



Veeam Endpoint Backup

Version 1.5

User Guide

March, 2016

© 2016 Veeam Software.

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

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

Important! 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

CONTENTS	3
CONTACTING VEEAM SOFTWARE	5
ABOUT THIS GUIDE	6
OVERVIEW	7
SOLUTION ARCHITECTURE	8
DATA BACKUP	9
Backup Types	9
How Backup Works	14
Scheduled and Ad-Hoc Backups	15
Backup Chain	19
Backup to Rotated Drives	23
DATA RESTORE	26
Volume-Level Restore	26
File-Level Restore	27
Volume Resize	28
VEEAM RECOVERY MEDIA	31
Drivers in Veeam Recovery Media	32
BITLOCKER ENCRYPTED VOLUMES SUPPORT	33
INTEGRATION WITH VEEAM BACKUP & REPLICATION	38
REQUIREMENTS	39
SYSTEM REQUIREMENTS	39
USED PORTS	41
LICENSING	43
INSTALLATION AND CONFIGURATION	44
BEFORE YOU BEGIN	44
INSTALLING VEEAM ENDPOINT BACKUP	45
INSTALLING VEEAM ENDPOINT BACKUP IN UNATTENDED MODE	46
USING SYSPREP AND VEEAM ENDPOINT BACKUP	47
UPGRADING VEEAM ENDPOINT BACKUP	48
UNINSTALLING VEEAM ENDPOINT BACKUP	49
WHAT YOU DO NEXT	50
GETTING STARTED	51
PERFORMING BACKUP	52
CREATING VEEAM RECOVERY MEDIA	52
PERFORMING BACKUP	61
Auto-Configuring Scheduled Backup Jobs	61
Configuring Scheduled Backup Job	62
Managing Backup Job	75
Controlling Backup Post-Job Action	77
Deleting Backups	78
Performing Ad-Hoc Backups	79
Performing Backup with Command Line Interface	82

PERFORMING RESTORE	84
RESTORING FROM VEEAM RECOVERY MEDIA	85
USING VEEAM ENDPOINT BACKUP AND MICROSOFT WINDOWS TOOLS	103
USING MICROSOFT WINDOWS RECOVERY ENVIRONMENT	105
RESTORING VOLUMES	106
RESTORING FILES AND FOLDERS.....	117
REPORTING	130
VIEWING STATISTICS IN CONTROL PANEL.....	131
Viewing Statistics for Separate Restore Points.....	133
Viewing Information About Job Retries.....	134
MONITORING BACKUP STATE WITH TRAY AGENT	136
MONITORING BACKUP PROCESS IN TASKBAR BUTTON	137
VIEWING AND DISMISSING VEEAM ENDPOINT BACKUP EVENTS.....	138
VIEWING JOB SESSION RESULTS IN EMAIL REPORTS.....	140
SPECIFYING SETTINGS.....	141
DISABLING BACKUP OVER METERED CONNECTIONS	142
THROTTLING BACKUP ACTIVITIES	143
MANAGING ROTATED DRIVES	144
DISABLING CONTROL PANEL NOTIFICATIONS	145
ENABLING EMAIL NOTIFICATIONS	146
CHECKING FOR NEW PRODUCT VERSIONS AND UPDATES.....	149
GETTING SUPPORT.....	150
REPORTING ISSUES.....	151
USING WITH VEEAM BACKUP & REPLICATION	152
SETTING UP USER PERMISSIONS ON BACKUP REPOSITORIES.....	153
PERFORMING DATA PROTECTION TASKS.....	155
Backing Up to Backup Repositories.....	155
Performing Backup Copy for Veeam Endpoint Backups.....	156
Archiving Veeam Endpoint Backups to Tape	158
PERFORMING RESTORE TASKS	159
Restoring Files and Folders.....	159
Restoring Application Items.....	160
Exporting Disks	161
PERFORMING ADMINISTRATION TASKS	168
Importing Veeam Endpoint Backups.....	169
Enabling and Disabling Scheduled Backup Jobs	170
Deleting Veeam Endpoint Backup Jobs.....	171
Removing Veeam Endpoint Backups	172
Viewing Veeam Endpoint Backup Statistics	174
Configuring Global Settings.....	174
Assigning Roles to Users	174
APPENDIX A. VEEAM ENDPOINT BACKUP EVENTS	175

CONTACTING VEEAM SOFTWARE

For Veeam Endpoint Backup, Veeam Software provides free support by email.

If you have any questions about the product functionality, use the Veeam Endpoint Backup Control Panel to submit a support case. To learn more, see [Getting Support](#).

ABOUT THIS GUIDE

This user guide provides information about main features of Veeam Endpoint Backup 1.5.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Endpoint Backup to protect his/her computer.

Document Revision History

Revision #	Date	Description of Changes
Revision 1	3/17/2016	Initial version of the document for Veeam Endpoint Backup 1.5.

OVERVIEW

Veeam Endpoint Backup is a free data protection and disaster recovery solution for physical machines. Veeam Endpoint Backup 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 Endpoint Backup 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 or on a Veeam backup repository.

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

- Start the OS from the Veeam Recovery Media and use Veeam Endpoint Backup 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 Endpoint Backup integrates with Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform advanced tasks with Veeam Endpoint backups: restore files and disks from backups, manage Veeam Endpoint backup jobs or backups created with these jobs.

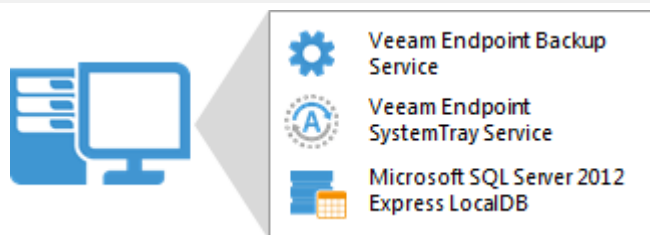
Solution Architecture

Veeam Endpoint Backup is set up on a computer whose data you want to protect.

Veeam Endpoint Backup has a one-service architecture. When you install the product, Veeam Endpoint Backup deploys the following components on the computer:

- *Veeam Endpoint Backup 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 Endpoint Tray* is a tray agent that communicates with the Veeam Endpoint Backup Service to let you monitor the backup operation status and provide quick access to main Veeam Endpoint Backup functions: starting backup and restore operations, viewing statistics for created backups and so on. The Veeam Endpoint Tray starts when you log on to the system and runs in the background.
- To store its configuration data, Veeam Endpoint Backup 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 Endpoint Backup Service. When the Veeam Endpoint Backup Service is stopped, the LocalDB subprocess is stopped, too.

Note: The account under which Veeam Endpoint Backup Service runs should not be changed. Configurations with custom account are not supported.



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

Backup Types

Veeam Endpoint Backup lets you create the following backup types:

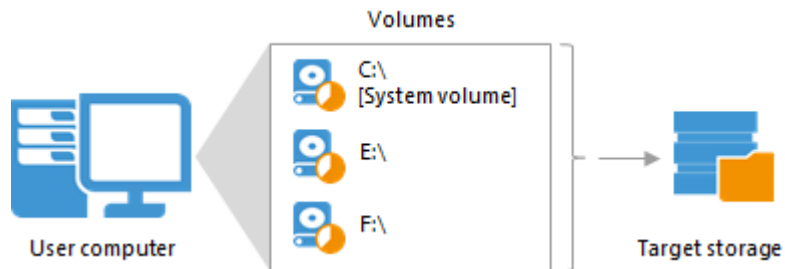
- Volume-level backup
- File-level backup

Volume-Level Backup

You can set up Veeam Endpoint Backup 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.

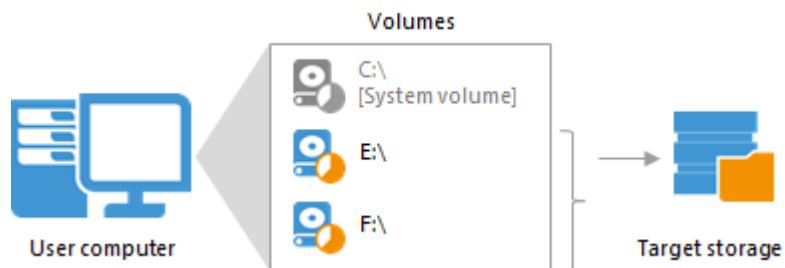
- When you back up the entire computer image, Veeam Endpoint Backup captures the content of all volumes on your computer. The resulting backup file contains all volume data and Microsoft Windows OS system data: system partition and boot partition. For GPT disks on Microsoft Windows 8, 8.1, 10, 2012 and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



- When you back up a specific computer volume, Veeam Endpoint Backup captures only the 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 Endpoint Backup 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 Endpoint Backup will capture only data on the system volume.

To learn more, see [System State Data Backup](#).

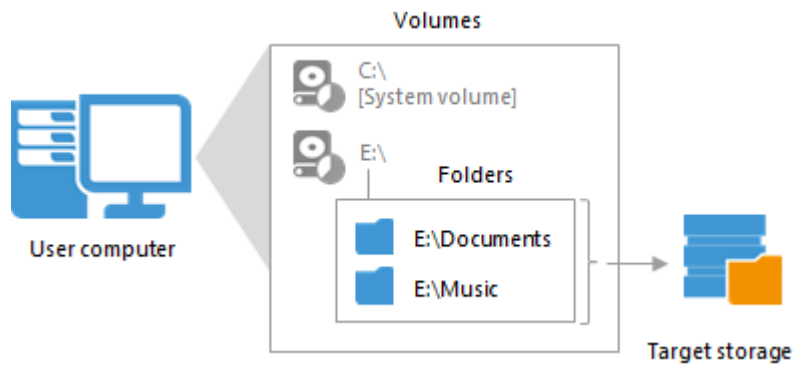


File-Level Backup

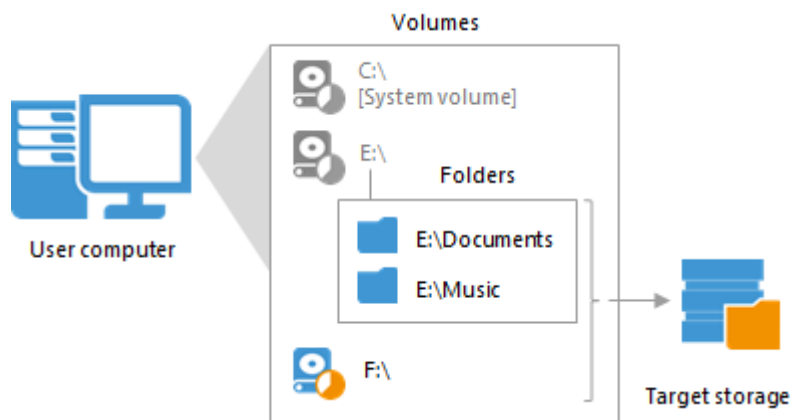
You can set up Veeam Endpoint Backup to create file-level backup. The file-level backup captures only data of individual folders on the computer. You can use the file-level backup to restore files and folders that you have added to the backup scope.

Veeam Endpoint Backup 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 these volume.
 - For backed up folders: folders that you have selected to back up, and files in these folders.

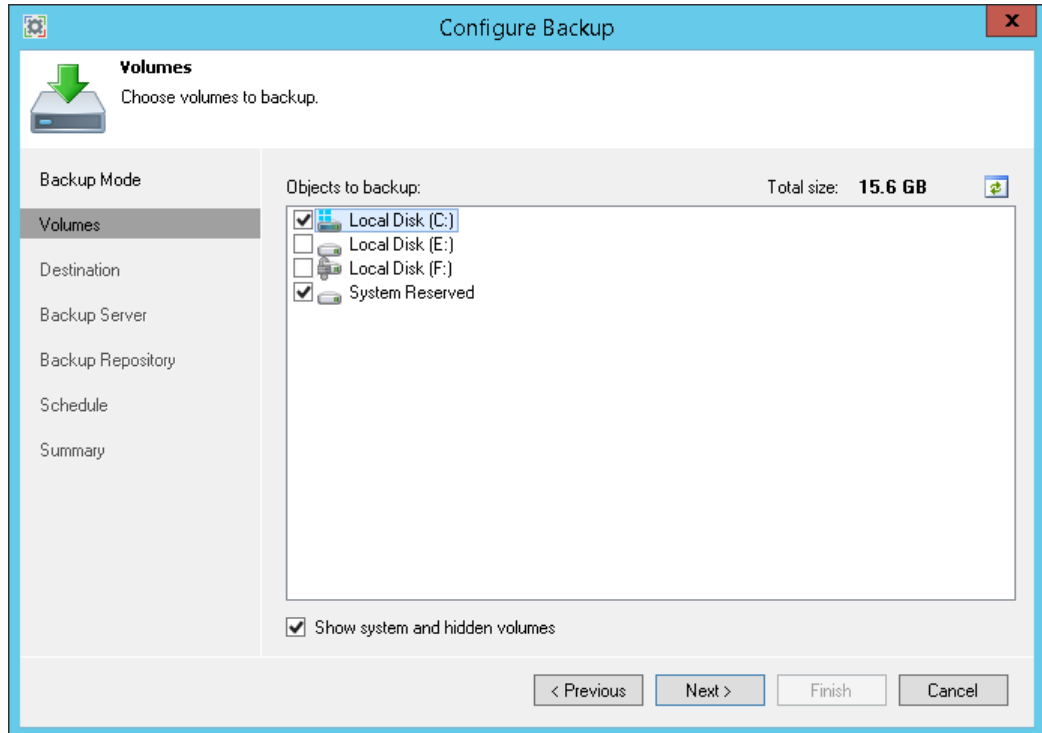


System State Data Backup

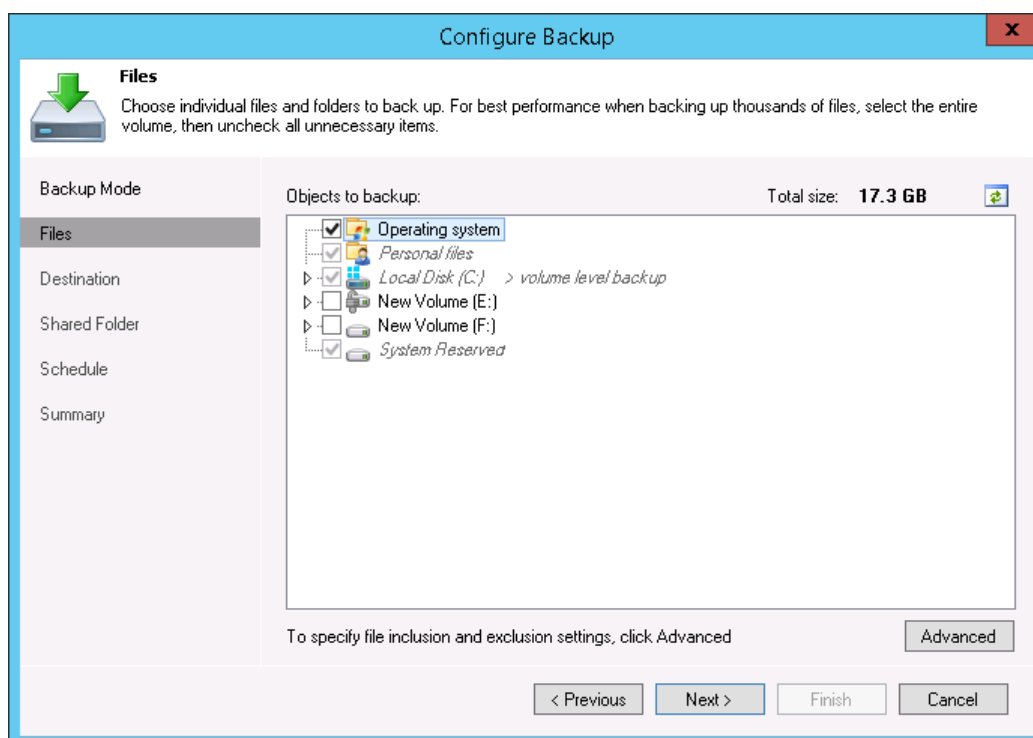
To be able to restore critical components related to the OS and start the OS after recovery, you must include in the backup the system volume (volume on which the OS is installed) and the System Reserved/UEFI or other system partitions.

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 Endpoint Backup automatically includes the System Reserved partition in the backup.

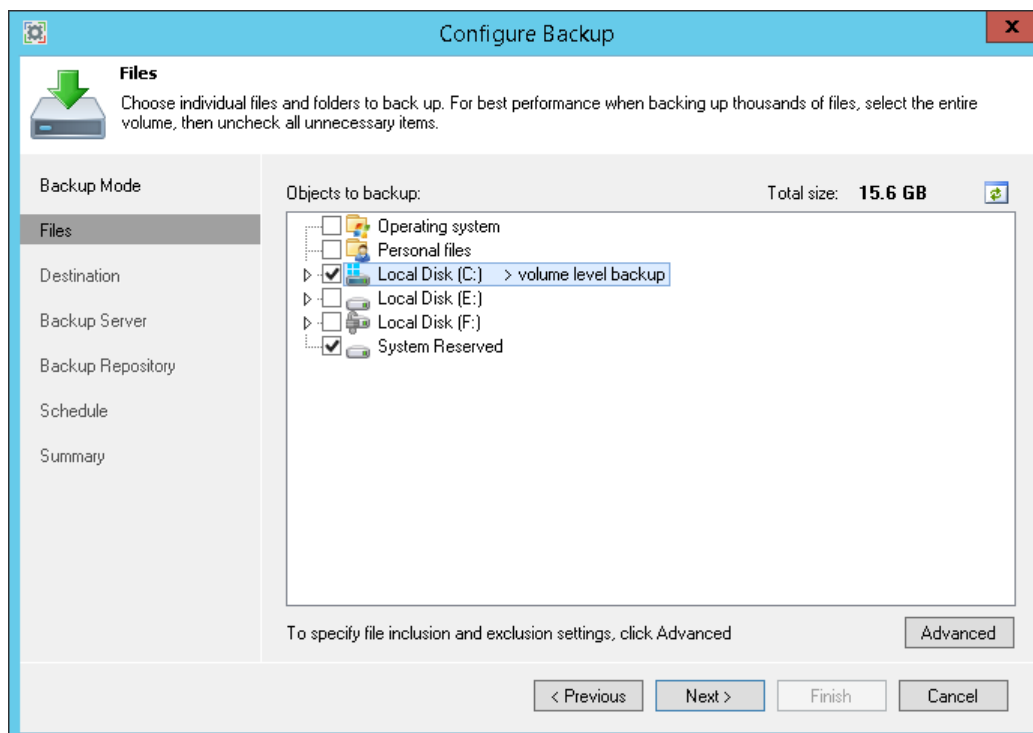


- File-level backup: *Operating system* data. When you select to back up the Operating System data, Veeam Endpoint Backup automatically includes in the backup all data related to the OS: the system volume, personal files and the System Reserved partition.



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.



How Backup Works

During backup, Veeam Endpoint Backup performs the following operations:

1. Veeam Endpoint Backup 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 Endpoint Backup creates a copy-only VSS snapshot. On Microsoft Windows Server versions, Veeam Endpoint Backup creates a full VSS snapshot.

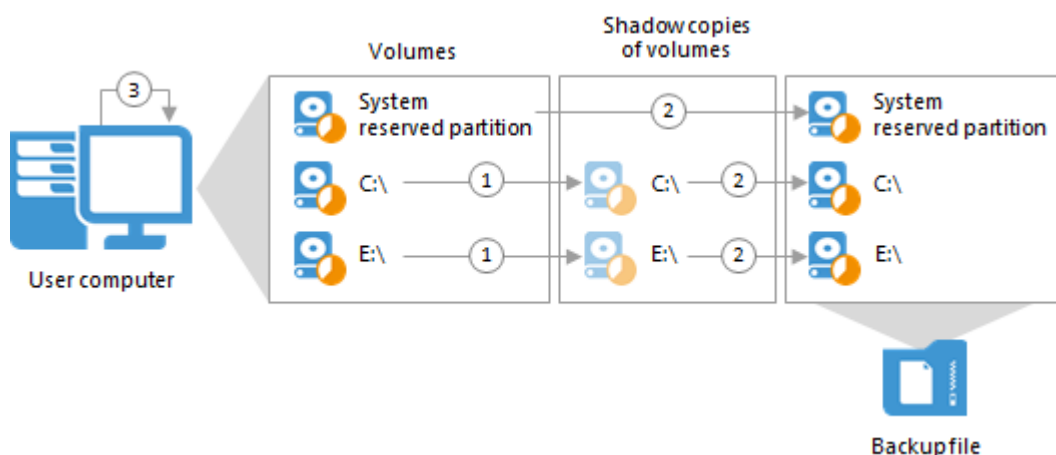
Veeam Endpoint Backup does not create a VSS snapshot for the EFI system partition on GPT disks as its data does not change during backup. For the System Reserved and other system partitions, VSS snapshot can be created if there is enough free disk space on the partition.

2. Veeam Endpoint Backup reads data from the created VSS snapshot, compresses it and copies it to the target location.
 - For volume-level backup, Veeam Endpoint Backup copies data blocks of the whole volume.
 - For file-level backup, Veeam Endpoint Backup 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 Endpoint Backup copies only those data that you have selected to back up.

In the target location, Veeam Endpoint Backup 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 Endpoint Backup automatically truncates transaction logs upon successful backup.

Important! The Veeam Endpoint 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 Endpoint Backup 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 and Ad-Hoc Backups

In Veeam Endpoint Backup, backup can run automatically, with a scheduled backup job, or can be performed on demand when needed.

Scheduled Backup Job

Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup, 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 Endpoint Backup launches the backup job according to the schedule you define. You can schedule the job to start at specific time daily or on specific week days.

For portable devices, Veeam Endpoint Backup 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 Endpoint Backup automatically retries the job every 10 minutes within the next 23 hours. To learn more, see [Automatic Job Retries](#).

Missed Backup Schedule

Veeam Endpoint Backup does not perform scheduled backups if the computer is powered off. To handle situations of short power outage or computer restart, Veeam Endpoint Backup 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 Endpoint Backup will automatically launch the scheduled job to back up your data.

Additionally, you can instruct Veeam Endpoint Backup 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 Endpoint Backup will not wait for the next scheduled backup. Instead, Veeam Endpoint Backup 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 Endpoint Backup to launch the backup job on specific events. Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will launch the backup job at the end of the working day, when you lock your computer. In addition, Veeam Endpoint Backup 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 Endpoint Backup will perform backup in the following order. At 10:00 PM, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will not perform backup at computer lock.

Automatic Job Retries

Veeam Endpoint Backup 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 Endpoint Backup automatically retries the job every 10 minutes within the next 23 hours.

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

Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will fail to wake it up due to limitations set by the OS itself.

Ad-Hoc Backup

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

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

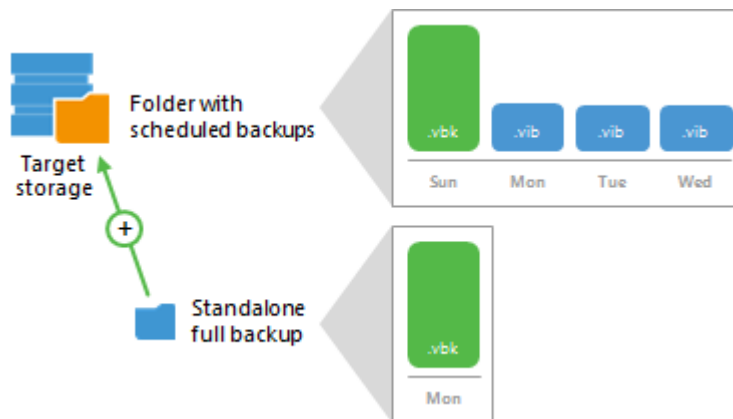
Veeam Endpoint Backup lets you create the following types of ad-hoc backups:

- **Standalone full backup**
- **Incremental backup**

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 Endpoint Backup 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 Endpoint Backup uses settings specified for the scheduled 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 scheduled 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.

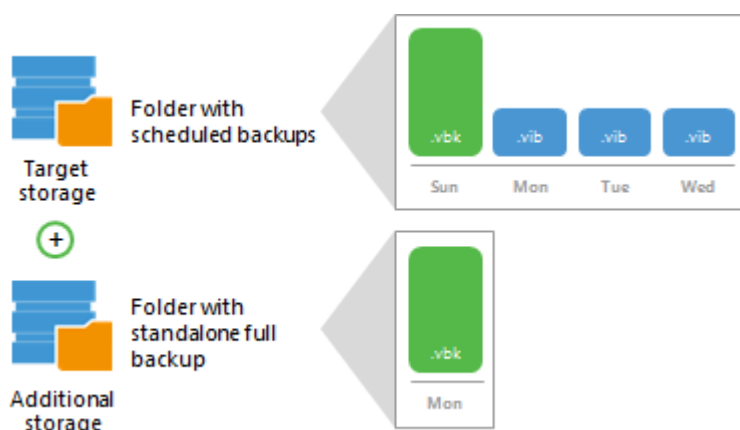
Standalone Full Backup to Another Location

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 Endpoint Backup 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

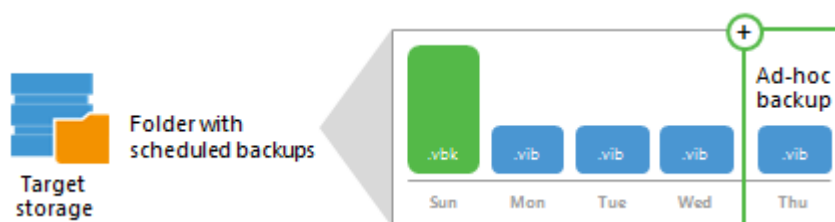
You cannot use Veeam backup repository as a target for backup to another location.



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 Endpoint Backup 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 Endpoint Backup 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](#).

Backup Chain

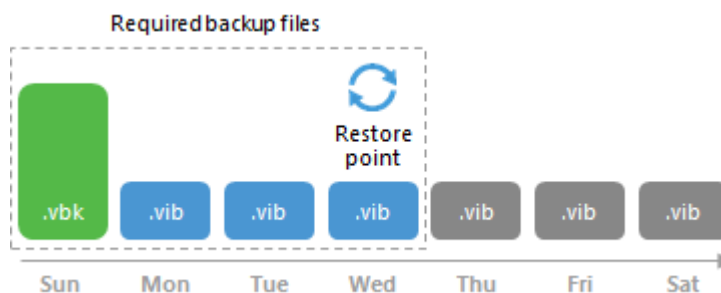
Every backup job session produces a new backup file in the target location. Backup files make up a backup chain. The backup chain can contain files of two types: full backup(s) and incremental backups.

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

Backup Retention Policy

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

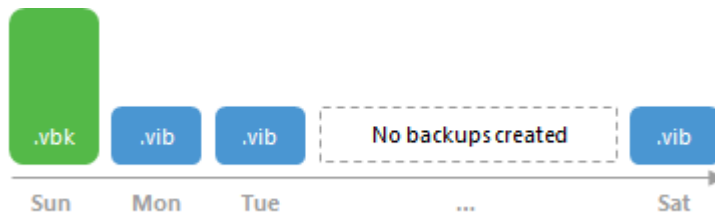
Veeam Endpoint Backup retains restore points for the last N days; the number of days is defined by the user. During every backup job session, Veeam Endpoint Backup checks if there is any obsolete restore point in the backup chain. If some restore point is obsolete, it is removed from the chain.

For retention policy settings, Veeam Endpoint Backup 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.

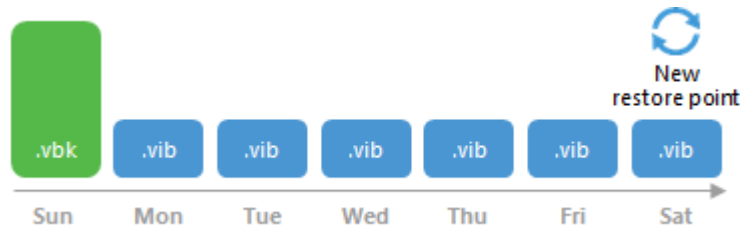
The backup job has successfully run 3 times and created 3 restore points in the backup chain. After that, you have turned off your computer for 10 days. When you turn on your computer, Veeam Endpoint Backup runs a backup job by schedule and creates a new restore point. The earliest restore point, however,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



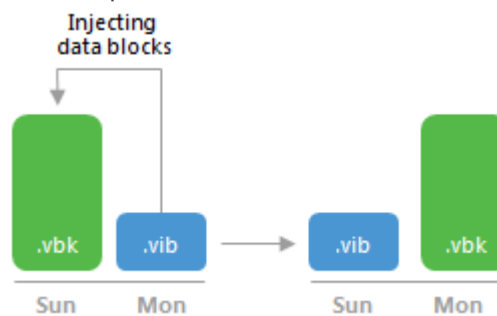
Removing Backups by Retention

When removing obsolete restore points, Veeam Endpoint Backup 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 Endpoint Backup uses the following rotation scheme:

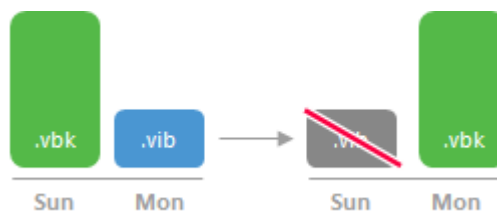
1. During every backup job session Veeam Endpoint Backup adds a backup file to the backup chain and checks if there is an obsolete restore point.



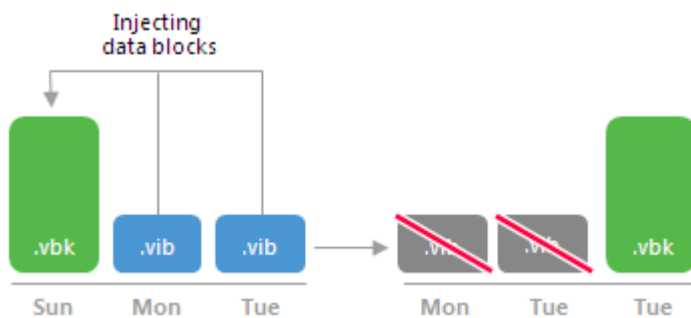
2. If an obsolete restore point exists, Veeam Endpoint Backup transforms the backup chain. As part of this process, it performs the following operations:
 - a. Veeam Endpoint Backup re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Endpoint Backup 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 Endpoint Backup makes sure that the backup chain is not broken, and you will be able to recover your data to any restore point.



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 Endpoint Backup 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 Endpoint Backup creates a separate backup chain on the new drive.
3. After you swap drives again, Veeam Endpoint Backup detects if there is a backup chain on the currently attached drive. If the backup chain exists, Veeam Endpoint Backup 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 Drive** 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 Drive
Choose locally attached drive to backup to.

Backup Mode
Files
Destination
Local Drive
Schedule
Summary

Local drives:

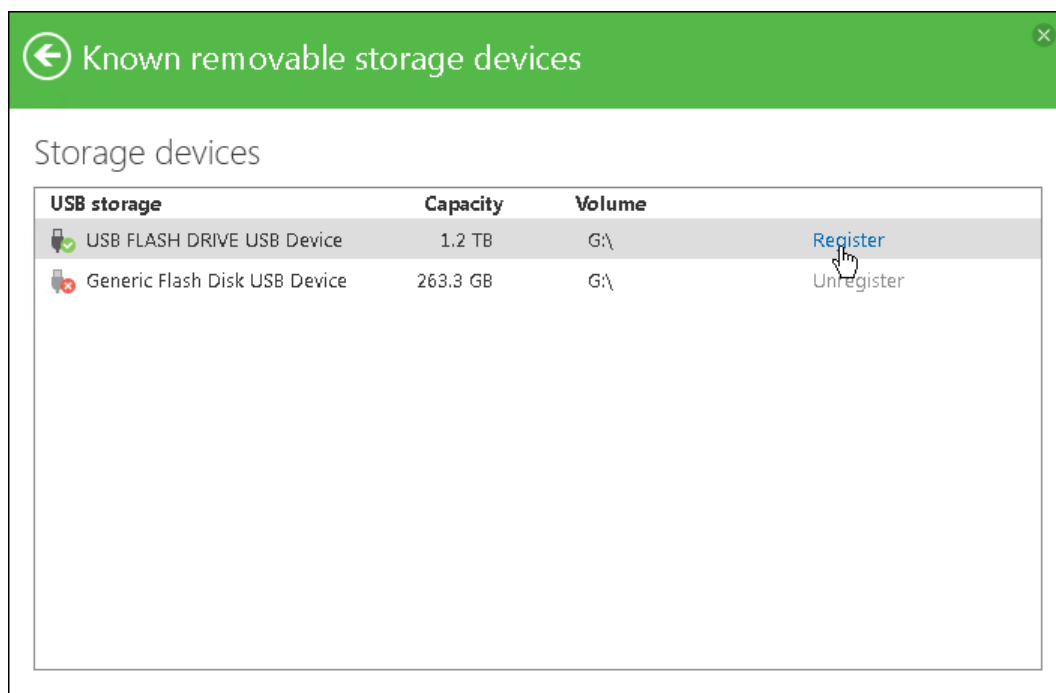
Storage device	Free space	Total space
Local Disk (C:)	45.3 GB	59.7 GB
Local Disk (E:)	59.8 GB	59.9 GB
Local Disk (F:)	29.5 GB	29.9 GB
Local Disk (G:)	233.4 GB	298.8 GB

Folder:
G:\VeeamBackup\ Browse

Backups to retain
Keep restore points for the last days when computer was used

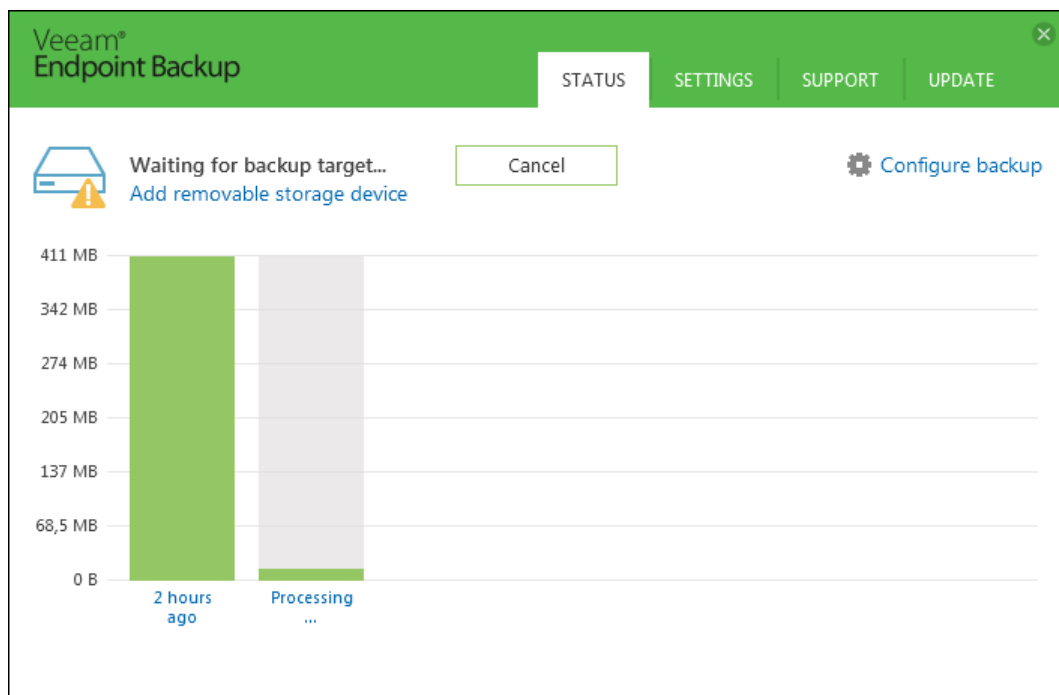
< Previous Next > Finish Cancel

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 Endpoint Backup. To do this:
 - a. Double-click the Veeam Endpoint Backup 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.



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

Data Restore

Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup uses a separate program — Virtual Disk Driver (VDD) 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 Endpoint Backup, you can resize backup volumes during [Volume-Level Restore](#). When you select to resize a volume, Veeam Endpoint Backup 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 **Veeam Endpoint Recovery** 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 Endpoint Backup performs the following operations:

1. When you select the **Resize** option to shrink a volume, Veeam Endpoint Backup mounts the backup volume to a temporary NTFS folder on the system drive, for example:

`C:\Users\Username\AppData\Local\Temp.`

2. Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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.

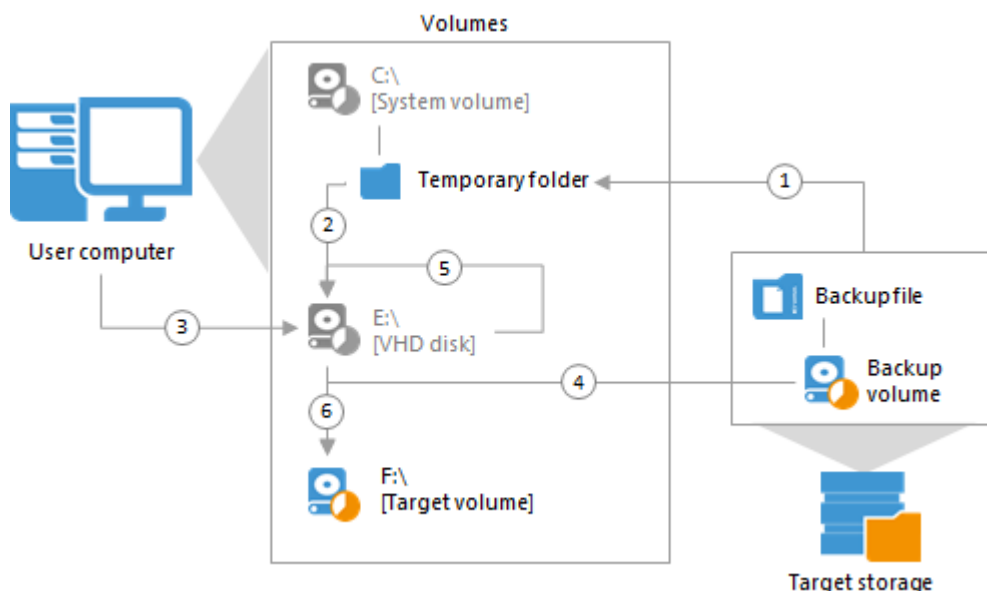
When the query is complete and you specify the desired size for the restored volume, Veeam Endpoint Backup unmounts the VHD disk.

4. When you start the restore process, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup unmounts the VHD disk.



How Volume Extend Works

When you restore a volume to a target location of the larger size, Veeam Endpoint Backup performs the following operations:

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

2. Veeam Endpoint Backup mounts the created NTFS folder as a VHD disk next to other disks that are present on the computer.

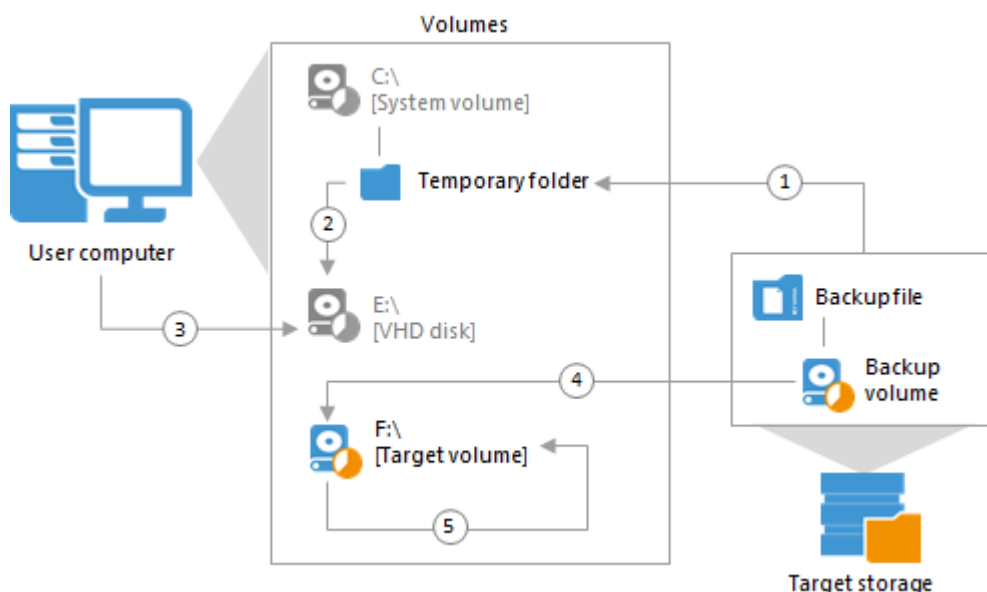
Mounting VBK file content as a VHD disk makes it possible for Veeam Endpoint Backup to use Microsoft Windows system's disk management tools to measure current size of the backup volume and maximum and minimum size for the restored volume.

3. Veeam Endpoint Backup 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 Endpoint Backup unmounts the VHD disk.

4. When you start the restore process, Veeam Endpoint Backup 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 Endpoint Backup extends the size of the target volume to the specified size.



Veeam Recovery Media

Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup or 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 Endpoint Backup recovery environment to fix the OS system errors on your computer or restore data from the backup. Veeam Endpoint Backup offers a set of tools for the computer system image and data recovery:

- Bare Metal Recovery — the Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 connections 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.

