Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to restore data from a cloud repository and specified settings for the cloud gateway.

Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the service provider.

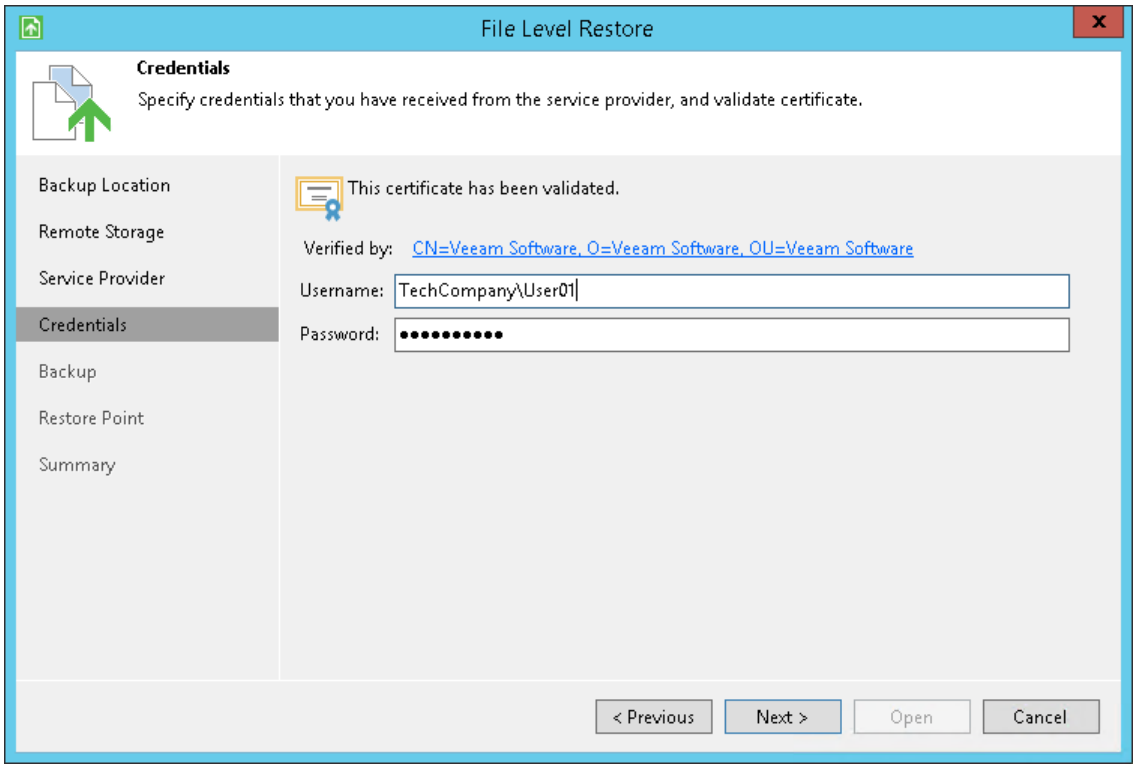
1. At the top of the wizard window, Veeam Agent for Microsoft Windows displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   - To view the TLS certificate, click the certificate link.
   - To verify if the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Fingerprint for certificate verification** field. Click **Verify**. Veeam Agent for Microsoft Windows will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. In the **Username** field, enter the user name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The user name of the subtenant account must be specified in the *TENANT\SUBTENANT* format.

3. In the **Password** field, provide a password for the tenant or subtenant account.

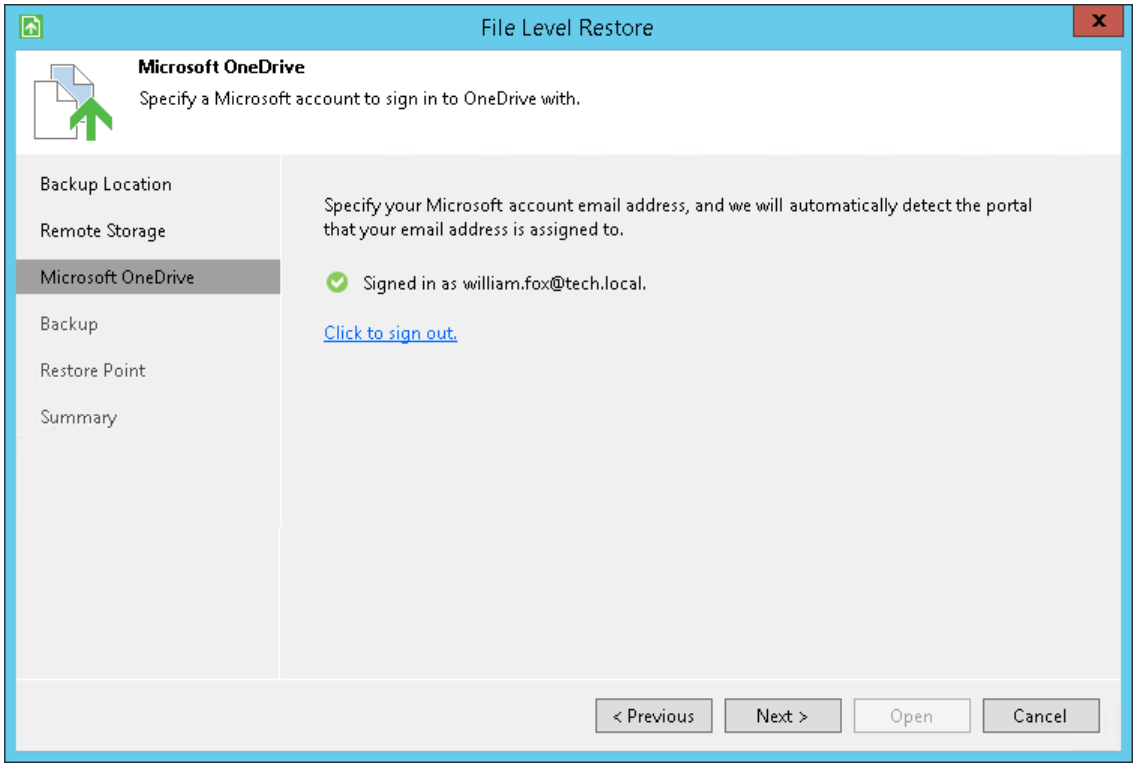


Microsoft OneDrive Settings

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

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

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



Step 5. Select Backup

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

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

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

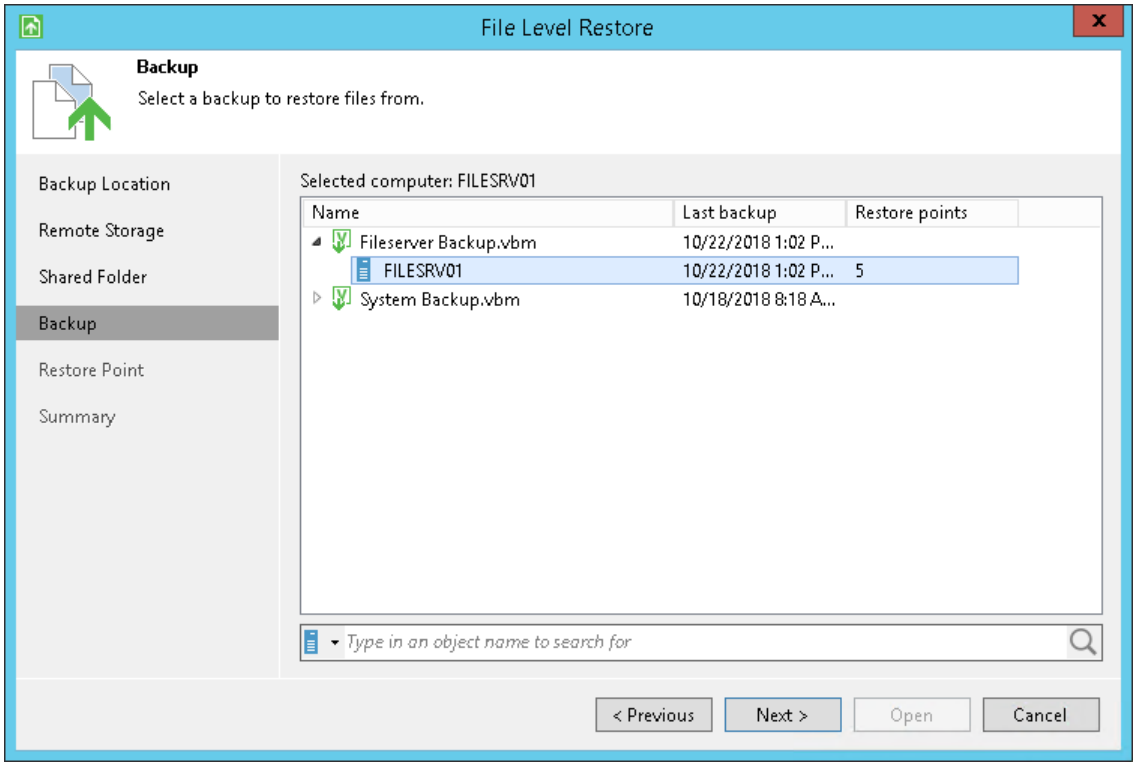
- If you specify credentials for the user who has access to the backup repository, the list of backups will include only backups created by this user.
- If you specify credentials for the user who is assigned the *Backup Administrator* or *Restore Operator* role on the backup server, the list of backups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

If you restore data from a backup stored on the cloud repository, Veeam Agent for Microsoft Windows displays only those backups that are accessible by the user whose credentials are specified at the Credentials step of the wizard:

- If you specify credentials for the tenant account, the list of backups will include backups created by all users who create backups under this account.
- If you specify credentials for the subtenant account, the list of backups will include only those Veeam Agent backups that were created under this subtenant account.

NOTE

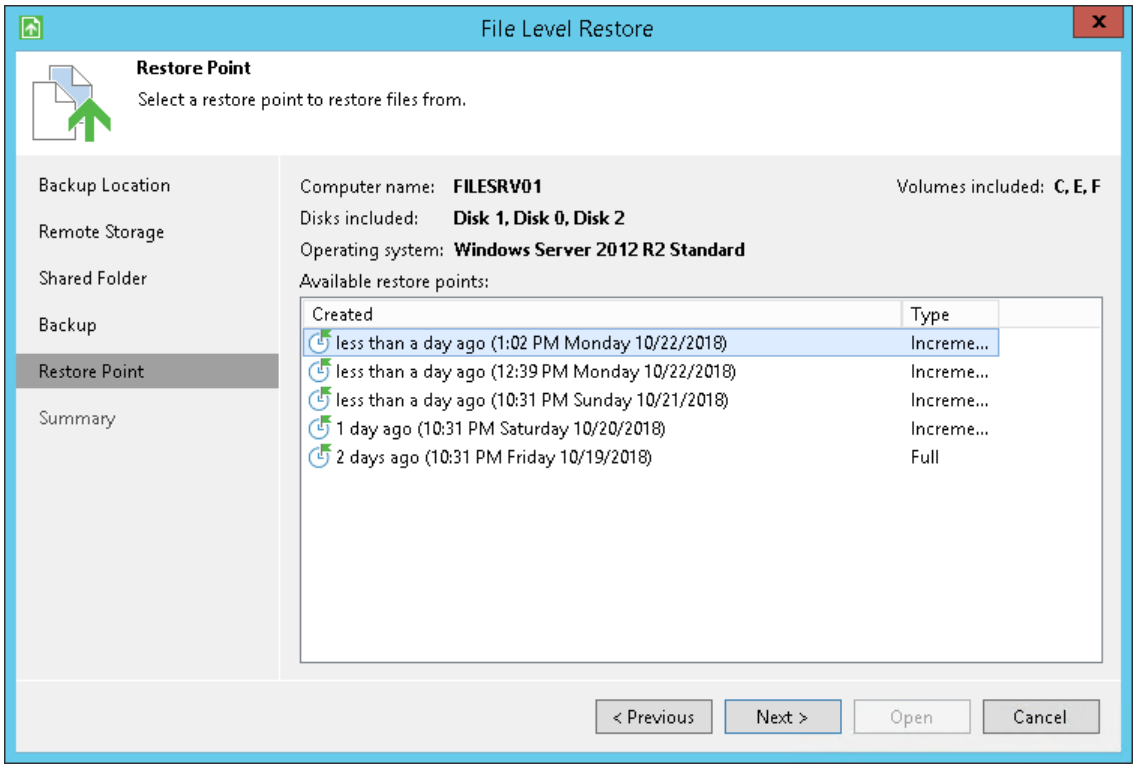
If you restore data from an encrypted backup that was created on another Veeam Agent computer, you need to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.



Step 6. Select Restore Point

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

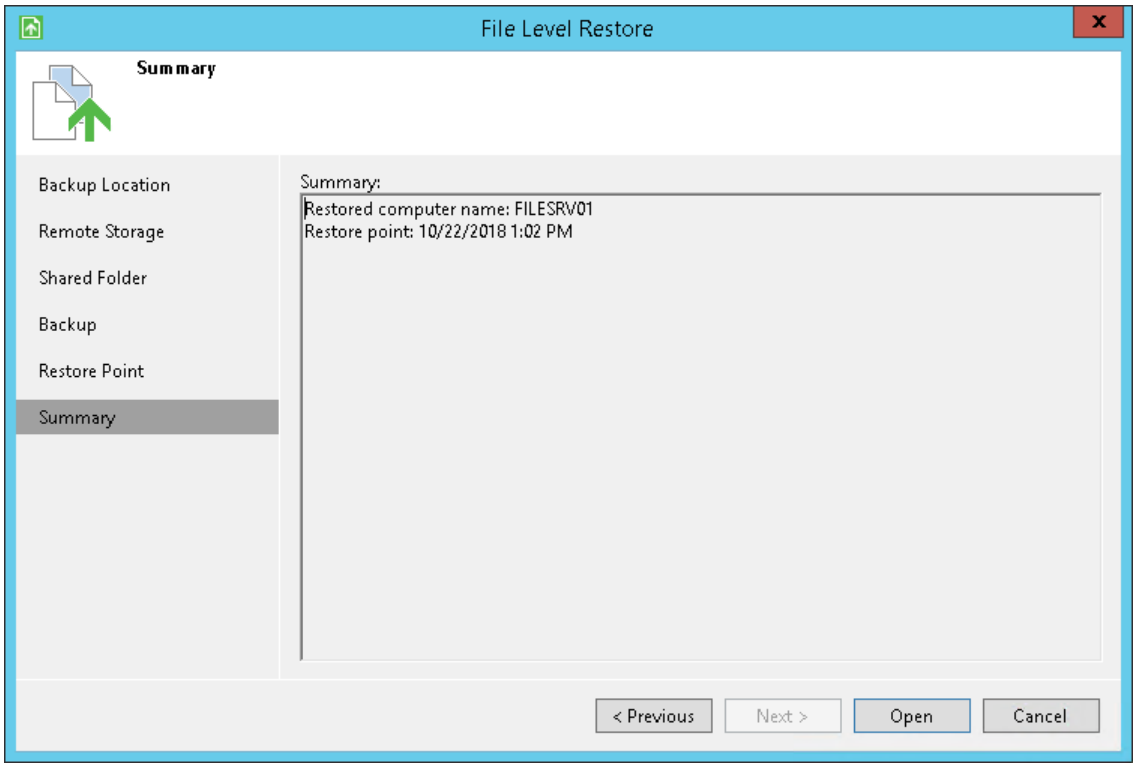
By default, Veeam Agent for Microsoft Windows uses the latest restore point. However, you can select any valid restore point to recover files and folders to a specific point in time.



Step 7. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of file-level restore.

1. Review settings of the restore process.
2. Click **Open**. Veeam Agent for Microsoft Windows will retrieve the content of the backup file, publish it directly into the file system of your computer and display it in the Veeam Backup browser.



Step 8. Save Restored Files

When the restore process is complete, Veeam Agent for Microsoft Windows opens the Veeam Backup browser displaying the content of the backup file.

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

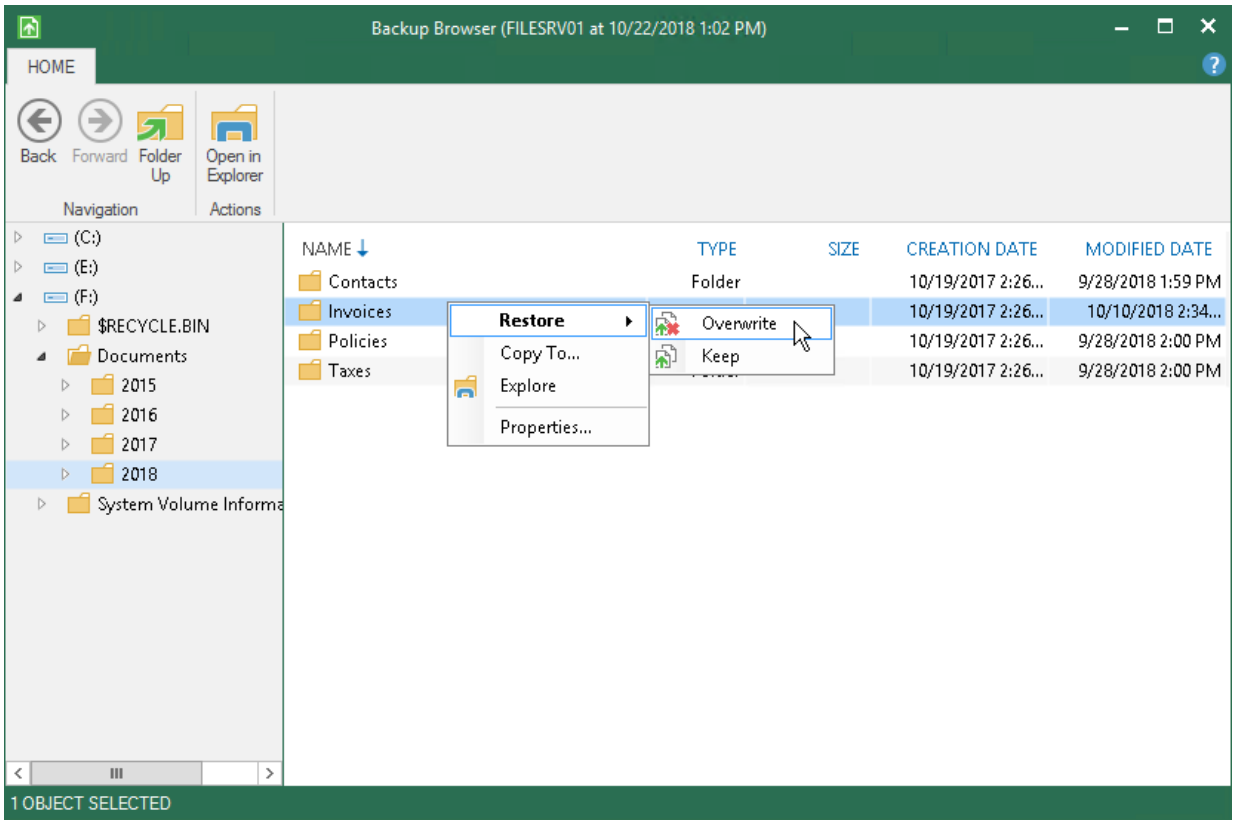
- Save files and folders to their initial location
- Save files and folders to a new location
- Open files in Microsoft Windows Explorer

After you finish working with files and folders, close the Veeam Backup browser.

Saving Files to Initial Location

To save restored files or folders to their initial location, right-click the necessary item in the file system tree or in the details pane on the right and select one of the following commands:

- To overwrite the original item on your computer with the item restored from the backup, select **Restore** > **Overwrite**.
- To save the item restored from the backup next to the original item on your computer, select **Restore** > **Keep**. Veeam Agent for Microsoft Windows will add the *RESTORED-* prefix to the restored file or folder name and save it in the same location where the original file resides.



Saving Files to New Location

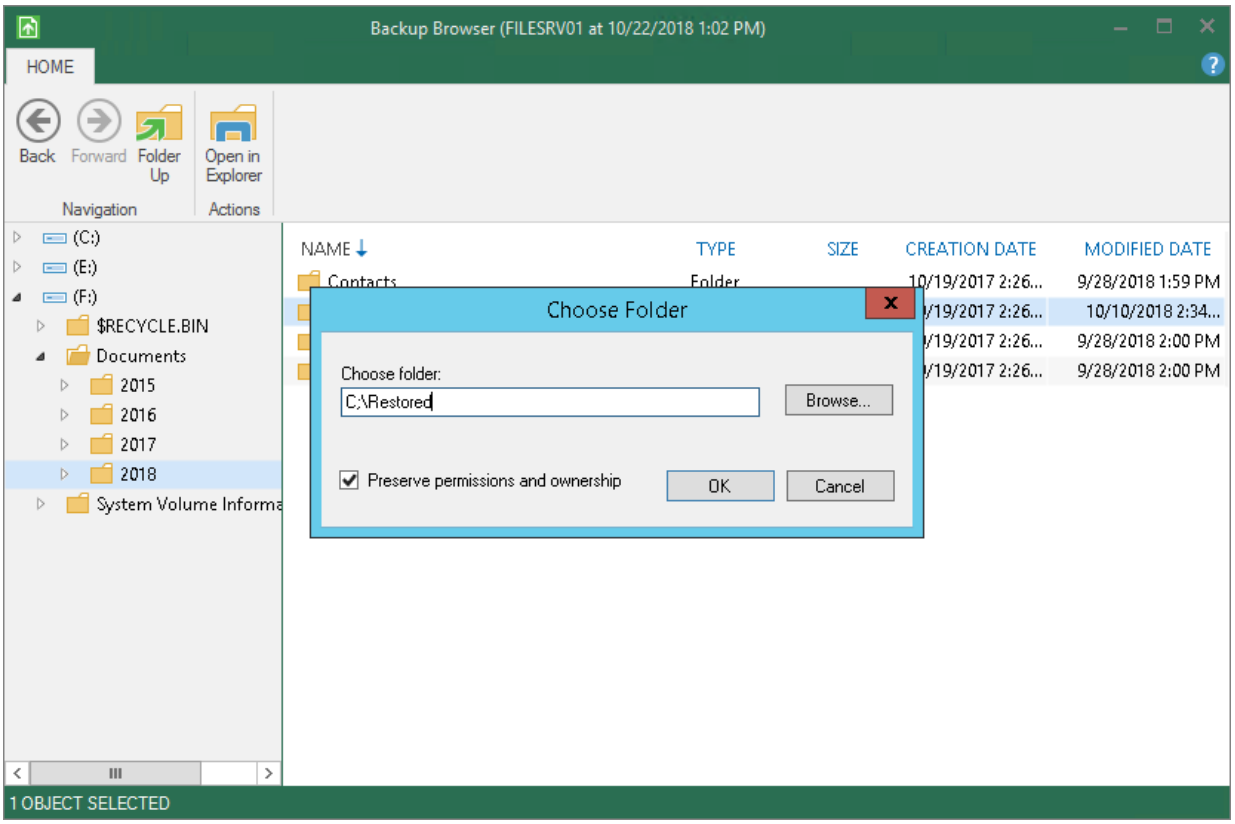
To save restored files or folders on your computer or to a network shared folder, right-click the necessary item in the file system tree or in the details pane on the right and select **Copy To**.

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

- Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored items. Veeam Agent for Microsoft Windows will copy selected files or folders with associated Access Control Lists, preserving granular access settings.

  Please note that if access settings of a file or folder that you want to restore are inherited from a parent folder, when you restore this file or folder without the parent folder, its access settings will not be preserved.

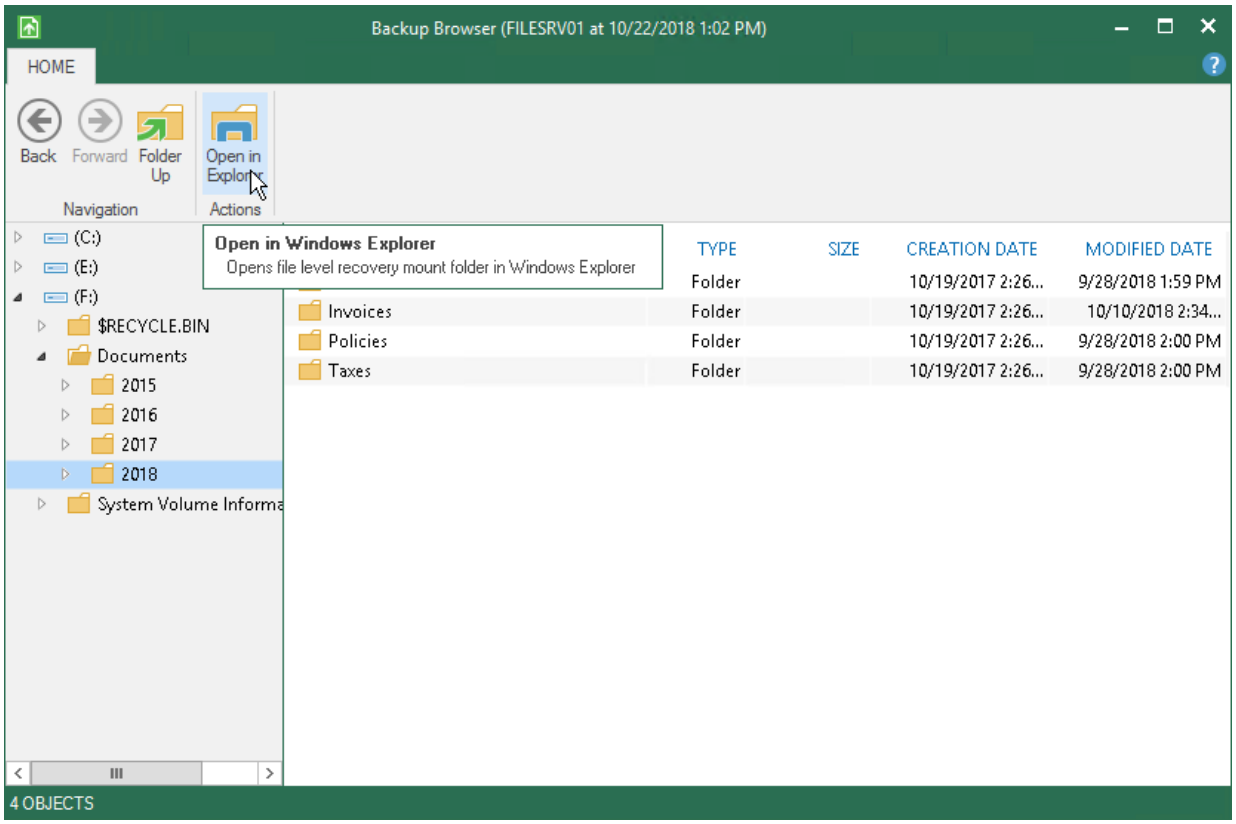
- Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored items. Veeam Agent for Microsoft Windows will change security settings: the user who launched the Veeam Agent for Microsoft Windows will be set as the owner of the restored items. Access permissions will be inherited from the folder to which the restored items are copied.



Working with Windows Explorer

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

- In Veeam Backup browser, select the necessary file or folder and click **Open in Explorer** on the toolbar. Veeam Agent for Microsoft Windows will open the selected folder or file in Microsoft Windows Explorer.
- Open Microsoft Windows Explorer and browse for restored files and folders. The backup content is mounted under the `C:\VeeamFLR\ServerName` folder.



We recommend that you use the Veeam Backup browser instead of Microsoft Windows Explorer for file-level restore. Use of the Veeam Backup browser has the following advantages:

1. You can browse the guest OS file system ignoring the file system ACL settings.
2. You can preserve permissions and ownership during file-level restore.

If you open the file system via the Microsoft Windows Explorer, these capabilities will not be available.

