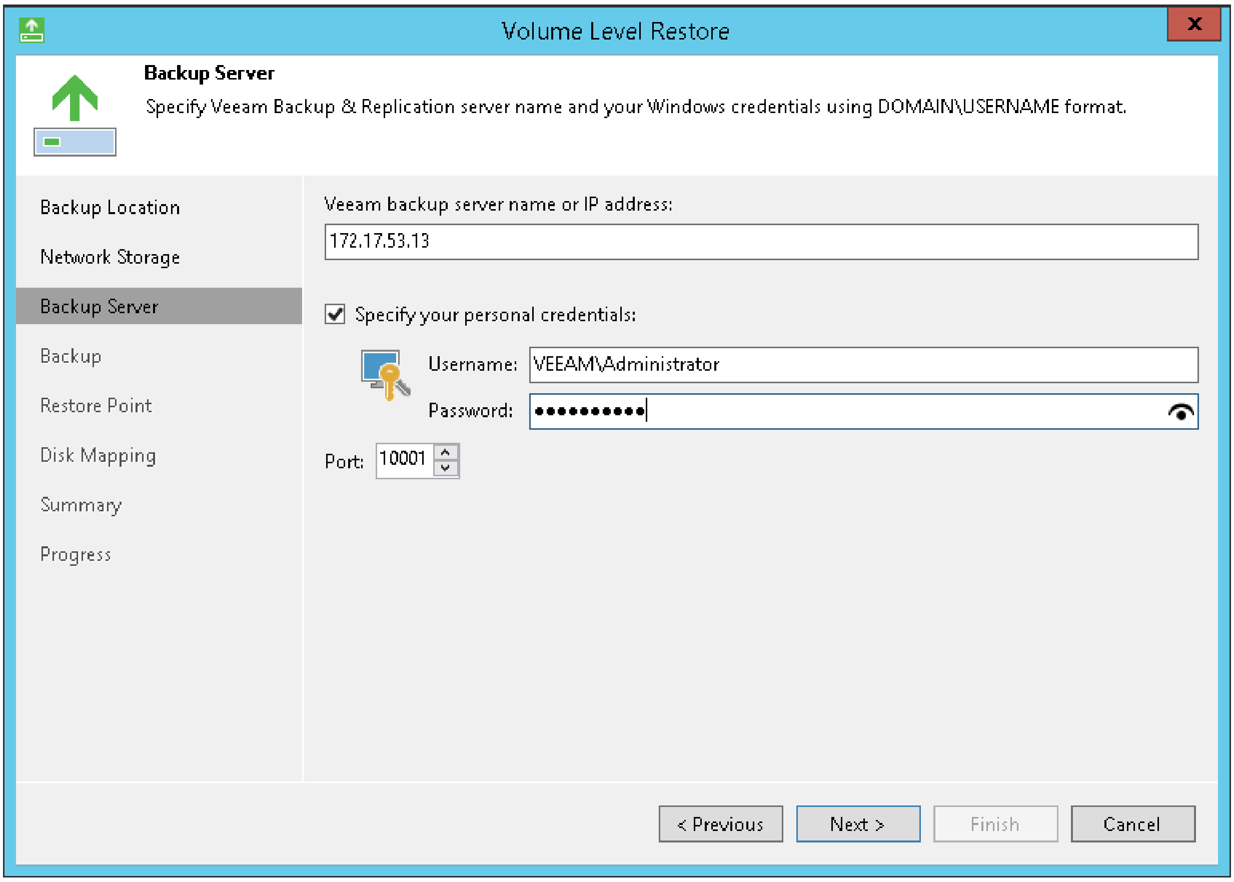
The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located on a backup repository.

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. 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 simply 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, this scenario is recommended for demo environments only.
3. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup repository. By default, Veeam Agent for Microsoft Windows uses port 10001.



Backup Server

Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.

Veeam backup server name or IP address: 172.17.53.13

☑ Specify your personal credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●

Port: 10001

IMPORTANT!

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

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:

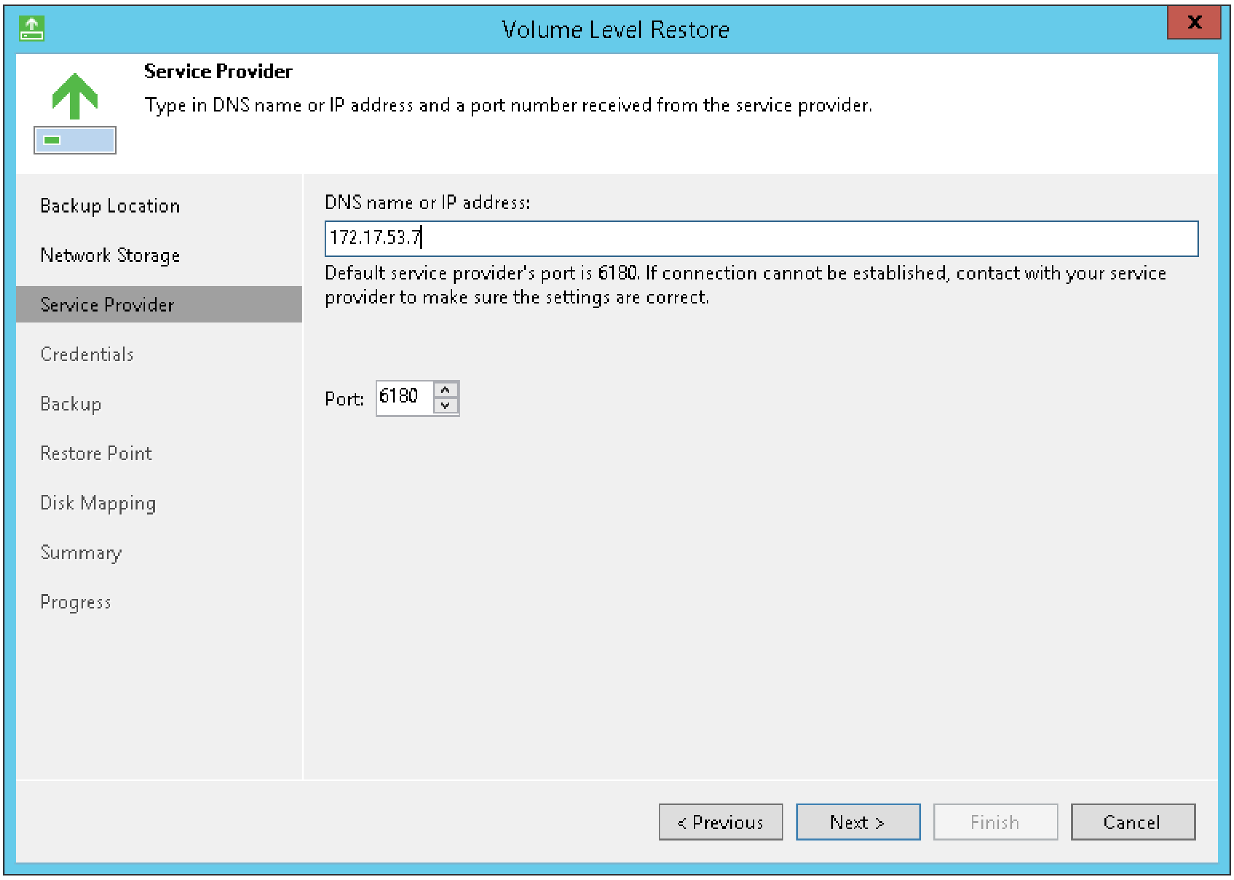
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

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.



DNS name or IP address: 172.17.53.7

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

Port: 6180

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.

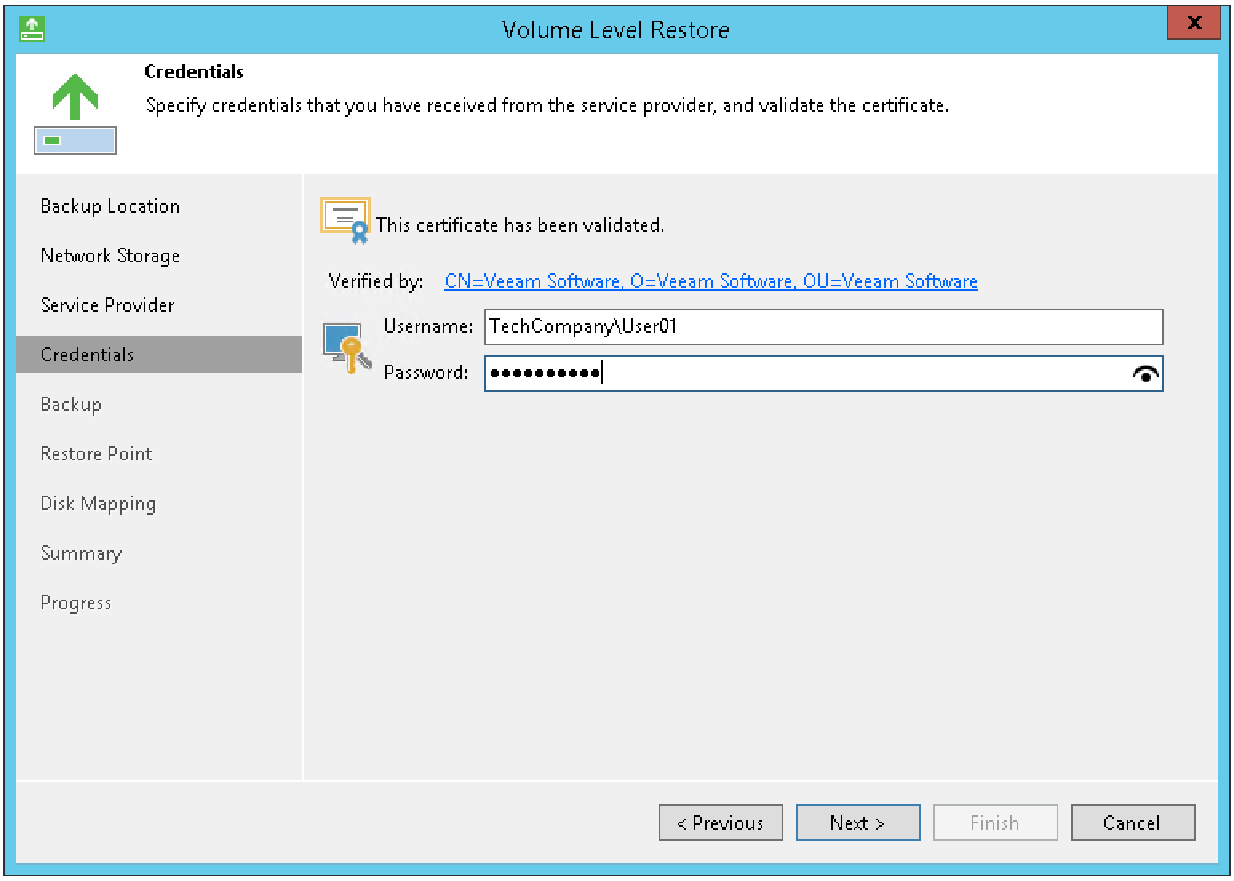
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   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.



Credentials

Specify credentials that you have received from the service provider, and validate the certificate.

This certificate has been validated.

Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software

Username: TechCompany\User01

Password: ●●●●●●●●●●

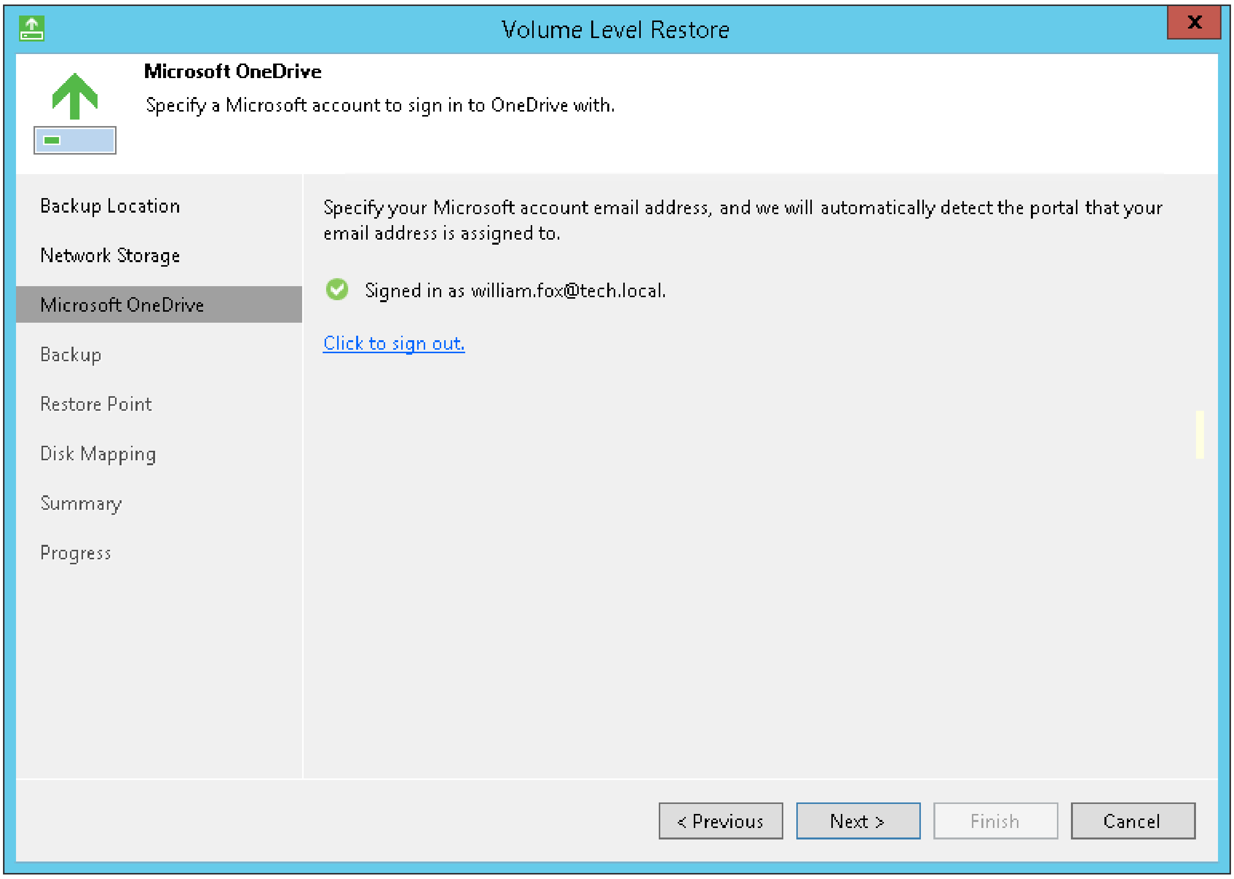
Microsoft OneDrive Settings

The **Microsoft OneDrive** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft OneDrive cloud storage.

Specify settings to connect to Microsoft OneDrive:

1. Click **Click to sign in to Microsoft OneDrive**.
2. In the **Microsoft OneDrive** window, follow instructions to specify credentials of the Microsoft OneDrive account that has access to the storage where the backup file resides and click **Sign in**.

If you want to change settings to connect to Microsoft OneDrive, click the **Click to sign out** link and repeat steps 1-2 to specify another account.



Volume Level Restore

Microsoft OneDrive

Specify a Microsoft account to sign in to OneDrive with.

Specify your Microsoft account email address, and we will automatically detect the portal that your email address is assigned to.

✓ Signed in as william.fox@tech.local.

Click to sign out.

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 a network shared folder or on a backup repository.

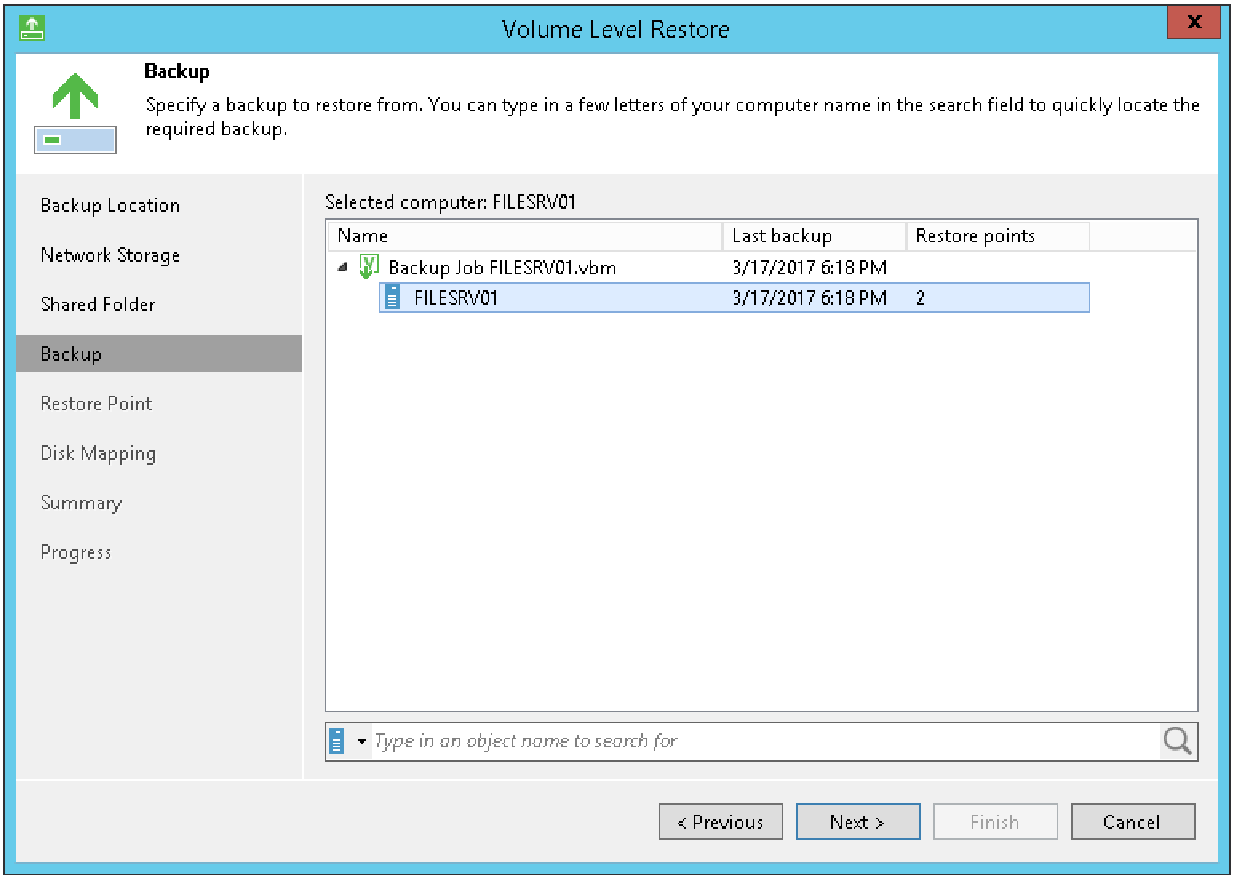
From the list of backups, select a backup from which you want to recover data. To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

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 on 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.

Selected computer: FILESRV01

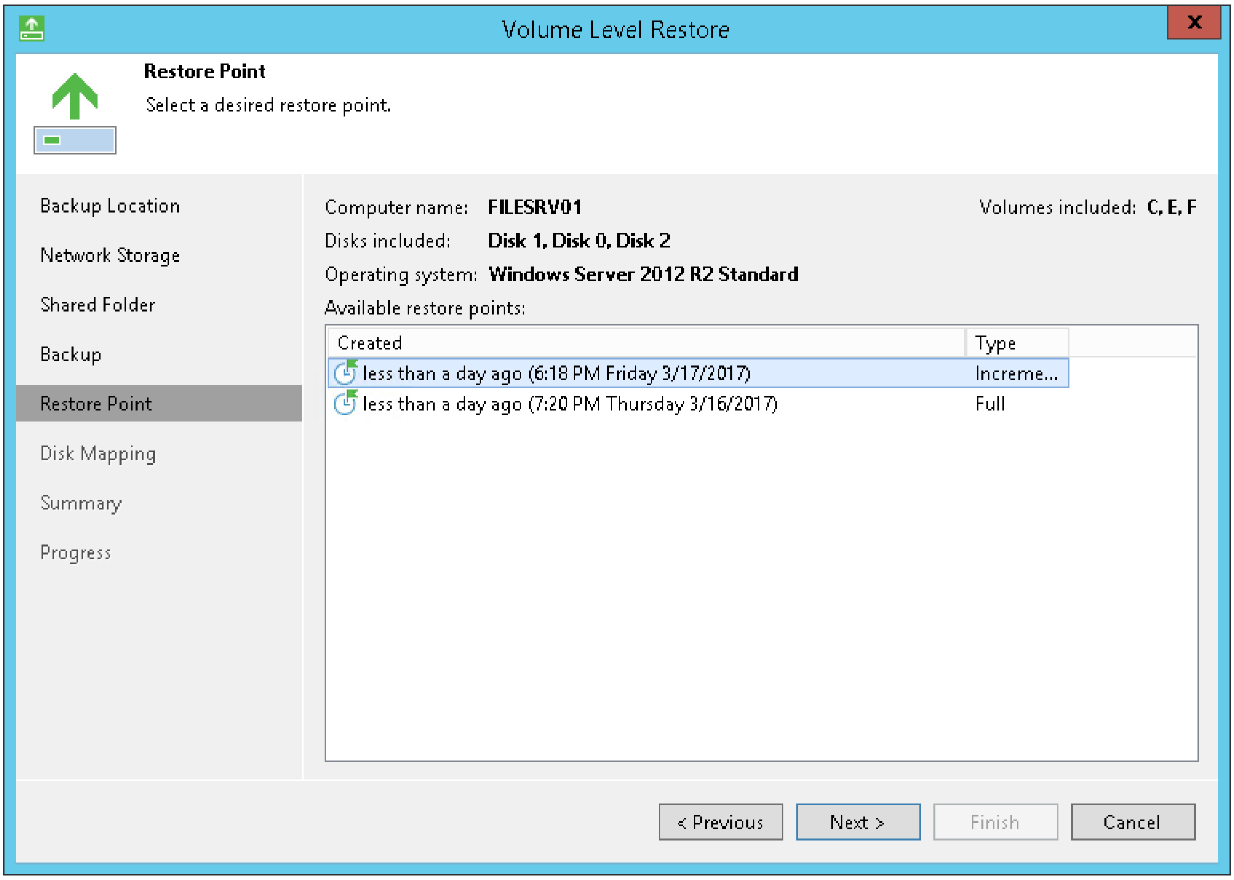
Name	Last backup	Restore points
Backup Job FILESRV01.vbm	3/17/2017 6:18 PM	
FILESRV01	3/17/2017 6:18 PM	2

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.



Restore Point

Select a desired restore point.

Computer name: **FILESRV01**

Volumes included: **C, E, F**

Disks included: **Disk 1, Disk 0, Disk 2**

Operating system: **Windows Server 2012 R2 Standard**

Available restore points:

Created	Type
less than a day ago (6:18 PM Friday 3/17/2017)	Increme...
less than a day ago (7:20 PM Thursday 3/16/2017)	Full

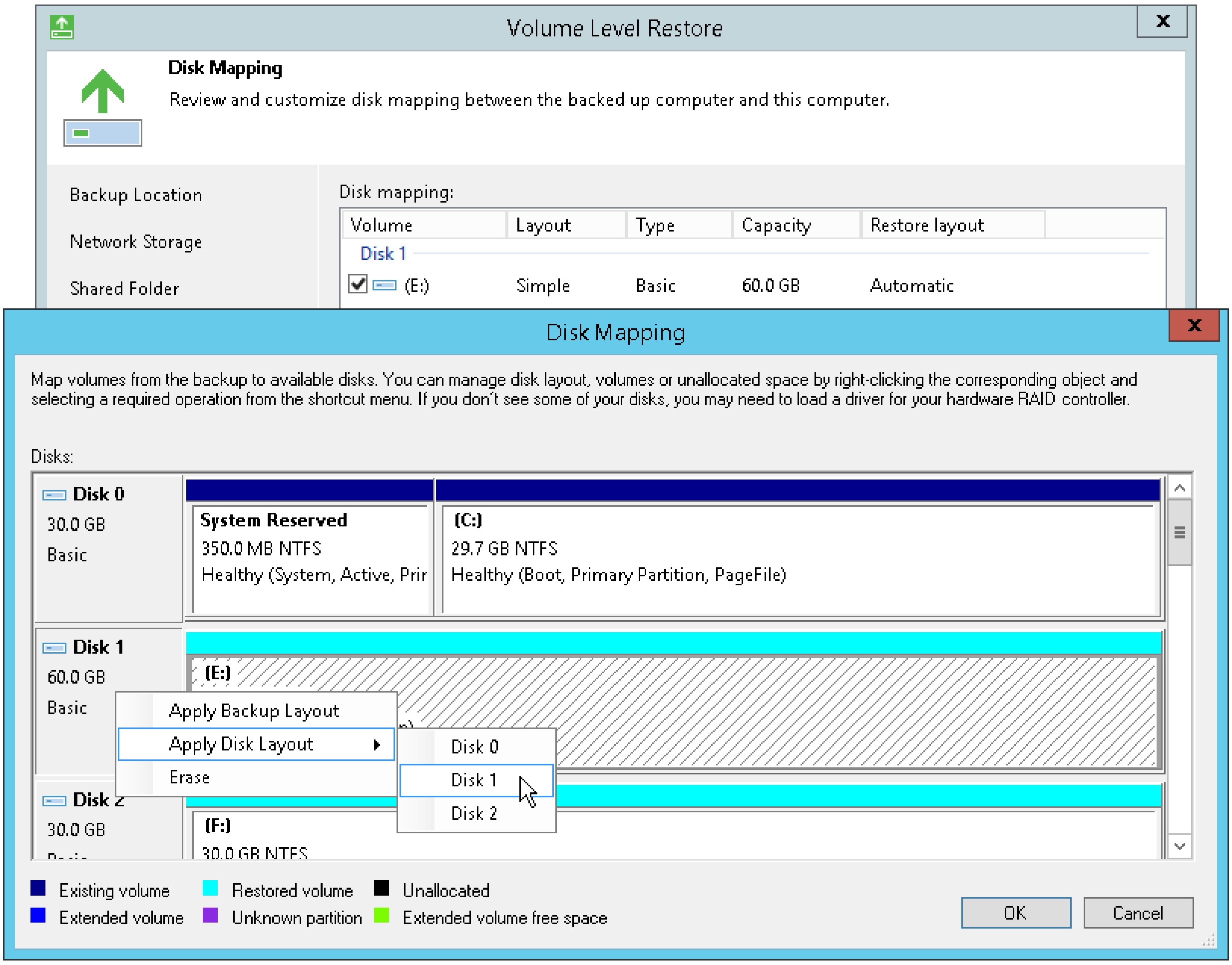
Step 7. Map Restored Disks

At the **Disk Mapping** step of the wizard, select what volume(s) you want to restore and map volumes from the backup to volumes on your 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 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.



Volume Level Restore

Disk Mapping

Review and customize disk mapping between the backed up computer and this computer.

Disk mapping:

Volume	Layout	Type	Capacity	Restore layout
Disk 1				
☑ (E:)	Simple	Basic	60.0 GB	Automatic

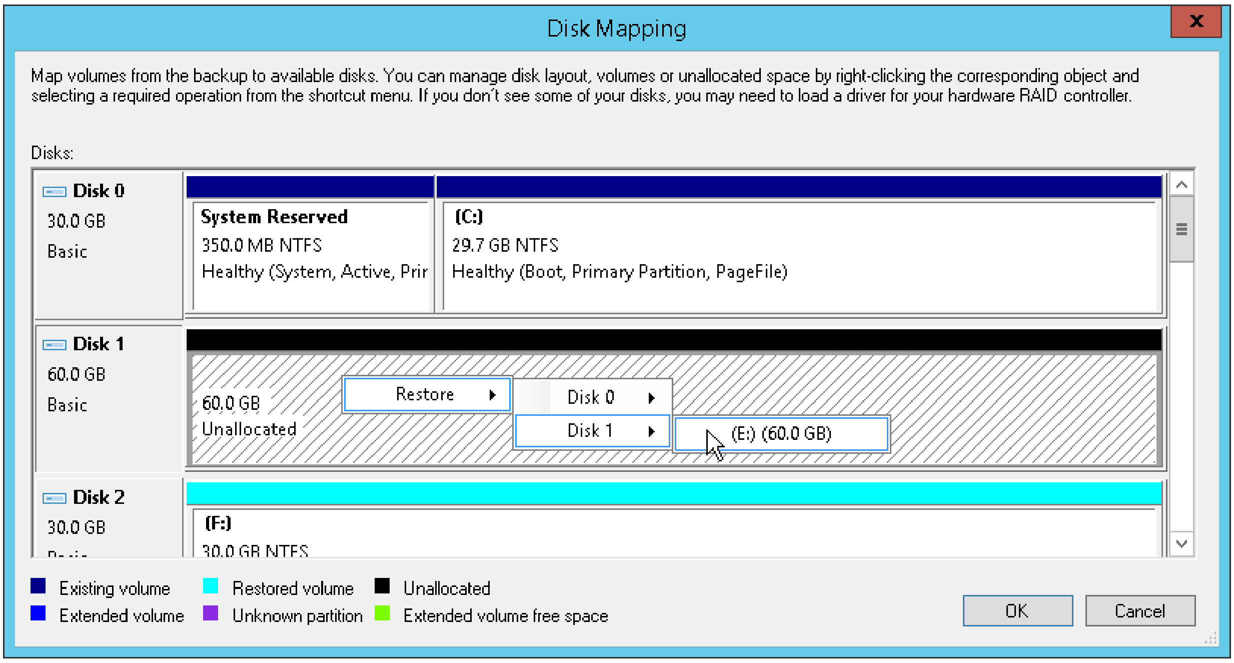
Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

- 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 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.



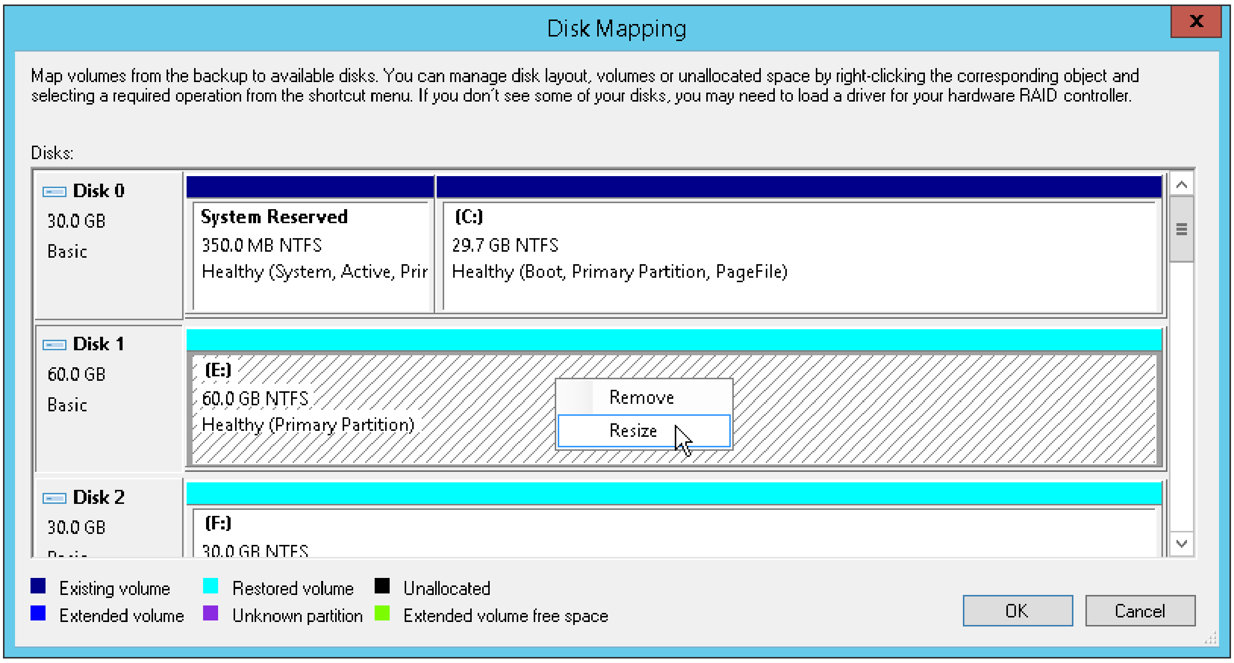
Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

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.



Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

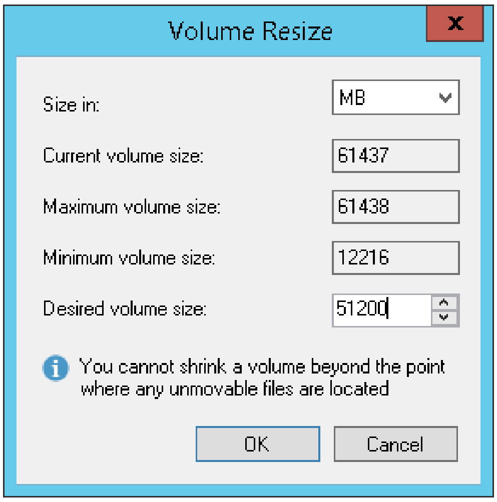
Step 8. Resize Restored Volumes

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.



Volume Resize

Size in: MB

Current volume size: 61437

Maximum volume size: 61438

Minimum volume size: 12216

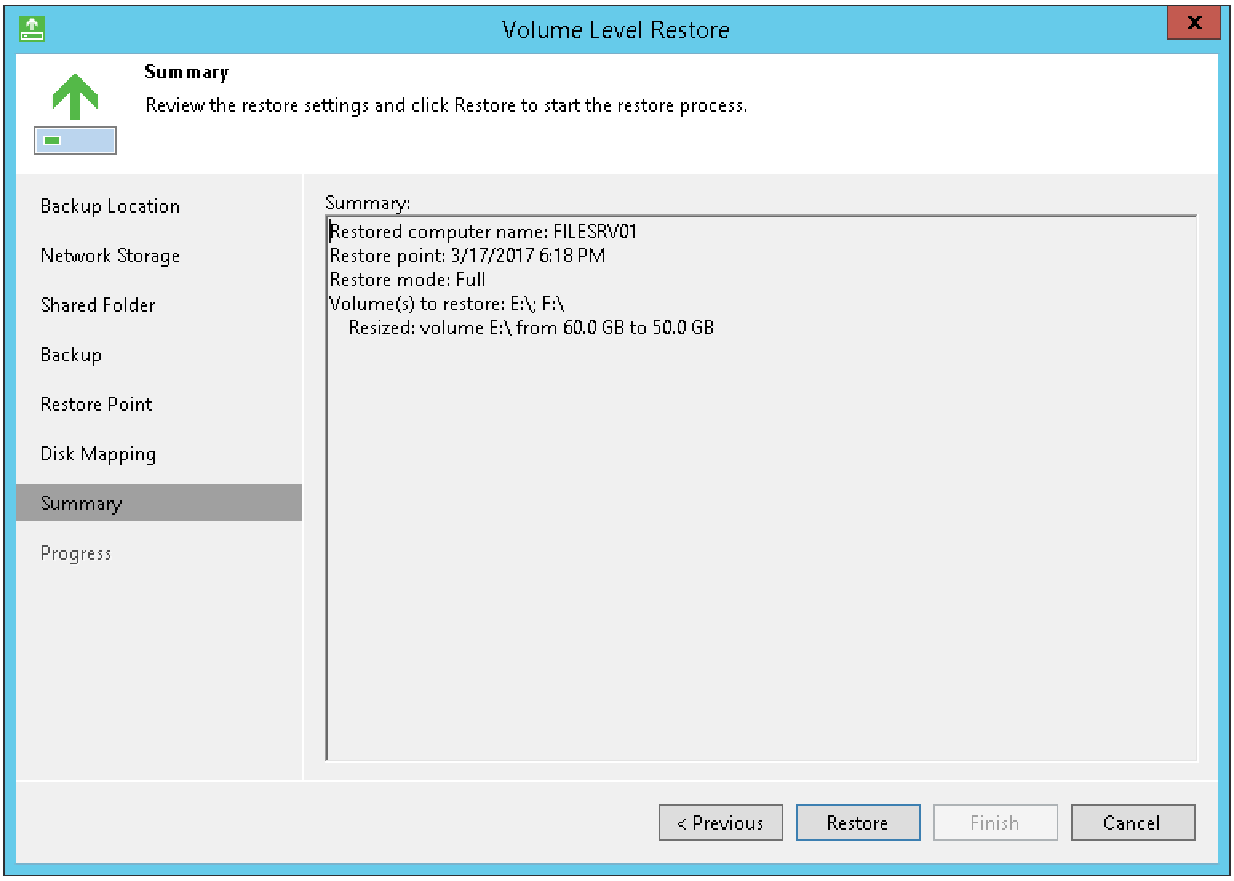
Desired volume size: 51200

You cannot shrink a volume beyond the point where any unmovable files are located

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.



Summary:

```
Restored computer name: FILESRV01
Restore point: 3/17/2017 6:18 PM
Restore mode: Full
Volume(s) to restore: E:\; F:\
   Resized: volume E:\ from 60.0 GB to 50.0 GB
```

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 simply target applications to restored files and work with them as usual.