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

- Drivers that are currently installed on your computer. Veeam Endpoint Backup 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

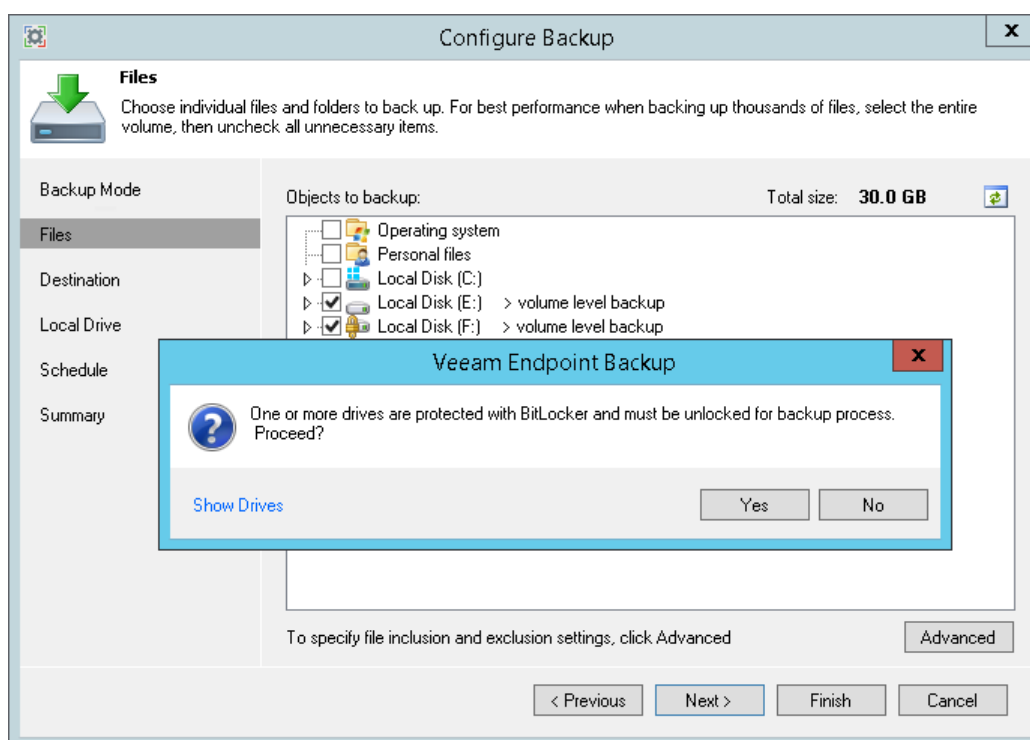
Veeam Endpoint Backup supports scenarios of data backup and restore to/from volumes encrypted with Microsoft Windows BitLocker.

Data Backup

You can create backups of BitLocker encrypted volumes and store backups created with Veeam Endpoint Backup on BitLocker encrypted volumes.

BitLocker encrypted volumes (both source and target) must be unlocked at the moment when Veeam Endpoint Backup 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.



Data Restore

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

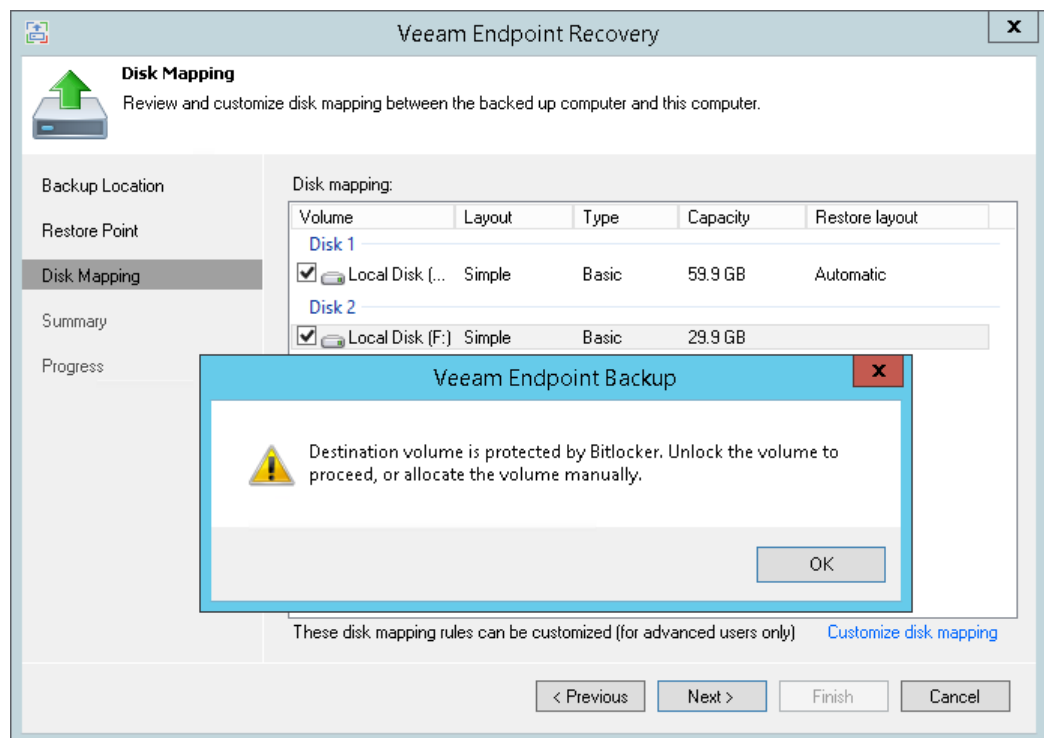
Veeam Endpoint Backup restores volumes in their initial state:

- 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.

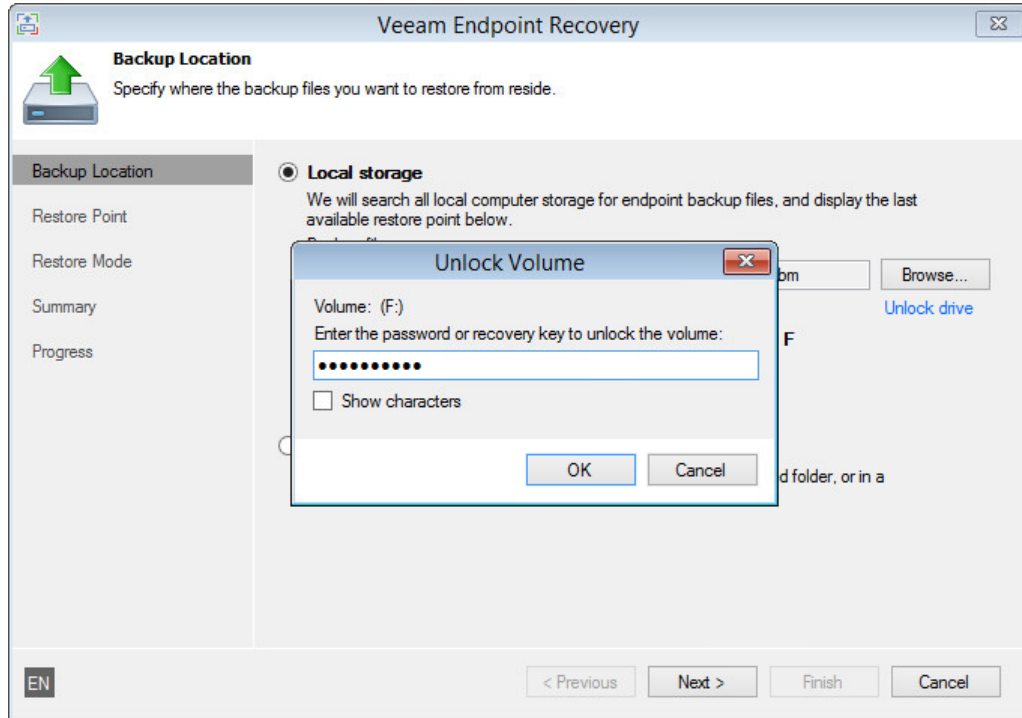
- If the backup file is stored on a locked volume, Veeam Endpoint Backup will fail to access it, and you will not be able to restore data from it.
- If you perform volume-level restore, and the target volume is locked, Veeam Endpoint Backup will display a warning and will ask you to unlock the volume.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



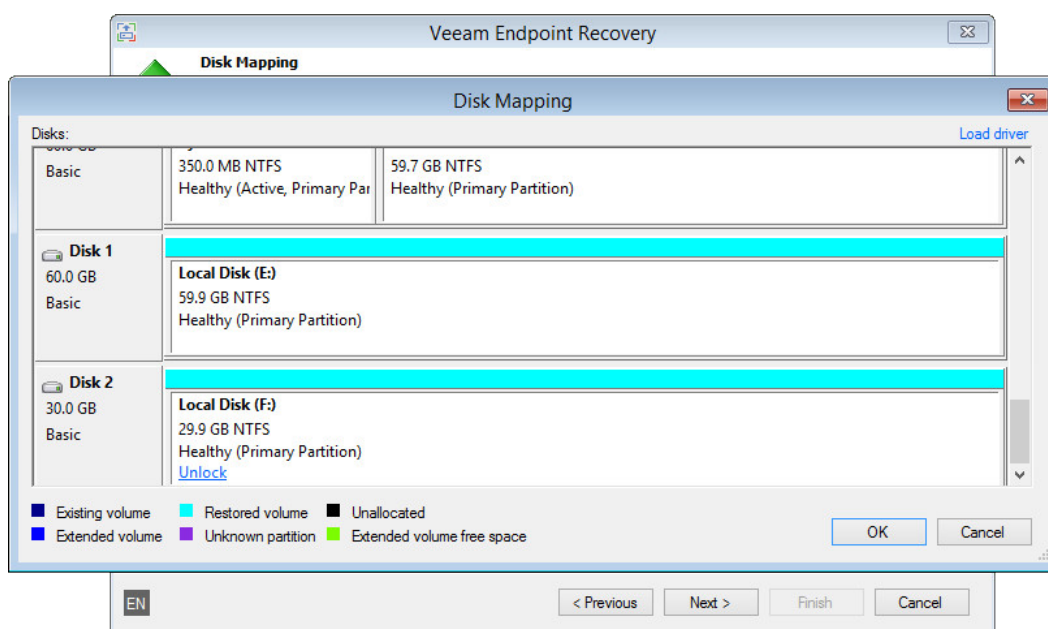
Veeam Recovery Media

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

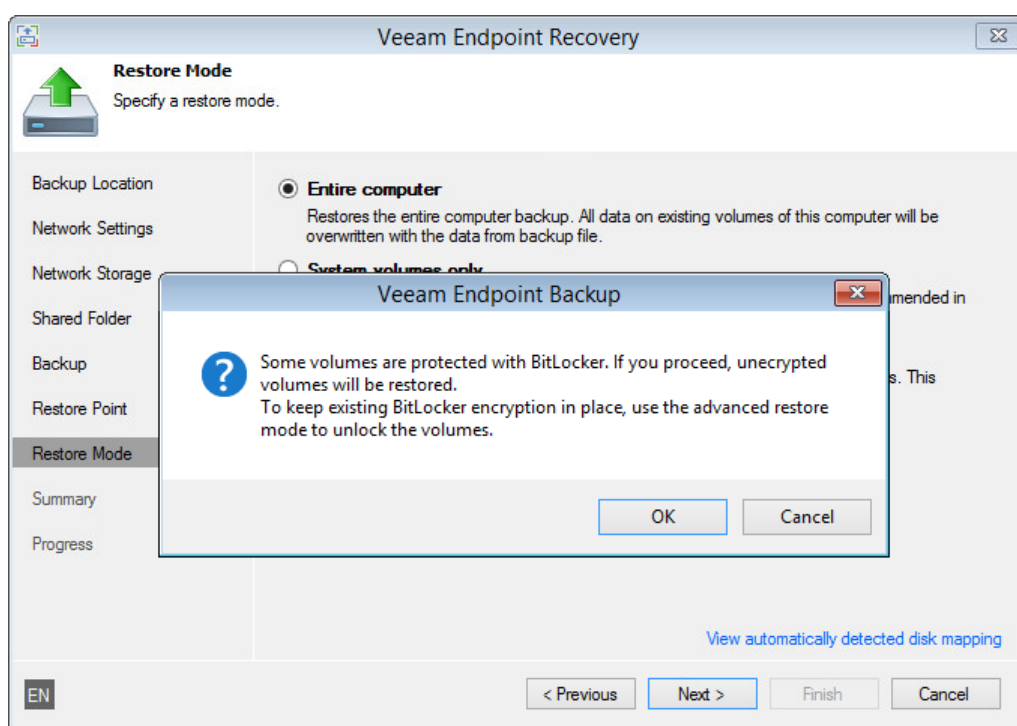
- If the backup file that you want to use for data restore resides on a locked volume, Veeam Endpoint Backup cannot access this backup file. To unlock the volume with the backup file, click **Unlock drive** under the **Backup file** field and enter a password for the volume.



- If the target volume is BitLocker encrypted and locked, at the **Restore Mode** step of the wizard Veeam Endpoint Backup displays a warning informing about it. You can use one of the following scenarios:
 - You can restore data to the target volume and keep BitLocker encryption enabled for the volume. To do this, you must unlock the volume before you start data restore.
To unlock the volume, click **Cancel** in the warning window. At the **Restore Mode** step of the wizard, select **Manual Restore**. At the **Disk Mapping** step of the wizard, click **Customize disk mapping** and click **Unlock** under the necessary volume.



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



Important! Veeam Endpoint Backup 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 Endpoint Backup triggers a VSS snapshot of a FAT32 formatted volume, the VSS snapshot is stored on another, non-FAT32 volume on the computer.

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

Integration with Veeam Backup & Replication

If you plan to use Veeam Endpoint Backup with Veeam Backup & Replication, you must install Veeam Backup & Replication 8.0 Update 2 or later on the Veeam backup server.

Important! Veeam Endpoint Backup cannot work with Veeam Backup & Replication that is located behind the NAT gateway.

You can store backup files created with Veeam Endpoint Backup 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 scheduled Veeam Endpoint Backup job.

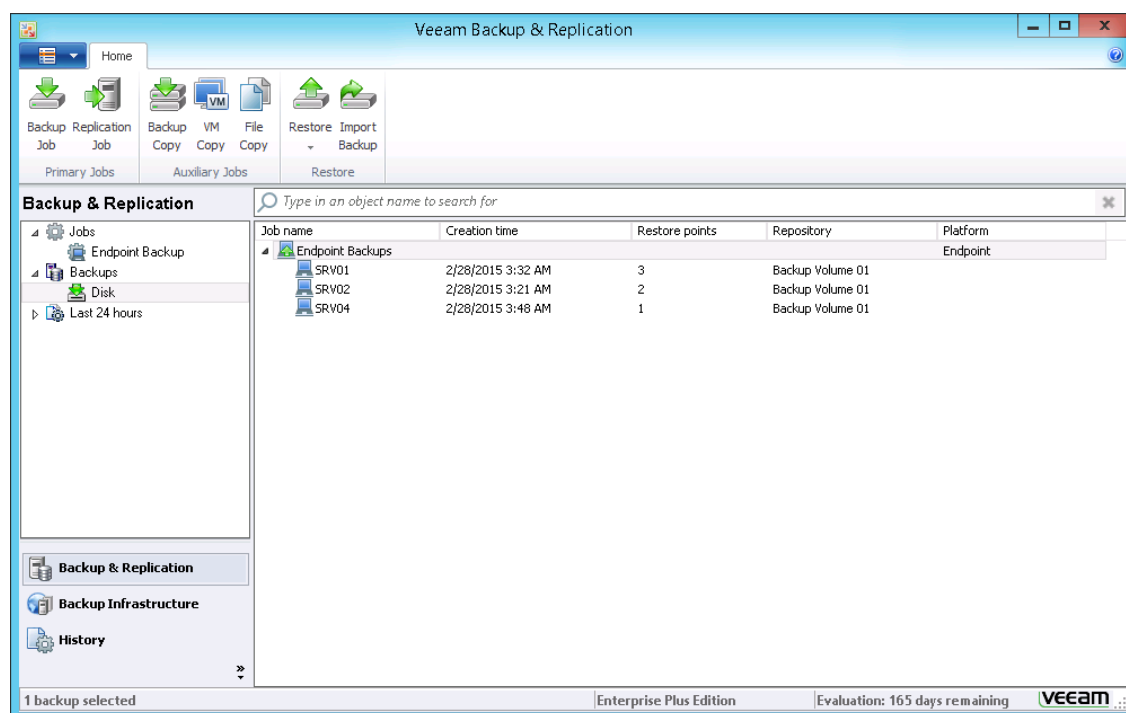
Veeam Endpoint Backup works with the backup repository as with any other target location. Backup files are stored to a separate folder; you can perform standard restore operations using these files.

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

- The Veeam Endpoint Backup scheduled backup job is displayed in the list of jobs in Veeam Backup & Replication.
- Backup files created with Veeam Endpoint Backup 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 Endpoint Backups:

- Perform data protection operations: copy Veeam Endpoint backups to secondary backup repositories and archive these backups to tape.
- Perform restore operations: restore individual files and folders, application items from Veeam Endpoint backups; restore computer disks and convert them to the VMDK, VHD or VHDX format.
- Perform administrative tasks: disable and delete Veeam Endpoint backup jobs, remove Veeam Endpoint backups and so on.



REQUIREMENTS

Before you install Veeam Endpoint Backup, 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	<p>CPU: x86-64 processor.</p> <p>Memory: 2 GB RAM.</p> <p>Disk Space: 150 MB for product installation.</p> <p>Network: 1 Mbps or faster. High latency and reasonably unstable WAN links are supported.</p> <p>System firmware: BIOS or UEFI.</p> <p>Drive encryption: Microsoft BitLocker (optional)</p>
OS	<p>Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported*:</p> <ul style="list-style-type: none">• Microsoft Windows 7 SP1• Microsoft Windows 8.x• Microsoft Windows 10**• Microsoft Windows Server 2008 R2 SP1• Microsoft Windows Server 2012• Microsoft Windows Server 2012 R2 <p>* Server Core installations of Microsoft Windows Server OSs are not supported.</p> <p>* Microsoft Failover Clusters are not supported.</p> <p>** Microsoft Windows 10 Education is supported starting from build 10586 and higher.</p>
Software	<p>The following required 3rd party software is included in the setup program and is installed automatically when installing the product:</p> <ul style="list-style-type: none">• Microsoft .NET Framework 4.5.2• Microsoft SQL Server 2012 Management Objects• Microsoft SQL Server System CLR Types <p>If you plan to use Veeam Endpoint Backup with Veeam Backup & Replication, you must install Veeam Backup & Replication 8.0 Update 2 or later on the Veeam backup server.</p>
Microsoft SQL Database	<p>Microsoft SQL Server 2012 Express LocalDB Edition (installed with the product).</p>

Backup Target

Backup can be performed to the following disk-based storage:

- Local (internal) storage of the protected endpoint (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 8.0 Update 2 or later backup repository.

Used Ports

Make sure that you open ports listed below to enable proper work of Veeam Endpoint Backup.

From	To	Protocol	Port	Notes
Veeam Endpoint Computer	Veeam Backup Server	TCP	10001	Default port used for communication with the Veeam Backup server. Data between the Veeam Endpoint computer and backup repositories is transferred directly, bypassing Veeam backup servers.
Veeam Backup Server	Veeam Endpoint Computer	TCP	9395	Default port used for communication with Veeam Endpoint computer.
		TCP	6183	Default port used by the Veeam Endpoint Service.
Communication with Veeam Backup & Replication Repositories				
Veeam Endpoint Computer	Linux server performing the role of a backup repository	TCP	22	Port used as a control channel from the Veeam Endpoint 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
	Shared folder CIFS (SMB) share	TCP UDP	135, 137 to 139, 445	Ports used as a transmission channel from the Veeam Endpoint 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.

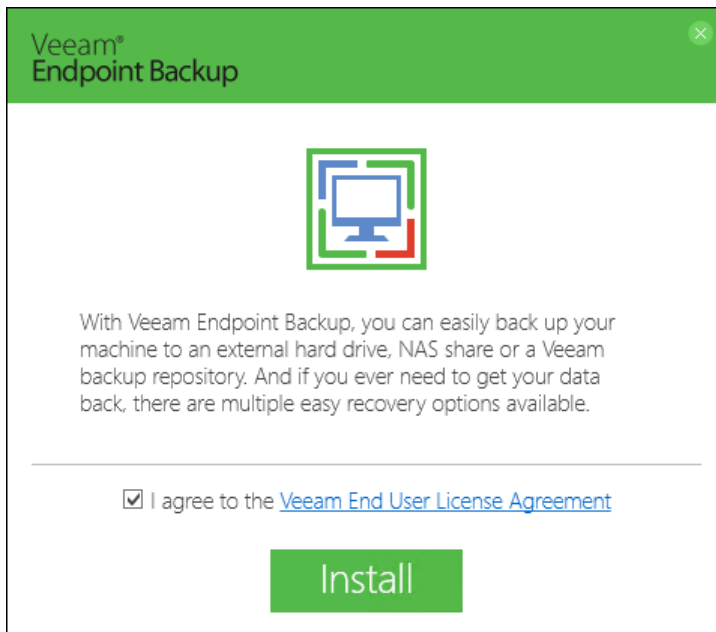
From	To	Protocol	Port	Notes
		TCP	1025 to 5000 (for Microsoft Windows 2003) 49152-65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see https://support.microsoft.com/kb/929851/en-us .
		TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.

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 Endpoint computers.

LICENSING

Veeam Endpoint Backup is a free product. You do not need to obtain or install any license to use it.

When you install Veeam Endpoint Backup, 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 Veeam website at: www.veeam.com/eula.html.



Integration with Veeam Backup & Replication

If you plan to use Veeam Endpoint Backup with Veeam Backup & Replication, you must install on the Veeam backup server a license for Veeam Backup & Replication Standard Edition or higher.

INSTALLATION AND CONFIGURATION

You can install Veeam Endpoint Backup 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 Endpoint Backup must satisfy system requirements specified in this document. To learn more, see [System Requirements](#).
2. You must run the Veeam Endpoint Backup 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 Endpoint Backup 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.

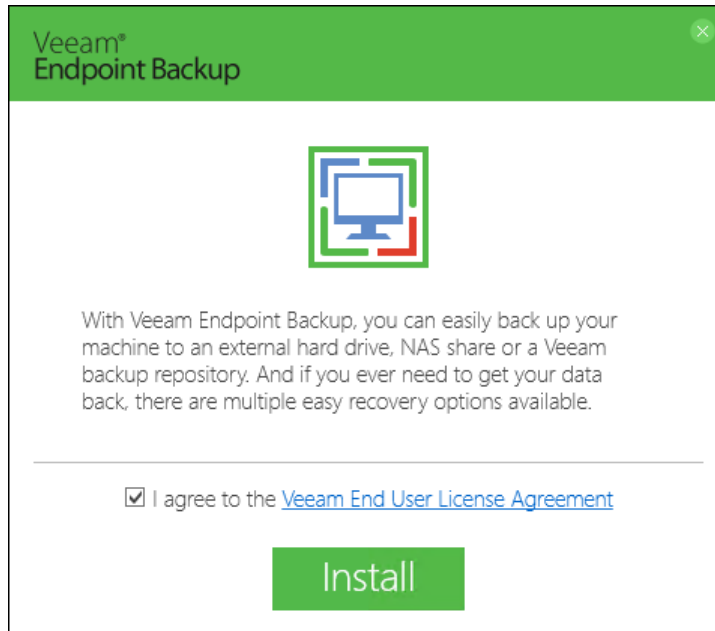
4. The product program files are placed to the %Program Files%\Veeam\Endpoint Backup folder on the system volume. Make sure that you have enough free space on the system volume to install the product. Veeam Endpoint Backup requires at least 150 MB.
5. [Recommended] If you want to configure a scheduled 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 Endpoint Backup 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 Endpoint Backup

To install Veeam Endpoint Backup:

1. Download the Veeam Endpoint Backup 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 Endpoint Backup, 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**.



4. After the installation process is complete, you can instruct Veeam Endpoint Backup to perform the following advanced actions:
 - Auto-configure settings for the backup job. To learn more, see [Auto-Configuring Scheduled Backup Jobs](#).
 - Create a recovery image for your computer. To learn more, see [Creating Veeam Recovery Media](#).

Installing Veeam Endpoint Backup in Unattended Mode

You can install Veeam Endpoint Backup 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 Endpoint Backup installation process in large-scale environments.

Prerequisite Software

During the product installation, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup but will not start the Veeam Endpoint Backup service. After you reboot the computer, the Veeam Endpoint Backup service will be started and Veeam Endpoint Backup will be fully functioning.

Installation Syntax

To install Veeam Endpoint Backup in the unattended mode, use a command with the following syntax:

```
<path_to_exe> /silent
```

where `<path_to_exe>` is a path to the Veeam Endpoint Backup installation file.

Using Sysprep and Veeam Endpoint Backup

You can pre-install Veeam Endpoint Backup 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 Endpoint Backup:

1. Install Veeam Endpoint Backup in a Microsoft Windows system image. To learn more, see [Installing Veeam Endpoint Backup](#).
2. Configure the backup job in the way you want it to work on computers with pre-installed Veeam Endpoint Backup. To learn more, see [Configuring Scheduled 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 Endpoint Backup 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 Endpoint Backup will re-generate its internal ID of the backup job. As a result, the backup job will be fully functional.

Upgrading Veeam Endpoint Backup

For Veeam Endpoint Backup, upgrade to newer versions is supported. You can start the upgrade process from the Veeam Endpoint Backup 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 Endpoint Backup are not impacted in any way.

To upgrade Veeam Endpoint Backup:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup icon in the system tray and select **Control Panel**.
2. Open the **Update** tab.
3. If the new version of Veeam Endpoint Backup is available, click **Download**.
4. When the download is complete, click **Install** to run the setup archive.
5. To upgrade Veeam Endpoint Backup, 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: In some cases, upgrade to the new version of Veeam Endpoint Backup may require computer reboot.

Tip: You can also download the Veeam Endpoint Backup 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 Endpoint Backup to a newer version in the unattended mode using the same command that is used for unattended installation. To learn more, see [Installing Veeam Endpoint Backup in Unattended Mode](#).

Uninstalling Veeam Endpoint Backup

To uninstall Veeam Endpoint Backup:

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

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

What You Do Next

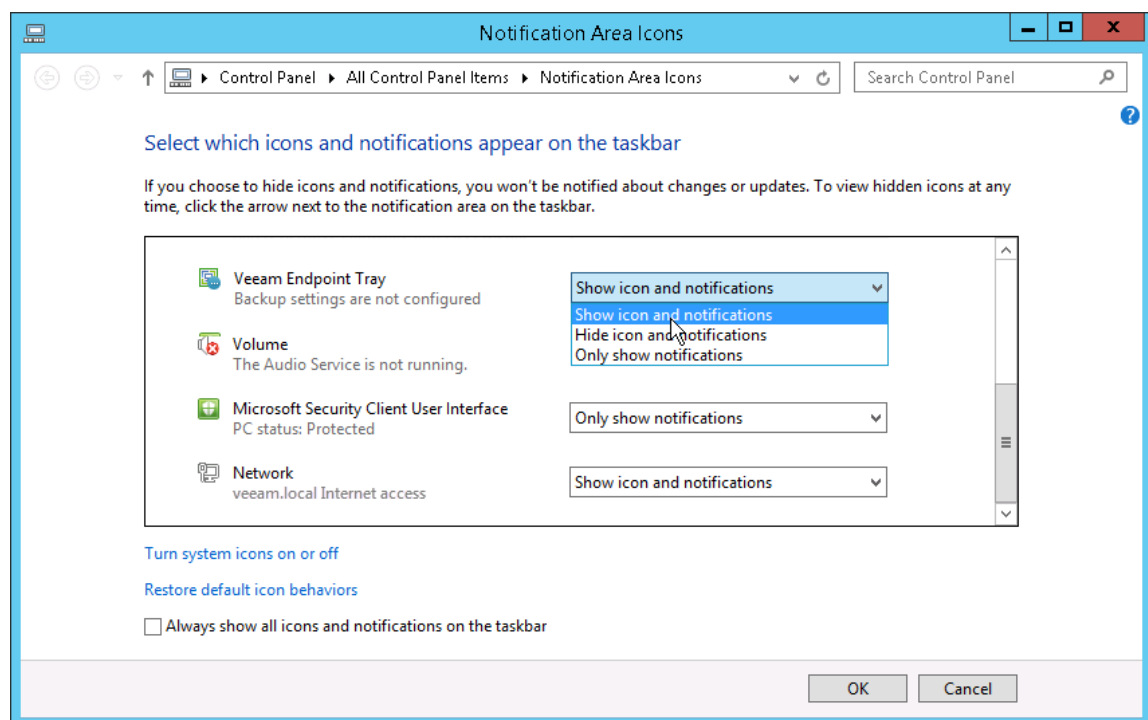
After the product installation, Veeam Endpoint Backup displays its icon in the system tray. You can use the system tray icon to perform main operations in Veeam Endpoint Backup:

- Configure the backup job and start ad-hoc backup operations
- Launch restore wizards
- Open the Veeam Endpoint Backup Control Panel
- Monitor the state of backup tasks and so on

Depending on the current settings of your Microsoft Windows OS, the Veeam Endpoint Backup 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 Endpoint Tray.
3. In the **Behaviors** column, set the **Show icon and notification** setting for it.
4. Click **OK**.



GETTING STARTED

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

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 necessary restore point.

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

3. **Specify Veeam Endpoint Backup settings.**

You can define resource usage settings during backup, instruct Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will include the drivers into the recovery image.
- [For RW CD/DVD/BD] During the recovery image creation, Veeam Endpoint Backup 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 Endpoint Backup 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)

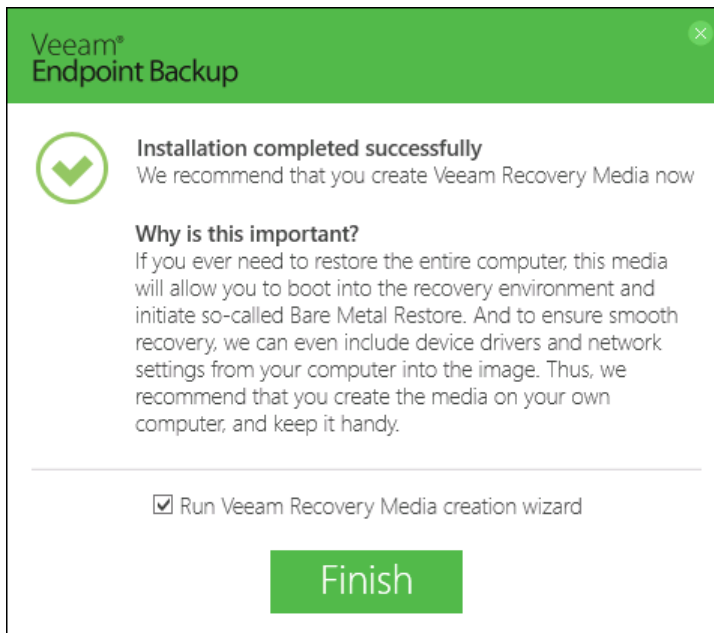
- If you want to include specific storage and network drivers into the recovery image, place them to a local folder on your computer or in a network shared folder on which you have read permissions. During the recovery image creation, you will be able to define a path to this folder, and Veeam Endpoint Backup 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 Endpoint Backup 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

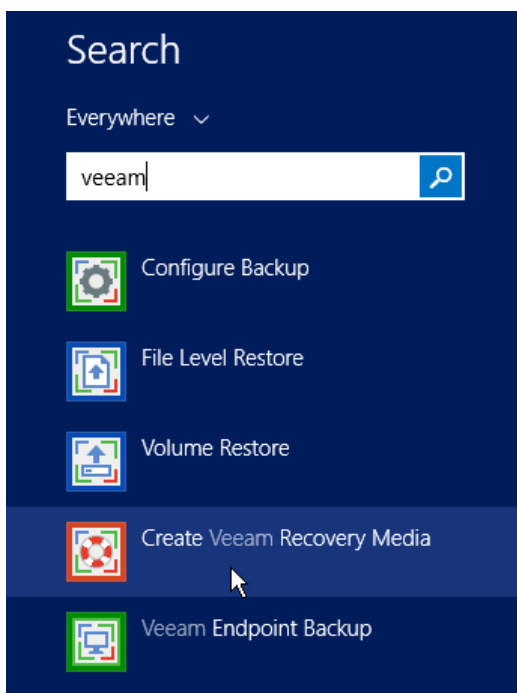
You can launch the **Create Veeam Recovery Media** wizard right after the product installation process or at any time later.

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 Endpoint Backup will automatically launch the **Create Veeam Recovery Media** 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.



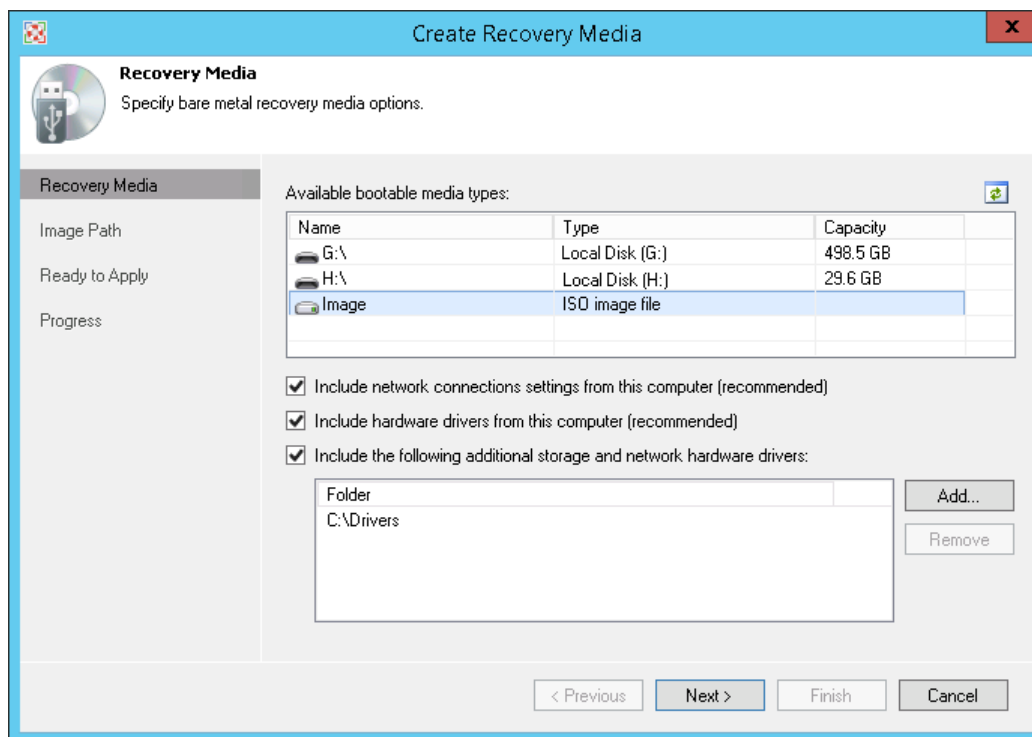
Step 2. Specify Recovery Media Options

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 Endpoint Backup 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 Endpoint Backup 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 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.
3. 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 Endpoint Backup 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.
4. 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.

Important! 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 Endpoint Backup injects all drivers in the Veeam Recovery Media into Windows RE and loads Windows RE 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.

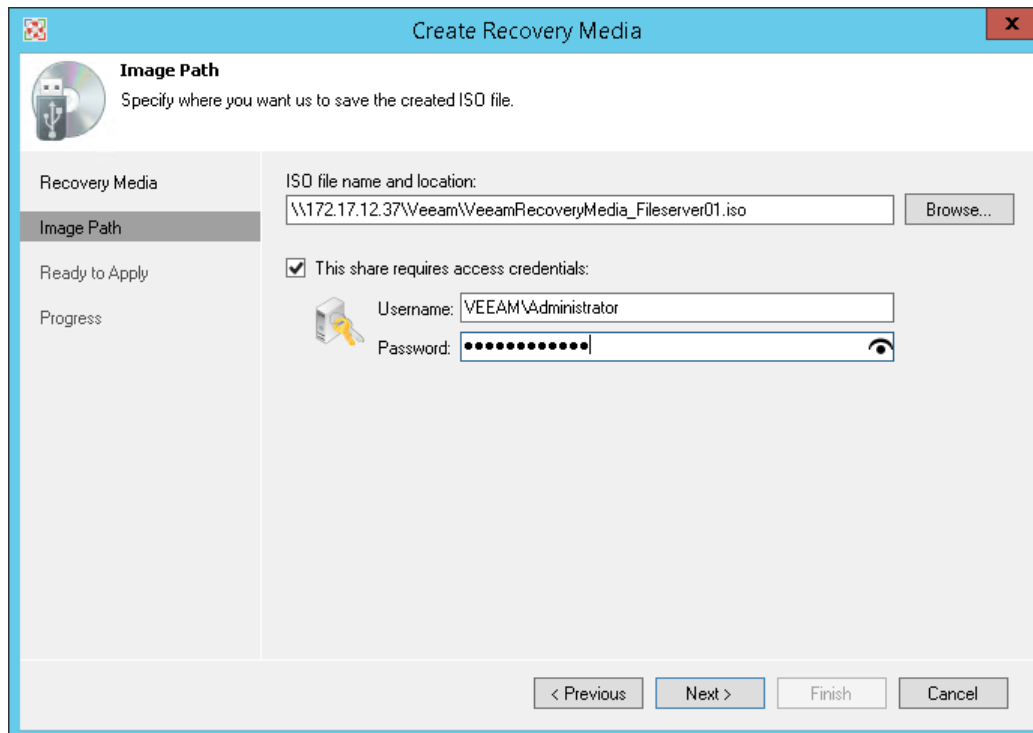
Select a location where you want to save the ISO file.

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.



The screenshot shows the 'Create Recovery Media' wizard window. The title bar is blue with the text 'Create Recovery Media' and a close button. The main window has a light blue header with a USB icon and the text 'Image Path' and 'Specify where you want us to save the created ISO file.' Below the header is a sidebar with four items: 'Recovery Media', 'Image Path' (selected), 'Ready to Apply', and 'Progress'. The main area contains the following fields and controls:

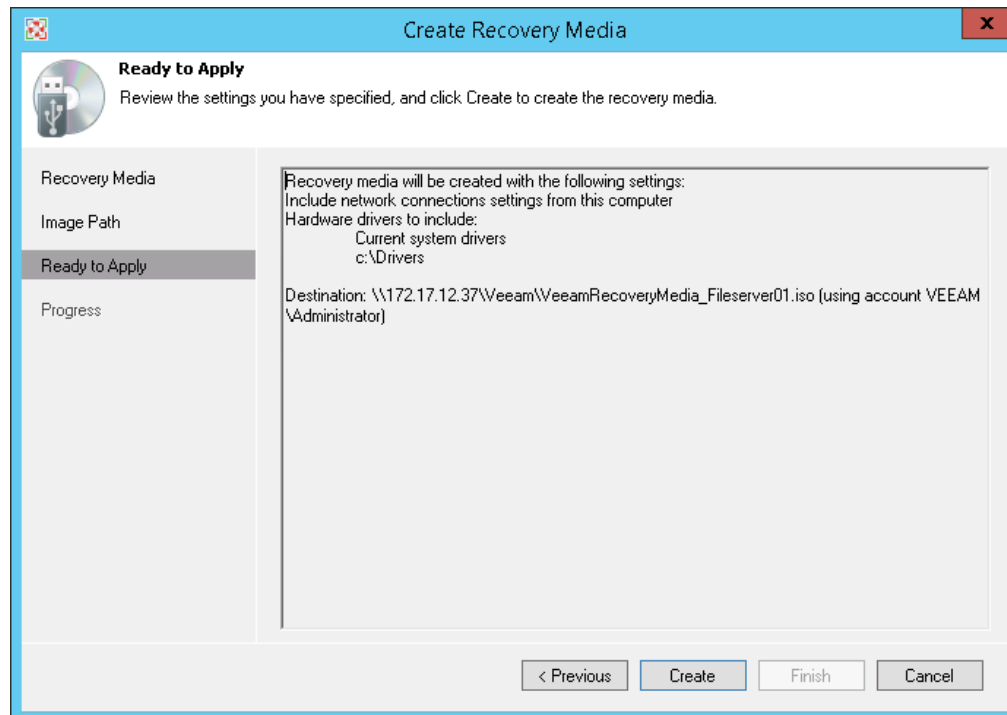
- 'ISO file name and location:' label above a text box containing '\\172.17.12.37\Veeam\VeeamRecoveryMedia_Filesaver01.iso' and a 'Browse...' button.
- A checked checkbox labeled 'This share requires access credentials:'.
- A 'Username:' label above a text box containing 'VEEAM\Administrator'.
- A 'Password:' label above a text box filled with dots, with an eye icon to its right.