To learn more, see *SeBackupPrivilege* and *SeRestorePrivilege* in this Microsoft article.

Elevating Access Rights

You can switch to another system user with the Veeam Backup browser. This may be helpful when you work under an account that does not have Administrator privileges and do not have the access rights to restore the file you need.

To switch the user, do the following:

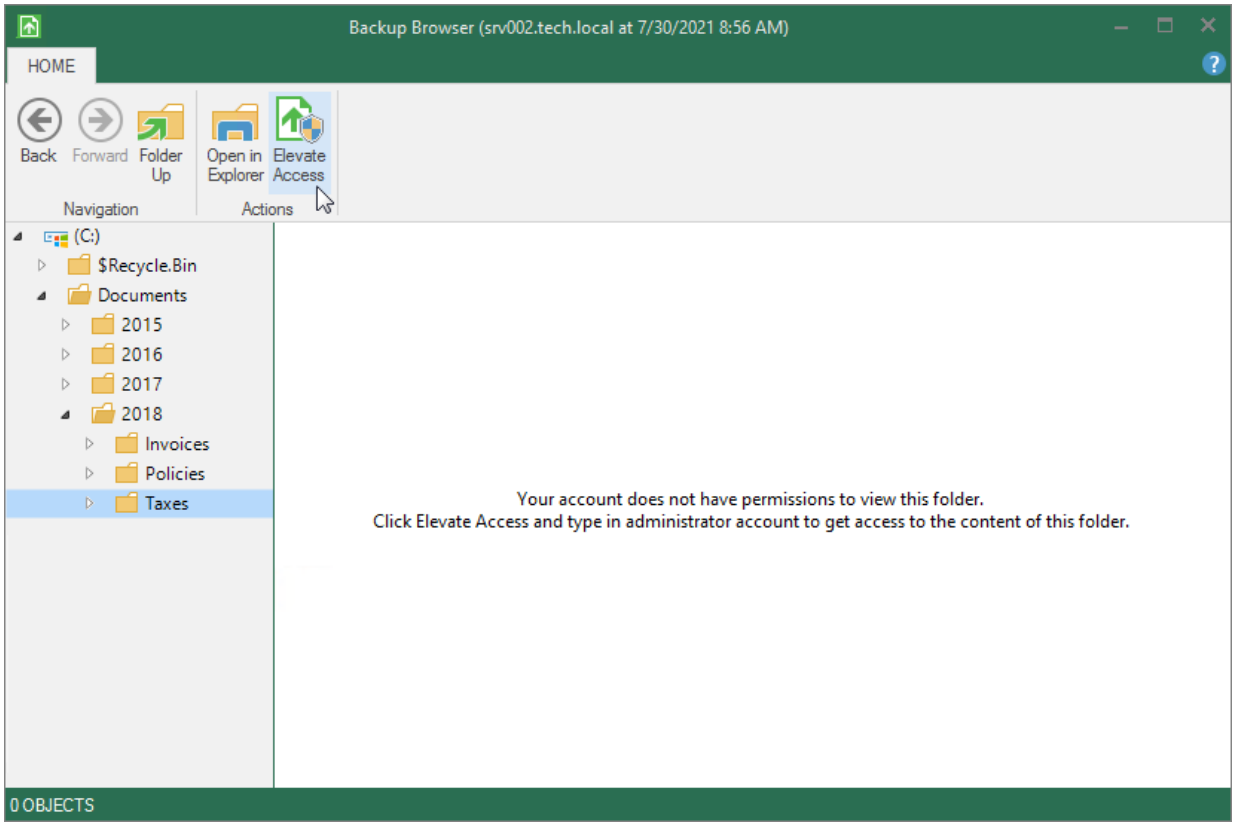
1. In Veeam Backup browser, click **Elevate Access** on the toolbar.

   Mind that Veeam Agent displays the **Elevate Access** button only if you open the Veeam Backup browser while working under an account that does not have Administrator privileges. To allow users without Administrator privileges to open the Veeam Backup browser and restore from the file-level backup, do one of the following:

   - If Veeam Agent operates in the standalone mode, use a registry value. For more information, contact Veeam Customer Support.
   - If Veeam Agent operates in the managed mode, use the Veeam Backup & Replication console. For more information, see the Veeam Agent for Microsoft Windows Settings section in the Veeam Agent Management Guide.

2. In the dialog window, provide credentials of the system user you need.

After that, Veeam Agent restarts the Veeam Backup browser with the updated access rights.



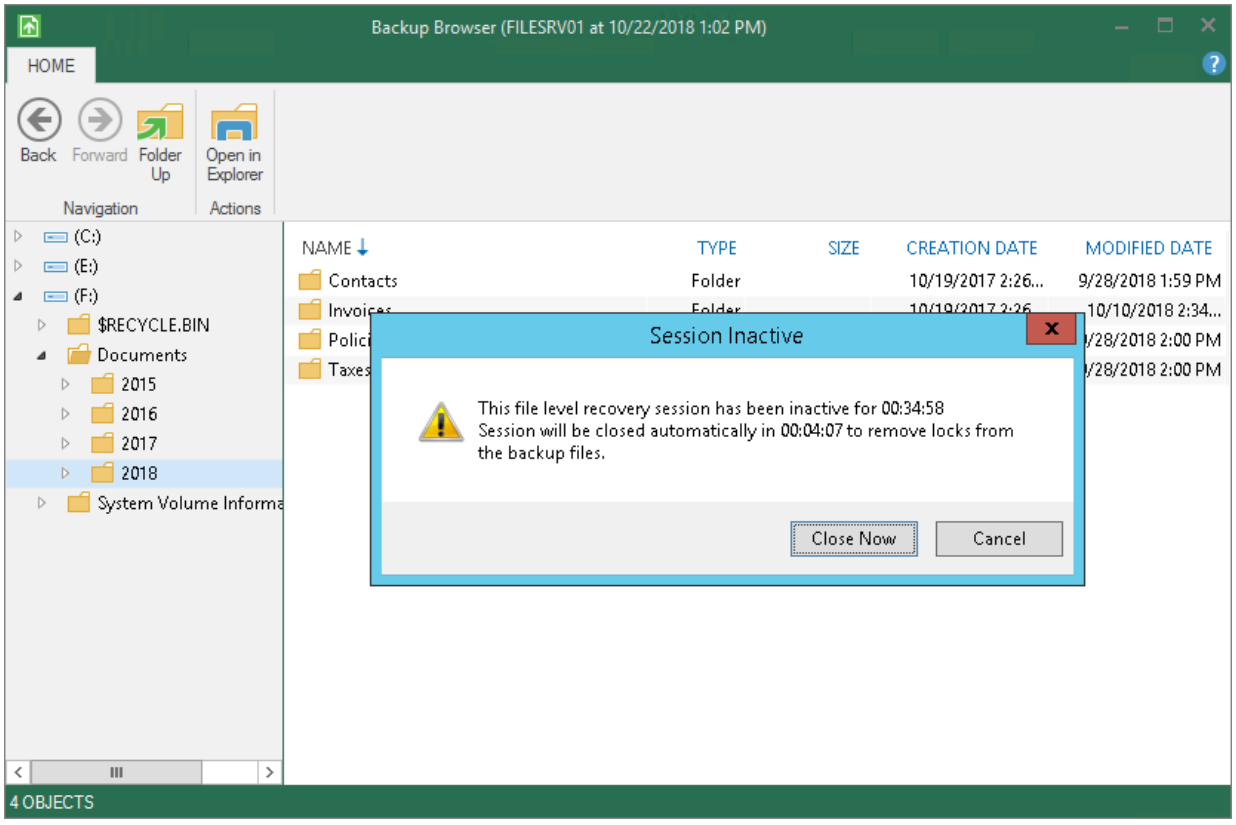
Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Agent for Microsoft Windows unmounts the backup content from your computer.

We recommend that you close the Veeam Backup browser after you finish restoring files and folders. Every 5 minutes, Veeam Agent for Microsoft Windows checks if there is any activity in the Veeam Backup browser. If the user or product components and services have not performed any actions for 30 minutes, Veeam Agent for Microsoft Windows displays a warning that the Veeam Backup browser is to be closed within 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 30 minutes. After this period expires, Veeam Agent for Microsoft Windows will display the warning again.
- You can perform no action at all. In this case, the Veeam backup browser will be automatically closed in 5 minutes.



Restoring Data from Encrypted Backups

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

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

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

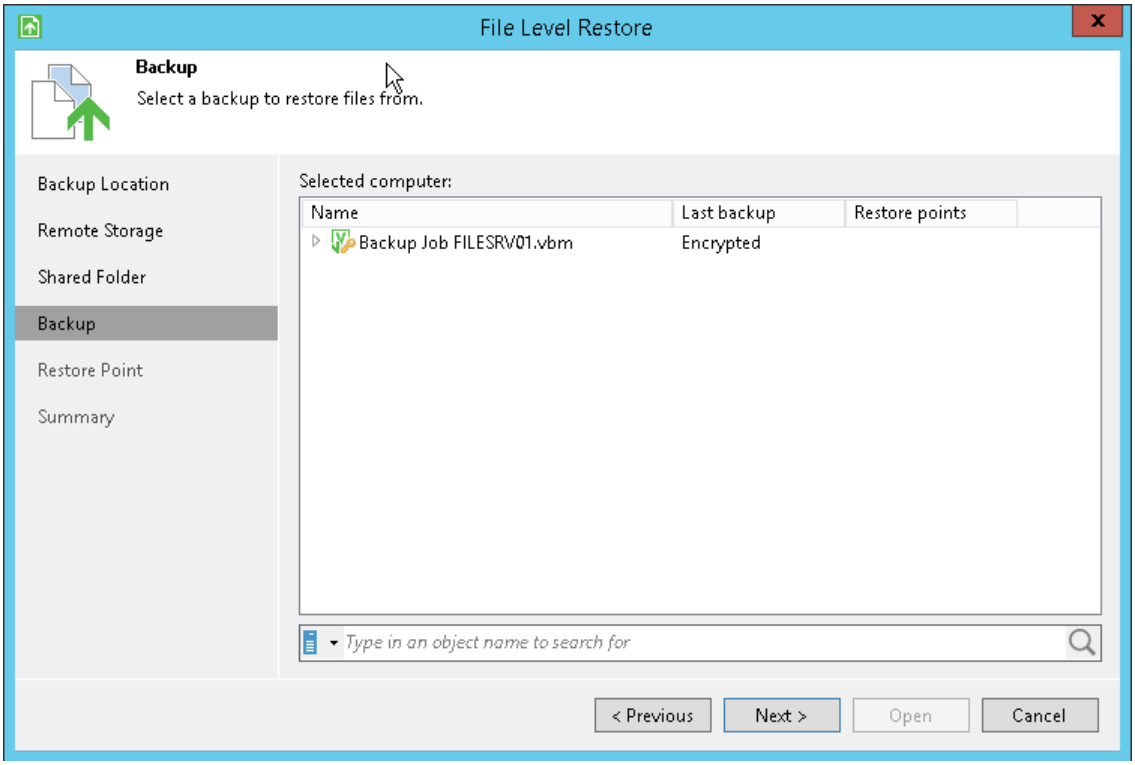
  - You encrypt and decrypt the backup file on the same Veeam Agent computer using the same Veeam Agent for Microsoft Windows database.
  - You have included encryption keys into the Veeam Recovery Media and perform bare metal recovery after booting from this Veeam Recovery Media. To learn more, see Specify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

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

To decrypt a backup file:

1. Launch the necessary data restore wizard:
   - If you want to perform file-level or volume-level restore from an encrypted backup that was created on another Veeam Agent computer, right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Restore** > **Individual files** or **Restore** > **Entire volumes**. To learn more, see Restoring Files and Folders and Restoring Volumes.
   - If you want to perform bare metal recovery from an encrypted backup, boot from the Veeam Recovery Media and launch the **Veeam Recovery Media** wizard. To learn more, see Restoring from Veeam Recovery Media.
2. At the **Backup Location** step of the wizard, specify where the encrypted backup file that you plan to use for restore resides. If the backup file resides in a remote location, at subsequent steps of the wizards, select the backup location type and specify settings to connect to the backup location.

3. At the **Backup** step of the wizard, select the encrypted backup.

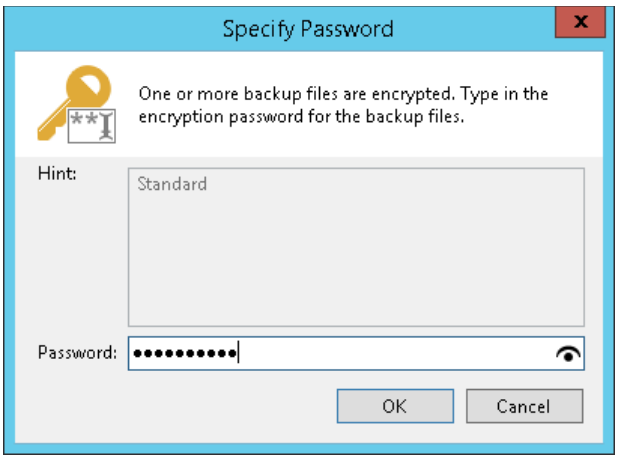


4. Veeam Agent for Microsoft Windows will display the **Specify Password** window. In the **Hint** field of the **Specify Password** window, Veeam Agent for Microsoft Windows displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.

5. In the **Password** field, enter the password for the backup file.

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

   If you enter correct password, Veeam Agent for Microsoft Windows will decrypt the backup metadata. You will be able to pass to the Restore Point step of the wizard and continue the restore operation in a regular manner.



Reporting

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

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

Viewing Statistics in Control Panel

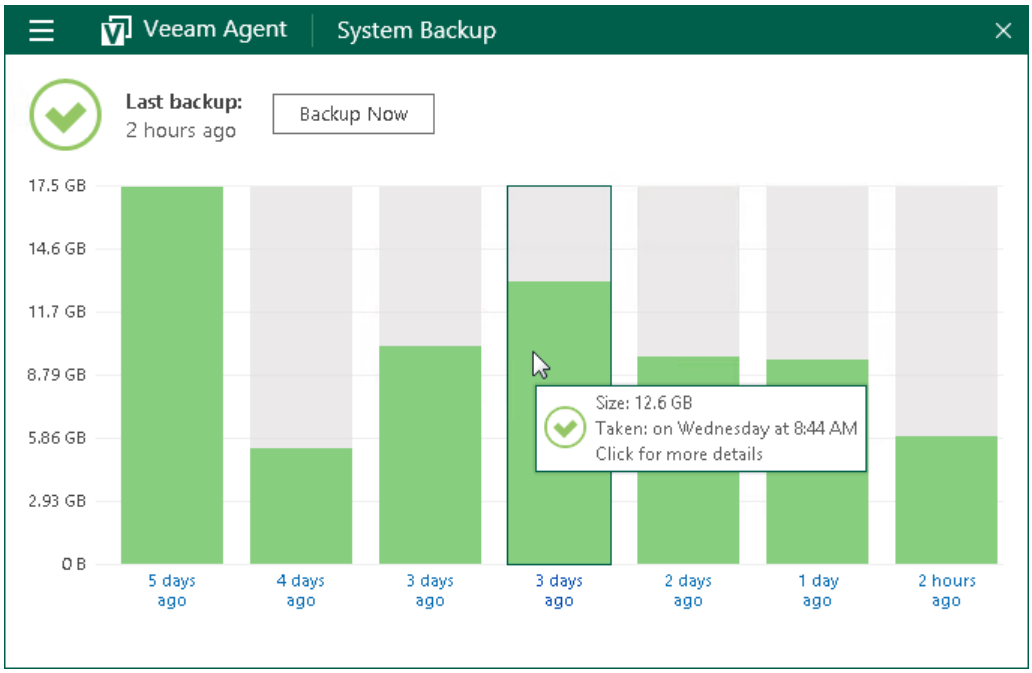
You can use the Veeam Agent control panel to view statistics about performed backups. To open the Control Panel, do either of the following:

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

For every configured backup job, Veeam Agent displays statistics in a separate view in the control panel. To identify the job whose statistics is currently displayed in the Control Panel, check the name of the job at the top of the Control Panel window.

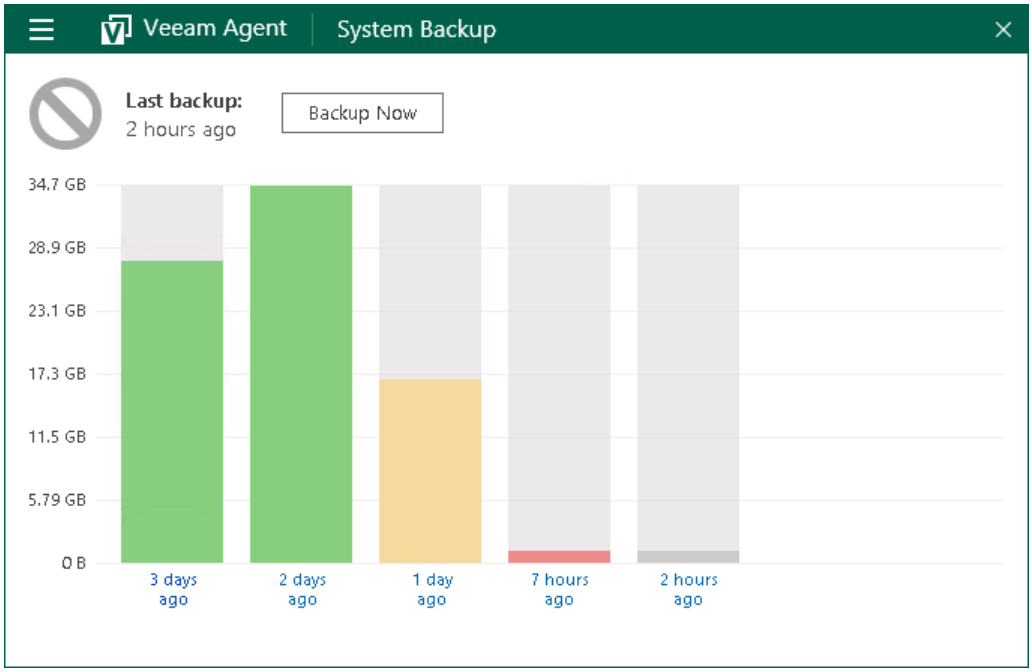
If you configured multiple backup jobs in Veeam Agent, after you open the Control Panel, the Control Panel displays statistics for the first job that you configured. To switch to another job, in the main menu, hover over the name of the necessary job and select **Open**.

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



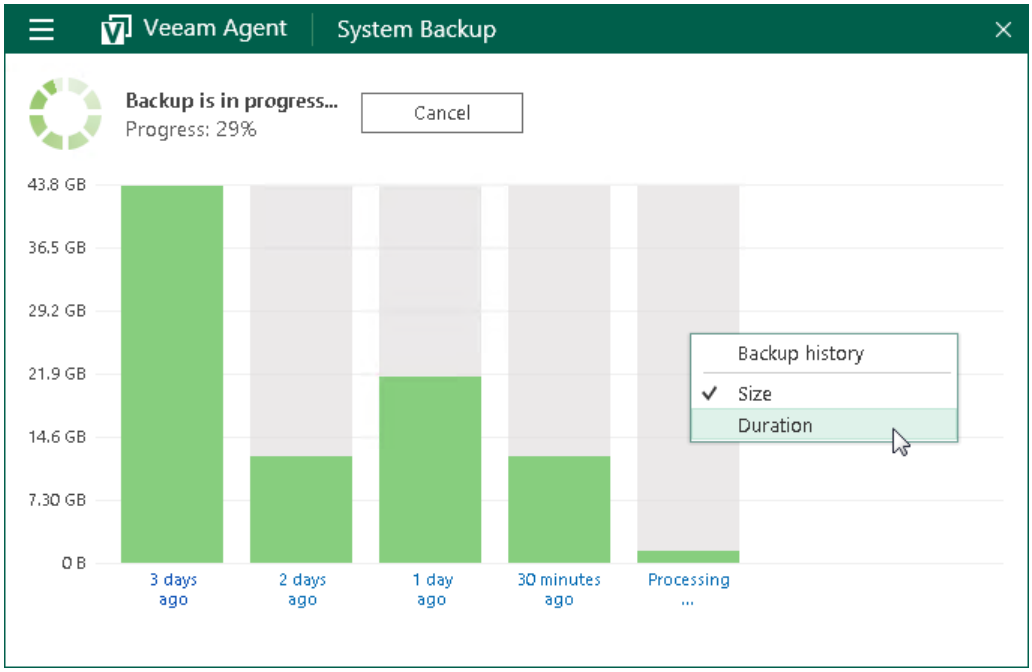
The bar color identifies the status of the backup job session. The backup job session can complete with one of the following statuses:

- *Success* (green color) — the backup job is currently running or has completed successfully.
- *Warning* (yellow color) — the backup job has completed with a warning. Veeam Agent for Microsoft Windows has managed to create the resulting backup file but you need to pay your attention to some alerts, for example: the target location is running low on disk space.
- *Error* (red color) — the backup job has completed with an error. The resulting backup file has not been created.
- *Canceled* (gray color) — the user has canceled the backup job session. The resulting backup file has not been created.

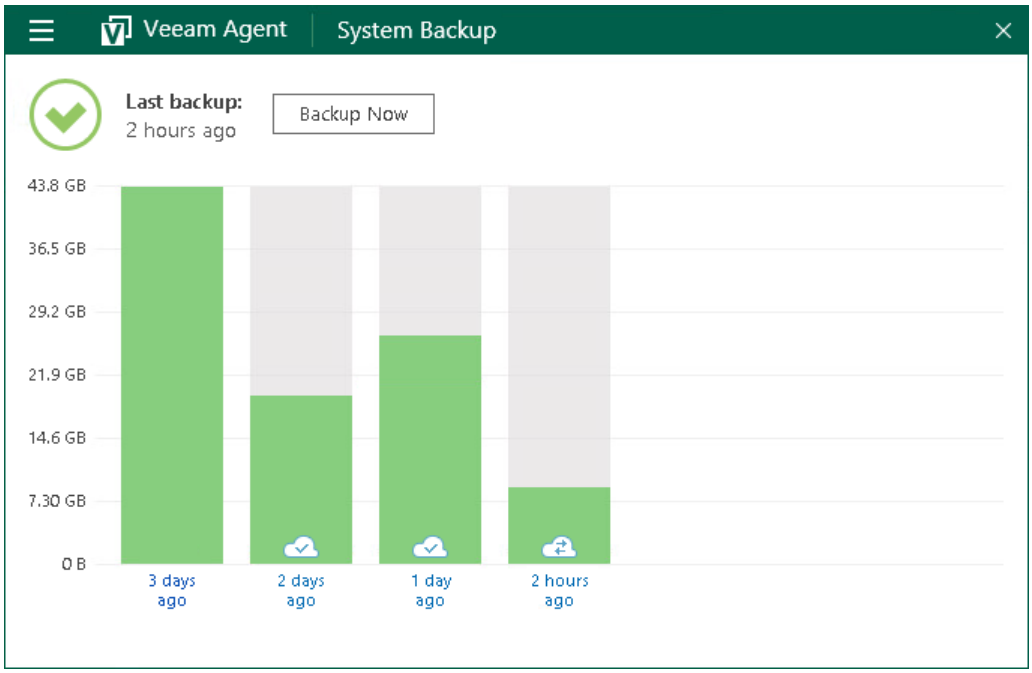


By default, Veeam Agent displays the size of created backup files. To display the duration of backup job sessions:

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



If the backup cache is enabled for the job, Veeam Agent for Microsoft Windows also displays status of the restore point created within the job session. To learn more, see Viewing Status of Restore Points in Backup Cache.



Viewing Statistics for Separate Restore Points

You can view the following information about separate restore points in the backup chain:

- View general statistics — for any separate restore point.
- View transaction log backup statistics — for restore points created by the backup job with transaction log backup enabled.

General Statistics

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

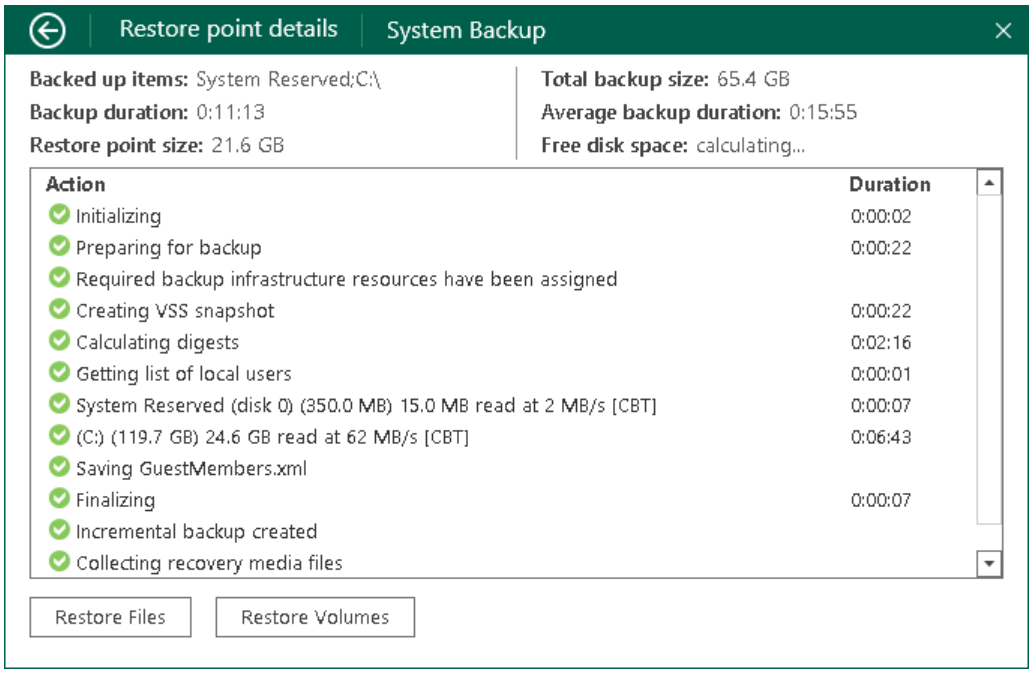
- Backed-up items: items that you have chosen to back up
- Backup duration: duration of the backup job session
- Restore point size: size of the resulting backup file
- Total backup size: total size of all backup files created by the backup job in the target location
- Average backup time: average time of all successful backup job sessions displayed in the chart
- Free disk space: amount of free disk space remaining in the target location
- Details on operations performed during the backup job session

To view the restore point statistics:

1. Double-click the Veeam Agent icon in the system tray or right-click the icon and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

   If multiple backup jobs are configured in Veeam Agent, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.
3. Click the necessary bar in the chart.
4. Veeam Agent will display detailed statistics on the selected backup job session. To get back to a chart view, click the arrow icon at the top left corner of the window.

If transaction log backup is enabled for the job, you can also view transaction log backup statistics. To learn more, see Transaction Log Backup Statistics.



Transaction Log Backup Statistics

If transaction log backup is enabled for the job, you can use the Veeam Agent control panel to view transaction log backup statistics.