Before You Begin

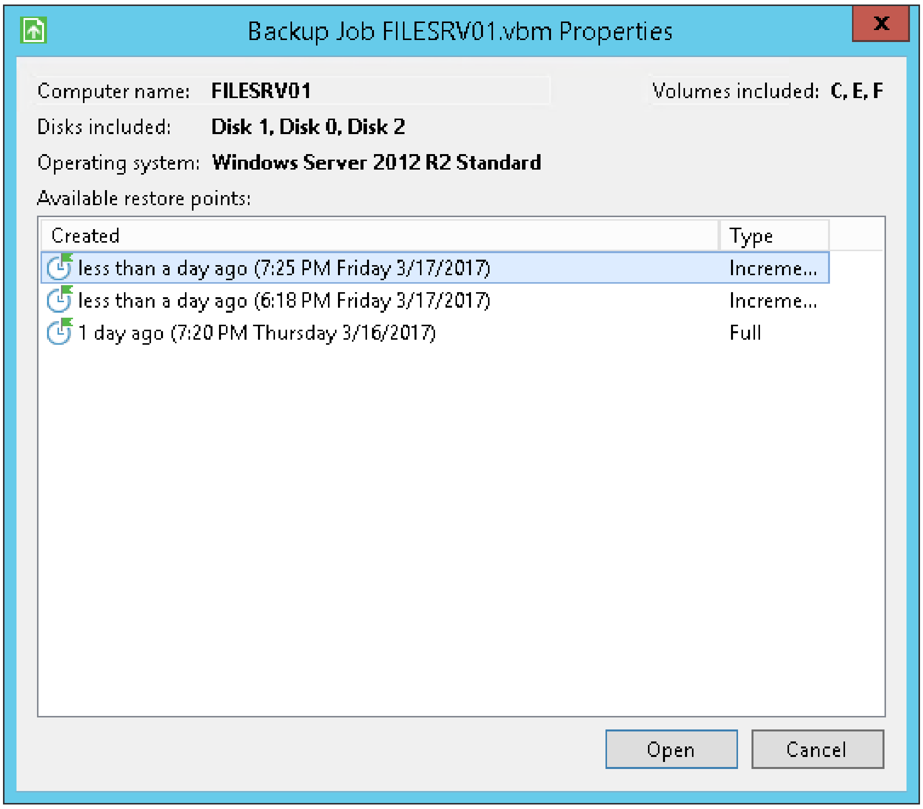
Before you begin the file-level restore process, check the following prerequisites:

- 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 on 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.

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**.
- From the main menu, select **All Programs** > **Veeam** > **File Level Restore**.
- Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**. In the **Status** view, 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.
- 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 **Restore**. Veeam Agent for Microsoft Windows will automatically publish the backup content into the computer file system and open the Veeam Backup browser.



Backup Job FILESRV01.vbm Properties

Computer name: **FILESRV01**   Volumes included: **C, E, F**

Disks included: **Disk 1, Disk 0, Disk 2**

Operating system: **Windows Server 2012 R2 Standard**

Available restore points:

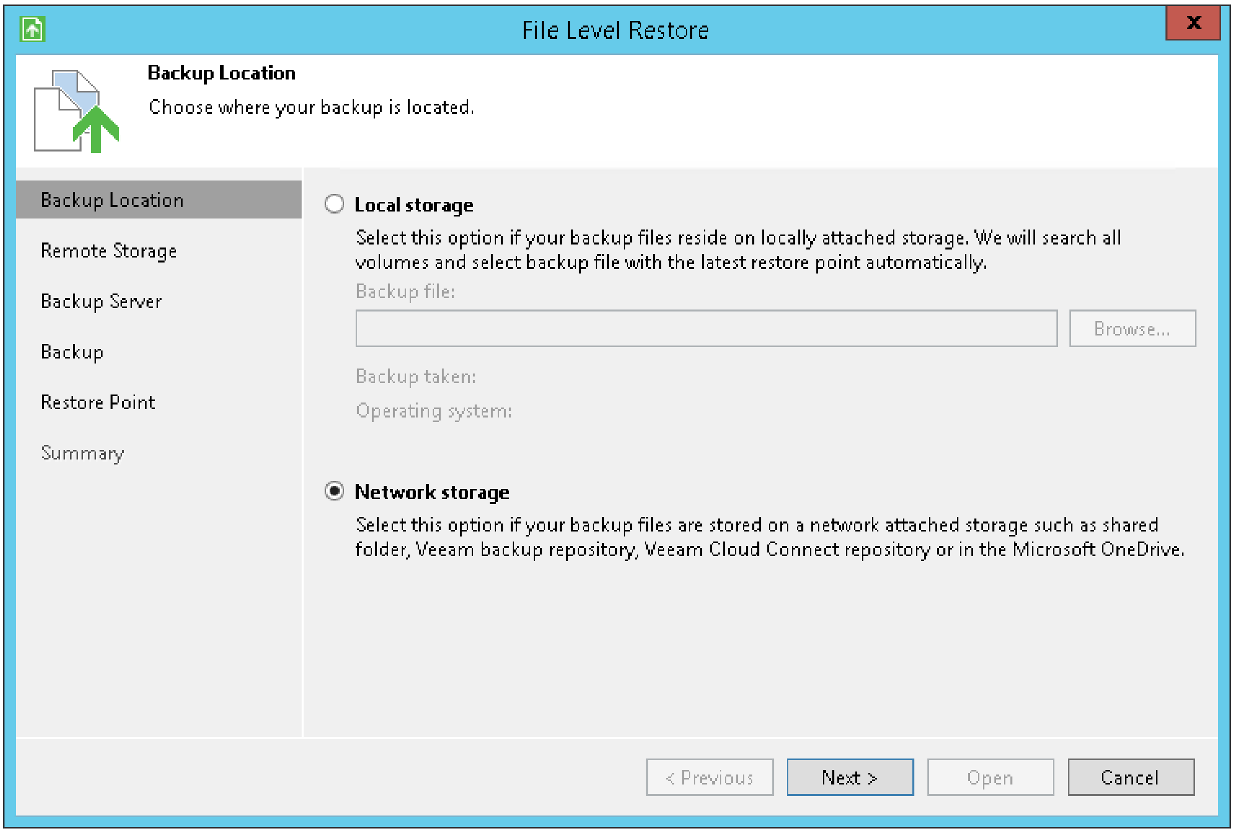
Created	Type
less than a day ago (7:25 PM Friday 3/17/2017)	Increme...
less than a day ago (6:18 PM Friday 3/17/2017)	Increme...
1 day ago (7:20 PM Thursday 3/16/2017)	Full

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.

By default, Veeam Agent for Microsoft Windows automatically locates the latest backup on the computer drive or in a network shared folder, and you pass immediately to the Restore Point step of the wizard. If Veeam Agent for Microsoft Windows fails to locate the backup for some reason or you want to use another backup for recovery, 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 a network shared folder, in a Microsoft OneDrive cloud storage, on a backup repository managed by a Veeam backup server or on 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.



File Level Restore

Backup Location

Choose where your backup is located.

○ **Local storage**

Select this option if your backup files reside on locally attached storage. We will search all volumes and select backup file with the latest restore point automatically.

Backup file:

Backup taken:

Operating system:

● **Network storage**

Select this option if your backup files are stored on a network attached storage such as shared folder, Veeam backup repository, Veeam Cloud Connect repository or in the Microsoft OneDrive.

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 a network shared folder, on a backup repository or a cloud repository.

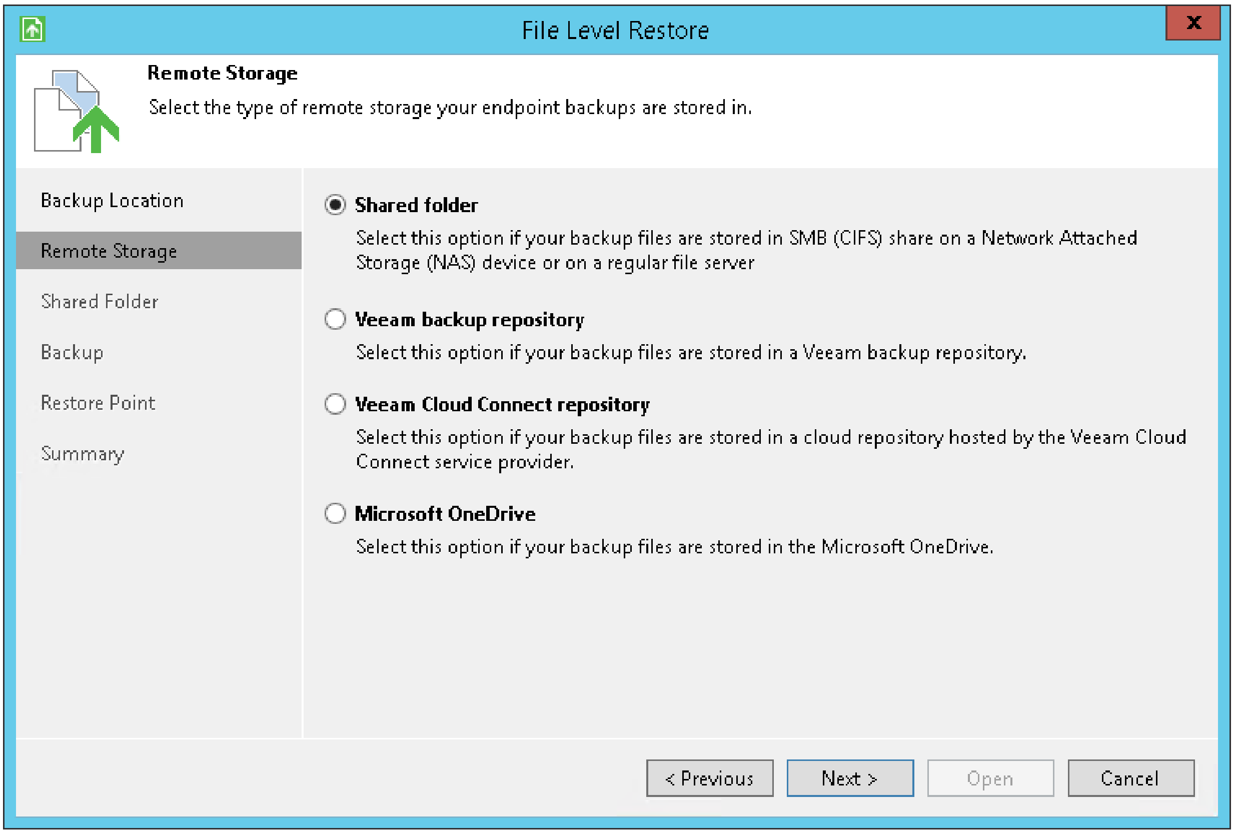
Specify where the backup file resides:

- **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 on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the Backup Server step of the wizard.
- **Veeam Cloud Connect repository** — select this option if the backup file resides on 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.
- **Microsoft OneDrive** — select this option if the backup file resides in the Microsoft OneDrive cloud storage. With this option selected, you will pass to the Microsoft OneDrive step of the wizard.

NOTE:

The **Microsoft OneDrive** option is not available if the Veeam Agent computer runs a Microsoft Windows Server OS.

Specify settings to connect to Microsoft OneDrive:



Remote Storage

Select the type of remote storage your endpoint backups are stored in.

● **Shared folder**

Select this option if your backup files are stored in SMB (CIFS) share on a Network Attached Storage (NAS) device or on a regular file server

○ **Veeam backup repository**

Select this option if your backup files are stored in a Veeam backup repository.

○ **Veeam Cloud Connect repository**

Select this option if your backup files are stored in a cloud repository hosted by the Veeam Cloud Connect service provider.

○ **Microsoft OneDrive**

Select this option if your backup files are stored in the Microsoft OneDrive.

Step 4. Specify Remote 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.
- Microsoft OneDrive settings — if you have selected the **Microsoft OneDrive** option at the Network Storage step of the wizard.

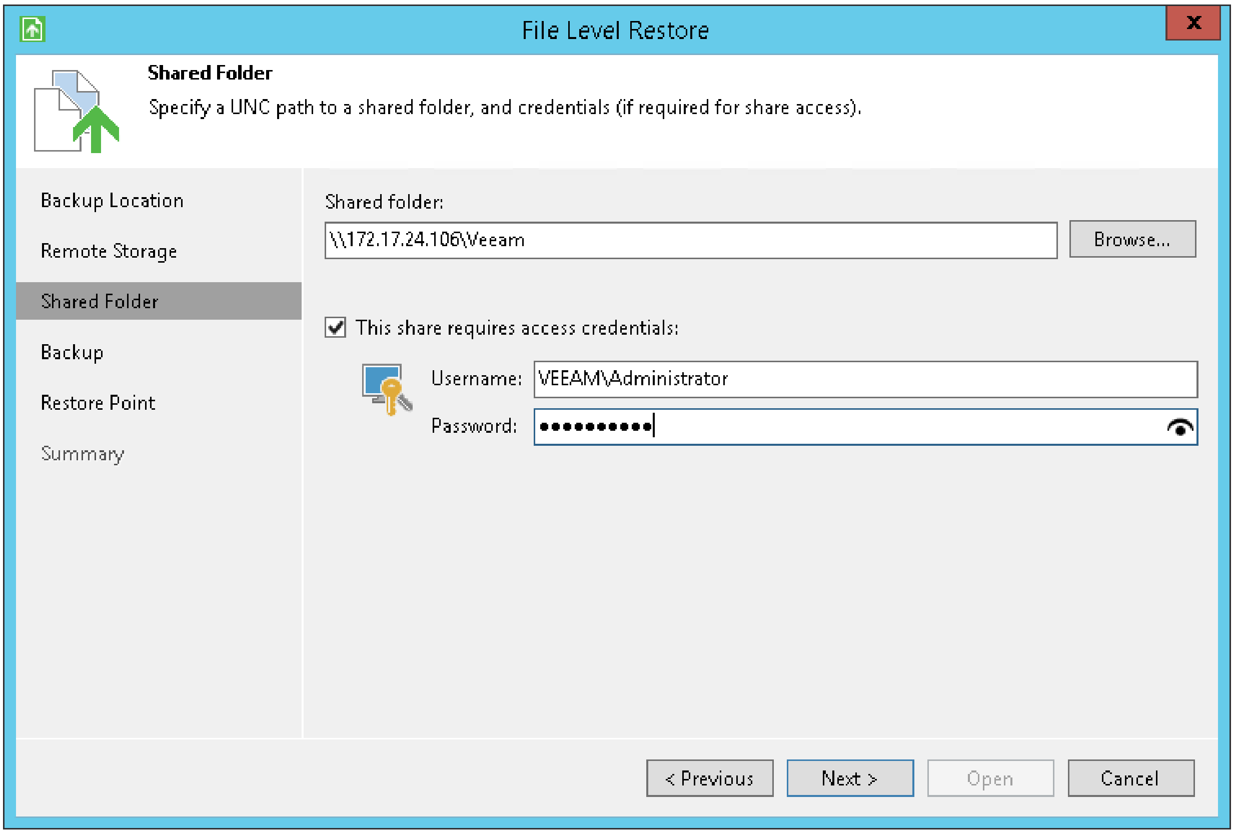
Shared Folder Settings

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 access permissions on this shared folder. The user name must be specified in the *DOMAIN\USERNAME* format.

   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.



Shared Folder

Specify a UNC path to a shared folder, and credentials (if required for share access).

Shared folder: \\172.17.24.106\Veeam

☑ This share requires access credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●●

Backup Server Settings

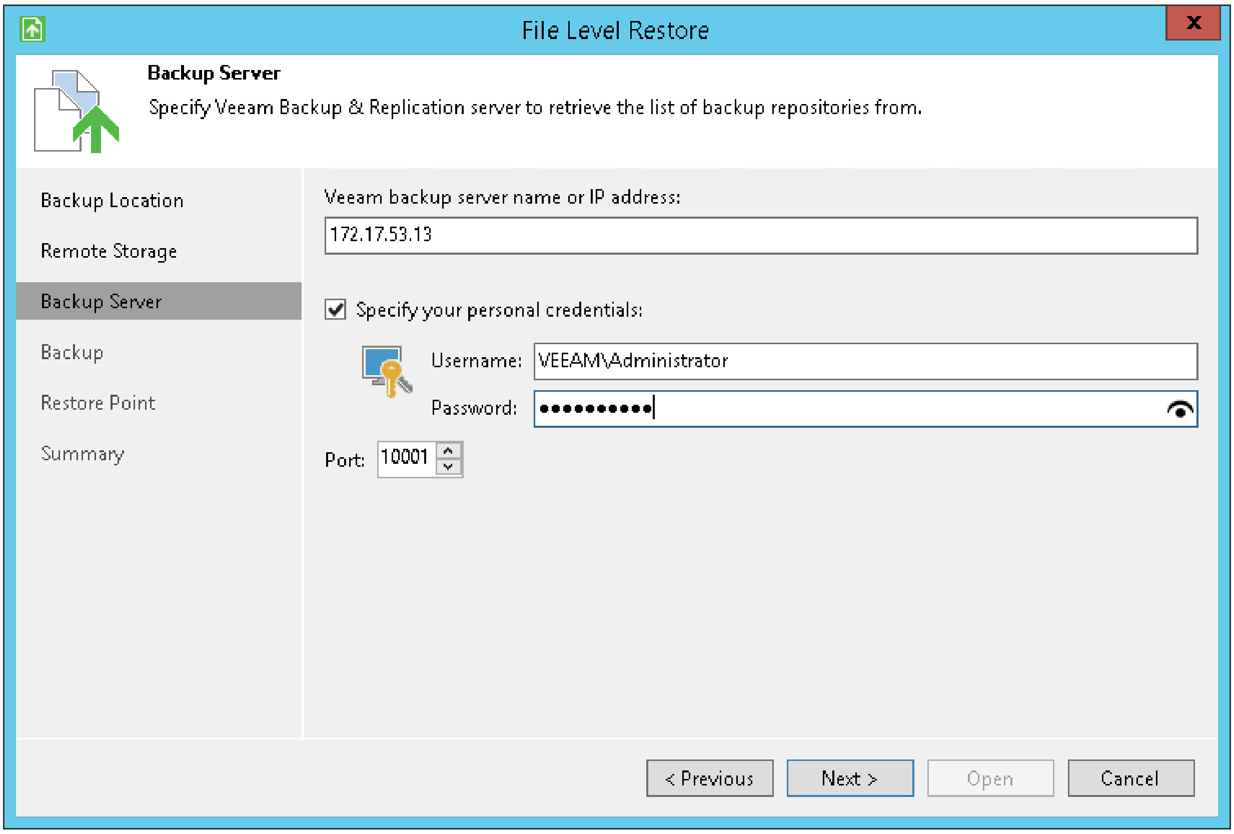
The **Backup Server** step of the wizard is available if you have chosen to restore data from a backup file located on a backup repository.

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. 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 simply 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, this scenario is recommended for demo environments only.
3. In the **Port** field, specify a number of the port over which Veeam Agent for Microsoft Windows must communicate with the backup repository. By default, Veeam Agent for Microsoft Windows uses port 10001.



File Level Restore

Backup Server

Specify Veeam Backup & Replication server to retrieve the list of backup repositories from.

Veeam backup server name or IP address: 172.17.53.13

☑ Specify your personal credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●●

Port: 10001

IMPORTANT!

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

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:

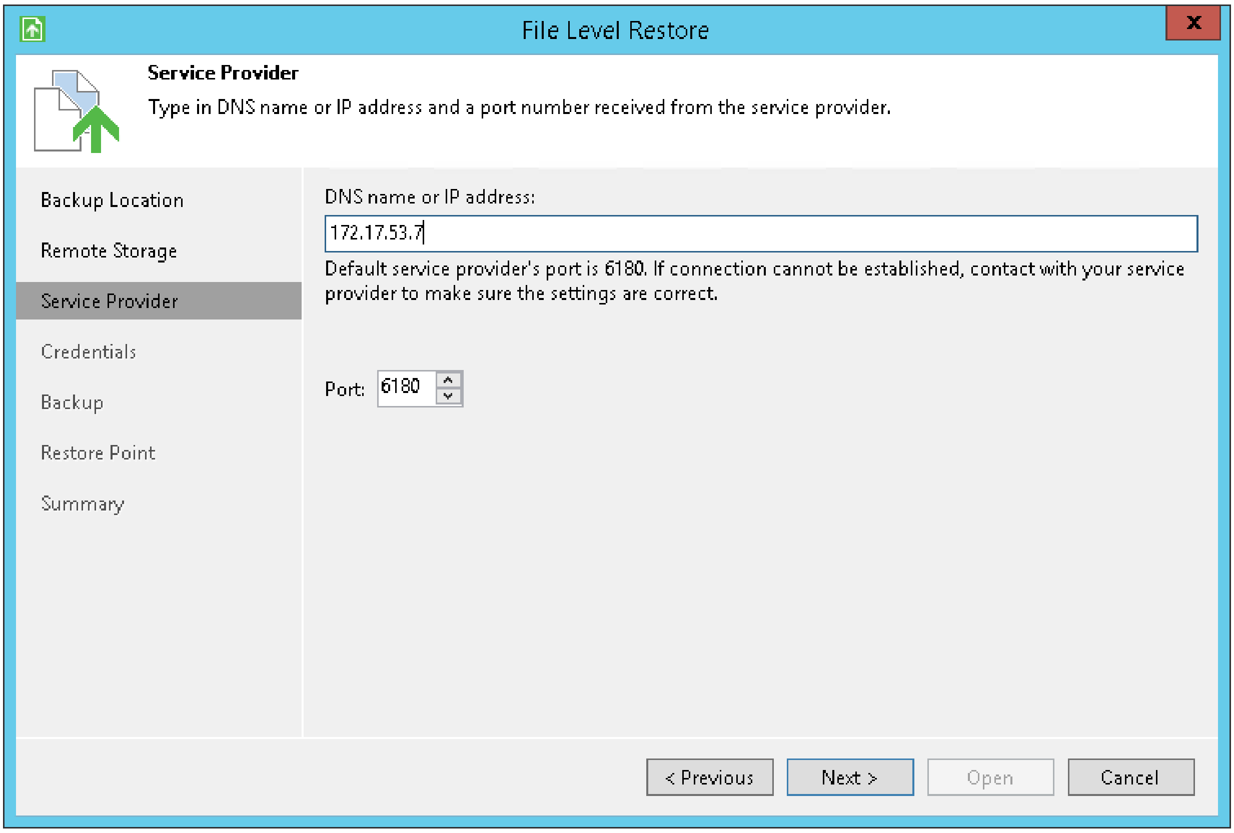
1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.

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.



Service Provider

Type in DNS name or IP address and a port number received from the service provider.

DNS name or IP address: 172.17.53.7

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

Port: 6180

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.

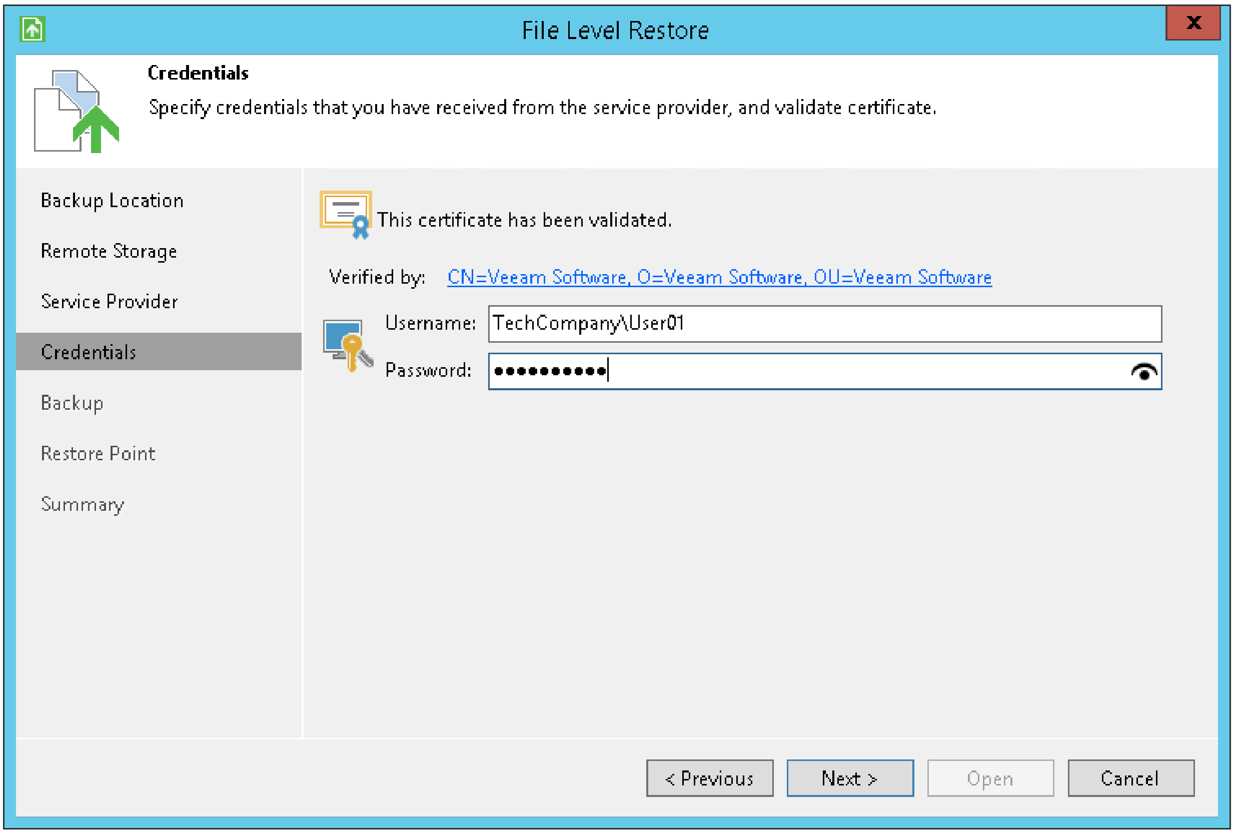
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   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.



Credentials

Specify credentials that you have received from the service provider, and validate certificate.

This certificate has been validated.

Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software

Username: TechCompany\User01

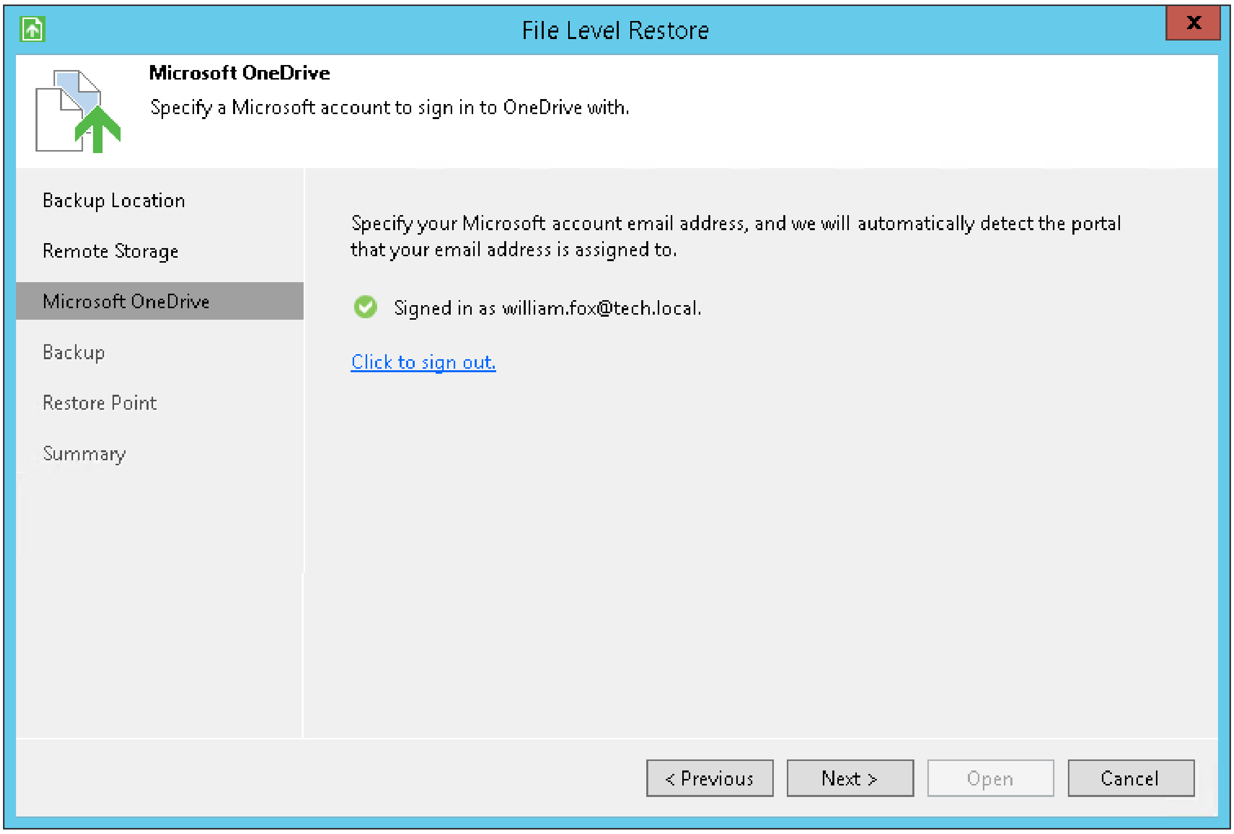
Password: ●●●●●●●●●●

Microsoft OneDrive Settings

The **Microsoft OneDrive** step of the wizard is available if you have chosen to restore data from a backup file located in the Microsoft OneDrive cloud storage.

1. Click **Click to sign in to Microsoft OneDrive**.
2. In the **Microsoft OneDrive** window, follow instructions to specify credentials of the Microsoft OneDrive account that has access to the storage where the backup file resides and click **Sign in**.

If you want to change settings to connect to Microsoft OneDrive, click the **Click to sign out** link and repeat steps 1-2 to specify another account.



Microsoft OneDrive

Specify a Microsoft account to sign in to OneDrive with.

Specify your Microsoft account email address, and we will automatically detect the portal that your email address is assigned to.

✓ Signed in as william.fox@tech.local.

Click to sign out.

Step 5. Select Backup

The **Backup** step of the wizard is available if you have chosen to restore data from a backup file that resides in a remote location — in a network shared folder, on a backup repository or on 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 on 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:

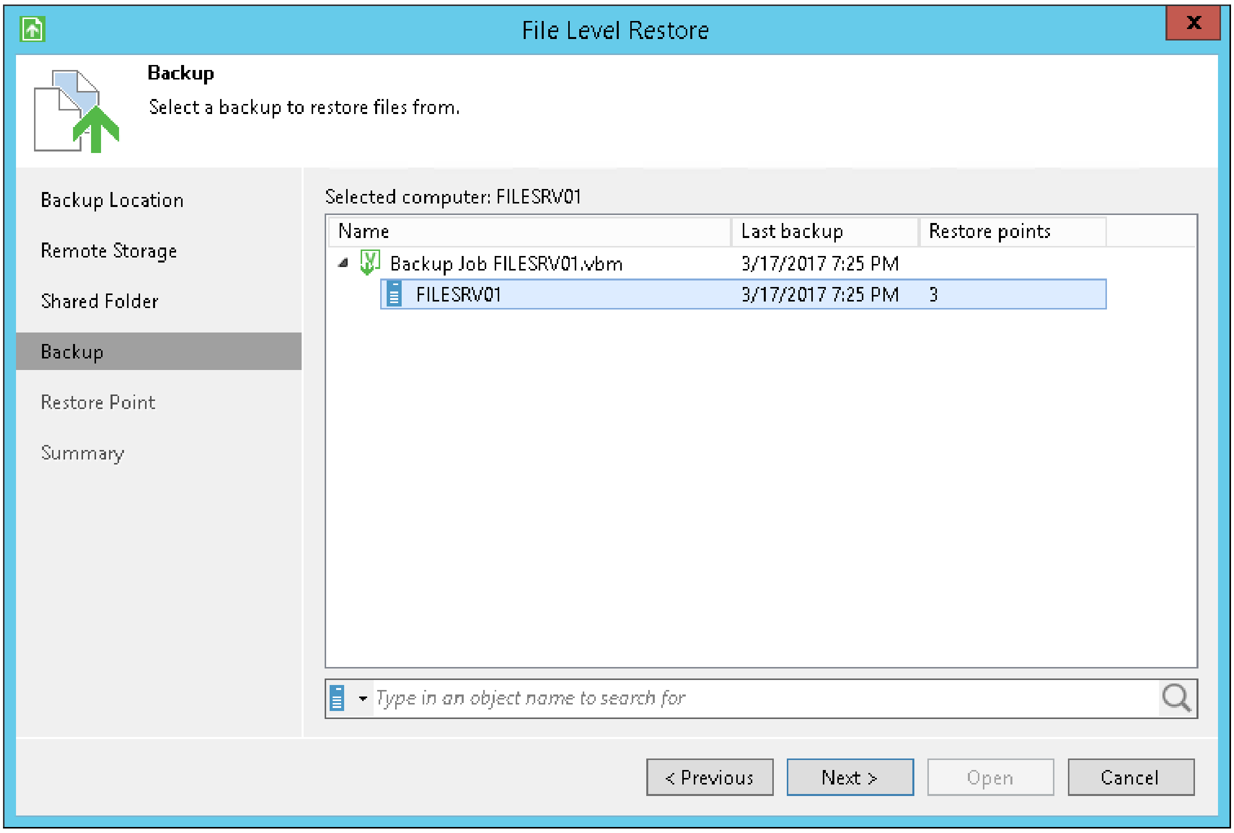
- If you specify credentials for the user who has access to the backup repository, the list of backups will include only backups created by this user.
- If you specify credentials for the user who is assigned the *Backup Administrator* or *Restore Operator* role on the backup server, the list of backups will include all Veeam Agent backups stored on the backup repository.

If you restore data from a backup stored on 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.



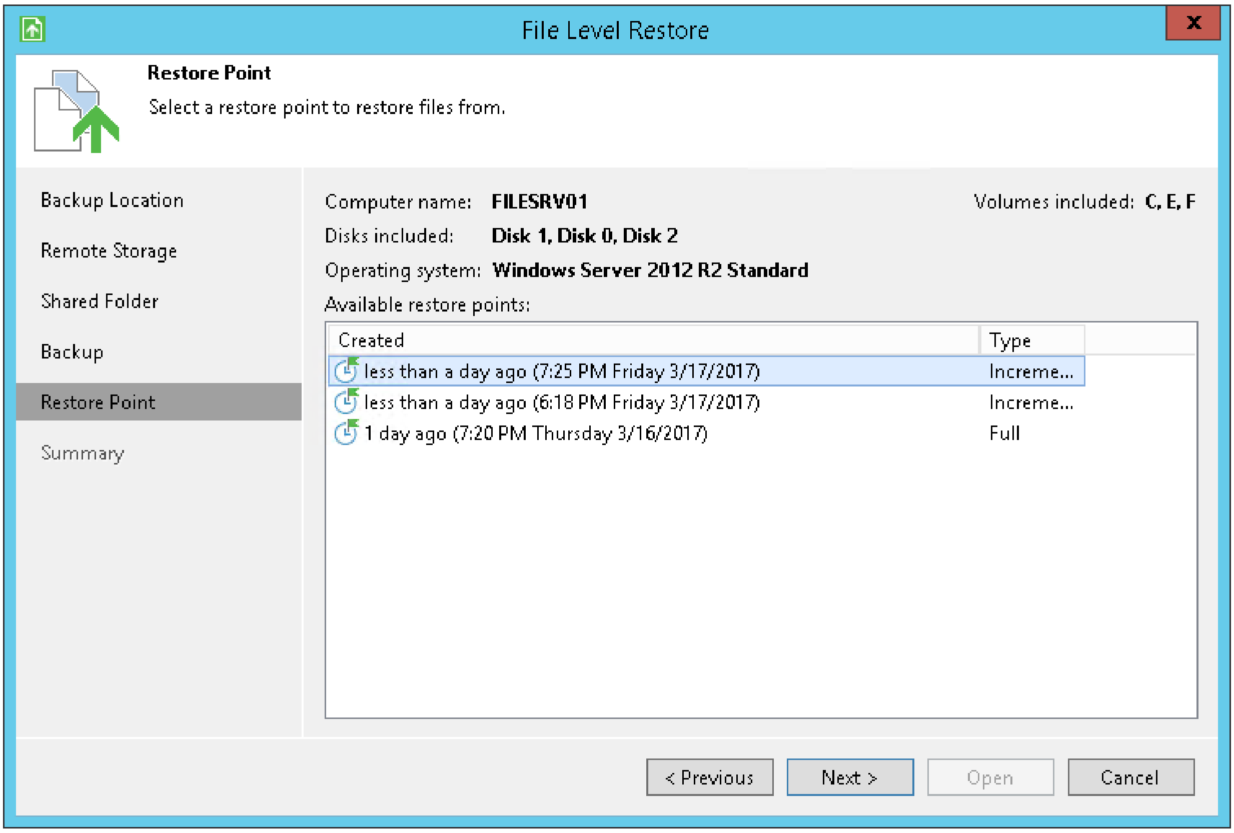
Selected computer: FILESRV01

Name	Last backup	Restore points
Backup Job FILESRV01.vbm	3/17/2017 7:25 PM	
FILESRV01	3/17/2017 7:25 PM	3

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.



Restore Point

Select a restore point to restore files from.