At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Review Recovery Image Settings

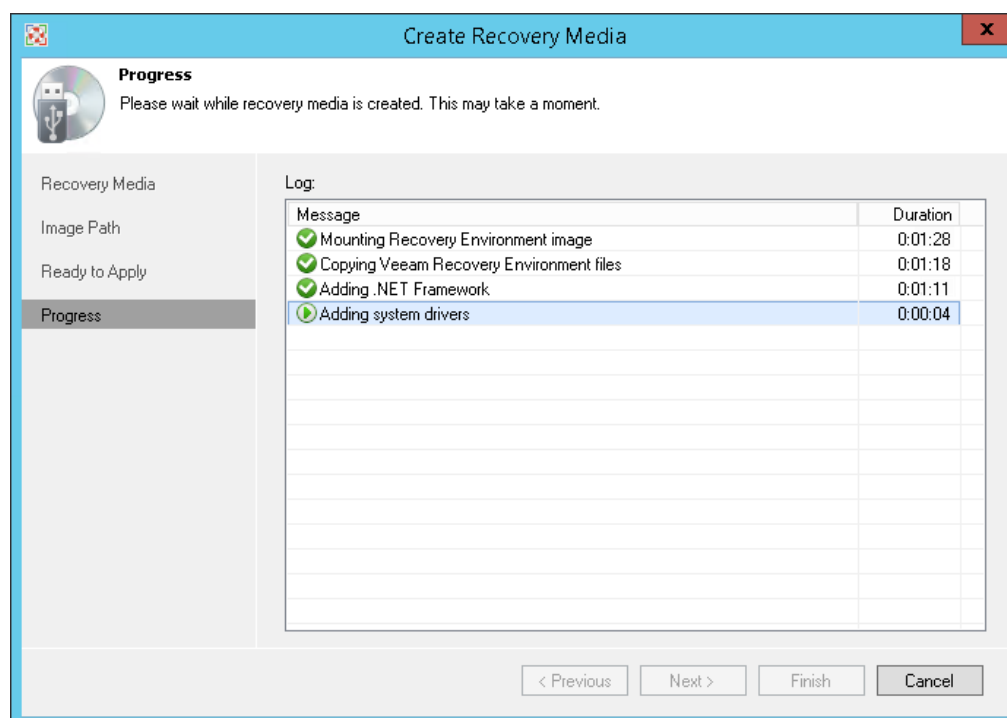
At the **Ready to Apply** step of the wizard, review settings of the recovery image that you plan to create and click **Create**.

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



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

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



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 Endpoint Backup lets you configure a scheduled backup job with the default settings right after the product installation, configure a scheduled 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 Endpoint Backup to auto-configure the scheduled backup job with the default settings. The backup job will have the following settings:

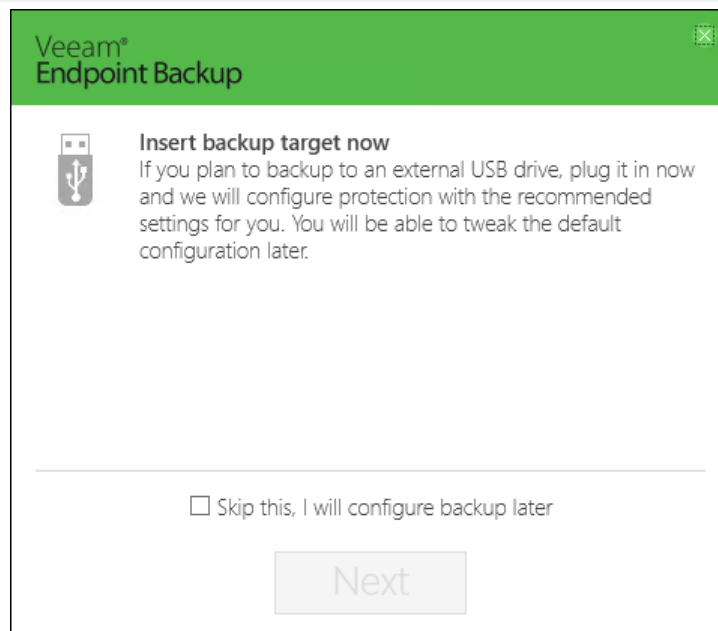
- Backup scope: entire computer
- Target destination: USB drive connected to the computer
- Schedule: 12:30 AM nightly

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.



Configuring Scheduled Backup Job

You can configure the backup job that will automatically back up your data by the defined schedule. 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.
- [For Veeam Backup & Replication repository targets] You can store created backups in a backup repository only if the backup server runs Veeam Backup & Replication 8.0 Update 2 or later.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. To learn more, see [Setting Up User Permissions on Backup Repositories](#).

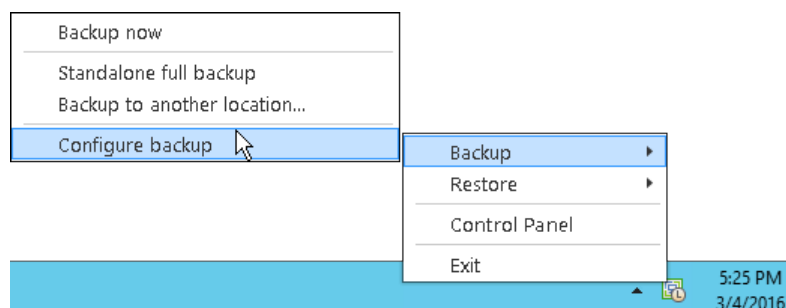
Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Endpoint Backup 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 Endpoint Backup icon in the system tray.
- Right-click the Veeam Endpoint Backup 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.



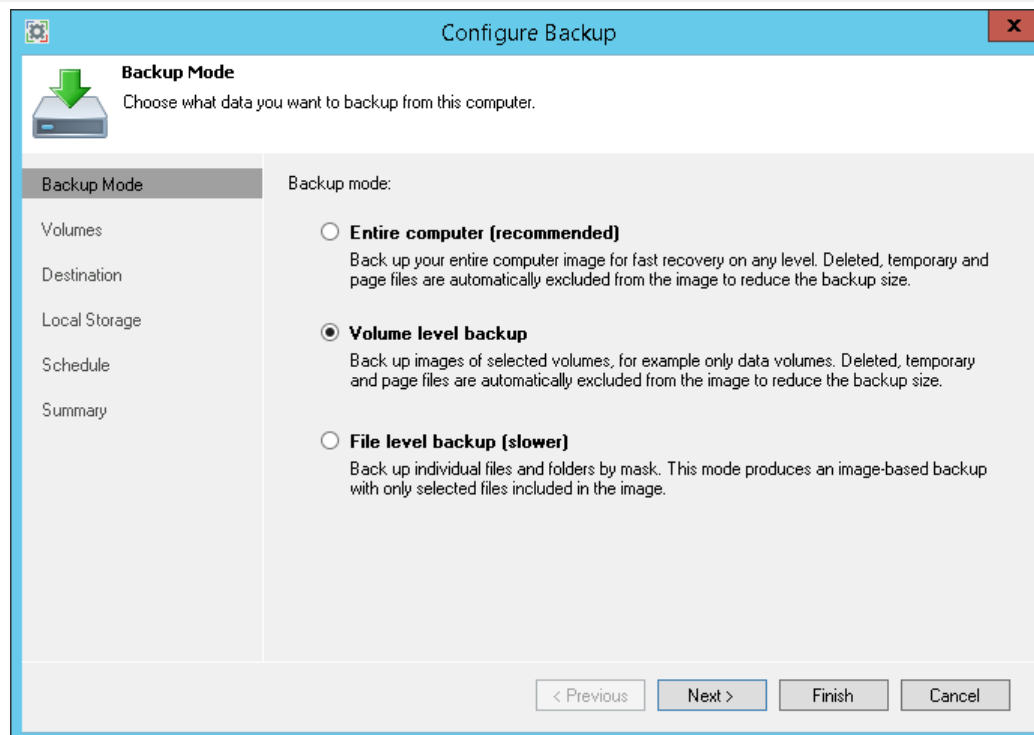
Step 2. Select Backup Mode

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. If you plan to back up all folders with files on a specific volume, it is recommended that you configure volume-level backup instead of file-level backup.



Step 3. Select 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.

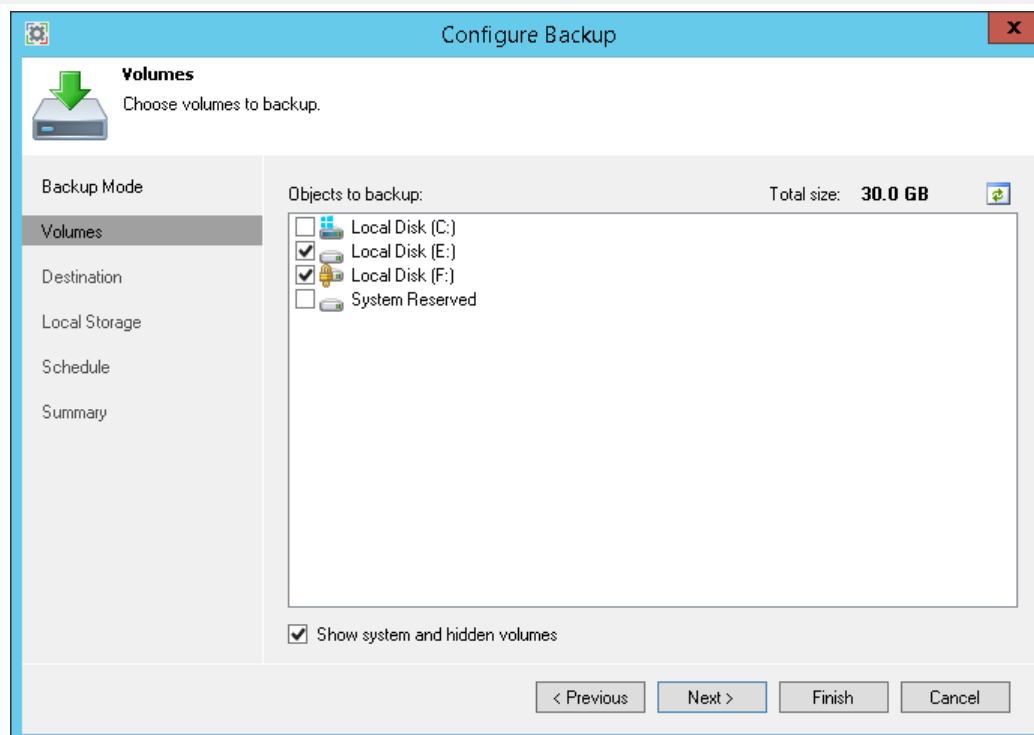
You can back up the following data:

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



Step 4. Select 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.

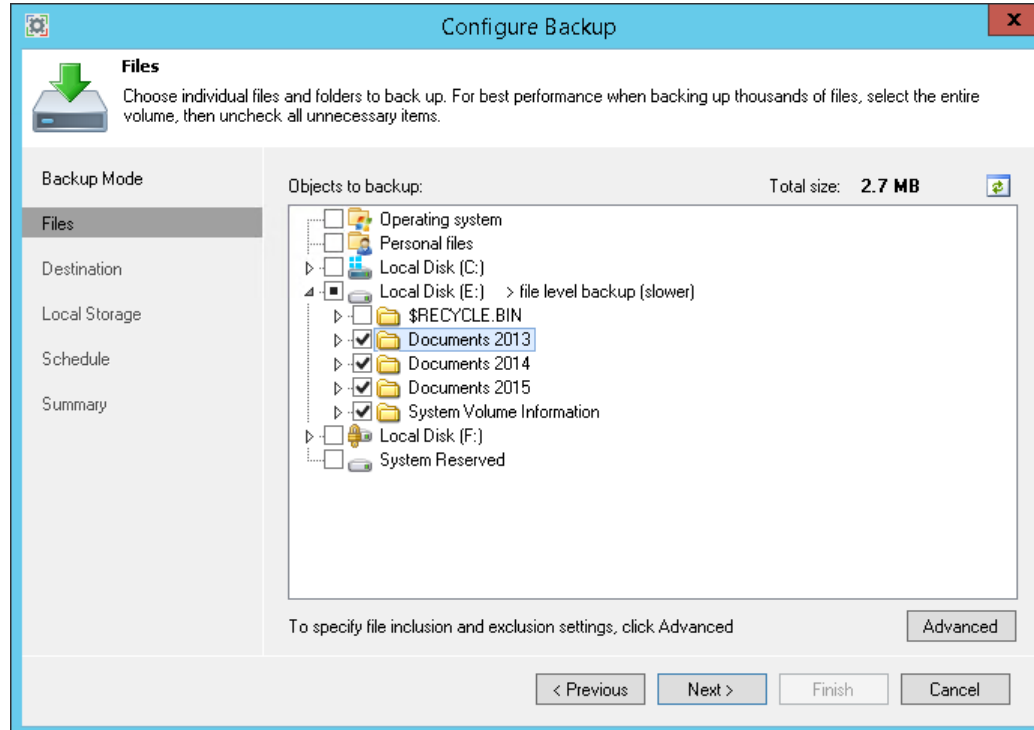
In the file-level backup mode, you can create two types of backups:

- 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 Endpoint Backup 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 Endpoint Backup will additionally back up the recovery partition. To learn more, see [System State Data Backup](#).
- Individual folders.
- Individual computer volumes.

Note: Veeam Endpoint Backup 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.



Configuring Filters

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

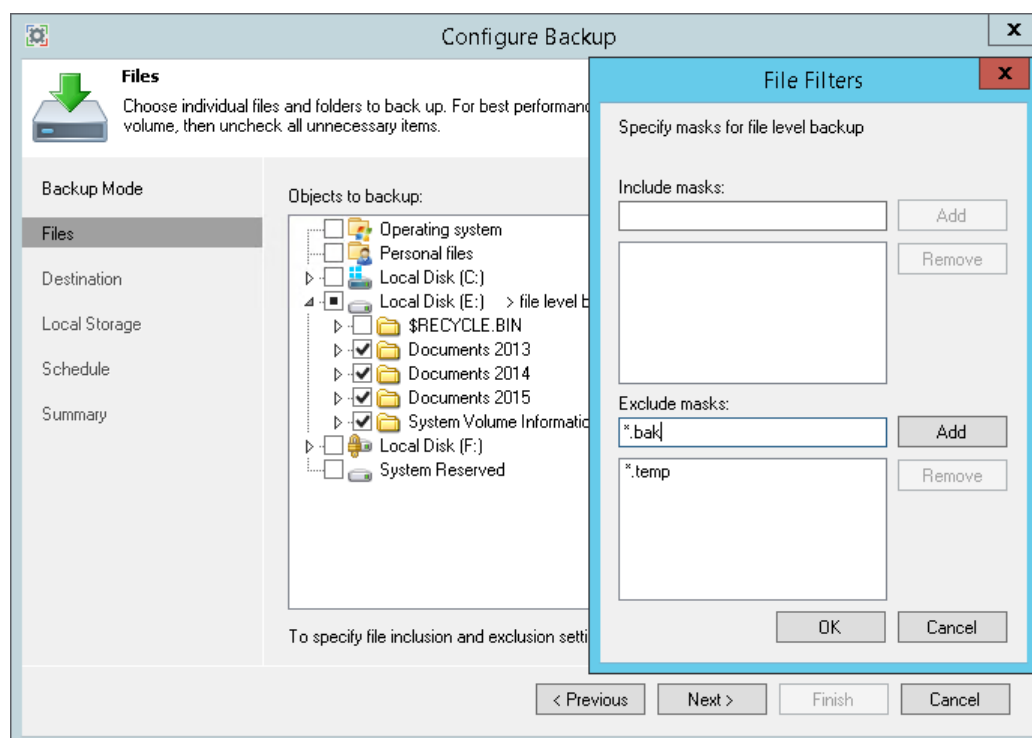
To configure a filter:

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



Step 5. Select Backup Destination

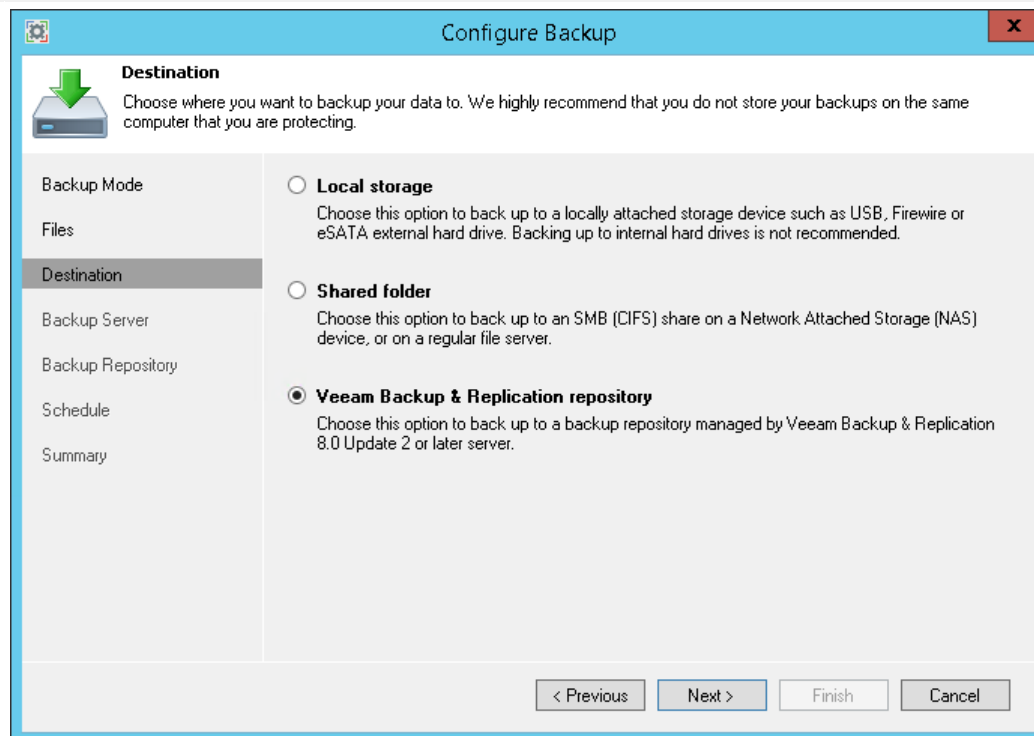
At the **Destination** step of the wizard, select a target location for the created backup.

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

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

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.

Important! If you select to store the backup on a local folder included in the backup scope, Veeam Endpoint Backup will automatically exclude this folder from the backup.



Step 6. Specify Local Storage Settings

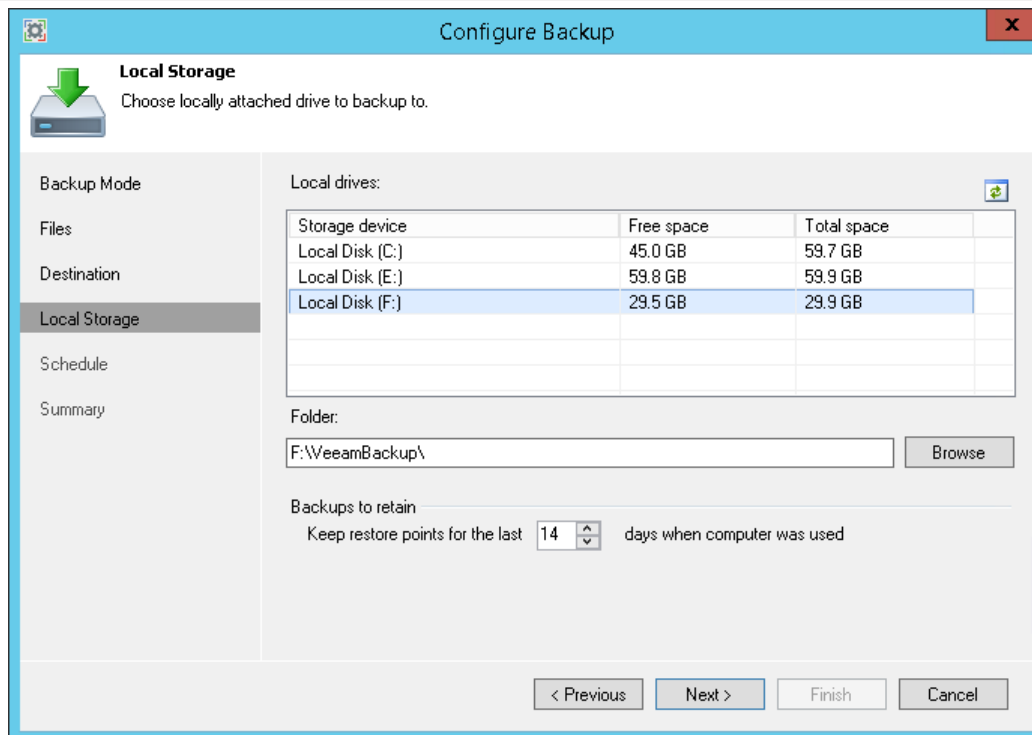
The **Local Storage** step of the wizard is available if you have chosen to save the backup on a local drive of your computer.

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 Endpoint Backup saves files in the `VeeamBackup` folder.
3. 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 Endpoint Backup keeps backup files for 14 days. After this period is over, Veeam Endpoint Backup will remove the earliest restore points from the backup chain.

To learn more, see [Backup Retention Policy](#).

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.



Configure Backup

Local Storage
Choose locally attached drive to backup to.

Backup Mode
Files
Destination
Local Storage
Schedule
Summary

Local drives:

Storage device	Free space	Total space
Local Disk (C:)	45.0 GB	59.7 GB
Local Disk (E:)	59.8 GB	59.9 GB
Local Disk (F:)	29.5 GB	29.9 GB

Folder:
F:\VeeamBackup\ Browse

Backups to retain
Keep restore points for the last days when computer was used

< Previous Next > Finish Cancel

Step 7. Specify 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 Endpoint Backup 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 Endpoint Backup 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\$*).

1. To view how much free space is available in the selected shared folder, click **Populate**.
2. 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 Endpoint Backup keeps backup files for 14 days. After this period is over, Veeam Endpoint Backup will remove the earliest restore points from the backup chain.

To learn more, see [Backup Retention Policy](#).

The screenshot shows the 'Configure Backup' wizard window with the 'Shared Folder' step selected. The window has a blue title bar and a sidebar on the left with options: Backup Mode, Files, Destination, Shared Folder (selected), Schedule, and Summary. The main area contains the following fields and controls:

- Shared folder:** A text box containing '\\172.17.25.37\Veeam' with a 'Browse...' button to its right.
- Free Space:** A disk icon followed by '251.1 GB free of 315.6 GB' and a 'Populate' button.
- Authentication:** A checked checkbox labeled 'This share requires access credentials:'.
- Username:** A text box containing 'VEEAM\Administrator'.
- Password:** A text box with masked characters (dots) and an eye icon to toggle visibility.
- Backups to retain:** A section with the text 'Keep restore points for the last' followed by a spinner box set to '14' and the text 'days when computer was used'.

At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 8. Specify Backup Server Settings

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

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

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. 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 Endpoint Backup 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 Endpoint 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 Endpoint Backup must communicate with the backup repository. By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will fail to connect to the Veeam backup server.

The screenshot shows the 'Configure Backup' wizard window. The 'Backup Server' step is selected in the left sidebar. The main area contains the following fields and options:

- Veeam backup server name or IP address:** 172.17.53.12
- ☒ **Specify your personal credentials:**
- Username:** VEEAM\Administrator
- Password:** (masked with dots)
- Port:** 10001

At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 9. Select Backup Repository

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

Important! You cannot use a scale-out backup repository as a target for the Veeam Endpoint Backup job.

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 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. 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 Endpoint Backup keeps backup files for 14 days. After this period is over, Veeam Endpoint Backup will remove the earliest restore points from the backup chain.

To learn more, see [Backup Retention Policy](#).

The screenshot shows the 'Configure Backup' wizard window. The 'Backup Repository' step is selected in the left sidebar. The main area displays the following settings:

- Backup repository:** A dropdown menu showing 'Backup Volume 01'. A refresh icon is visible to the right of the dropdown.
- Destination:** A disk icon followed by the text '1.2 TB free of 4.1 TB'.
- Backups to retain:** A section with the label 'Keep restore points for the last' followed by a spinner box set to '14' and the text 'days when computer was used'.

At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 10. Specify Backup Schedule

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 Endpoint Backup 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 Endpoint Backup to start the scheduled backup job when you power on the computer.
 - *Skip backup* — select this option if you want Veeam Endpoint Backup not to start the scheduled backup job when the computer is powered on. Veeam Endpoint Backup will perform backup at the next scheduled time.
4. If you want Veeam Endpoint Backup 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 Endpoint Backup to bring your computer to the standby mode.
 - *Shutdown* — select this option if you want Veeam Endpoint Backup to shut down your computer.
 - *Hibernate* — select this option if you want Veeam Endpoint Backup 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 Endpoint Backup applies this setting only to scheduled backups. If you start standalone full backup or incremental backup manually, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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**.

Important! If the power scheme on your computer does not allow using wake up timers, Veeam Endpoint Backup will ask you to change the power scheme settings. Click **Yes** to allow Veeam Endpoint Backup 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**.

Configure Backup

Schedule
Choose when you want backup job to be started automatically.

Backup Mode
Volumes
Destination
Shared Folder
Schedule
Summary

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 shutdown at this time Backup once powered on

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)

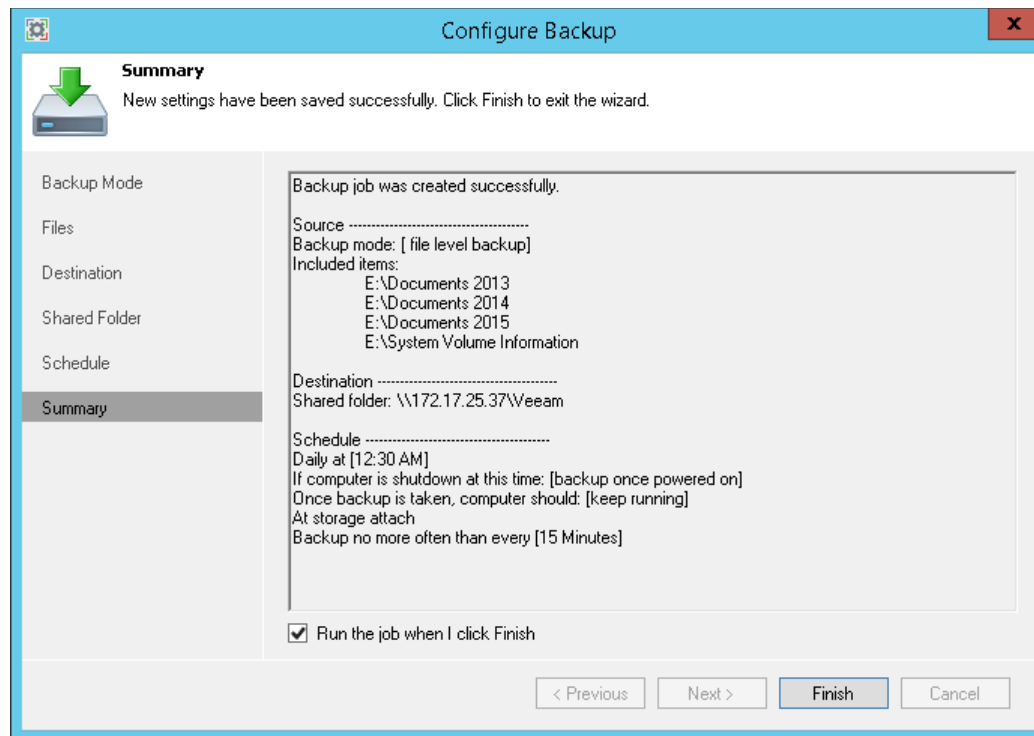
Back up no more often than every 2 Hour

< Previous Save Finish Cancel

Step 11. 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**.



What You Do Next

After you configure the scheduled backup job, Veeam Endpoint Backup displays a clock over its icon in the system tray. The clock identifies that your computer is protected with the scheduled backup job. Veeam Endpoint Backup 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

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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will perform full data backup. All subsequent backup sessions will produce incremental backups — Veeam Endpoint Backup 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 Endpoint Backup 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.

Disabling and Enabling 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.

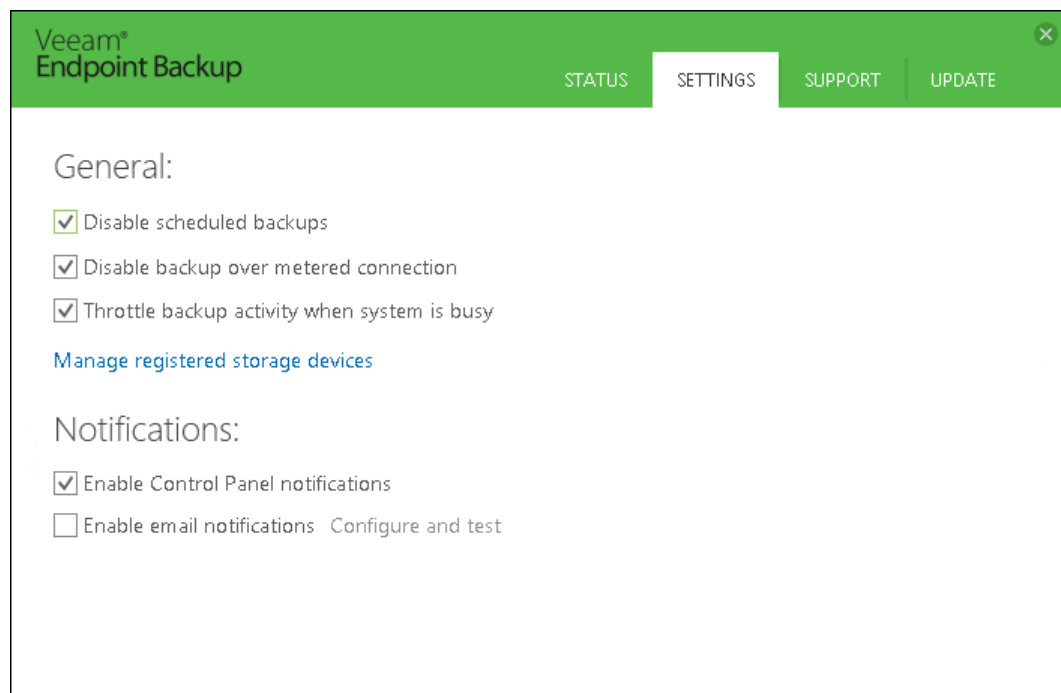
The disabling option is applicable only to the scheduled backup job. You can create standalone full backups and perform ad-hoc incremental backup even if the backup job is disabled.

To disable the scheduled backup job:

1. Double-click the Veeam Endpoint Backup 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 Endpoint Backup 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.



Controlling Backup Post-Job Action

You can set up Veeam Endpoint Backup to perform a finalizing action after the backup job completes successfully:

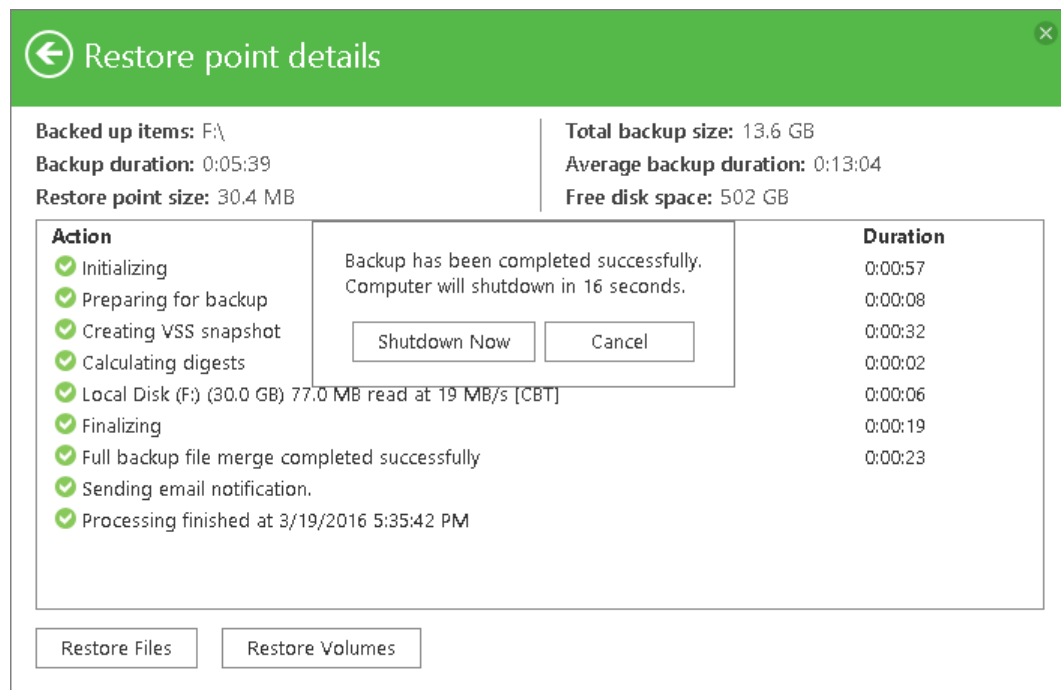
- *Sleep* — bring your computer to the standby mode.
- *Hibernate* — bring your computer to the hibernate mode.
- *Shutdown* — shut down your computer.

To learn more, see [Specify Backup Schedule](#).

When the backup job completes, Veeam Endpoint Backup 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 Endpoint Backup will perform the specified action when timeout expires.



Deleting Backups

Backup files created with Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will produce a new full backup. All subsequent backups will be incremental.

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 Endpoint Backup lets you perform the following types of ad-hoc backups:

- [Standalone full backup](#)
- [Backup to another location](#)
- [Incremental ad-hoc backup](#)

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:

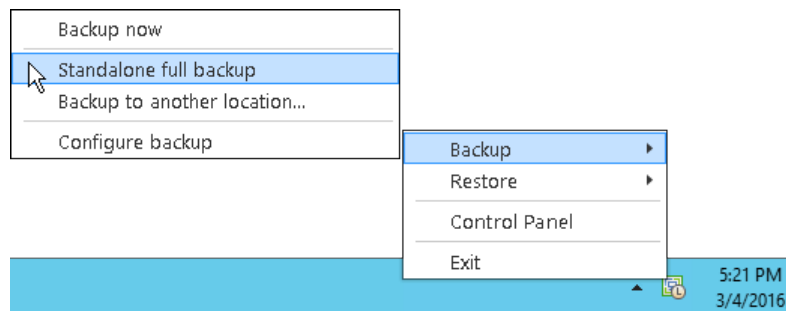
- The backup job must be configured.
- You cannot create a standalone full backup if a backup task of any type is currently running. This includes a scheduled backup, standalone full backup or ad-hoc incremental backup.

To create a standalone full backup:

1. Right-click the Veeam Endpoint Backup icon in the system tray.
2. Select **Backup > Standalone full backup**. Veeam Endpoint Backup 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

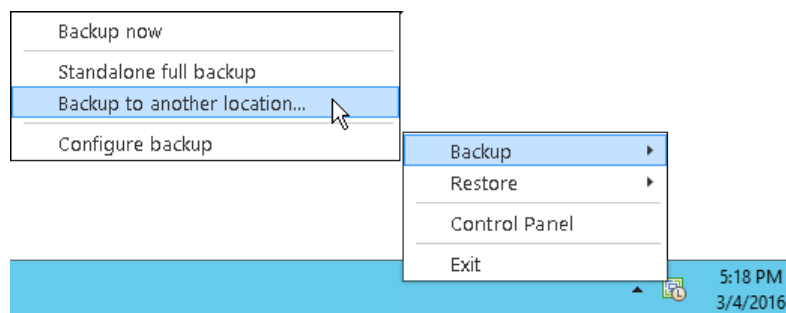
You can create a standalone full backup in a separate location that is not specified as a target location in the backup job settings. Performing backup to another location is similar to creating regular standalone full backups. The main difference is that you must manually select a target location in which Veeam Endpoint Backup will save the backup file.

Before you perform backup to another location, check the following prerequisites:

1. The backup job must be configured.
2. 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 or ad-hoc incremental backup.

To perform backup to another location:

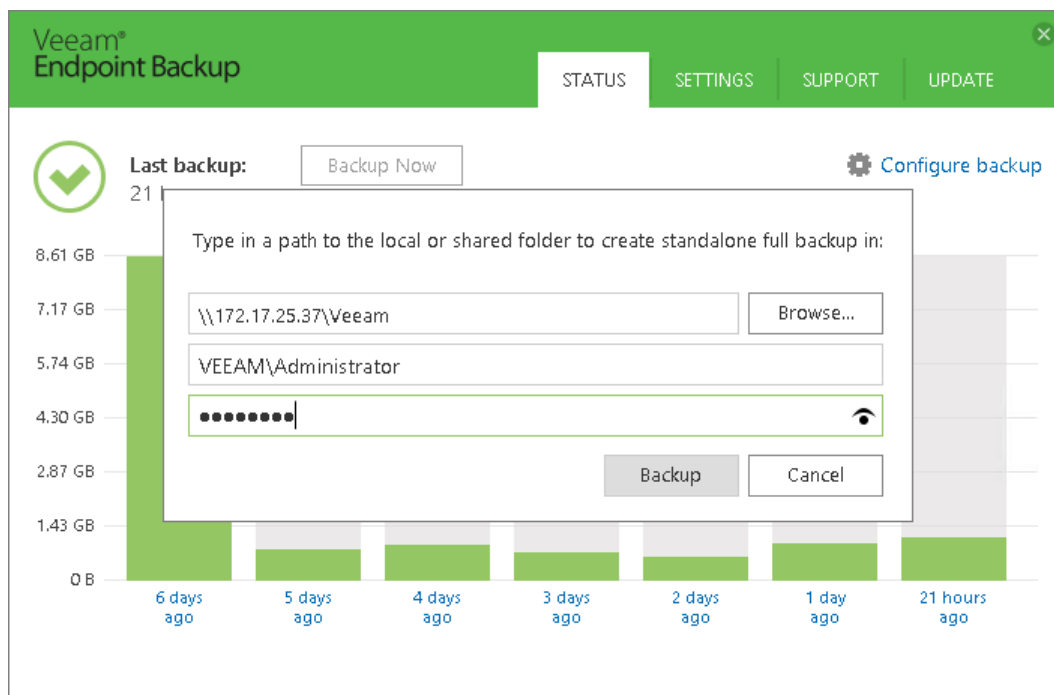
1. Right-click the Veeam Endpoint Backup icon in the system tray.
2. Select **Backup > Backup to another location**.



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 Endpoint Backup 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>.



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.

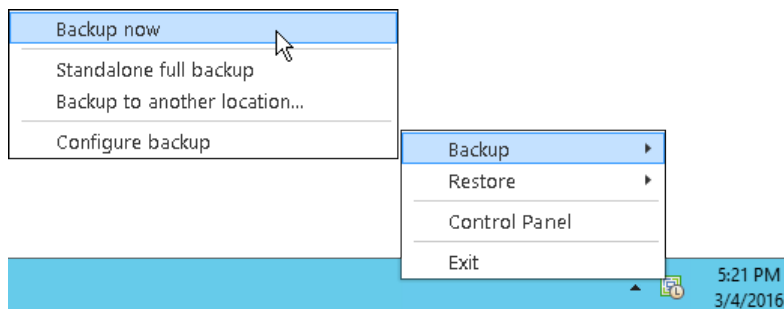
Before you perform ad-hoc incremental backup, check the following prerequisites:

- 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 or ad-hoc incremental backup.

To perform ad-hoc incremental backup, do one of the following:

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

Veeam Endpoint Backup 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.



Performing Backup with Command Line Interface

In addition to running scheduled backup jobs and performing ad-hoc backups from the Veeam Endpoint Backup 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.

Creating Incremental Backups

To perform an incremental 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! If you specify a network shared folder as a target location for standalone full backup, Veeam Endpoint Backup will use credentials that are specified in the backup job settings to connect to the shared folder. You cannot specify custom credentials 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 Endpoint Backup 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

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 Endpoint Backup 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 Endpoint Backup or standard Microsoft Windows tools to diagnose problems and fix errors. You can also use a backup created with Veeam Endpoint Backup 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 Endpoint Backup or system image created with Microsoft Windows. Make sure that the backup or system image is available on the computer drive (local or external), a network shared folder or on the backup repository managed by a Veeam backup server.
- 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.