Veeam Agent for Microsoft Windows provides the following information about transaction log processing:

- Protected databases: number of databases that were backed up at least once during the last session
- Unprotected databases: number of databases that failed to be backed up during the last session
- Excluded databases: databases excluded from processing. Databases may be excluded for the following reasons: database status is *Offline*, database recovery model is set to *Simple*, database is read-only, database was deleted after the latest full backup.
- Average log size: average amount of data read from the OS through all intervals
- Max log size: maximal amount of data read from the OS over all 15-min intervals
- Total log size: total amount of data written to the target location
- SLA: how many log backup intervals completed in time with successful log backup (calculated as percentage of total number of intervals)
- Misses: how many intervals were missed (number of intervals)
- Max delay: difference between the configured log backup interval and time actually required for log backup. If exceeded, a warning is issued.
- Details on operations performed during the transaction log backup job session

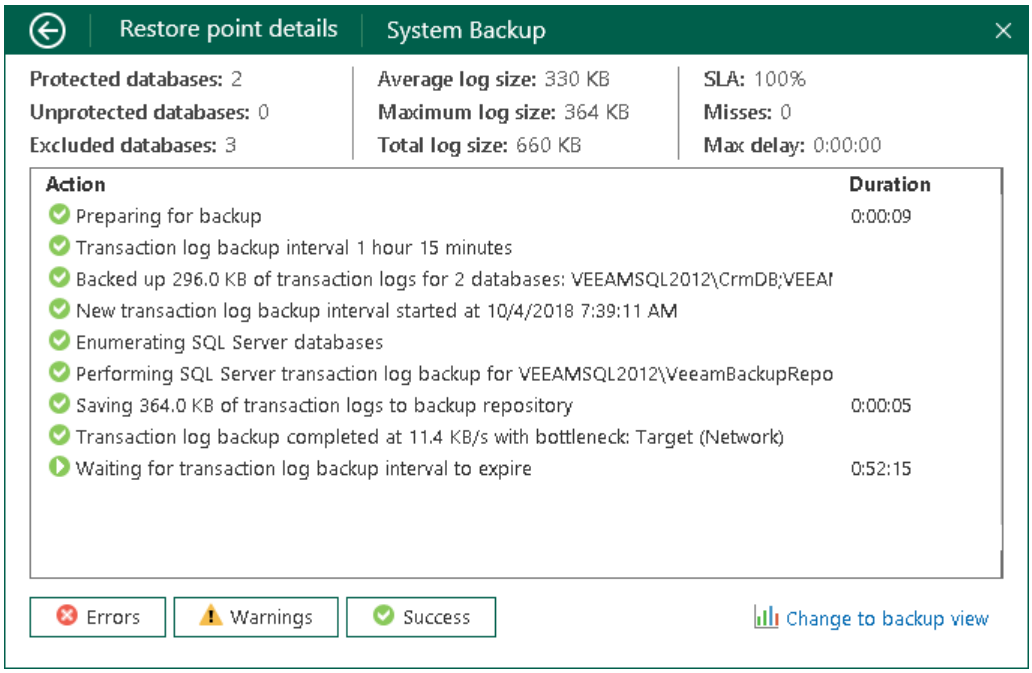
To view statistics on the transaction log backup processing:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray or right-click the icon and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

   If multiple backup jobs are configured in Veeam Agent for Microsoft Windows, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.
3. Click the necessary bar in the chart.

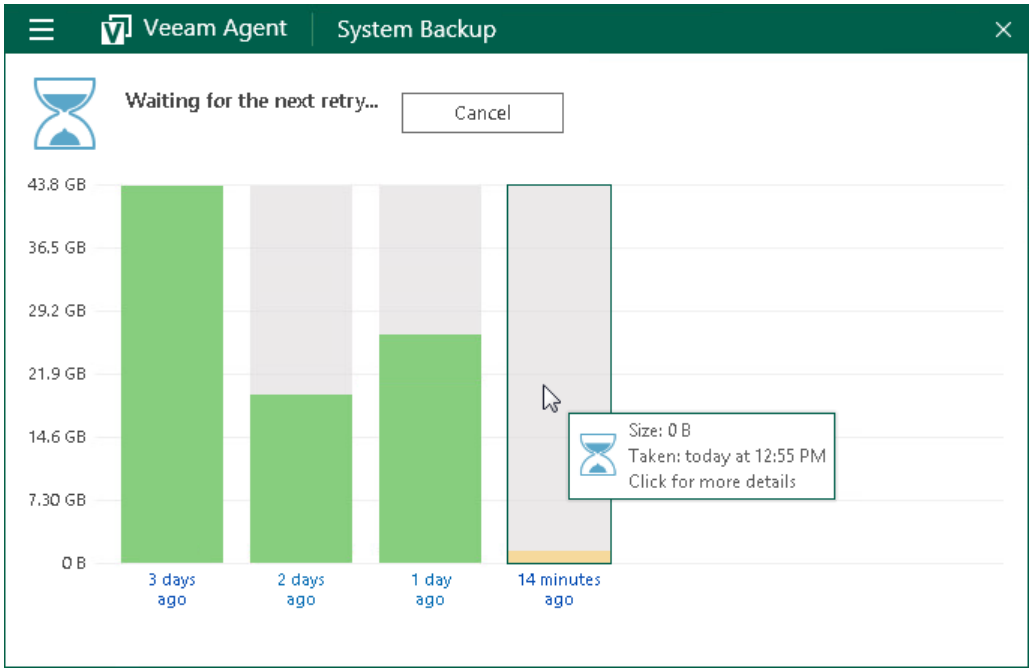
4. In the **Restore point details** window, click the **Change to database view** link at the bottom right corner of the window. Veeam Agent for Microsoft Windows will display detailed statistics on the transaction log backup. To get back to the general statistics for the selected restore point, click the **Change to backup view** link.

   To get back to a chart view, click the arrow icon at the top left corner of the window.



Viewing Information About Job Retries

If the backup job started by schedule has failed for some reason, Veeam Agent for Microsoft Windows retries the job. All backup job retries are performed within one backup job session. For this reason, Veeam Agent for Microsoft Windows displays them as one bar in the chart.



NOTE

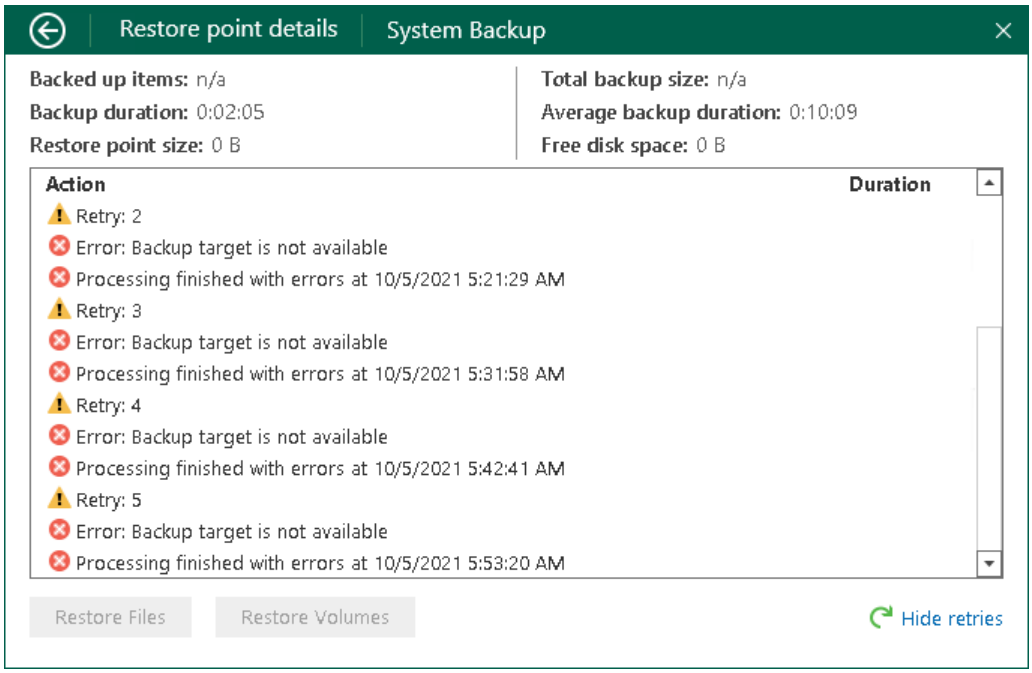
For portable devices, Veeam Agent for Microsoft Windows does not automatically retry the backup job if a device is working on battery and the battery level is below 20%.

To view detailed information about the backup job retries:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. At the top of the control panel window, check the name of the backup job.

   If multiple backup jobs are configured in Veeam Agent for Microsoft Windows, and you want to view statistics of another job, in the main menu, hover over the name of the necessary job and select **Open**.
3. Click the necessary bar in the chart.
4. At the bottom right corner of the window, click the **Show retries** link.

5. After you view details, you can hide them. To do this, at the bottom right corner of the window, click the **Hide retries** link.



Viewing Status of Restore Points in Backup Cache

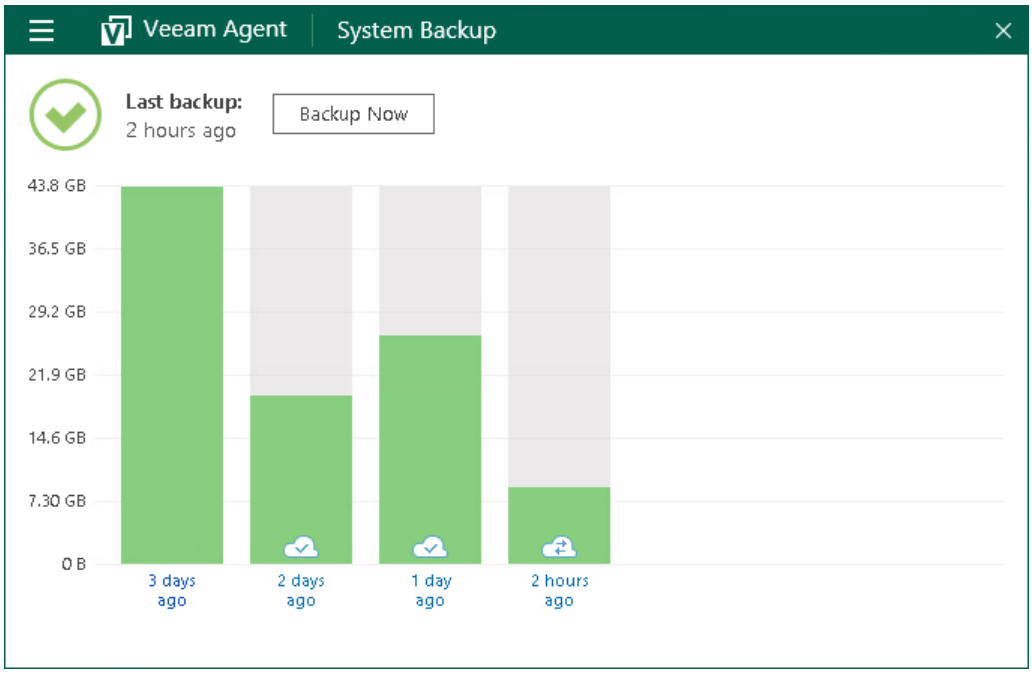
If the backup cache is enabled for the job, you can monitor status of restore points in the backup cache. Veeam Agent for Microsoft Windows displays the restore point status through the icon on a bar in the chart.

The icon can be in one of the following states:

Icon	Description	Backup state
	Check mark over the icon.	The backup file created within the backup session is saved on the target storage.
–	No icon.	The backup file created within the backup session is saved in the backup cache.
	Sync sign over the icon.	The backup file is being uploaded from the backup cache to the target storage.
	Error sign over the icon.	The backup file was not uploaded to the target storage and has been deleted from the backup cache.

TIP

You can also monitor the backup cache activity and view detailed statistics on the restore point upload process. To learn more, see Monitoring Backup Cache Activity.



Monitoring Backup State with Tray Agent

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

The icon can be in one of the following states:

Icon	Description	Backup state
	Question mark over the icon	The backup job is not configured.
	Veeam Agent for Microsoft Windows icon	The backup job is set up but scheduling settings for the job are not configured.
	Animated icon	The backup task is being performed. To view the backup task progress, hover the mouse over the icon.
	Clock over the icon	The latest session of the scheduled backup job has completed successfully; waiting for the next backup job session.
	Sync sign over the icon	Veeam Agent is uploading backup file(s) from the backup cache to the target storage.
	Cancel sign over the icon	The latest session of the scheduled backup job has been canceled.
	Error sign over the icon	An error occurred during the latest backup job session, and the session was terminated.
	Minus sign over the icon	The scheduled backup job is disabled.
	Grey icon	The tray agent is not connected to the Veeam Agent for Microsoft Windows service.

Icon	Description	Backup state
	Warning sign over the icon	• The backup job has completed with a warning, for example, the target location is running low on space. • [If you have selected a removable storage device as a target destination in the backup job settings] The target removable storage device is not connected to the computer. In this case, Veeam Agent also displays a warning on the notifications bar in the control panel. You can attach the target removable storage device to the computer within 10 minutes, and Veeam Agent will automatically start the scheduled backup job.

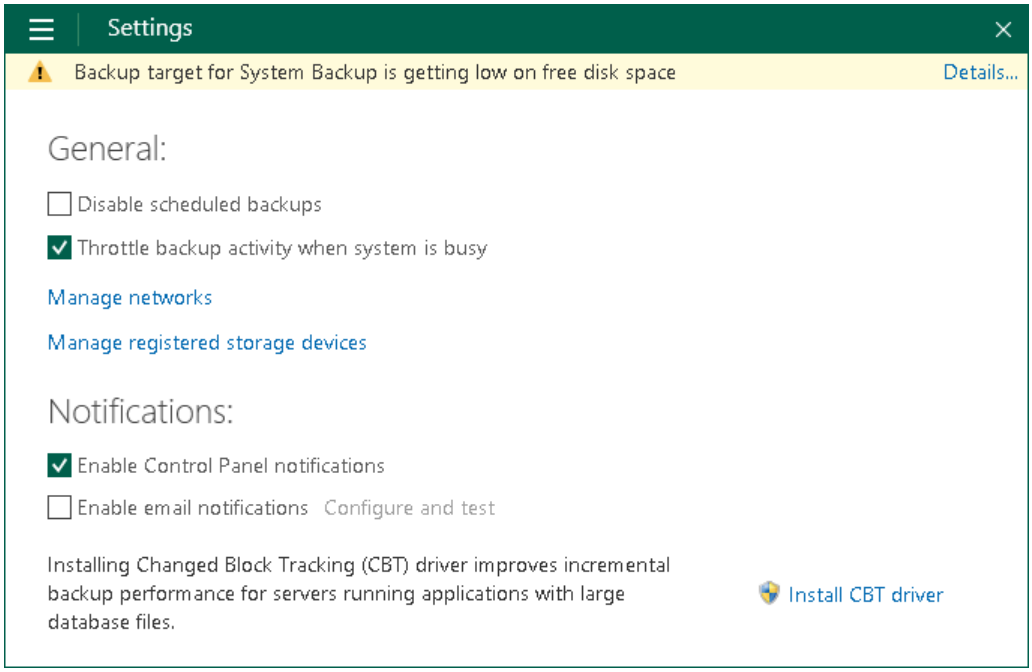
Monitoring Backup Process in Taskbar Button

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



Viewing and Dismissing Veeam Agent Events

If a warning event occurs, Veeam Agent displays a notification bar with the event description in the control panel window. You can get detailed information about events and dismiss events not to get alerted of them in future. For the full list of notifications, see Control Panel Notifications.



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

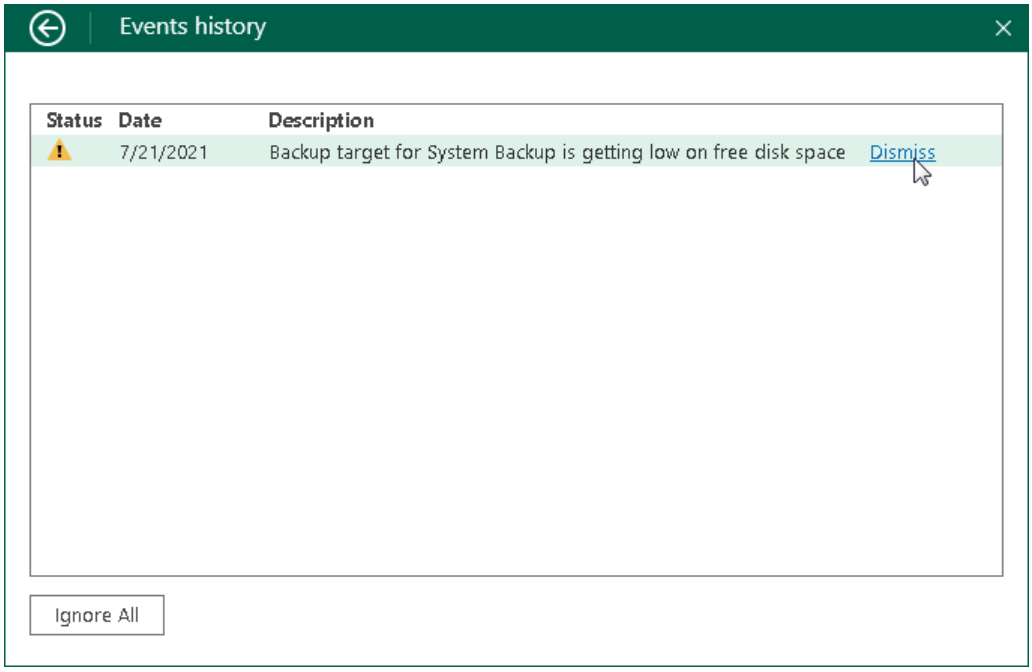
1. Double-click the Veeam Agent icon in the system tray, or right-click the Veeam Agent icon in the system tray and select **Control Panel**.
2. Click **Details** on the notification bar at the top of the control panel window.

To dismiss events:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. Click **Details** on the notification bar at the top of the control panel window.
3. Click **Dismiss** next to the necessary event. To dismiss all events at once, click **Ignore All** at the bottom left corner of the window.

TIP

You can disable notifications at all. To learn more, see Disabling Control Panel Notifications.



Control Panel Notifications

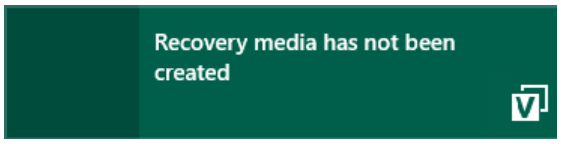
Veeam Agent for Microsoft Windows can inform you about the following events using the notification bar:

Notification	Description
New software update is available	A newer version of Veeam Agent for Microsoft Windows is available for download.
Veeam Recovery Media must be recreated due to a recent Veeam Agent for Microsoft Windows upgrade	You must recreate the Veeam Recovery Media after you have upgraded Veeam Agent for Microsoft Windows to the newer version.
Recovery media OS version is different from the current OS version	You must recreate the Veeam Recovery Media after you have updated the Microsoft Windows OS.
Recovery media has not been created	You have not created the Veeam Recovery Media yet. If the OS on the computer fails to boot, you will not be able to boot the OS using the Veeam Recovery Media to diagnose and fix problems, or restore data from the backup.
Backup target is not available, backup is postponed	Veeam Agent for Microsoft Windows is unable to detect the backup target at the time when the scheduled backup job must start (for example, the backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification during the job retry sessions.
Backup target is not available	Veeam Agent for Microsoft Windows is unable to detect the backup target by the moment when the scheduled backup job must start (for example, backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification after the job has failed.
Backup target has not been seen for N days	The backup target has not been seen for N days. This notification is displayed if scheduled backups have not been created for 2 days or more.
Backup target is getting low on free disk space	Free space on the target storage disk is below 10%. If Veeam Agent for Microsoft Windows does not have enough disk space for backup operation, the job session will fail.
Skipping scheduled backup, because battery level is too low	[For laptops and tablets] The battery level is below 20%. Veeam Agent for Microsoft Windows does not start a new backup session in this case.

Notification	Description
This application is managed by your system administrator	This notification is displayed if Veeam Agent for Microsoft Windows is operating in the read-only mode. Veeam Agent for Microsoft Windows operates in the read-only mode if backup operations are managed by Veeam Backup & Replication or Veeam Availability Console.
Your license will expire in N days	The Veeam Agent for Microsoft Windows license will expire, and the grace period will start in N days.
Your license has expired and needs to be renewed	The Veeam Agent for Microsoft Windows license has expired, and the grace period has started. During the grace period, you can perform all types of backup and restore operations. You must obtain a new license before the end of the grace period.
Your license has expired, and your grace period is over	The Veeam Agent for Microsoft Windows license has expired, and the grace period is over. In this case, Veeam Agent for Microsoft Windows does not perform backup operations. However, you are able to restore data from existing backups. To use Veeam Agent for Microsoft Windows in the full functionality mode, you must obtain a new license.

Viewing Events with Windows Notification Center

In addition to displaying notifications about Veeam Agent events in the control panel window, Veeam Agent can inform you about its events using the Windows Notification Center. Once an event occurs, a message notifying about this event will appear on the Microsoft Windows desktop. This lets you view the notification without the need to open the Veeam Agent Control Panel and take the necessary actions immediately. For the full list of notifications that appears on the Microsoft Windows desktop, see Windows Desktop Notifications.



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

To disable desktop notifications, right-click the message and select **Turn off notifications for Veeam Agent for Microsoft Windows**.

Windows Desktop Notifications

Veeam Agent for Microsoft Windows can inform you about the following events using the Windows Notification Center:

Notification	Description
New software update is available	A newer version of Veeam Agent for Microsoft Windows is available for download.
Veeam Recovery Media must be recreated due to a recent Veeam Agent for Microsoft Windows upgrade	You must recreate the Veeam Recovery Media after you have upgraded Veeam Agent for Microsoft Windows to the newer version.
Recovery media OS version is different from the current OS version	You must recreate the Veeam Recovery Media after you have updated the Microsoft Windows OS.
Recovery media has not been created	You have not created the Veeam Recovery Media yet. If the OS on the computer fails to boot, you will not be able to boot the OS using the Veeam Recovery Media to diagnose and fix problems, or restore data from the backup.
Backup target is not available	Veeam Agent for Microsoft Windows is unable to detect the backup target by the moment when the scheduled backup job must start (for example, backup target is a removable storage device that is not currently connected to the Veeam Agent computer). Veeam Agent for Microsoft Windows displays this notification after the job has failed.
Your license will expire in N days	The Veeam Agent for Microsoft Windows license will expire, and the grace period will start in N days.
Your license has expired and needs to be renewed	The Veeam Agent for Microsoft Windows license has expired, and the grace period has started. During the grace period, you can perform all types of backup and restore operations. You must obtain a new license before the end of the grace period.
Your license has expired, and your grace period is over	The Veeam Agent for Microsoft Windows license has expired, and the grace period is over. In this case, Veeam Agent for Microsoft Windows does not perform backup operations. However, you are able to restore data from existing backups. To use Veeam Agent for Microsoft Windows in the full functionality mode, you must obtain a new license.

Viewing Job Session Results in Email Reports

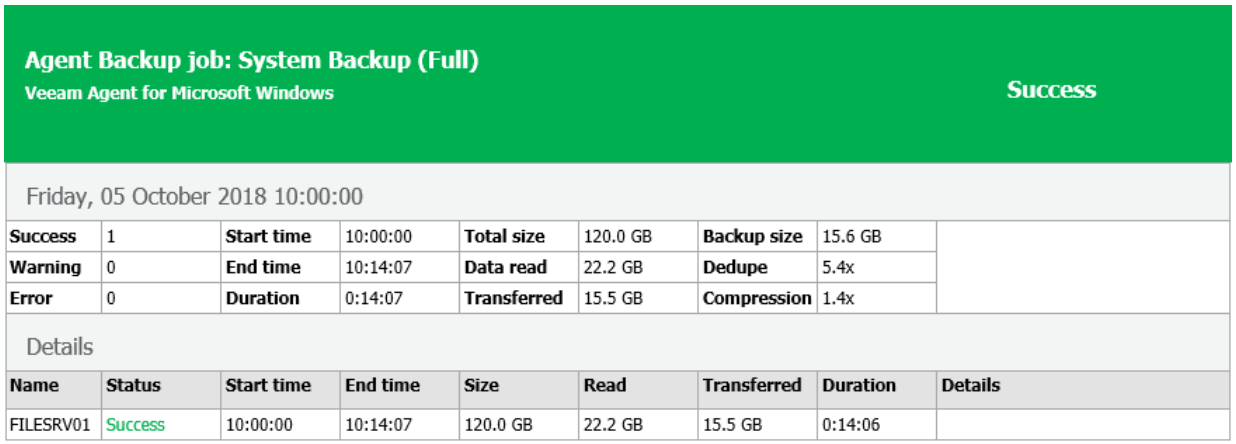
You can receive email notifications with Veeam Agent for Microsoft Windows job results. When the backup job session completes, Veeam Agent for Microsoft Windows will send a report containing data on the job session to the specified email address.

The report contains the following data:

- Cumulative job session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression and deduplication ratios.
- Detailed statistics for the computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).
- If the backup job is set up to create database log backups, the report contains statistics for the database log backup job: a list of databases that were backed up at least once during the last session and information for the latest log processing intervals.
- If you use the backup cache, the report also contains statistics on the backup cache activity: a list of restore points created in the backup cache, their status and upload details. To learn more about the backup cache, see Backup Cache.

To receive email reports, you must enable and configure email notifications in the Veeam Agent for Microsoft Windows Control Panel. To learn more, see Enabling Email Notifications. Once email notifications are configured, Veeam Agent for Microsoft Windows will send email report for every backup job session that is started by schedule, manually or when you perform standalone full or incremental ad-hoc backup.

If the scheduled backup job fails, Veeam Agent for Microsoft Windows does not send a report after every job retry. Instead, Veeam Agent for Microsoft Windows sends one report on the first error within the job session and another report on the last job session result — success or error.



Agent Backup job: System Backup (Full)
Veeam Agent for Microsoft Windows **Success**

Friday, 05 October 2018 10:00:00

Success	1	**Start time**	10:00:00	**Total size**	120.0 GB	**Backup size**	15.6 GB
Warning	0	**End time**	10:14:07	**Data read**	22.2 GB	**Dedupe**	5.4x
Error	0	**Duration**	0:14:07	**Transferred**	15.5 GB	**Compression**	1.4x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FILESRV01	Success	10:00:00	10:14:07	120.0 GB	22.2 GB	15.5 GB	0:14:06	

Specifying Settings

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

- Throttle backup activities.
- Restrict network connections usage.
- Manage backup storage devices.
- Disable Control Panel notifications.
- Enable email notifications.
- Check for new product versions and updates.

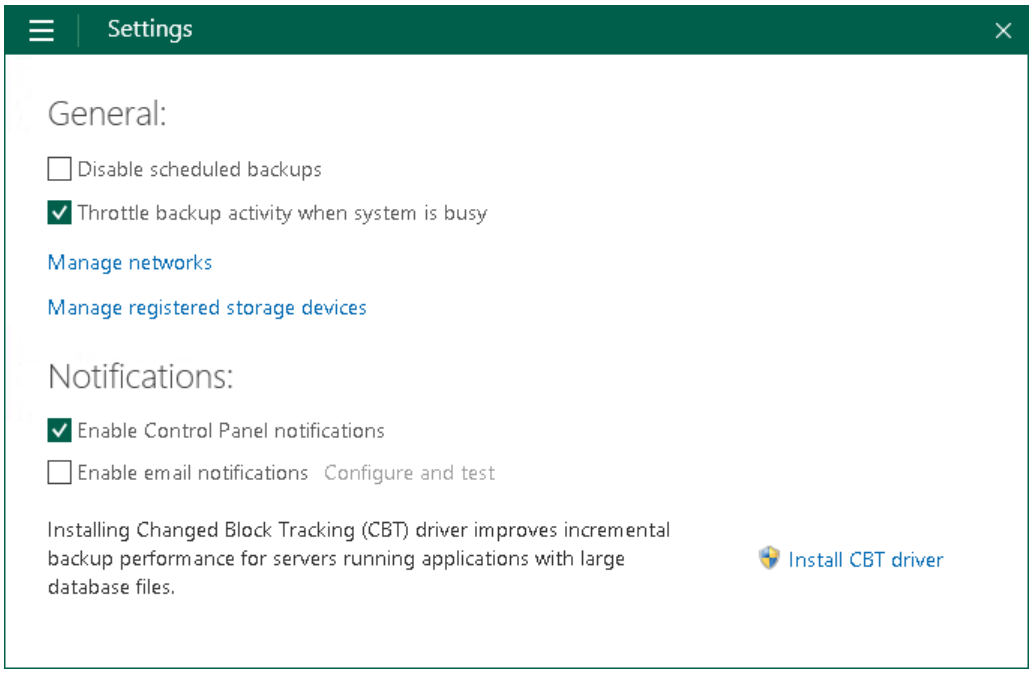
Throttling Backup Activities

You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup. The throttling option can help you avoid situations when backup tasks consume all available hard disk resources and hinder work of other applications and services.