Computer name: **FILESRV01**

Volumes included: **C, E, F**

Disks included: **Disk 1, Disk 0, Disk 2**

Operating system: **Windows Server 2012 R2 Standard**

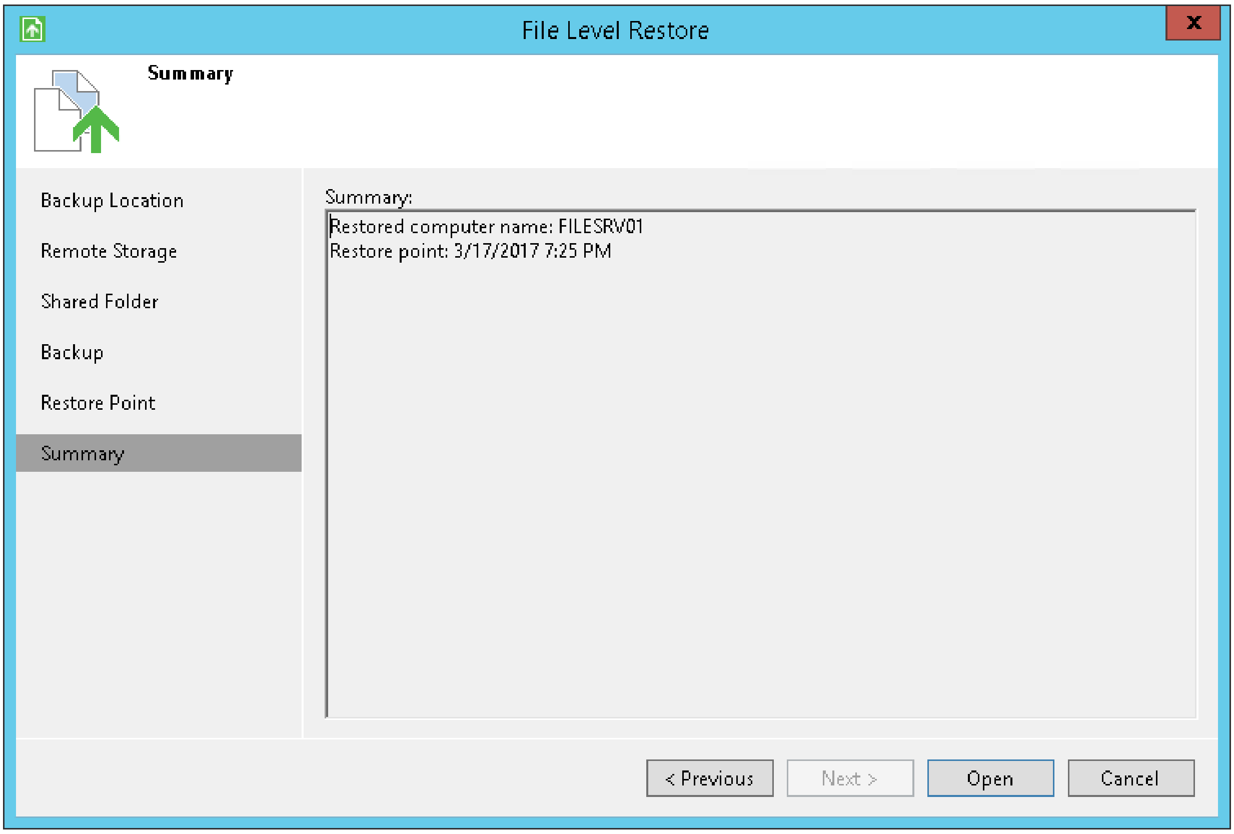
Available restore points:

Created	Type
less than a day ago (7:25 PM Friday 3/17/2017)	Increme...
less than a day ago (6:18 PM Friday 3/17/2017)	Increme...
1 day ago (7:20 PM Thursday 3/16/2017)	Full

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 **Finish**. 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.



Summary:

Restored computer name: FILESRV01
Restore point: 3/17/2017 7:25 PM

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:

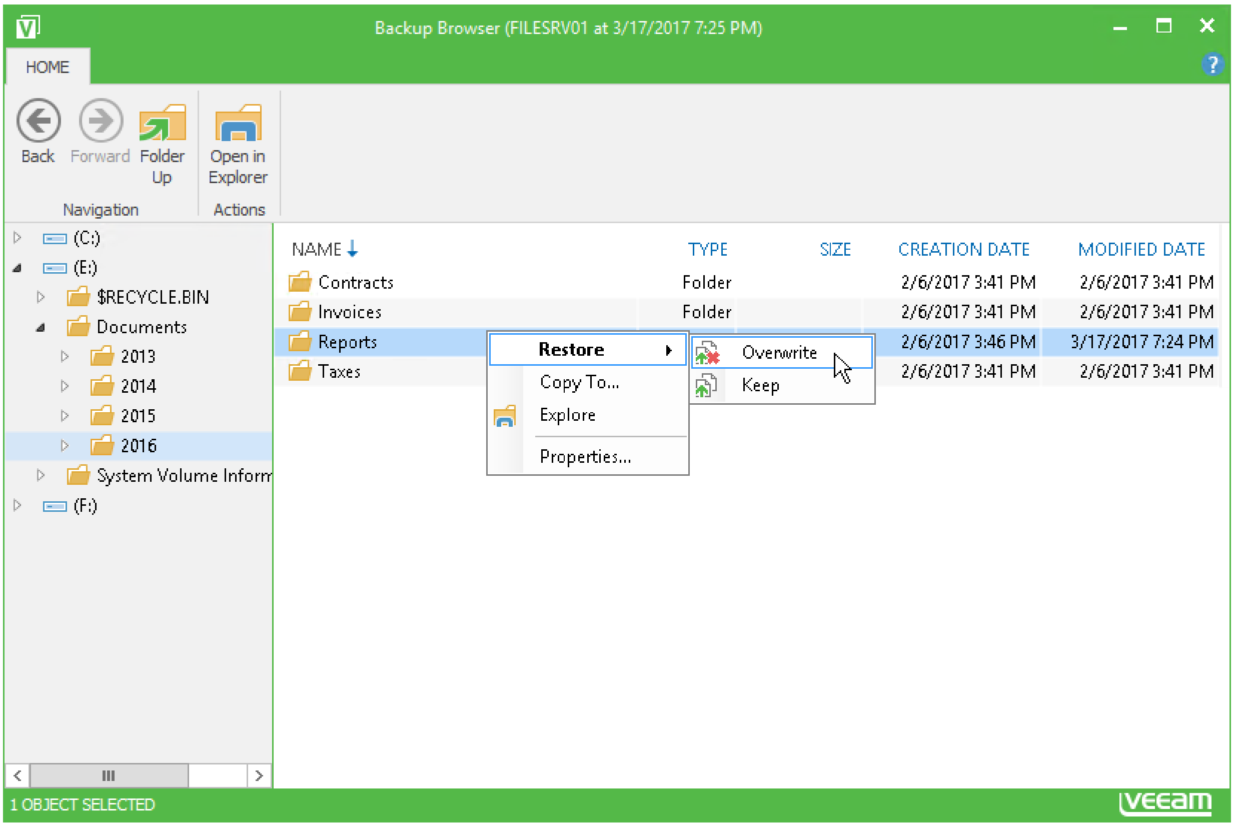
- Save files and folders to their initial location
- Save files and folders to a new location
- Open files in Microsoft Windows Explorer

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.



NAME	TYPE	SIZE	CREATION DATE	MODIFIED DATE
Contracts	Folder		2/6/2017 3:41 PM	2/6/2017 3:41 PM
Invoices	Folder		2/6/2017 3:41 PM	2/6/2017 3:41 PM
Reports			2/6/2017 3:46 PM	3/17/2017 7:24 PM
Taxes			2/6/2017 3:41 PM	2/6/2017 3:41 PM

Saving Files to New Location

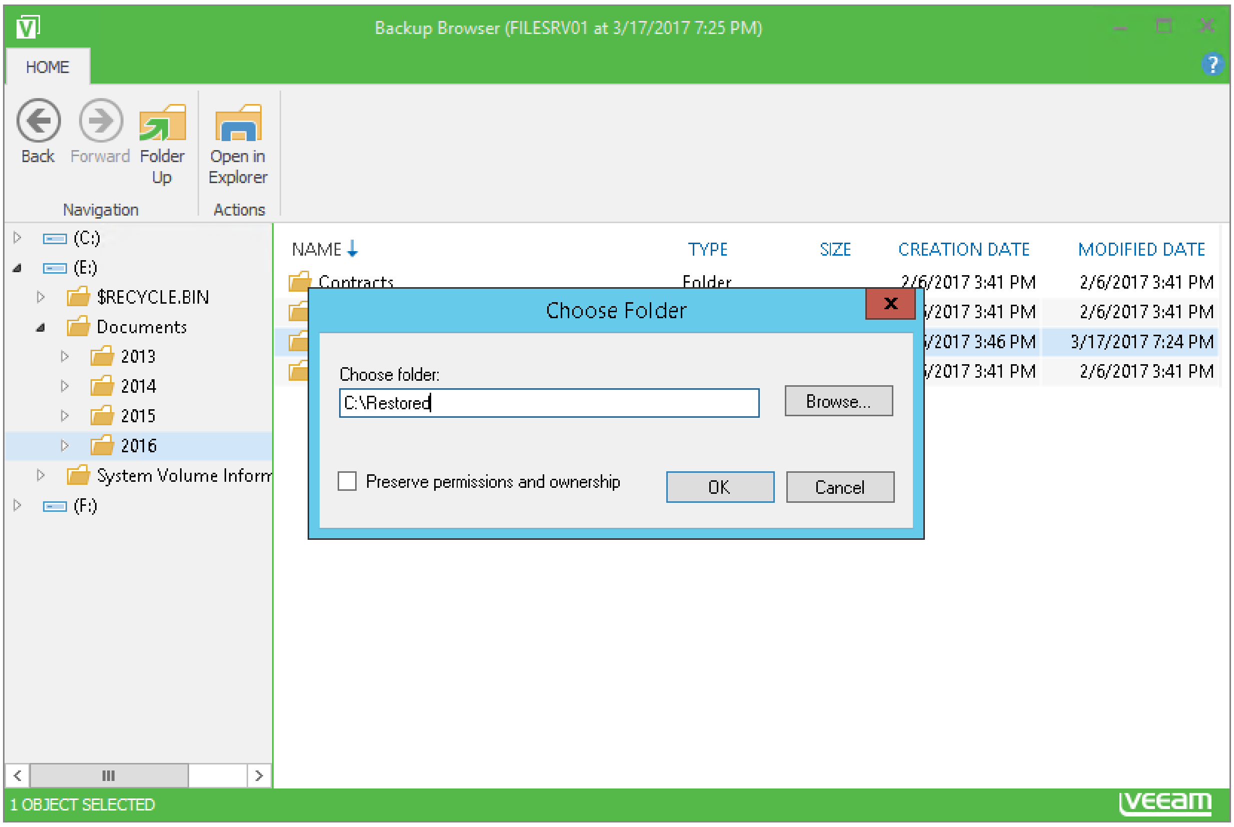
To save restored files or folders on your computer or to a network shared folder, right-click the necessary item in the file system tree or in the details pane on the right and select **Copy To**.

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.

  Please note that 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.



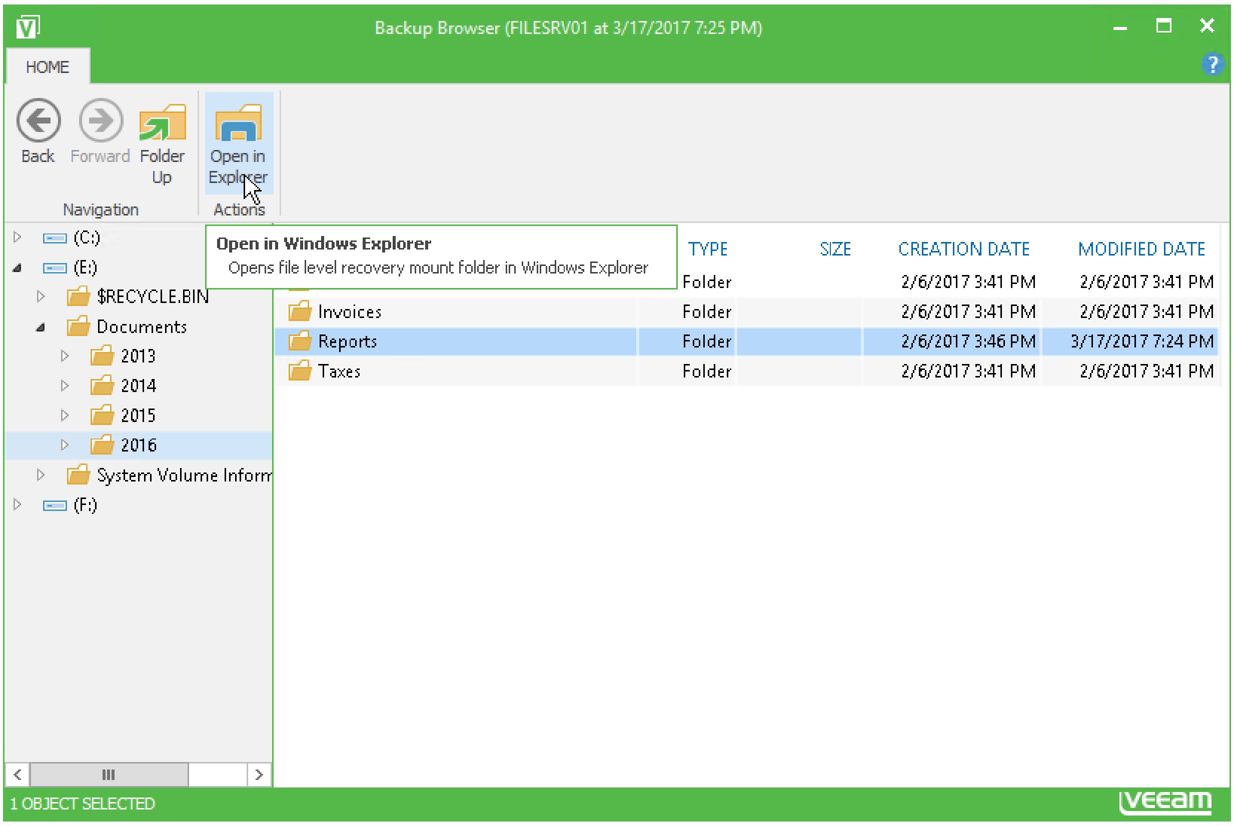
Choose folder: C:\Restored

□ Preserve permissions and ownership

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 to restored files and folders. The backup content is mounted under the `C:\VeeamFLR\ServerName` folder.



Open in Windows Explorer
Opens file level recovery mount folder in Windows Explorer

	TYPE	SIZE	CREATION DATE	MODIFIED DATE
	Folder		2/6/2017 3:41 PM	2/6/2017 3:41 PM
Invoices	Folder		2/6/2017 3:41 PM	2/6/2017 3:41 PM
Reports	Folder		2/6/2017 3:46 PM	3/17/2017 7:24 PM
Taxes	Folder		2/6/2017 3:41 PM	2/6/2017 3:41 PM

It is recommended 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 via the Microsoft Windows Explorer, these capabilities will not be available.

To learn more, see *SeBackupPrivilege* and *SeRestorePrivilege* at https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx.

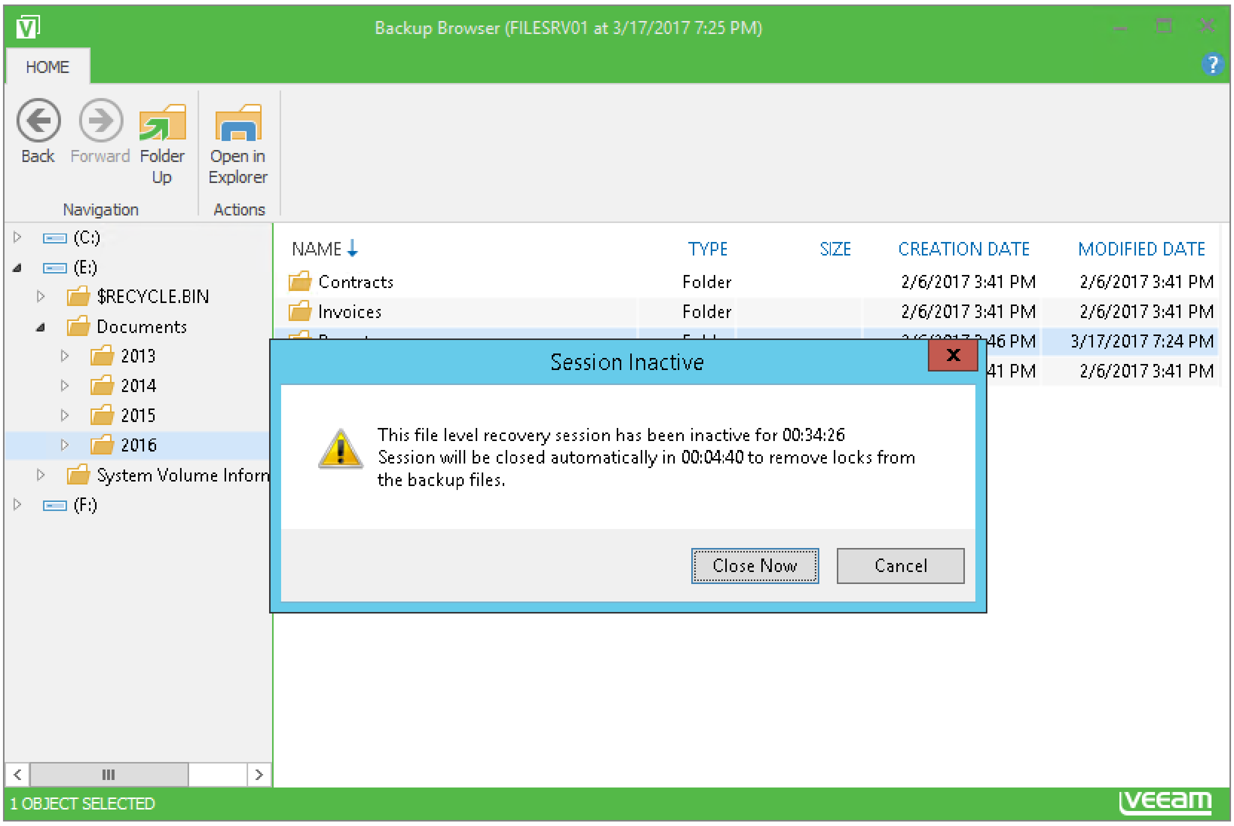
Closing Veeam Backup Browser

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.

It is recommended 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.



This file level recovery session has been inactive for 00:34:26
Session will be closed automatically in 00:04:40 to remove locks from the backup files.

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.

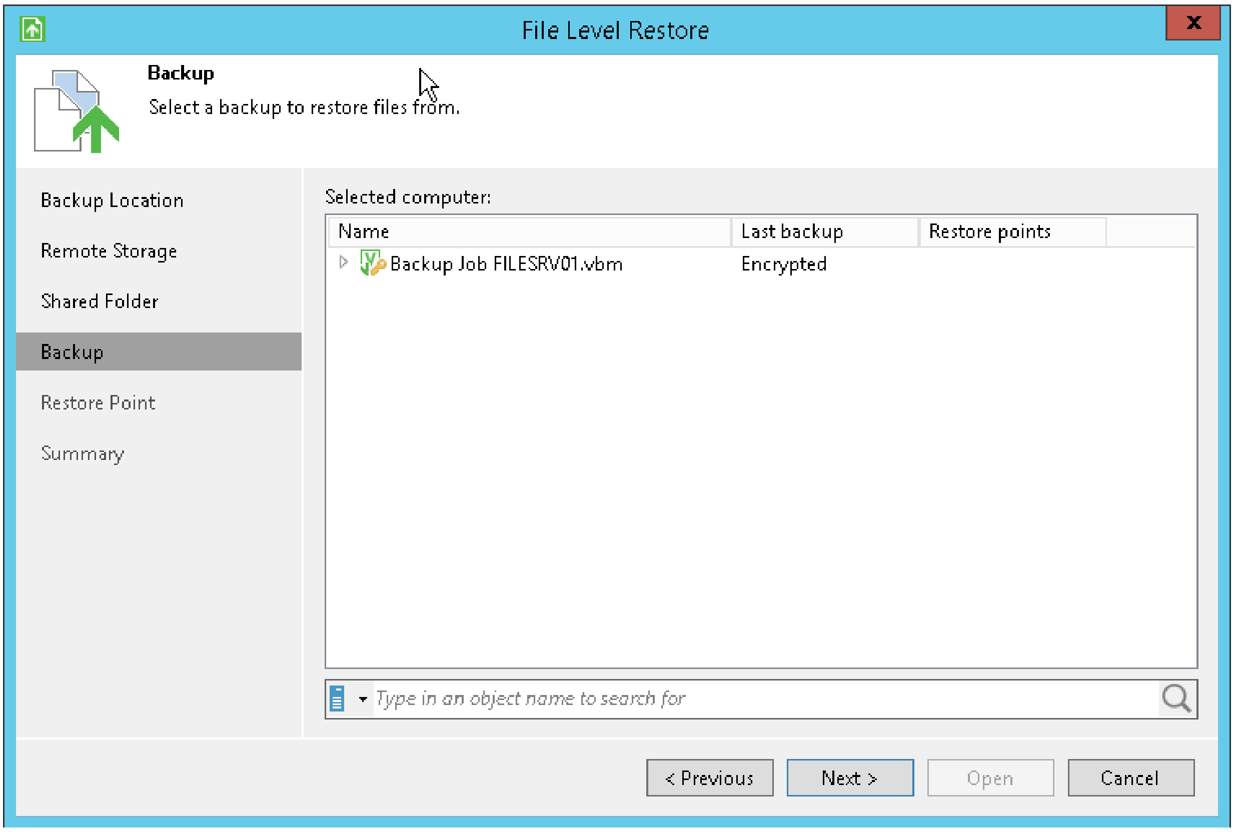
  Automatic data decryption can be performed in one of the following situations:

  - 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.



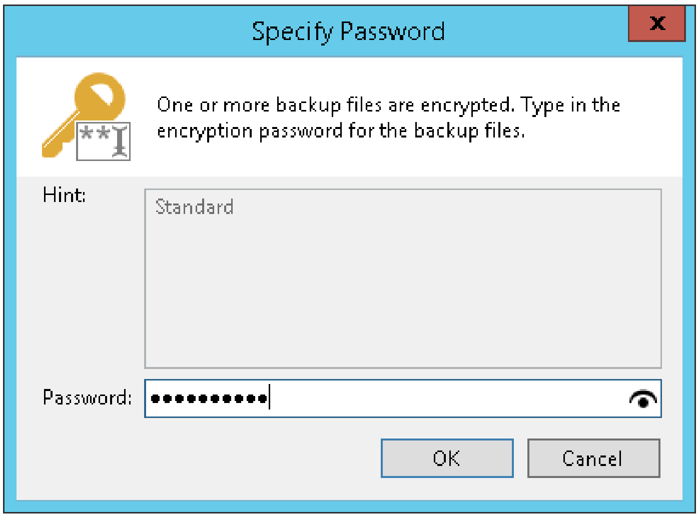
Name	Last backup	Restore points
Backup Job FILESRV01.vbm	Encrypted	

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.



Specify Password

One or more backup files are encrypted. Type in the encryption password for the backup files.

Hint: Standard

Password: ●●●●●●●●●●●

Reporting

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

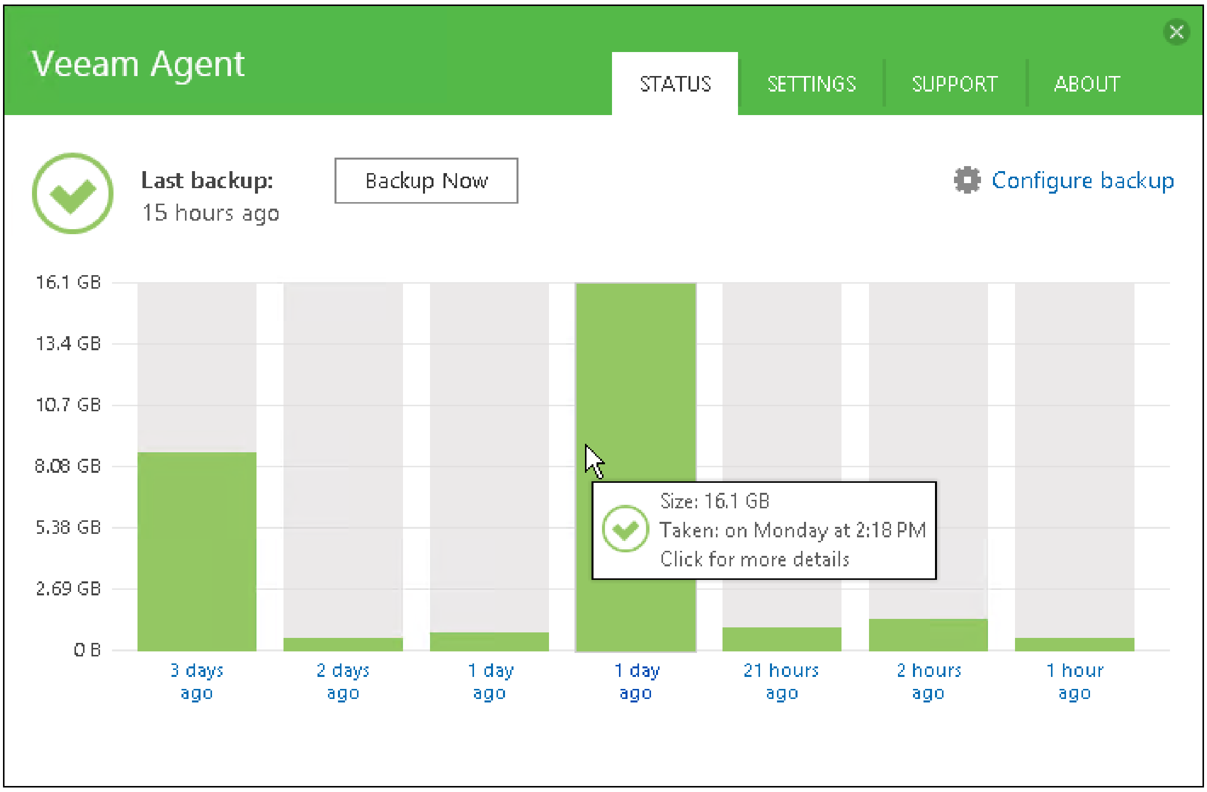
- You can view information about performed backups in the Control Panel.
- You can get information about the backup status using the Veeam Agent for Microsoft Windows tray agent.
- You can get information about the backup progress using the Veeam Agent for Microsoft Windows taskbar button.
- You can get information about Veeam Agent for Microsoft Windows events using the events bar in the Control Panel.
- You can get information about performed backups in email reports.

Viewing Statistics in Control Panel

You can use the Veeam Agent for Microsoft Windows Control Panel to view statistics about performed backups. To open the Control Panel, do either of the following:

- 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 **Control Panel**.

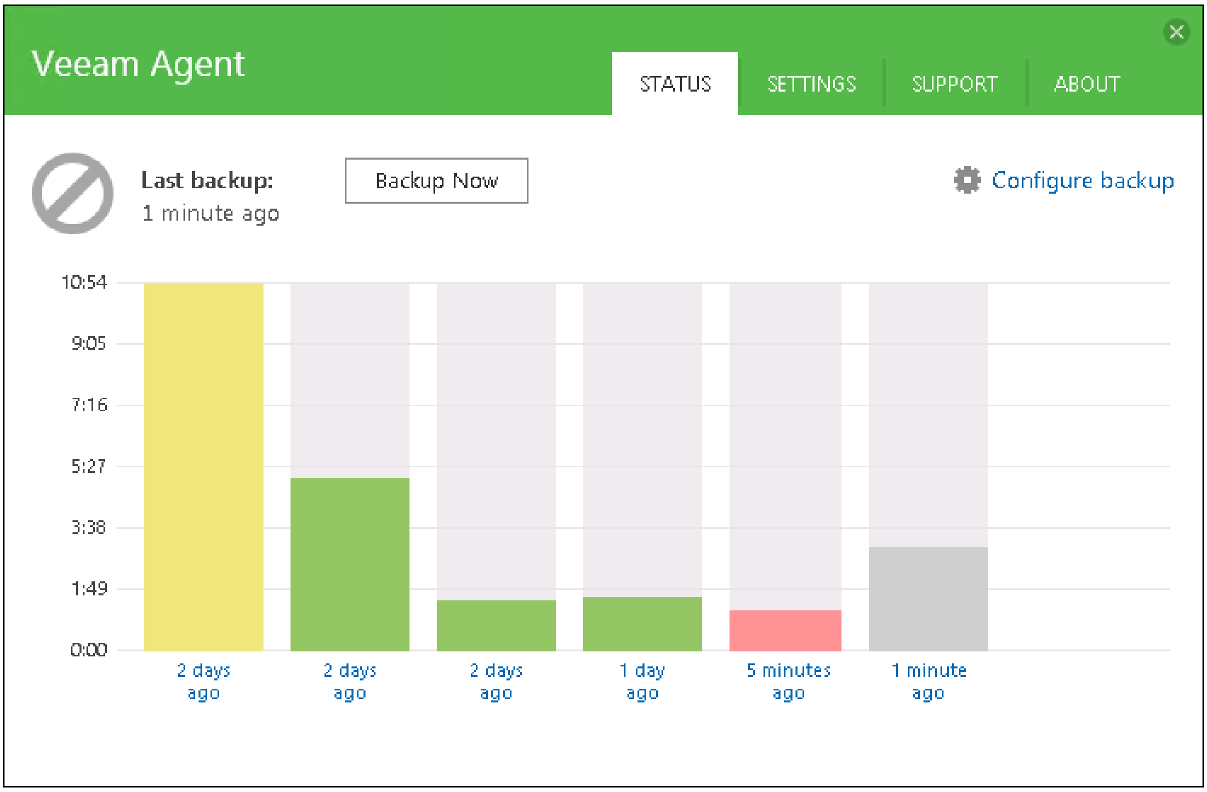
The **Status** view in the Control Panel displays information about backup job sessions that run previously and a backup job session that is currently running. Every bar represents a separate backup job session. To view general information about a specific job session, hover the mouse over the necessary bar in the chart. Veeam Agent for Microsoft Windows will provide the following details: backup status, backup time and size of the resulting backup file.



Size: 16.1 GB
Taken: on Monday at 2:18 PM
Click for more details

The bar color identifies the status of the backup job session. The backup job session can complete with one of the following statuses:

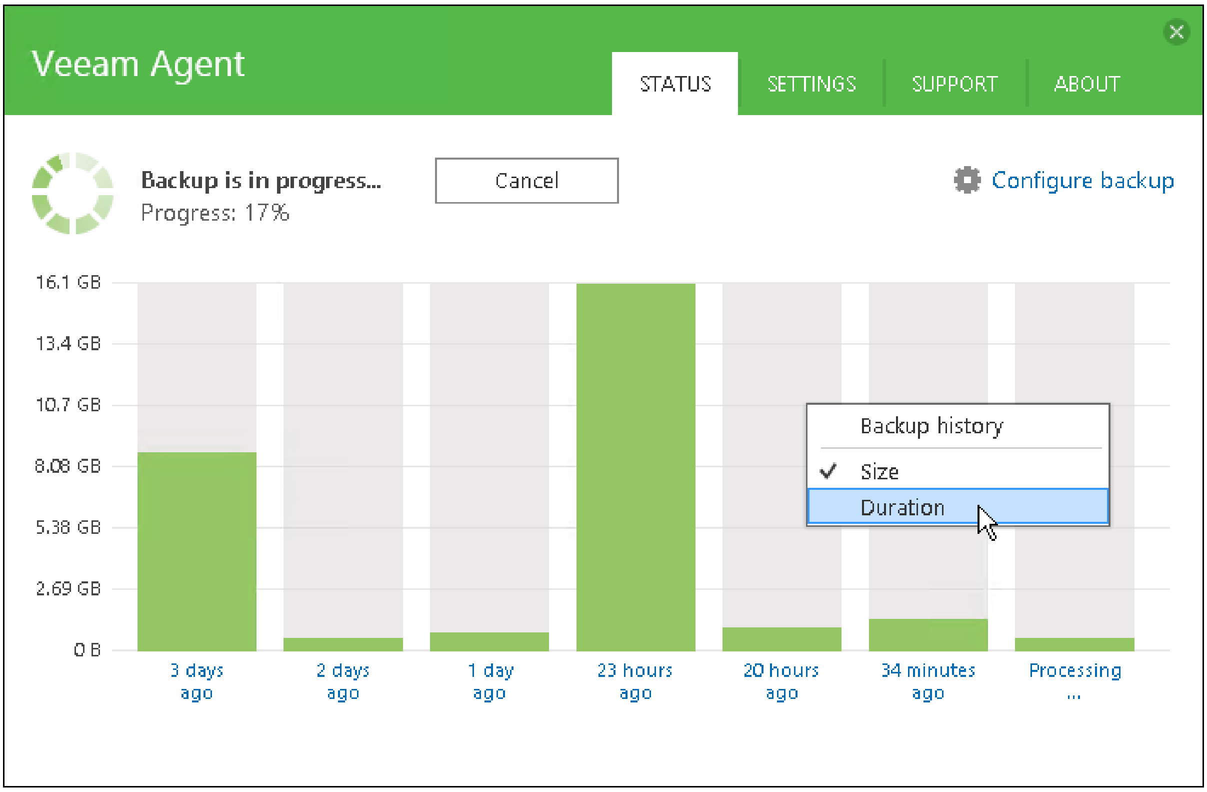
- *Success* (green color) — the backup job is currently running or has completed successfully.
- *Warning* (yellow color) — the backup job has completed with a warning. Veeam Agent for Microsoft Windows has managed to create the resulting backup file but you need to pay your attention to some alerts, 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.



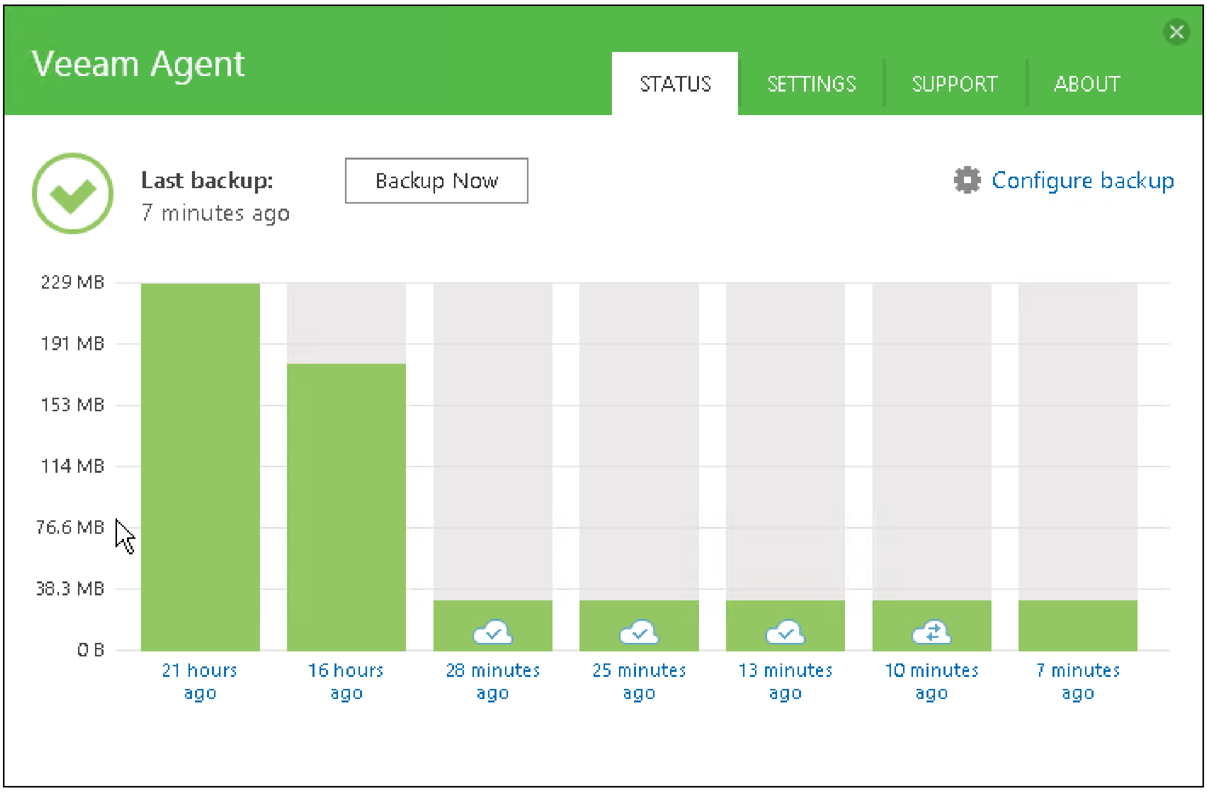
By default, Veeam Agent for Microsoft Windows displays the size of created backup files. To display the duration of backup job sessions:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**.
2. In the **Status** 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.



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

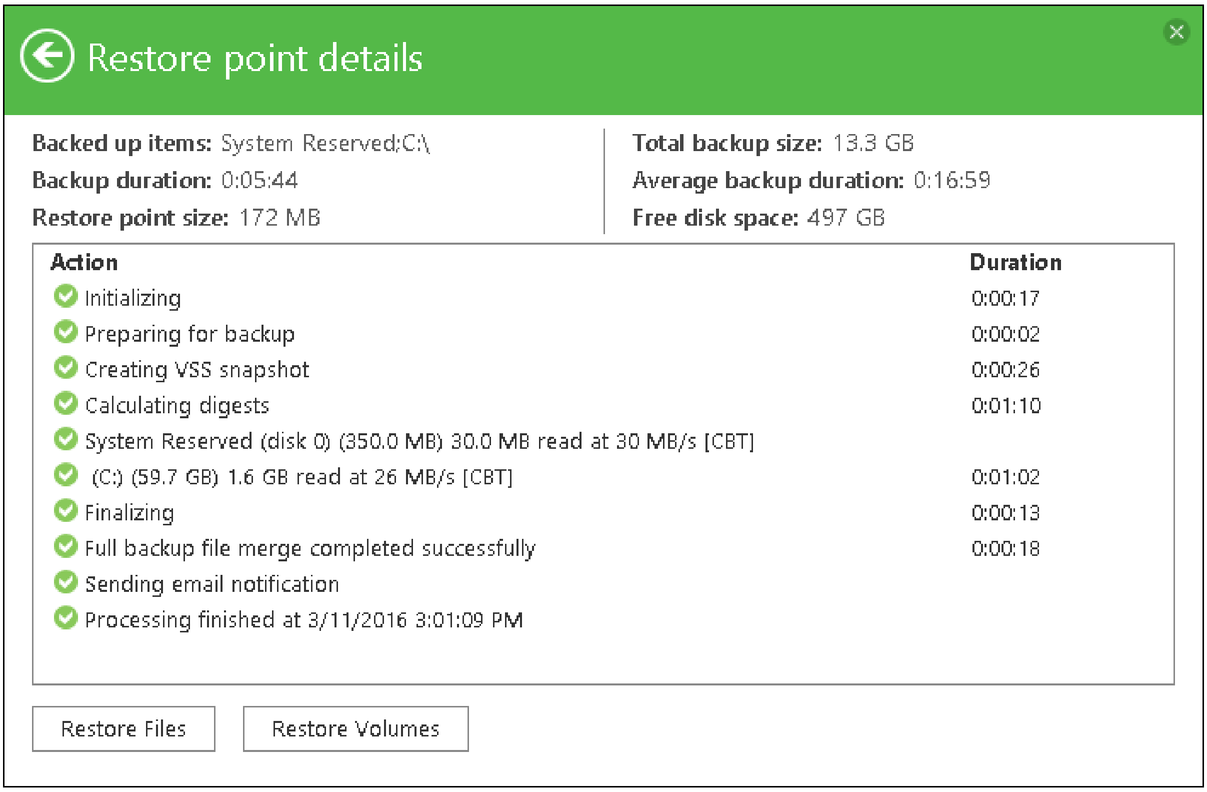
Veeam Agent for Microsoft Windows provides the following information about separate restore points in the backup chain:

- 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
- 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 for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**.
2. In the **Status** view, click the necessary bar in the chart.
3. Veeam Agent for Microsoft Windows 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 lean more, see Transaction Log Backup Statistics.