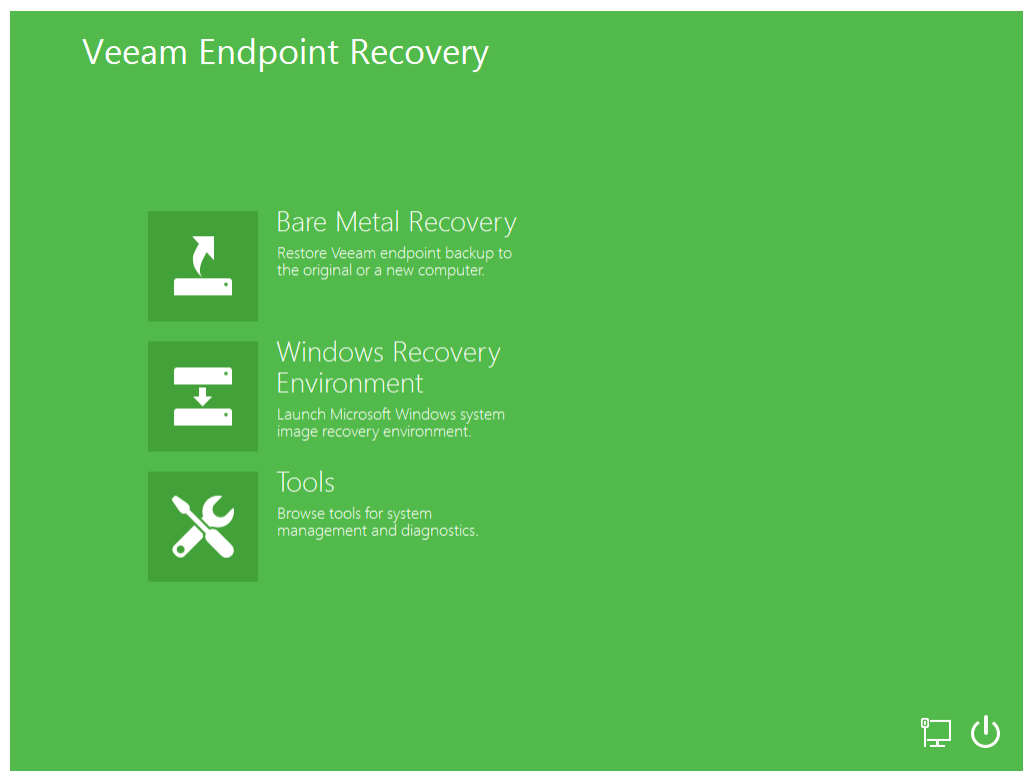
Mind the following:

- When you create a Veeam Recovery Media, Veeam Endpoint Backup 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 Endpoint Recovery** 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 Endpoint Recovery** 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 Endpoint Backup 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 Endpoint Backup offers the following tools:
 - **Bare Metal Recovery** — the Veeam Endpoint Backup 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 Endpoint Backup and Microsoft Windows utilities for advanced computer administration.



Tip:

To shut down or restart your computer, click the **Power Options** button at the bottom right corner of the **Veeam Endpoint Recovery** screen and select the necessary option: **Shut down** or **Restart**.

Step 2. Select Network Adapter or Wireless Network

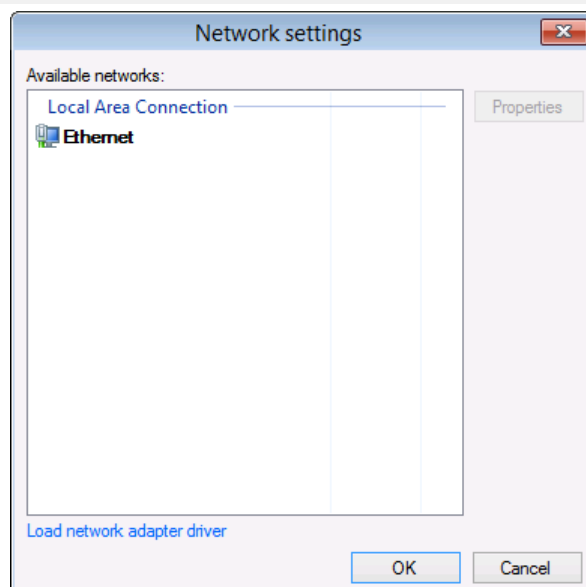
To open the **Network settings** window, click the **Network Settings** button at the bottom right corner of the **Veeam Endpoint Recovery** screen.

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 Endpoint Backup 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 TCP/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 Endpoint Backup does not detect available networks and there are no network settings included in the Veeam Recovery Media.



Installing Network Adapter Drivers

The list of networks can be empty. This can happen in two situations:

- The driver for the network adapter is included in the Veeam Recovery Media but failed to be installed automatically for some reason.
- The driver for the network adapter is not included in the Veeam Recovery Media.

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

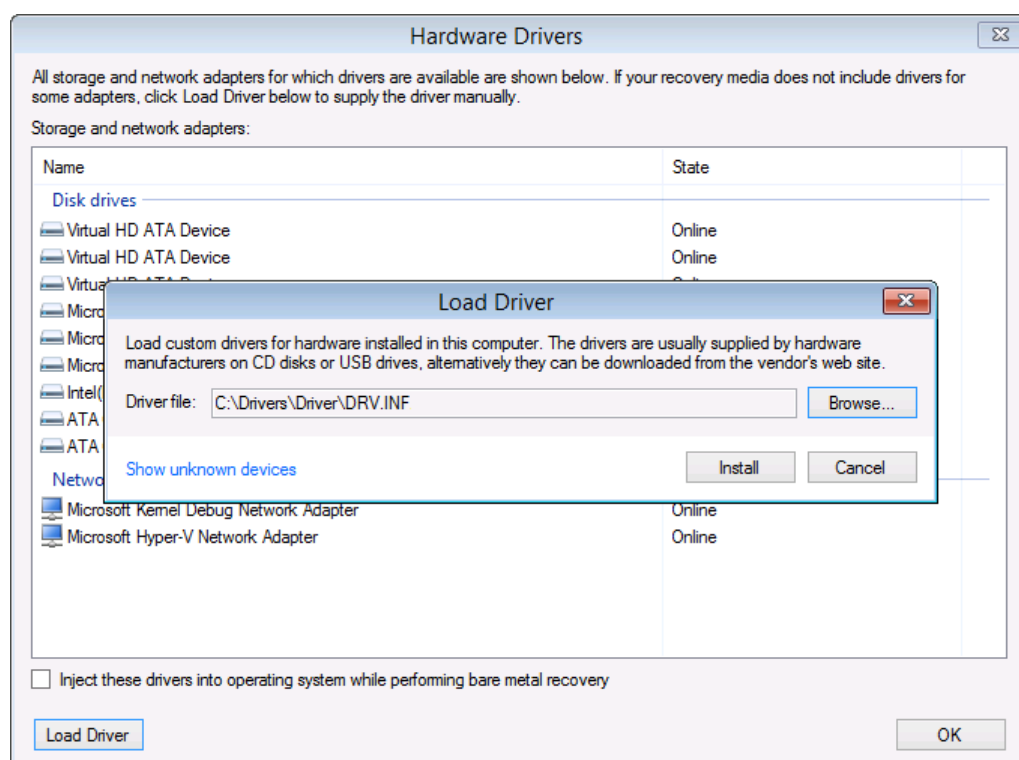
1. At the **Network settings** window, click **Load network adapter driver**.
2. In the **Hardware Drivers** window, select the necessary device.

If you want to include in the restored operating system all the drivers that were saved to the Veeam Recovery Media, select the **Inject these drivers into operating system while performing bare metal recovery** option. In case the option is not selected, the restored operating system will include only default Windows hardware drivers.

1. Click the **Install** link next to the selected device.

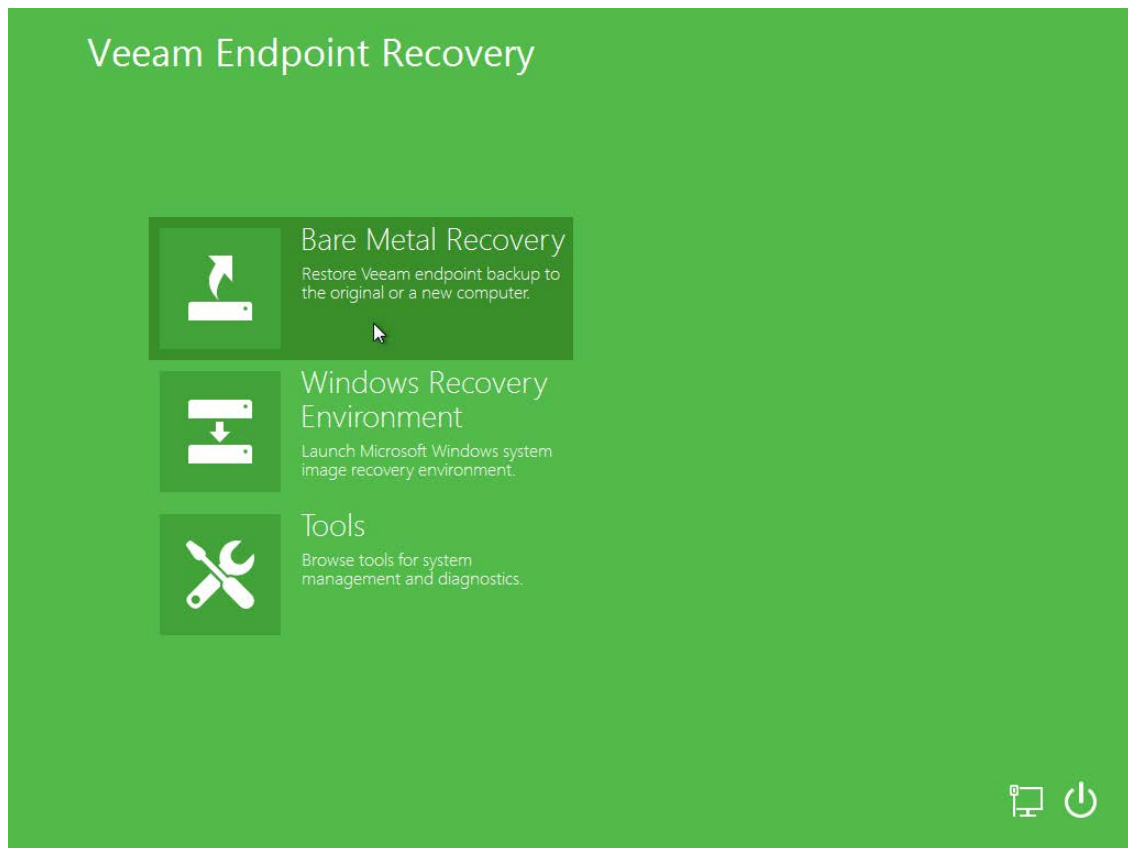
To install drivers that were not included in the Veeam Recovery Media:

1. At the **Network settings** window, click **Load network adapter driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the **Show unknown devices** link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.



Step 3. Launch Veeam Endpoint Recovery Wizard

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

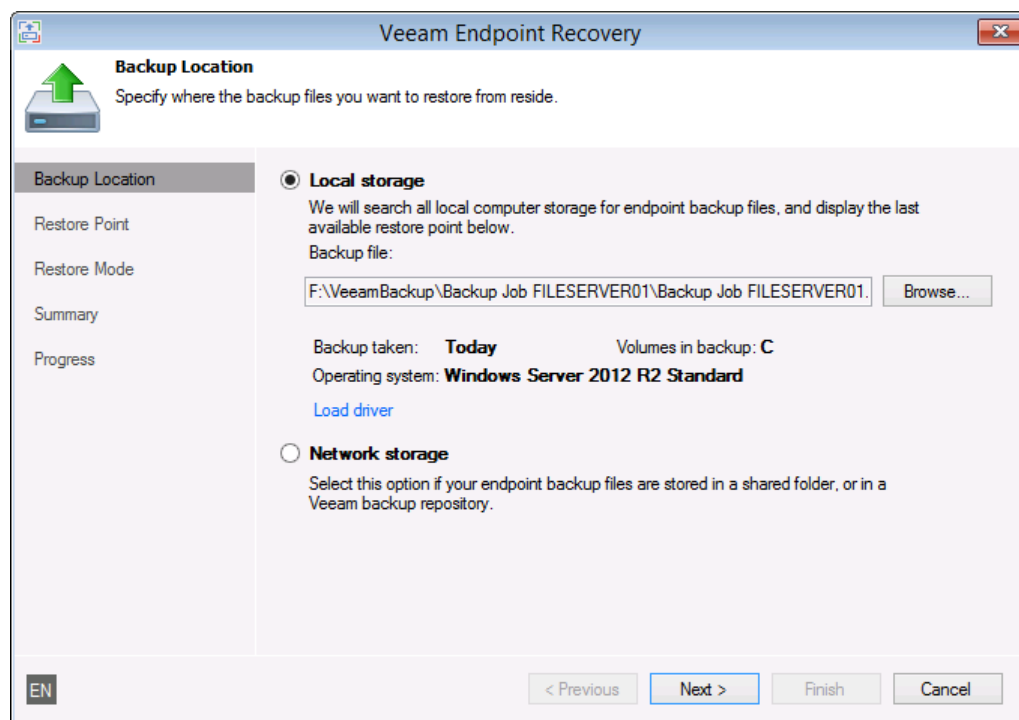


Step 4. Specify Backup File Location

At the **Backup Location** step of the wizard, specify where the backup file that you want to use for data recovery is located.

By default, Veeam Endpoint Backup automatically locates the latest backup on the computer drive and you pass immediately to the **Restore Point** step of the wizard. If Veeam Endpoint Backup fails to locate the backup on the local computer drive for some reason, or the backup file is located in a network shared folder or on a backup 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 is located in a remote location — in a network shared folder or on a Veeam backup repository. In this case, the **Veeam Endpoint Recovery** wizard will include additional steps for specifying the backup file location settings.



Installing Drivers for Remote Storage Devices

A removable storage device with the backup file may not be displayed in the list of devices. This can happen in two situations:

- The driver for the remote storage device is included in the Veeam Recovery Media but failed to be installed automatically for some reason.
- The driver for the remote storage device is not included in the Veeam Recovery Media.

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

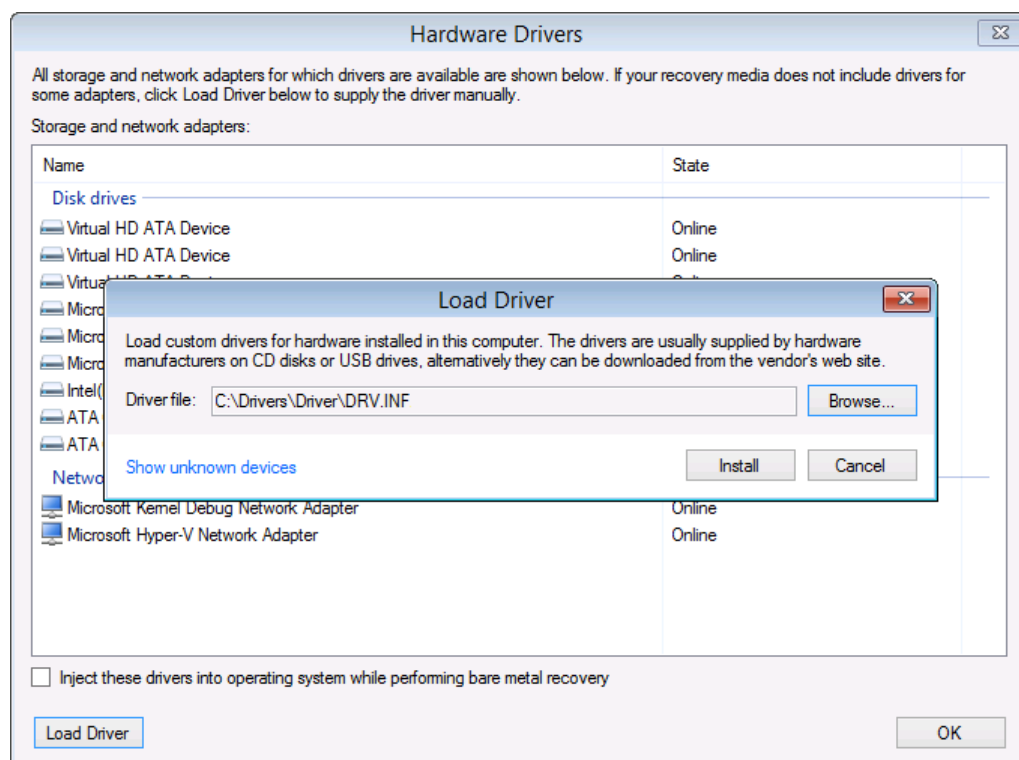
1. At the **Backup Location** step of the wizard, click **Load driver**.
2. In the **Hardware Drivers** window, select the necessary device.

If you want to include in the restored operating system all the drivers that were saved to the Veeam Recovery Media, select the **Inject these drivers into operating system while performing bare metal recovery** option. In case the option is not selected, the restored operating system will include only default Windows hardware drivers.

1. Click the **Install** link next to the selected device.

To install drivers that were not included in the Veeam Recovery Media:

1. At the **Backup Location** step of the wizard, click **Load driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the **Show unknown devices** link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.

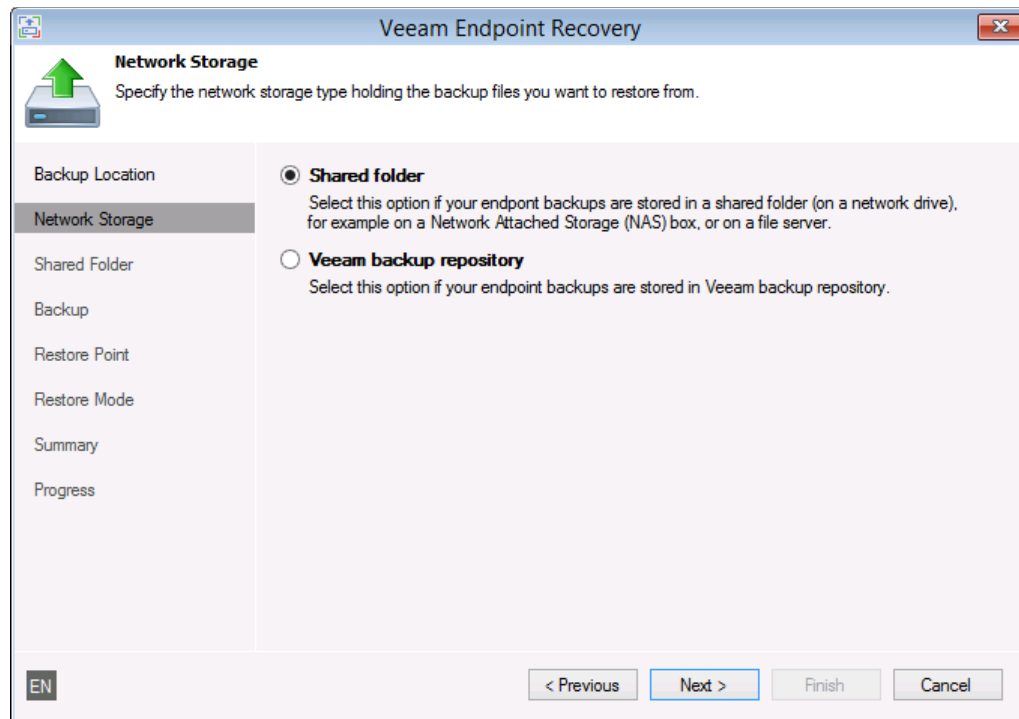


Step 5. Select Remote Storage

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 or on a backup 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.



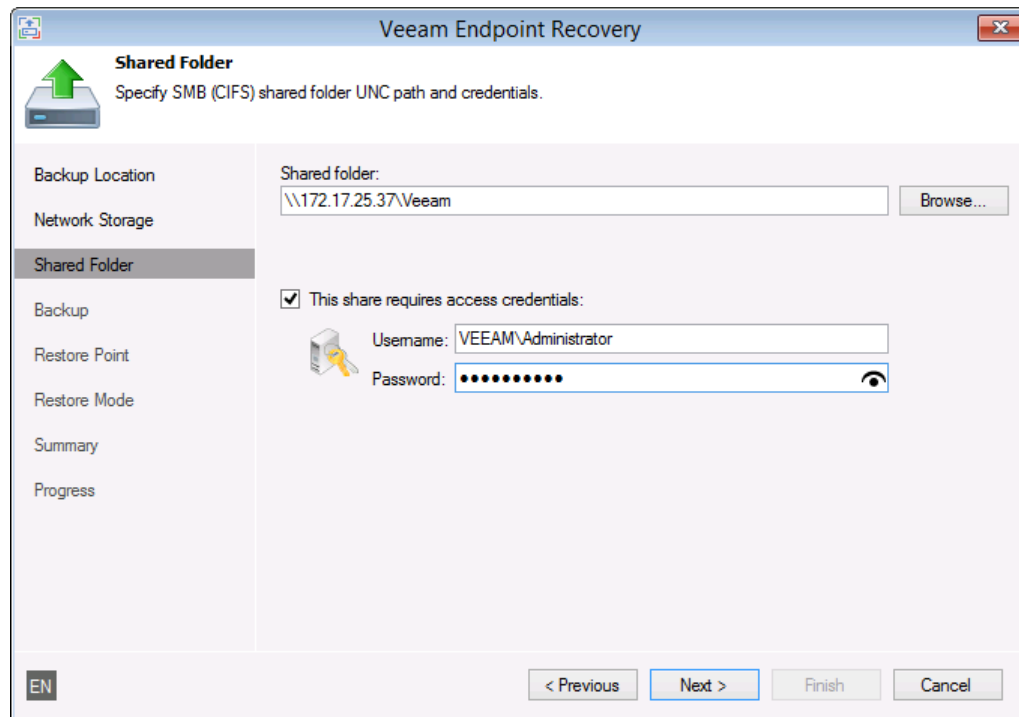
Step 6. Specify Shared Folder Settings

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\USERNAME* format.

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



The screenshot shows the 'Veeam Endpoint Recovery' window with the 'Shared Folder' tab selected. The window title is 'Veeam Endpoint Recovery'. The tab is labeled 'Shared Folder' with a green arrow icon. Below the tab, it says 'Specify SMB (CIFS) shared folder UNC path and credentials.' On the left, there is a sidebar with options: 'Backup Location', 'Network Storage', 'Shared Folder' (selected), 'Backup', 'Restore Point', 'Restore Mode', 'Summary', and 'Progress'. The main area contains the 'Shared folder:' field with the value '\\172.17.25.37\Veeam' and a 'Browse...' button. Below this, there is a checkbox labeled 'This share requires access credentials:' which is checked. To the left of the checkbox is a key icon. Below the checkbox, there are two fields: 'Username:' with the value 'VEEAM\Administrator' and 'Password:' with a masked password '••••••••' and an eye icon to toggle visibility. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'EN' logo is in the bottom left corner.

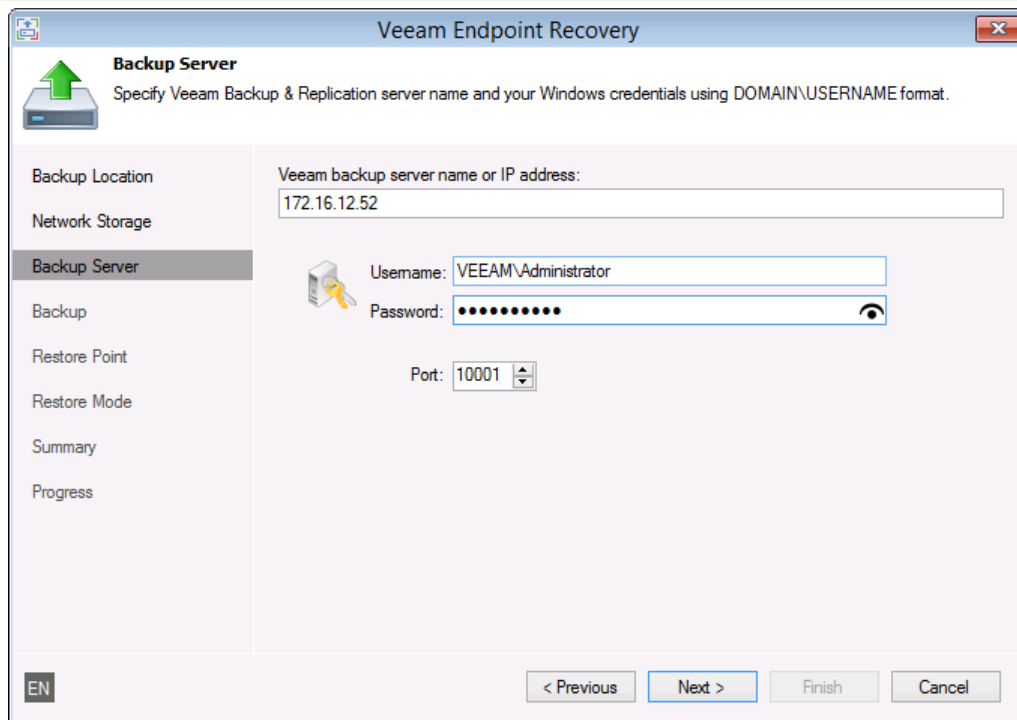
Step 7. Specify Backup Server Settings

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 Endpoint Backup must communicate with the backup repository. By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will fail to connect to the Veeam backup server.



The screenshot shows the 'Veeam Endpoint Recovery' wizard window, specifically the 'Backup Server' step. The window title is 'Veeam Endpoint Recovery'. On the left is a navigation pane with options: Backup Location, Network Storage, Backup Server (selected), Backup, Restore Point, Restore Mode, Summary, and Progress. The main area contains the following fields and instructions:

- Backup Server** (with a green arrow icon): Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.
- Veeam backup server name or IP address:** A text box containing '172.16.12.52'.
- Username:** A text box containing 'VEEAM\Administrator'.
- Password:** A text box with masked characters (dots) and a visibility toggle icon.
- Port:** A spinner box set to '10001'.

At the bottom, there are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel' (disabled). A small 'EN' logo is in the bottom left corner.

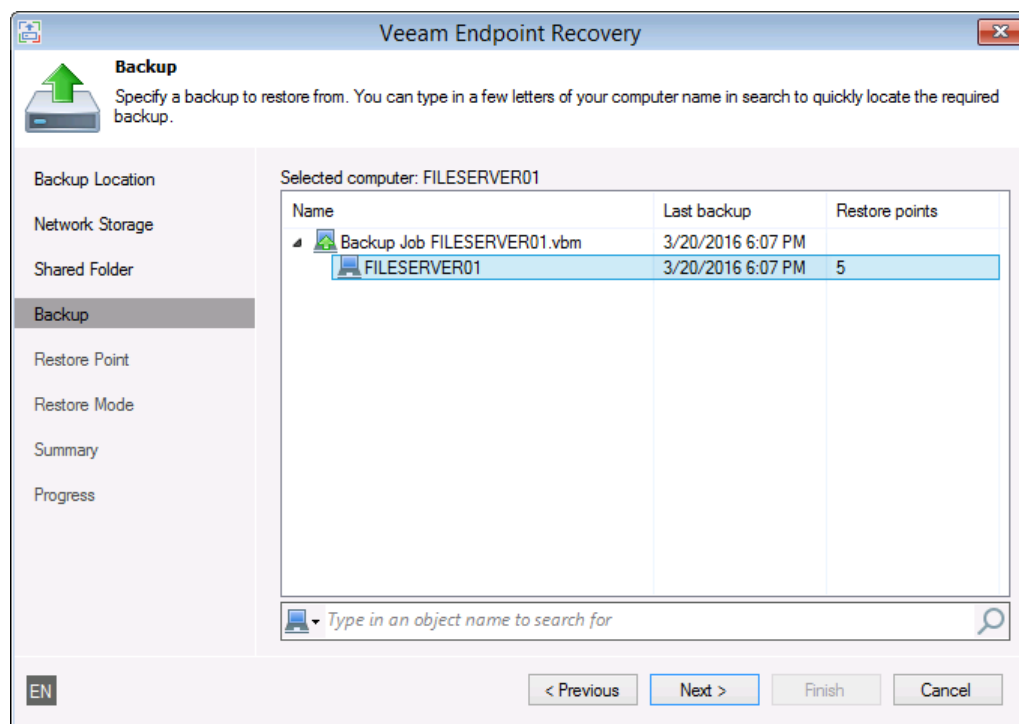
Step 8. Select Backup

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 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 Endpoint Backup 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 Endpoint backups stored on the backup repository.

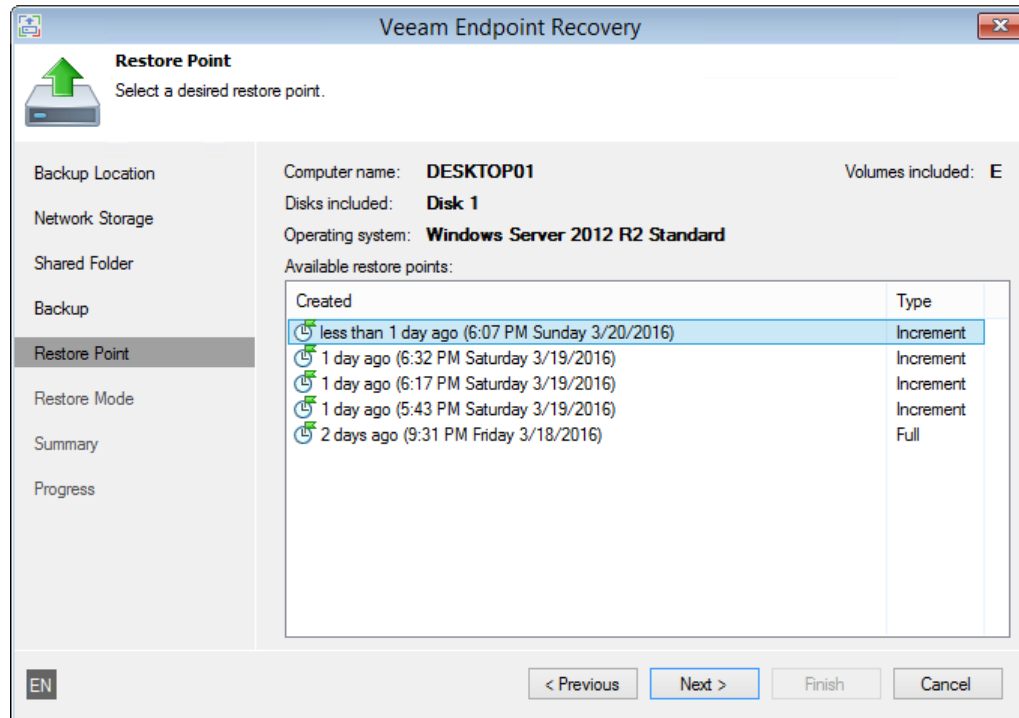


Step 9. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will display only 2 restore points in the list.



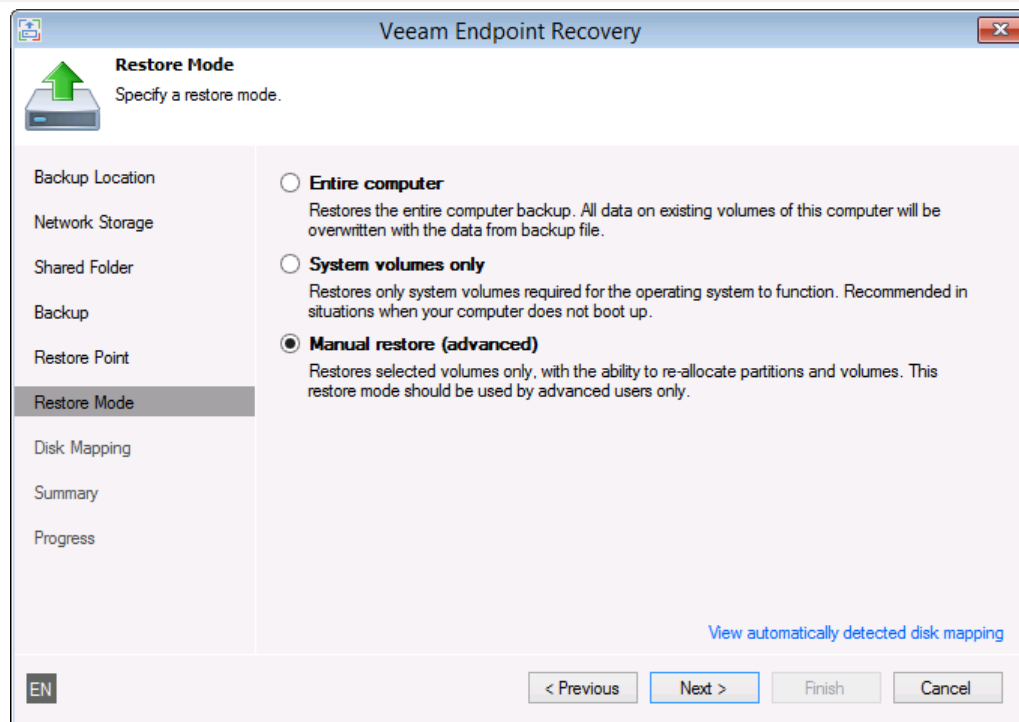
Step 10. Select Data Restore Mode

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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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.



Step 11. Map Restored Disks

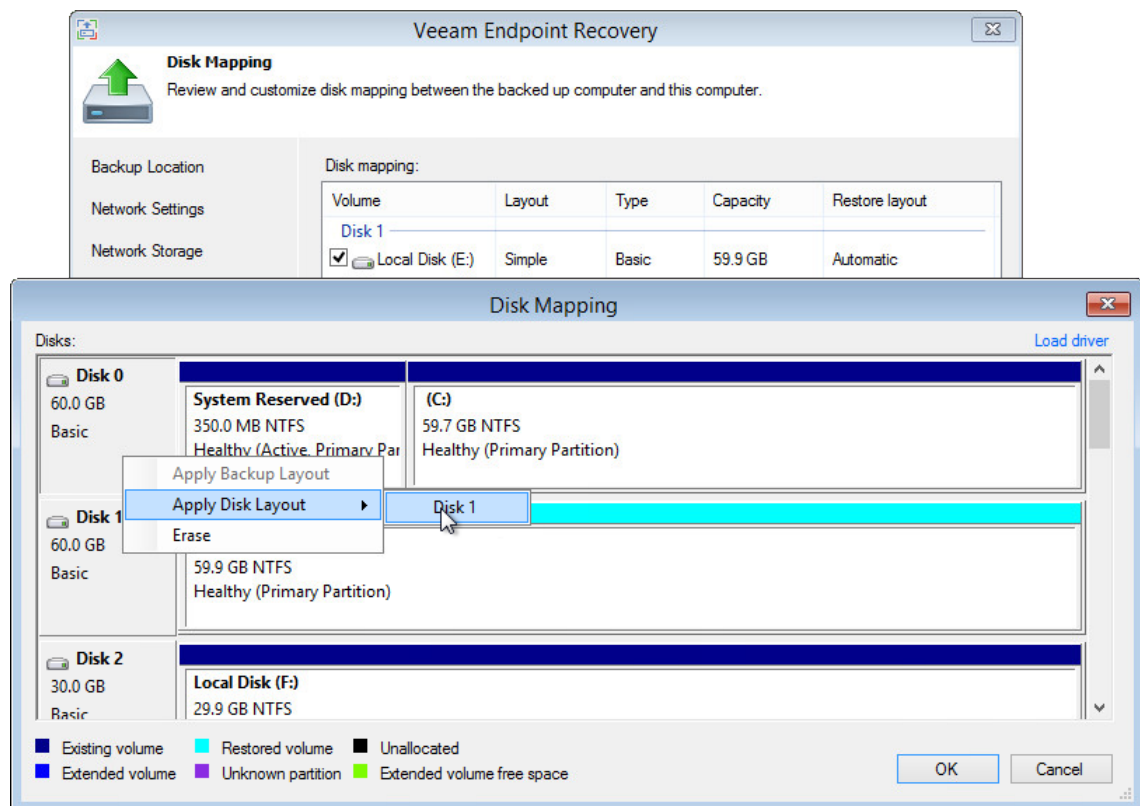
The **Disk Mapping** step of the wizard is available if at the **Restore Mode** step of the wizard you have chosen to restore data in the *Manual* mode.

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.

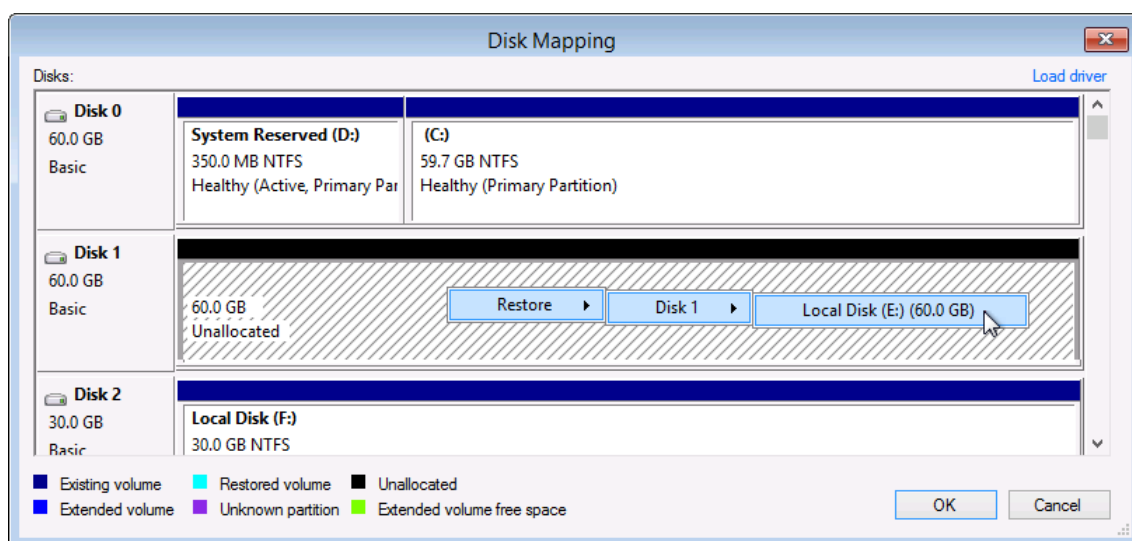
To map volumes:

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 Endpoint Backup 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:
 - a. 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.



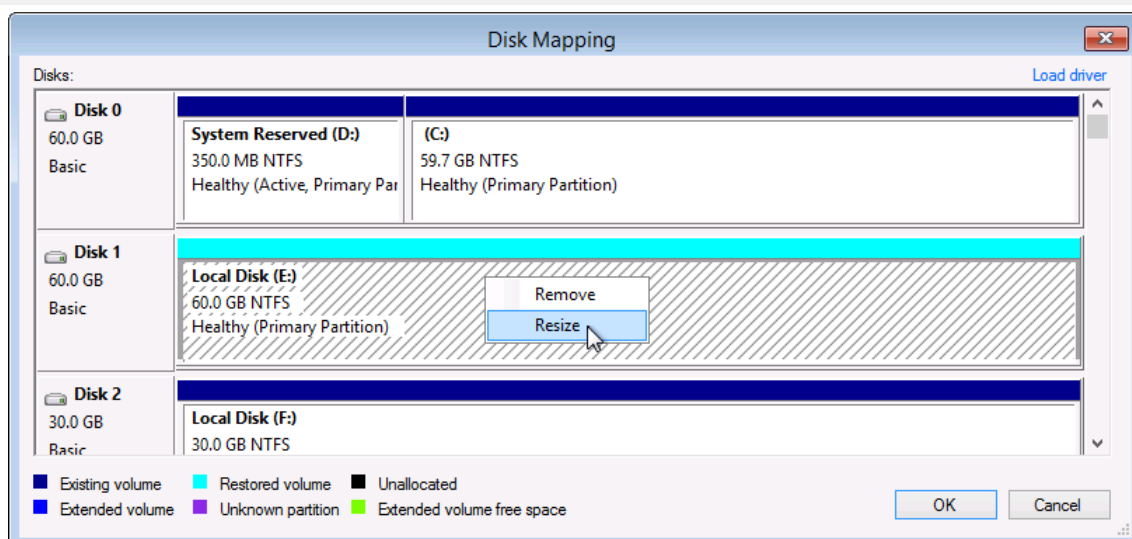
- b. Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

If you want to change disk layout configured by Veeam Endpoint Backup, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



3. [For restore with volume resize] You can resize a volume mapped by Veeam Endpoint Backup 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 Endpoint Backup will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Endpoint Backup will prepare to shrink the volume to the size of available disk space.



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:

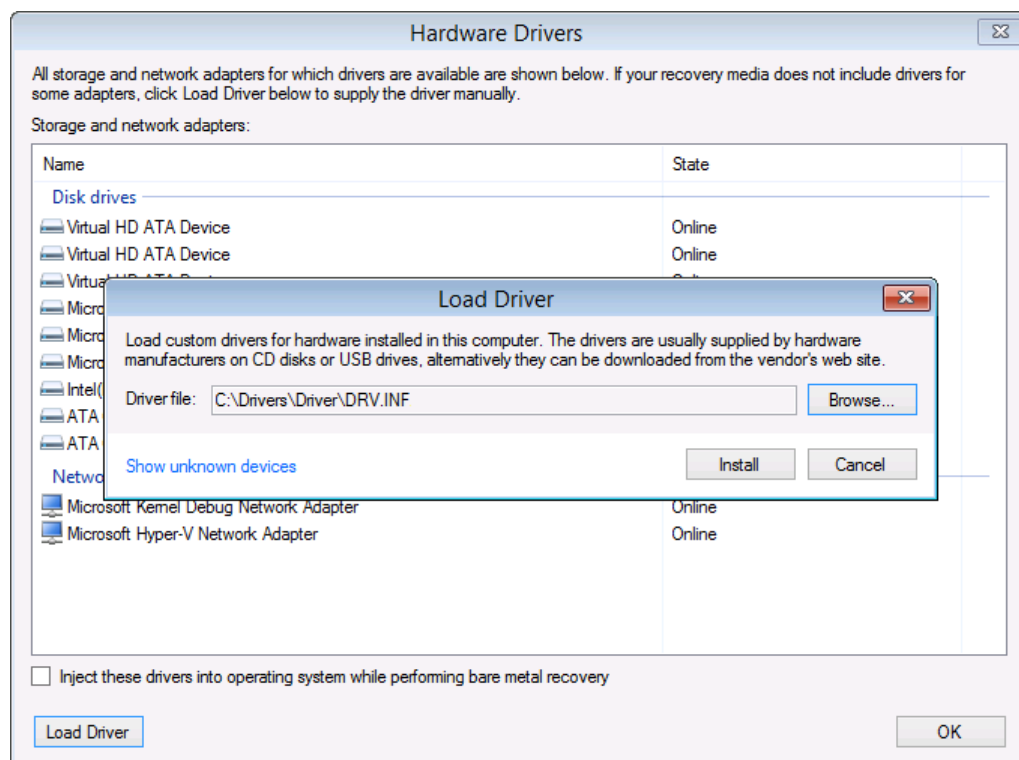
1. At the **Disk Mapping** step of the wizard, click **Load driver**.
2. In the **Hardware Drivers** window, select the necessary device.