With throttling enabled, Veeam Agent for Microsoft Windows sets low priority for Veeam Agent for Microsoft Windows components engaged in the backup process (in particular, the *VeeamAgent.exe* process). If this option is not enabled, Veeam Agent for Microsoft Windows components have normal priority.

To enable the throttling option for backup activities:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Select the **Throttle backup activity when system is busy** check box.



Restricting Network Connections Usage

You can instruct Veeam Agent for Microsoft Windows to throttle network traffic for backup jobs and disable backup over Internet connections of certain types. This helps limit the impact of Veeam Agent operations on network performance and avoid extra costs.

Network usage settings apply to all types of backups: scheduled and ad-hoc. To restrict network connections usage for Veeam Agent, you can perform the following tasks:

- Limit bandwidth consumption for Veeam Agent.
- Disable backup over metered connections.
- Disable backup over VPN connections.
- Allow Veeam Agent to use specific Wi-Fi networks only.

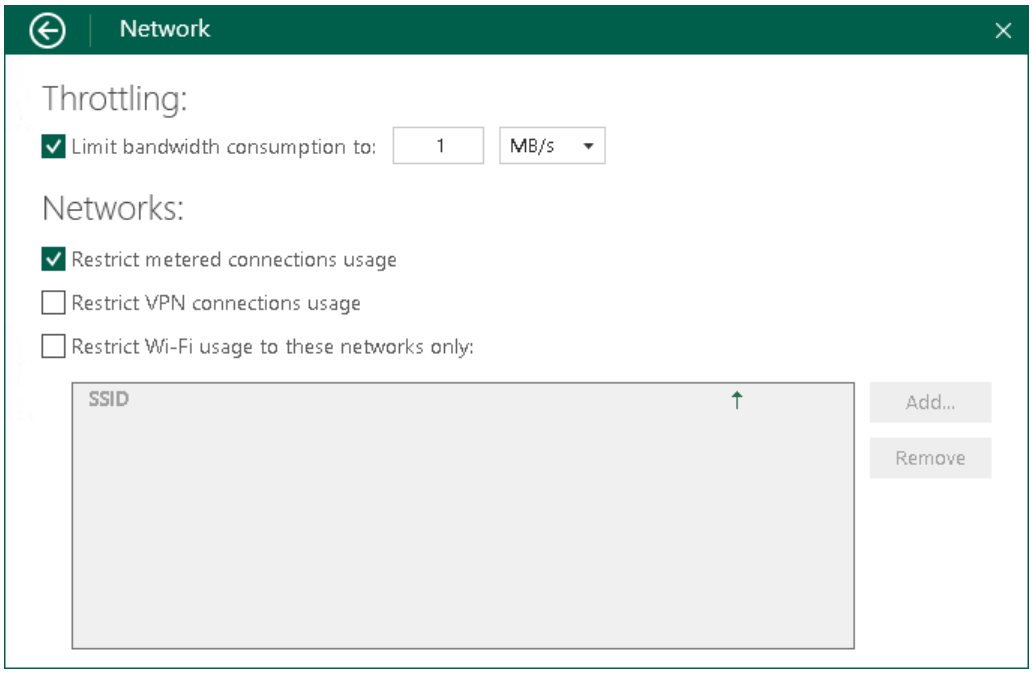
Limiting Bandwidth Consumption

To reduce the impact of Veeam Agent operations on network performance, you can limit bandwidth consumption for Veeam Agent backup jobs. Limiting bandwidth consumption prevents jobs from utilizing the entire bandwidth available in your environment to ensure that enough traffic is provided for other network operations. We strongly recommend to limit bandwidth consumption if you perform backup to a remote location over a slow network connection.

> **NOTE**
>
> Bandwidth consumption limit does not apply to restore operations.

By default, Veeam Agent is set up to use the entire bandwidth available in your environment. To limit bandwidth consumption for Veeam Agent backup jobs:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Throttling** section, select the **Limit bandwidth consumption to** check box and specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.



Disabling Backup over Metered Connections

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

Mind the following limitations and requirements:

- Veeam Agent disables backup over metered Internet connections only on computers that run Microsoft Windows 8.1 and later. If the computer runs an earlier version of Microsoft Windows, this option is not applicable.
- You must specify which connections are metered in Microsoft Windows. To learn more, see this Microsoft article.

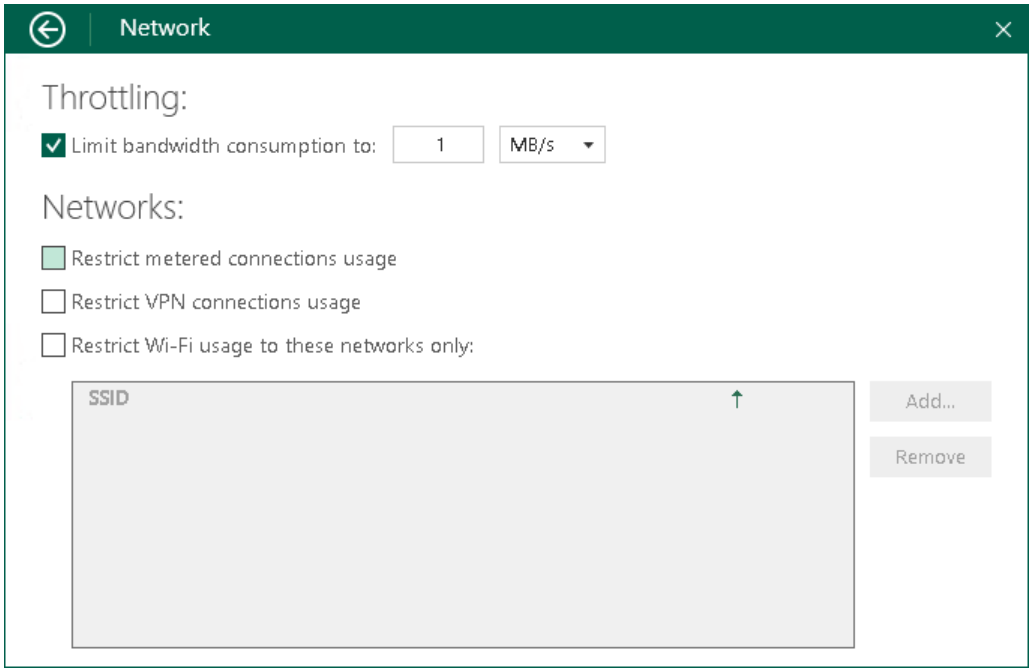
By default, backup over metered connections is disabled. To enable backup over metered connections:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Networks** section, clear the **Restrict metered connections usage** check box.

NOTE

For the cases when backup over metered connections is disabled, consider the following:

- If you start the backup job manually when only a metered connection is available, Veeam Agent for Microsoft Windows will display a warning and ask you to confirm that you want to use this connection for backup.
- If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use metered connections for backup.
- If you enable the backup cache for the backup job, and this backup job starts upon schedule when only a metered connection is available, Veeam Agent for Microsoft Windows will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.



Disabling Backup over VPN Connections

Veeam Agent can disable backup over VPN connections. This helps you avoid extra costs if your VPN service provider charges you by the amount of data sent and received by your computer. Veeam Agent automatically detects VPN connections and will not perform backup when your computer is on such connection.

By default, backup over VPN connections is enabled. To disable backup over VPN connections:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. In the **Networks** section, select the **Restrict VPN connections usage** check box.

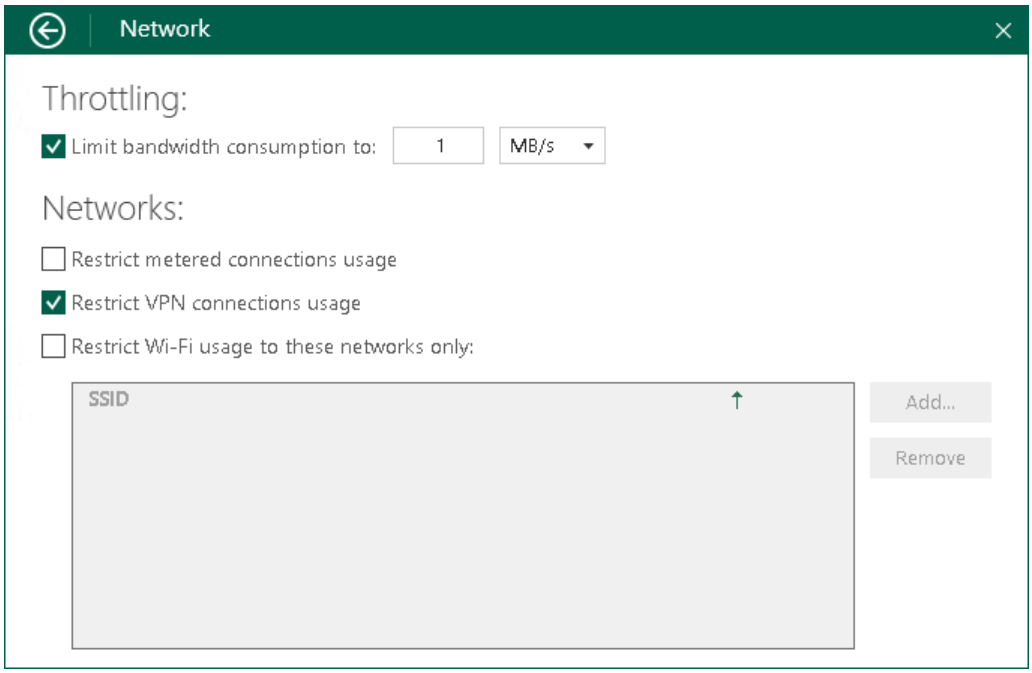
Keep in mind that Veeam Agent detects VPN connections created with Microsoft Windows in-built tools and the following 3rd party VPN providers:

- Cisco AnyConnect
- Fortinet SSL VPN
- Open VPN

NOTE

For the cases when backup over VPN connections is disabled, consider the following:

- If you start the backup job manually when only a VPN connection is available, Veeam Agent will display a warning and ask you to confirm that you want to use this connection for backup.
- If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use VPN connections for backup.
- If you enable the backup cache for the backup job, and this backup job starts upon schedule when only a VPN connection is available, Veeam Agent will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.



Selecting Wireless Networks for Backup

You can restrict usage of Wi-Fi networks for Veeam Agent for Microsoft Windows. This may be useful, for example, to avoid transmission of backed-up data over insecure or slow wireless network connections.

By default, Veeam Agent for Microsoft Windows is set up to back up data over any Wi-Fi network to which the Veeam Agent computer is connected. You can select one or more specific Wi-Fi networks and instruct Veeam Agent for Microsoft Windows to perform backup over these networks only. Backup over other wireless networks will be disabled.

To restrict usage of wireless networks:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage networks** link.
4. Select the **Restrict Wi-Fi usage to these networks only** check box and click **Add.**
5. Select one or more Wi-Fi networks in the list and click **Save**.

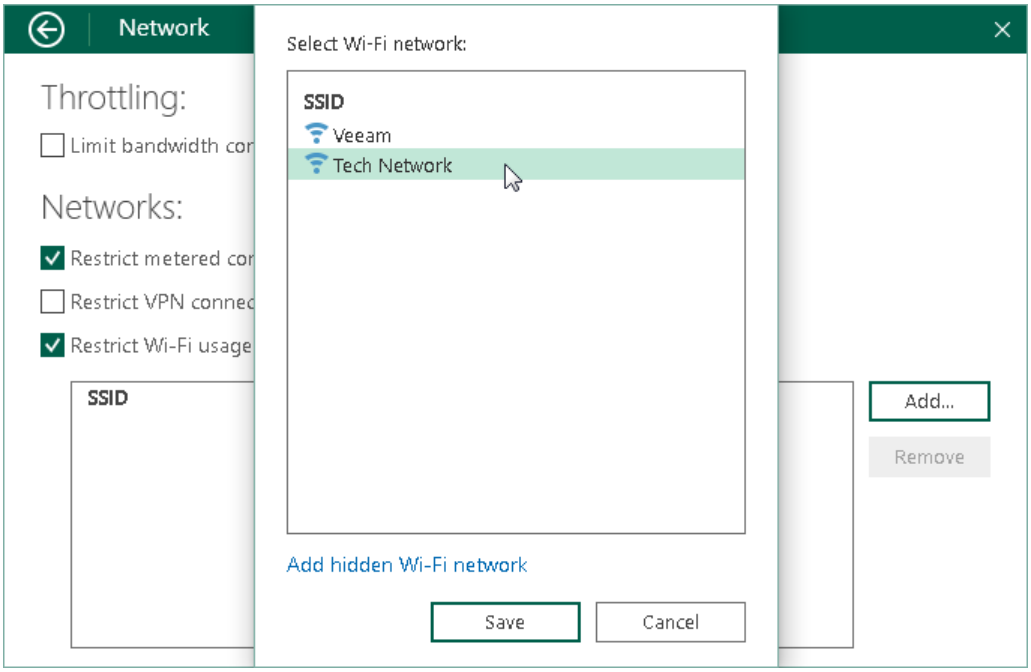
   If you want to allow Veeam Agent to back up data over a hidden wireless network, click the **Add hidden Wi-Fi network** link. In the displayed window, specify the SSID of the necessary network and click **Save**.

   If you want to restrict usage over any wireless networks, select the **Restrict Wi-Fi usage to these networks only** check box and do not add any networks to the list.

NOTE

For the cases when backup over Wi-Fi networks is restricted, consider the following:

- If you start the backup job manually when selected Wi-Fi networks are not available, Veeam Agent for Microsoft Windows will display a warning and ask you to confirm that you want to use this connection for backup.
- If you start the backup job with the command line interface, Veeam Agent will ignore the setting and will use all available Wi-Fi networks for backup.
- If you enable the backup cache for the backup job, and this backup job starts upon schedule when selected Wi-Fi networks are not available, Veeam Agent for Microsoft Windows will save the backup file to the backup cache. If the backup cache is not enabled, the backup job will fail.



Managing Rotated Drives

You can use a rotated drives scheme for storing backups. To do this, you can create backups on several external drives (for example, USB or FireWire) and swap these drives when needed.

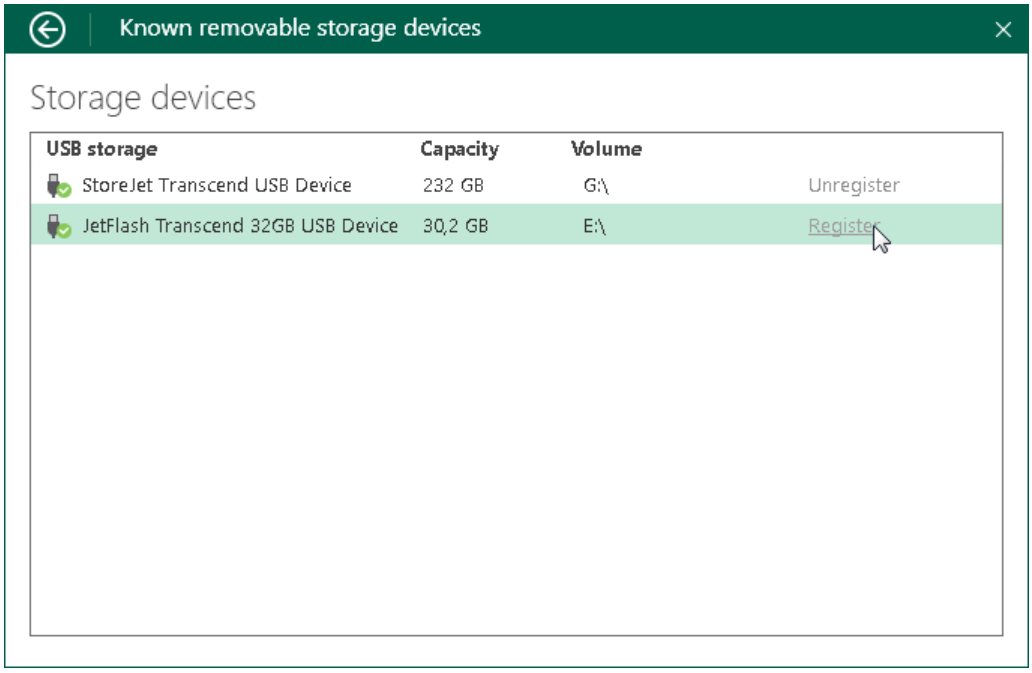
The drive on which you plan to store a backup must be registered in Veeam Agent for Microsoft Windows. If the drive is not registered, Veeam Agent for Microsoft Windows will not be able to detect the drive and store a backup on it.

Mind the following limitations:

- You can register and unregister drives if you have selected to store backups on an external drive connected to the computer. If you have selected to store backups on a local computer drive, in a network shared folder or on a backup repository, registering options will be disabled.
- You cannot unregister all drives at once. At least one drive will remain registered in Veeam Agent for Microsoft Windows.

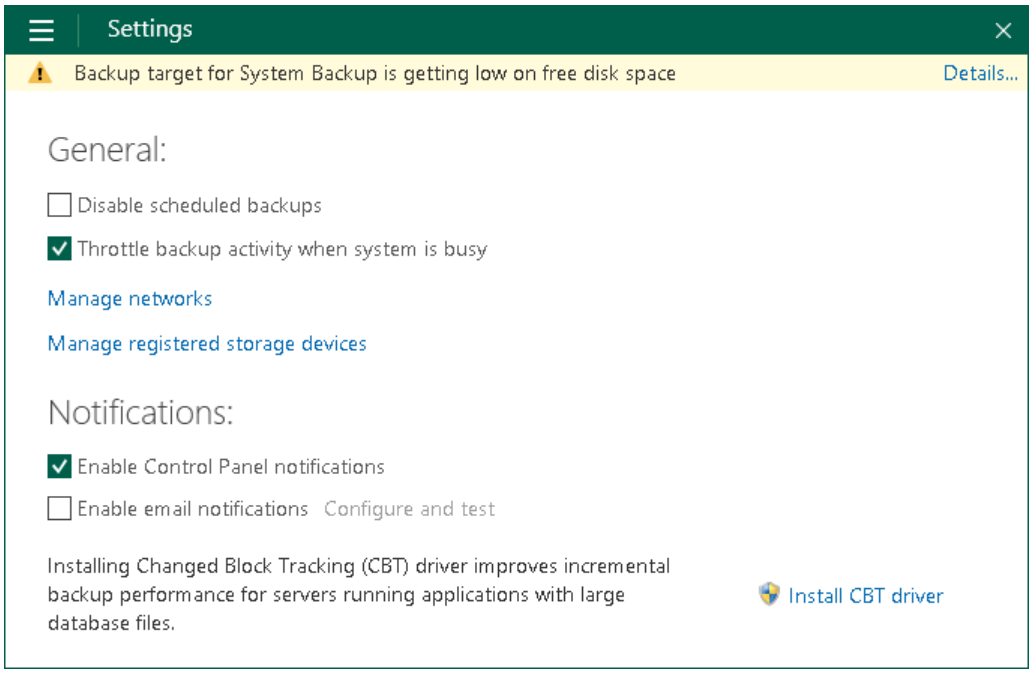
To register and unregister a drive in Veeam Agent for Microsoft Windows:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click the **Manage registered storage devices** link.
4. In the list of devices, click **Register/Unregister** next to the necessary backup storage device.



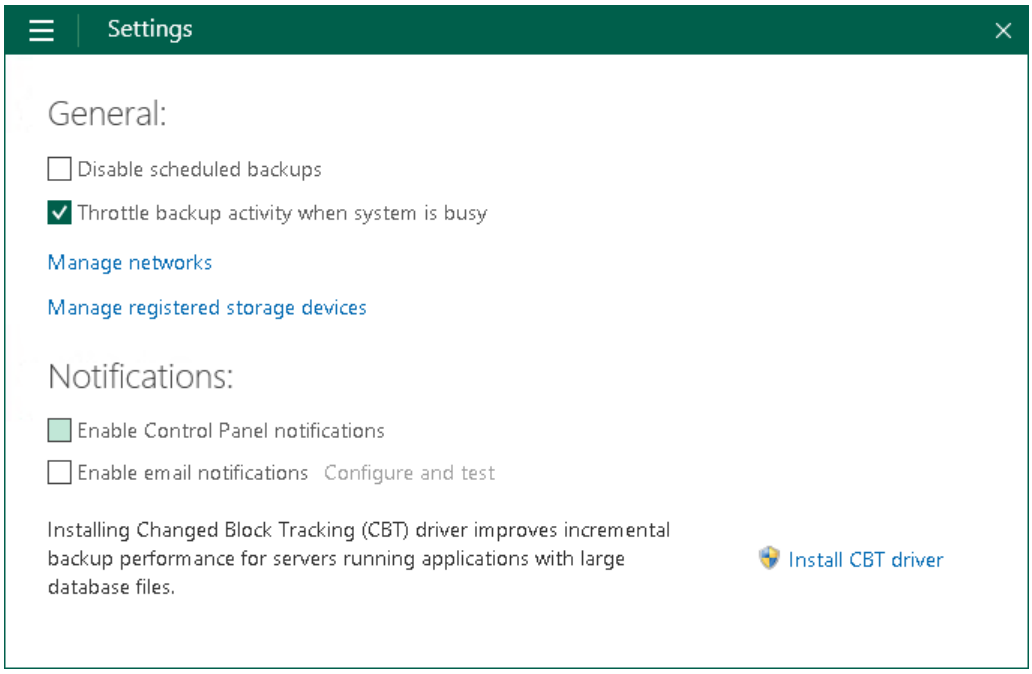
Disabling Control Panel Notifications

Veeam Agent for Microsoft Windows displays warning and information messages on the notification bar in the Control Panel. If necessary, you can disable Veeam Agent notifications.



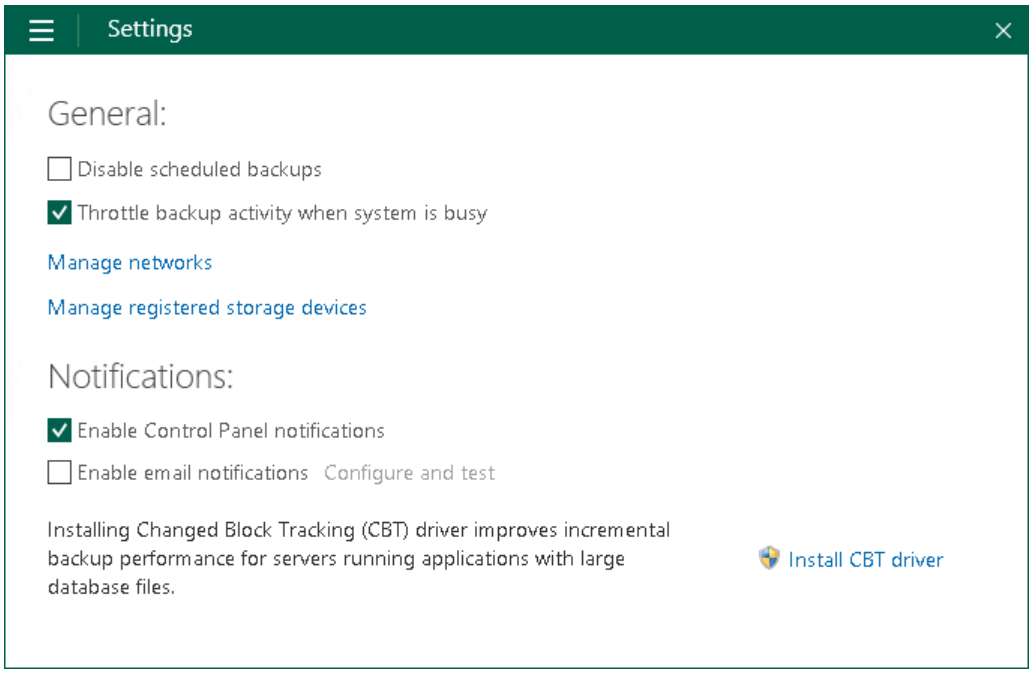
To disable notifications:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. In the **Notifications** section, clear the **Enable Control Panel notifications** check box.



Enabling Email Notifications

You can enable Veeam Agent for Microsoft Windows email notifications to receive reports containing data on the latest backup job session statistics and result.



To enable email notifications:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. In the **Notifications** section, select the **Enable email notifications** check box and click the **Configure and test** link.
4. In the **Configure and test email notifications** window, in the **Email settings** section, in the **Your email address** field, specify the recipient address.

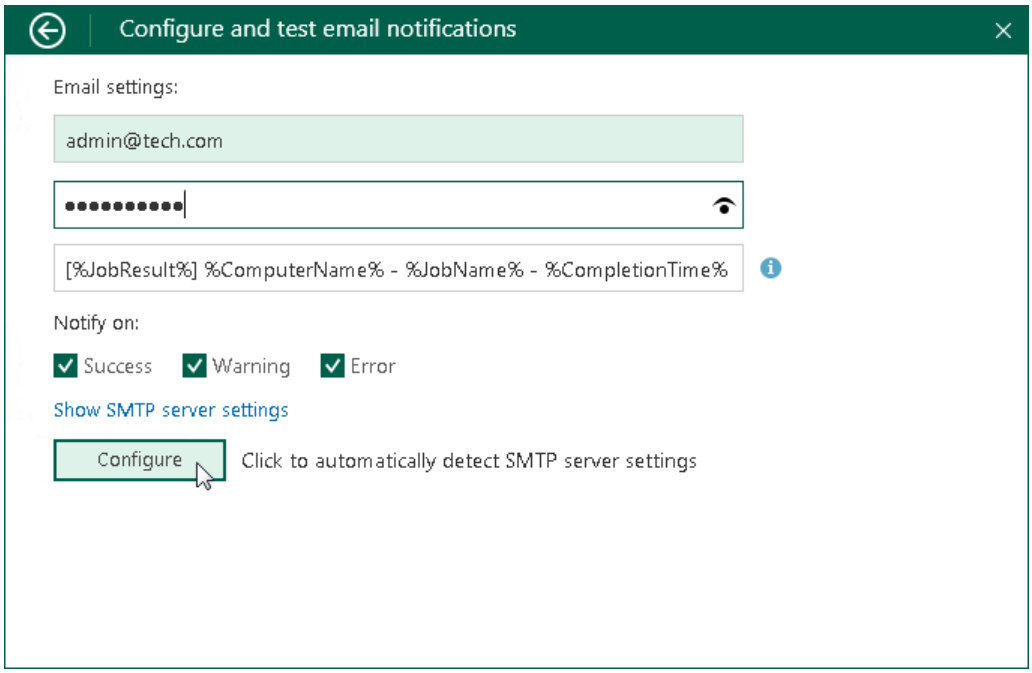
   Veeam Agent will send email notifications to the specified address. This address will be also displayed as the sender address in the email notification headers.