Backed up items: System Reserved;C:\
Backup duration: 0:05:44
Restore point size: 172 MB

Total backup size: 13.3 GB
Average backup duration: 0:16:59
Free disk space: 497 GB

Action	Duration
✓ Initializing	0:00:17
✓ Preparing for backup	0:00:02
✓ Creating VSS snapshot	0:00:26
✓ Calculating digests	0:01:10
✓ System Reserved (disk 0) (350.0 MB) 30.0 MB read at 30 MB/s [CBT]	
✓ (C:) (59.7 GB) 1.6 GB read at 26 MB/s [CBT]	0:01:02
✓ Finalizing	0:00:13
✓ Full backup file merge completed successfully	0:00:18
✓ Sending email notification	
✓ Processing finished at 3/11/2016 3:01:09 PM	

Transaction Log Backup Statistics

If transaction log backup is enabled for the job, you can use the Veeam Agent for Microsoft Windows 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.
- 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

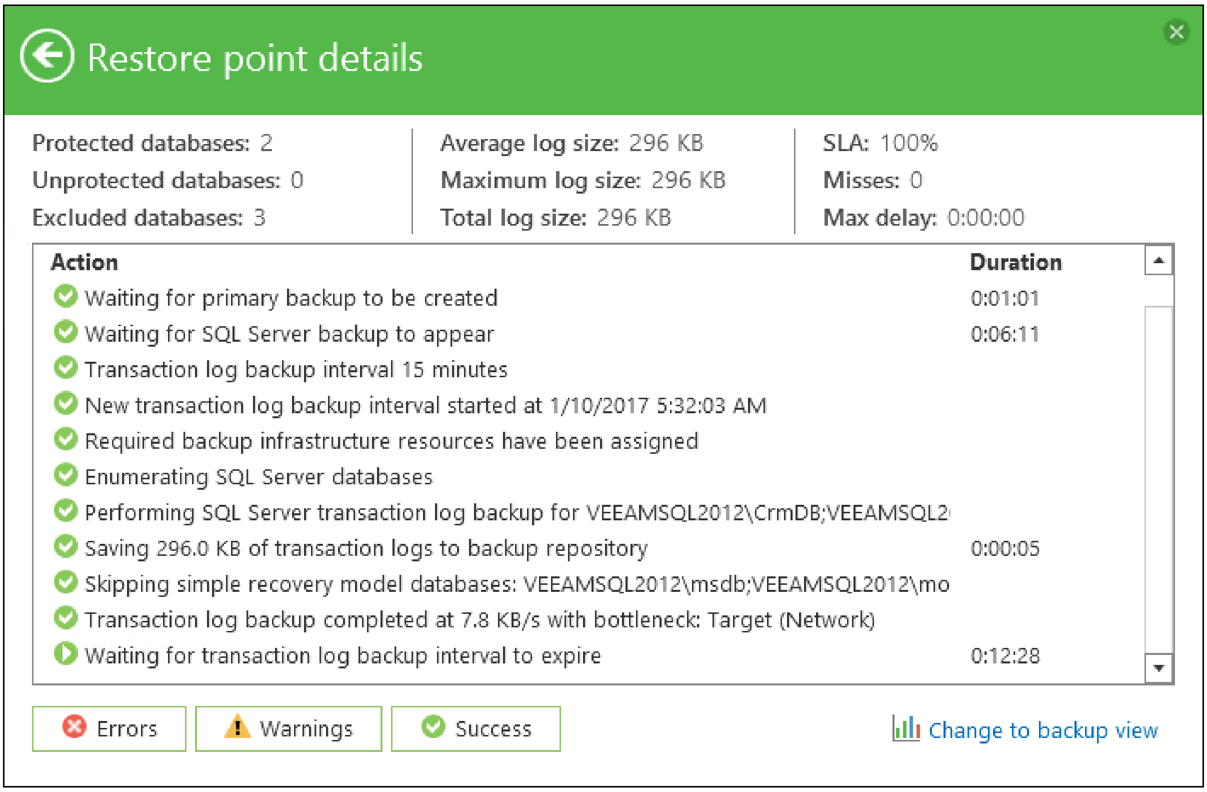
To view statistics on the transaction log backup processing:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**.

2. In the **Status** view, click the necessary bar in the chart.

3. 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.



Protected databases: 2
Unprotected databases: 0
Excluded databases: 3

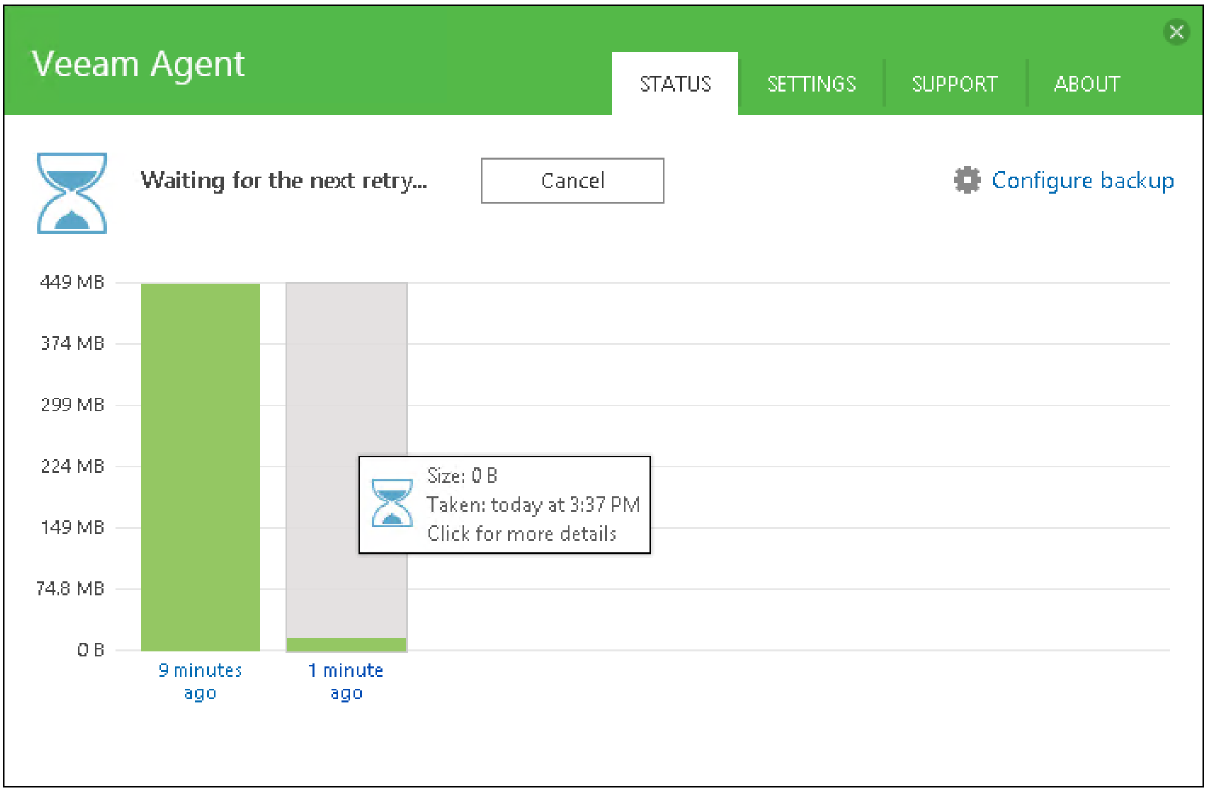
Average log size: 296 KB
Maximum log size: 296 KB
Total log size: 296 KB

SLA: 100%
Misses: 0
Max delay: 0:00:00

Action	Duration
✓ Waiting for primary backup to be created	0:01:01
✓ Waiting for SQL Server backup to appear	0:06:11
✓ Transaction log backup interval 15 minutes	
✓ New transaction log backup interval started at 1/10/2017 5:32:03 AM	
✓ Required backup infrastructure resources have been assigned	
✓ Enumerating SQL Server databases	
✓ Performing SQL Server transaction log backup for VEEAMSQL2012\CrmDB;VEEAMSQL2	
✓ Saving 296.0 KB of transaction logs to backup repository	0:00:05
✓ Skipping simple recovery model databases: VEEAMSQL2012\msdb;VEEAMSQL2012\mo	
✓ Transaction log backup completed at 7.8 KB/s with bottleneck: Target (Network)	
▶ Waiting for transaction log backup interval to expire	0:12:28

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:

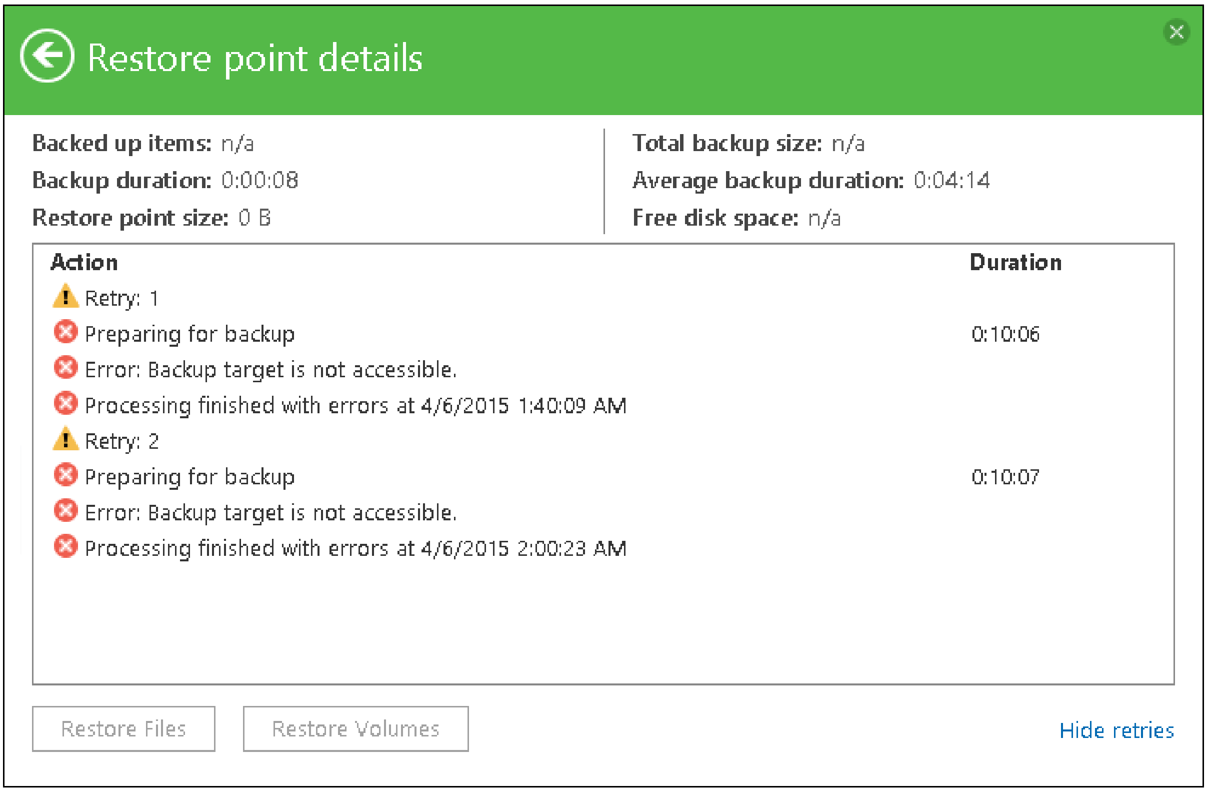
For portable devices, Veeam Agent for Microsoft Windows does not automatically retry the backup job if a device is working on battery.

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. In the **Status** view, click the necessary bar in the chart.

3. At the bottom right corner of the window, click the **Show retries** link.

4. 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

Backed up items: n/a
Backup duration: 0:00:08
Restore point size: 0 B

Total backup size: n/a
Average backup duration: 0:04:14
Free disk space: n/a

Action	Duration
⚠ Retry: 1	
⊗ Preparing for backup	0:10:06
⊗ Error: Backup target is not accessible.	
⊗ Processing finished with errors at 4/6/2015 1:40:09 AM	
⚠ Retry: 2	
⊗ Preparing for backup	0:10:07
⊗ Error: Backup target is not accessible.	
⊗ Processing finished with errors at 4/6/2015 2:00:23 AM	

Viewing Status of Restore Points in Backup Cache

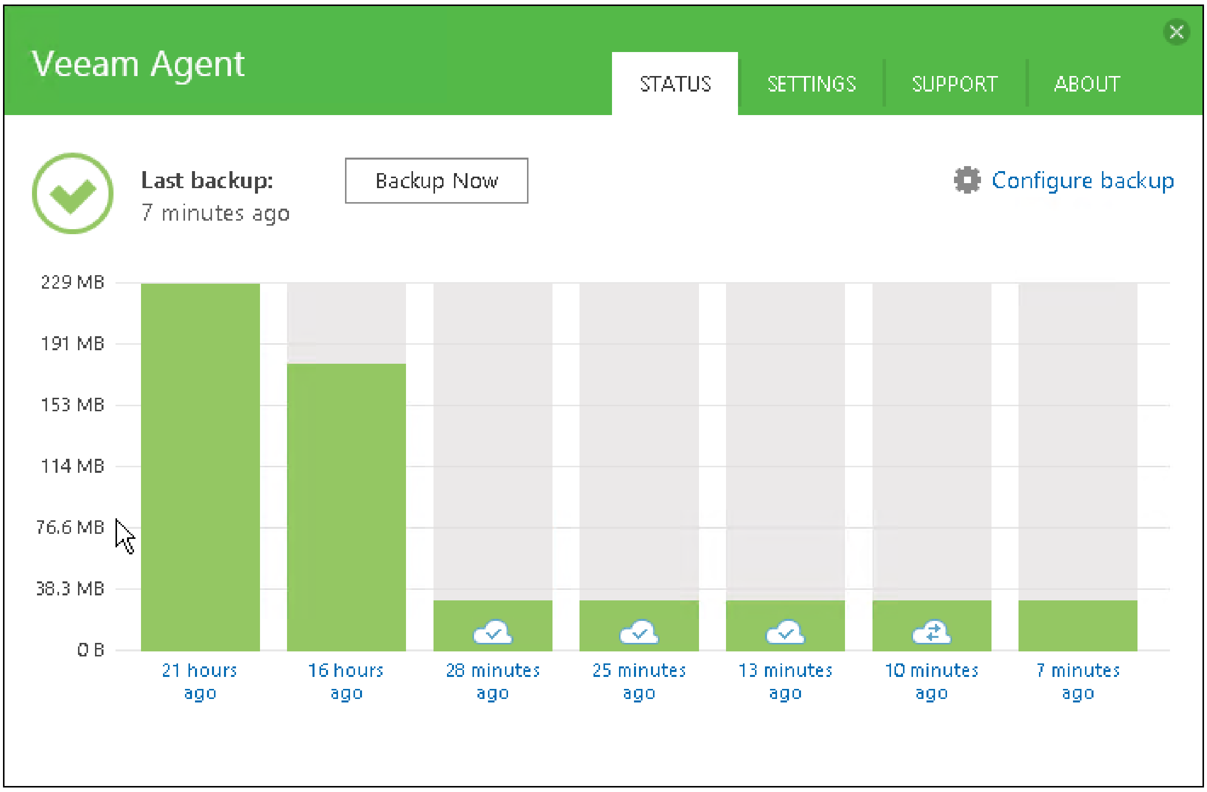
If the backup cache is enabled for the job, you can monitor status of restore points in the backup cache. Veeam Agent for Microsoft Windows displays the restore point status through the icon on a bar in the chart.

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 and 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

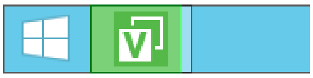
The Veeam Agent for Microsoft Windows icon displayed in the system tray lets you monitor the state of your backups and get informed about the computer protection status.

The icon can be in one of the following states:

Icon	Description	Backup state
V	Question mark over the icon	The backup job is not configured.
V	Veeam Agent for Microsoft Windows icon	The backup job is set up but scheduling settings for the job are not configured.
V	Animated icon	The backup task is being performed. To view the backup task progress, hover the mouse over the icon.
V	Clock over the icon	The latest session of the scheduled backup job has completed successfully; waiting for the next backup job session.
V	Sync sign over the icon	Veeam Agent for Microsoft Windows is uploading backup file(s) from the backup cache to the target storage.
V	Cancel sign over the icon	The latest session of the scheduled backup job has been canceled.
V	Error sign over the icon	An error occurred during the latest backup job session, and the session was terminated.
V	Minus sign over the icon	The scheduled backup job is disabled.
V	Grey icon	The tray agent is not connected to the Veeam Agent for Microsoft Windows service.
V	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 for Microsoft Windows also displays a warning on the notifications bar in the Control Panel. You can attach the target removable storage device to the computer within 10 minutes, and Veeam Agent for Microsoft Windows will automatically start the scheduled backup job.

Monitoring Backup Process in Taskbar Button

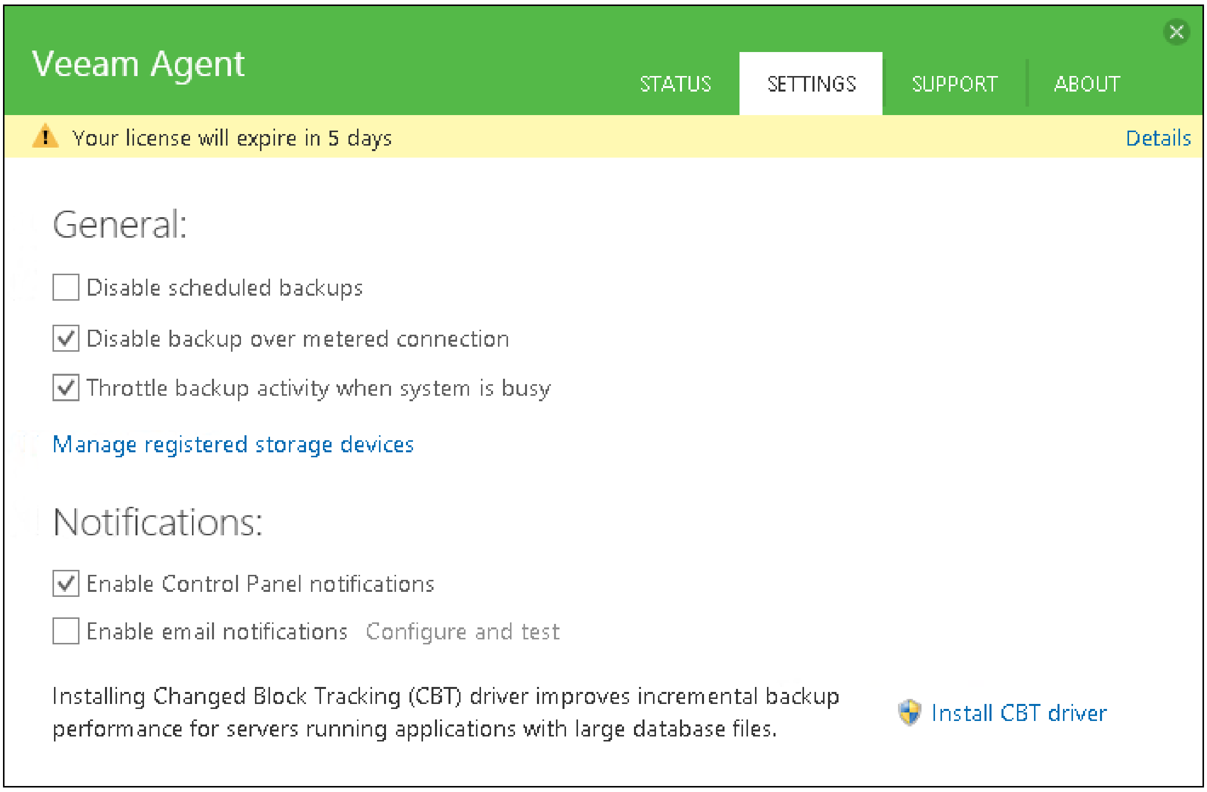
You can monitor the backup process with the Veeam Agent for Microsoft Windows taskbar button. Veeam Agent for Microsoft Windows displays on the taskbar button a green progress bar that reflects the bar for the currently running job session in the Control Panel. As a result, you can track the process 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 for Microsoft Windows displays a notification bar with the event description in the Control Panel window. Veeam Agent for Microsoft Windows can inform you about the following events using the notification bar:

- The Veeam Recovery Media has not been created.
- The Veeam Recovery Media needs to be updated (for example, after you have updated the Microsoft Windows OS).
- The backup storage is getting low on free disk space.
- The target backup location is not accessible by the moment when the scheduled backup job must start.
- 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.
- [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.
- A newer version of Veeam Agent for Microsoft Windows is available.
- The Veeam Agent for Microsoft Windows license will expire in N days.
- The Veeam Agent for Microsoft Windows has expired. To continue using the product, you need to obtain a new license.



Your license will expire in 5 days

General:

☐ Disable scheduled backups

☑ Disable backup over metered connection

☑ Throttle backup activity when system is busy

Notifications:

☑ Enable Control Panel notifications

☐ Enable email notifications

Installing Changed Block Tracking (CBT) driver improves incremental backup performance for servers running applications with large database files.

You can get detailed information about events and dismiss events not to get alerted of them in future.

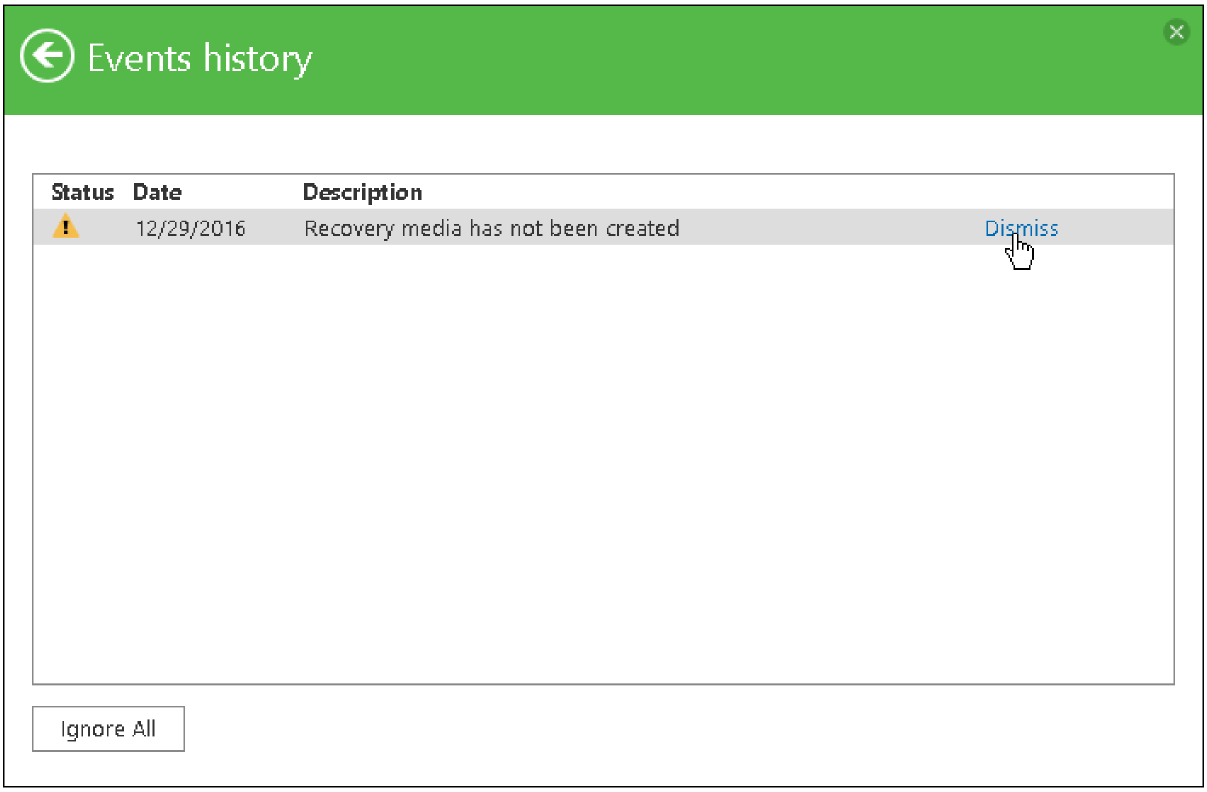
Veeam Agent for Microsoft Windows displays only the latest event in the notification bar. To view detailed information about all event:

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.

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.



Status	Date	Description	
⚠	12/29/2016	Recovery media has not been created	Dismiss

Viewing Job Session Results in Email Reports

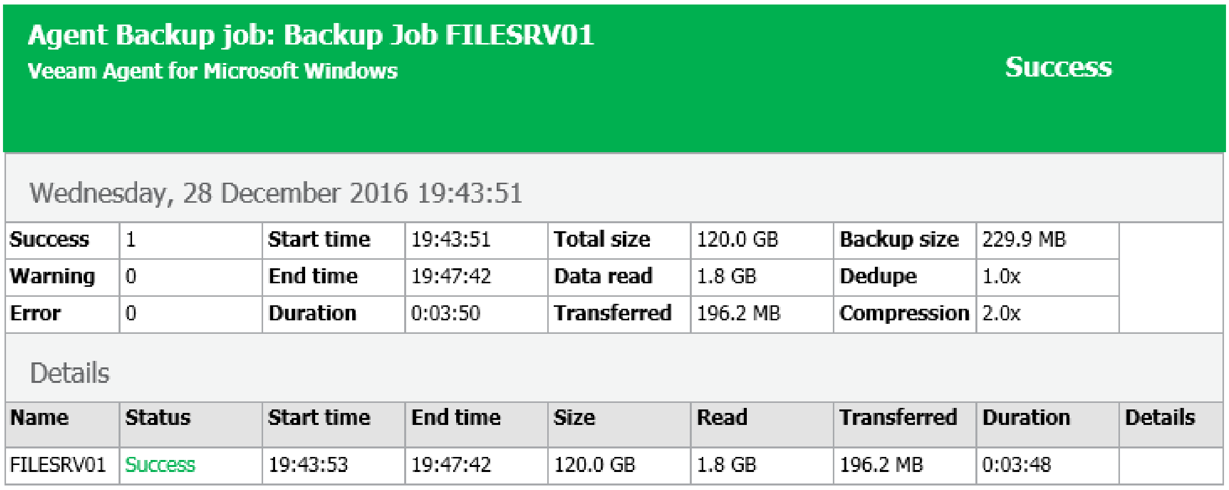
You can receive email notifications with Veeam Agent for Microsoft Windows job results. When the backup job session completes, Veeam Agent for Microsoft Windows will send a report containing data on the job session to the specified email address.

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: Backup Job FILESRV01
Veeam Agent for Microsoft Windows

Success

Wednesday, 28 December 2016 19:43:51

Success	1	**Start time**	19:43:51	**Total size**	120.0 GB	**Backup size**	229.9 MB
Warning	0	**End time**	19:47:42	**Data read**	1.8 GB	**Dedupe**	1.0x
Error	0	**Duration**	0:03:50	**Transferred**	196.2 MB	**Compression**	2.0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FILESRV01	Success	19:43:53	19:47:42	120.0 GB	1.8 GB	196.2 MB	0:03:48	

Specifying Settings

You can use global settings of Veeam Agent for Microsoft Windows to accomplish the following tasks:

- Disable and enable the scheduled backup job
- Disable backup over metered connections
- Throttle backup activities
- Manage backup storage devices
- Disable Control Panel notifications
- Enable email notifications
- Check for new product versions and updates

Disabling Backup over Metered Connections

Veeam Agent for Microsoft Windows can disable backup over metered Internet connections to help you avoid extra costs. If you use a metered Internet connection, a service provider charges by the amount of data sent and received by your computer. Veeam Agent for Microsoft Windows can automatically detect metered connections and will not perform backup when your computer is on such connection.

The disable setting applies to all types of backups: scheduled and ad-hoc. Mind the following limitations and requirements:

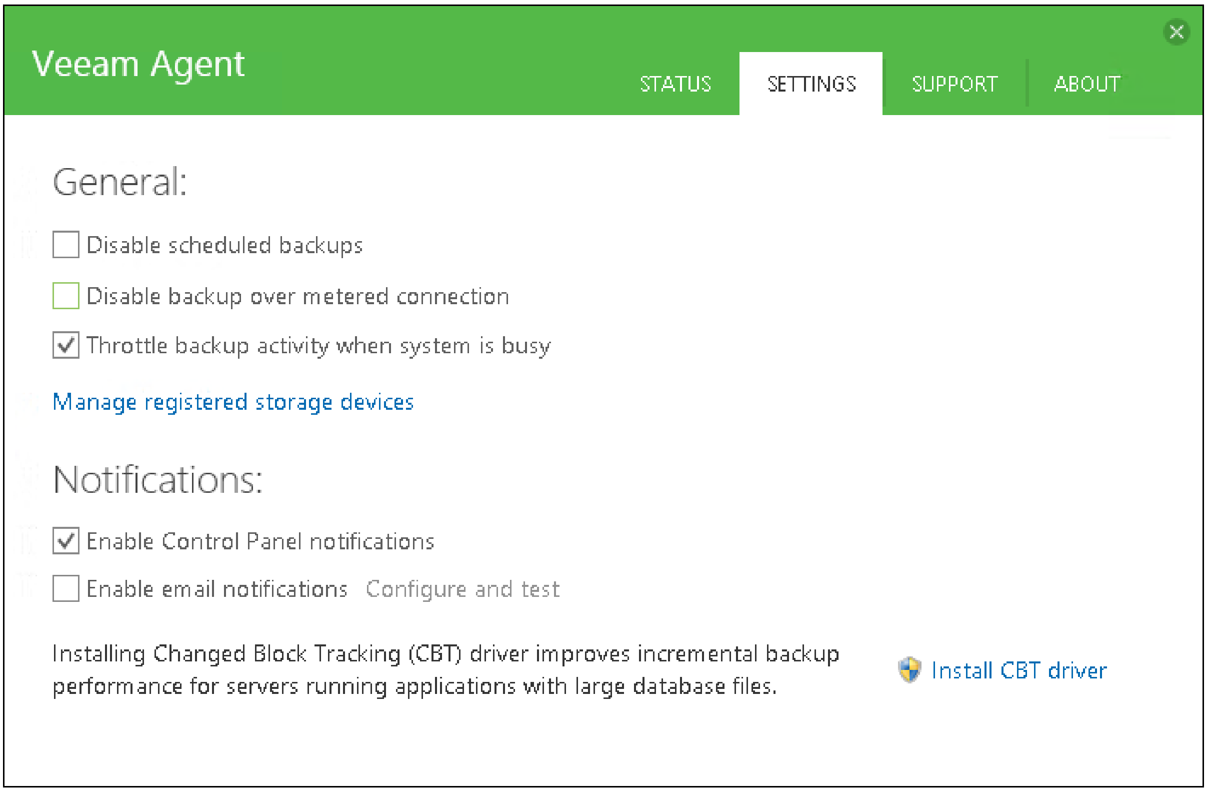
- Veeam Agent for Microsoft Windows disables backup over metered Internet connections only on computers that run Microsoft Windows 8 and later. If the computer runs an earlier version of Microsoft Windows, this option is not applicable.
- You must specify which connections are metered in Microsoft Windows. To learn more, see https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

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. At the top of the window, click the **Settings** tab.
3. Clear **Disable backup over metered connection** check box.

NOTE:

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.



General:

☐ Disable scheduled backups

☐ Disable backup over metered connection

☑ Throttle backup activity when system is busy

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 for servers running applications with large database files.

Install CBT driver

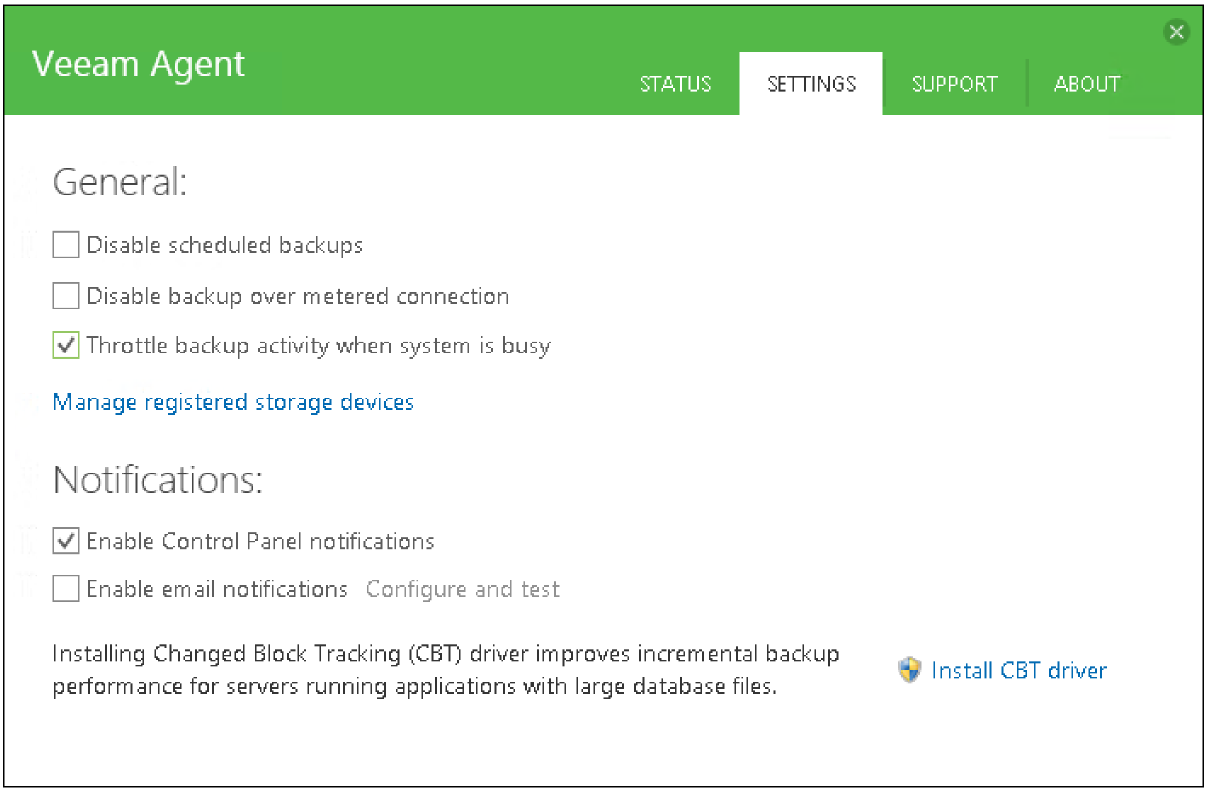
Throttling Backup Activities

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. At the top of the window, click the **Settings** tab.
3. Select the **Throttle backup activity when system is busy** check box.



General:

□ Disable scheduled backups

□ Disable backup over metered connection

☑ Throttle backup activity when system is busy

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 for servers running applications with large database files.

Install CBT driver

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.

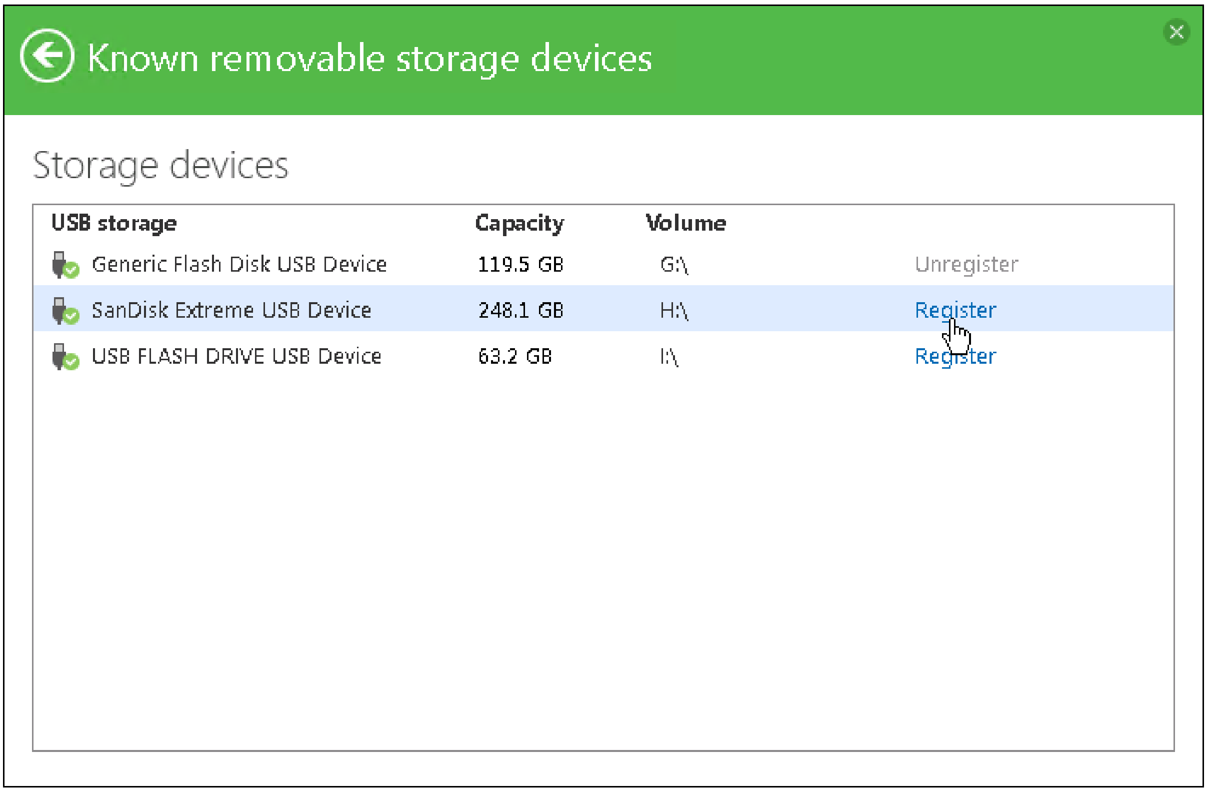
The drive on which you plan to store a backup must be registered in Veeam Agent for Microsoft Windows. If the drive is not registered, Veeam Agent for Microsoft Windows will not be able to detect the drive and store a backup on it.