If you want to save drivers for all listed devices to the restored operating system, select the **Inject these drivers into operating system while performing bare metal recovery** option.

1. Click the **Install** link next to the selected device.

To install drivers that were not included in the Veeam Recovery Media:

1. At the **Disk Mapping** step of the wizard, click **Load driver**.
2. At the bottom of the **Hardware Drivers** window, click the **Load Driver** button and select the INF file in the driver package folder. You can also click the **Show unknown devices** link to see a list of all existing devices without drivers. This information may help you to identify the exact device for which you need to install the driver.
3. Click **Install**.



Step 12. Resize Restored Volumes

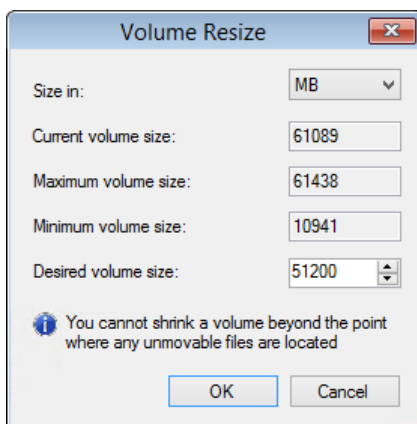
At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. You can resize a volume if you have chosen to restore data in the *Manual* mode and customize disk layout. A volume will be shrunk or extended to the specified size during the process of data restore.

Note: By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Endpoint Backup will extend the volume to 60,2 GB.

To resize a volume:

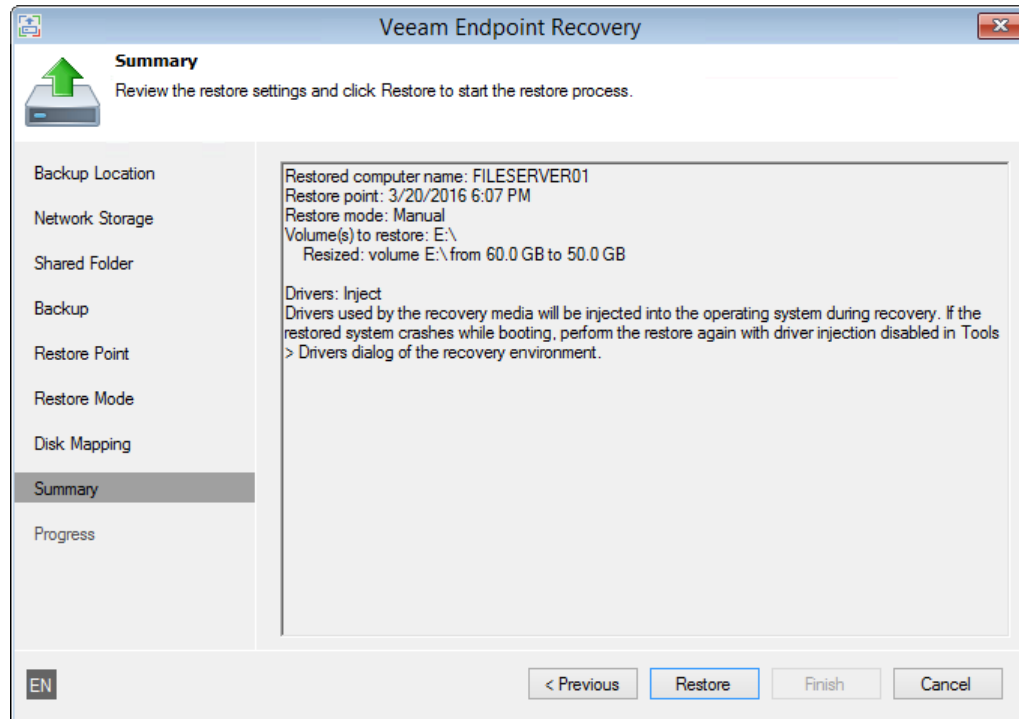
1. Specify a volume you want to resize:
 - a. Right-click a restored volume mapped to a target disk and select **Resize**.
 - b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Endpoint Backup will prompt you to shrink the restored volume.
2. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.



Step 13. 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 Endpoint Backup will perform partition re-allocation operations if necessary, restore the necessary data from the backup and overwrite data on your computer with it.



Using Veeam Endpoint Backup 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 Endpoint Backup offers its native tools and standard Microsoft Windows recovery tools.

Important! Veeam Endpoint Backup 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 Endpoint Recovery** 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 Endpoint Backup debug logs to a ZIP file and save this file on a removable storage appliance attached to your computer.

← 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

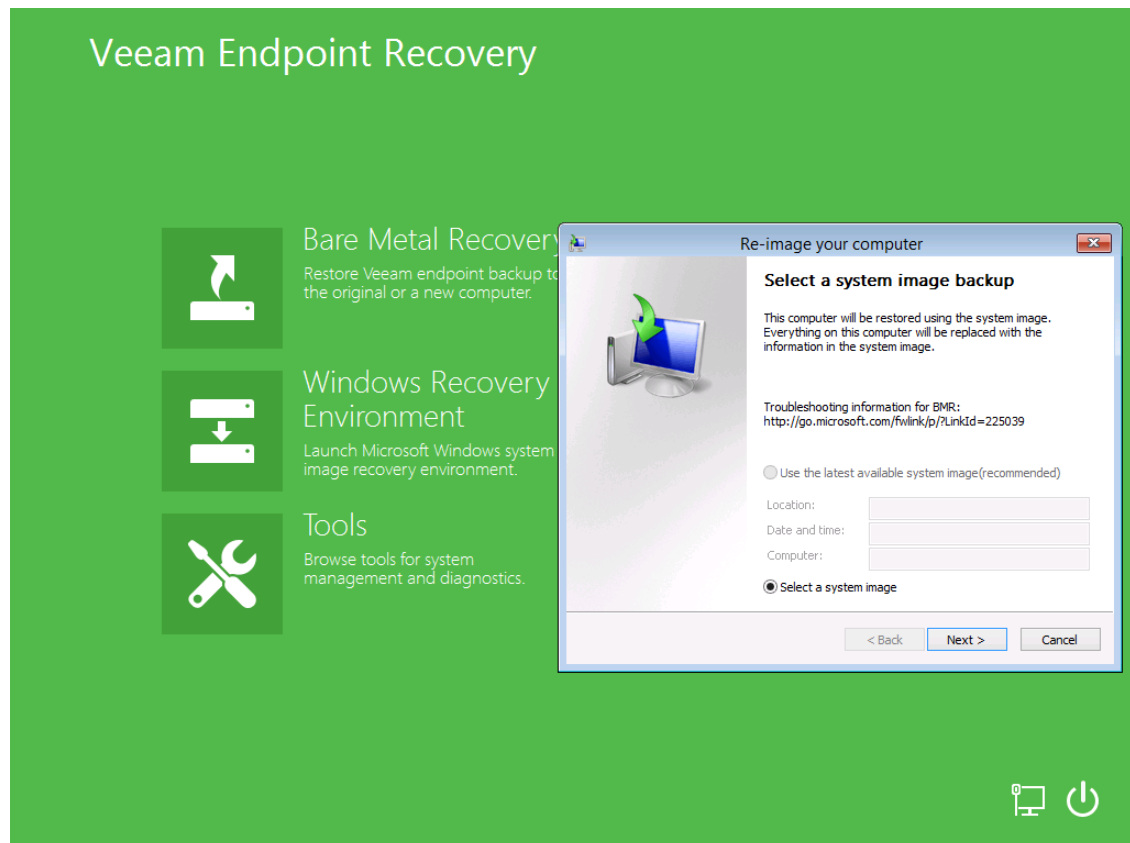
Saves recovery appliance debug log files to a removable storage.

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 Endpoint Recovery** 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>.



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 Endpoint Backup 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 Endpoint Backup 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](#).

Volume-level restore has the following limitations:

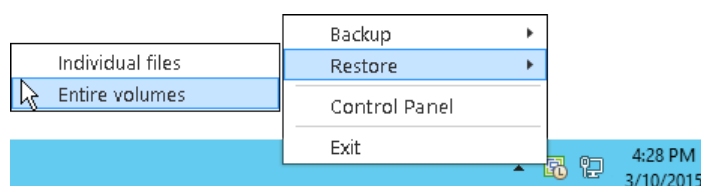
- You cannot restore the system volume to its original location.
- You cannot restore a volume to the volume on which the Microsoft Windows swap file is hosted.
- You cannot restore a volume to the volume where the backup file that you use for restore is located.

To overcome the first two limitations, you can boot from the recovery image and use the **Veeam Endpoint Recovery** wizard for volume-level restore. To learn more, see [Restoring from Veeam Recovery Media](#).

Step 1. Launch Veeam Endpoint Recovery Wizard

To launch the **Veeam Endpoint Recovery** wizard, do either of the following:

- Right-click the Veeam Endpoint Backup icon in the system tray and select **Restore > Entire volumes**.
- Double-click the Veeam Endpoint Backup 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. In this case, you will pass immediately to the [Restore Point](#) step of the wizard.
- From the Microsoft Windows start menu, select **All Programs > Veeam > Tools > Volume Restore**.

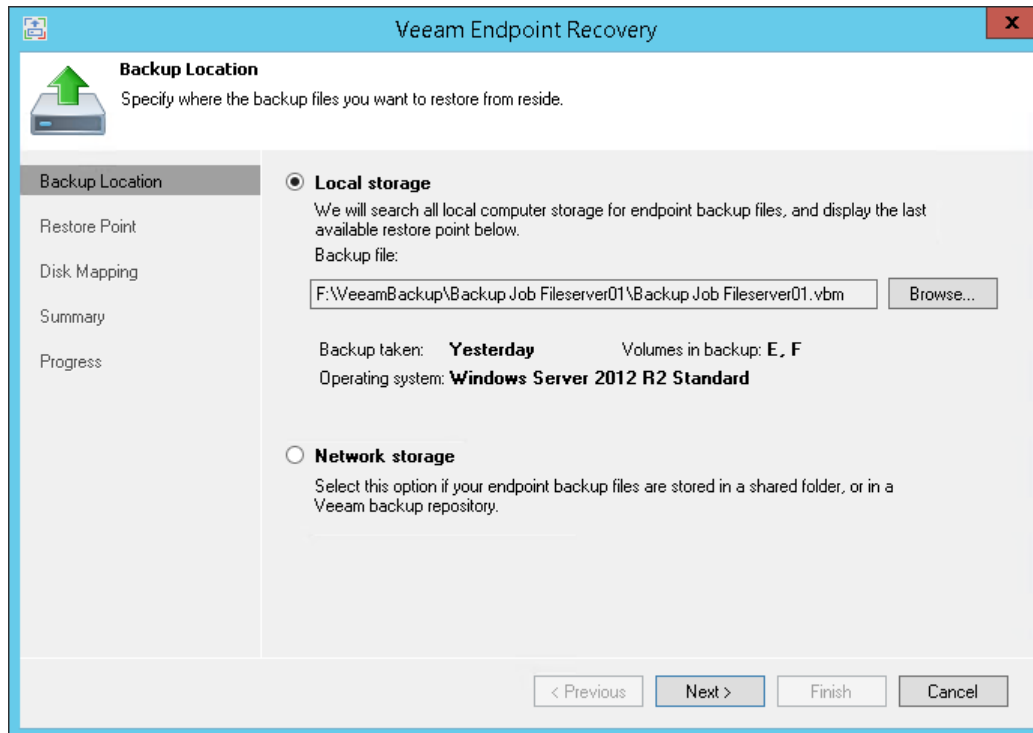


Step 2. Specify Backup File Location

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

By default, Veeam Endpoint Backup 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 Endpoint Backup 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 or on a backup repository managed by a Veeam backup server. In this case, the **Veeam Endpoint Recovery** wizard will include additional steps for specifying file location settings.



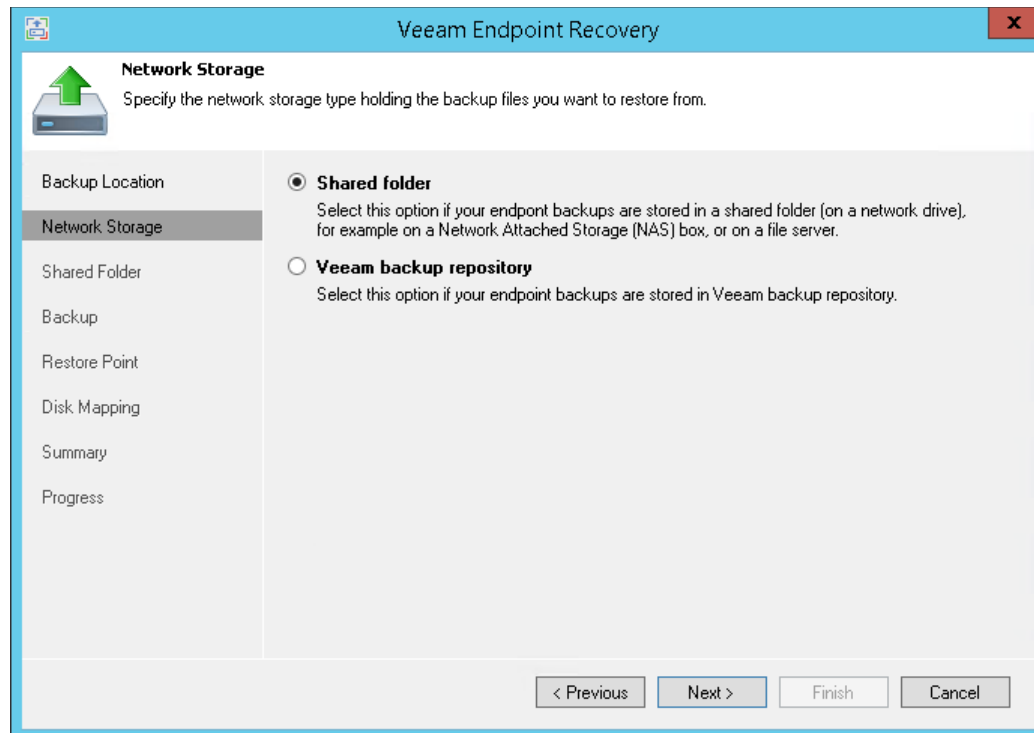
The screenshot shows the 'Veeam Endpoint Recovery' window, specifically the 'Backup Location' step. The window has a blue title bar and a sidebar on the left with icons for 'Backup Location', 'Restore Point', 'Disk Mapping', 'Summary', and 'Progress'. The main area is titled 'Backup Location' with a green arrow icon and the instruction 'Specify where the backup files you want to restore from reside.' There are two radio button options: 'Local storage' (selected) and 'Network storage'. The 'Local storage' section includes a description, a 'Backup file:' label, a text box containing 'F:\VeeamBackup\Backup Job Fileserver01\Backup Job Fileserver01.vbm', and a 'Browse...' button. Below this, it shows 'Backup taken: Yesterday' and 'Volumes in backup: E, F', and 'Operating system: Windows Server 2012 R2 Standard'. The 'Network storage' section is currently inactive. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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 or on a backup 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.



Step 4. Specify Shared Folder Settings

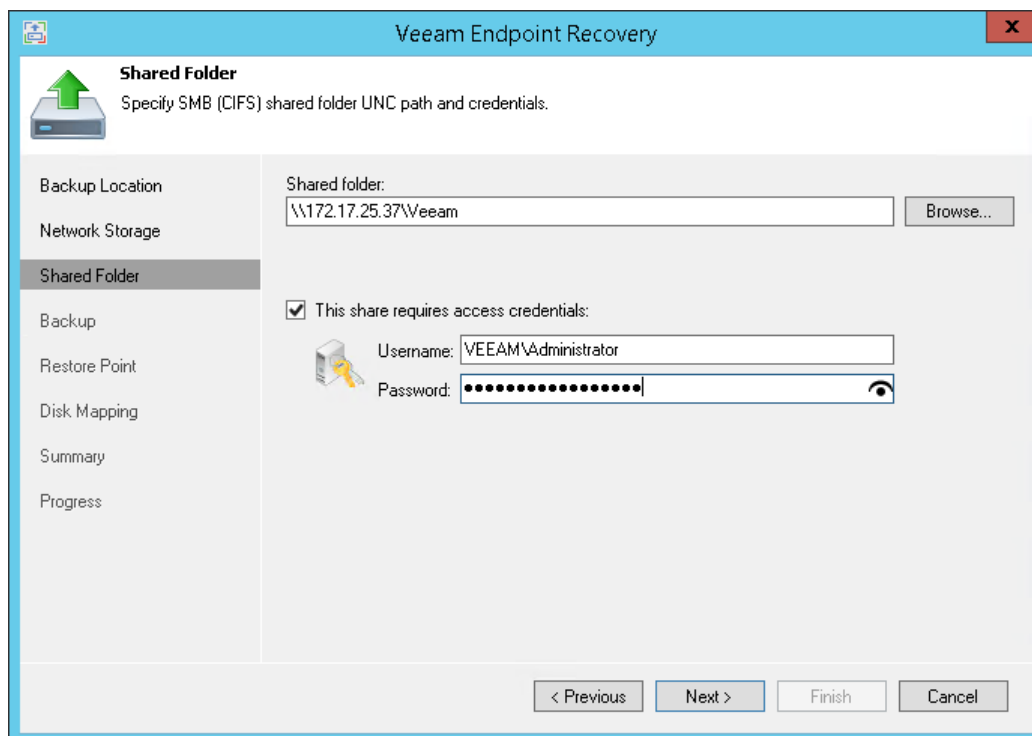
The **Shared Folder** step of the wizard is available if you have chosen to restore data from a backup file located in a network shared folder.

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 Endpoint Backup 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.



The screenshot shows the 'Veeam Endpoint Recovery' window with the 'Shared Folder' tab selected. The window title is 'Veeam Endpoint Recovery'. The 'Shared Folder' section has a subtitle 'Specify SMB (CIFS) shared folder UNC path and credentials.' Below this, there is a 'Shared folder:' text box containing '\\172.17.25.37\Veeam' and a 'Browse...' button. A checkbox labeled 'This share requires access credentials:' is checked. Below the checkbox, there is a 'Username:' text box containing 'VEEAM\Administrator' and a 'Password:' text box filled with dots. An eye icon is visible on the right side of the password field. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Specify 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:

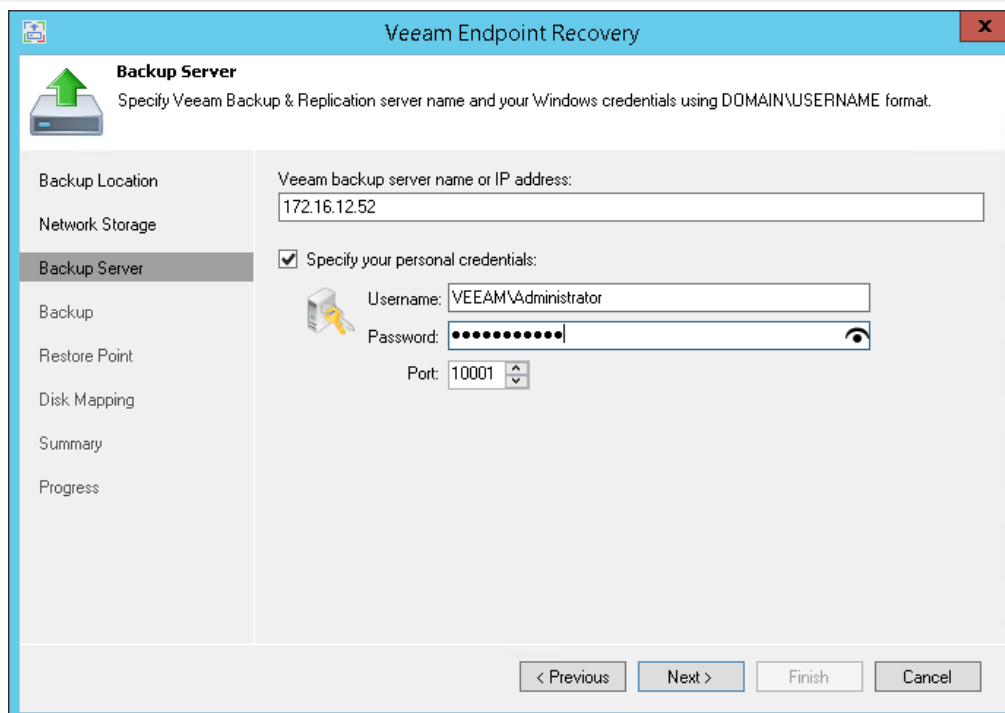
1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. Select the **Specify your personal credentials** check box. In the **Username** and **Password** fields, enter a user name and password of the account that has access to this backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup must communicate with the backup repository. By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will fail to connect to the Veeam backup server.



The screenshot shows the 'Veeam Endpoint Recovery' window, specifically the 'Backup Server' step. The window has a blue title bar and a sidebar on the left with navigation options: Backup Location, Network Storage, Backup Server (selected), Backup, Restore Point, Disk Mapping, Summary, and Progress. The main area contains the following fields and controls:

- Backup Server** (with a green arrow icon): Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.
- Veeam backup server name or IP address:** A text box containing '172.16.12.52'.
- ☒ **Specify your personal credentials:**
- Username:** A text box containing 'VEEAM\Administrator'.
- Password:** A text box with masked characters (dots) and a toggle icon.
- Port:** A spinner box set to '10001'.
- At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

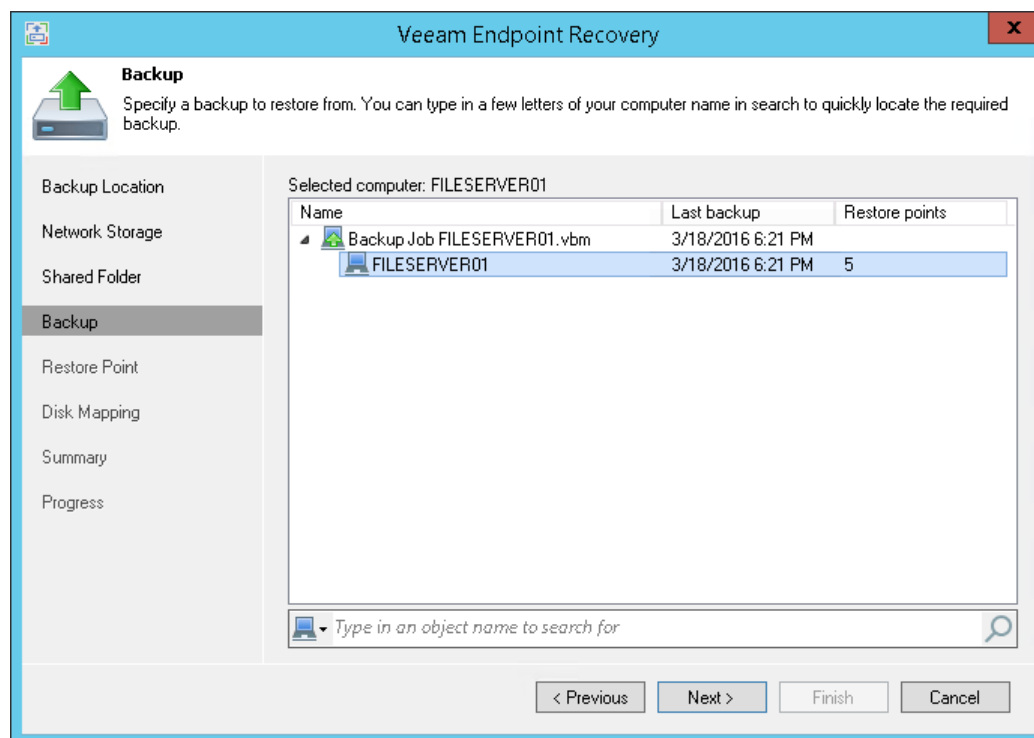
Step 6. Select Backup

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 Endpoint Backup 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 Endpoint backups stored on the backup repository.

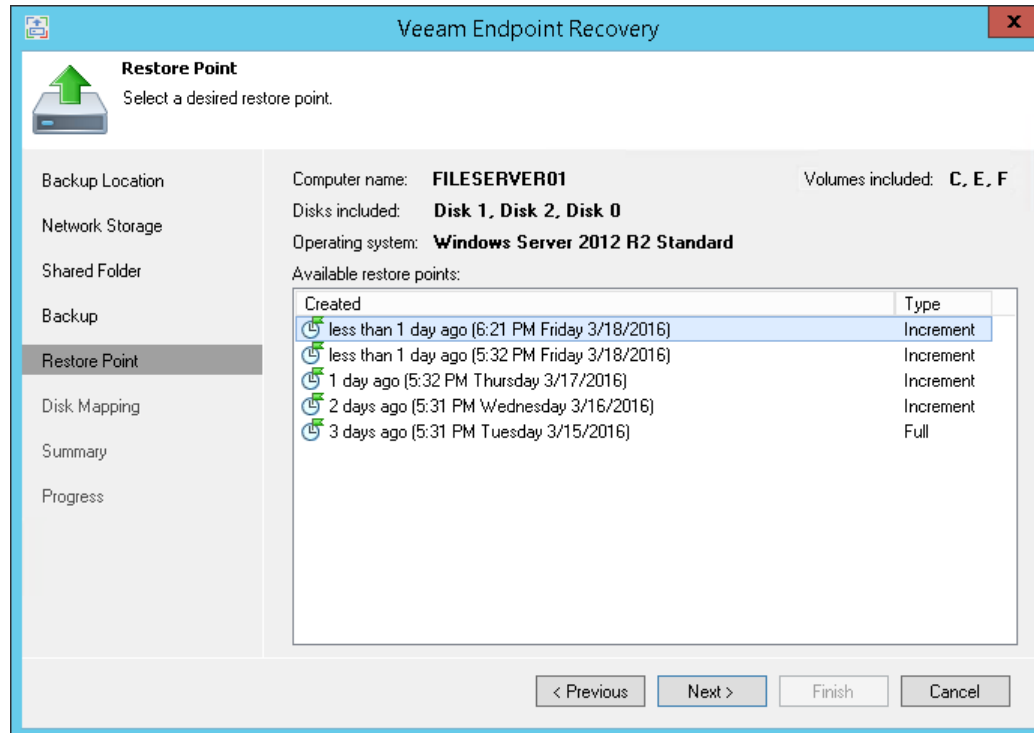


Step 7. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Endpoint Backup uses the latest restore point. However, you can select any valid restore point to recover volumes to a specific point in time.

Veeam Endpoint Backup 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 Endpoint Backup will display only 3 restore points in the list.



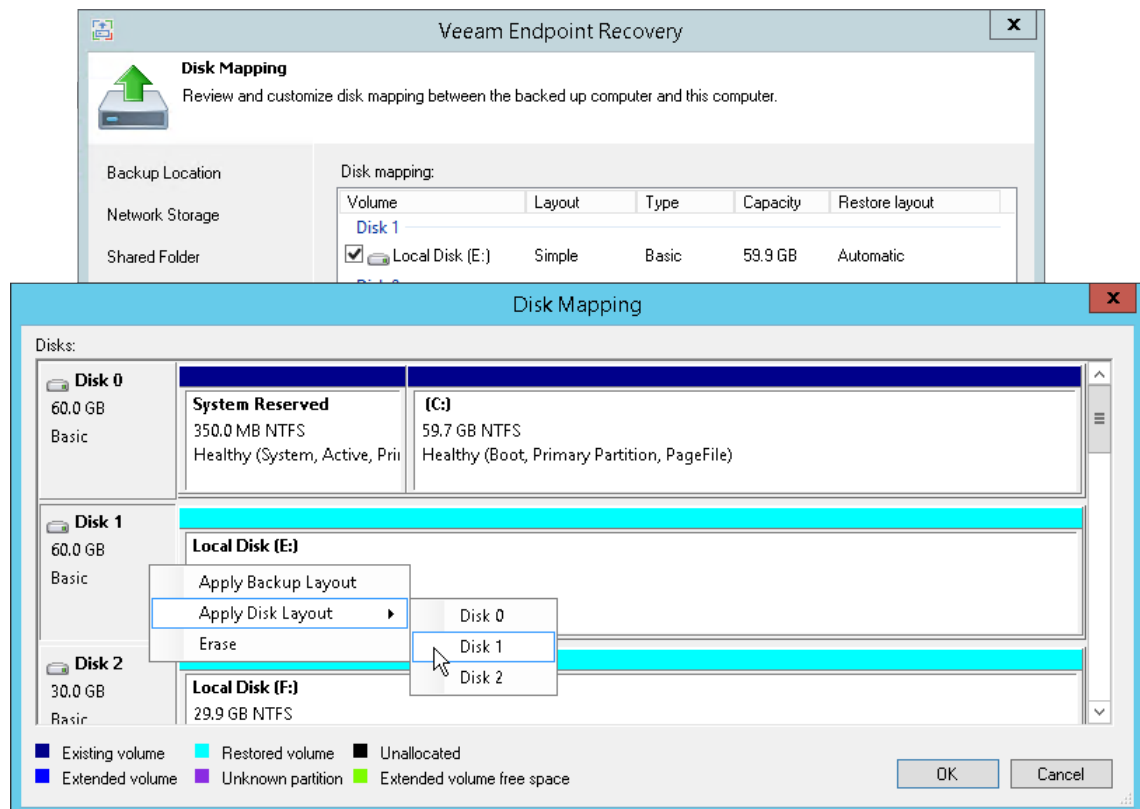
Step 8. Map Restored Disks

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.

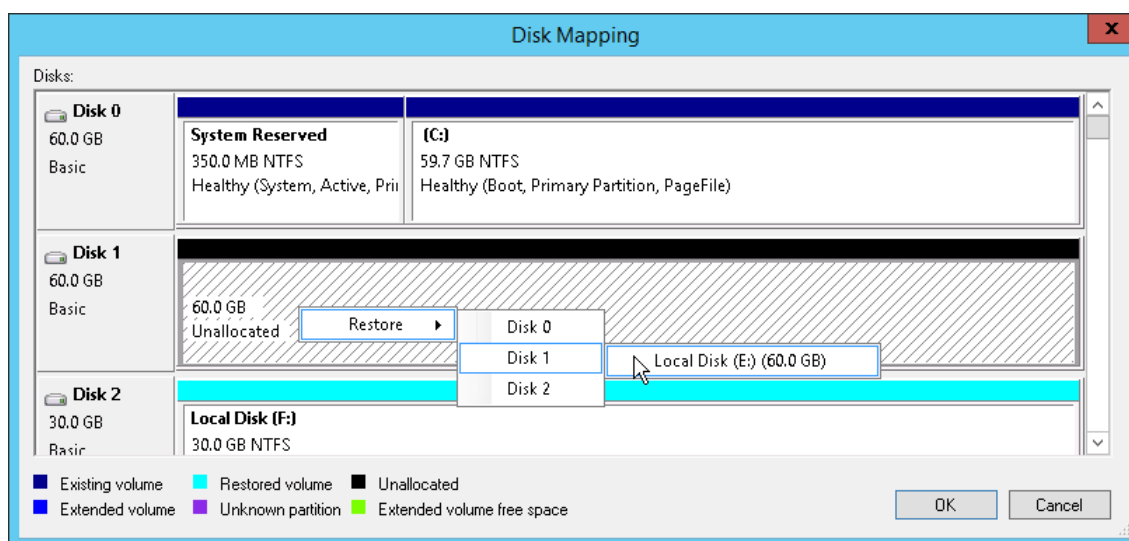
To select volumes to restore:

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 Endpoint Backup 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:
 - a. 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.



- b. 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.

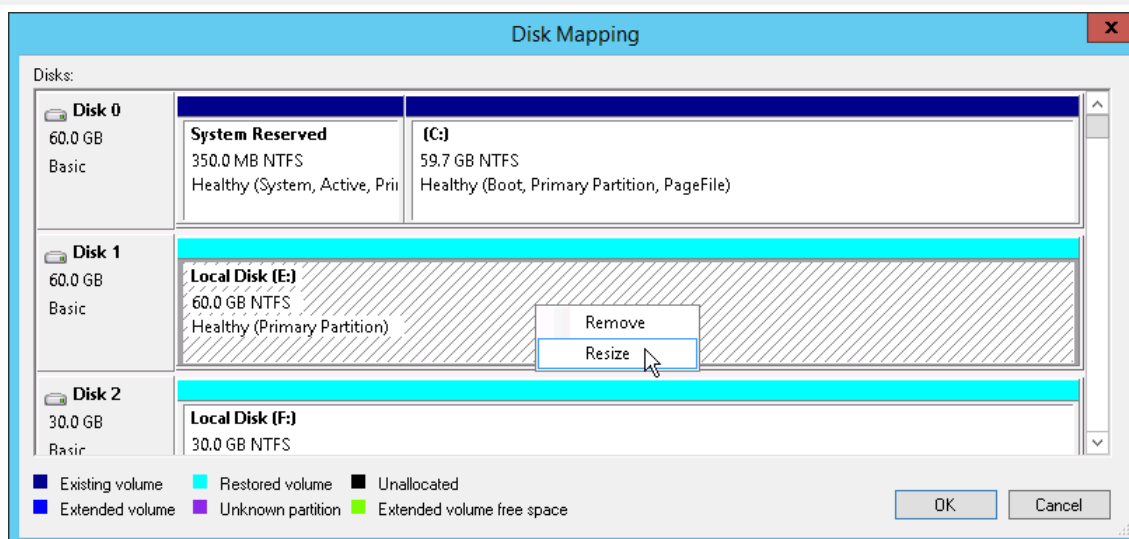
If you want to change disk layout configured by Veeam Endpoint Backup, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



3. [For restore with volume resize] You can resize a volume mapped by Veeam Endpoint Backup 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 Endpoint Backup will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Endpoint Backup will prepare to shrink the volume to the size of available disk space.



Step 9. Resize Restored Volumes

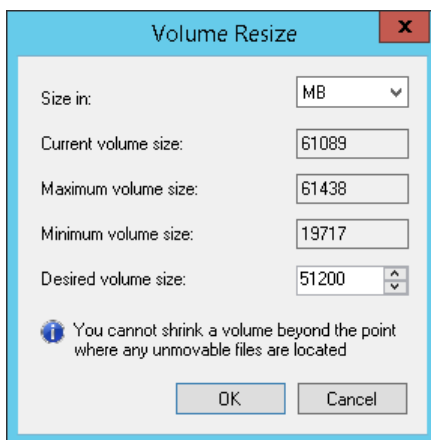
At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. You can resize a volume if you have chosen to restore data in the *Manual* mode and customize disk layout. A volume will be shrunk or extended to the specified size during the process of data restore.

Note: By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Endpoint Backup will extend the volume to 60,2 GB.

To resize a volume:

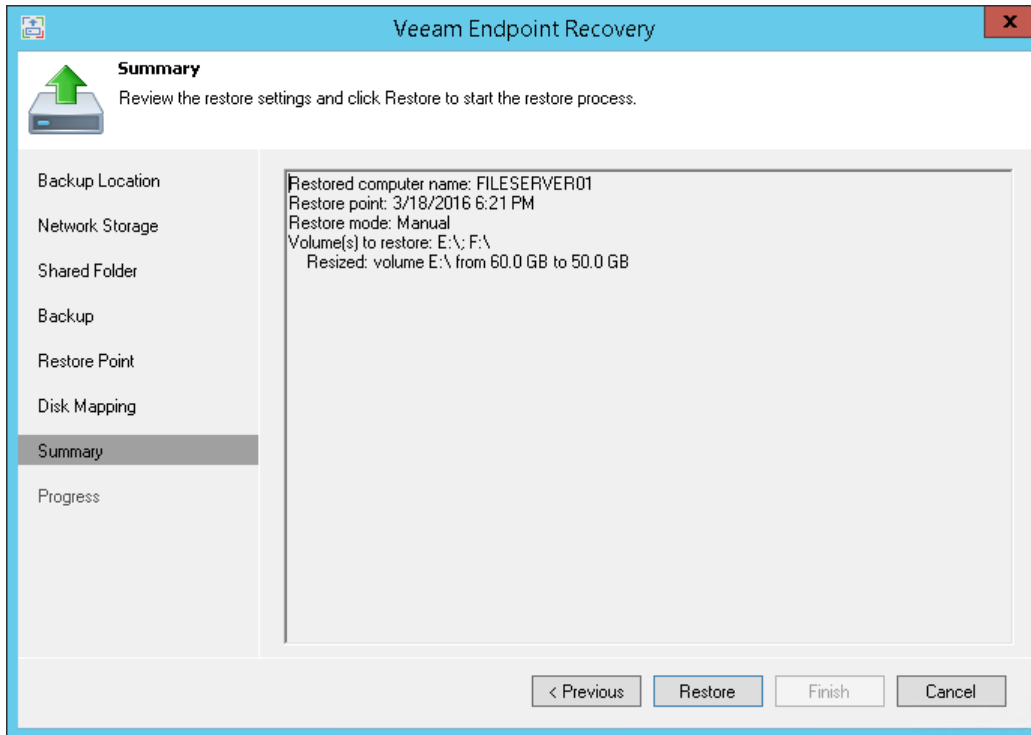
1. Specify a volume you want to resize:
 - a. Right-click a restored volume mapped to a target disk and select **Resize**.
 - b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Endpoint Backup will prompt you to shrink the restored volume.
2. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.



Step 10. 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 Endpoint Backup will perform partition re-allocation operations if necessary, restore the necessary volume data from the backup and overwrite volume data on your computer with the restored data.



Restoring Files and Folders

If some files and folders on your computer get lost or corrupted, you can restore them from backups. For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

When you perform file-level restore, Veeam Endpoint Backup 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

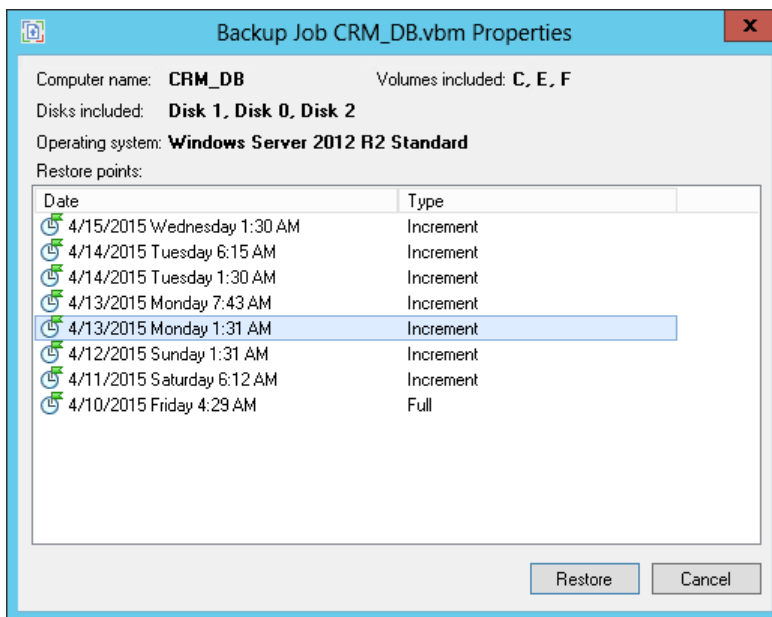
Before you begin the file-level restore process, check the following prerequisites:

- 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](#).

Step 1. Launch File Level Restore Wizard

To launch the **File Level Restore** wizard, do either of the following:

- Right-click the Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will automatically publish the backup content into the computer file system and [open the Veeam Backup browser](#).