   [For Workstation and Server product editions] Keep in mind that you can specify several recipient addresses with Veeam Agent Configurator. To learn more, see the Notification Settings section in the Veeam Agent Configurator Reference.
5. If the SMTP server requires authentication, in the **Password** field, specify a password for the account that has rights to access the SMTP server.
6. In the **Email subject** filed, specify a subject for the sent message. You can use the following variables in the subject:
   a. *%ComputerName%*
   b. *%JobName%*
   c. *%JobResult%*
   d. *%CompletionTime%*

7. In the **Notify on** section, select the **Success**, **Warning** and/or **Error** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
8. Click **Configure**. Veeam Agent will try to automatically detect SMTP server settings. If the SMTP server settings are detected successfully, Veeam Agent 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 Agent database.



Configuring SMTP Server Settings

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

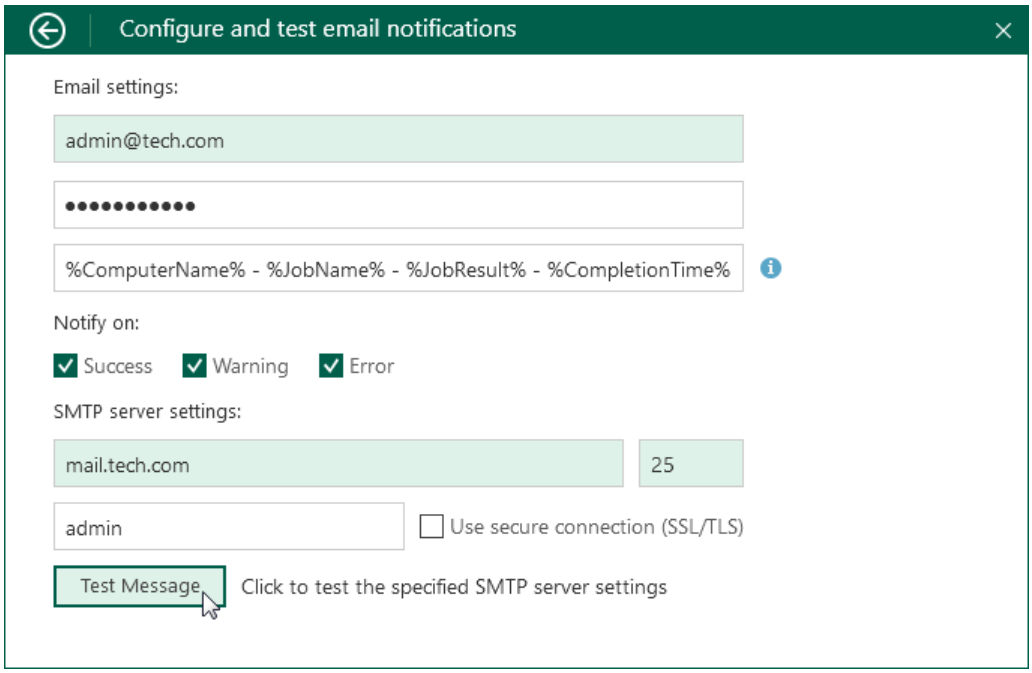
To configure SMTP server settings:

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

TIP

Keep in mind the following:

- 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 a new recipient address in the **Your email address** field and click **Configure**. Veeam Agent for Microsoft Windows will try to detect settings for the specified email address.
- If you want to get email notifications using Microsoft Office 365, you must establish a secure connection to the *smtp.office365.com* server over port *587*. For more information, see this Microsoft article.



Checking for New Product Versions and Updates

You can set up Veeam Agent for Microsoft Windows to automatically notify you about new product versions and updates. When a new version or patch becomes available, Veeam Agent for Microsoft Windows displays a notification in the notification bar. You can download the setup file and update Veeam Agent for Microsoft Windows. To learn more, see Upgrading Veeam Agent for Microsoft Windows.

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

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **About**.
3. In the **Update** section, clear the **Automatically check and notify me on available updates** check box.

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

> **NOTE**
>
> Consider the following:
>
> - To get information about available product updates, Veeam Agent for Microsoft Windows sends request to the Veeam Update Notification Server (autolk.veeam.com).
> - For downloading setup files, Veeam Agent uses the Background Intelligent Transfer Service (BITS). If this service is disabled on the Veeam Agent computer, Veeam Agent for Microsoft Windows will not be able to download a setup file.

Managing Veeam CBT Driver

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

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

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

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

- Install the Veeam CBT driver.
- Remove the Veeam CBT driver.
- Remove the Veeam CBT driver with Veeam Recovery Media.
- Reset the Veeam CBT driver.

Installing Veeam CBT Driver

You can install the Veeam CBT driver at any time you need. This operation is available if you use the Server edition of Veeam Agent for Microsoft Windows on a computer that runs a Microsoft Windows Server OS. To learn about other requirements and limitations for the Veeam CBT driver, see Veeam Changed Block Tracking Driver.

IMPORTANT

Consider the following:

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

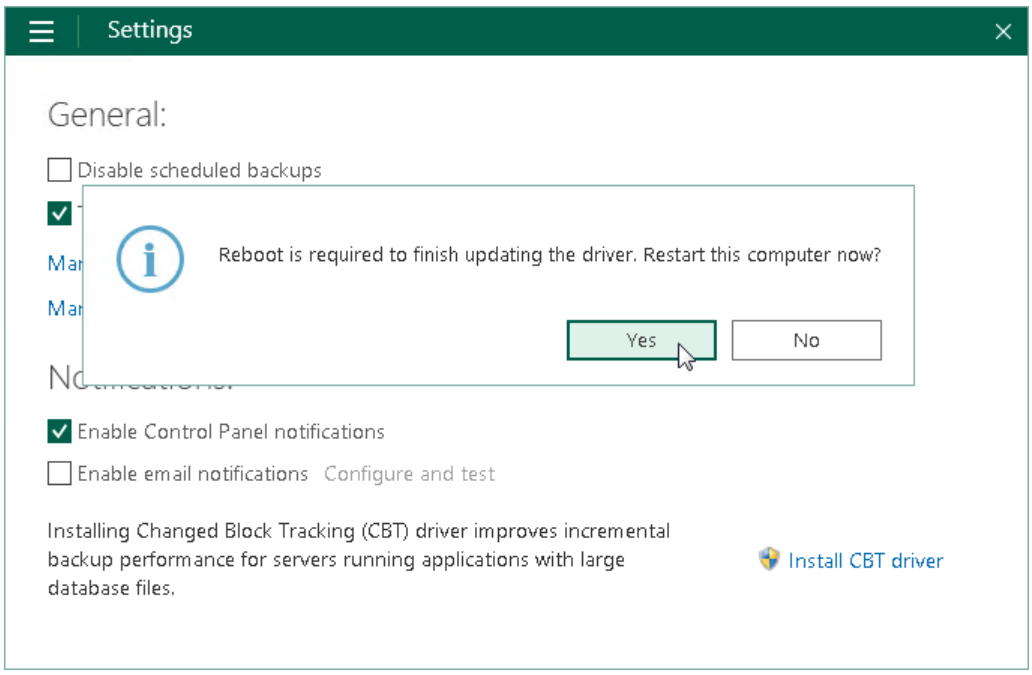
  The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver. To learn more, see this Microsoft KB article.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, 2012 or 2012 R2 if one or more volumes on this computer are encrypted with Microsoft BitLocker (or other encryption tool), or if you plan to use Microsoft BitLocker to encrypt volumes on this computer. Concurrent operation of Microsoft BitLocker and Veeam CBT driver may result in driver failures and may prevent the OS from starting.

To install the Veeam CBT driver:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click **Install CBT driver**.

4. To complete the installation process, Veeam Agent for Microsoft Windows needs to reboot the computer. To reboot the computer immediately, in the displayed window, click **Yes**. After Veeam Agent for Microsoft Windows reboots the computer, the driver will start tracking blocks that are changing on the volume(s) whose data you chose to back up in the backup job settings.

   If you choose not to reboot the computer immediately, Veeam Agent for Microsoft Windows will continue to use the default CBT mechanism until the next computer reboot.



Removing Veeam CBT Driver

You can quickly remove the Veeam CBT driver, for example, if your Veeam Agent computer does not run applications with large database files any more, and you do not need to perform advanced change block tracking on this computer.

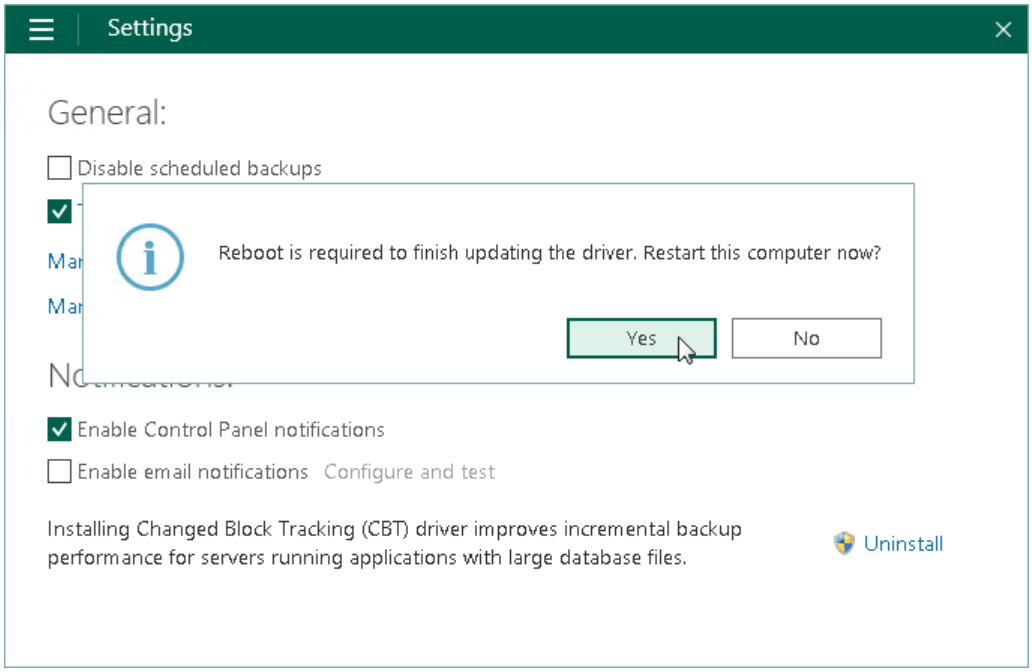
To remove the Veeam CBT driver:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Settings**.
3. Click **Uninstall**.
4. To complete the uninstallation process, Veeam Agent for Microsoft Windows needs to reboot the computer. To reboot the computer immediately, in the displayed window, click **Yes**. After computer reboot, Veeam Agent for Microsoft Windows will use the default CBT mechanism to get the list of changed data blocks.

TIP

You can also uninstall the Veeam CBT driver in the Microsoft Windows control panel:

1. From the **Start** menu, select **Control Panel** > **Programs and Features**.
2. In the programs list, right-click **Veeam CBT Driver** and select **Uninstall**.
3. In the displayed window, click **Yes**.



Removing CBT Driver with Veeam Recovery Media

You can use the Veeam Recovery Media to remove the Veeam CBT driver from your Veeam Agent computer. This operation may be required, for example, if the OS on your computer fails to start after you have installed the Veeam CBT driver in Veeam Agent for Microsoft Windows.

To remove the Veeam CBT driver:

1. Boot from the Veeam Recovery Media.
2. On the Veeam Recovery Media screen, click **Tools** > **Command Prompt** or press **[Shift]** + **[F10]**.
3. Use a command with the following syntax:

```
X:\VeeamRecovery\Veeam.Endpoint.Recovery.exe -RemoveVeeamCBTDriver
```

4. Reboot the Veeam Agent computer.

NOTE

Veeam Agent for Microsoft Windows will remove the Veeam CBT Driver from the Veeam Agent computer. However, a record about the driver will remain in the Microsoft Windows control panel. To remove the record, from the **Start** menu, select **Control Panel** > **Programs and Features**. Then right-click **Veeam CBT Driver** in the programs list and select **Uninstall**.

Resetting CBT

In some cases, it may be required to reset CBT data collected by the Veeam CBT driver. For example, this may be necessary if you want to avoid performing active full backup after a volume was changed in a non-Windows OS.

To reset CBT, run the command line interface with administrative privileges and use one of the following commands:

- To reset CBT for all volumes of the Veeam Agent computer, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT all
```

- To reset CBT for a specific volume, use a command with the following syntax:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT %volumeMountPoint%
```