Mind 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 on 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. Click the **Settings** tab.
3. Click the **Manage registered backup storage devices** link.
4. In the list of devices, click **Register/Unregister** next to the necessary backup storage device.

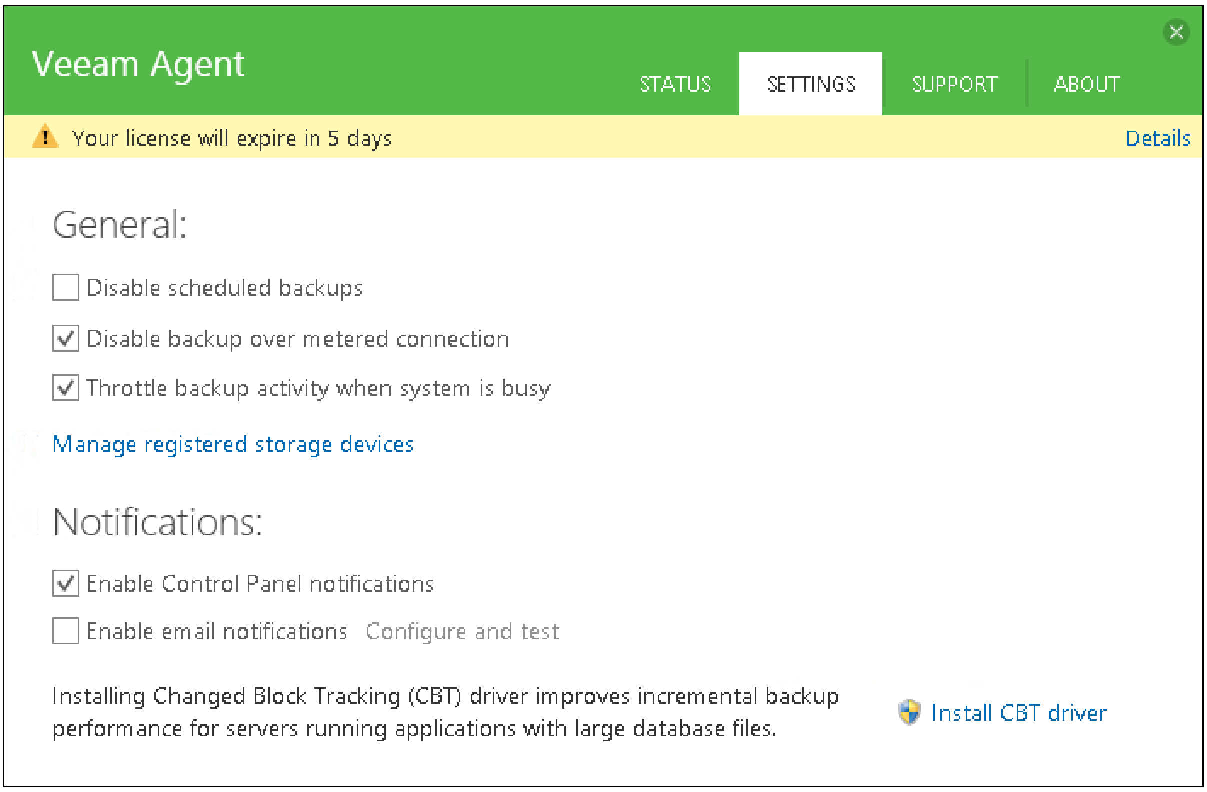


Storage devices

USB storage	Capacity	Volume	
Generic Flash Disk USB Device	119.5 GB	G:\	Unregister
SanDisk Extreme USB Device	248.1 GB	H:\	Register
USB FLASH DRIVE USB Device	63.2 GB	I:\	Register

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.



Your license will expire in 5 days

General:

□ Disable scheduled backups

☑ Disable backup over metered connection

☑ Throttle backup activity when system is busy

Notifications:

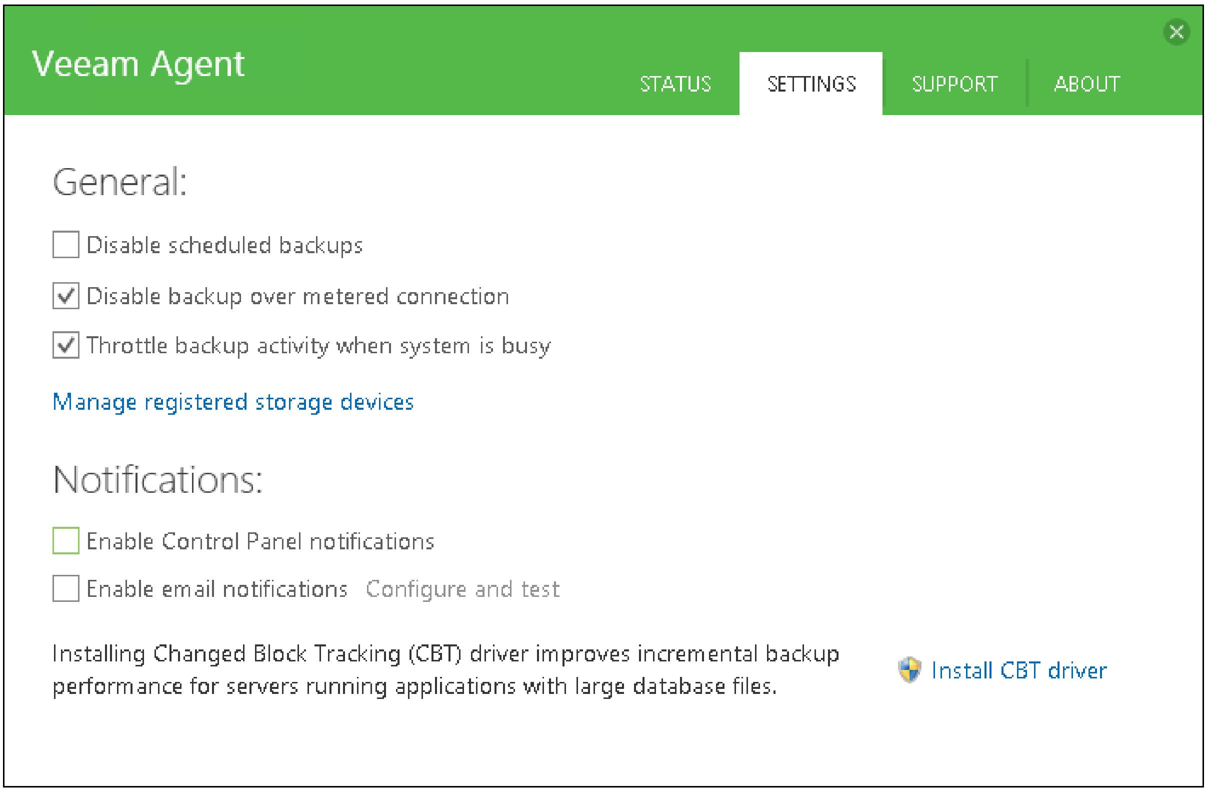
☑ Enable Control Panel notifications

□ Enable email notifications

Installing Changed Block Tracking (CBT) driver improves incremental backup performance for servers running applications with large database files.

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. At the top of the window, click the **Settings** tab.
3. In the **Notifications** section, clear the **Enable Control Panel notifications** check box.



General:

□ Disable scheduled backups

☑ Disable backup over metered connection

☑ Throttle backup activity when system is busy

Manage registered storage devices

Notifications:

□ Enable Control Panel notifications

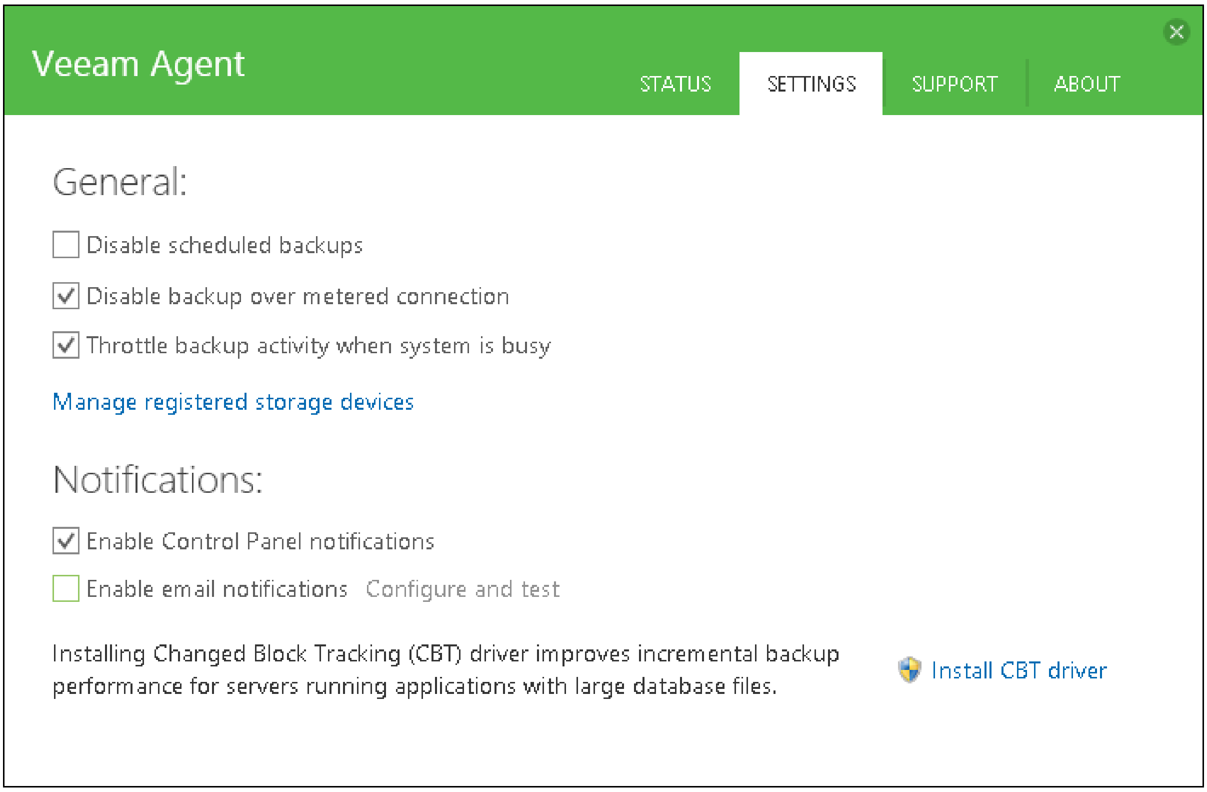
□ Enable email notifications   Configure and test

Installing Changed Block Tracking (CBT) driver improves incremental backup performance for servers running applications with large database files.

Install CBT driver

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.



General:

□ Disable scheduled backups

☑ Disable backup over metered connection

☑ Throttle backup activity when system is busy

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 for servers running applications with large database files.

Install CBT driver

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. At the top of the window, click the **Settings** tab.

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, in the **Email settings** section, specify the recipient address.

   Veeam Agent for Microsoft Windows will send email notifications to the specified address. This address will be also displayed as the sender address in the email notification headers.

5. If the SMTP server requires authentication, specify a password for the account that has rights to access the SMTP server.

6. Specify a subject for the sent message. You can use the following variables in the subject:

   a. %ComputerName%

   b. %JobResult%

   c. %CompletionTime%

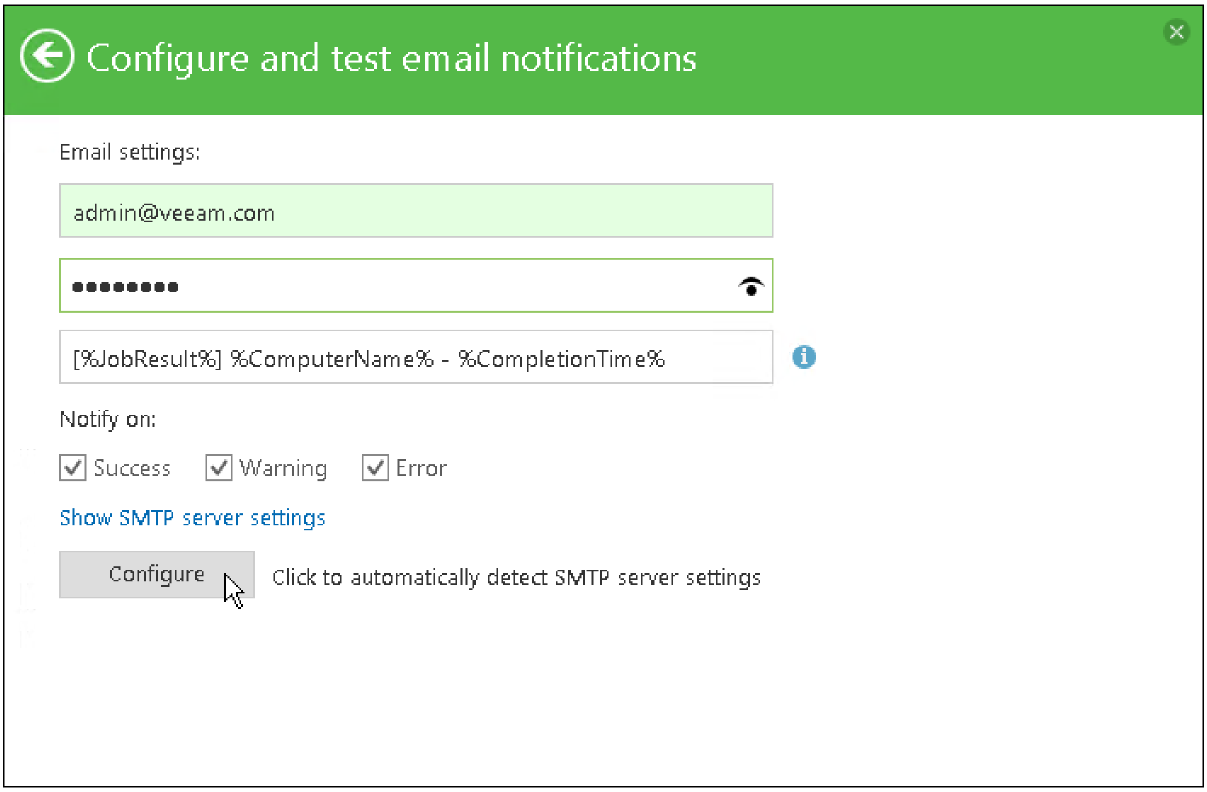
7. In the **Notify on** section, select the **Success**, **Warning** and/or **Error** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.

8. Click **Configure**. Veeam Agent for Microsoft Windows will try to automatically detect SMTP server settings. If the SMTP server settings are detected successfully, Veeam Agent for Microsoft Windows will display the settings (SMTP server name, port and user name), send a test message to the specified email address and save the email notification settings in the database.

   You can change automatically detected settings in the **SMTP server settings** section. You can perform this operation manually at any time. To learn more, see Configuring SMTP Server Settings.

   If the SMTP server settings are not validated for some reason, Veeam Agent for Microsoft Windows will display a link to the following Veeam Knowledge Base article: https://www.veeam.com/kb2109. You can refer to this article for additional information on the SMTP server settings configuration.

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 for Microsoft Windows database.



Configure and test email notifications

Email settings:

admin@veeam.com

●●●●●●●●

[%JobResult%] %ComputerName% - %CompletionTime%

Notify on:

☑ Success ☑ Warning ☑ Error

Show SMTP server settings

Configure

Click to automatically detect SMTP server settings

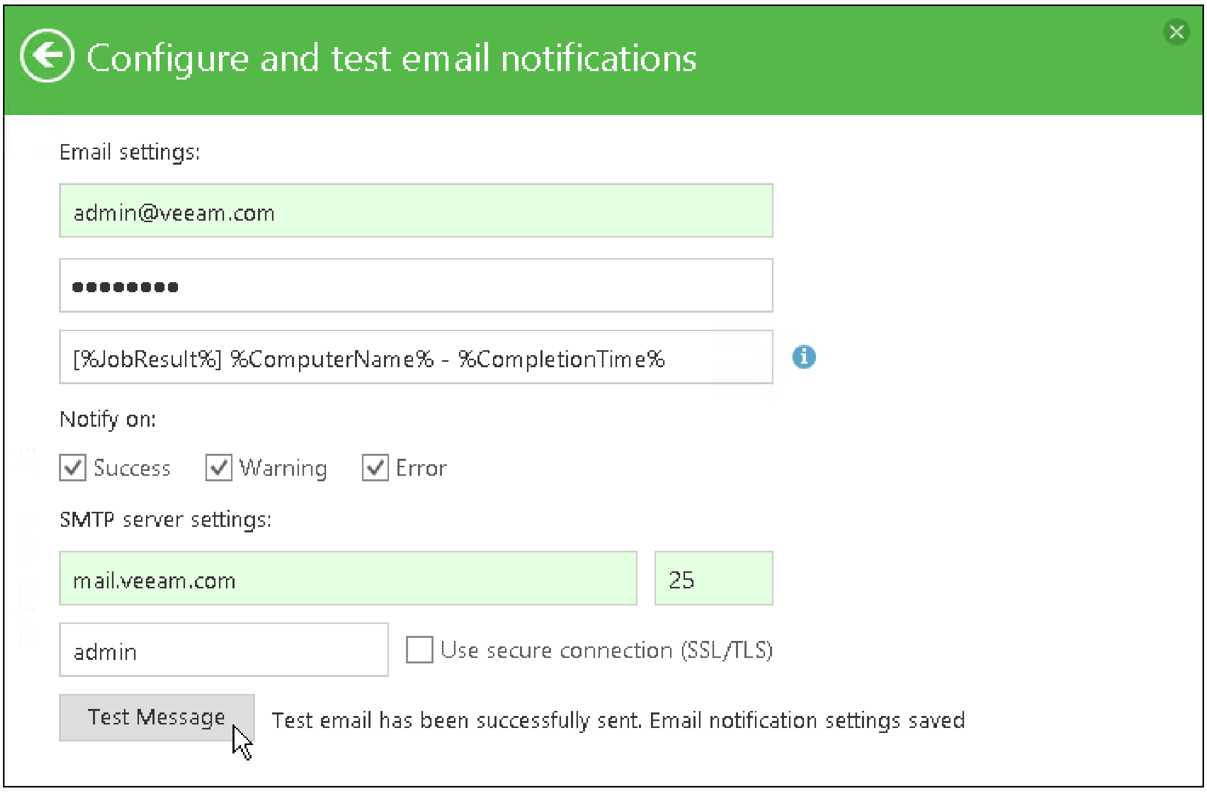
Configuring SMTP Server Settings

When you specify recipient email address and password, Veeam Agent for Microsoft Windows tries to automatically detect settings to connect to the SMTP server. You can change automatically detected settings, for example, when Veeam Agent for Microsoft Windows does not detect correct settings for some reason.

To configure SMTP server settings:

1. Click the **Show SMTP server settings** link.
2. Enter a full DNS name or IP address of the SMTP server that will be used for sending email notifications.
3. Specify the port number for the SMTP server.
4. Specify a user name for the account that has rights to access the SMTP server.
5. To use a secure SSL/TLS connection for email operations, select the **Use secure connection** check box.
6. Click **Test Message** to validate the SMTP server settings and send a test email.

> **TIP:**
>
> To change the email notification settings, clear the entered values from the **SMTP server DNS name or IP address**, **Port** and **User name** fields, enter the new recipient address and click **Configure**. Veeam Agent for Microsoft Windows will try to detect settings for the specified email address.



Configure and test email notifications

Email settings:

admin@veeam.com

●●●●●●●●

[%JobResult%] %ComputerName% - %CompletionTime%

Notify on:

☑ Success ☑ Warning ☑ Error

SMTP server settings:

mail.veeam.com

25

admin

□ Use secure connection (SSL/TLS)

Test email has been successfully sent. Email notification settings saved

Checking for New Product Versions and Updates

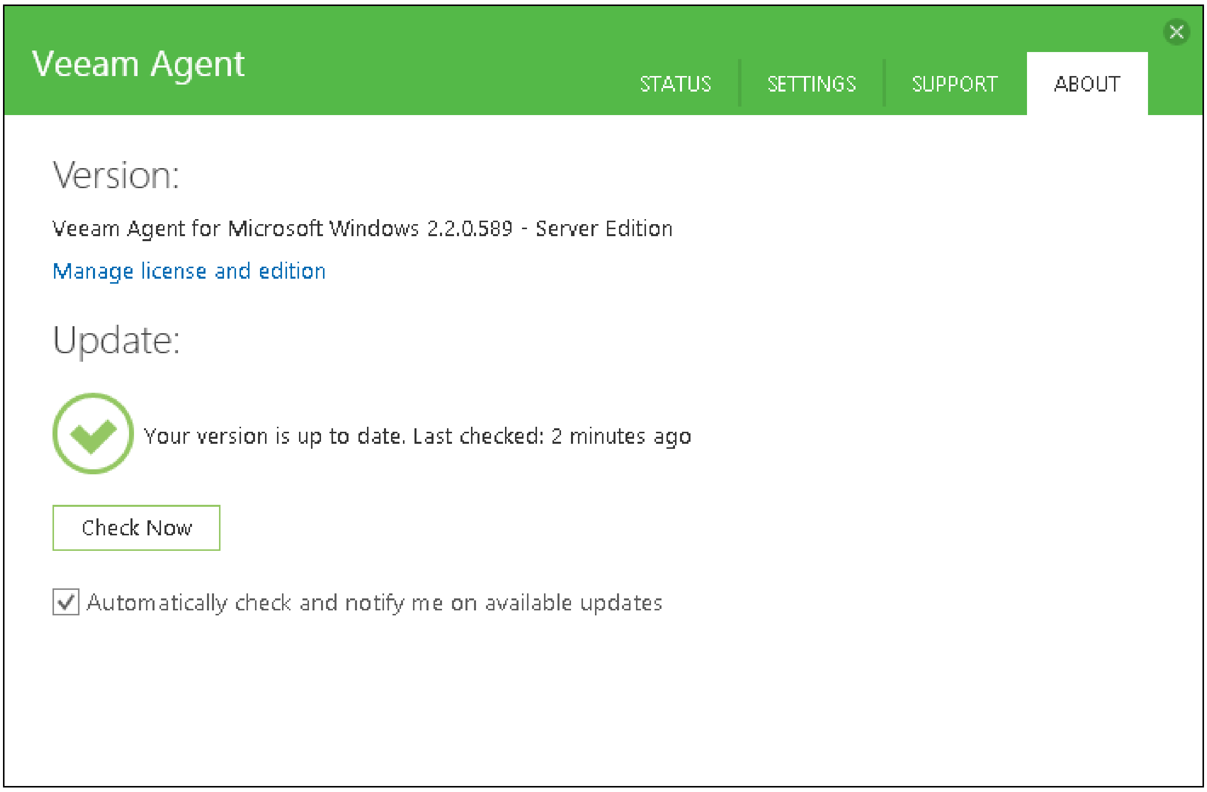
You can set up Veeam Agent for Microsoft Windows to automatically notify you about new product versions and updates. When a new version or patch becomes available, Veeam Agent for Microsoft Windows displays a notification in the notification bar. You can download the setup file and update Veeam Agent 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. Click the **About** tab.
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:**
>
> For downloading setup files, Veeam Agent for Microsoft Windows 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.



Version:

Veeam Agent for Microsoft Windows 2.2.0.589 - Server Edition

Manage license and edition

Update:

Your version is up to date. Last checked: 2 minutes ago

☑ Automatically check and notify me on available updates

Managing Veeam CBT Driver

You can set up Veeam Agent for Microsoft Windows to use the Veeam CBT driver instead of the default CBT mechanism. This option is available if the Veeam Agent computer meets the following requirements:

- Runs a Microsoft Windows Server OS
- Runs the Server edition of Veeam Agent for Microsoft Windows

The Veeam CBT driver offers more efficient changed block tracking mechanism that will be useful for servers running applications with large database files. To learn more, see Changed Block Tracking Driver.

You can perform the following operations with the Veeam CBT driver in Veeam Agent for Microsoft Windows:

- Install the Veeam CBT driver.
- Remove the Veeam CBT driver.

Installing Veeam CBT Driver

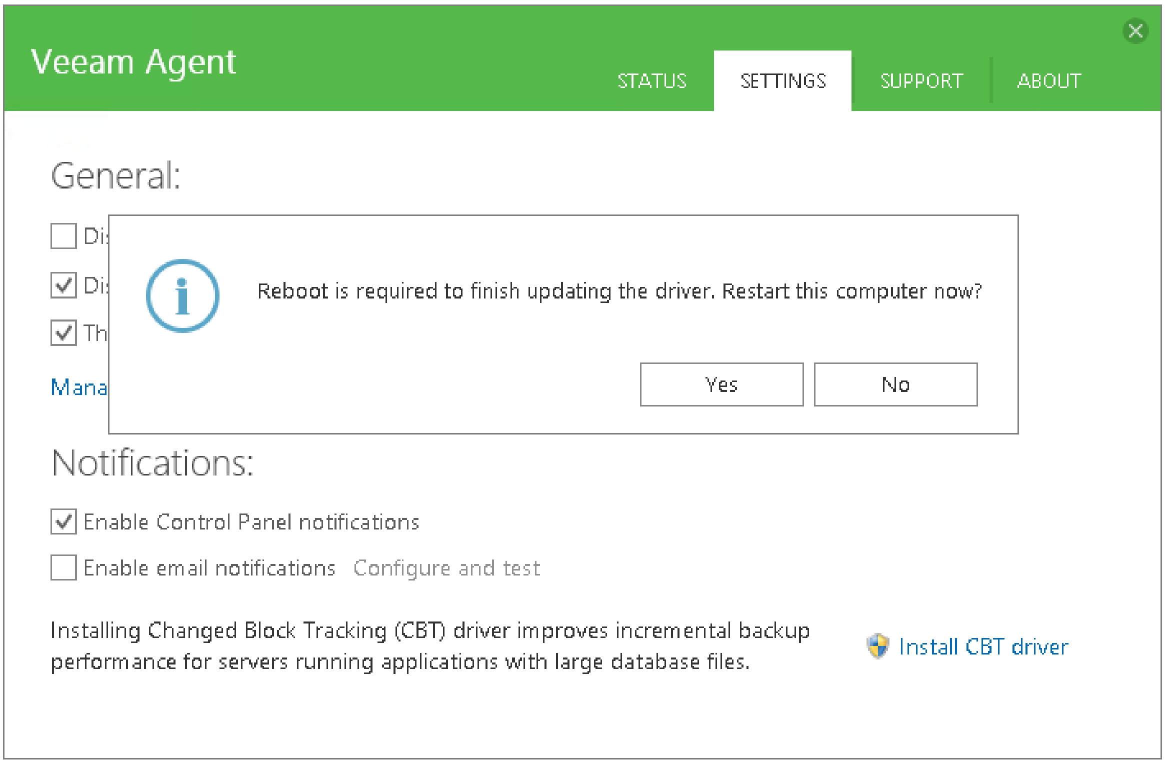
You can install the Veeam CBT driver at any time you need. This operation is available if you use the Server edition of Veeam Agent for Microsoft Windows on a computer that runs a Microsoft Windows Server OS.

> **IMPORTANT!**
>
> Consider the following:
>
> - Prior to installing the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2, make sure that update KB3033929 is installed in the OS. To learn more, see https://www.microsoft.com/en-us/download/details.aspx?id=46083.
> - Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2, 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.

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. At the top of the window, click the **Settings** tab.
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 **OK**. After Veeam Agent for Microsoft Windows reboots the computer, the driver will start tracking blocks that are changing on the volume(s) 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.



General:

□ Di

☑ Di

☑ Th

Mana

Reboot is required to finish updating the driver. Restart this computer now?

Notifications:

☑ Enable Control Panel notifications

□ Enable email notifications Configure and test

Installing Changed Block Tracking (CBT) driver improves incremental backup performance for servers running applications with large database files.

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.

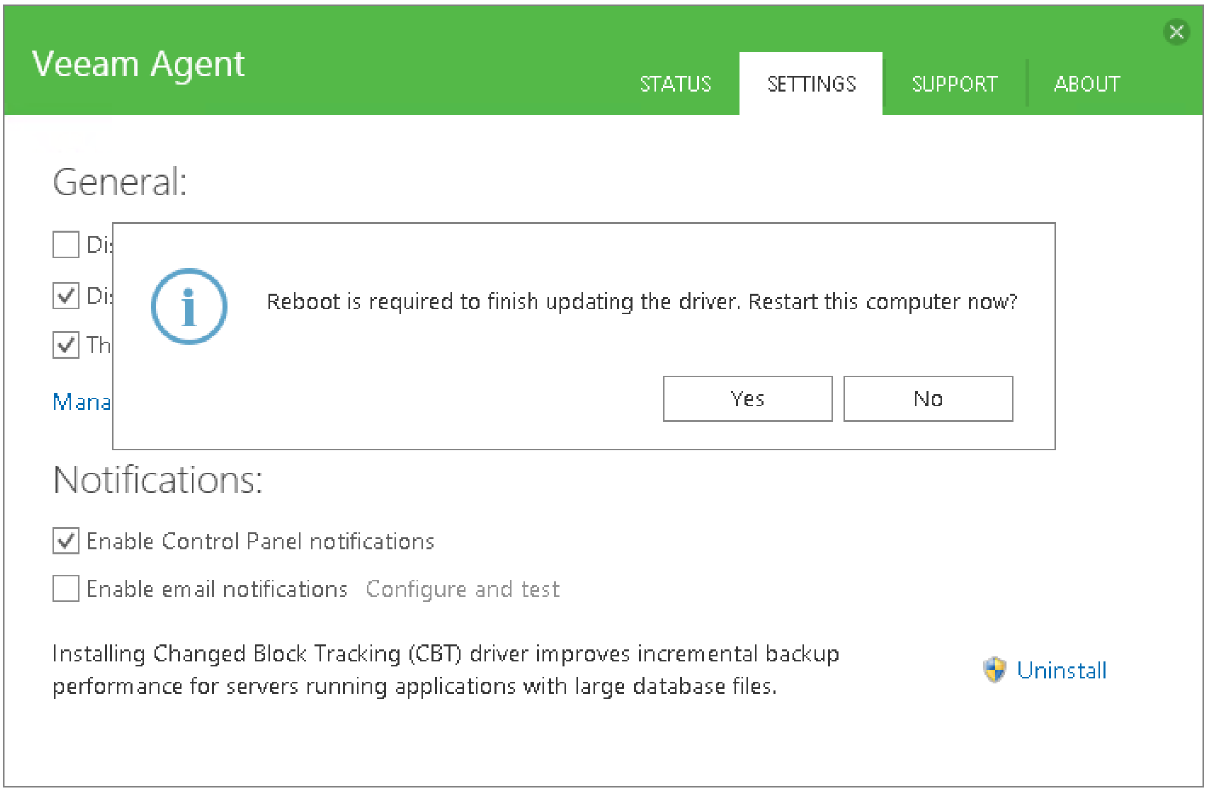
To remove the Veeam CBT driver:

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. At the top of the window, click the **Settings** tab.
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 **OK**. 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 **OK**.



General:

□ Di

☑ Di

☑ Th

Mana

Reboot is required to finish updating the driver. Restart this computer now?

Notifications:

☑ Enable Control Panel notifications

□ Enable email notifications Configure and test

Installing Changed Block Tracking (CBT) driver improves incremental backup performance for servers running applications with large database files.

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%` is a mount point of the volume, for example: `C:\`.
  - `%volumeUUID%` is an 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 volume(s).

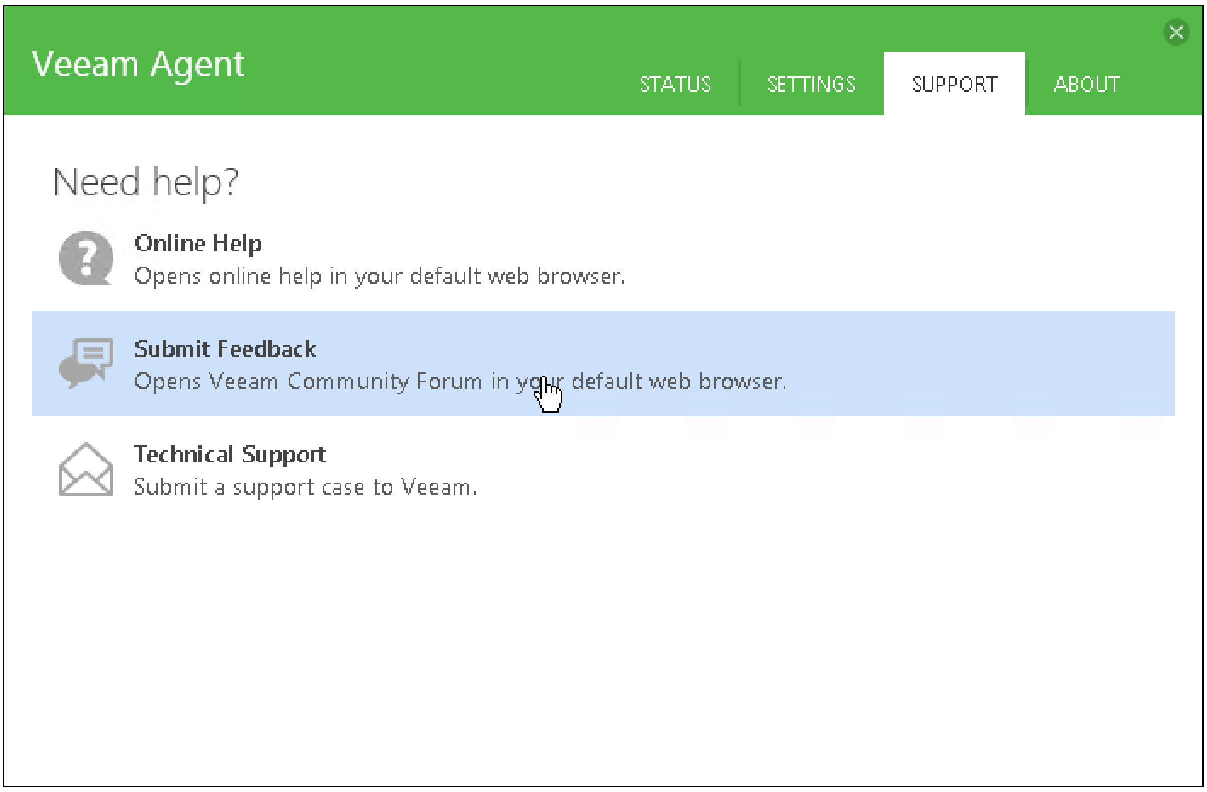
Getting Support

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

- You can open online help for Veeam Agent for Microsoft Windows.
- You can visit Veeam Community Forums at https://forums.veeam.com and share your opinion or ask a question.
- You can submit a support case to the Veeam Support Team directly from the product. To learn more, see Reporting Issues.

To access help and support options in Veeam Agent for Microsoft Windows:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. Click the **Support** link at the top of the window.
3. Click one of available options to get support on the product.



Need help?

Online Help
Opens online help in your default web browser.

Submit Feedback
Opens Veeam Community Forum in your default web browser.

Technical Support
Submit a support case to Veeam.

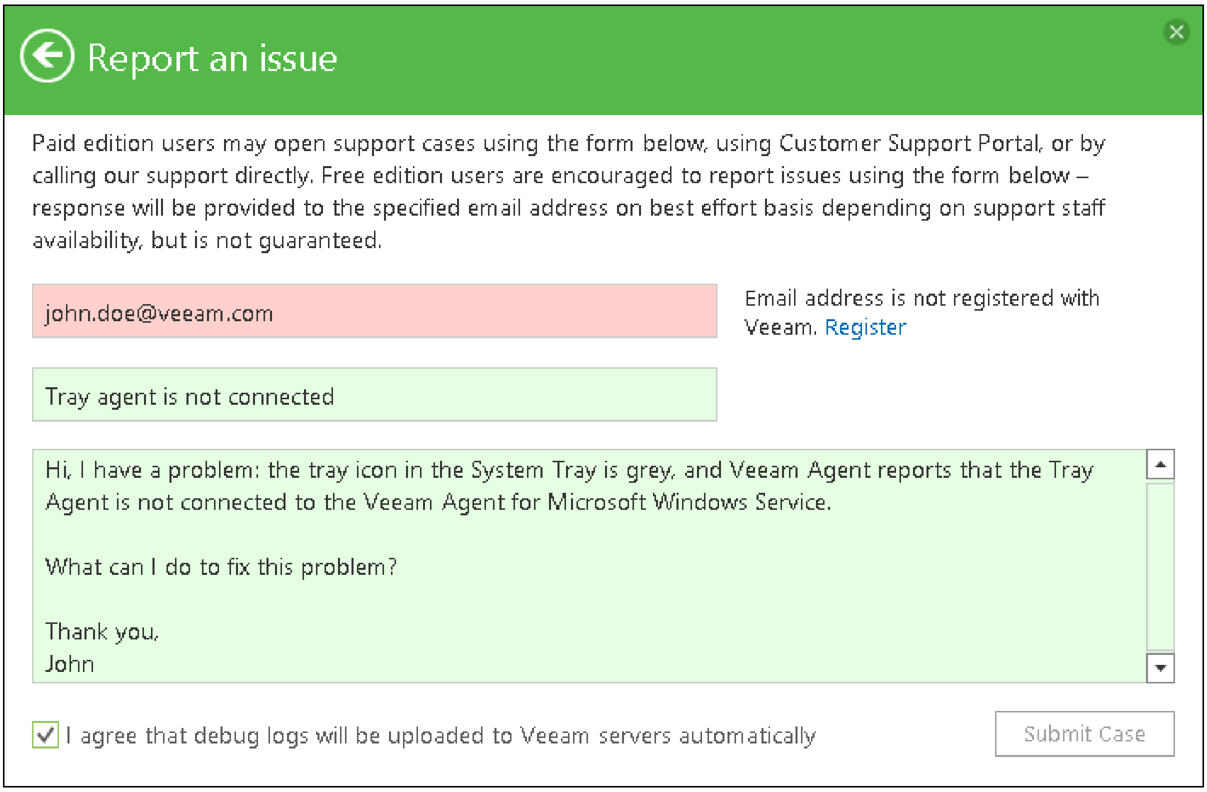
Reporting Issues

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. Click the **Support** tab.
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 Center 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 for Microsoft Windows will automatically collect logs from your computer (without additional warnings) and open a support case at the Veeam Customer Center Portal.