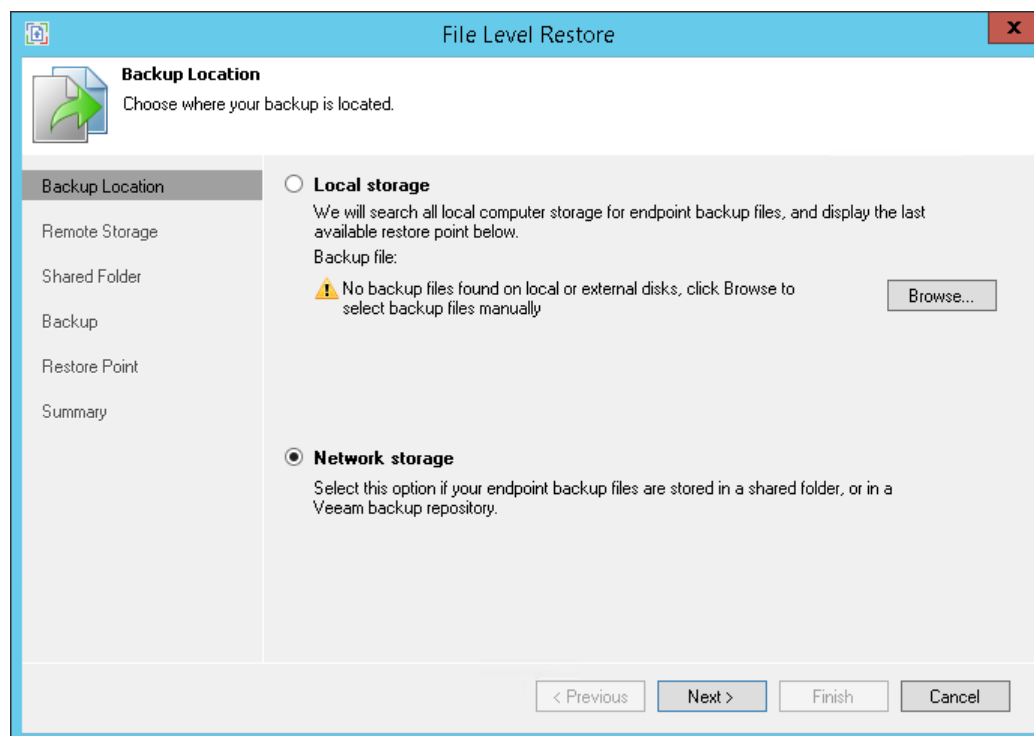


Step 2. Specify Backup File Location

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

By default, Veeam Endpoint Backup 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 Endpoint Backup 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 or on a backup repository connected to a Veeam backup server. In this case, the **File Level Restore** wizard will include additional steps for specifying file location settings.

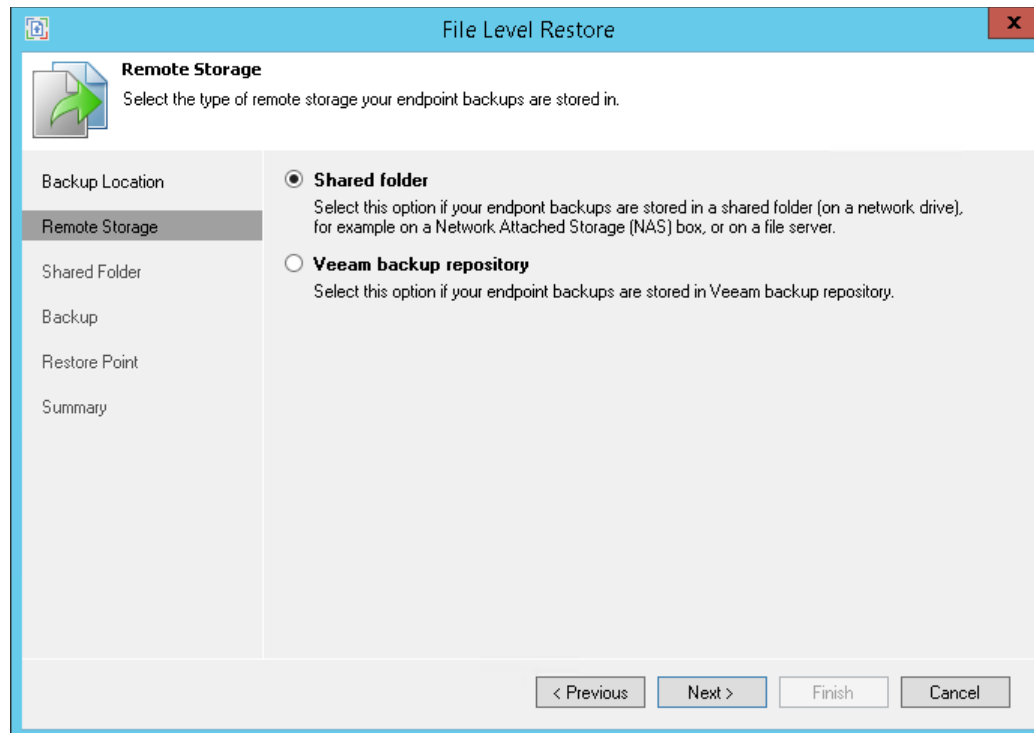


Step 3. Select Remote Storage Type

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



Step 4. Specify Shared Folder Settings

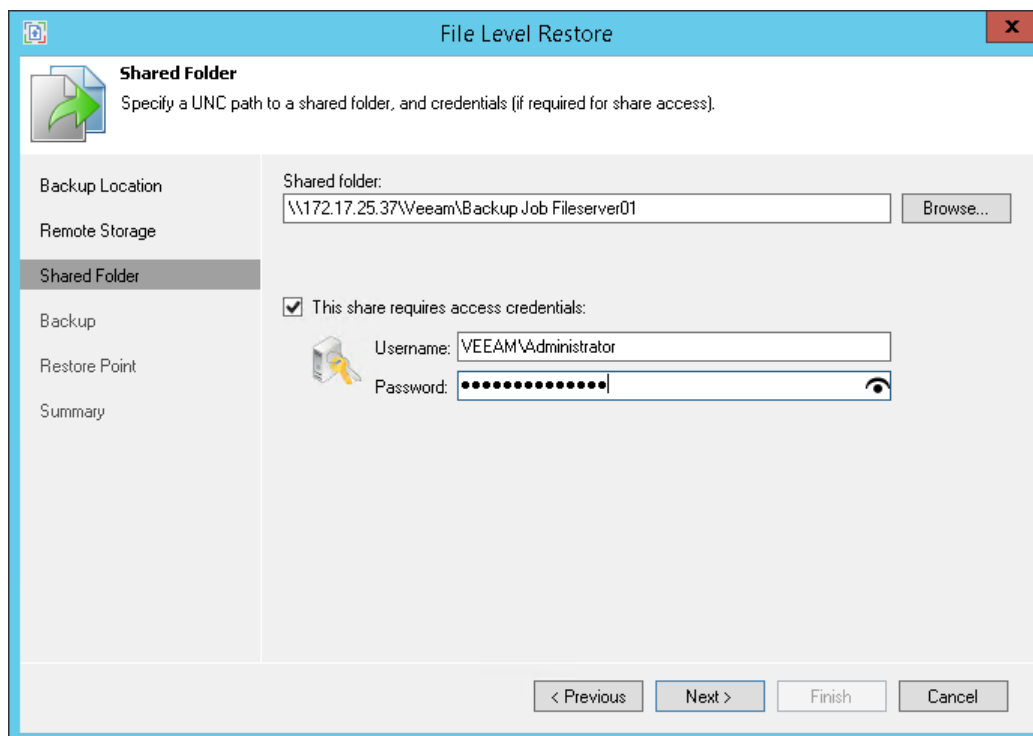
The **Shared Folder** step of the wizard is available if you have chosen to restore data from a backup file located in a network shared folder.

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 Endpoint Backup 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.



The screenshot shows the 'File Level Restore' wizard window. The 'Shared Folder' step is selected in the left-hand navigation pane. The main area contains the following fields and controls:

- Shared folder:** A text box containing the UNC path '\\172.17.25.37\\Veeam\\Backup Job Fileserver01'. A 'Browse...' button is to the right.
- ☒ **This share requires access credentials:**
- Username:** A text box containing 'VEEAM\Administrator'.
- Password:** A text box with masked characters (dots) and an eye icon on the right to toggle visibility.

At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Specify 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup must communicate with the backup repository. By default, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will fail to connect to the Veeam backup server.

File Level Restore

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

Backup Location
Remote Storage
Backup Server
Backup
Restore Point
Summary

Veeam backup server name or IP address:
172.6.12.52

☒ Specify your personal credentials:

Username: VEEAM\Administrator
Password: [masked]
Port: 10001

< Previous Next > Finish Cancel

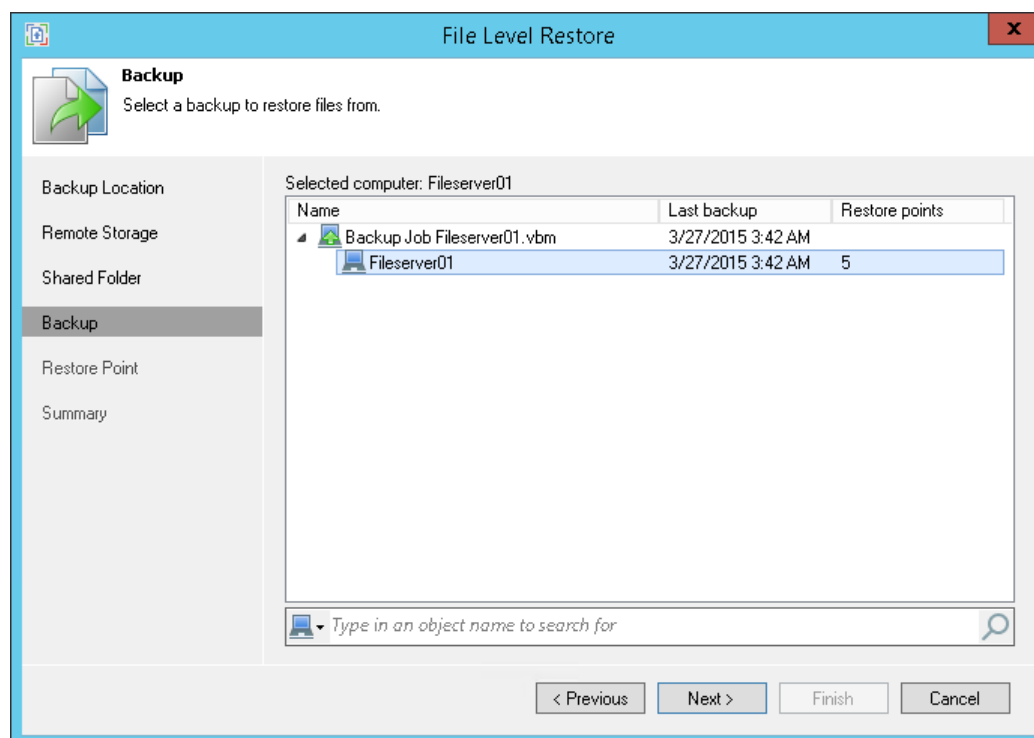
Step 6. Select Backup

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 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]**.

If you restore data from a backup stored on the backup repository, Veeam Endpoint Backup displays only those backups that are accessible by the user whose credentials are specified at the **Backup Server** step of the wizard:

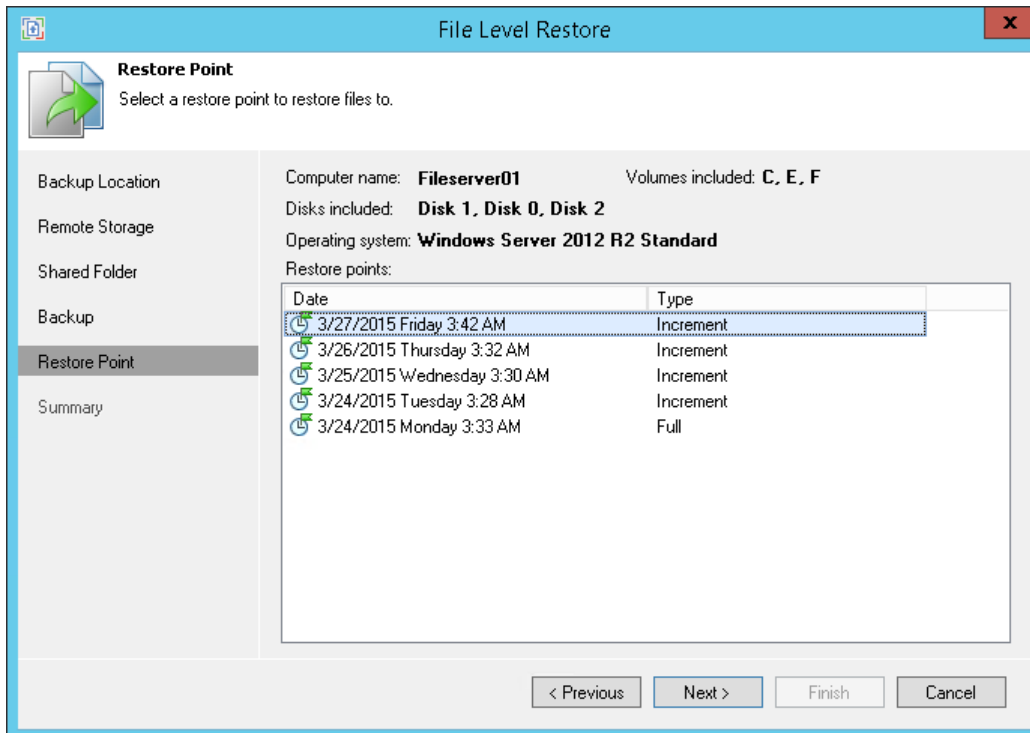
- If you specify credentials for the user who has access to the backup repository, the list of backups will include only backups created by this user.
- If you specify credentials for the user who is assigned the *Backup Administrator* or *Restore Operator* role on the backup server, the list of backups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



Step 7. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

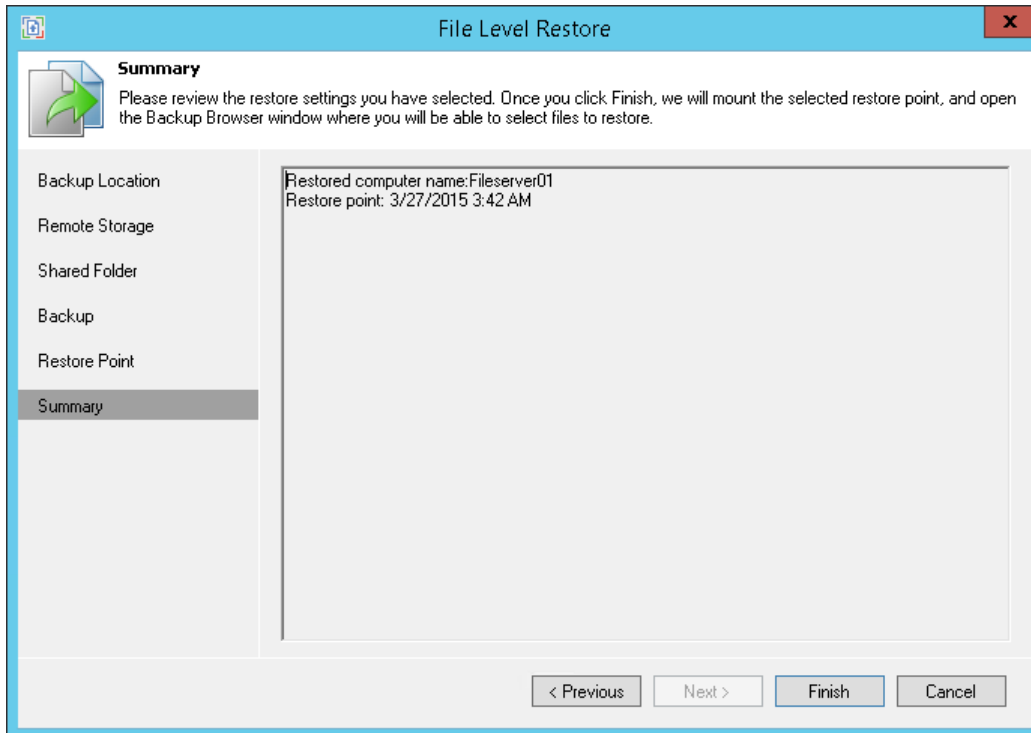
By default, Veeam Endpoint Backup uses the latest restore point. However, you can select any valid restore point to recover files and folders to a specific point in time.



Step 8. 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 Endpoint Backup will retrieve the content of the backup file, publish it directly into the file system of your computer and display it in the Veeam Backup browser.



Step 9. Save Restored Files

When the restore process is complete, Veeam Endpoint Backup opens the Veeam Backup browser displaying the content of the backup file.

You can perform the following operations with restored files and folders:

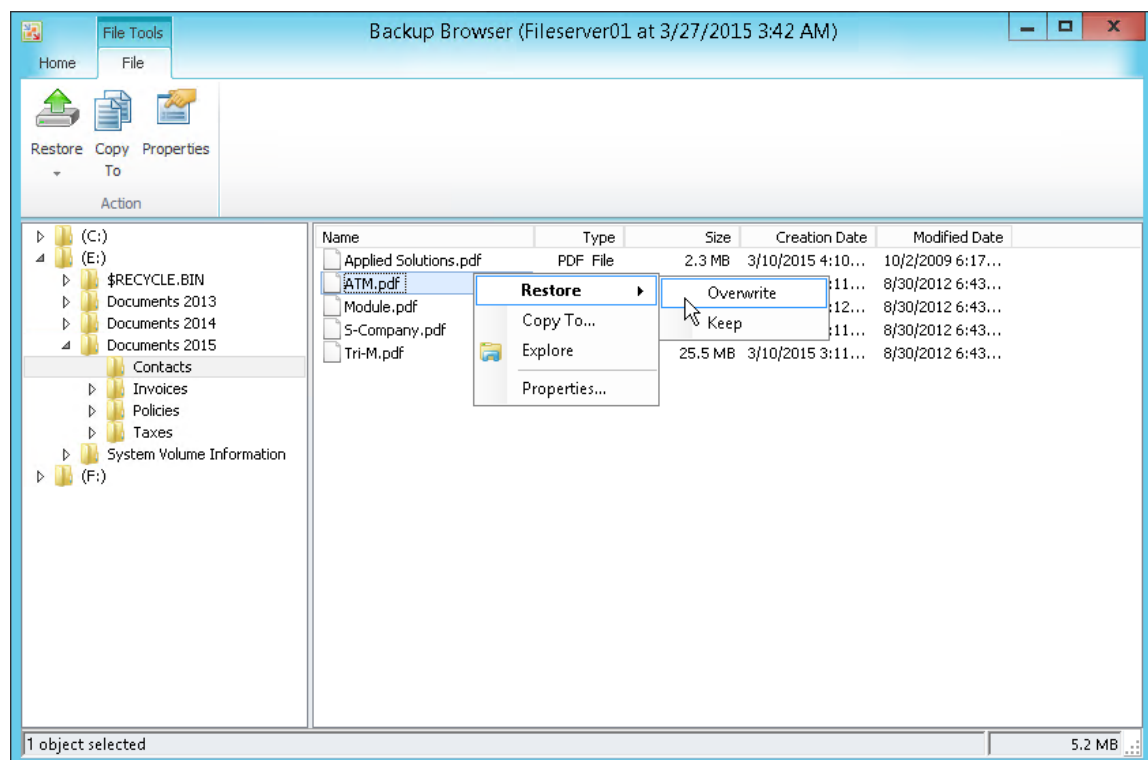
- Save files and folders to their initial location
- Save files and folders to a new location
- Open files in Microsoft Windows Explorer

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 Endpoint Backup will add the *RESTORED-* prefix to the restored file or folder name and save it in the same location where the original file resides.

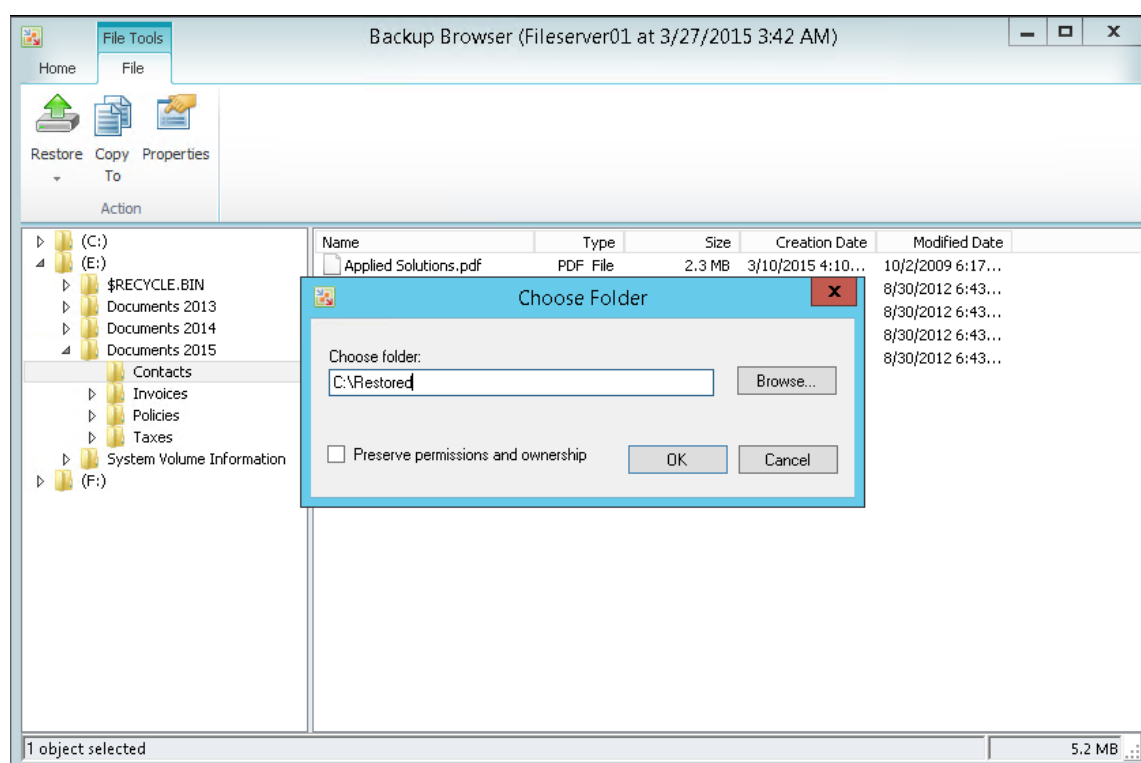


Saving Files to New Location

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

When restoring file objects, you can choose to preserve their original NTFS permissions:

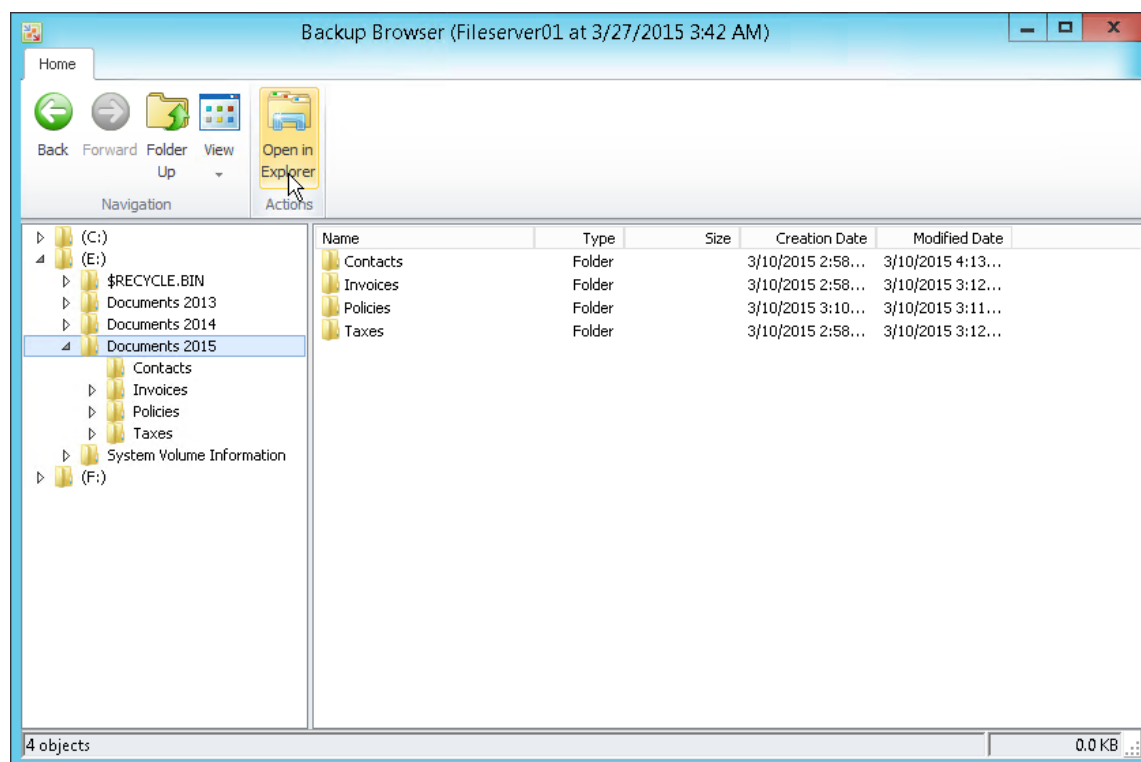
- Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored items. Veeam Endpoint Backup will copy selected files or folders with associated Access Control Lists, preserving granular access settings.
- Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored items. Veeam Endpoint Backup will change security settings: the user who launched the Veeam Endpoint Backup will be set as the owner of the restored items. Access permissions will be inherited from the folder to which the restored items are copied.



Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders. To do this, do either of the following:

- In Veeam Backup browser, select the necessary file or folder and click **Open in Explorer** on the toolbar. Veeam Endpoint Backup 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.



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](https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx).

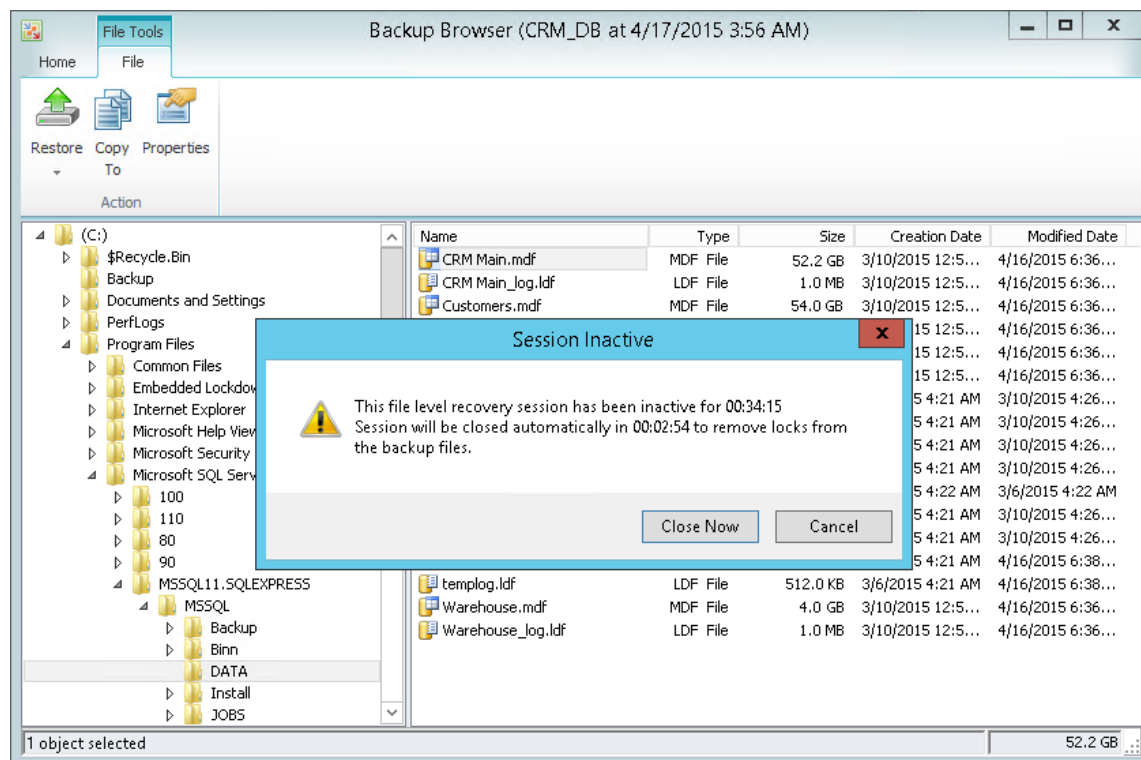
Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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.



REPORTING

Veeam Endpoint Backup provides several ways to get information about performed backups:

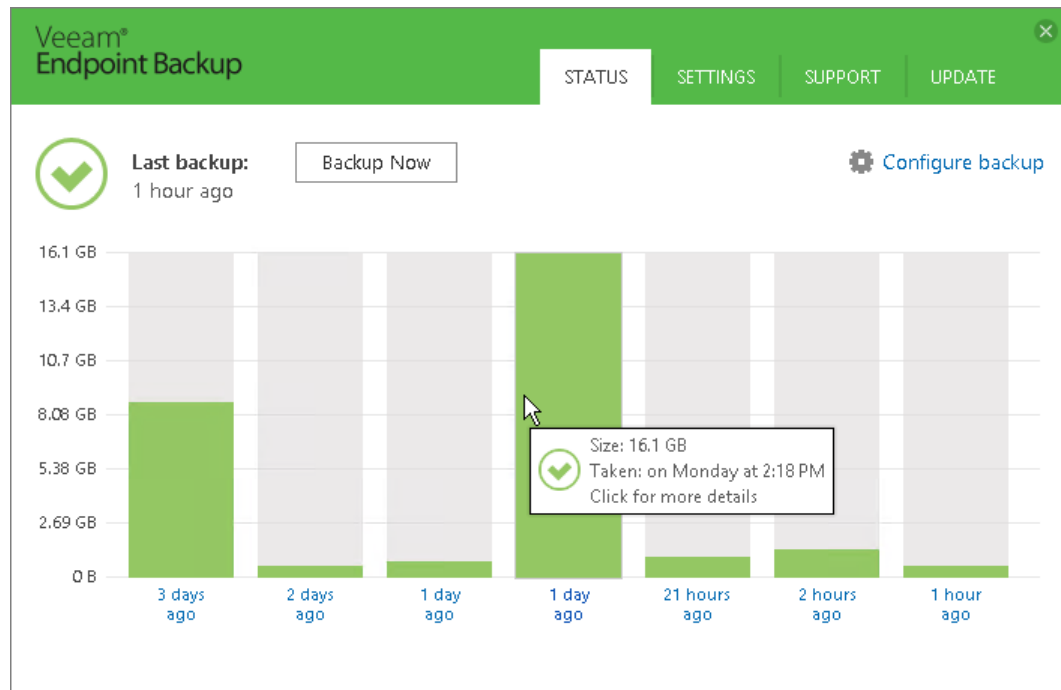
- You can view information about performed backups in the Control Panel.
- You can get information about the backup status using the Veeam Endpoint Backup tray agent.
- You can get information about the backup progress using the Veeam Endpoint Backup taskbar button.
- You can get information about Veeam Endpoint Backup 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 Endpoint Backup Control Panel to view statistics about performed backups. To open the Control Panel, do either of the following:

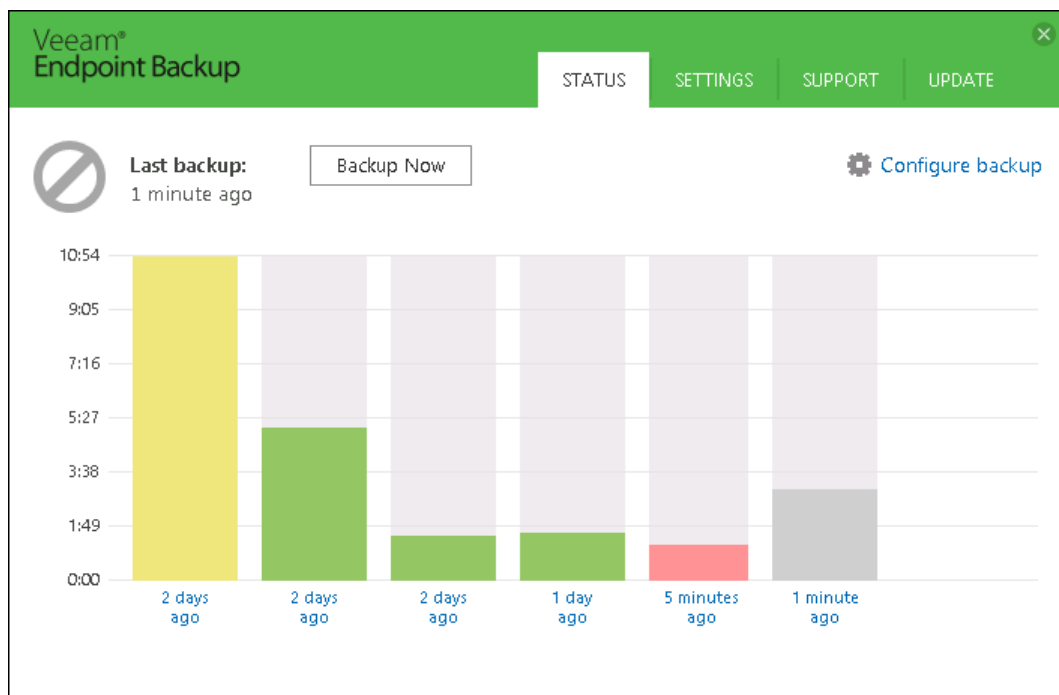
- Double-click the Veeam Endpoint Backup icon in the system tray.
- Right-click the Veeam Endpoint Backup icon in the system tray and select **Control Panel**.

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 Endpoint Backup will provide the following details: backup status, backup time and size of the resulting backup file.



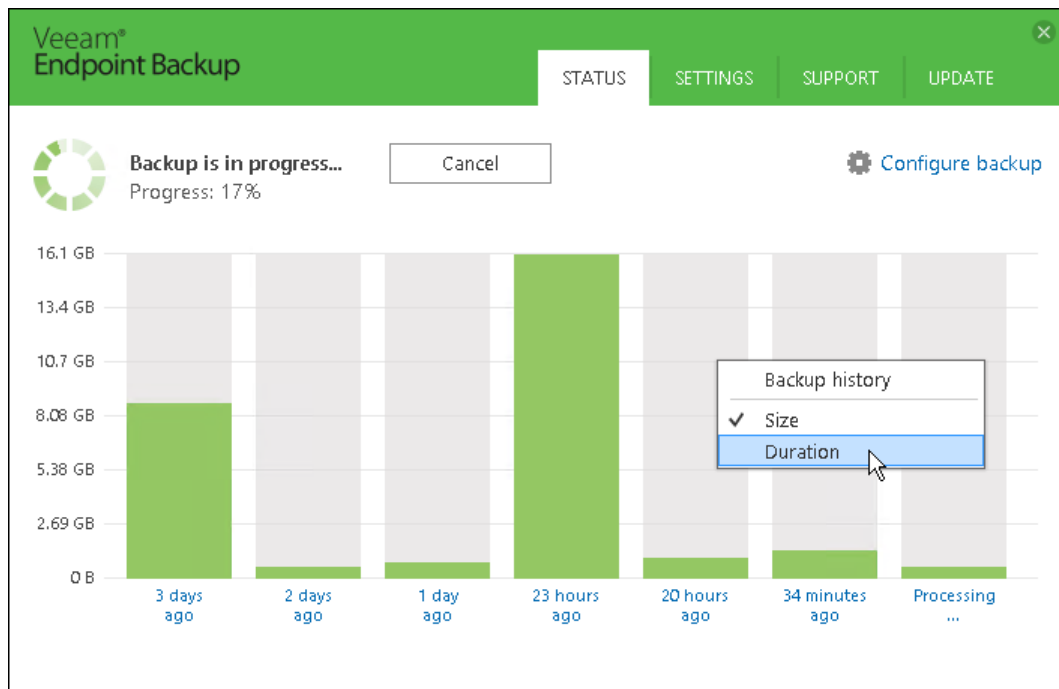
The bar color identifies the status of the backup job session. The backup job session can complete with one of the following statuses:

- **Success** (green color) — the backup job is currently running or has completed successfully.
- **Warning** (yellow color) — the backup job has completed with a warning. Veeam Endpoint Backup 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 Endpoint Backup displays the size of created backup files. To display the duration of backup job sessions:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the icon and select **Control Panel**.
1. In the **Status** view, right-click the backup job sessions chart.
2. In the **Backup history** menu, select the **Duration** option.





Viewing Statistics for Separate Restore Points

Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup will display details 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.

 Restore point details 

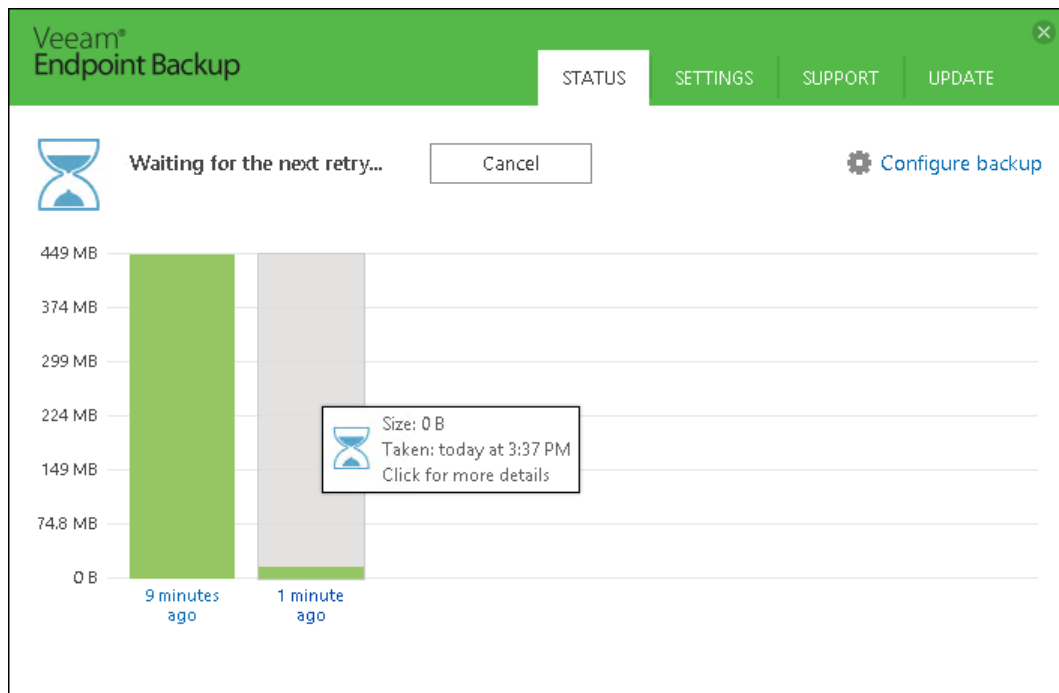
Backed up items: System Reserved;C:\	Total backup size: 13.3 GB
Backup duration: 0:05:44	Average backup duration: 0:16:59
Restore point size: 172 MB	Free disk space: 497 GB

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	

Restore FilesRestore Volumes

Viewing Information About Job Retries



If the backup job started by schedule has failed for some reason, Veeam Endpoint Backup retries it every 10 minutes within 23 hours. All backup job retries are performed within one backup job session. For this reason, Veeam Endpoint Backup displays them as one bar in the chart.



Note: For portable devices, Veeam Endpoint Backup 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 Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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	

Restore Files











Restore Volumes

[Hide retries](#)

Monitoring Backup State with Tray Agent

The Veeam Endpoint Backup 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
	Ellipsis over the icon	The scheduled backup job is not configured.
	Progress indicator over the icon	The backup task is being performed. To view the backup task progress, hover the mouse over the icon.
	Veeam Endpoint Backup icon	The backup job is set up but scheduling settings for the job are not configured.
	Clock over the icon	The latest session of the scheduled backup job has completed successfully; waiting for the next backup job session.
	Cancel sign over the icon	The latest session of the scheduled backup job has been canceled.
	Error sign over the icon	An error occurred during the latest backup job session, and the session was terminated.
	Minus sign over the icon	The scheduled backup job is disabled.
	Grey icon	The tray agent is not connected to the Veeam Endpoint Backup service.
	Warning sign over the icon	The backup job has completed with a warning, for example, the target location is running low on space.
	Warning sign over the disk	<p>[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.</p> <p>In this case, Veeam Endpoint Backup 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 Endpoint Backup will automatically start the scheduled backup job.</p>

Monitoring Backup Process in Taskbar Button

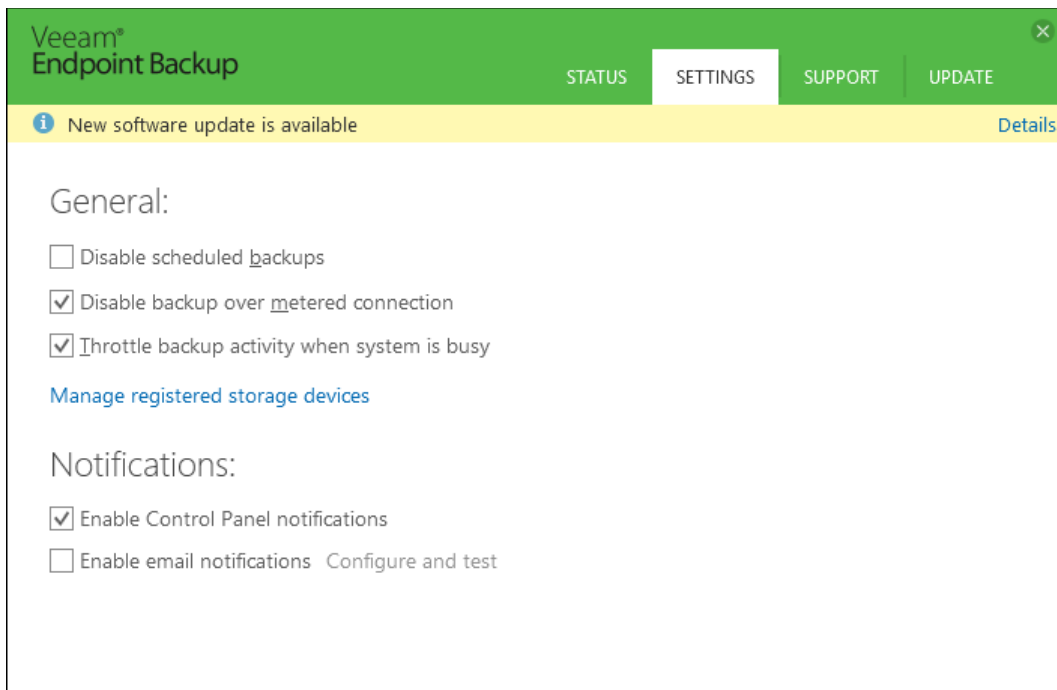
You can monitor the backup process with the Veeam Endpoint Backup taskbar button. Veeam Endpoint Backup displays on the taskbar button a green progress bar that reflects the bar for the currently running job session in the Control Panel. As a result, you can track the process of the backup file creation while working with another application without having to switch to the Control Panel.