or

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.EndPoint.Manager.exe" RESETCBT %volumeUUID%
```

where:

  - `%volumeMountPoint%` — mount point of the volume, for example: `C:\`.
  - `%volumeUUID%` — ID of the volume, for example: `\\?\Volume{1214be80-1165-41e5-8244-8fbf79d85c31}`.

After CBT reset, during the next backup job session, Veeam Agent for Microsoft Windows will create incremental backup. The backup job session will require greater time, because Veeam Agent for Microsoft Windows will need to read all data from the backed-up volume(s).

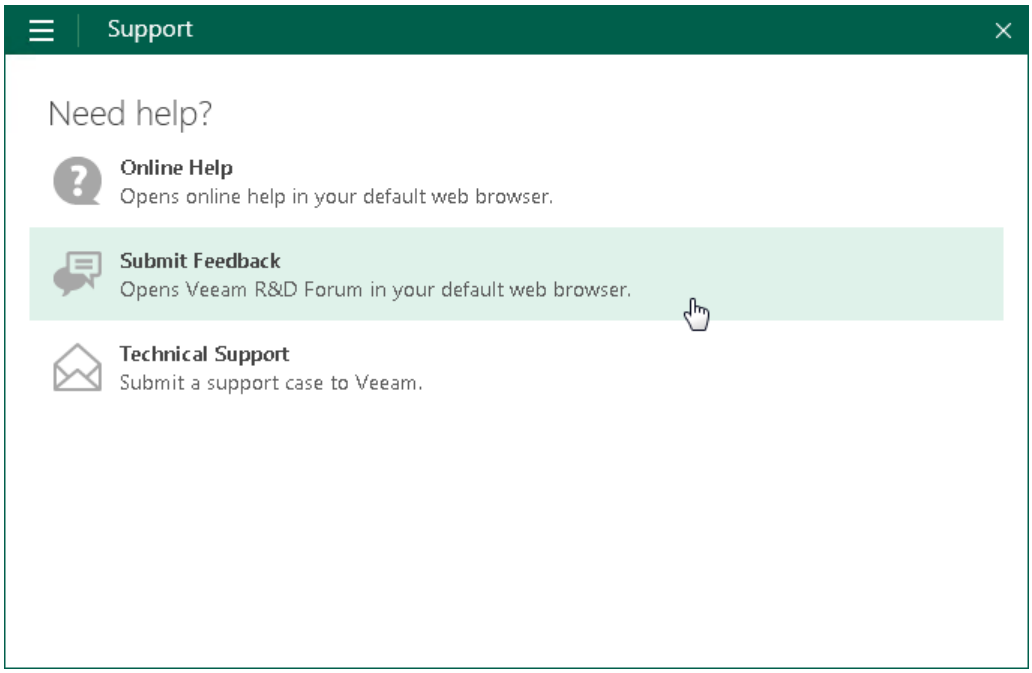
Getting Support

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

- You can search for the information on the necessary subject in the current Veeam Agent for Microsoft Windows User Guide.
- You can visit Veeam R&D Forums and share your opinion or ask a question.
- You can submit a support case to the Veeam Customer Support directly from the product. To learn more, see Reporting Issues.

To access help and support options in Veeam Agent:

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



Reporting Issues

You can submit a support case in the Control Panel. To submit a support case:

1. Double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Support**.
3. Click **Technical Support**.
4. In the email field of the **Report an issue** window, enter a valid email address.

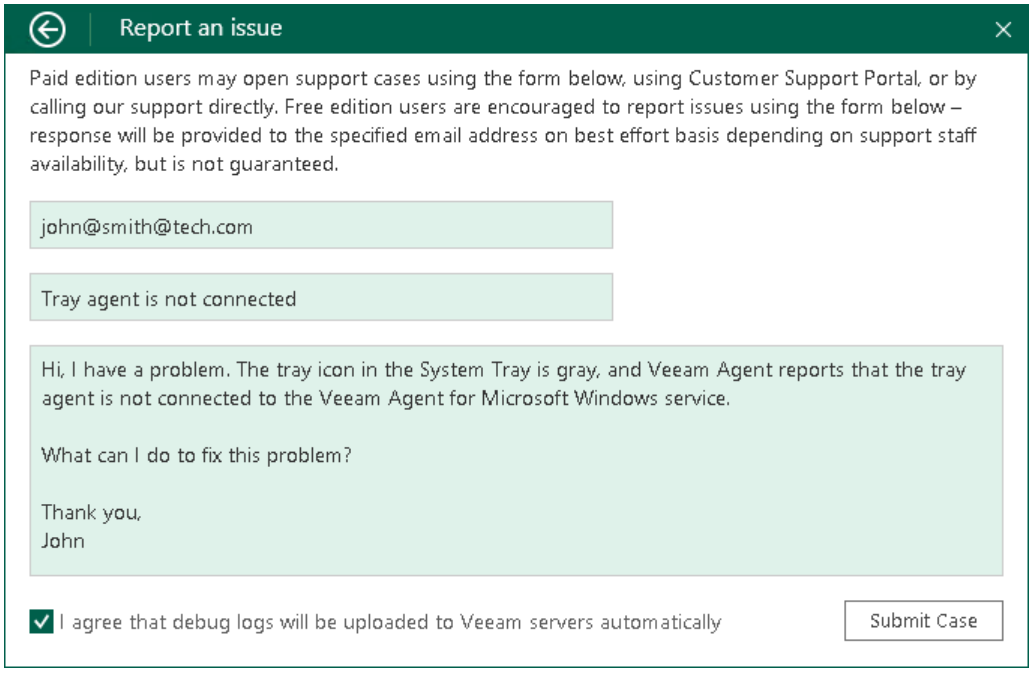
   If the email address that you have entered in not registered at the Veeam Customer Support Portal, click **Register** on the right of the email field. Veeam Software will register your email address and send you a verification email to the specified address. When you receive a verification email, open it and click a link provided in the email to complete the verification procedure. After the verification procedure is complete, you will be able to submit a support case.
5. In the description fields, enter a short and detailed description of your problem.
6. Select the **I agree that debug logs will be uploaded to Veeam servers automatically** check box and click **Submit Case**.

Veeam Agent will automatically collect logs from your computer (without additional warnings) and open a support case at the Veeam Customer Support Portal.

IMPORTANT

Mind the following:

- If you have any questions about the product functionality, do not submit a support case via the Veeam Customer Support Portal and do not send an email to the Veeam Customer Support directly. To submit a support case, use the Control Panel in Veeam Agent for Microsoft Windows.
- You can submit a support case only in the Control Panel of the current version of Veeam Agent. If you use older version of Veeam Agent, upgrade Veeam Agent and check whether the problem still exists in the current version. If the problem exists, use the Control Panel to submit a support case.



Using with Veeam Backup & Replication

If you have the Veeam backup infrastructure deployed in the production environment, you can use Veeam Agent for Microsoft Windows together with Veeam Backup & Replication.

IMPORTANT

If you plan to use Veeam Agent for Microsoft Windows 5.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a on the Veeam backup server. Veeam Agent for Microsoft Windows 4.0 supports integration with Veeam Backup & Replication 11 or later as well.

NOTE

This and subsequent sections describe tasks with Veeam Backup & Replication available for Veeam Agent for Microsoft Windows operating in the standalone mode. For information about tasks available in Veeam Backup & Replication within the Veeam Agent management scenario, see Veeam Agent Management Guide.

Tasks with Veeam Backup & Replication

Veeam Backup & Replication lets you perform a number of additional data protection and disaster recovery tasks, as well as administrative actions with Veeam Agent backups. You can:

- Grant access permissions on backup repositories.
- Manage Veeam Agent licenses.

Data protection tasks

- Create Veeam Agent backups on backup repositories.
- Create Veeam Agent backups on Veeam Cloud Connect repositories.
- Copy Veeam Agent backups to secondary backup repositories.
- Archive Veeam Agent backups to tape.

Restore tasks

- Restore Veeam Agent backups to Hyper-V VMs.
- Restore Veeam Agent backups to VMware vSphere VMs.
- Restore volumes from Veeam Agent backups.
- Restore files and folders from Veeam Agent backups.
- Restore application items from Veeam Agent backups.
- Restore disks from Veeam Agent backups.
- Restore data from Veeam Agent backups to Amazon EC2.
- Restore data from Veeam Agent backups to Microsoft Azure.
- Export restore points of Veeam Agent backups to standalone full backup files.

Administrative tasks

- Import Veeam Agent backups.
- Enable and disable Veeam Agent backup jobs.
- Delete Veeam Agent backup jobs.
- View Veeam Agent backup job statistics.
- Remove Veeam Agent backups.
- View Veeam Agent backup properties.
- Configure global settings.
- Assign roles to users.

Setting Up User Permissions on Backup Repositories

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

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

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

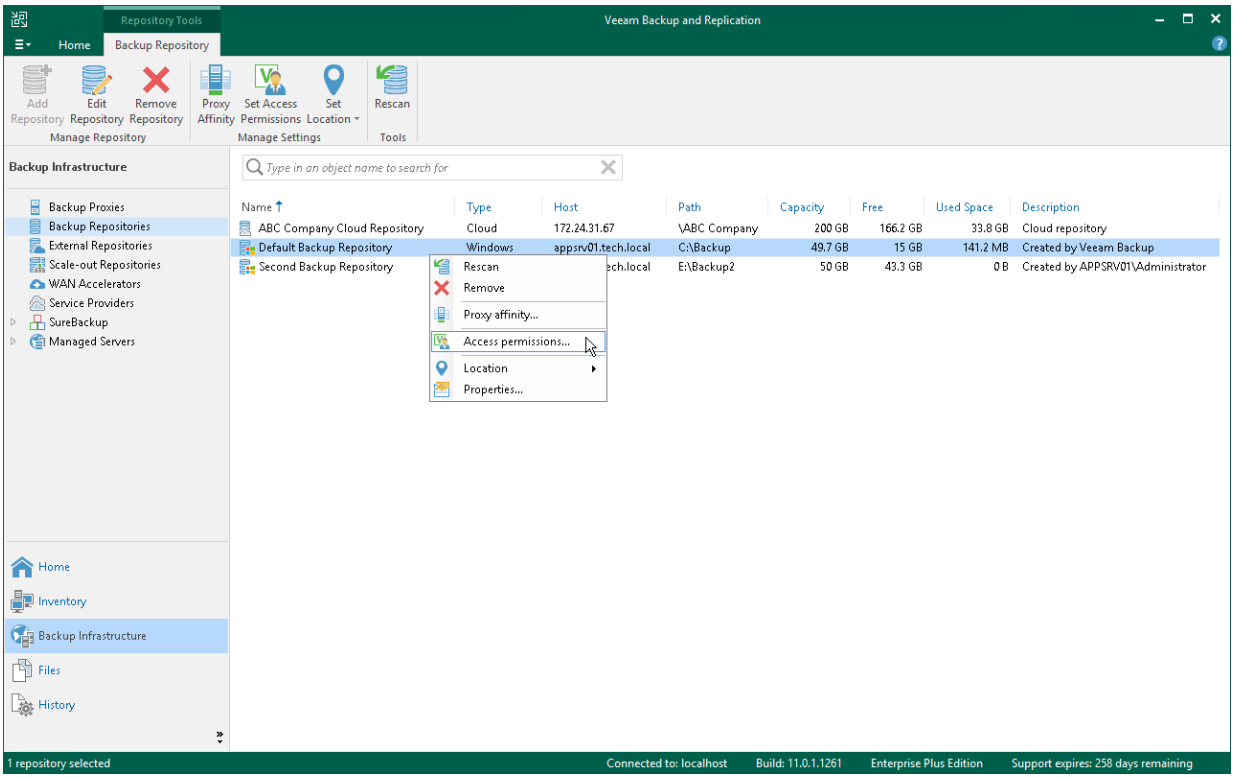
Right after installation, access permissions on the default backup repository are set to *Allow to everyone* for testing and evaluation purposes. If necessary, you can change these settings.

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

To grant access permissions to a security principal:

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.
2. In the inventory pane, click one of the following nodes:
   - The **Backup Repositories** node — if you want to grant access permissions on a regular backup repository to Veeam Agent users.
   - The **Scale-out Repositories** node — if you want to grant access permissions on a scale-out backup repository to Veeam Agent users.

3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon, or right-click the backup repository and select **Access permissions**. If you do not see the **Set Access Permissions** button on the ribbon or the **Access permissions** command is not available in the shortcut menu, press and hold the **[CTRL]** key, right-click the backup repository and select **Access permissions**.



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

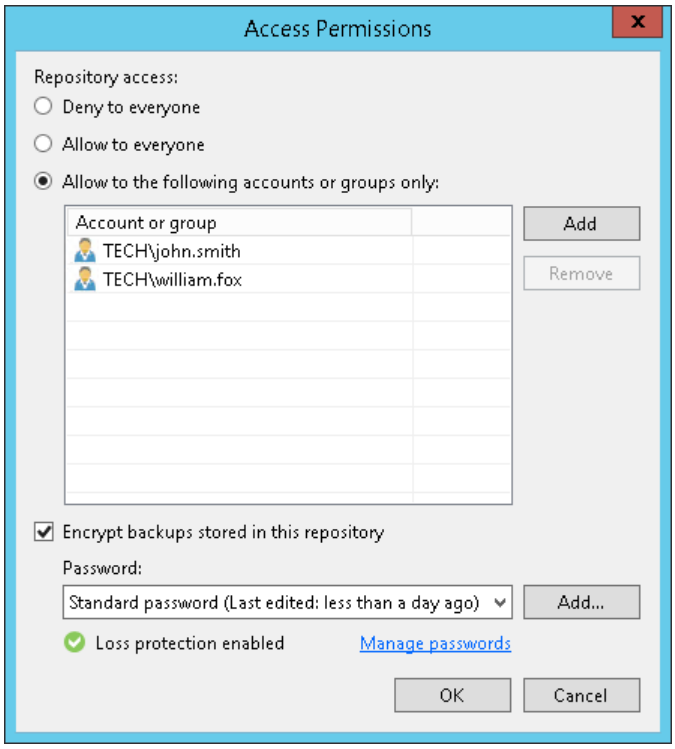
   - **Allow to everyone** — select this option if you want all users to be able to store backups on this backup repository. Setting access permissions to *Everyone* is equal to granting access rights to the *Everyone* Microsoft Windows group (*Anonymous* users are excluded). However, we recommend this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

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

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

IMPORTANT

If Veeam Agent for Microsoft Windows is set up to use the backup cache, and the backup cache contains one or more restore points, Veeam Agent for Microsoft Windows will automatically remove these restore points from the backup cache after you enable or disable the encryption option for the backup repository.



Managing License

If you plan to use Veeam Agent for Microsoft Windows with Veeam Backup & Replication, you must install a license in Veeam Backup & Replication or Veeam Backup Enterprise Manager. The license must have a total number of instances that is sufficient to protect machines (servers and workstations) on which you plan to install Veeam Agent for Microsoft Windows. For more information, see Veeam Licensing Policy.

After Veeam Agent for Microsoft Windows connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming instances in the license. The product edition for Veeam Agent is selected depending on the type of the Microsoft Windows OS running on the Veeam Agent computer. You can switch to another commercial edition of Veeam Agent for Microsoft Windows manually if needed. If you do not want Veeam Agents to consume instances, you can restrict instance consumption. For details, see Managing Instance Consumption by Veeam Agents.

The number of backup jobs configured in Veeam Agent for Microsoft Windows does not impact instance consumption. For example, if 2 backup jobs are configured in Veeam Agent for Microsoft Windows that operates in the Server edition, this Veeam Agent for Microsoft Windows will consume instances required for 1 server.

Veeam Agent for Microsoft Windows obtains information about the license from Veeam Backup & Replication and keeps it locally on the Veeam Agent computer. Information about the license is valid for 32 days. If Veeam Agent for Microsoft Windows does not connect to Veeam Backup & Replication during this period, Veeam Backup & Replication will revoke its license.

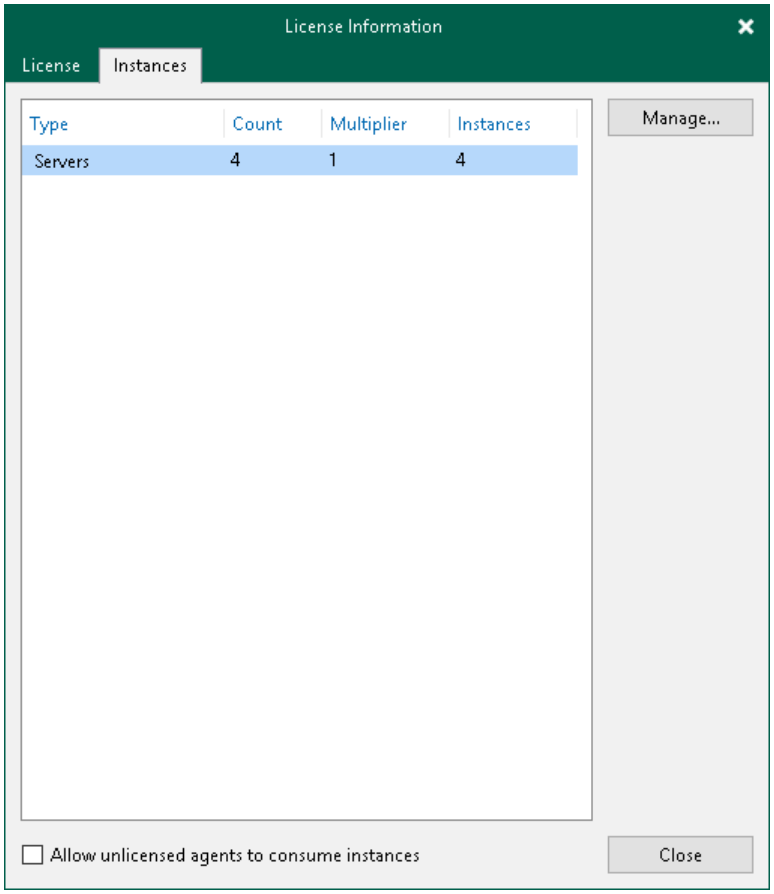
> **NOTE**
>
> In addition to managing Veeam Agent for Microsoft Windows licenses, you can use the Veeam Backup & Replication console to manage Veeam Agent backup jobs and perform operations with backups created by these jobs.
>
> If your backup server is connected to Veeam Backup Enterprise Manager, you can use Veeam Backup Enterprise Manager to manage licenses and perform restore tasks with Veeam Agent backups. You cannot manage Veeam Agent backup jobs with Veeam Backup Enterprise Manager.

Managing Instance Consumption by Veeam Agents

By default, Veeam Backup & Replication allows Veeam Agents to connect to the Veeam backup server and consume instances in the license. If you do not want Veeam Agents to consume instances, you can restrict instance consumption.

To restrict instance consumption by Veeam Agents:

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



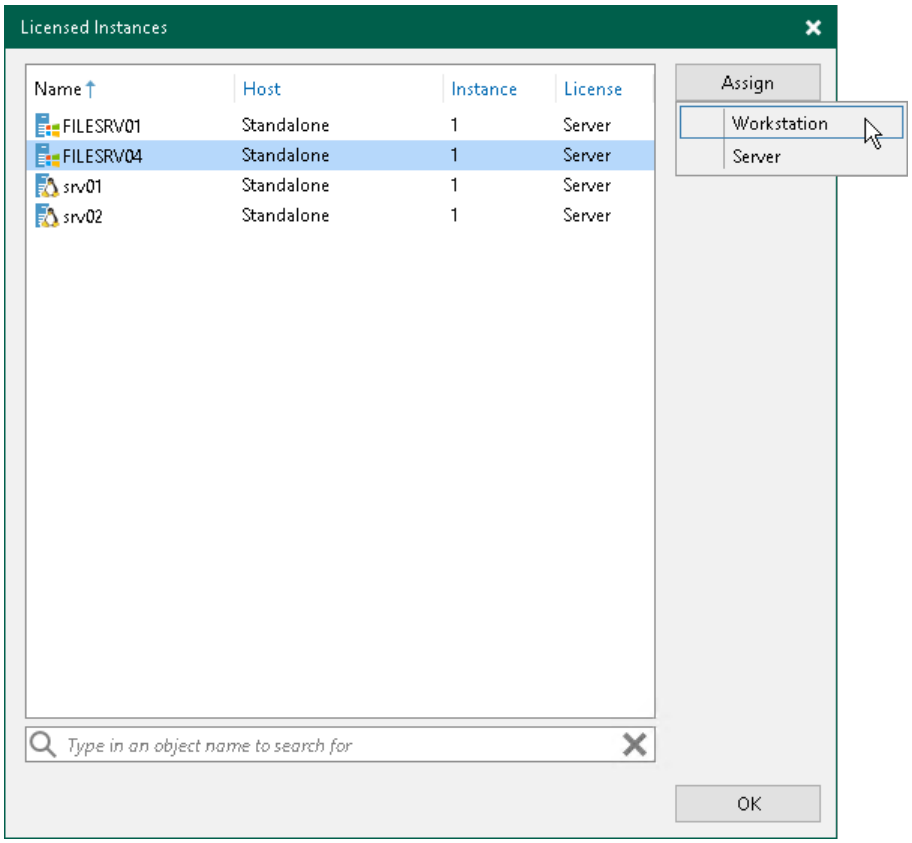
Assigning License to Veeam Agent

After Veeam Agent for Microsoft Windows connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. The product edition for Veeam Agent for Microsoft Windows is selected depending on the type of the Microsoft Windows OS running on the protected computer.