Report an issue

Paid edition users may open support cases using the form below, using Customer Support Portal, or by calling our support directly. 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.doe@veeam.com

Email address is not registered with Veeam. Register

Tray agent is not connected

Hi, I have a problem: the tray icon in the System Tray is grey, 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

IMPORTANT!

Mind the following:

- If you have any questions about the product functionality, do not submit a support case via the Veeam Customer Center Portal and do not send an email to the Veeam Support Team 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 for Microsoft Windows. If you use older version of Veeam Agent for Microsoft Windows, upgrade Veeam Agent for Microsoft Windows and check whether the problem still exists in the current version. If the problem exists, use the Control Panel to submit a support case.

Using with Veeam Backup & Replication

If you have the Veeam backup infrastructure deployed in the production environment, you can use Veeam Agent for Microsoft Windows together with Veeam Backup & Replication.

> **IMPORTANT!**
>
> If you plan to use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install Veeam Backup & Replication 9.5 Update 3 or later on the Veeam backup server.

Supported Product Editions

When you use Veeam Agent for Microsoft Windows together with Veeam Backup & Replication, available functionality depends on what product editions you have in the production environment. Supported product editions and available tasks are listed in the table below:

Veeam Backup & Replication License/Edition	Veeam Agent License/Edition	Automated Deployment*	Backup to Veeam backup repository
Free	Free	No	No
Free	Paid	No	Yes, with advanced functionality (Veeam Agent license must be installed in Veeam Backup & Replication, and Veeam Backup & Replication must be in the full functionality mode)
Paid	Free	No	Yes, without advanced functionality
Paid	Paid	No	Yes, with advanced functionality (Veeam Agent license must be installed in Veeam Backup & Replication, and Veeam Backup & Replication must be in the full functionality mode)

* The subsequent sections describe tasks with Veeam Backup & Replication available for Veeam Agent for Microsoft Windows operating in the standalone mode. Automated Veeam Agent deployment is available as a part of the Veeam Agent management scenario only. For information about Veeam Agent management in Veeam Backup & Replication, see the Veeam Agent Management Guide at: https://www.veeam.com/documentation-guides-datasheets.html.

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:

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 files and folders from Veeam Agent backups
- Restore application items from Veeam Agent backups
- Restore disks from Veeam Agent backups
- Restore data from Veeam Agent backups to Microsoft Azure

Administrative tasks

- Import Veeam Agent backups
- Enable and disable Veeam Agent backup jobs
- Delete Veeam Agent backup jobs
- Remove Veeam Agent backups
- View Veeam Agent backup statistics
- Configure global settings
- Assign roles to users

Setting Up User Permissions on Backup Repositories

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

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

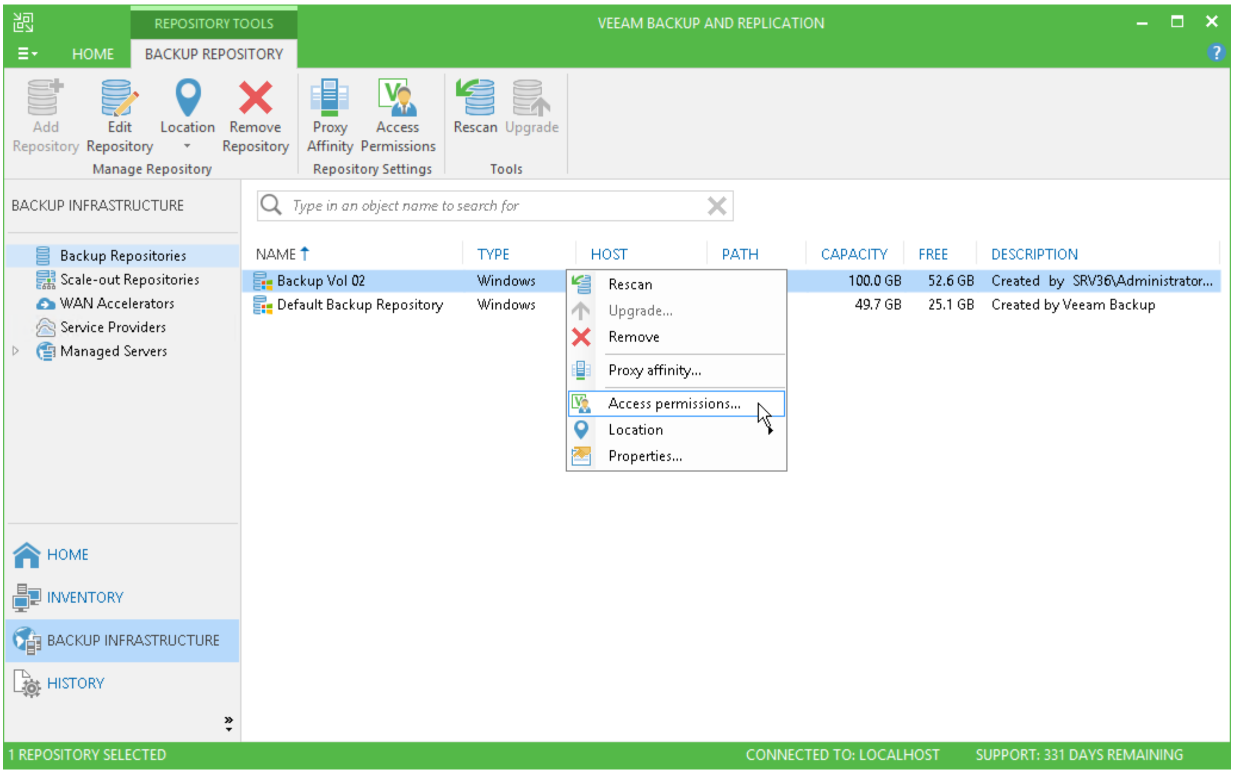
> **NOTE:**
>
> If you plan to create backups on a Veeam backup repository with Veeam Agent backup jobs configured in Veeam Backup & Replication, you do not need to grant access permissions on the backup repository to users. In the Veeam Agent management scenario, to establish a connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. To learn more, see the *Configuring Security Settings* section in the Veeam Agent Management Guide at: https://www.veeam.com/documentation-guides-datasheets.html.

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

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 **Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**. If you do not see the **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**.



NAME ↑	TYPE	HOST	PATH	CAPACITY	FREE	DESCRIPTION
Backup Vol 02	Windows			100.0 GB	52.6 GB	Created by SRV36\Administrator...
Default Backup Repository	Windows			49.7 GB	25.1 GB	Created by Veeam Backup

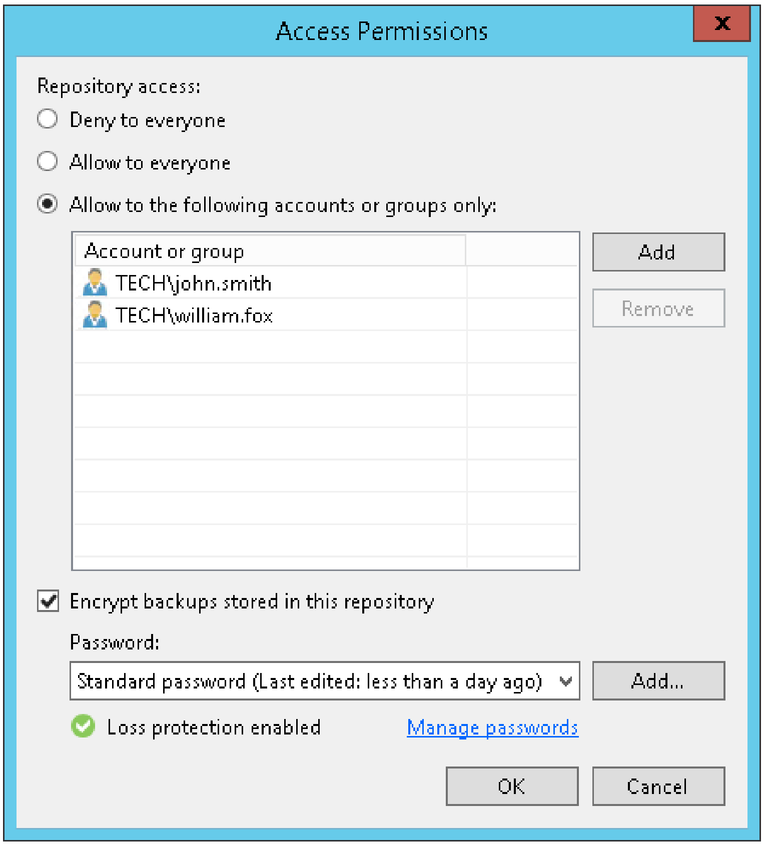
4. In the **Access Permissions** window, specify to whom you want to grant access permissions on this backup repository:

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

5. If you want to encrypt Veeam Agent backup files stored on the backup repository, select the **Encrypt backups stored on 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 for Microsoft Windows is set up to use the backup cache, and the backup cache contains one or more restore points, Veeam Agent for Microsoft Windows will automatically remove these restore points from the backup cache after you enable or disable the encryption option for the backup repository.



Repository access:

○ Deny to everyone

○ Allow to everyone

● Allow to the following accounts or groups only:

Account or group
TECH\john.smith
TECH\william.fox

☑ Encrypt backups stored in this repository

Password: Standard password (Last edited: less than a day ago)

Loss protection enabled

Managing Veeam Agent License

If you plan to use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install a Veeam Agent for Microsoft Windows license in Veeam Backup & Replication. In this case, you need to manage product licenses and functionality modes from the Veeam Backup & Replication console or Veeam Backup Enterprise Manager. This scenario may be suitable for customers who have Veeam backup infrastructure deployed in their environment and want to manage licenses for all Veeam products at one place.

> **NOTE:**
>
> In addition to managing Veeam Agent for Microsoft Windows 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 Veeam Agent licenses and perform restore tasks with Veeam Agent backups. You cannot manage Veeam Agent backup jobs with Veeam Backup Enterprise Manager.

You must obtain a license for the total number of machines on which you plan to install Veeam Agent for Microsoft Windows. Machines that run Microsoft Windows OSes intended for servers and workstations are tracked separately in the license.

After Veeam Agent for Microsoft Windows connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. If the license supports both the workstation and server editions of Veeam Agent for Microsoft Windows, the product edition is selected depending on the type of the Microsoft Windows OS running on the protected computer. You can switch to another commercial edition of Veeam Agent for Microsoft Windows manually if needed.

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

> **NOTE:**
>
> If you have been using Veeam Endpoint Backup FREE with Veeam Backup & Replication, after you install the Veeam Agent for Microsoft Windows license in Veeam Backup & Replication, Veeam Endpoint Backup FREE will become unable to connect to the Veeam backup server and create backups the Veeam backup repository.

Veeam Agent for Microsoft Windows keeps information about the license in its database. Information about the license is valid for 32 days. If Veeam Agent for Microsoft Windows does not connect to Veeam Backup & Replication during this period, Veeam Backup & Replication will revoke its license.

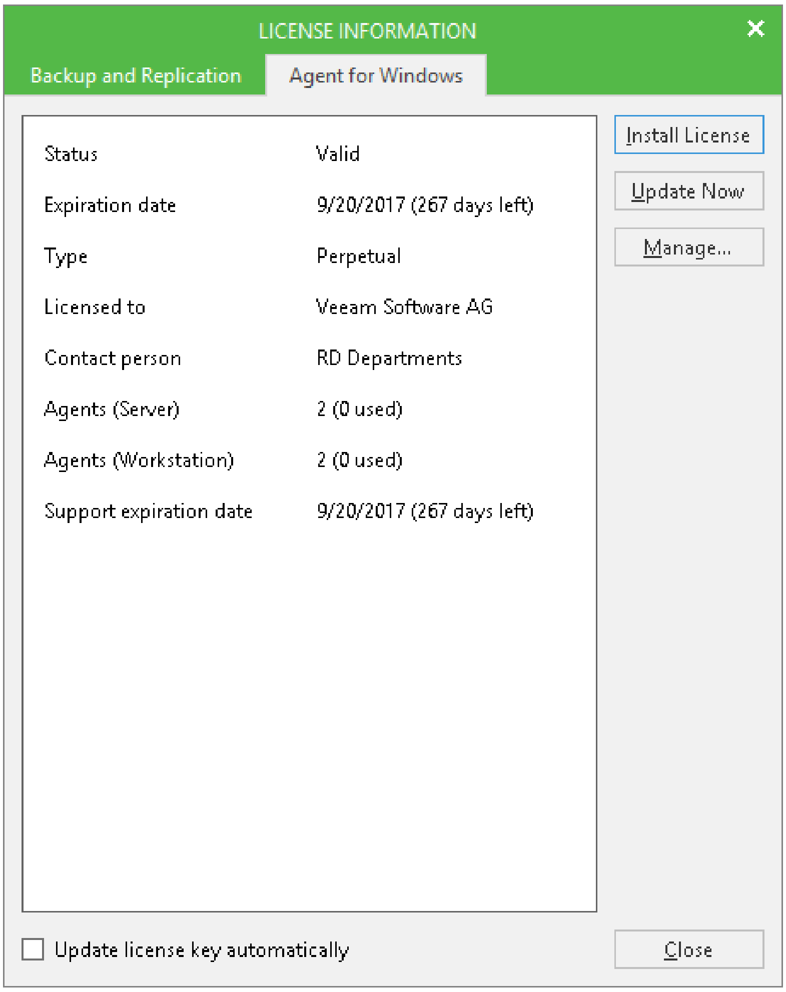
Installing License

You can install a Veeam Agent license in Veeam Backup & Replication. In this case, you will be able to manage product licenses and functionality modes from the Veeam Backup & Replication console.

To install a license:

1. In Veeam Backup & Replication, from the main menu, select **License**.
2. Click **Install License** and browse to the LIC file.
3. Veeam Backup & Replication will display a window notifying that Veeam Agents that are already connected to the backup server will start consuming the license. Click **Yes** to continue the installation process.

4. After the license is installed, information about the license will become available in the **Agent for Windows** tab of the **License Information** window.



Status	Valid
Expiration date	9/20/2017 (267 days left)
Type	Perpetual
Licensed to	Veeam Software AG
Contact person	RD Departments
Agents (Server)	2 (0 used)
Agents (Workstation)	2 (0 used)
Support expiration date	9/20/2017 (267 days left)

□ Update license key automatically

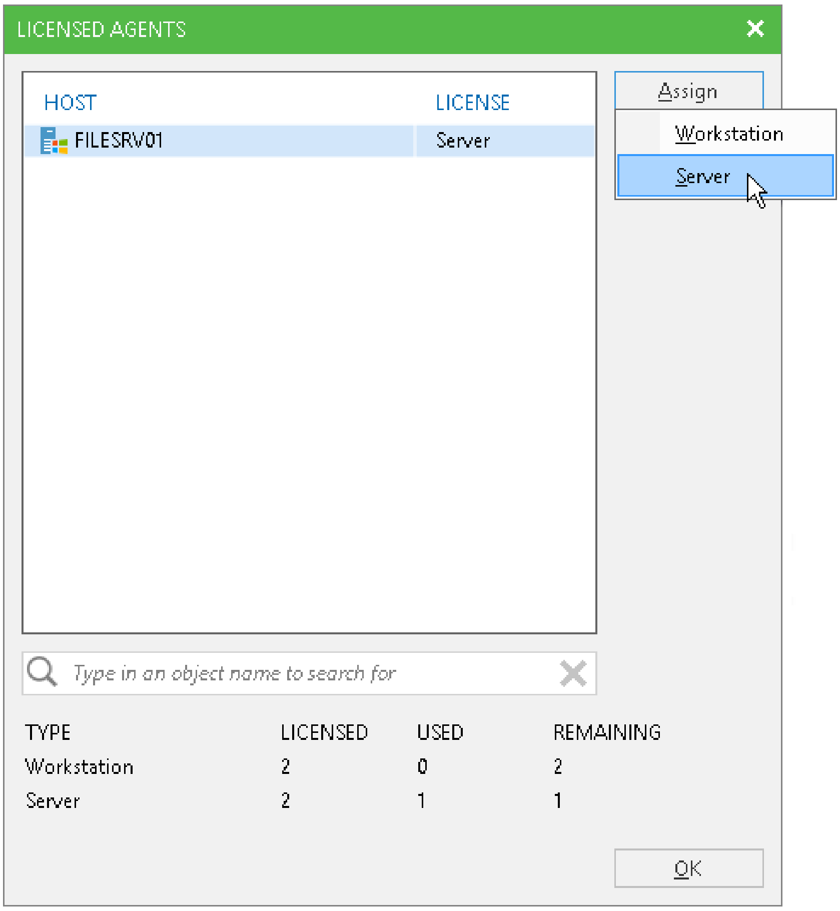
Assigning License to Veeam Agent

After Veeam Agent for Microsoft Windows connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. If the license supports both the workstation and server editions of Veeam Agent for Microsoft Windows, the product edition will be selected depending on the type of the Microsoft Windows OS running on the protected computer.

You can also assign a license to Veeam Agent for Microsoft Windows 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 **Agent for Windows** tab and click **Manage**.
3. In the **Licensed Agents** window, select the Veeam Agent to which you want to assign the license, click **Assign** and select the desired product edition: *Workstation* or *Server*.



HOST	LICENSE
FILESRV01	Server

TYPE	LICENSED	USED	REMAINING
Workstation	2	0	2
Server	2	1	1

Viewing Licensed Agents and Revoking License

When Veeam Agent for Microsoft Windows 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 **Agent for Windows** tab and click **Manage**.

If no Veeam Agents are connected to the backup server after you have installed a Veeam Agent license, the list is empty. After you run Veeam Agent backup jobs, the list will include Veeam Agents that have established a connection with the backup server.

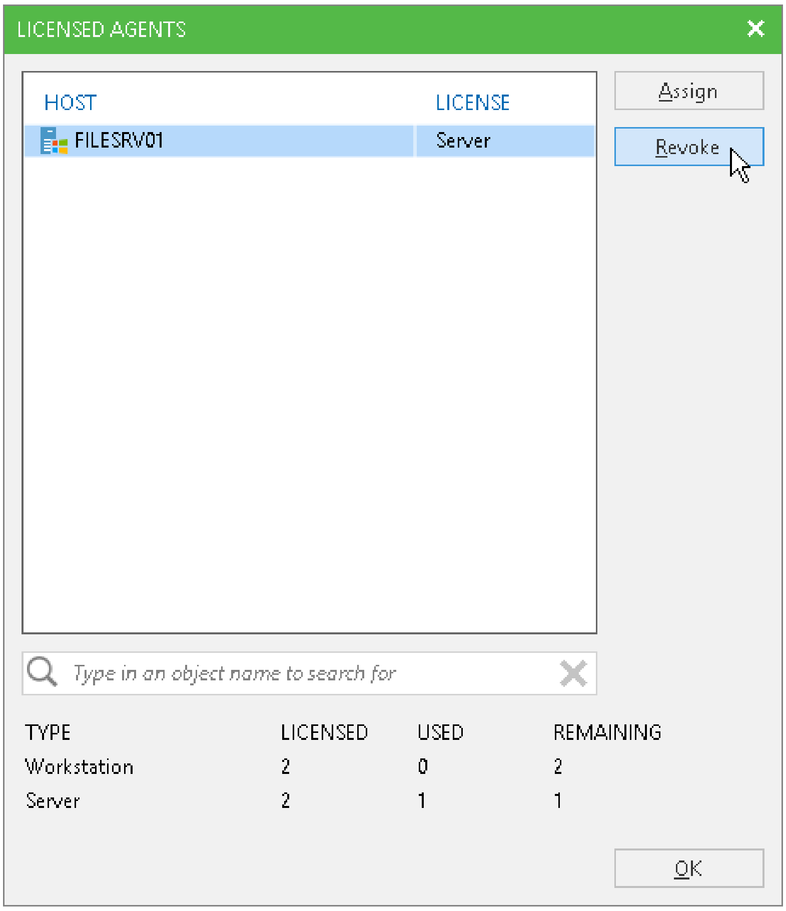
Revoking License from Veeam Agents

You can revoke the license from some Veeam Agents and re-apply it to other Veeam Agents. 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 **Agent for Windows** tab and click **Manage**.
3. In the **Licensed Agents** 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 Veeam Agents in the backup infrastructure.

   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 Agents** 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.



HOST	LICENSE
FILESRV01	Server

TYPE	LICENSED	USED	REMAINING
Workstation	2	0	2
Server	2	1	1

Performing Data Protection Tasks

You can perform the following data protection tasks:

- Back up your data and store the resulting backup files on one of the following types of Veeam backup repositories:
  - On a backup repository managed by a Veeam backup server
  - On 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 for Microsoft Windows on 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.

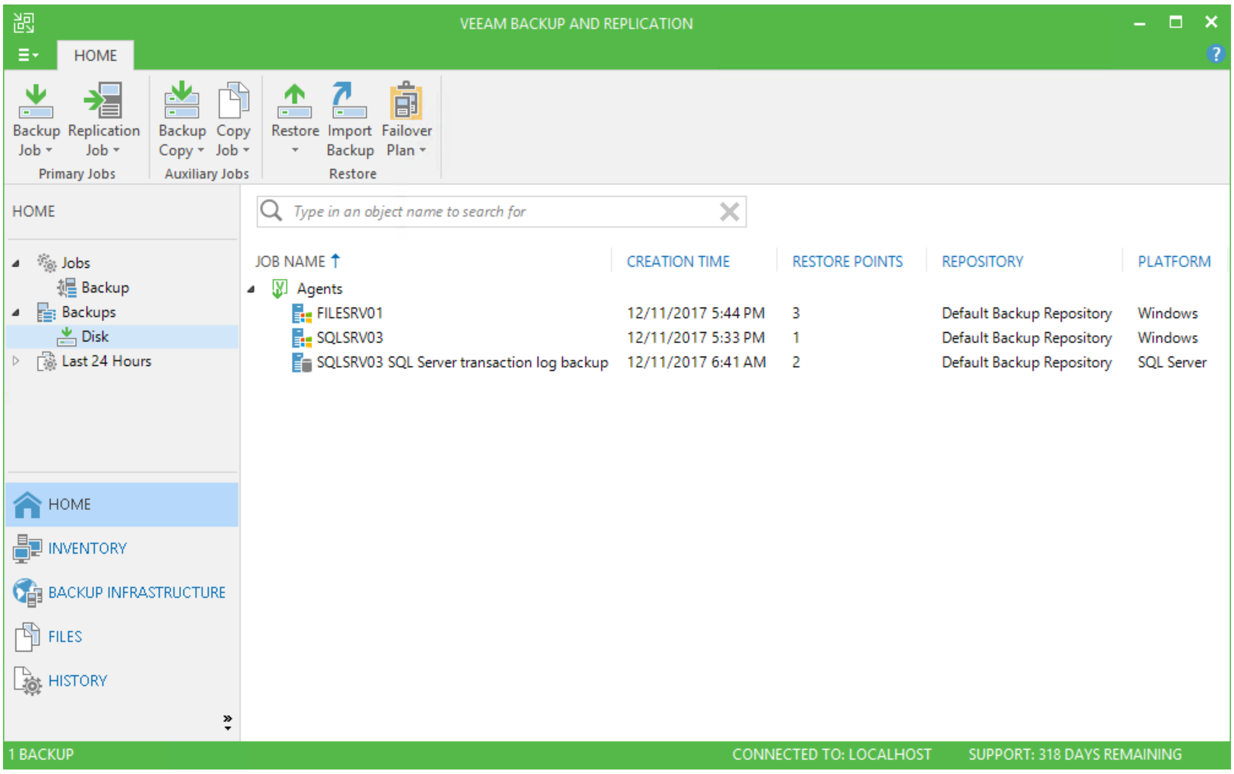
> **NOTE:**
>
> A Veeam Agent backup job can be started automatically upon the defined schedule or manually from the Veeam Agent computer. You cannot start, stop, retry or edit Veeam Agent backup jobs in the Veeam Backup & Replication console.

The user who creates a Veeam Agent backup on the backup repository is set as the owner of the backup file. Only the backup file owner can access this file and restore data from it. Other users cannot see backups created by the backup file owner.

> **NOTE:**
>
> If the user is granted restore permissions on the Veeam backup server, the user will be able to see all backups on the backup repository.

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 for Microsoft Windows are available under the **Backups** > **Disk** node in the **Home** view.

The backup administrator working with Veeam Backup & Replication can manage Veeam Agent backup jobs and restore data from Veeam Agent backups. To learn more, see Performing Restore Tasks and Performing Administration Tasks.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01	12/11/2017 5:44 PM	3	Default Backup Repository	Windows
SQLSRV03	12/11/2017 5:33 PM	1	Default Backup Repository	Windows
SQLSRV03 SQL Server transaction log backup	12/11/2017 6:41 AM	2	Default Backup Repository	SQL Server

Backing Up to Cloud Repositories

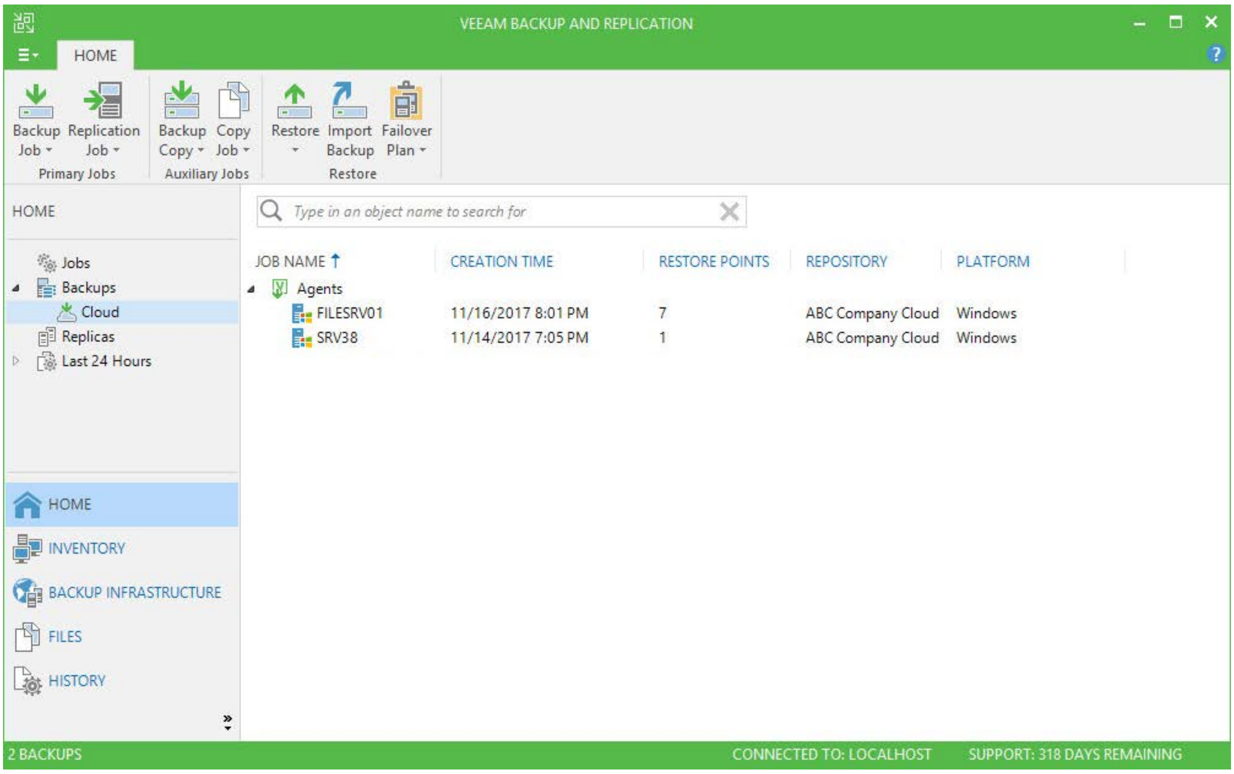
You can store backups created with Veeam Agent for Microsoft Windows on cloud repositories provided to you by a Veeam Cloud Connect service provider. To do this, you must connect to the service provider and point the backup job to the cloud repository. To learn more, see Specify Service Provider Settings.

Veeam Agent Backups on Tenant Side

Backups created with Veeam Agent for Microsoft Windows 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 on 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



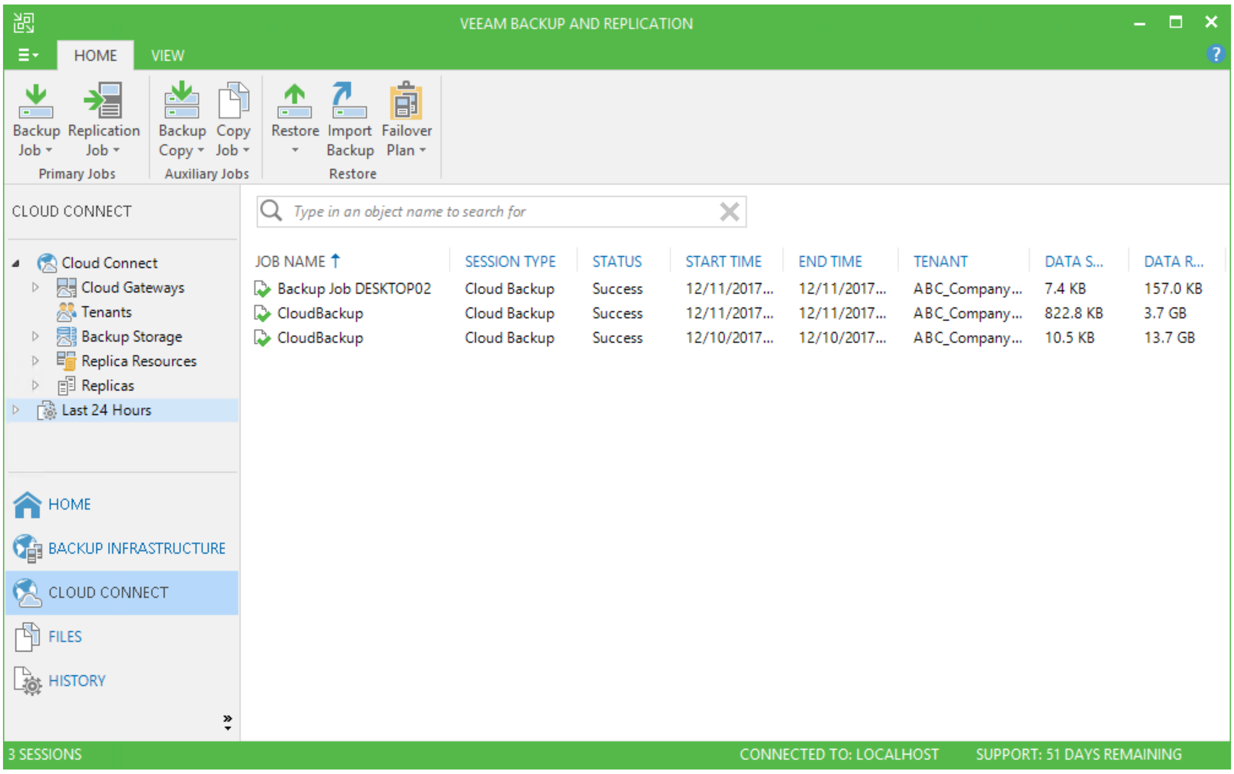
JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01	11/16/2017 8:01 PM	7	ABC Company Cloud	Windows
SRV38	11/14/2017 7:05 PM	1	ABC Company Cloud	Windows

2 BACKUPS   CONNECTED TO: LOCALHOST   SUPPORT: 318 DAYS REMAINING

Veeam Agent Backups on Service Provider Side

The service provider can view information about backup and restore sessions performed by Veeam Agent users within the last 24 hours period. The list of sessions is available under the **Last 24 hours** node in the **Cloud Connect** view of the Veeam Backup & Replication console deployed on the service provider side.

The service provider cannot perform restore tasks with Veeam Agent backups that are stored on the cloud repository.



JOB NAME	SESSION TYPE	STATUS	START TIME	END TIME	TENANT	DATA S...	DATA R...
Backup Job DESKTOP02	Cloud Backup	Success	12/11/2017...	12/11/2017...	ABC_Company...	7.4 KB	157.0 KB
CloudBackup	Cloud Backup	Success	12/11/2017...	12/11/2017...	ABC_Company...	822.8 KB	3.7 GB
CloudBackup	Cloud Backup	Success	12/10/2017...	12/10/2017...	ABC_Company...	10.5 KB	13.7 GB

Performing Backup Copy for Veeam Agent Backups

You can configure backup copy jobs that will copy backups created with Veeam Agent for Microsoft Windows to a secondary backup repository.

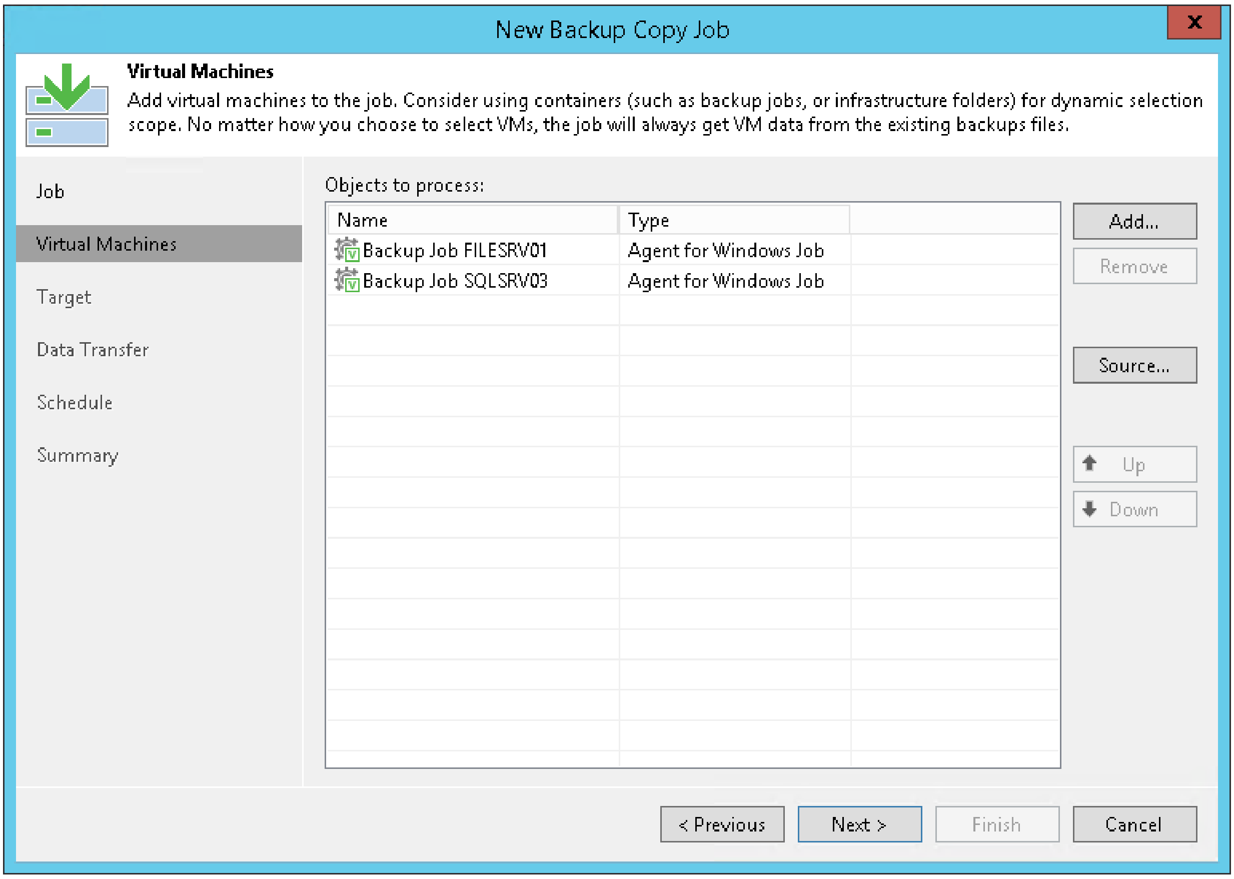
Backup copy jobs treat Veeam Agent backups as usual backup files. The backup copy job setup and processing procedures practically do not differ from the regular ones. To learn more about backup copy jobs, see Veeam Backup & Replication Documentation.

NOTE:

You can map a Veeam Agent backup copy job only to backups created by the following types of jobs:

- Veeam Agent backup copy job that processes backups created by Veeam Agent for Microsoft Windows operating in the standalone mode
- Veeam Agent backup job configured directly on a Veeam Agent Computer

You cannot map a backup copy job to a backup created by a Veeam Agent backup job configured in Veeam Backup & Replication.



New Backup Copy Job

Virtual Machines

Add virtual machines to the job. Consider using containers (such as backup jobs, or infrastructure folders) for dynamic selection scope. No matter how you choose to select VMs, the job will always get VM data from the existing backups files.