Viewing and Dismissing Veeam Endpoint Backup Events

If a warning event occurs, Veeam Endpoint Backup displays a notification bar with the event description in the Control Panel window. Veeam Endpoint Backup 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 Endpoint Backup does not start a new backup session in this case.
- A newer version of Veeam Endpoint Backup is available.



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

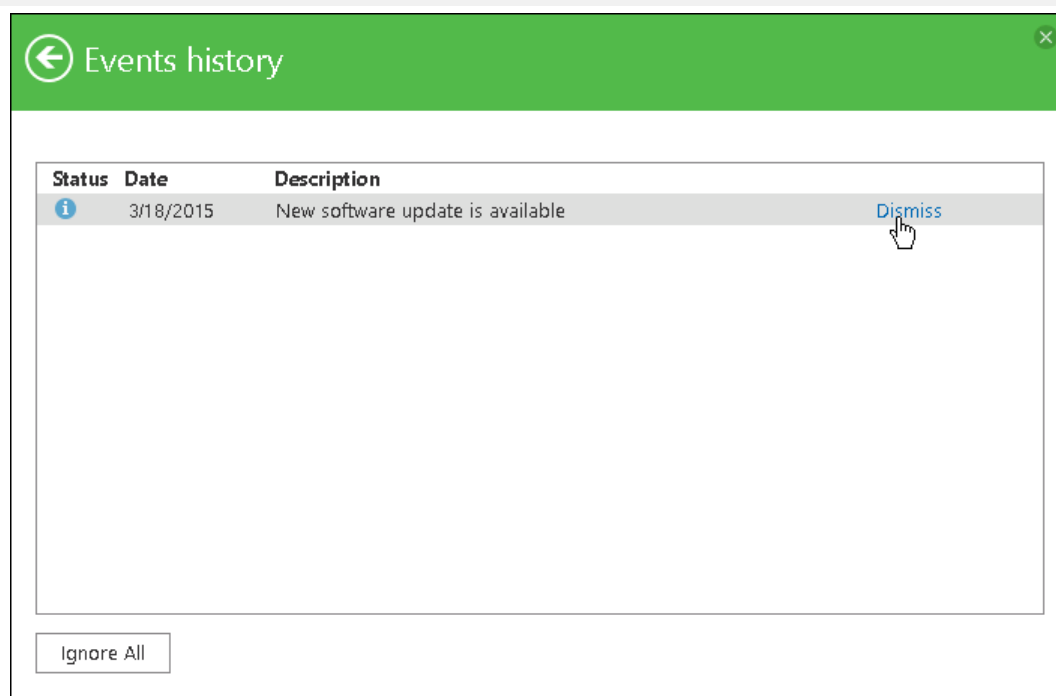
Veeam Endpoint Backup displays only the latest event in the notification bar. To view detailed information about all event:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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 Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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](#).



Viewing Job Session Results in Email Reports

You can receive email notifications with Veeam Endpoint Backup job results. When the backup job session completes, Veeam Endpoint Backup 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).

To receive email reports, you must enable and configure email notifications in the Veeam Endpoint Backup Control Panel. To learn more, see [Enabling Email Notifications](#). Once email notifications are configured, Veeam Endpoint Backup 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 Endpoint Backup does not send a report after every job retry. Instead, Veeam Endpoint Backup sends one report on the first error within the job session and another report on the last job session result — success or error.

Endpoint Backup job: Backup Job DESKTOP01

Veeam Endpoint Backup

Success

Monday, 29 February 2016 17:30:01

Success	1	Start time	17:30:01	Total size	60.3 GB	Backup size	1.0 GB	
Warning	0	End time	17:35:50	Data read	3.0 GB	Dedupe	1.0x	
Error	0	Duration	0:05:49	Transferred	1017.7 MB	Compression	1.6x	

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
DESKTOP01	Success	17:30:04	17:35:50	60.3 GB	3.0 GB	1017.7 MB	0:05:45	

SPECIFYING SETTINGS

You can use global settings of Veeam Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup can automatically detect metered connections and will not perform backup when your computer is on such connection.

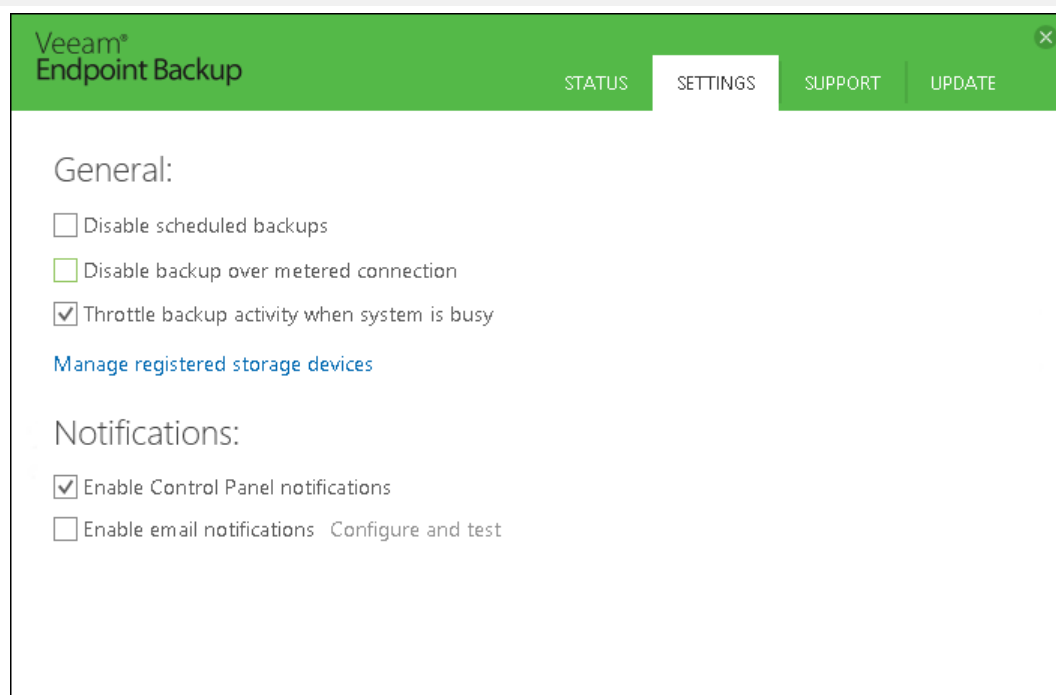
The disable setting applies to all types of backups: scheduled and ad-hoc. Mind the following limitations and requirements:

- Veeam Endpoint Backup 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 <http://windows.microsoft.com/en-US/windows-8/metered-internet-connections-frequently-asked-questions>.

By default, backup over metered connections is disabled. To enable backup over metered connections:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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 Endpoint Backup will display a warning and ask you to confirm that you want to use this connection for backup.



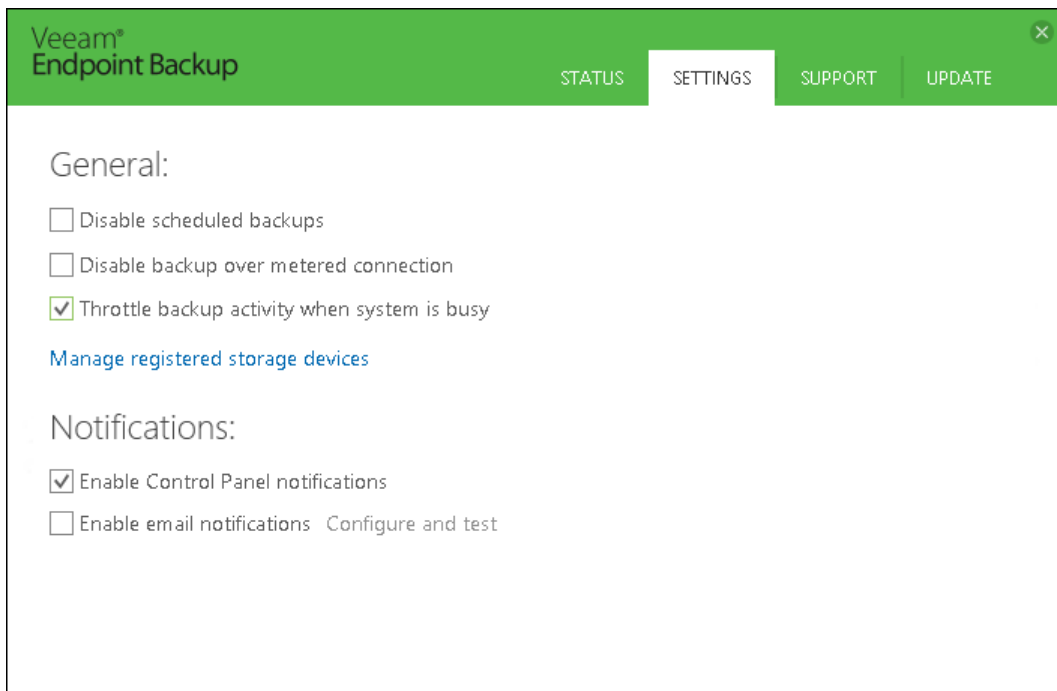
Throttling Backup Activities

You can instruct Veeam Endpoint Backup 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 Endpoint Backup sets low priority for Veeam Endpoint Backup components engaged in the backup process. If this option is not enabled, Veeam Endpoint Backup components have normal priority.

To enable the throttling option for backup activities:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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.



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.

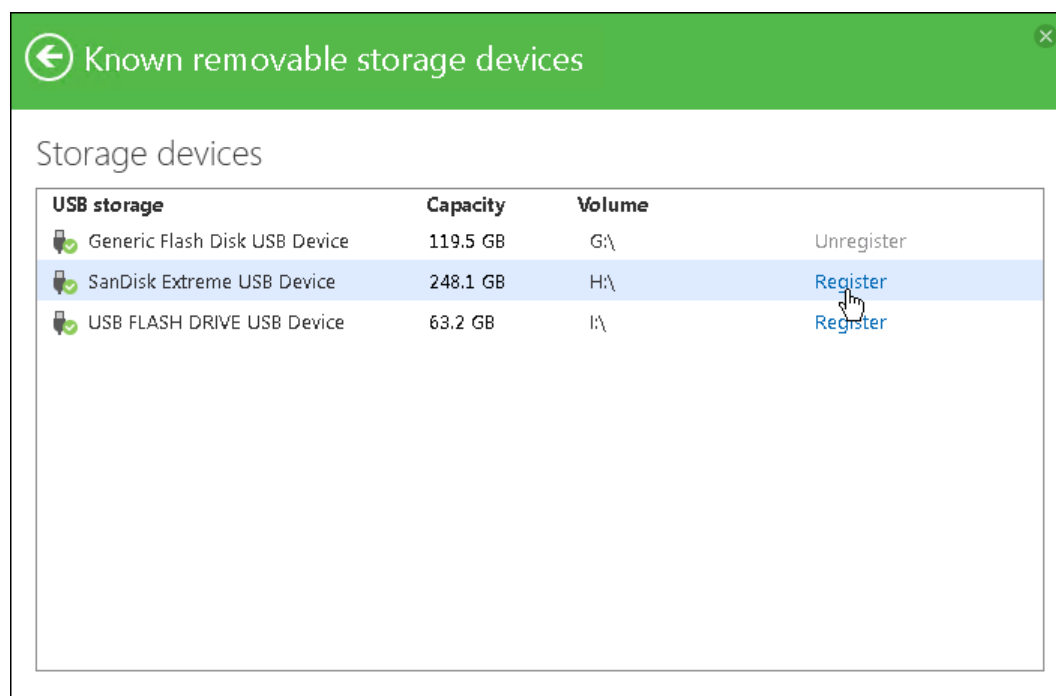
The drive on which you plan to store a backup must be registered in Veeam Endpoint Backup. If the drive is not registered, Veeam Endpoint Backup will not be able to detect the drive and store a backup on it.

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 Endpoint Backup.

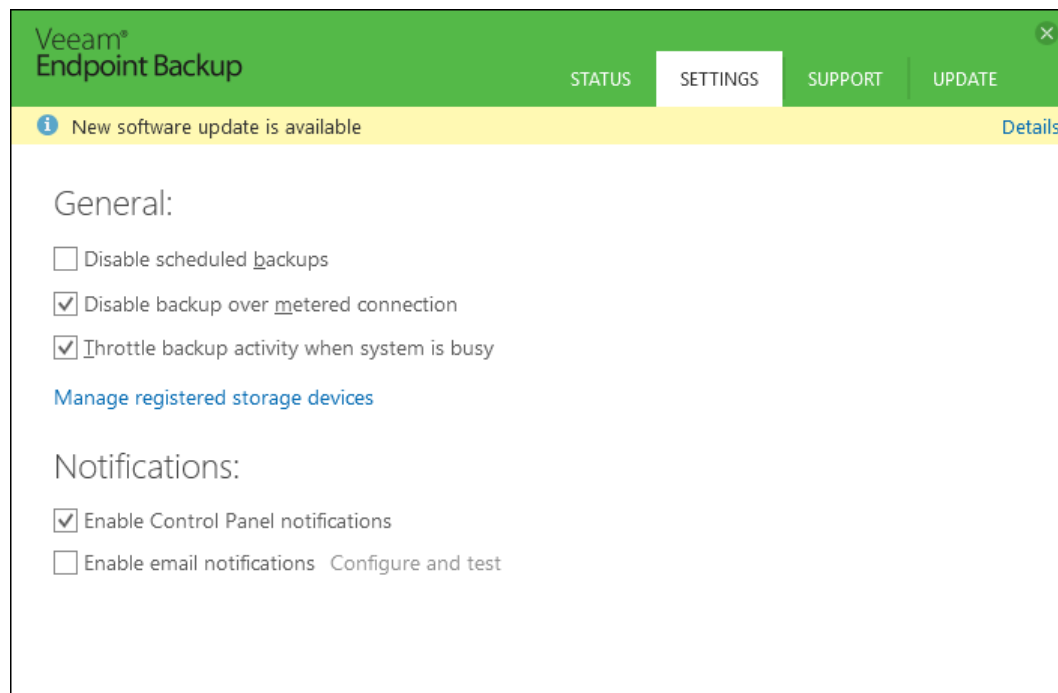
To register and unregister a drive in Veeam Endpoint Backup:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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.



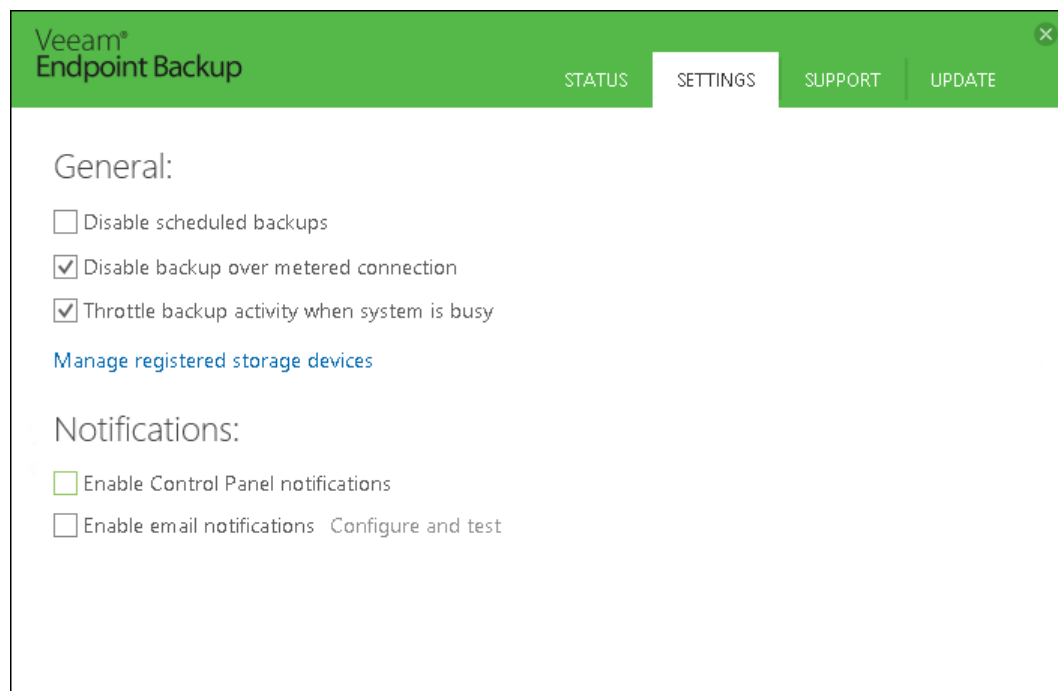
Disabling Control Panel Notifications

Veeam Endpoint Backup displays warning and information messages on the notification bar in the Control Panel. If necessary, you can disable Veeam Endpoint Backup notifications.



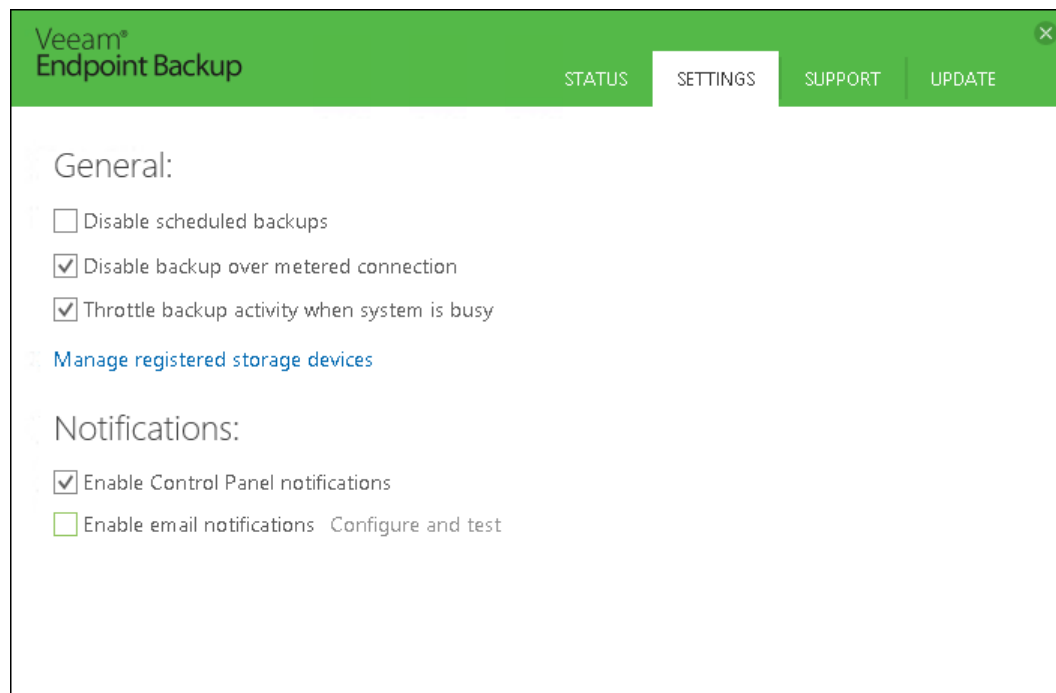
To disable notifications:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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.



Enabling Email Notifications

You can enable Veeam Endpoint Backup email notifications to receive reports containing data on the latest backup job session statistics and result.





To enable email notifications:


1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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.
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 Endpoint Backup will try to automatically detect SMTP server settings. If the SMTP server settings are detected successfully, Veeam Endpoint Backup 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](#).

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 Endpoint Backup database.

 Configure and test email notifications 

Email settings:





Notify on:

☒ Success ☒ Warning ☒ Error

[Show SMTP server settings](#)

Click to automatically detect SMTP server settings.

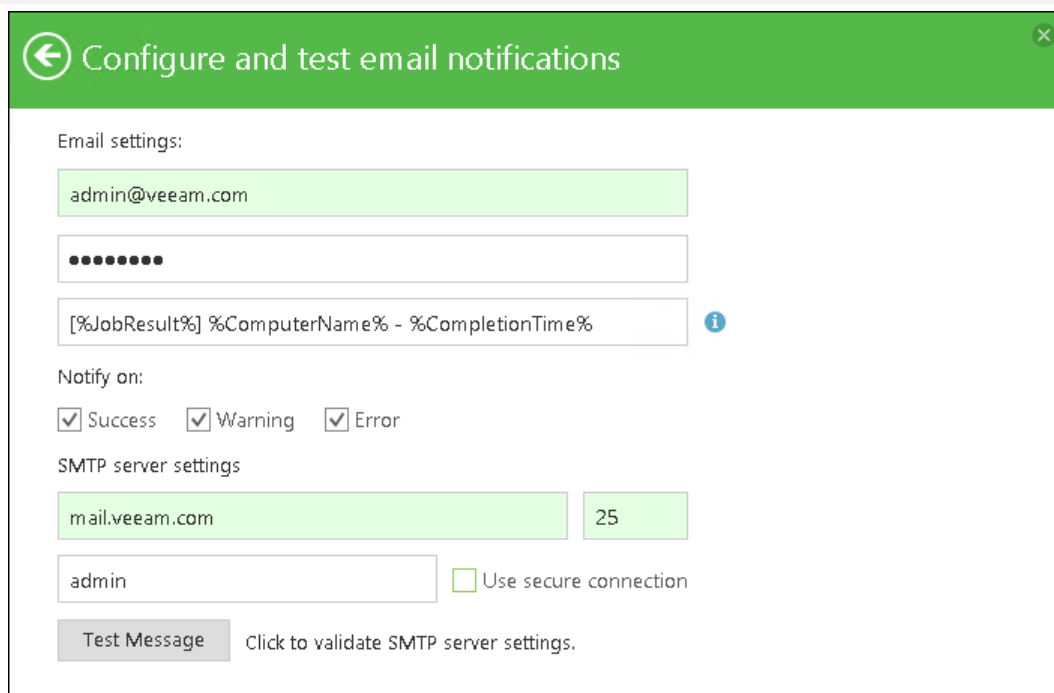
Configuring SMTP Server Settings

When you specify recipient email address, Veeam Endpoint Backup tries to automatically detect settings to connect to the SMTP server. You can change automatically detected settings, for example, when Veeam Endpoint Backup 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.

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 Endpoint Backup will try to detect settings for the specified email address.



The screenshot shows a dialog box titled "Configure and test email notifications" with a green header bar. Inside the dialog, there are several sections for configuring email settings:

- Email settings:** Includes a text field for the recipient email address (containing "admin@veeam.com"), a password field (masked with dots), and a text field for the email body template (containing "[%JobResult%] %ComputerName% - %CompletionTime%").
- Notify on:** Includes three checkboxes: "Success" (checked), "Warning" (checked), and "Error" (checked).
- SMTP server settings:** Includes a text field for the SMTP server DNS name (containing "mail.veeam.com"), a text field for the port number (containing "25"), a text field for the user name (containing "admin"), and a checkbox for "Use secure connection" (unchecked).
- Test Message:** A button labeled "Test Message" with the text "Click to validate SMTP server settings." next to it.

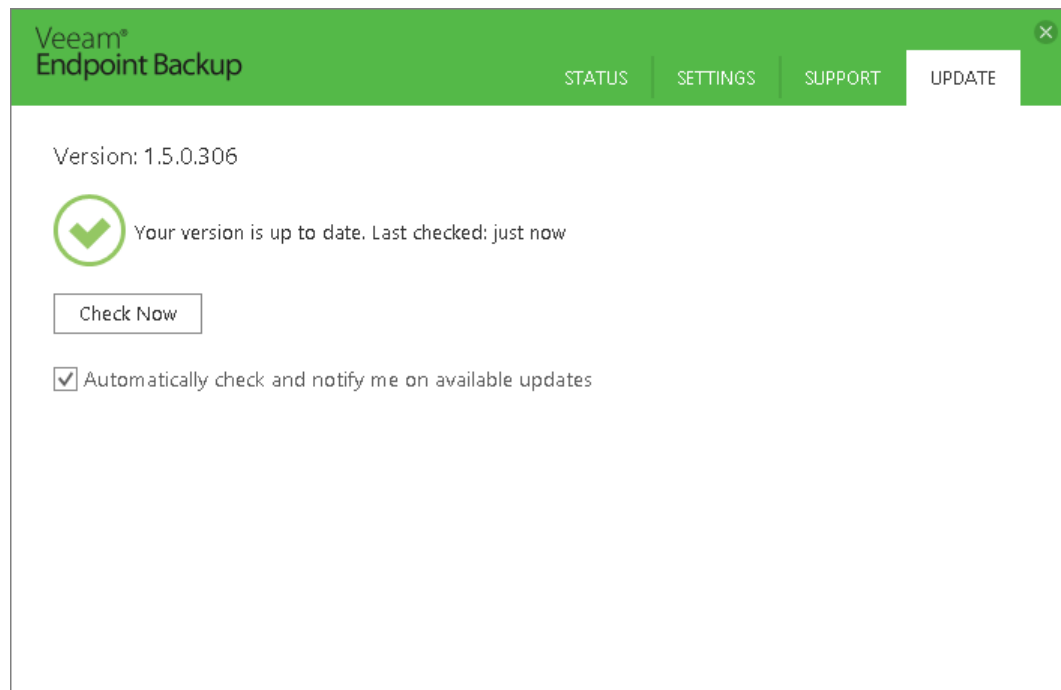
Checking for New Product Versions and Updates

You can set up Veeam Endpoint Backup to automatically notify you about new product versions and updates. When a new version or patch becomes available, Veeam Endpoint Backup displays a notification in the notification bar. You can download the setup file and update Veeam Endpoint Backup. To learn more, see [Upgrading Veeam Endpoint Backup](#).

By default, automatic notifications are enabled. To disable notifications:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup icon in the system tray and select **Control Panel**.
2. Click the **Update** tab.
3. Clear the **Automatically check and notify me on available updates** check box.

To manually check if product updates are available, click **Check Now**.



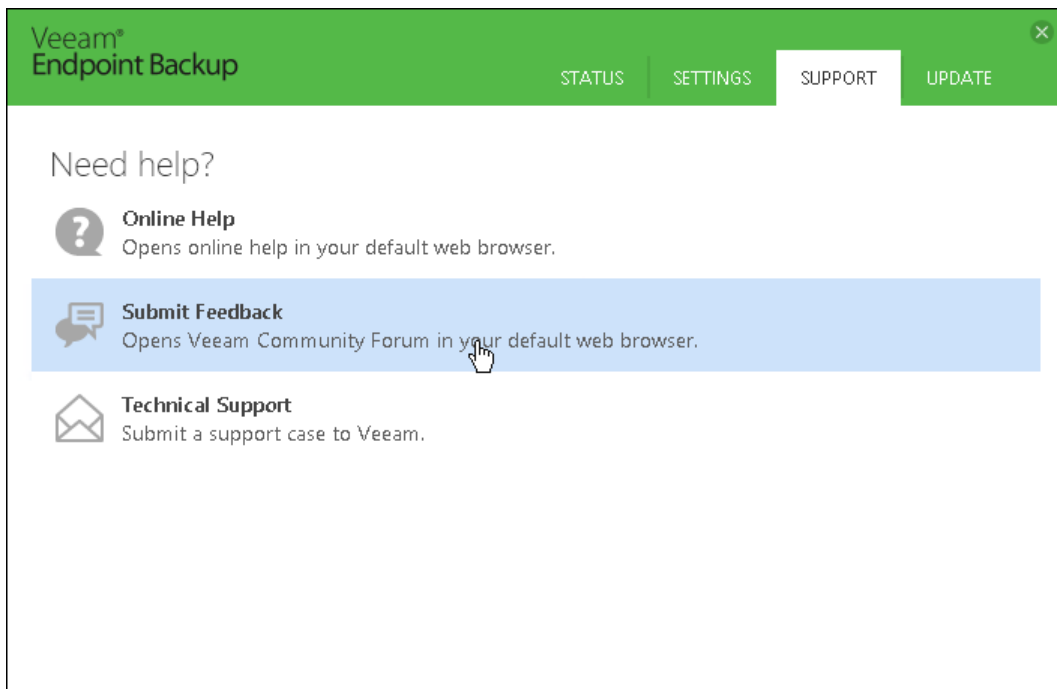
GETTING SUPPORT

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

- You can open online help for Veeam Endpoint Backup.
- 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 Endpoint Backup:

1. Right-click the Veeam Endpoint Backup 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.



Reporting Issues

For Veeam Endpoint Backup, Veeam Software provides support by email only.

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 Endpoint Backup.
- You can submit a support case only in the Control Panel of the current version of Veeam Endpoint Backup. If you use older version of Veeam Endpoint Backup, upgrade Veeam Endpoint Backup and check whether the problem still exists in the current version. If the problem exists, use the Control Panel to submit a support case.

To submit a support case in the Control Panel:

1. Double-click the Veeam Endpoint Backup icon in the system tray or right-click the Veeam Endpoint Backup 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 is 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 Endpoint Backup will automatically collect logs from your computer and open a support case at the Veeam Customer Center Portal.

Report an issue

For this free product, we offer email-only support depending on our staff availability. You will receive a response to the email address provided in the form below. Please, do not contact Veeam Customer Support directly with any queries related to this free product.

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 Endpoint Backup reports that the Tray Agent is not connected to the Veeam Endpoint Backup Service.

What can I do to fix the problem?

Thank you,
John

☒ I agree that debug logs will be uploaded to Veeam servers automatically

Submit Case

USING WITH VEEAM BACKUP & REPLICATION

If you plan to use Veeam Endpoint Backup with Veeam Backup & Replication, you must install Veeam Backup & Replication 8.0 Update 2 or later on the Veeam backup server.

Veeam Endpoint Backup integrates with Veeam Backup & Replication and lets you perform a number of additional disaster recovery tasks and administrative actions with Veeam Endpoint backups. You can:

Data protection tasks

- Create Veeam Endpoint backups on backup repositories
- Copy Veeam Endpoint backups to secondary backup repositories
- Archive Veeam Endpoint backups to tape

Restore tasks

- Restore files and folders from Veeam Endpoint backups
- Restore application items from Veeam Endpoint backups
- Restore disks from Veeam Endpoint backups

Administrative tasks

- Import Veeam Endpoint backups
- Enable and disable Veeam Endpoint backup jobs
- Delete Veeam Endpoint Backup jobs
- Remove Veeam Endpoint backups
- View Veeam Endpoint 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.

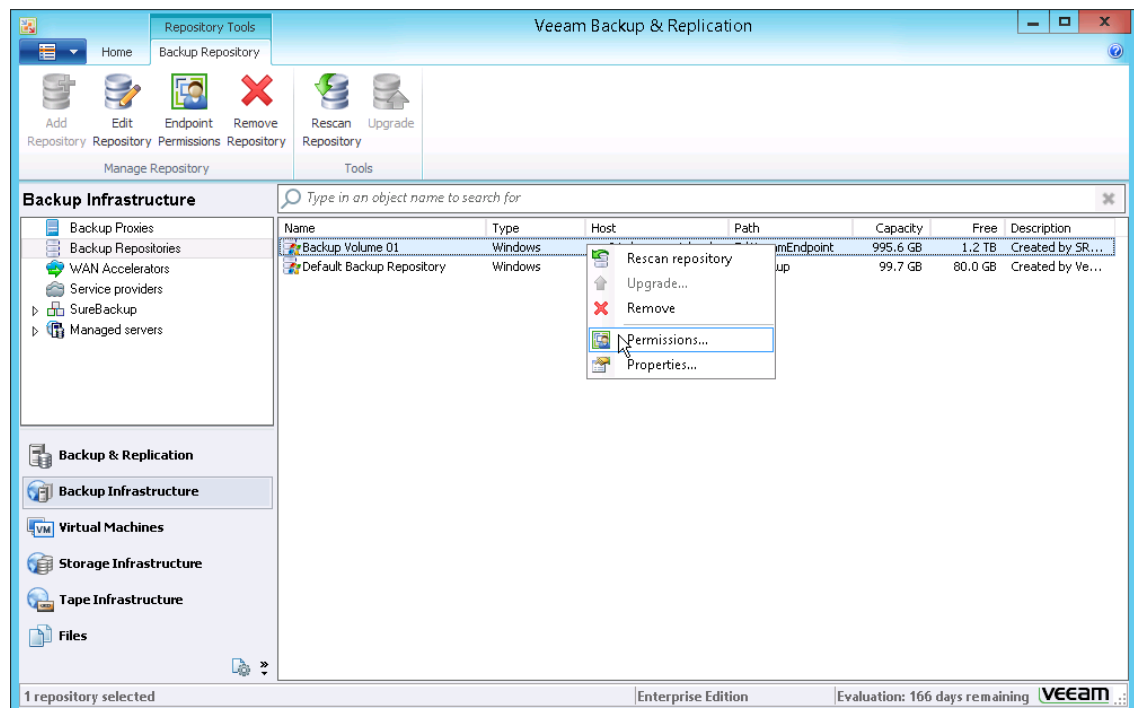
Access permissions are granted to security principals such as users and AD groups by the backup administrator working with Veeam Backup & Replication. Users with granted access permissions can target Veeam Endpoint backup jobs at this backup repository and perform restore from backups located on this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

Mind the following presets and limitations:

- 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.
- You cannot set up user permissions for cloud repositories and save Veeam Endpoint backups directly to these repositories. However, you can configure a backup copy job to copy Veeam Endpoint backups from a regular backup repository to the cloud repository. To learn more, see [Performing Backup Copy for Veeam Endpoint Backups](#).

To grant access permissions to a security principal:

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Backup Repositories** node.
3. In the working area, select the necessary backup repository and click **Endpoint Permissions** on the ribbon or right-click the backup repository and select **Permissions**. If you do not see the **Endpoint Permissions** button on the ribbon or the **Permissions** command is not available in the shortcut menu, press and hold the **[CTRL]** key, right-click the backup repository and select **Permissions**.



4. In the **Endpoint Backup Permissions** window, specify to whom you want to grant access permissions on this backup repository:
 - **Allow 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 only the following users or groups** — 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 Endpoint backup files stored on the backup repository, select the **Encrypt backup files 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](#).

Endpoint Backup Permissions

Repository access:

☐ Deny everyone

☐ Allow everyone

☒ Allow only the following users or groups:

User or group	
VEEAM\jdoe	
VEEAM\msmith	
VEEAM\nwhite	

Add Remove

☒ Encrypt backups stored in this repository

Password:

Standard password (Password age: 2 days) Add...

☒ Loss protection enabled [Manage passwords](#)

OK Cancel

Performing Data Protection Tasks

You can perform the following data protection tasks:

- Back up your data and store the resulting backup files on a backup repository managed by a Veeam backup server
- Copy Veeam Endpoint backups from the backup repository to a secondary backup repository with backup copy jobs
- Archive Veeam Endpoint backups to tapes with backup to tape jobs

Backing Up to Backup Repositories

You can store backups created with Veeam Endpoint Backup on backup repositories connected to Veeam backup servers. To do this, you must perform the following actions:

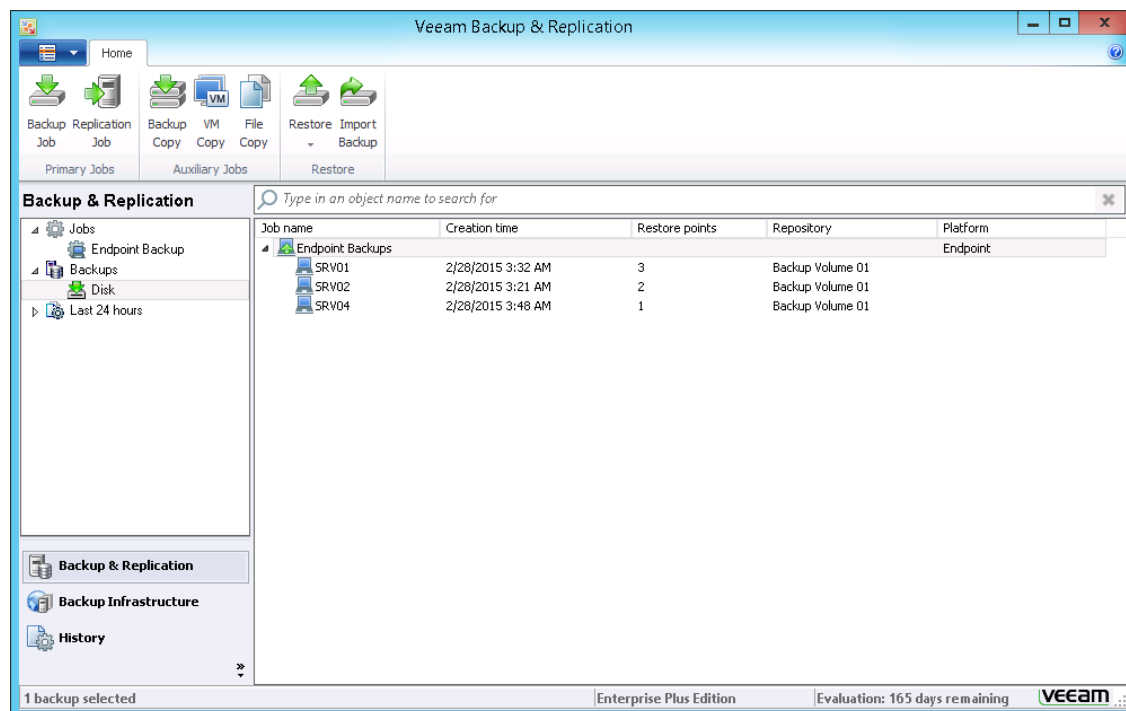
1. Set up user permissions at the backup repository side.
2. Point the Veeam Endpoint backup job to the backup repository.

The user who creates a Veeam Endpoint 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, s/he 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 > Endpoint Backup** node in the **Backup & Replication** view. Backups created with Veeam Endpoint Backup are available under the **Disk** node in **Backup & Replication** view.

The backup administrator working with Veeam Backup & Replication can manage Veeam Endpoint backup jobs and restore data from these backups. To learn more, see [Performing Restore Tasks](#) and [Performing Administration Tasks](#).

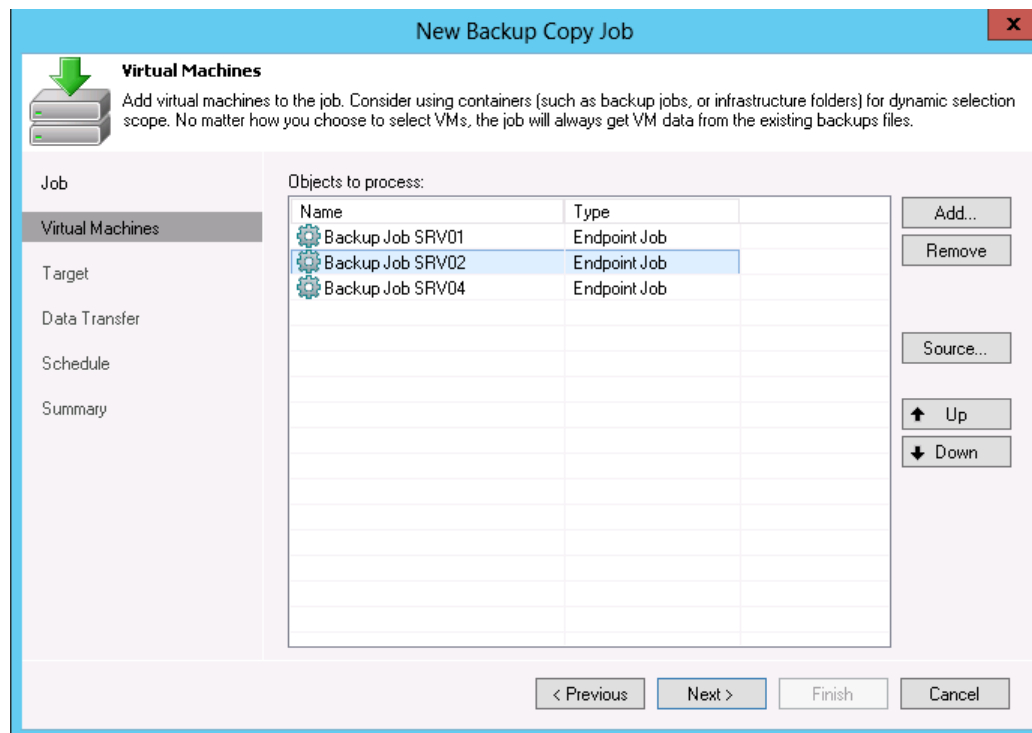


Performing Backup Copy for Veeam Endpoint Backups

You can configure backup copy jobs that will copy backups created with Veeam Endpoint Backup to a secondary backup repository.