You can also assign a license to Veeam Agent for Microsoft Windows manually if needed. When you assign a license, you can select the product edition, too.

To assign a license:

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



Viewing Licensed Veeam Agents and Revoking License

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

To view a list of licensed Veeam Agents:

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

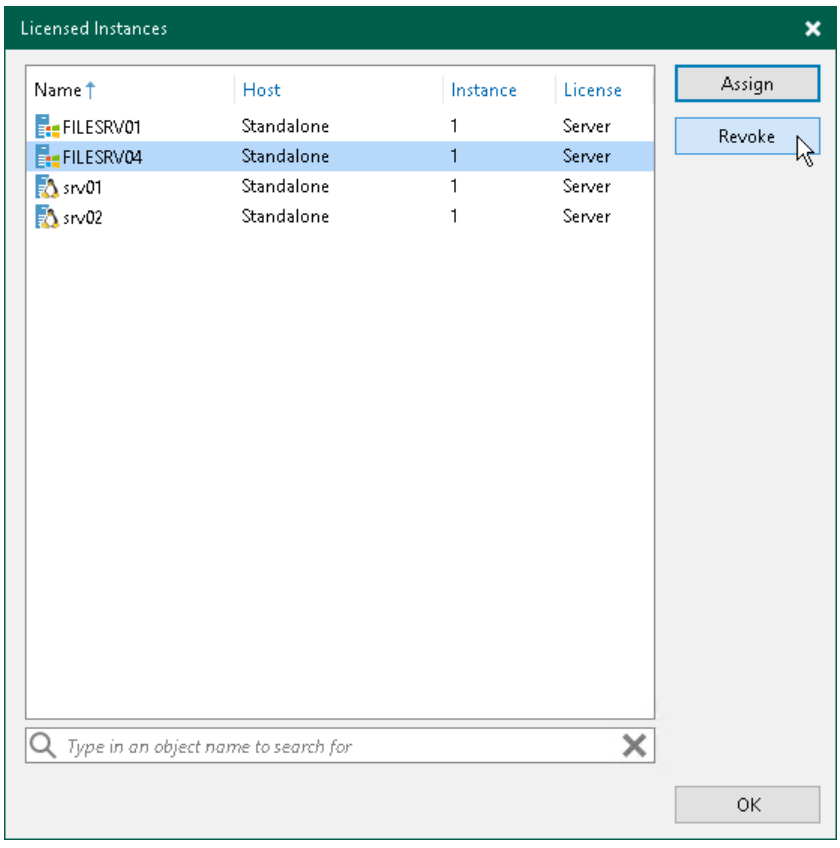
In the list of licensed instances, Veeam Backup & Replication displays Veeam Agents that have established a connection with the backup server when you created the backup job.

Revoking License from Veeam Agents

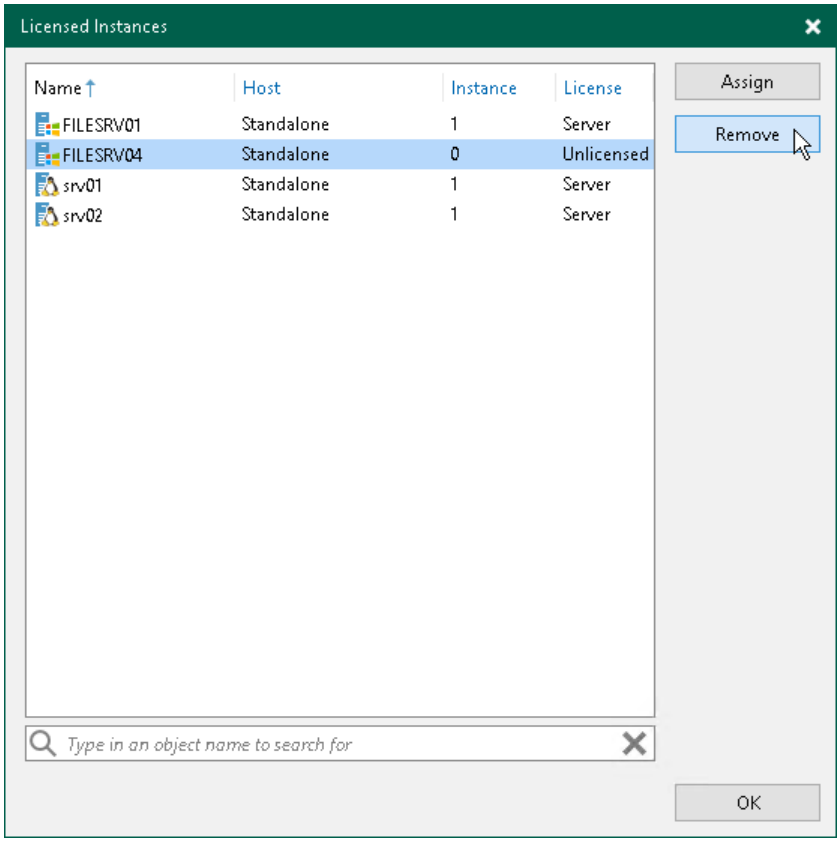
You can revoke the license from some Veeam Agents and re-apply it to other protected workloads. License revoking can be helpful, for example, if you do not want to use some Veeam Agents with Veeam Backup & Replication anymore.

To revoke a license from the Veeam Agent:

1. In Veeam Backup & Replication, from the main menu, select **License**.
2. In the **License Information** window, select the **Instances** tab and click **Manage**.
3. In the **Licensed Instances** window, select a Veeam Agent and click **Revoke**. Veeam Backup & Replication will revoke the license from the Veeam Agent, and the license will be freed for other workloads that you want to protect with Veeam products.



The Veeam Agent from which you have revoked the license will become unable to connect to the Veeam backup server but will remain in the **Licensed Instances** list. To allow this Veeam Agent to create backups in the Veeam backup repository, select the Veeam Agent and click **Remove**. During the next backup job session, the Veeam Agent will connect to the Veeam backup server and start consuming the license.



Performing Data Protection Tasks

You can perform the following data protection tasks:

- Back up your data and store the resulting backup files on one of the following types of Veeam backup repositories:
  - On a backup repository managed by a Veeam backup server
  - On a Veeam Cloud Connect repository
- Copy Veeam Agent backups from the backup repository to a secondary backup repository with backup copy jobs
- Archive Veeam Agent backups to tapes with backup to tape jobs

Backing Up to Backup Repositories

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

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

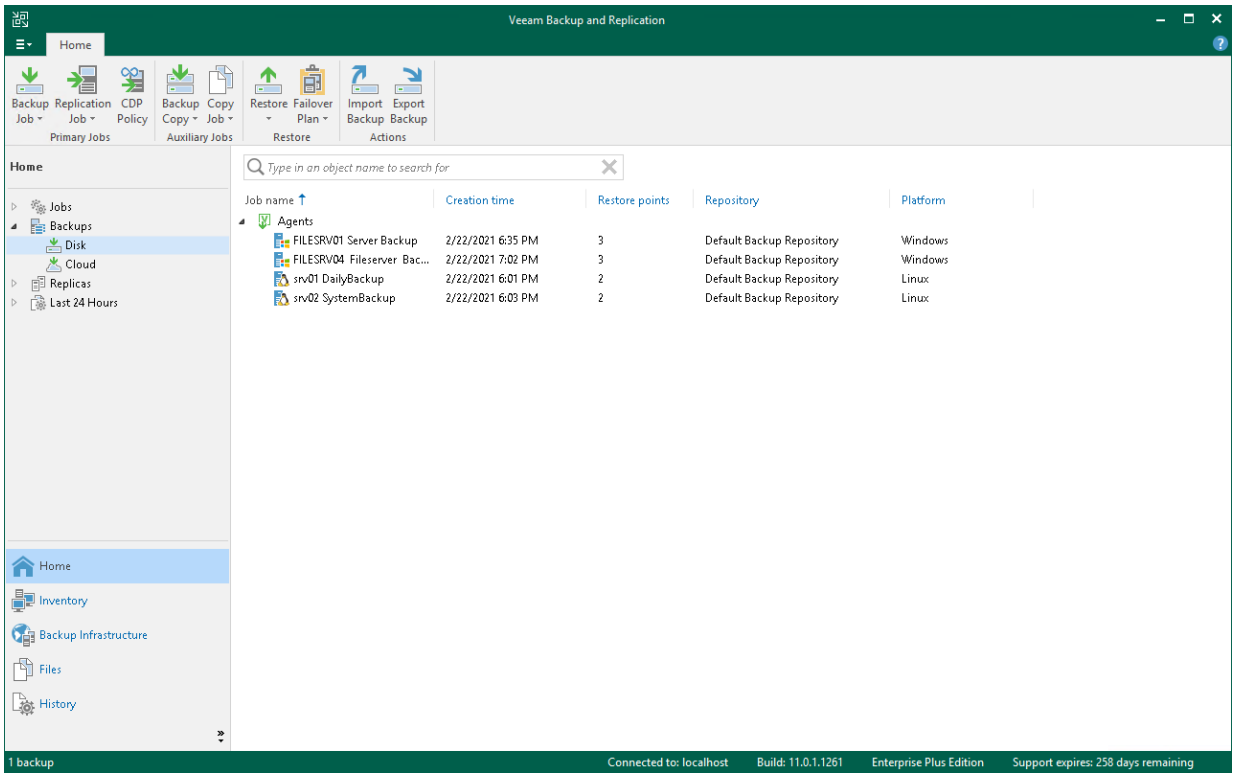
NOTE

Consider the following:

- A Veeam Agent backup job can be started automatically upon the defined schedule or manually from the Veeam Agent computer. You cannot start, stop, retry or edit Veeam Agent backup jobs in the Veeam Backup & Replication console.
- If the user is granted restore permissions on the Veeam backup server, the user will be able to see all backups on the backup repository.
- The user who creates a Veeam Agent backup on the backup repository is set as the owner of the backup file. The backup file owner can access this file and restore data from it. If the user who is not the backup file owner needs to perform operations with the backup file, the user must have the Veeam Backup & Replication role that allows to perform these operations. To learn more about roles, see the Roles and Users section in the Veeam Backup & Replication User Guide.

Backup jobs targeted at the backup repository become visible in Veeam Backup & Replication under the **Jobs** > **Backup** node in the **Home** view. Backups created with Veeam Agent are available under the **Backups** > **Disk** node in the **Home** view.

The Veeam Backup Administrator working with Veeam Backup & Replication can manage Veeam Agent backup jobs and restore data from Veeam Agent backups. To learn more, see Performing Restore Tasks and Performing Administration Tasks.



Backing Up to Cloud Repositories

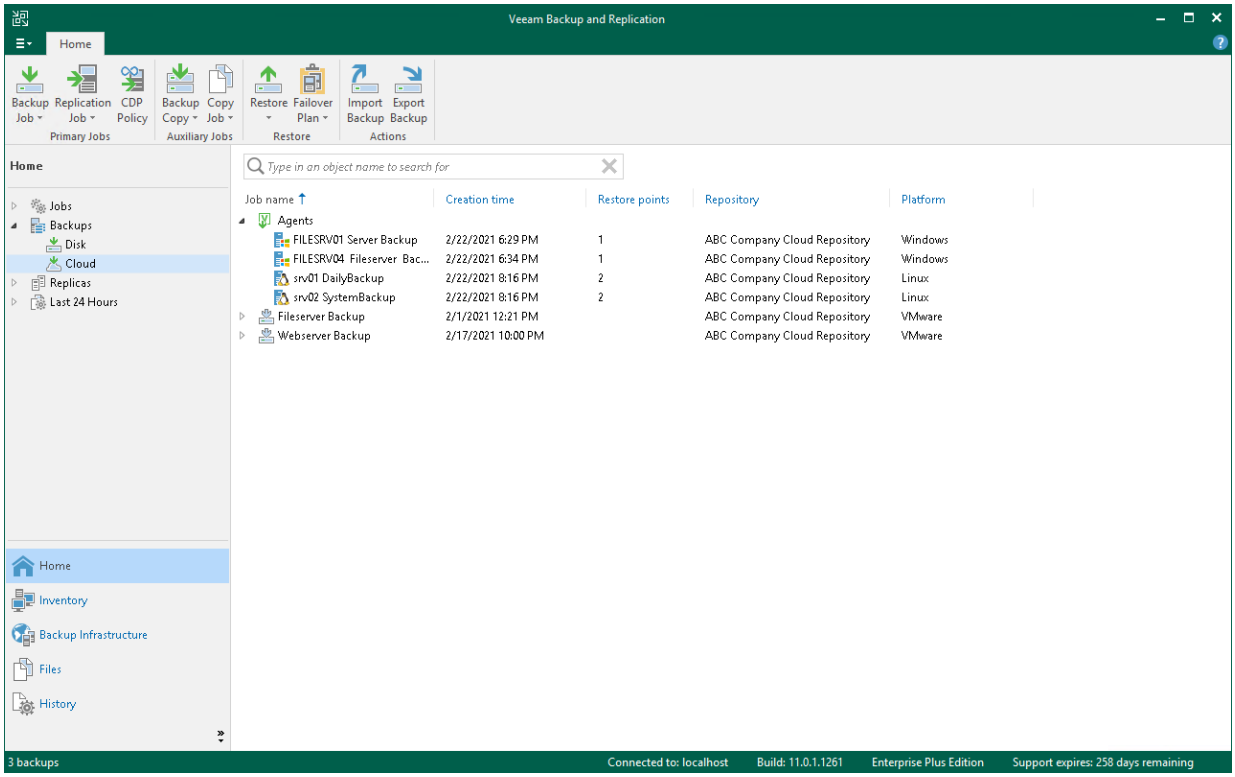
You can store backups created with Veeam Agent for Microsoft Windows on cloud repositories provided to you by a Veeam Cloud Connect service provider. To do this, you must connect to the service provider and point the backup job to the cloud repository. To learn more, see Specify Service Provider Settings.

Veeam Agent Backups on Tenant Side

Backups created with Veeam Agent for Microsoft Windows are available under the **Cloud** node in the **Home** view of the Veeam Backup & Replication console deployed on the tenant side.

The backup administrator working with Veeam Backup & Replication on the tenant side can manage Veeam Agent backups created on the cloud repository and restore data from such backups. To recover data from a Veeam Agent backup, you can perform the following operations:

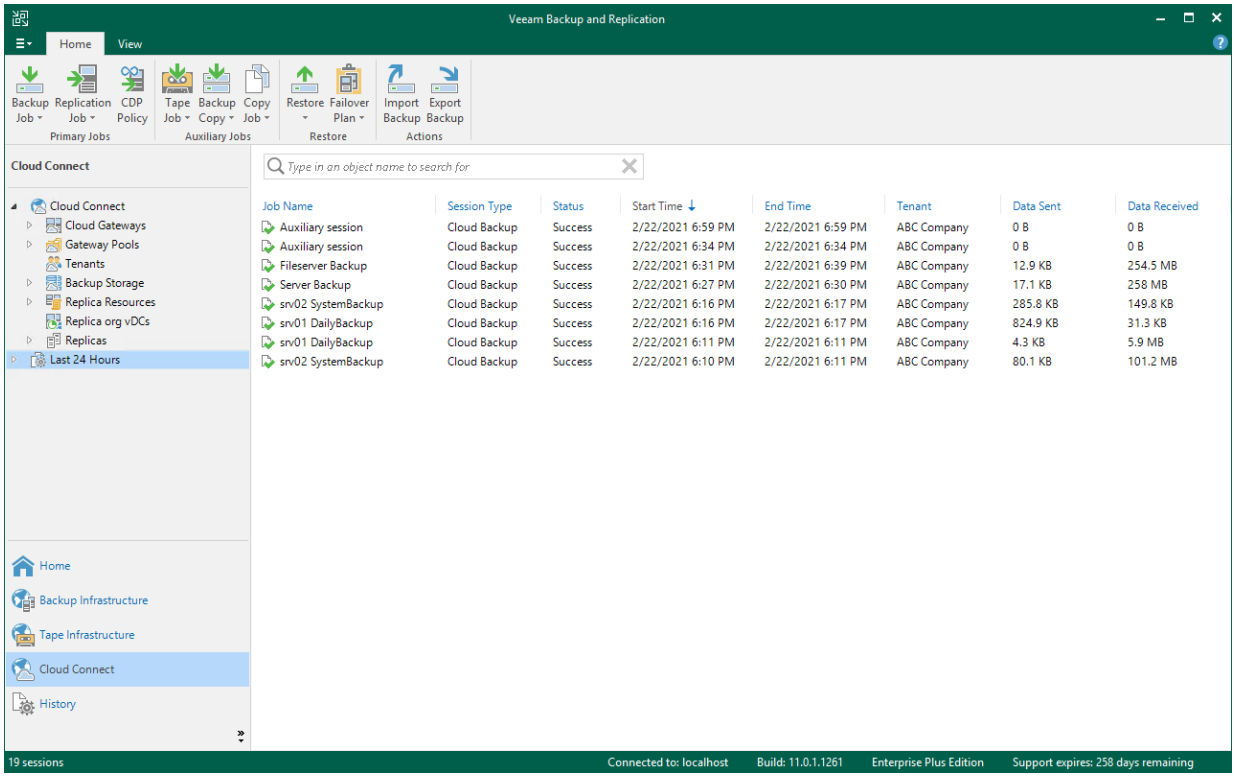
- Export computer disks as virtual disks
- Restore guest OS files
- Export restore points to standalone full backup files.



Veeam Agent Backups on Service Provider Side

The service provider can view information about backup and restore sessions performed by Veeam Agent users. The full list of sessions is available in the **History** view of the Veeam backup console deployed on the service provider side. The list of sessions performed within the last 24 hours is available under the **Last 24 hours** node in the **Cloud Connect** view of the Veeam backup console on the service provider side. The service provider cannot view detailed statistics about individual sessions in the list.

The service provider cannot perform restore tasks with Veeam Agent backups that are stored on the cloud repository.



Performing Backup Copy for Veeam Agent Backups

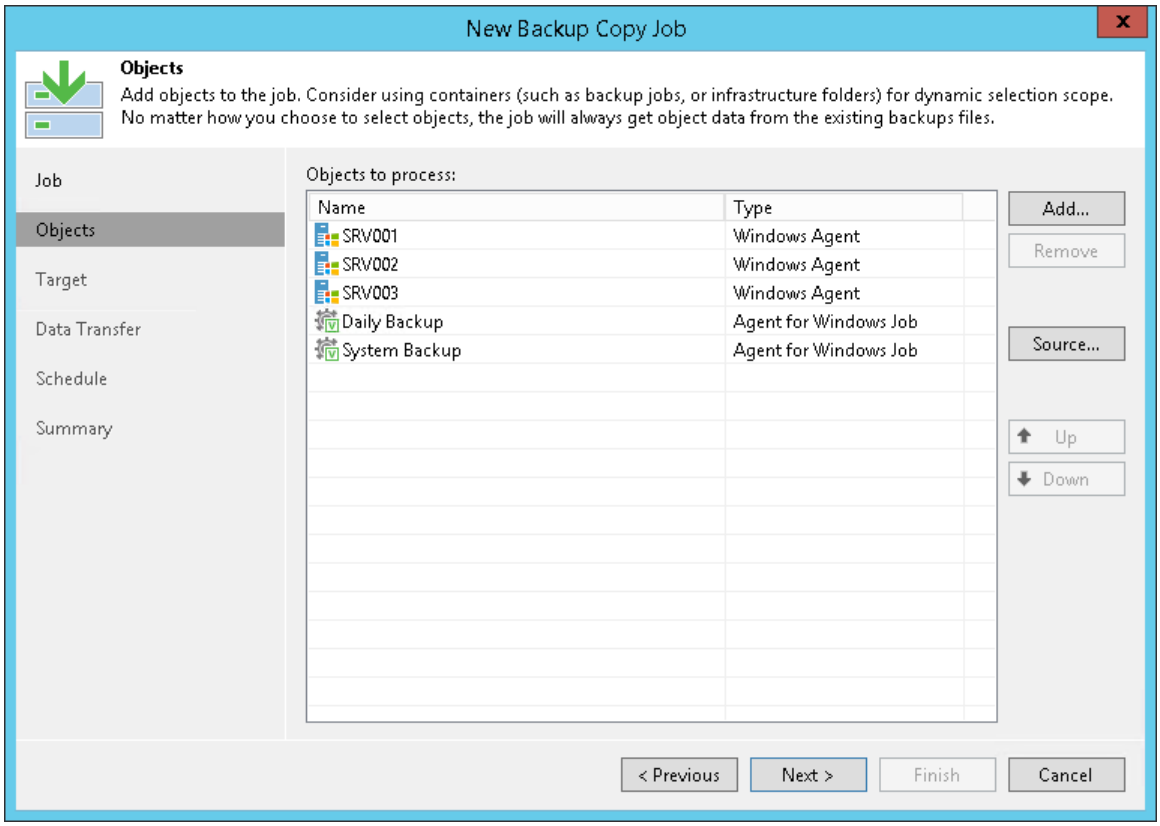
You can configure backup copy jobs that will copy backups created with Veeam Agent for Microsoft Windows to a secondary backup repository.

Backup copy jobs treat Veeam Agent backups as usual backup files. The backup copy job setup and processing procedures practically do not differ from the same procedures for a backup copy job that processes VM backups. To learn more about backup copy jobs, see the Backup Copy section in the Veeam Backup & Replication User Guide.

Mind the following:

- You can process backups created by Veeam Agent only with backup copy jobs for Microsoft Windows computer backups. You cannot add a Veeam Agent backup as an additional source of a backup copy job that processes VM backups.
- You can process backups created by Veeam Agent operating in the standalone mode only with backup copy jobs operating in the periodic copy mode. Immediate copy mode is not supported.
- You can process backups created by Veeam Agent operating in the managed mode with backup copy jobs operating in the periodic and immediate copy modes.

  Mind that for immediate copy mode, only Veeam Agent backups created by jobs managed by the backup server are supported.
- When mapping a backup copy job to a Veeam Agent backup, consider the limitations listed in the Backup File Mapping section in the Veeam Backup & Replication User Guide.



Restoring Data from Copies of Veeam Agent Backups

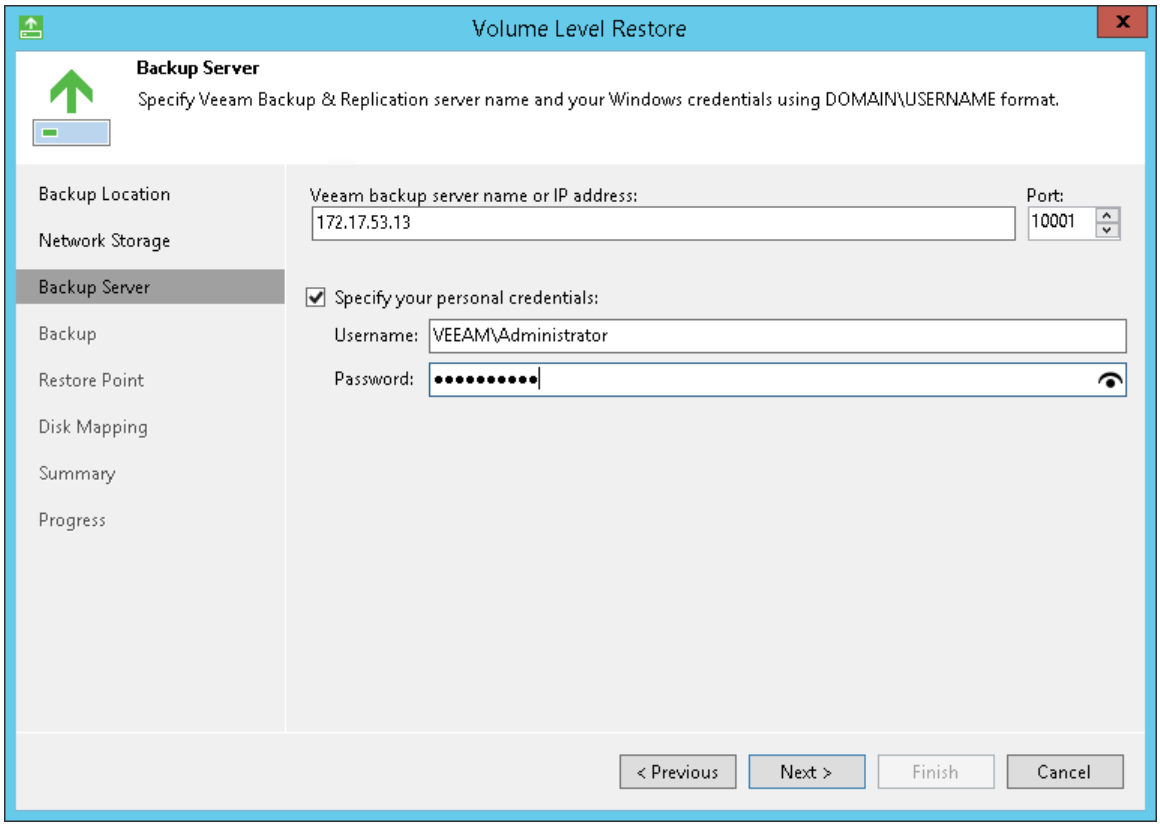
Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

To overcome this limitation, you can delegate the restore task to backup administrators who work with Veeam Backup & Replication. Backup administrators can use Veeam Backup & Replication options to recover data from such backups: for example, perform file-level restore or retrieve necessary application items with Veeam Explorers.

You can also restore data from the copied backup stored on the target repository using Veeam Agent for Microsoft Windows.

To do this:

1. In Veeam Agent for Microsoft Windows, launch the **Volume Level Restore** wizard to restore volumes or **File Level Restore** wizard to restore files and folders. You can also boot from the Veeam Recovery Media and launch the **Veeam Recovery Media** wizard for data restore.
2. At the **Backup Location** step of the wizard, select **Network storage**.
3. At the **Network Storage** step of the wizard, select to restore data from the backup repository.
4. At the **Backup Server** wizard, specify settings for the Veeam backup server that manages the target backup repository where the copied backup is located.
5. Select the **Specify your personal credentials** check box and provide credentials for the user who has the *Veeam Backup Administrator* or *Veeam Restore Operator* role on the Veeam backup server.
6. Pass through the next steps of the wizard and select a backup and restore point from which you want to restore data.

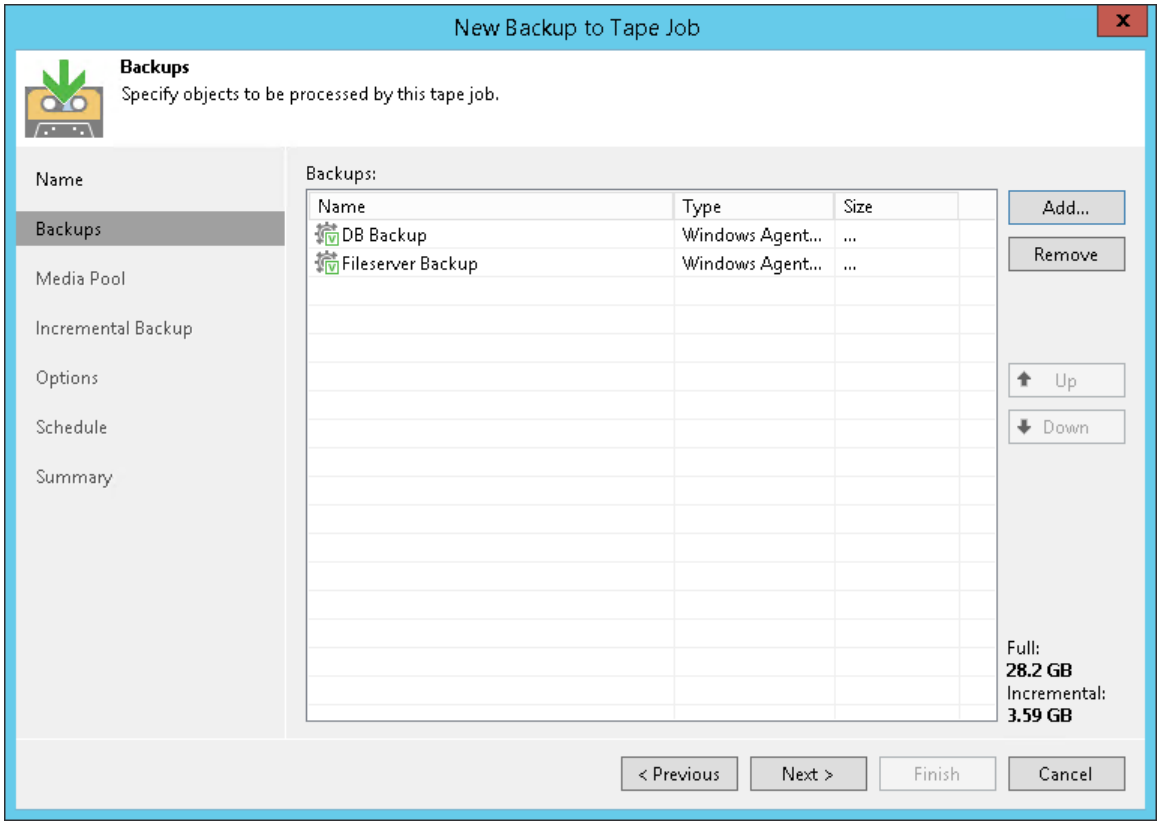


Archiving Veeam Agent Backups to Tape

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

Backup to tape jobs treat Veeam Agent backups as usual backup files. The archiving job setup and processing procedures practically do not differ from the regular ones. To learn more about backup to tape jobs, see Veeam Backup & Replication Documentation.

> **NOTE**
>
> Note that in backup to tape job schedule, you cannot select the **After this job** option for a Veeam Agent job that was configured directly on a Veeam Agent computer.



Performing Restore Tasks

You can perform the following restore operations:

- Restore Veeam Agent backups to Hyper-V VMs
- Restore Veeam Agent backups to VMware vSphere VMs
- Restore volumes from Veeam Agent backups
- Restore individual files and folders from Veeam Agent backups
- Restore application items from Veeam Agent backups with Veeam Explorers
- Export computer disks as VMDK, VHD or VHDX disks
- Restore data from Veeam Agent backups to Microsoft Azure
- Restore data from Veeam Agent backups to Amazon EC2
- Export restore points of Veeam Agent backups to standalone full backup files

Restoring Veeam Agent Backup to Hyper-V VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For Instant Recovery to a Hyper-V VM, you can use Veeam Agent backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

A restored Hyper-V VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

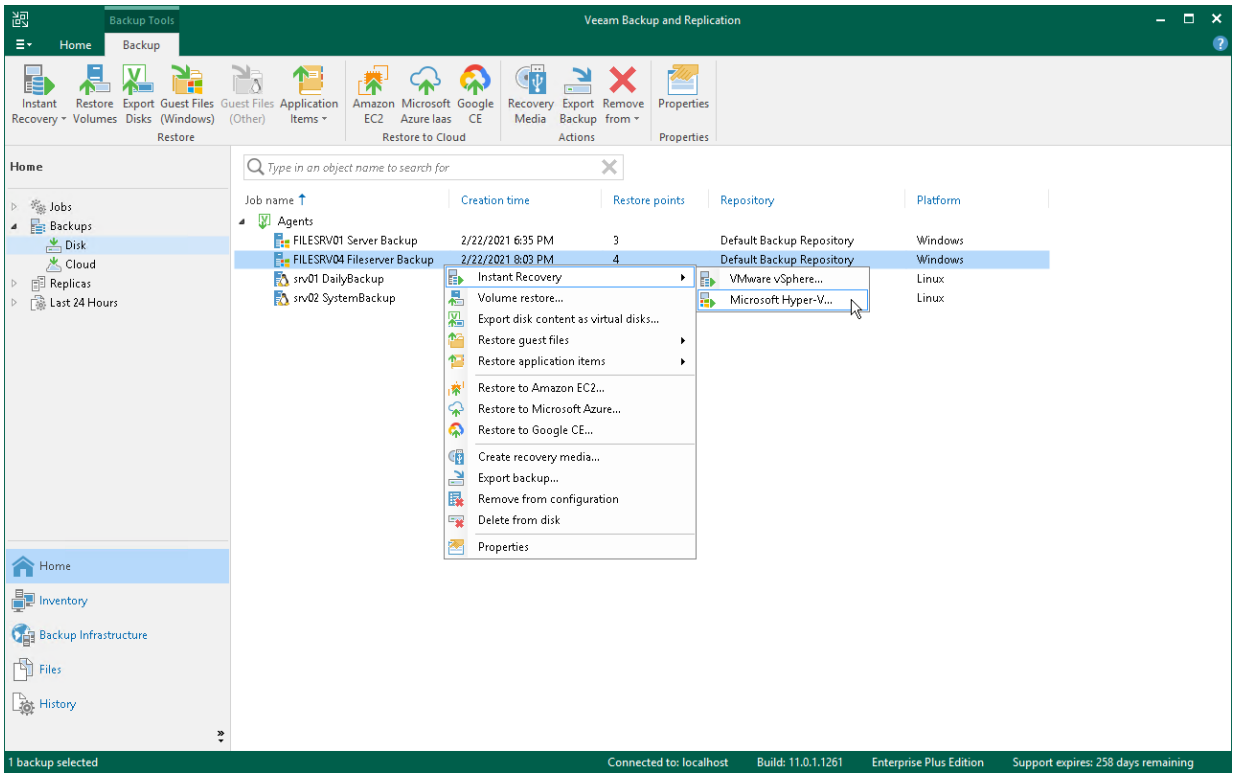
- Amount of RAM