Objects to process:

Name	Type
Backup Job FILESRV01	Agent for Windows Job
Backup Job SQLSRV03	Agent for Windows Job

Restoring Data from Copies of Veeam Agent Backups

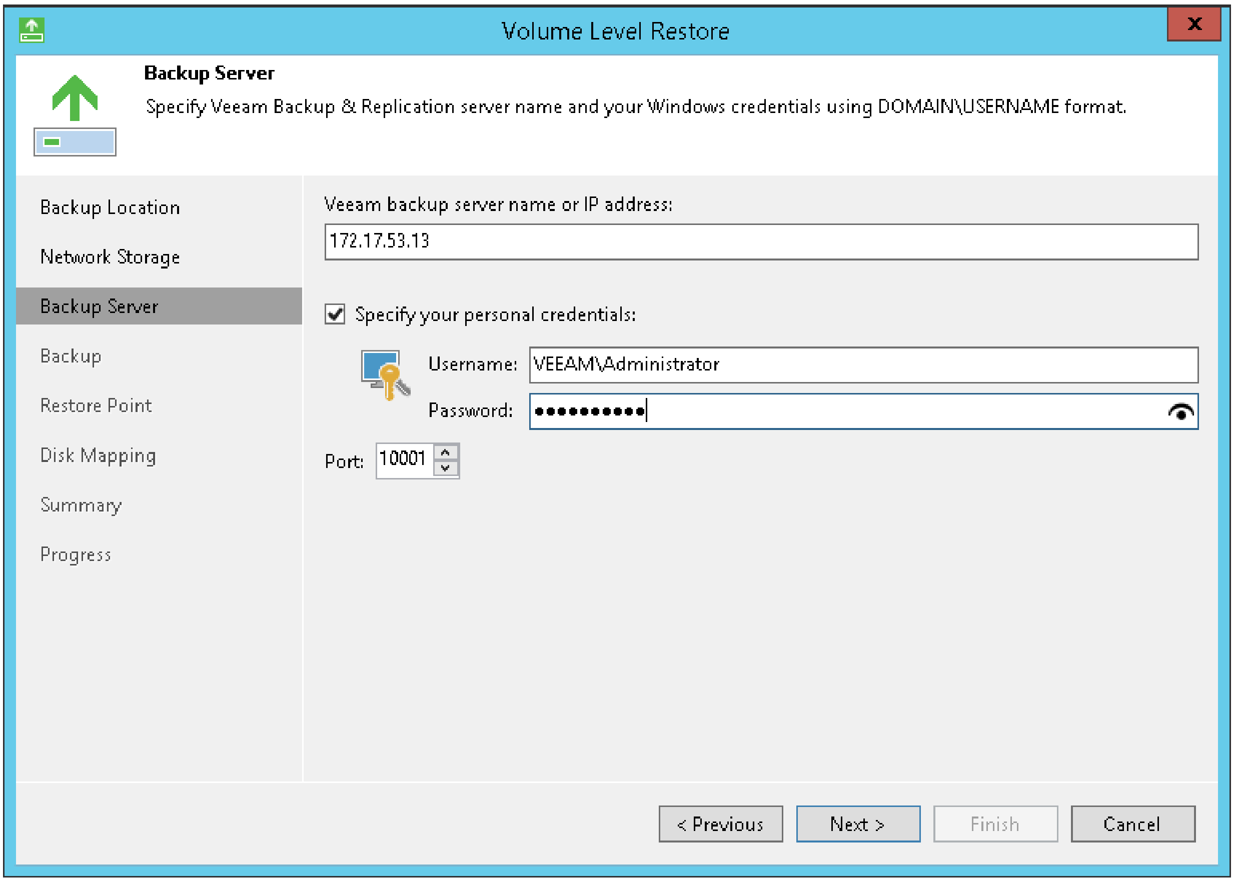
Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

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 on the target repository using Veeam Agent for Microsoft Windows.

To do this:

1. In Veeam Agent for Microsoft Windows, 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.



Volume Level Restore

Backup Server

Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.

Veeam backup server name or IP address: 172.17.53.13

☑ Specify your personal credentials:

Username: VEEAM\Administrator

Password: ●●●●●●●●●●

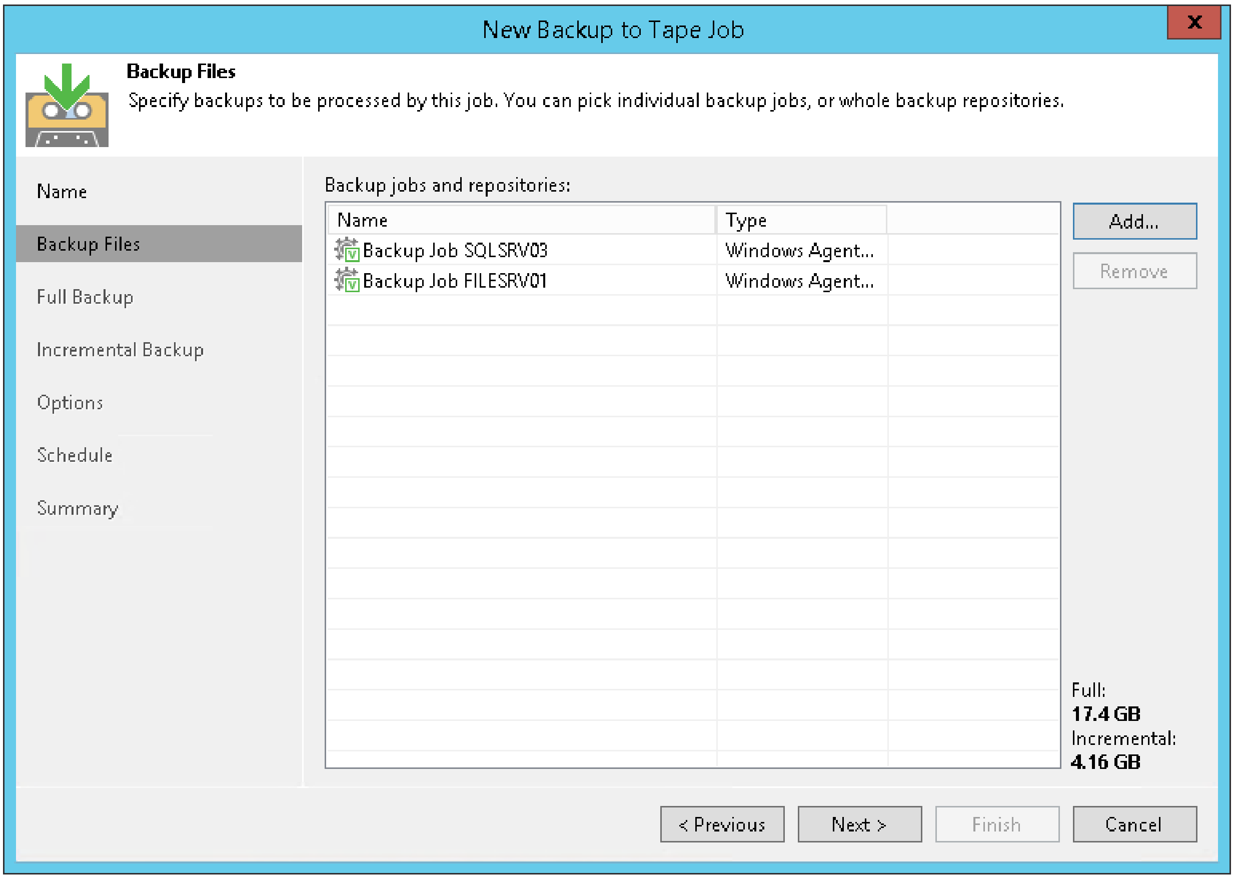
Port: 10001

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 Veeam Backup & Replication Documentation.

> **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.



Name	Type
Backup Job SQLSRV03	Windows Agent...
Backup Job FILESRV01	Windows Agent...

Full:
17.4 GB
Incremental:
4.16 GB

Performing Restore Tasks

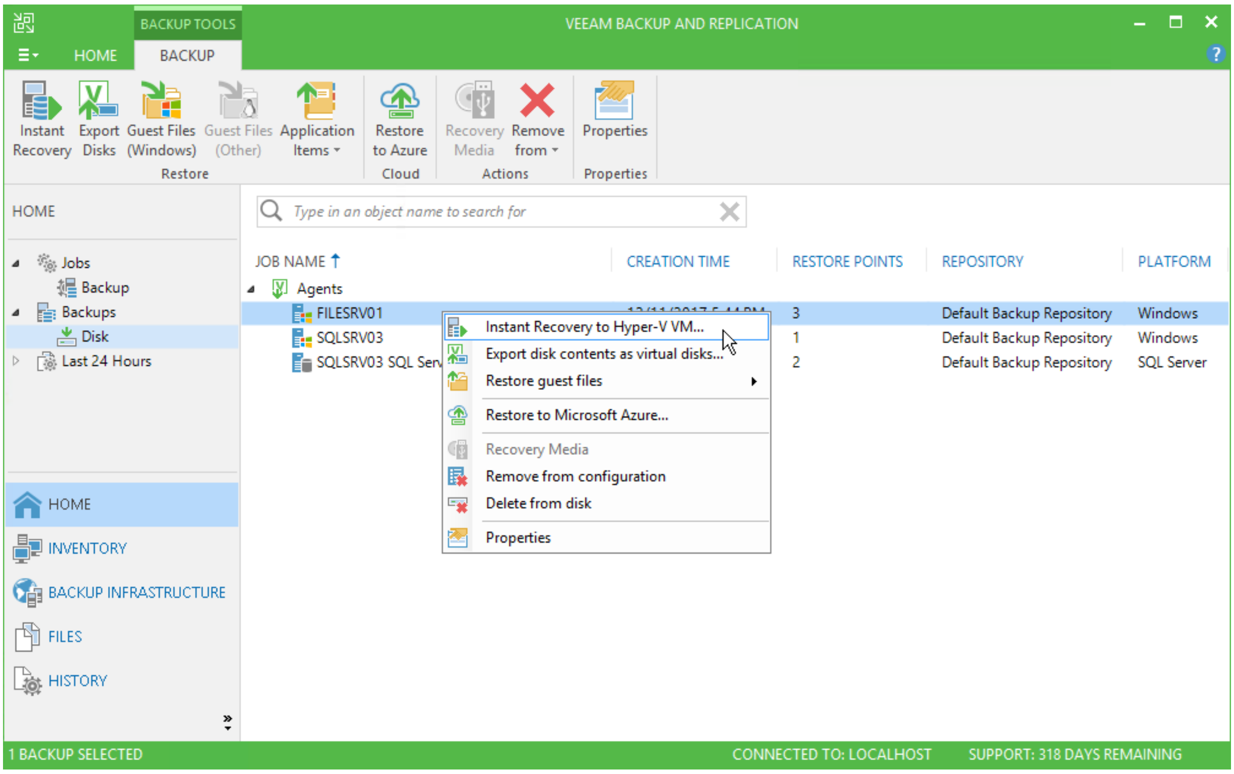
You can perform the following restore operations:

- Restore Veeam Agent backups to Hyper-V VMs
- 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
- Restore data from Veeam Agent backups to Microsoft Azure

Restoring Veeam Agent Backup to Hyper-V VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For instant recovery to a Hyper-V VM, you can use Veeam Agent backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

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 VM 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 about instant VM recovery, see the *Instant VM Recovery* section in the Veeam Backup & Replication User Guide at https://www.veeam.com/documentation-guides-datasheets.html.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01	12/11/2017 5:44 PM	3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Serv		2	Default Backup Repository	SQL Server

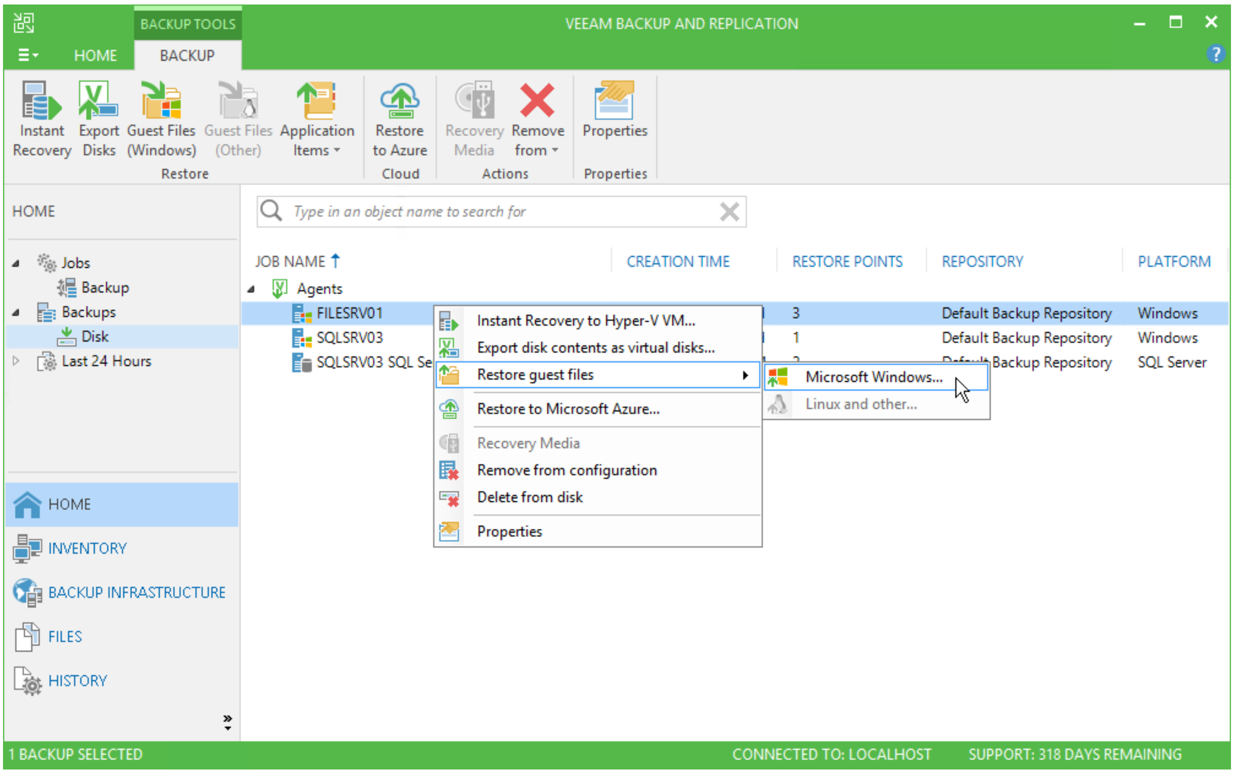
Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups. For file-level restore, you can use Veeam Agent backups created on the following types of target storage:

- Veeam backup repository
- Veeam Cloud Connect repository

For Veeam Agent backups created on the cloud repository, you can perform restore tasks in Veeam Backup & Replication deployed on the tenant backup server. The service provider cannot perform restore tasks with Veeam Agent backups.

The procedure of file-level restore practically does not differ from a regular one. To learn more about file-level restore, see Veeam Backup & Replication Documentation.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
FILESRV01		3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Se		2	Default Backup Repository	SQL Server

Restoring Application Items

You can use Veeam Explorers to restore application items from backups created with 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

For backups created by Veeam Agent backup jobs with guest processing options enabled, the procedure of application-item restore does not differ from the regular one. To learn more about the application-item restore procedure, see Veeam Backup & Replication Documentation.

Exporting Disks

You can restore computer disks from volume-level backups and convert them to disks of the VMDK, VHD or VHDX format.

During disks restore, Veeam Agent for Microsoft Windows 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 Agent for Microsoft Windows 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 Agent for Microsoft Windows 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 ESX(i) 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 format.

VHD/VHDX disks are always restored as dynamically expanding.

Veeam Agent for Microsoft Windows supports batch disk restore. For example, if you choose to restore 2 computer disks, Veeam Agent for Microsoft Windows will convert them to 2 virtual disks and store these disks in the specified location.

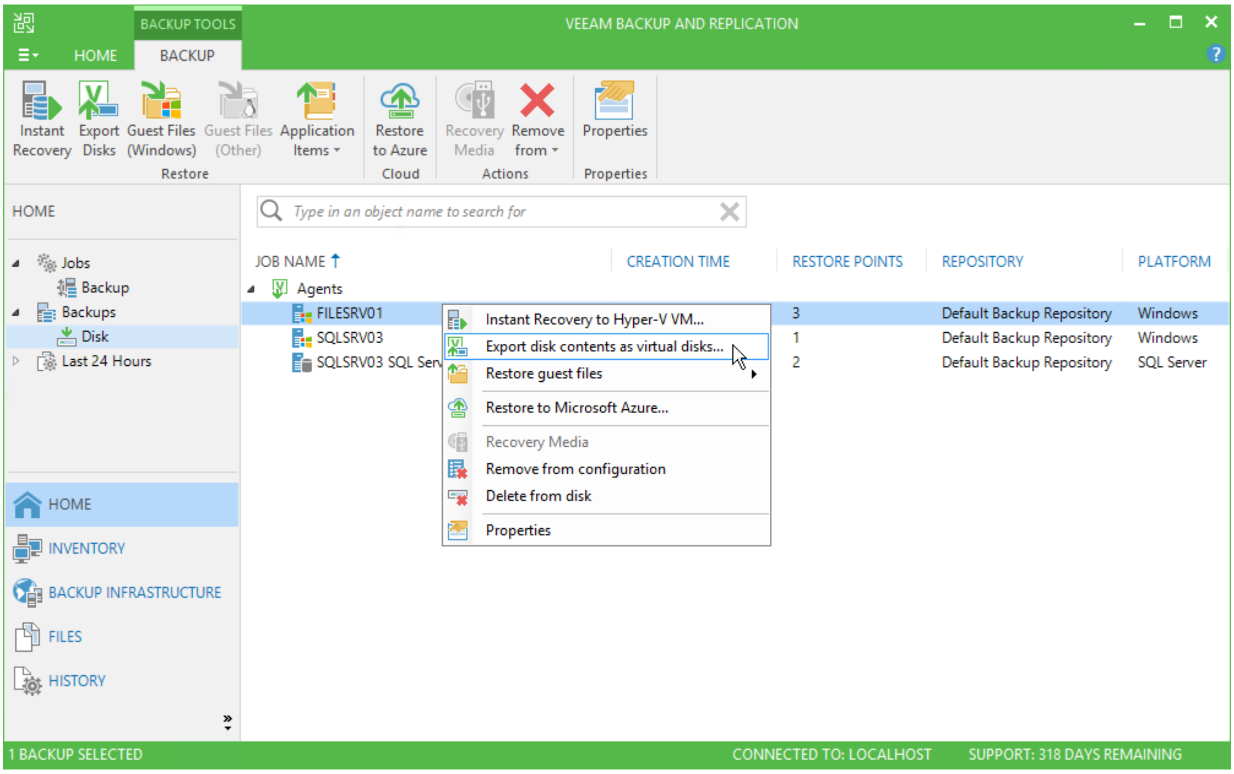
To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

- In Veeam Backup & Replication, open the Home tab and click **Restore** > **Agents** > **Export disk contents as virtual disks**. In this case, you will be able to select the necessary Veeam Agent backup at the Backup step of the wizard.
- In Veeam Backup & Replication, open the **Home** view. Then do the following:
    - [For backups stored on a regular backup repository] In the inventory pane, click **Disk** under the **Backups** node. In the working area, expand the **Agents** node, right-click the necessary backup and select **Export disk contents as virtual disks**.
    - [For backups stored on a cloud repository] In the inventory pane, click **Cloud** under the **Backups** node. In the working area, expand the **Agents** node, right-click the necessary backup and select **Export disk contents as virtual disks**.

  In this case, you will pass immediately to the Restore Point step of the wizard.



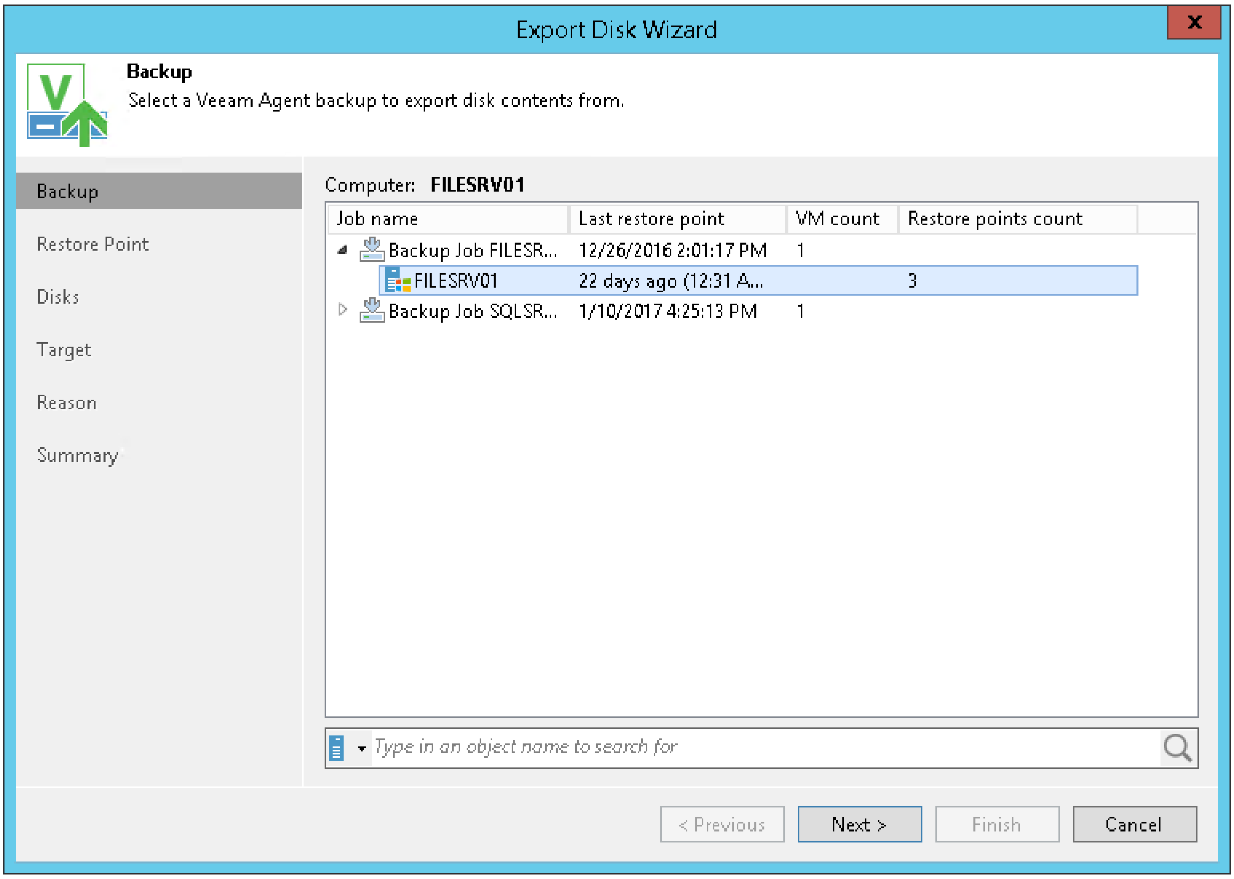
JOB NAME ↑	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
FILESRV01		3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Serv		2	Default Backup Repository	SQL Server

Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to restore disk(s). In the list of backups, Veeam Agent for Microsoft Windows displays all backups that are currently hosted on the on the following types of target storage:

- Veeam backup repository
- Veeam Cloud Connect repository

Make sure that you select a volume-level backup in the list.



Export Disk Wizard

Backup

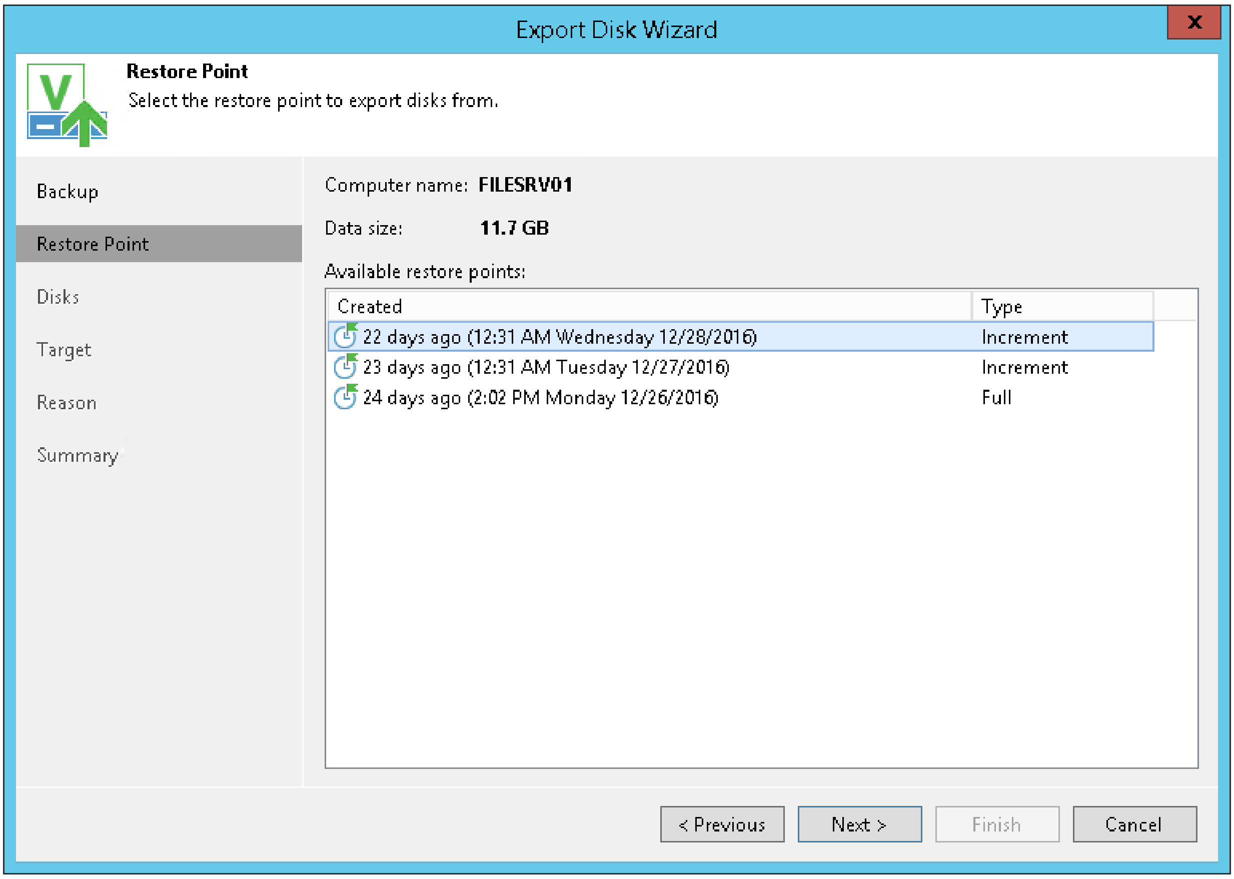
Select a Veeam Agent backup to export disk contents from.

Computer: **FILESRV01**

Job name	Last restore point	VM count	Restore points count
Backup Job FILESR...	12/26/2016 2:01:17 PM	1	
FILESRV01	22 days ago (12:31 A...		3
Backup Job SQLSR...	1/10/2017 4:25:13 PM	1	

Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disk(s). In the list of points, Veeam Agent for Microsoft Windows displays all restore points that have been created. Make sure that you select a restore point that relates to a volume-level backup.



Export Disk Wizard

Restore Point

Select the restore point to export disks from.

Computer name: **FILESRV01**

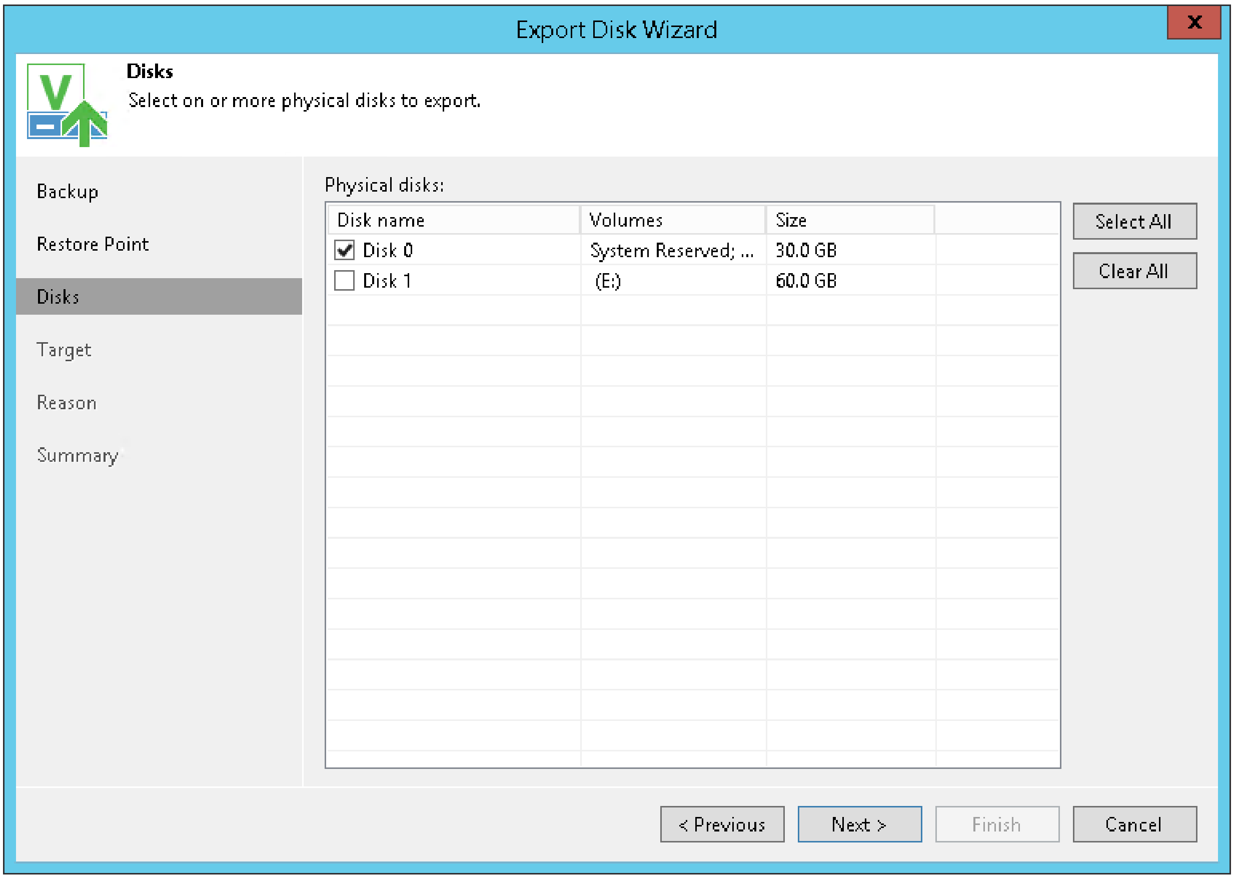
Data size: **11.7 GB**

Available restore points:

Created	Type
22 days ago (12:31 AM Wednesday 12/28/2016)	Increment
23 days ago (12:31 AM Tuesday 12/27/2016)	Increment
24 days ago (2:02 PM Monday 12/26/2016)	Full

Step 4. Select Disks

At the **Disks** step of the wizard, select check boxes next to those disks that you want to export.



Disk name	Volumes	Size
☑ Disk 0	System Reserved; ...	30.0 GB
□ Disk 1	(E:)	60.0 GB

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 ESX(i) 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:

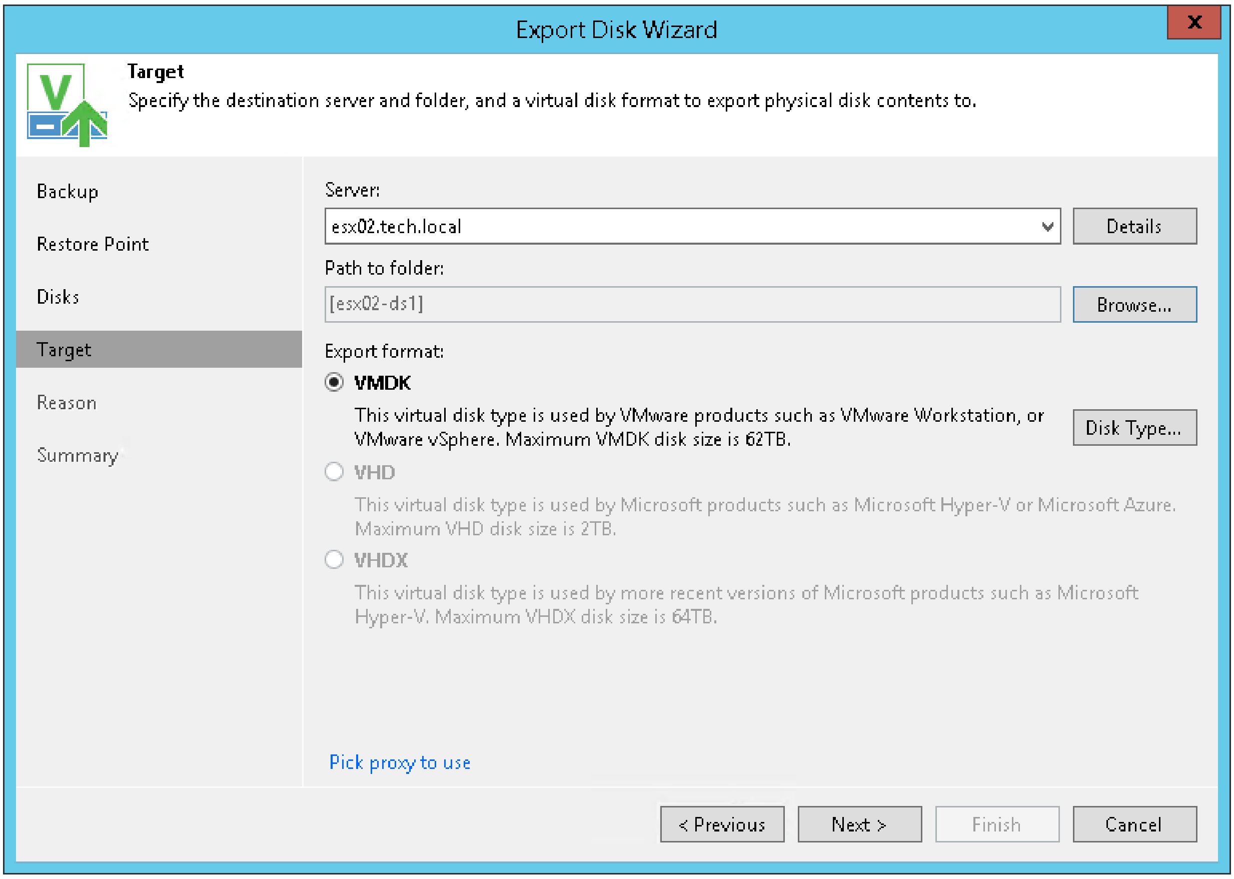
   - **VMDK** — select this option if you want to save the resulting virtual disk in the VMware VMDK format.

   - **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).

NOTE:

If you have selected to store the resulting virtual disk to a datastore, you will be able to save the virtual disk in the VMDK format only. Other options will be disabled.



Export Disk Wizard

Target

Specify the destination server and folder, and a virtual disk format to export physical disk contents to.

Server: esx02.tech.local

Path to folder: [esx02-ds1]

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.

○ VHD

This virtual disk type is used by Microsoft products such as Microsoft Hyper-V or Microsoft Azure. Maximum VHD disk size is 2TB.

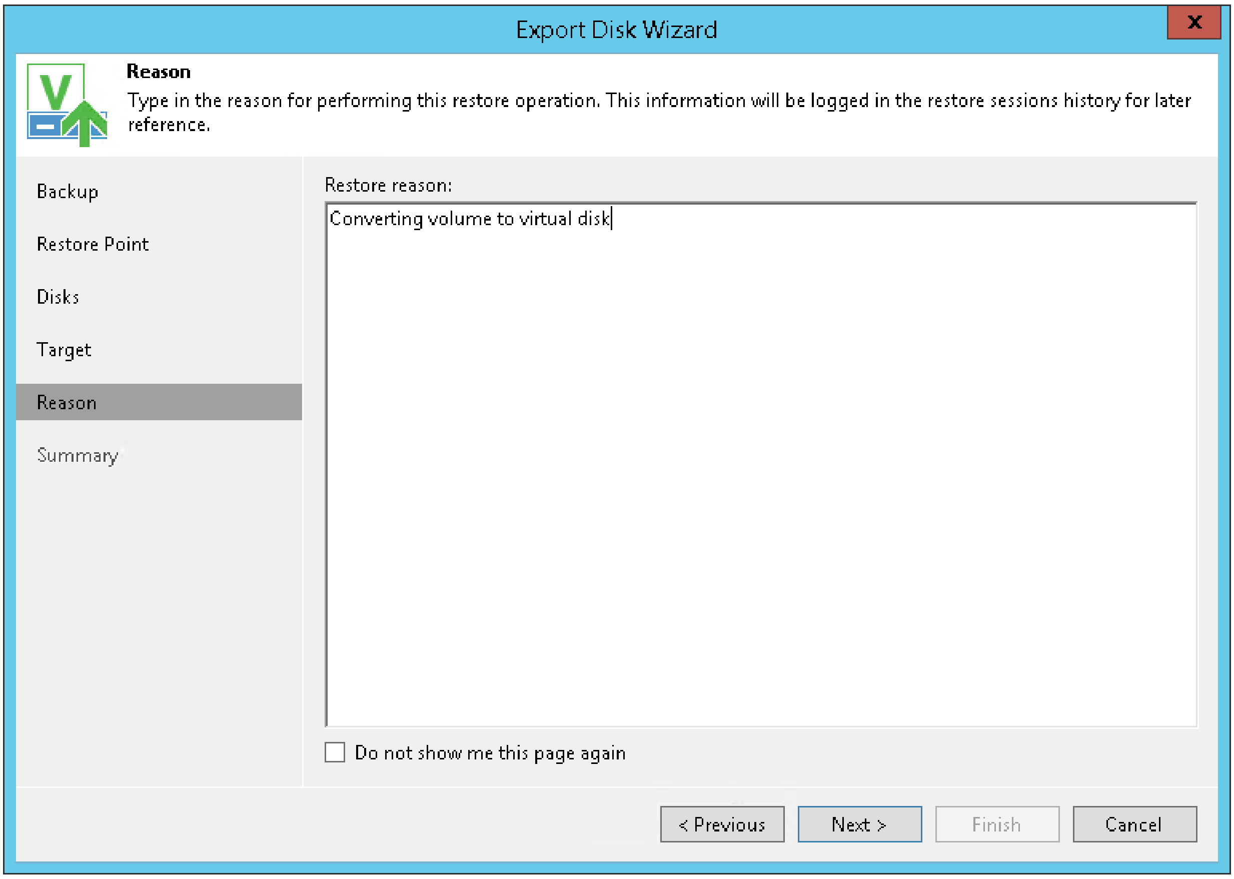
○ VHDX

This virtual disk type is used by more recent versions of Microsoft products such as Microsoft Hyper-V. Maximum VHDX disk size is 64TB.