Backup copy jobs treat Veeam Endpoint 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](#).

Backup copy jobs processing Veeam Endpoint backups have one limitation: you cannot use backup mapping for Veeam Endpoint backups. As a result, if you have a full Veeam Endpoint backup on the target repository, you will not be able to use this backup as a "seed" for the backup copy job. The backup copy job will always copy the whole Veeam Endpoint backup chain to the target repository.



Restoring Data from Copies of Veeam Endpoint 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 Endpoint Backup.

To do this:

1. In Veeam Endpoint Backup, launch the **Veeam Endpoint Recovery** 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 Endpoint Recovery** 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.

The screenshot shows the 'Veeam Endpoint Recovery' wizard window. The title bar is blue with the text 'Veeam Endpoint Recovery' and a close button. The main window has a light blue header with a green arrow icon and the text 'Backup Server'. Below the header, it says 'Specify Veeam Backup & Replication server name and your Windows credentials using DOMAIN\USERNAME format.' On the left, there is a vertical list of steps: 'Backup Location', 'Network Storage', 'Backup Server' (which is highlighted), 'Backup', 'Restore Point', 'Disk Mapping', 'Summary', and 'Progress'. The main area contains the following fields: 'Veeam backup server name or IP address:' with a text box containing '172.17.53.12'; a checked checkbox 'Specify your personal credentials:'; a 'Username:' field with 'VEEAM\Administrator'; a 'Password:' field with masked characters; and a 'Port:' field with a dropdown menu showing '10001'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Archiving Veeam Endpoint Backups to Tape

You can configure backup to tape jobs to archive Veeam Endpoint backups to tape.

Backup to tape jobs treat Veeam Endpoint 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](#).

Backup to tape jobs processing Veeam Endpoint backups have one limitation: you cannot link jobs that process Veeam Endpoint backups to other jobs. Use other scheduling options instead.

New Backup to Tape Job

Backup Files
Specify backups to be processed by this job. You can pick individual backup jobs, or complete backup repositories.

Name	Type
Backup Job SRV04	Endpoint Backup
Backup Job SRV03	Endpoint Backup

Full: **85.6 GB**
Incremental: **15.2 GB**

< Previous Next > Finish Cancel

Performing Restore Tasks

You can perform the following restore operations:

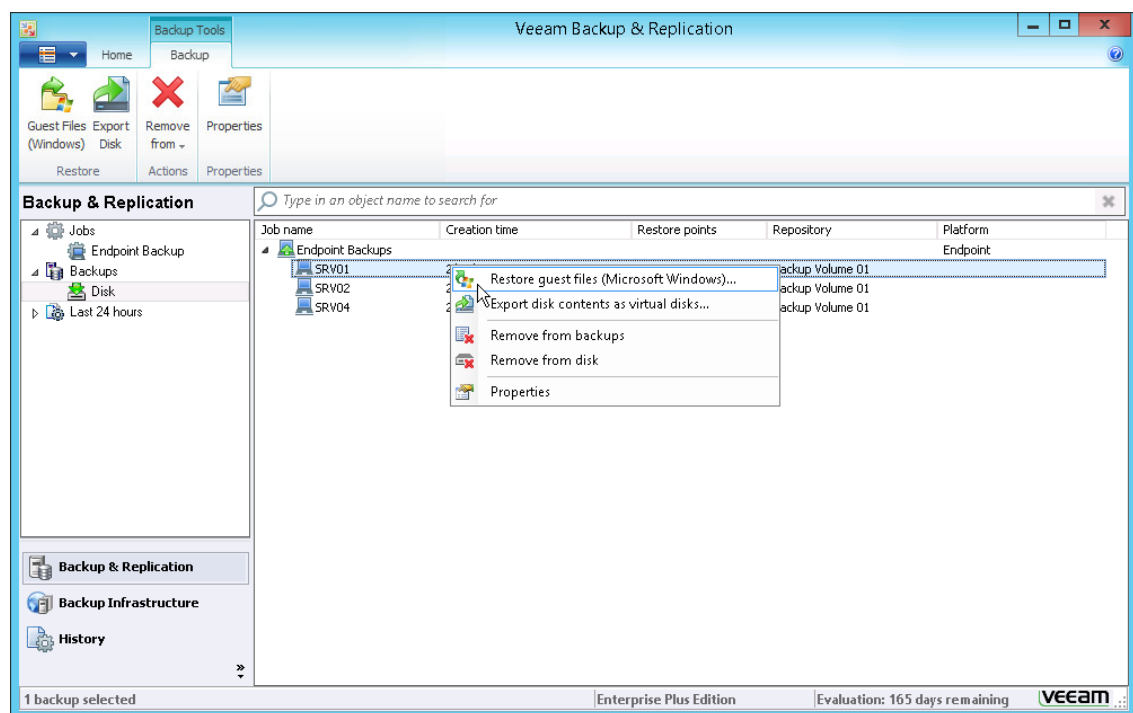
- Restore individual files and folders from Veeam Endpoint backups
- Restore application items from Veeam Endpoint backups with Veeam Explorers
- Export computer disks as VMDK, VHD or VHDX disks

Restoring Files and Folders

You can restore individual files and folders from Veeam Endpoint 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](#).

File-level restore from Veeam Endpoint backups has one limitation: you cannot restore files to their original location. Instead, use the **Copy To** option to save restored files and folders in a new location.



Restoring Application Items

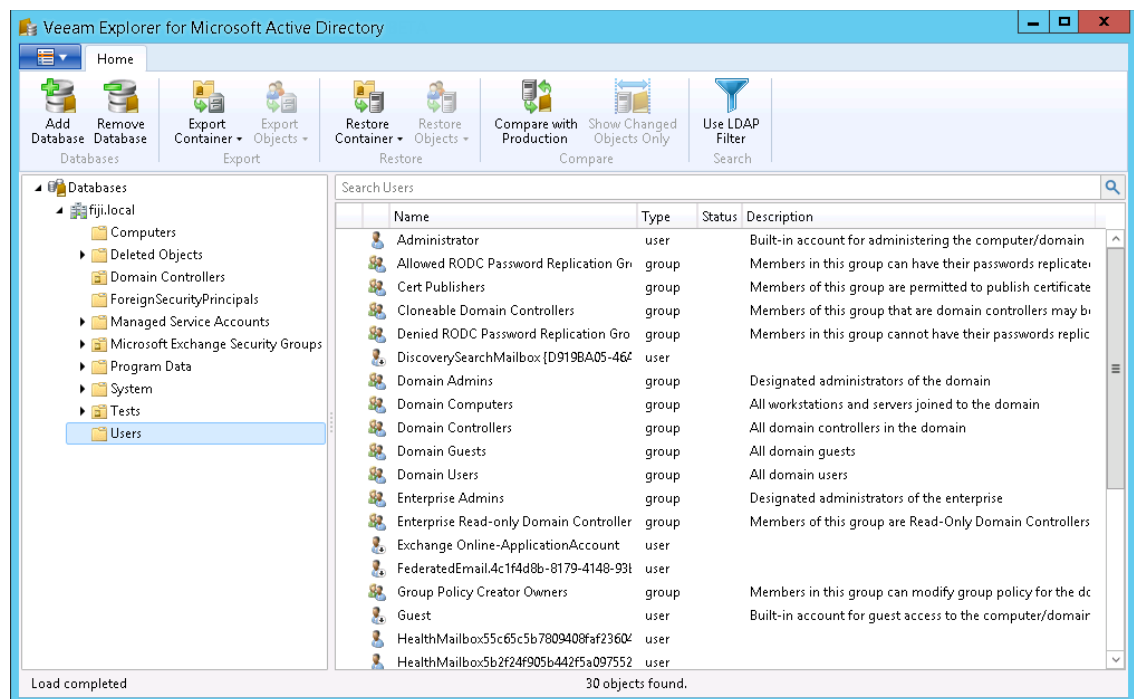
You can use Veeam Explorers to restore application items from backups created with Veeam Endpoint Backup. Veeam Backup & Replication lets you restore items and objects from the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server

The procedure of application-item restore does not differ from the regular one. To restore application items:

1. In Veeam Backup & Replication, locate the necessary Veeam Endpoint backup.
2. Open the necessary Veeam Explorer to initiate application-item restore.
3. Use the Veeam Explorer to restore application items you need.

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 Endpoint Backup 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 Endpoint Backup 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 Endpoint Backup 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.

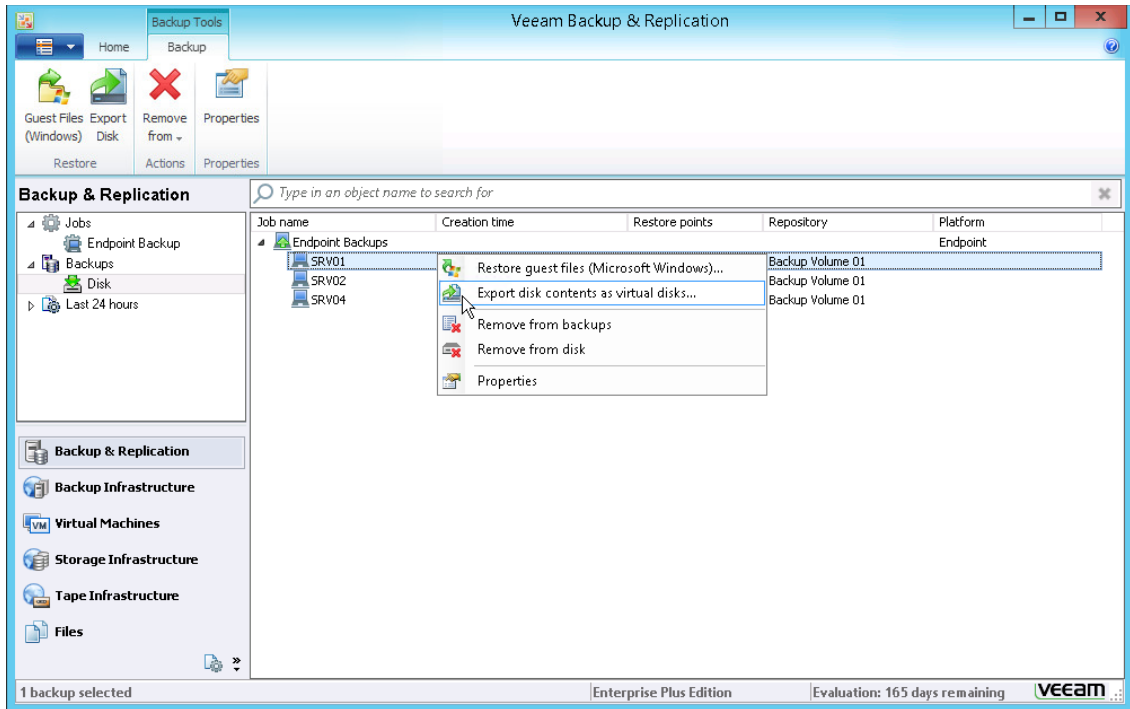
Veeam Endpoint Backup supports batch disk restore. For example, if you choose to restore 2 computer disks, Veeam Endpoint Backup will convert them to 2 virtual disks and store these disks in the specified location.

To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

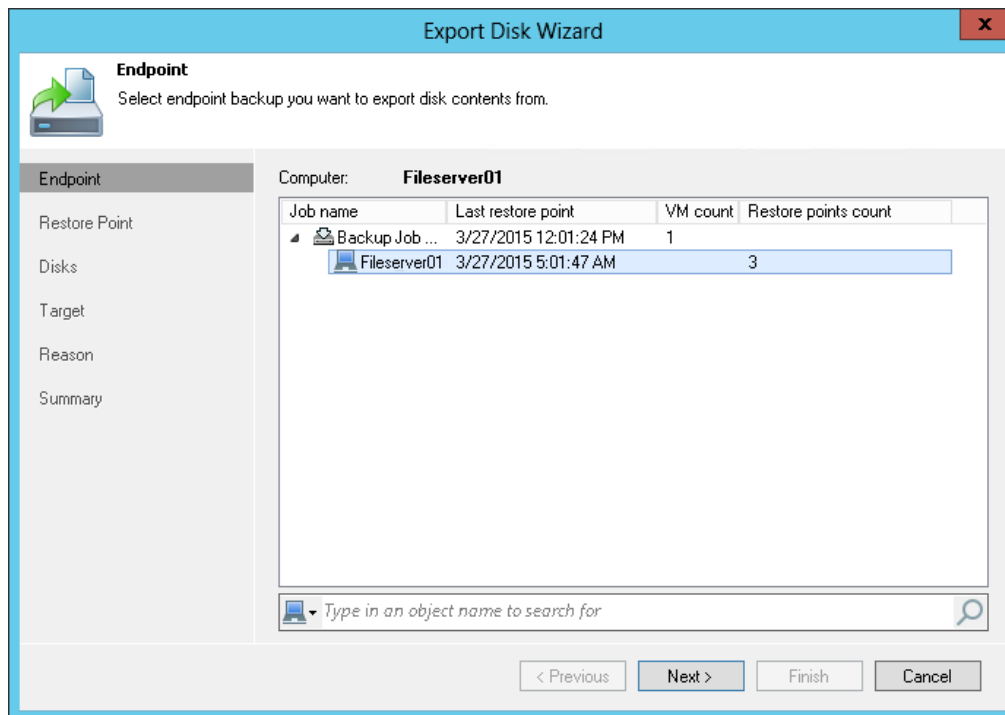
To launch the **Veeam Endpoint Recovery** wizard, do either of the following:

- In Veeam Backup & Replication, open the **Home** tab and click **Restore** > **Endpoint** > **Export disk contents as virtual disks**.
- In Veeam Backup & Replication, open the **Backup & Replication** view. In the inventory pane, click **Disk** under the **Backups** node. In the working area, expand the **Endpoint Backups** 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.



Step 2. Select Backup

At the **Endpoint** step of the wizard, select a backup from which you want to restore disk(s). In the list of backups, Veeam Endpoint Backup displays all backups that are currently hosted on the backup repository. Make sure that you select a volume-level backup in the list.



Export Disk Wizard

Endpoint
Select endpoint backup you want to export disk contents from.

Endpoint

Restore Point

Disks

Target

Reason

Summary

Computer: **Fileserver01**

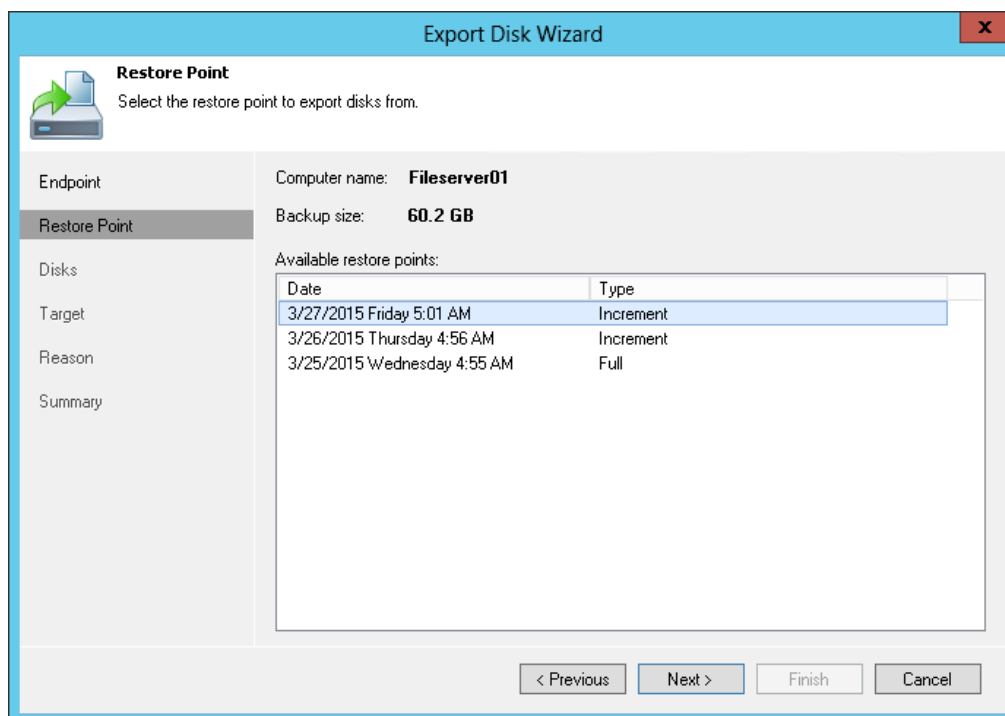
Job name	Last restore point	VM count	Restore points count
Backup Job ...	3/27/2015 12:01:24 PM	1	
Fileserver01	3/27/2015 5:01:47 AM	3	

Type in an object name to search for

< Previous Next > Finish Cancel

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 Endpoint Backup 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.

Endpoint

Restore Point

Disks

Target

Reason

Summary

Computer name: **Fileserver01**

Backup size: **60.2 GB**


Available restore points:

Date	Type
3/27/2015 Friday 5:01 AM	Increment
3/26/2015 Thursday 4:56 AM	Increment
3/25/2015 Wednesday 4:55 AM	Full

< Previous Next > Finish Cancel

Step 4. Select Disks

At the **Disks** step of the wizard, select check boxes next to those disks that you want to export.



Disks

Select on or more physical disks to export.

Endpoint

Restore Point

Disks

Target

Reason

Summary

Physical disks:

Disk name	Volumes	Size
<input checked="" type="checkbox"/> Disk 1	Local Disk (E:)	59.9 GB

Select All

Clear All

< Previous

Next >

Finish

Cancel

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.

Endpoint
Restore Point
Disks
Target
Reason
Summary

Server:
esx18.veeam.local Details

Path to folder:
[datastore3] Browse...

Export format:

☒ **VMDK**
This virtual disk type is used by VMware products such as VMware Workstation, or VMware vSphere. Maximum VMDK disk size is 62TB.

☐ **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.

< Previous Next > Finish Cancel

Step 6. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

Tip: If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.

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.

Endpoint
Restore Point
Disks
Target
Reason
Summary

Restore reason:
Converting volume to virtual disk

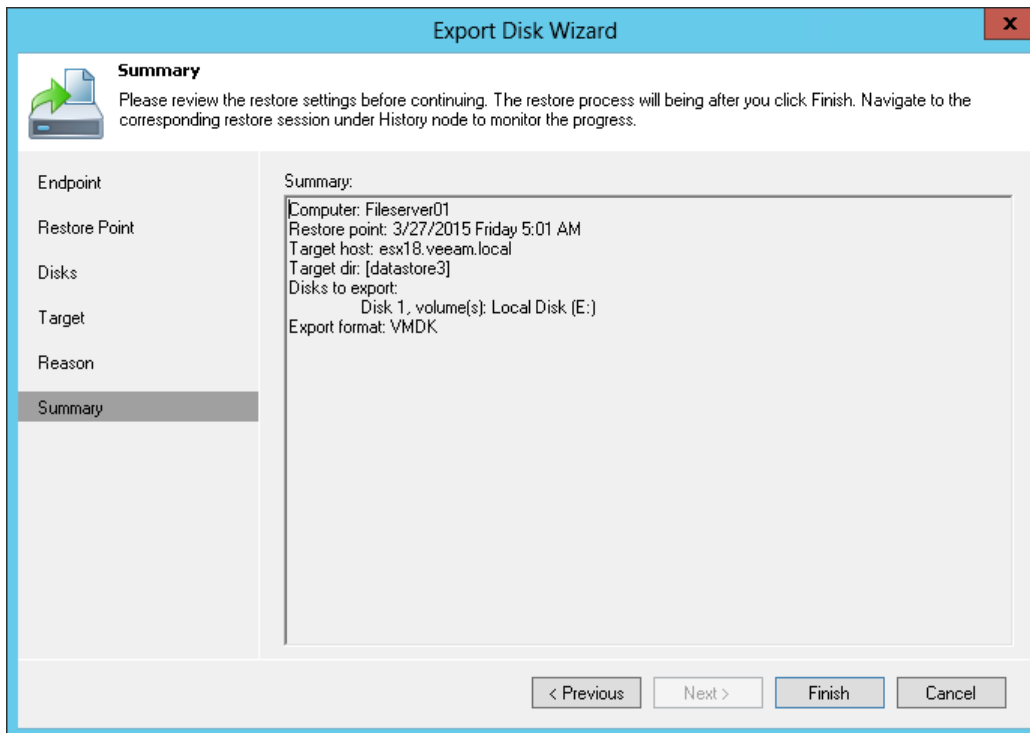
☐ Do not show me this page again

< Previous Next > Finish Cancel

Step 7. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure disk restore.

1. Review details for the disk to be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.



Performing Administration Tasks

You can manage Veeam Endpoint backup jobs and backups created with these jobs. Veeam Backup & Replication allows you to perform the following administration tasks:

- Import Veeam Endpoint backups
- Enable and disable Veeam Endpoint backup jobs
- Remove Veeam Endpoint backup jobs
- Remove Veeam Endpoint backups
- View Veeam Endpoint backup properties
- Configure global settings
- Assign roles to users

Importing Veeam Endpoint Backups

You may need to import a Veeam Endpoint backup in the Veeam Backup & Replication console in the following situations:

- The Veeam Endpoint backup is stored on a drive managed by another computer (not the Veeam backup server).
- The Veeam Endpoint backup is stored on a backup repository managed by another Veeam backup server.
- The Veeam Endpoint backup has been removed in the Veeam Backup & Replication console.

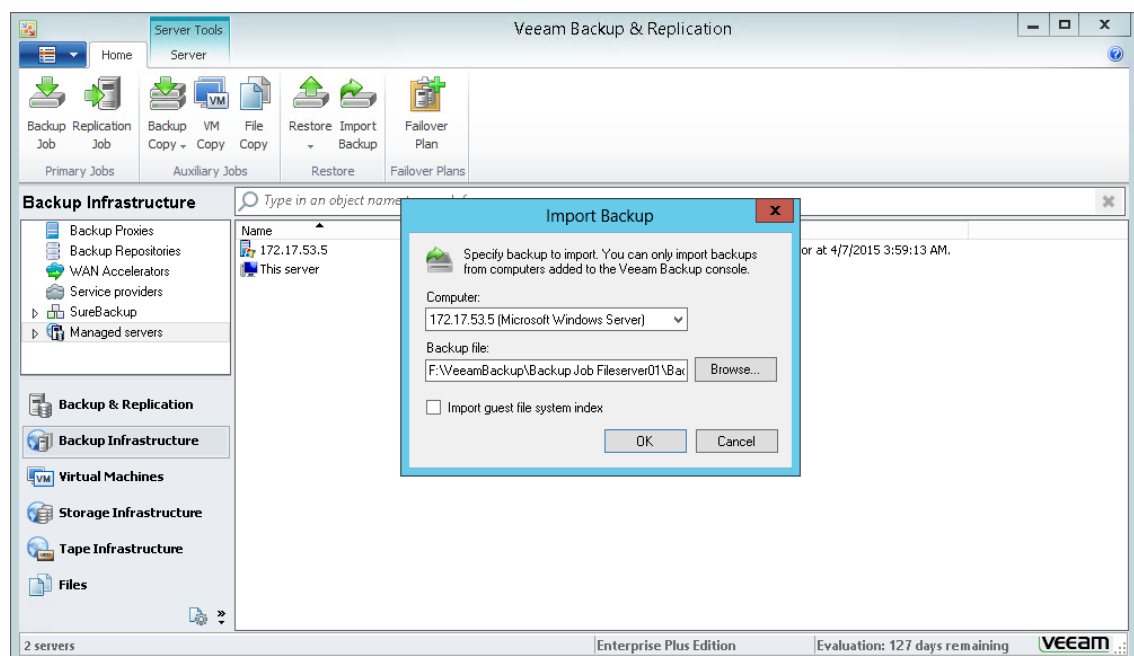
After importing, the Veeam Endpoint backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

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 Endpoint 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 **Backup & Replication** view, under the **Backups > Disk (imported)** node in the inventory pane.



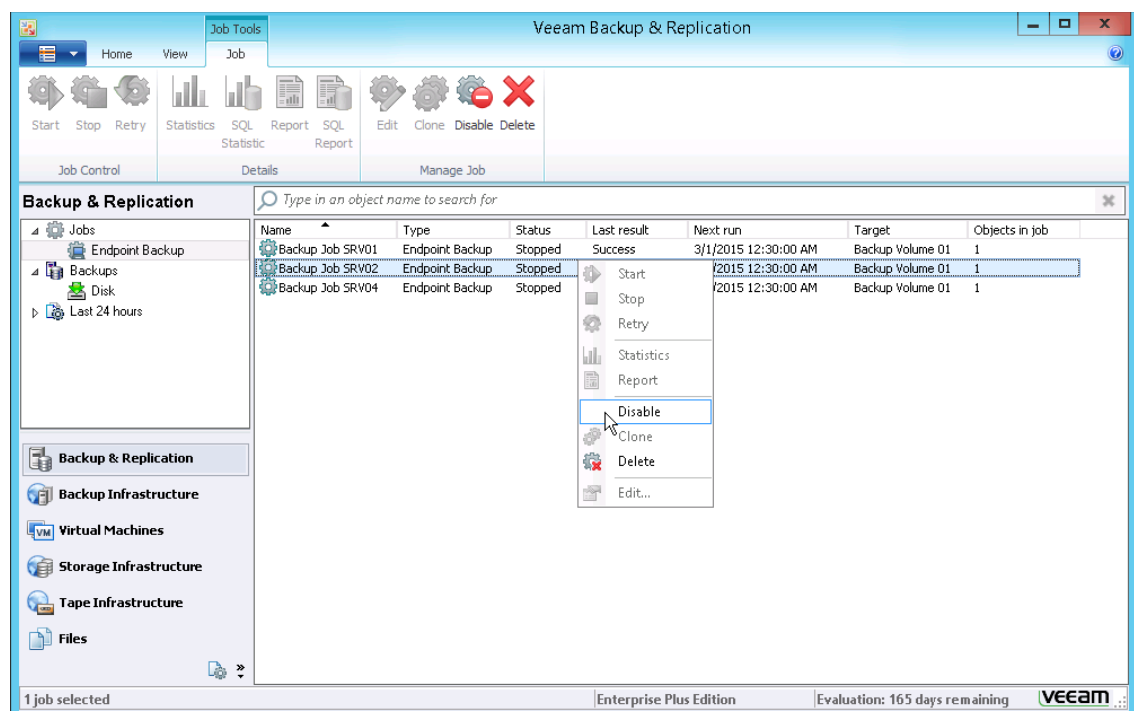
Enabling and Disabling Scheduled Backup Jobs

You can disable and enable Veeam Endpoint 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 Endpoint Backup 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 **Backup & Replication** view.
2. Under the **Jobs** node, click **Endpoint Backup**.
3. Click **Disable** on the toolbar 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.



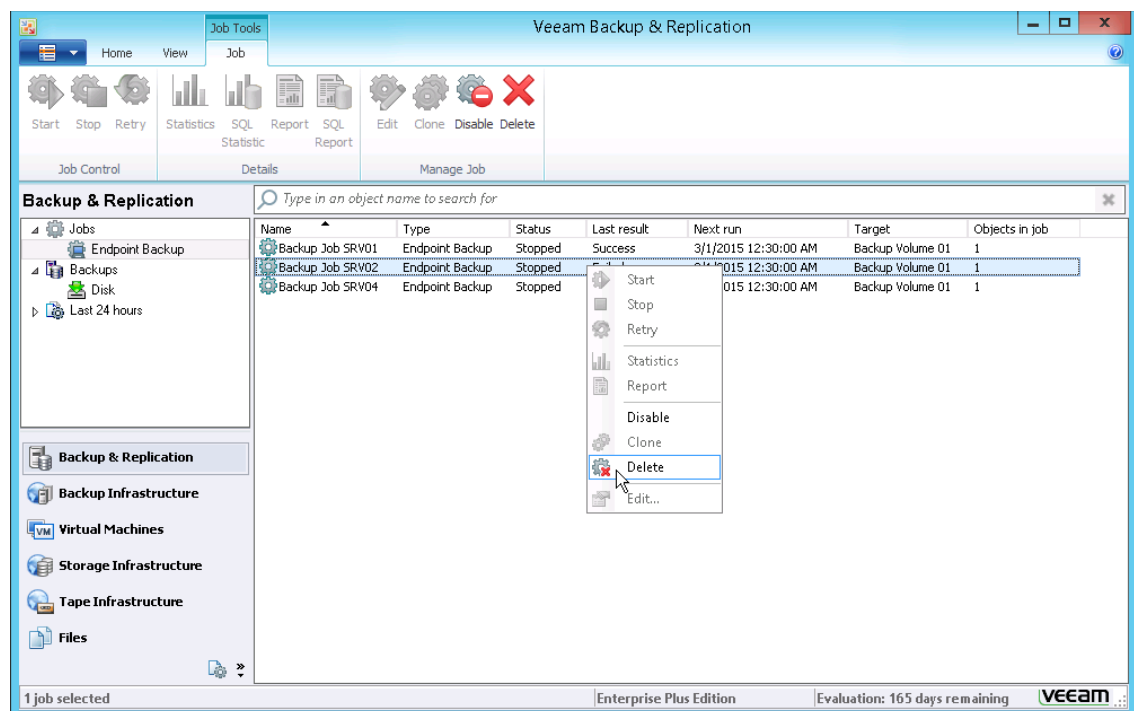
Deleting Veeam Endpoint Backup Jobs

You can delete Veeam Endpoint backup jobs.

When you delete a Veeam Endpoint backup job, Veeam Backup & Replication removes all records about the job from its database and console. When the user starts a new Veeam Endpoint 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 **Backup & Replication** view.
2. Under the **Jobs** node, click **Endpoint Backup**.
3. Click **Delete** on the toolbar or right-click the necessary job in the working area and select **Delete**.



Removing Veeam Endpoint Backups

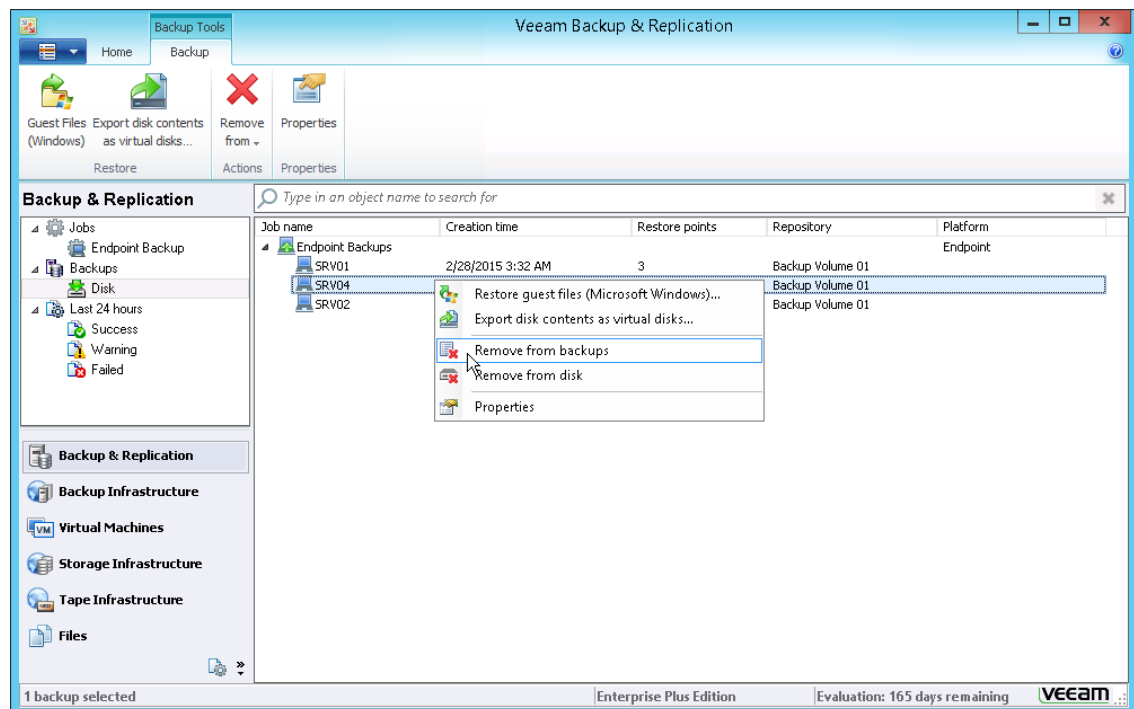
You can remove Veeam Endpoint backups from Veeam Backup & Replication or permanently delete Veeam Endpoint backups from the backup repository.

Removing from Backups

When you remove a Veeam Endpoint backup from backups, 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 Endpoint Backups](#).

To remove a Veeam Endpoint backup from backups:

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 **Endpoint Backups** node, select the necessary backup and click **Remove from > Backups** on the toolbar or right-click the backup and select **Remove from backups**.

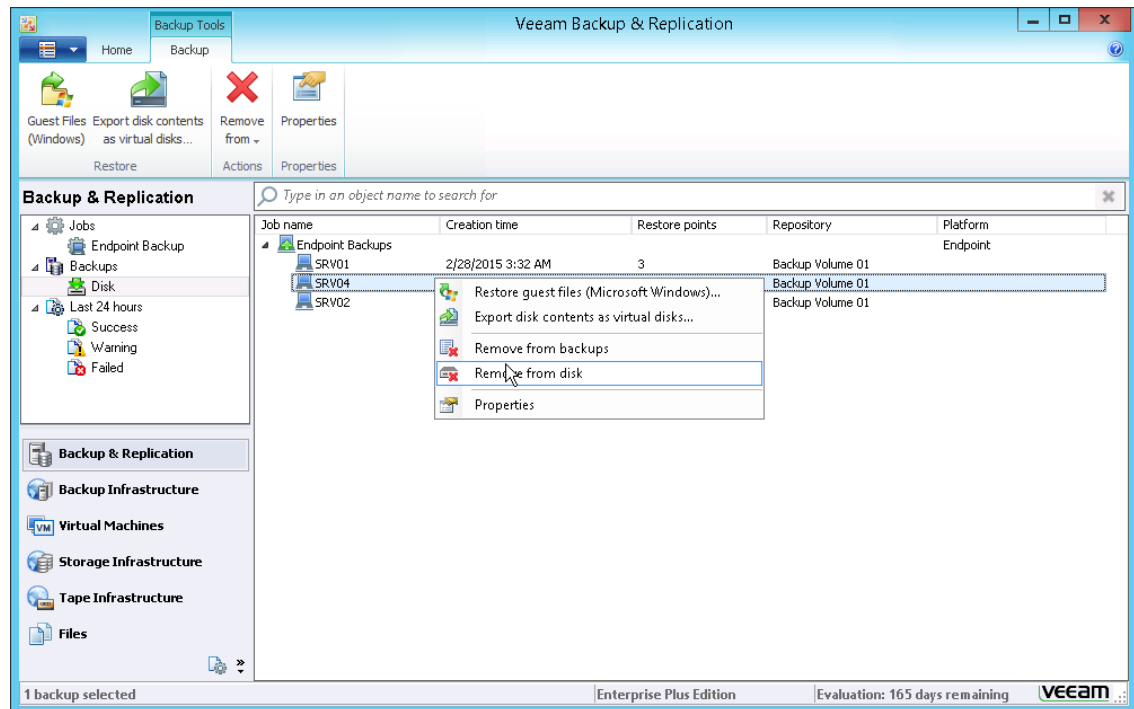


Removing from Backup Repository

When you remove a Veeam Endpoint backup from backups, 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 Endpoint 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 **Endpoint Backups** node, select the necessary backup and click **Remove from > Disk** on the toolbar or right-click the backup and select **Remove from disk**.

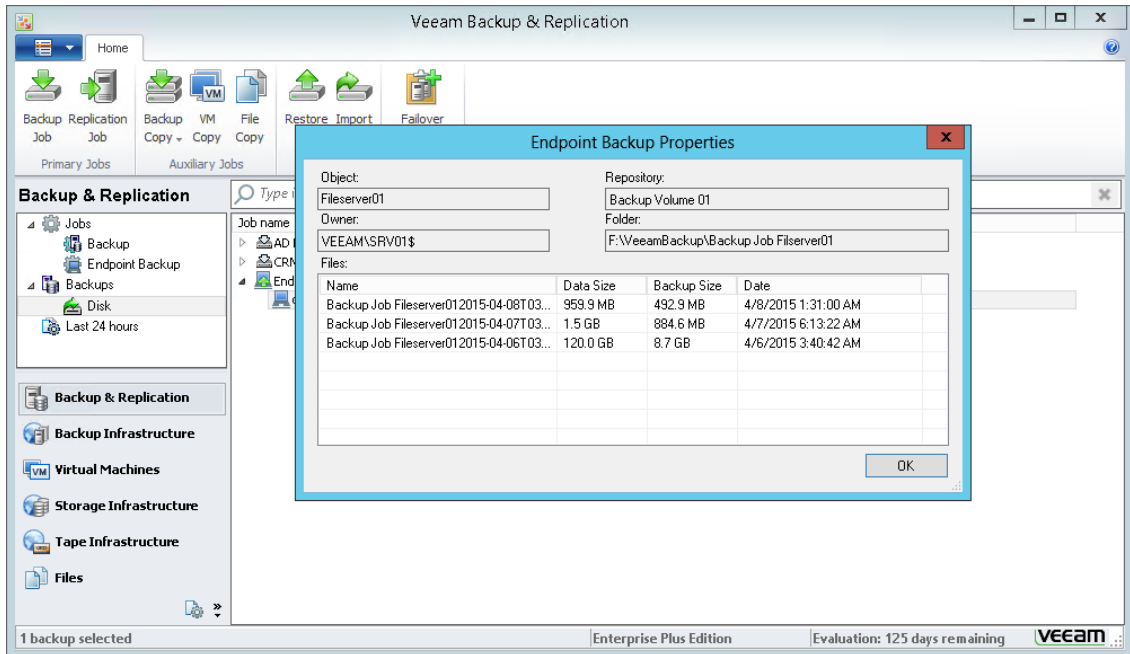


Viewing Veeam Endpoint Backup Statistics

You can view statistics about Veeam Endpoint backups.

To view Veeam Endpoint backup statistics:

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 **Endpoint Backups** node, select the necessary backup and click **Properties** on the toolbar or right-click the backup and select **Properties**.



Configuring Global Settings

Global settings configured on the Veeam backup server apply to Veeam Endpoint backup jobs as well. You can:

- Configure network throttling settings so that Veeam Endpoint backup job does not consume all network resources.
- Configure global email settings to get alerted about the Veeam Endpoint backup job results.

To learn more, see [Veeam Backup & Replication Documentation](#).

Assigning Roles to Users

User roles configured on the Veeam backup server apply to Veeam Endpoint backup jobs as well.

To learn more, see [Veeam Backup & Replication Documentation](#).

APPENDIX A. VEEAM ENDPOINT BACKUP EVENTS

Veeam Endpoint Backup 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 Endpoint Backup.

Event ID	Name	Description	Event Log	Source	Severity
110	Backup Job Started	EndpointBackup job 'Backup Job <computername>' has been started [by user <username>].	Veeam Endpoint Backup	Veeam Endpoint Backup	Information
190	Backup Job Finished	EndpointBackup job 'Backup Job <computername>' finished with <job status>. Job details: <additional information about the job results>*.	Veeam Endpoint Backup	Veeam Endpoint Backup	Information Warning Error
191	Backup Job Retry	EndpointBackup job 'Backup Job <computername>' finished with Error and will be retried. Job details: <additional information about the job results>*.	Veeam Endpoint Backup	Veeam Endpoint Backup	Warning
10010	Restore Point Created	<computername> restore point has been created.	Veeam Endpoint Backup	Veeam Endpoint Backup	Information
10050	Restore Point Removed	Restore point for <computername> has been removed according to the configured retention policy.	Veeam Endpoint Backup	Veeam Endpoint Backup	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 Endpoint Backup.	System	User32	Information
23010	Backup Job Created	EndpointBackup job 'Backup Job <computername>' has been created.	Veeam Endpoint Backup	Veeam Endpoint Backup	Information

Event ID	Name	Description	Event Log	Source	Severity
23050	Backup Job Modified	EndpointBackup job 'Backup Job <computername>' has been modified.	Veeam Endpoint Backup	Veeam Endpoint Backup	Information
23051	Veeam Endpoint Modified	Veeam Endpoint Backup option <optionname> has been changed.***	Veeam Endpoint Backup	Veeam Endpoint Backup	Information
26010	USB Device Ejected	Target USB device has been successfully ejected.	Veeam Endpoint Backup	Veeam Endpoint Backup	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 Endpoint Backup to shut down the computer on successful backup.

*** The event is triggered if the user has changed any Veeam Endpoint Backup setting other than backup job settings.