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.



Export Disk Wizard

Reason

Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Restore reason:

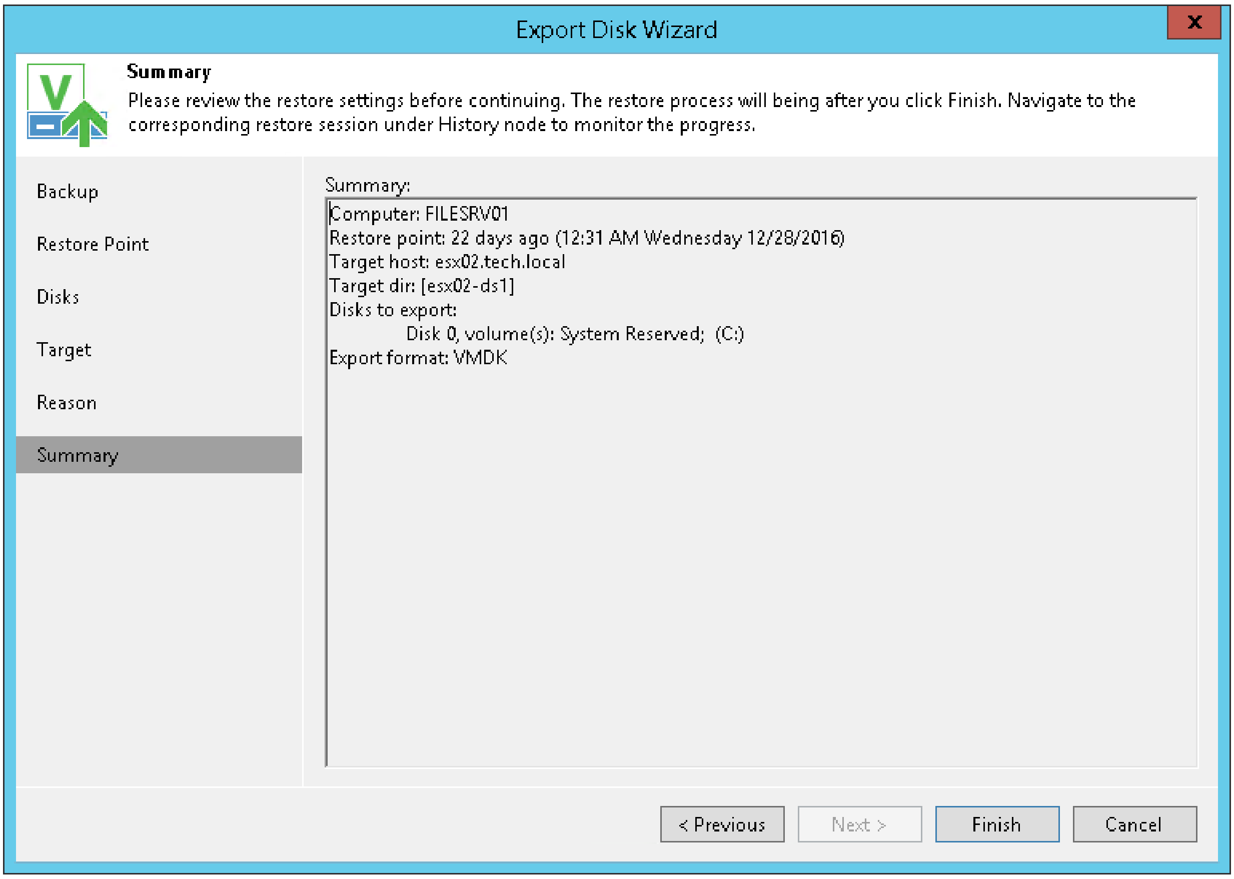
Converting volume to virtual disk

□ Do not show me this page again

Step 7. Complete Restore Process

At the **Summary** step of the wizard, complete the disk restore procedure.

1. Review details for the disk to be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.



Summary

Please review the restore settings before continuing. The restore process will being after you click Finish. Navigate to the corresponding restore session under History node to monitor the progress.

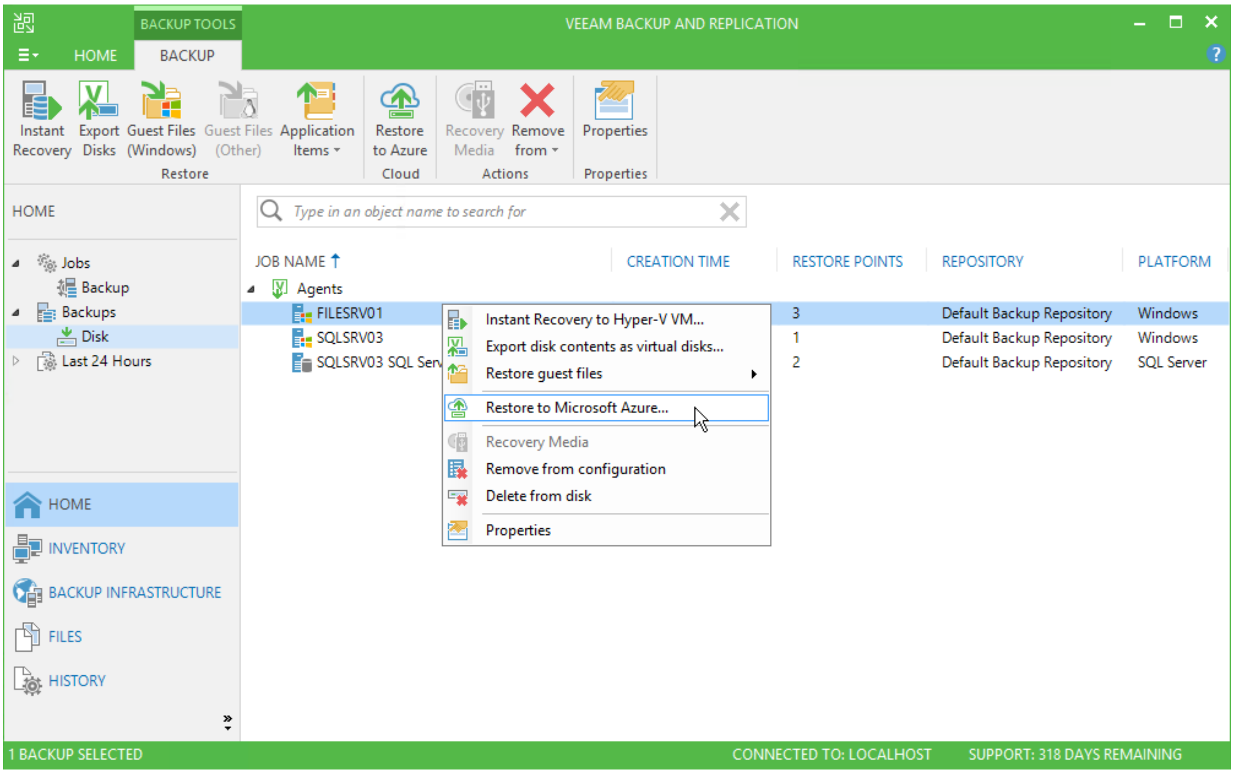
Summary:

```
Computer: FILESRV01
Restore point: 22 days ago (12:31 AM Wednesday 12/28/2016)
Target host: esx02.tech.local
Target dir: [esx02-ds1]
Disks to export:
        Disk 0, volume(s): System Reserved;  (C:)
Export format: VMDK
```

Restoring to Microsoft Azure

You can restore machines from backups created with Veeam Agent for Microsoft Windows to Microsoft Azure.

The procedure of restore to Microsoft Azure practically does not differ from a regular one. To learn more about restore to Microsoft Azure, see Veeam Backup & Replication Documentation.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01		3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Serv		2	Default Backup Repository	SQL Server

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
- Remove Veeam Agent backup jobs
- View Veeam Agent backup job statistics
- Remove Veeam Agent backups
- View Veeam Agent backup properties
- 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 on a backup repository managed by another Veeam backup server.
- The Veeam Agent backup has been removed in the Veeam Backup & Replication console.

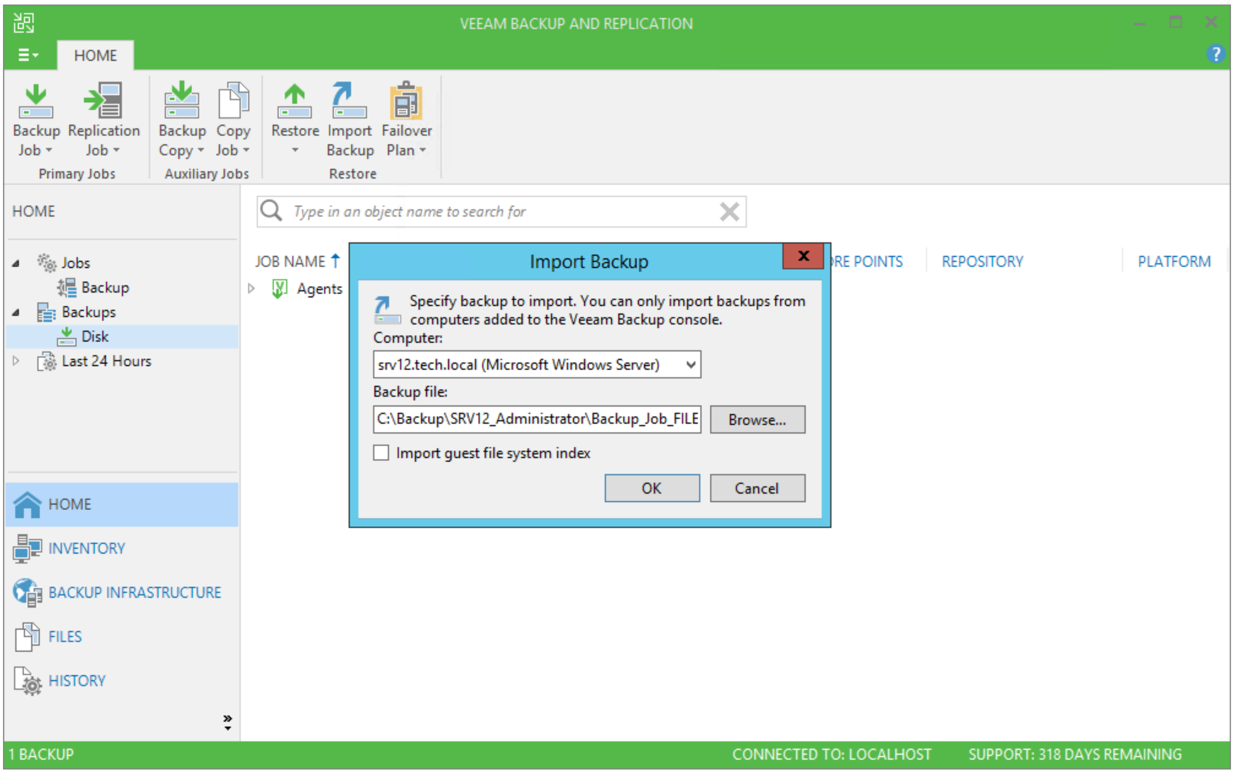
After importing, the Veeam Agent backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

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. It is recommended 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.



Specify backup to import. You can only import backups from computers added to the Veeam Backup console.

Computer: srv12.tech.local (Microsoft Windows Server)

Backup file: C:\Backup\SRV12_Administrator\Backup_Job_FILE

□ Import guest file system index

Importing Encrypted Backups

You can import Veeam Agent backups that were encrypted by Veeam Backup & Replication or Veeam Agent for Microsoft Windows.

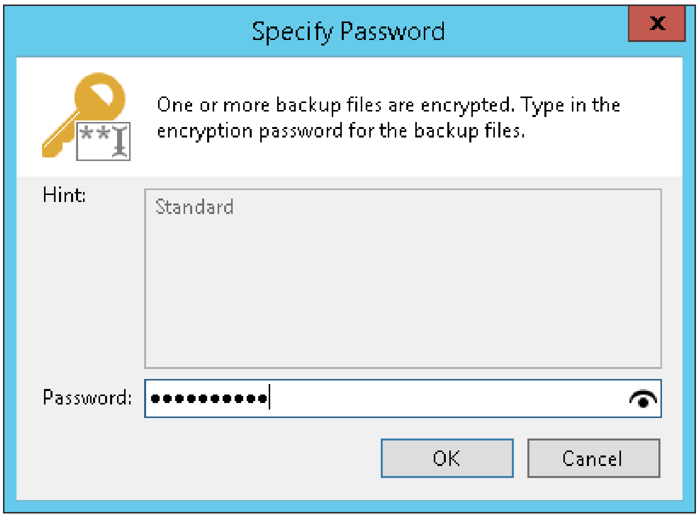
To import an encrypted backup file:

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.


Specify Password

One or more backup files are encrypted. Type in the encryption password for the backup files.

Hint: Standard

Password: ●●●●●●●●●●

Enabling and Disabling Veeam Agent Backup Jobs

You can disable and enable Veeam Agent jobs in Veeam Backup & Replication.

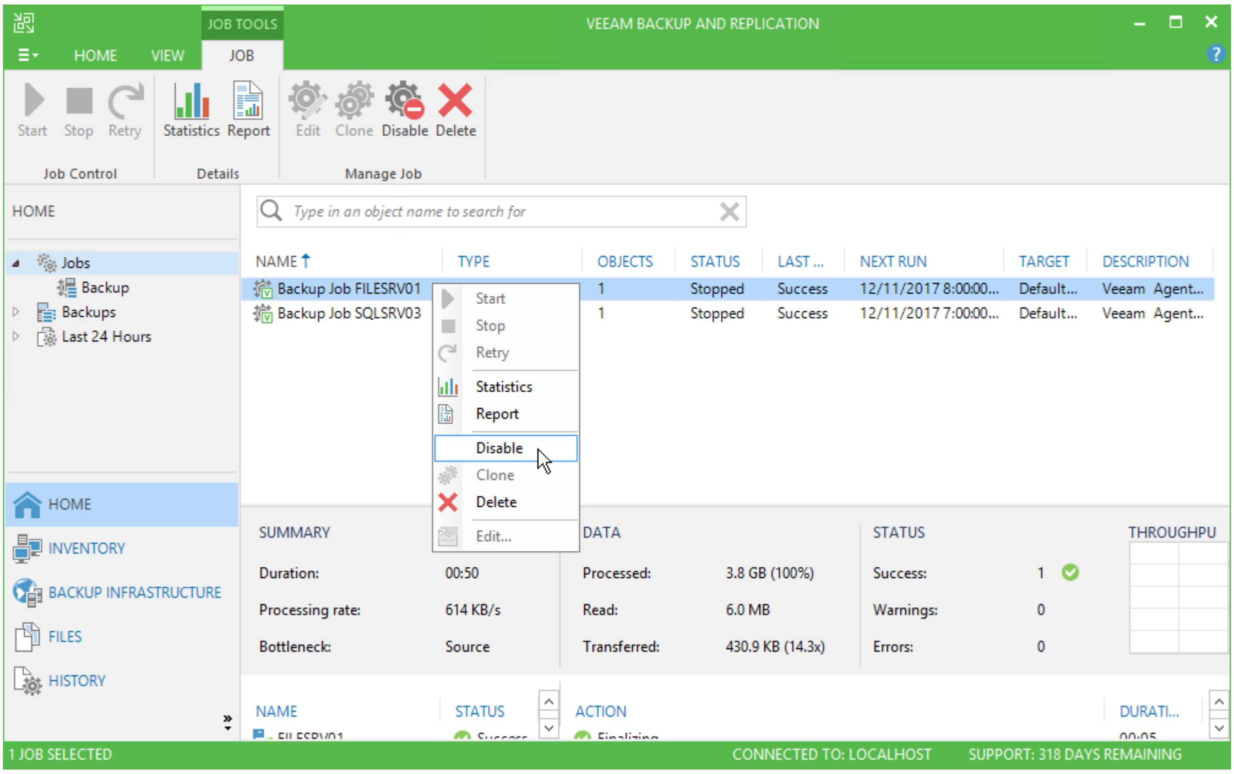
When you disable the job, you prohibit the user to store the resulting backup to the backup repository. If the user starts a disabled job manually or the job starts by schedule, the job session will fail and report the "*The job has been disabled by the Veeam Backup & Replication administrator*" error. To let Veeam Agent for Microsoft Windows store backups to 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.



NAME	TYPE	OBJECTS	STATUS	LAST ...	NEXT RUN	TARGET	DESCRIPTION
Backup Job FILESRV01		1	Stopped	Success	12/11/2017 8:00:00...	Default...	Veeam Agent...
Backup Job SQLSRV03		1	Stopped	Success	12/11/2017 7:00:00...	Default...	Veeam Agent...

SUMMARY		DATA		STATUS		THROUGHPU
Duration:	00:50	Processed:	3.8 GB (100%)	Success:	1 ✓	
Processing rate:	614 KB/s	Read:	6.0 MB	Warnings:	0	
Bottleneck:	Source	Transferred:	430.9 KB (14.3x)	Errors:	0	

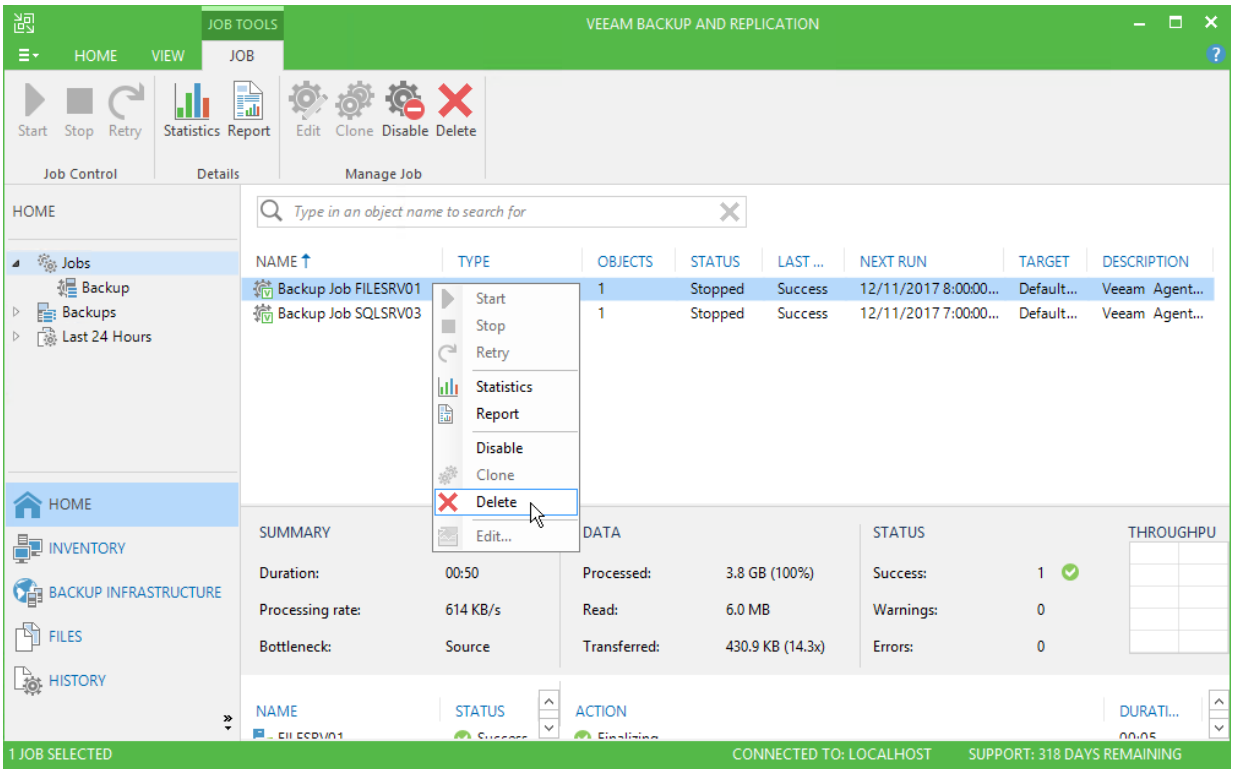
Deleting Veeam Agent Backup Jobs

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 to the Veeam Backup & Replication database. To remove the job permanently, you must delete the job and unassign access rights permissions for this user from the backup repository.

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**.



NAME ↑	TYPE	OBJECTS	STATUS	LAST ...	NEXT RUN	TARGET	DESCRIPTION
Backup Job FILESRV01		1	Stopped	Success	12/11/2017 8:00:00...	Default...	Veeam Agent...
Backup Job SQLSRV03		1	Stopped	Success	12/11/2017 7:00:00...	Default...	Veeam Agent...

SUMMARY

Duration: 00:50
Processing rate: 614 KB/s
Bottleneck: Source

DATA

Processed: 3.8 GB (100%)
Read: 6.0 MB
Transferred: 430.9 KB (14.3x)

STATUS

Success: 1 ✓
Warnings: 0
Errors: 0

THROUGHPU

NAME	STATUS	ACTION	DURATI...
FILESRV01	Success	Finalizing	00:05

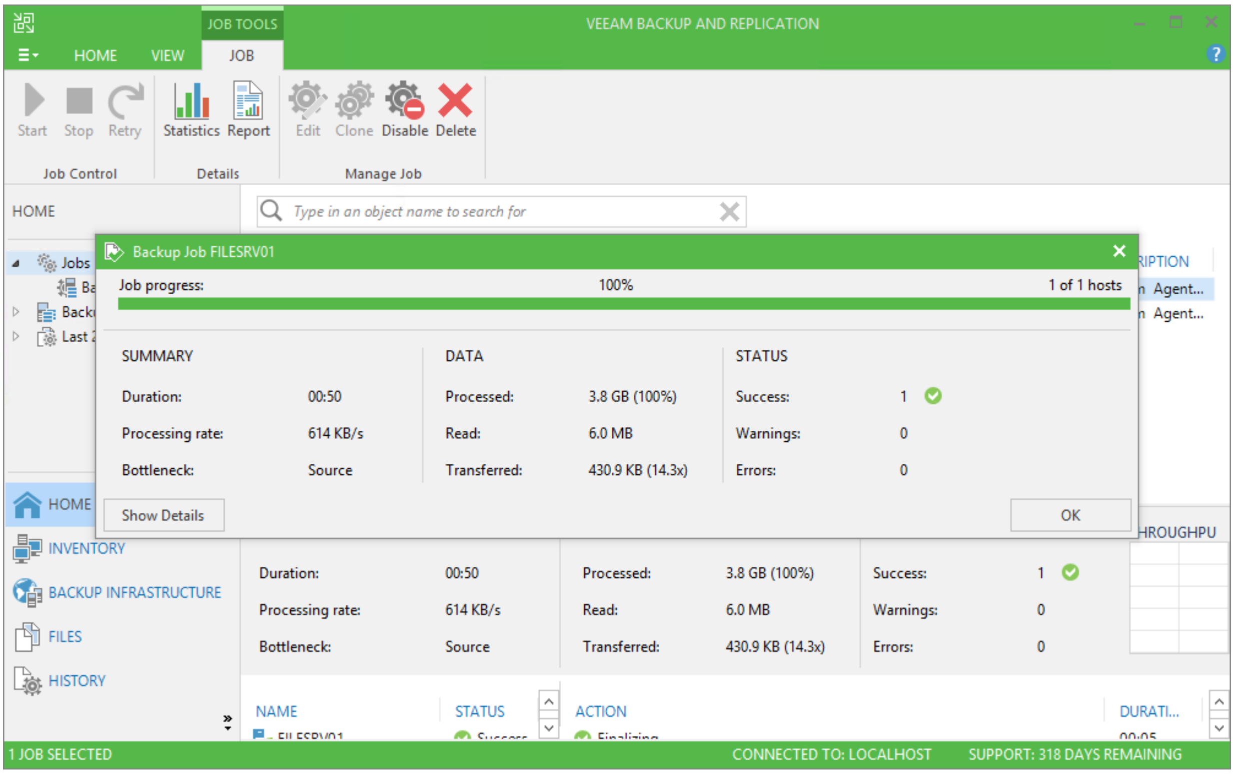
Viewing Veeam Agent Backup Job Statistics

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 main differences are the following:

- The list of objects included in the job contains a Veeam Agent computer instead of one or several VMs.
- Detailed statistics become available in the Veeam Backup & Replication console after the Veeam Agent job session completes. For currently running sessions, Veeam Backup & Replication displays duration and the name of the Veeam Agent computer only.

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**.



Backup Job FILESRV01

Job progress: 100% 1 of 1 hosts

SUMMARY		DATA		STATUS	
Duration:	00:50	Processed:	3.8 GB (100%)	Success:	1 ✓
Processing rate:	614 KB/s	Read:	6.0 MB	Warnings:	0
Bottleneck:	Source	Transferred:	430.9 KB (14.3x)	Errors:	0

Removing Veeam Agent Backups

You can remove Veeam Agent backups from Veeam Backup & Replication or permanently delete Veeam Agent backups from the backup repository.

Removing from Configuration

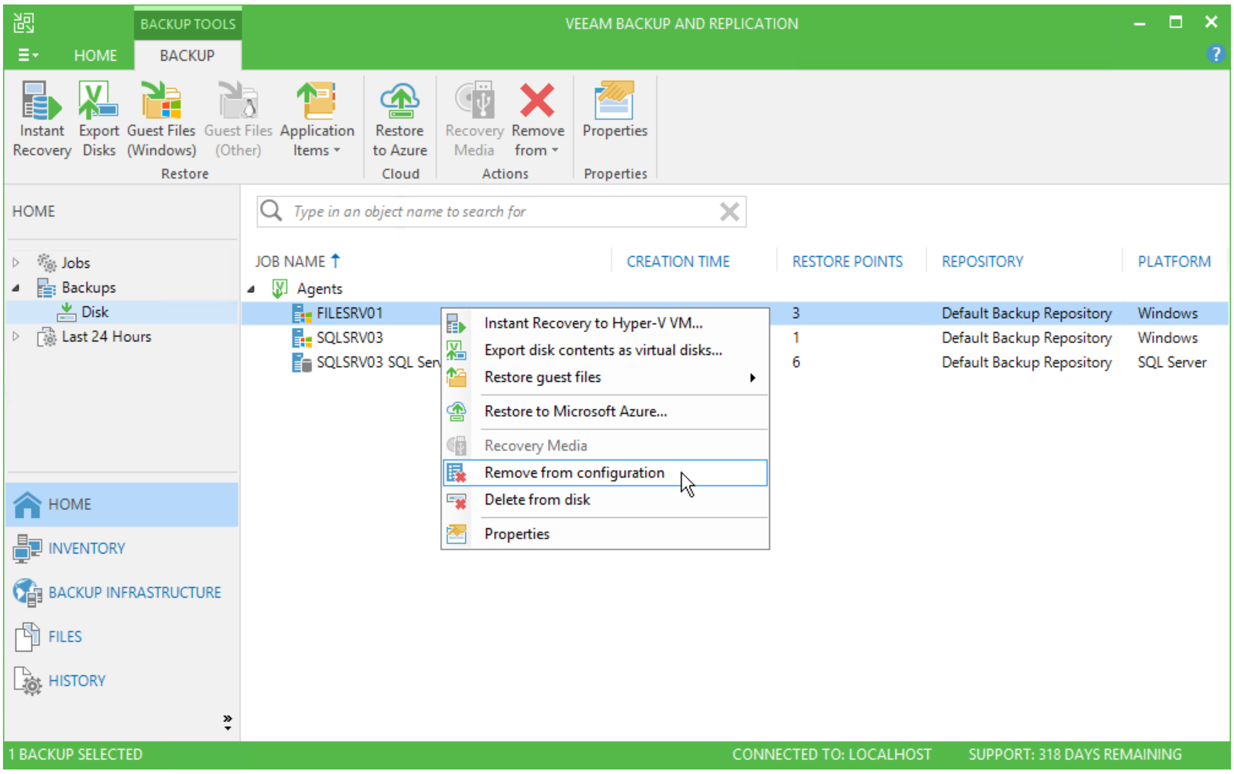
When you remove a Veeam Agent backup from configuration, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it. To learn more, see Importing Veeam Agent Backups.

To remove a Veeam Agent backup from configuration:

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 **Remove from > Configuration** on the ribbon or right-click the backup and select **Remove from configuration.**

IMPORTANT!

You should not remove a Veeam Agent backup from configuration if Veeam Agent for Microsoft Windows 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 for Microsoft Windows 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.



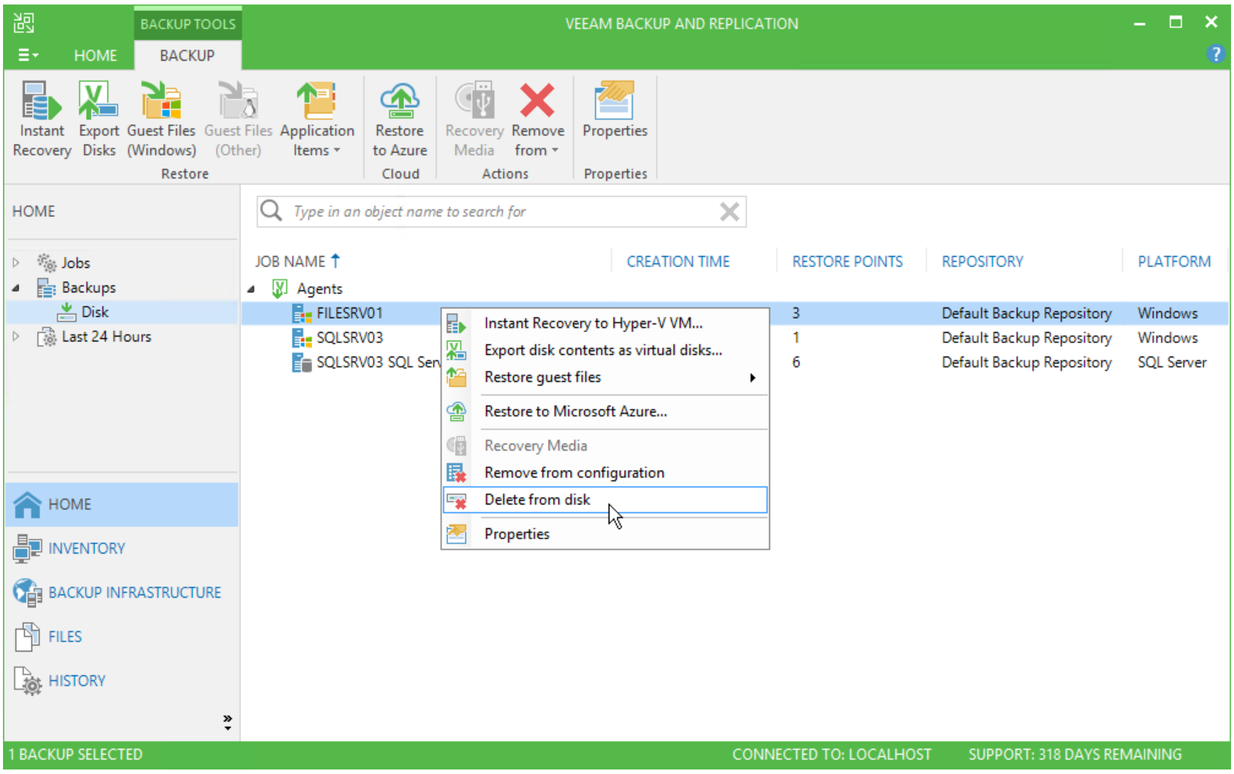
JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01		3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Ser		6	Default Backup Repository	SQL Server

Removing from Backup Repository

When you remove a Veeam Agent backup from backup repository, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files are removed from the backup repository, too.

To remove a Veeam Agent backup from the backup repository:

1. In Veeam Backup & Replication, open the **Backup & Replication** 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 **Remove from > Disk** on the toolbar or right-click the backup and select **Delete from disk.**



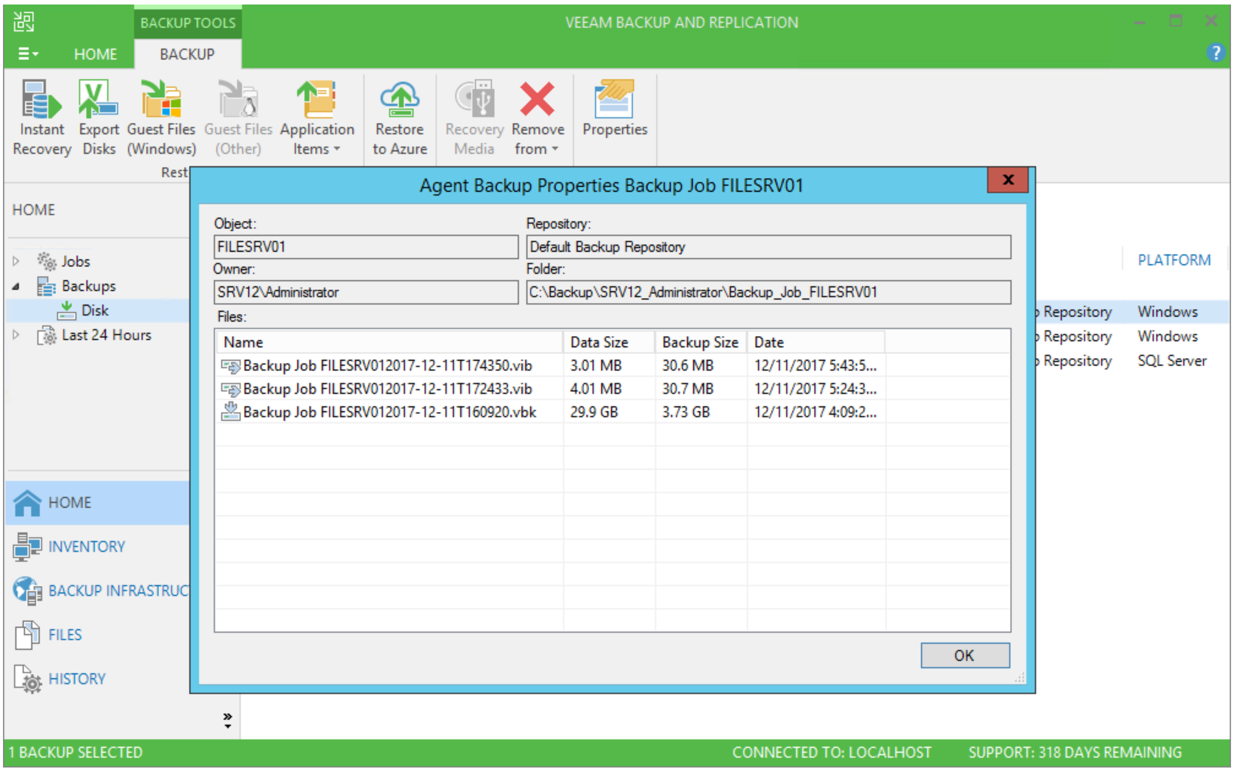
JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
Agents				
FILESRV01		3	Default Backup Repository	Windows
SQLSRV03		1	Default Backup Repository	Windows
SQLSRV03 SQL Serv		6	Default Backup Repository	SQL Server

Viewing Veeam Agent Backup Statistics

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**.



Agent Backup Properties Backup Job FILESRV01

Object: FILESRV01

Repository: Default Backup Repository

Owner: SRV12\Administrator

Folder: C:\Backup\SRV12_Administrator\Backup_Job_FILESRV01

Files:

Name	Data Size	Backup Size	Date
Backup Job FILESRV012017-12-11T174350.vib	3.01 MB	30.6 MB	12/11/2017 5:43:5...
Backup Job FILESRV012017-12-11T172433.vib	4.01 MB	30.7 MB	12/11/2017 5:24:3...
Backup Job FILESRV012017-12-11T160920.vbk	29.9 GB	3.73 GB	12/11/2017 4:09:2...

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.
- Configure global email settings to get alerted about the Veeam Agent backup job results. 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 Veeam Backup & Replication Documentation.

Assigning Roles to Users

User roles configured on the Veeam backup server apply to Veeam Agent backup jobs as well.

To learn more, see Veeam Backup & Replication Documentation.

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 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 https://helpcenter.veeam.com/docs/agentforwindows/configurator/.

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 'Backup Job <computername>' has been started [by user <username>].	Veeam Agent	Veeam Agent	Information
190	Backup Job Finished	Veeam Agent 'Backup Job <computername>' finished with <job status>. Job details: <additional information about the job results>*.	Veeam Agent	Veeam Agent	Information Warning Error
191	Backup Job Retry	Veeam Agent 'Backup Job <computername>' finished with Error and will be retried. Job details: <additional information about the job results>*.	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
1074	Computer shut down**	The process C:\Windows\system32\Shutdown.exe (<computername>) has initiated the shutdown of computer <computername> 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
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
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 <computername> backup job has been created.	Veeam Agent	Veeam Agent	Information
23050	Backup Job Modified	The <computername> backup job has been modified.	Veeam Agent	Veeam Agent	Information
23051	Agent Modified	Veeam Agent option <optionname> has been changed.***	Veeam Agent	Veeam Agent	Information
23110	Backup Mode Changed	The <computername> backup mode has been changed from <previousmode> to <currentmode>.	Veeam Agent	Veeam Agent	Information
23120	Backup Source Updated	The <computername> 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.****	Veeam Agent	Veeam Agent	Information
179	Managed mode Disabled	Veeam Agent has been switched to free mode.****	Veeam Agent	Veeam Agent	Information

201	Read-only mode Enabled	Read only UI access has been enabled.****	Veeam Agent	Veeam Agent	Information
202	Read-only mode Disabled	Read only UI access has been disabled.****	Veeam Agent	Veeam Agent	Information

* Job details contain information about the reason for completing the job with the Warning or Error status.

** The event is triggered if the user has instructed Veeam Agent for Microsoft Windows to shut down the computer on successful backup.

*** The event is triggered if the user has changed any Veeam Agent for Microsoft Windows setting other than backup job settings.

**** The event can be triggered if Veeam Agent for Microsoft Windows is managed by a Remote Monitoring and Management platform, for example, LabTech.