- Number of CPU cores
- Number of network adapters
- Network adapter settings
- BIOS UUID

  If you do not want to preserve the backed-up machine UUID for a Hyper-V VM, you can create a new UUID during the Instant Recovery configuration process.
- Number of disks and volumes
- Size of volumes

If you restore a Veeam Agent computer to a Hyper-V VM, consider the following:

- You cannot recover an EFI-based Veeam Agent computer that runs Windows 7, Windows Server 2008 or Windows Server 2008 R2 to a Hyper-V VM. These OSes can be restored only to a Generation 1 VM that does not support EFI. To learn more, see this Microsoft article.
- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- Veeam Agent computer disks are recovered as dynamically expanding virtual disks.
- By default, Veeam Backup & Replication automatically powers on a VM after restore. If you do not want to power on a VM after restore, you can change this setting during the Instant Recovery configuration process.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to Hyper-V VMs section in the Veeam Backup & Replication User Guide.



Restoring Veeam Agent Backup to VMware vSphere VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment. For Instant Recovery to a VMware vSphere VM, you can use Veeam Agent backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

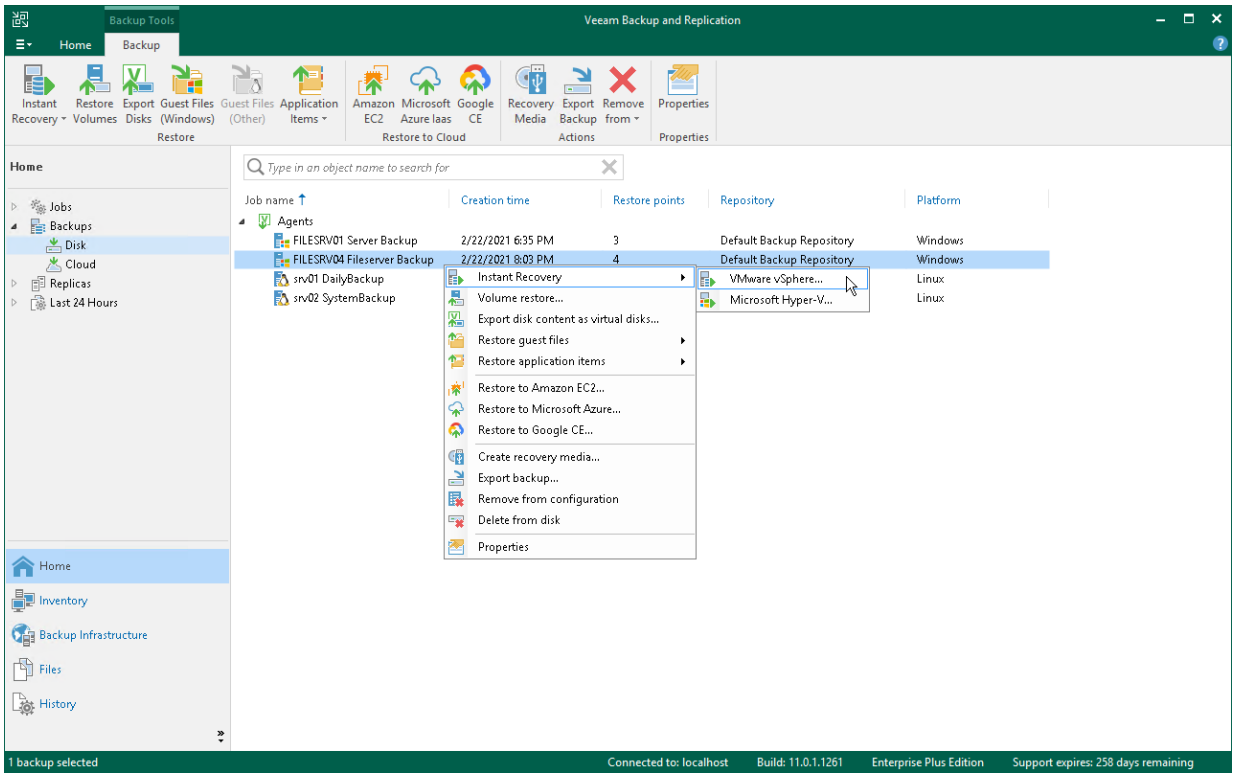
A restored VMware vSphere VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

- Amount of RAM
- Number of CPU cores
- Number of network adapters
- Network adapter settings
- BIOS UUID (If you do not want to preserve the backed-up machine UUID for a VMware vSphere VM, you can create a new UUID during the Instant Recovery configuration process.)
- Number of disks and volumes
- Size of volumes

If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- If you restore a workload to the production network, make sure that the original workload is powered off.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to VMware vSphere VMs section in the Veeam Backup & Replication User Guide.



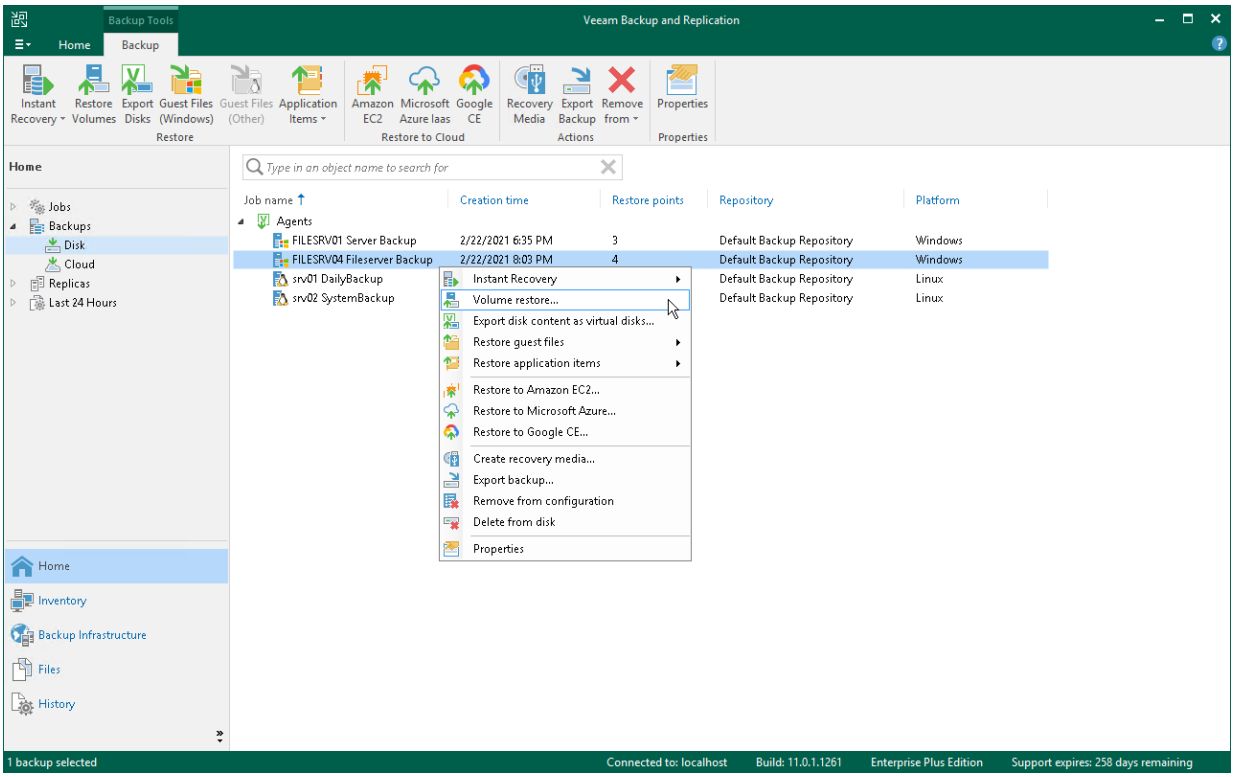
Restoring Volumes

You can use the Veeam Backup & Replication console to restore a specific computer volume or all volumes from a volume-level backup created with Veeam Agent for Microsoft Windows.

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

For volume-level restore, you can use backups that were created in a Veeam backup repository. You cannot restore volumes from a Veeam Agent backup created in a Veeam Cloud Connect repository.

The procedure of volume-level restore from a standalone Veeam Agent backup does not differ from the same procedure for a backup created with Veeam Agent that operates in the managed mode. To learn more, see the Restoring Volumes section in the Veeam Agent Management Guide.



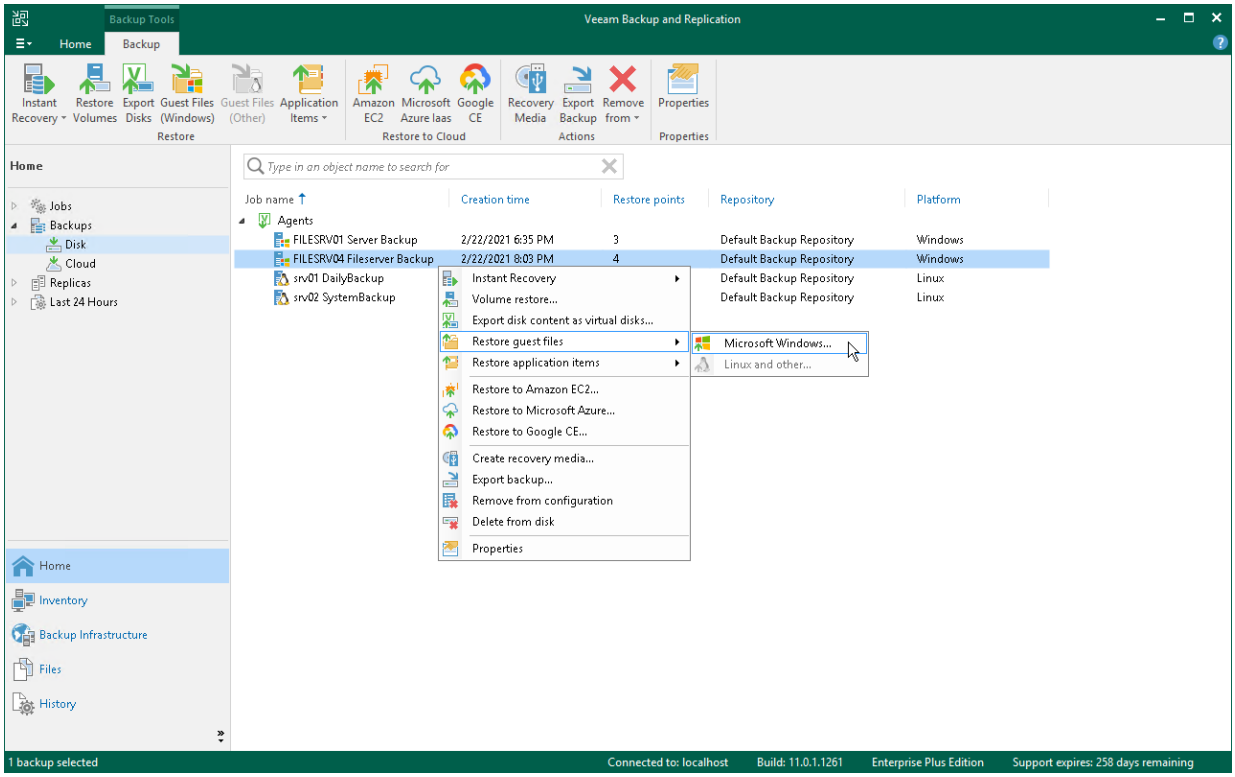
Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups. For file-level restore, you can use Veeam Agent backups created on the following types of target storage:

- Veeam backup repository
- Veeam Cloud Connect repository

For Veeam Agent backups created on the cloud repository, you can perform restore tasks in Veeam Backup & Replication deployed on the tenant backup server. The service provider cannot perform restore tasks with Veeam Agent backups.

The procedure of file-level restore practically does not differ from a regular one. To learn more about file-level restore, see Veeam Backup & Replication Documentation.



Restoring Application Items

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

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

The procedure of application-item restore from Veeam Agent backups differs depending on the type of the backup repository that you use to create Veeam Agent backups.

- For Veeam Agent backups created in a Veeam backup repository, the procedure of application-item restore does not differ from the same procedure for VM backups. To learn more, see the Restoring Application Items section in the Veeam Backup & Replication User Guide.
- For Veeam Agent backups created in a cloud repository, you can perform application-item restore using the backup console on the tenant Veeam Backup & Replication server. To learn more, see Restoring Application Items from Cloud Repository.

Restoring Application Items from Cloud Repository

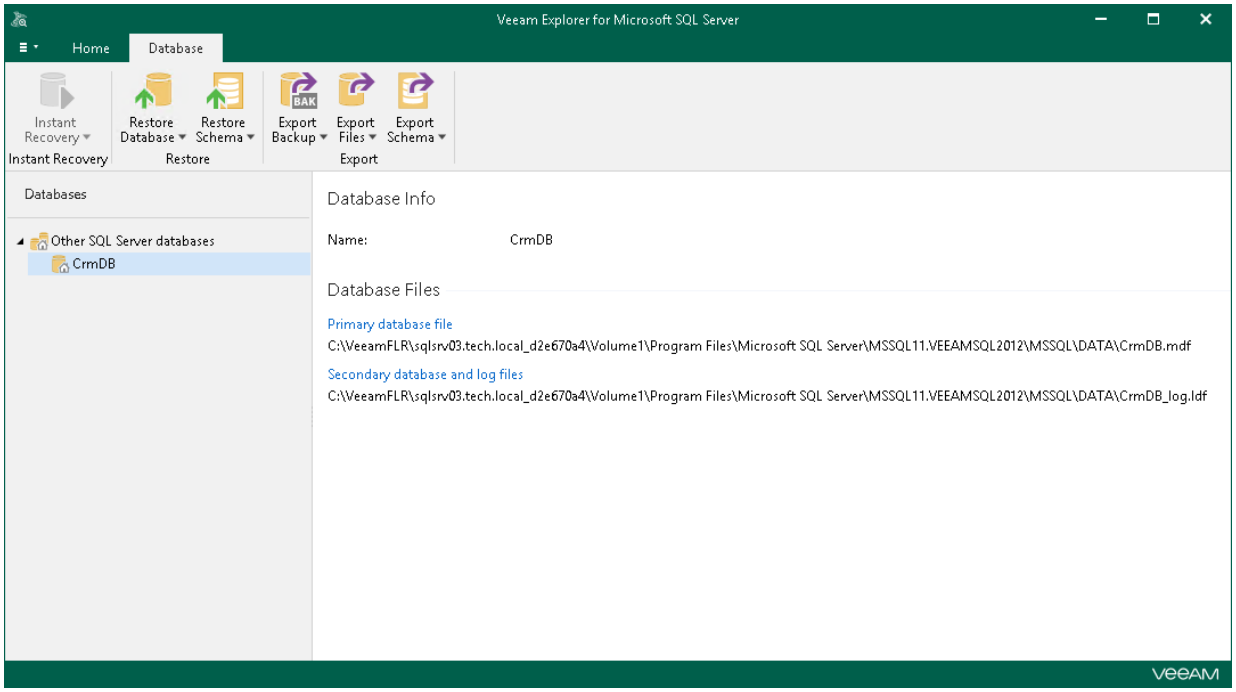
If you use Veeam Agent for Microsoft Windows to create backups in a cloud repository, you can restore data from such backups using the backup console on the tenant Veeam Backup & Replication server.

To restore application items from a cloud repository:

1. In the tenant Veeam Backup & Replication console, locate the necessary Veeam Agent backup.
2. Open the Veeam Backup browser.
3. In the Veeam Backup browser, browse for the database file of the application whose items you want to restore (DIT, EDB, MDF and so on).
4. Double-click the database file to open the corresponding Veeam Explorer.
5. Use the Veeam Explorer to restore application items you need.

NOTE

To learn more about application item restore from a cloud repository, refer to this Veeam KB article.



Exporting Disks

You can restore computer disks from volume-level backups and convert them to disks of the VMDK, VHD or VHDX format.

During disks restore, Veeam Agent for Microsoft Windows creates standard virtual disks that can be used by VMware vSphere and Microsoft Hyper-V VMs.

- When you restore a disk in the VMDK format, Veeam Agent for Microsoft Windows creates a pair of files that make up the VM virtual disk: a descriptor file and file with the virtual disk content.
- When you restore a disk in the VHD/VHDX format, Veeam Agent for Microsoft Windows creates a file of the VHD or VHDX format.

You can save converted disks locally on any server added to the backup infrastructure or place disks on a datastore connected to an ESXi host (for VMDK disk format only). VMDK disks can be restored as thin provision and thick disks:

- Disks restored to a datastore are saved in the thin provisioned format.
- Disks restored to a server are saved in the thick format.

VHD/VHDX disks are always restored as dynamically expanding.

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

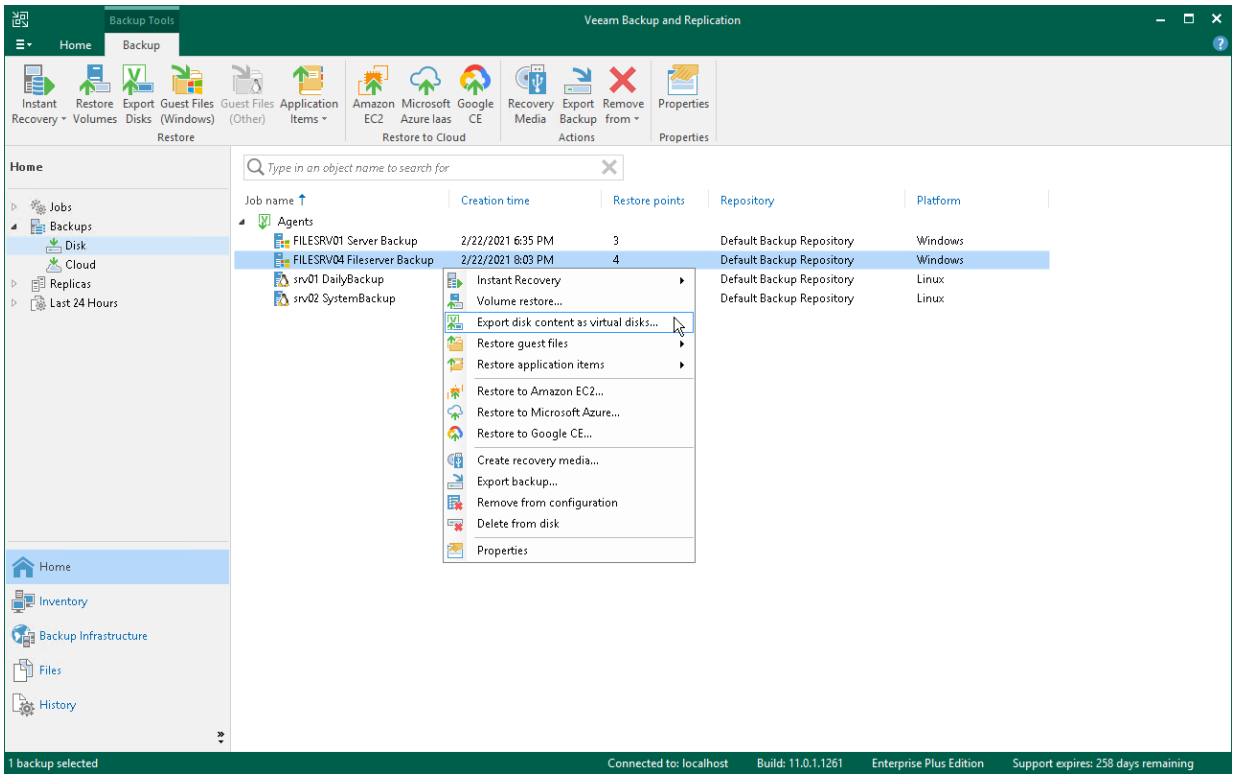
To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

- In Veeam Backup & Replication, open the Home tab and click **Restore** > **Agents** > **Export disk contents as virtual disks**. In this case, you will be able to select the necessary Veeam Agent backup at the Backup step of the wizard.
- In Veeam Backup & Replication, open the **Home** view. Then do the following:
  - [For backups stored on a regular backup repository] In the inventory pane, click **Disk** under the **Backups** node. In the working area, expand the **Agents** node, right-click the necessary backup and select **Export disk content as virtual disks**.
  - [For backups stored on a cloud repository] In the inventory pane, click **Cloud** under the **Backups** node. In the working area, expand the **Agents** node, right-click the necessary backup and select **Export disk content as virtual disks**.

  In this case, you will pass immediately to the Restore Point step of the wizard.

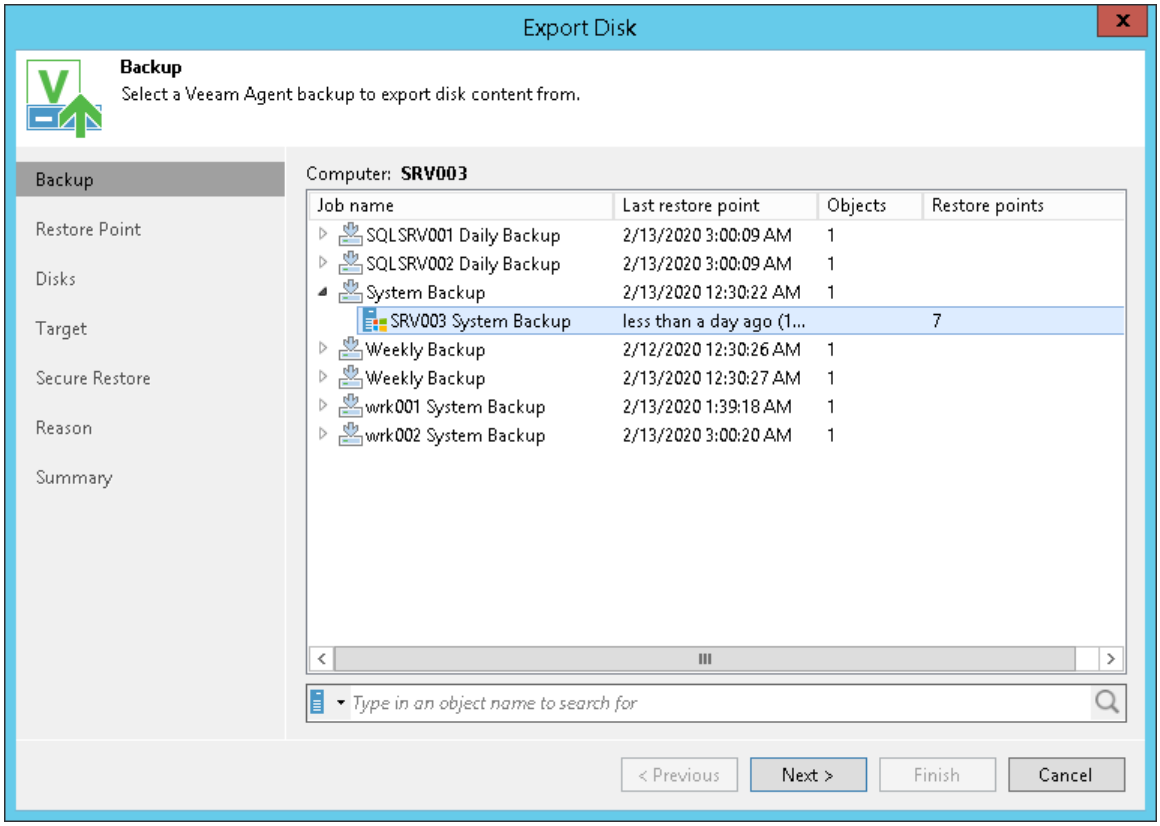


Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to restore disk(s). In the list of backups, Veeam Agent for Microsoft Windows displays all backups that are currently hosted on the on the following types of target storage:

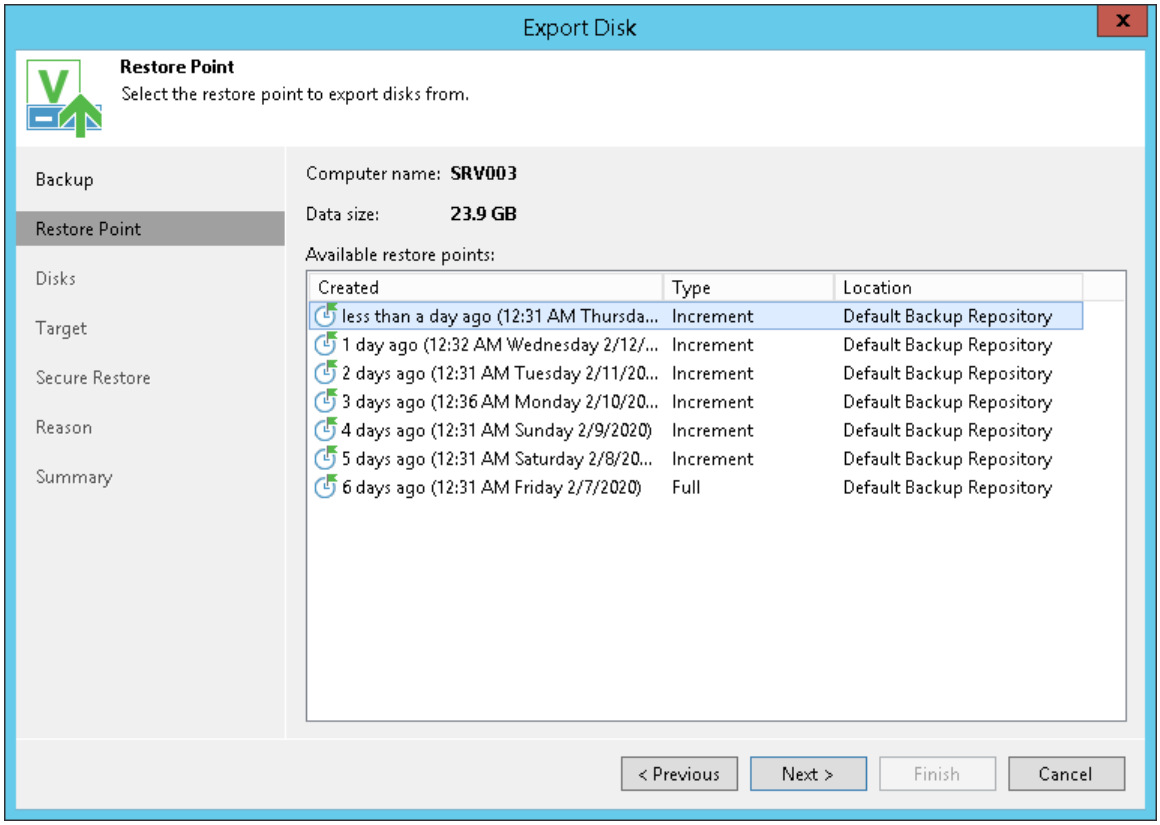
- Veeam backup repository
- Veeam Cloud Connect repository

Make sure that you select a volume-level backup in the list.



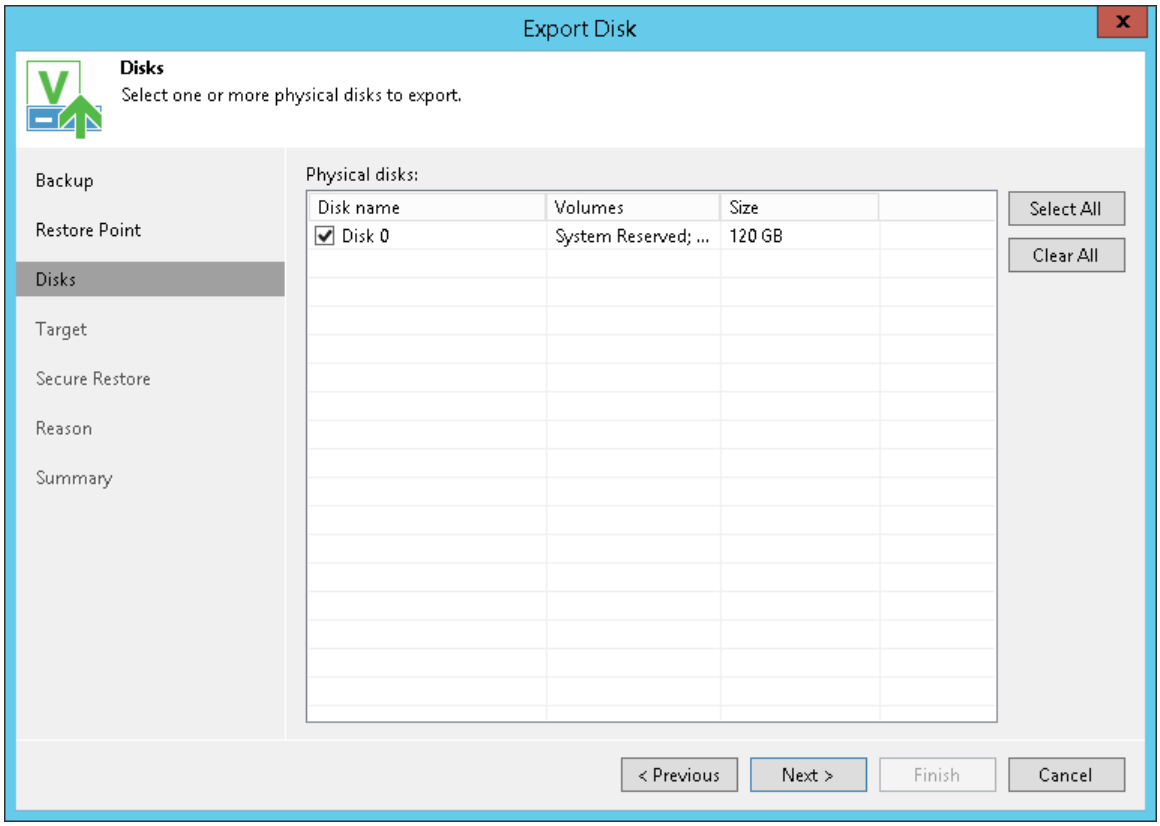
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disk(s). In the list of points, Veeam Agent for Microsoft Windows displays all restore points that have been created. Make sure that you select a restore point that relates to a volume-level backup.



Step 4. Select Disks

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



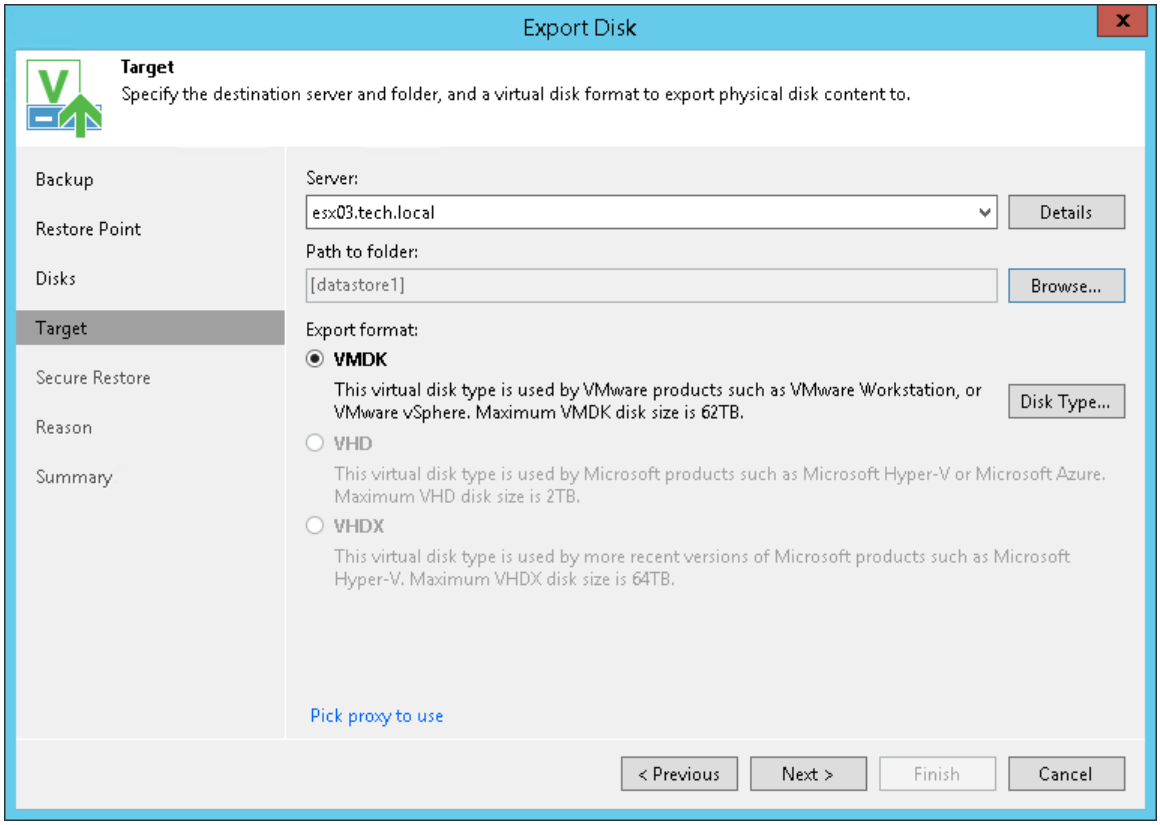
Step 5. Select Destination and Disk Format

At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

1. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.
2. In the **Path** to folder field, specify a folder on the server or datastore where the virtual disks must be placed.
3. Select the export format for disks:
   - **VMDK** — select this option if you want to save the resulting virtual disk in the VMware VMDK format.
   - **VHD** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHD format.
   - **VHDX** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).

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.



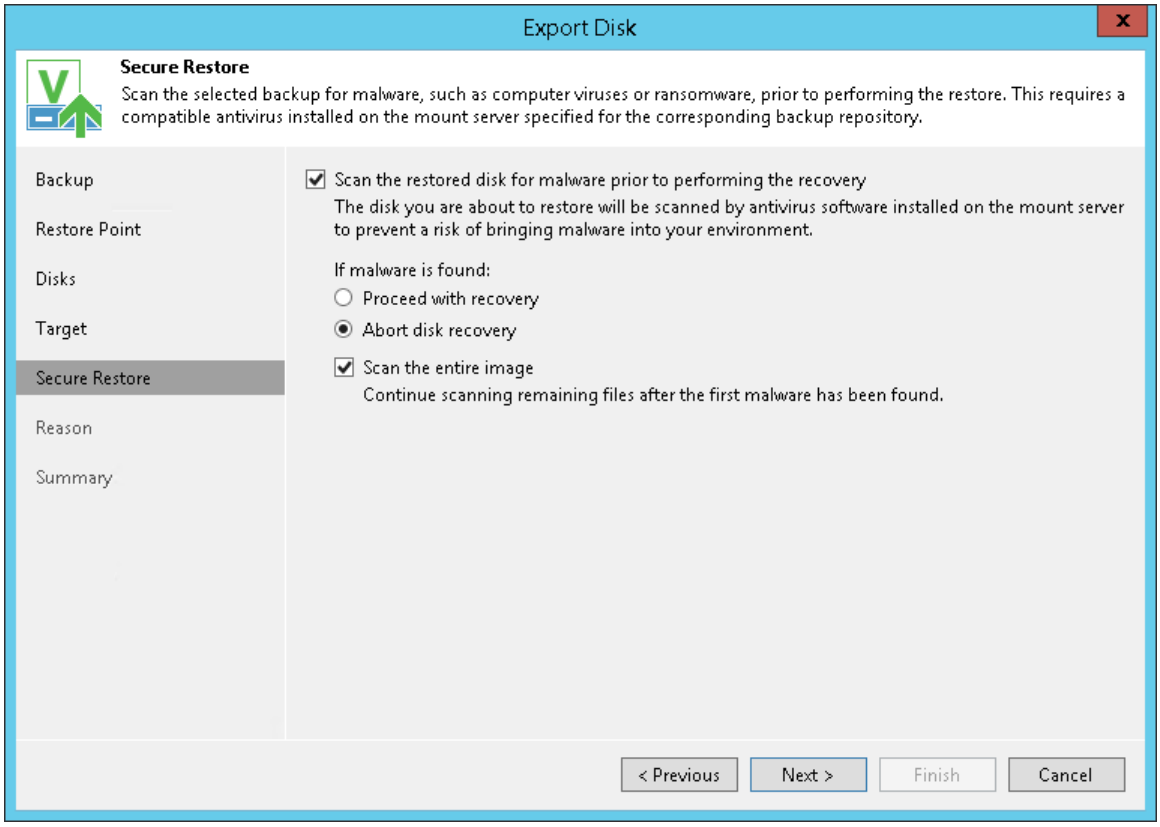
Step 6. Specify Secure Restore Settings

The **Secure Restore** step of the wizard is available if you export disks from a Veeam Agent backup of a Microsoft Windows machine.

At this step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan restored disk data with antivirus software before restoring the disk. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

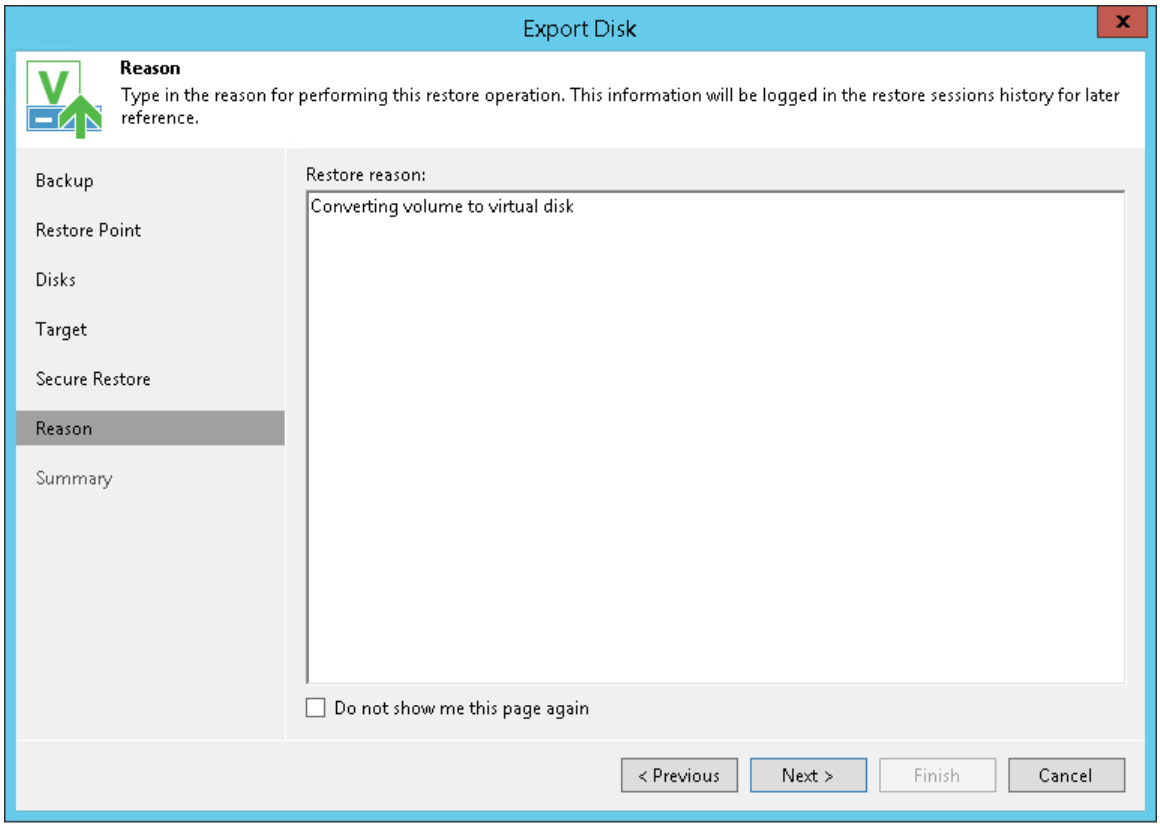
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing recovery** check box.
1. Instruct Veeam Backup & Replication what to perform in case malware is found:
    - Select **Proceed with recovery** if you want to continue the recover process, despite the found malware threat.
    - Select **Abort disk recovery** if you want to stop the recovery process after the first malware threat is found.
2. Select the **Scan the entire image** check box if you want the antivirus software to continue disk scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Antivirus Scan Results section in the Veeam Backup & Replication User Guide.



Step 7. Specify Restore Reason

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

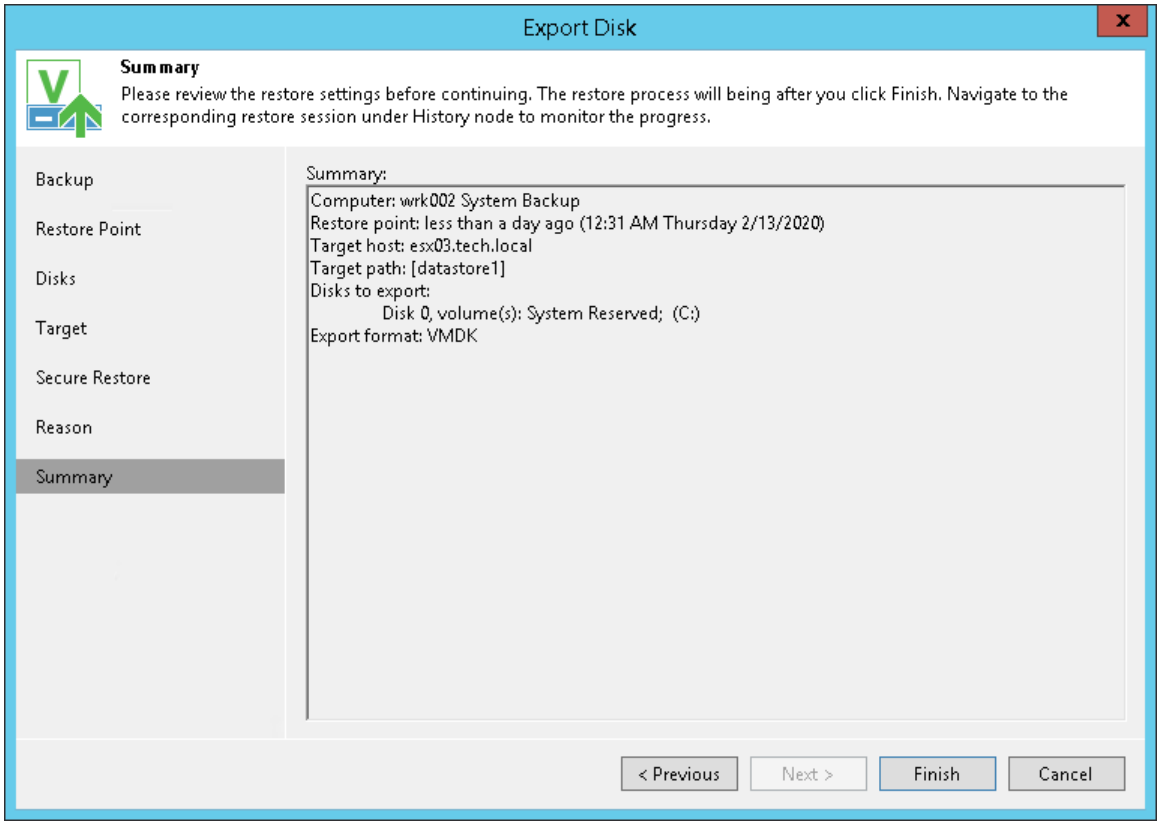
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. Complete Restore Process

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

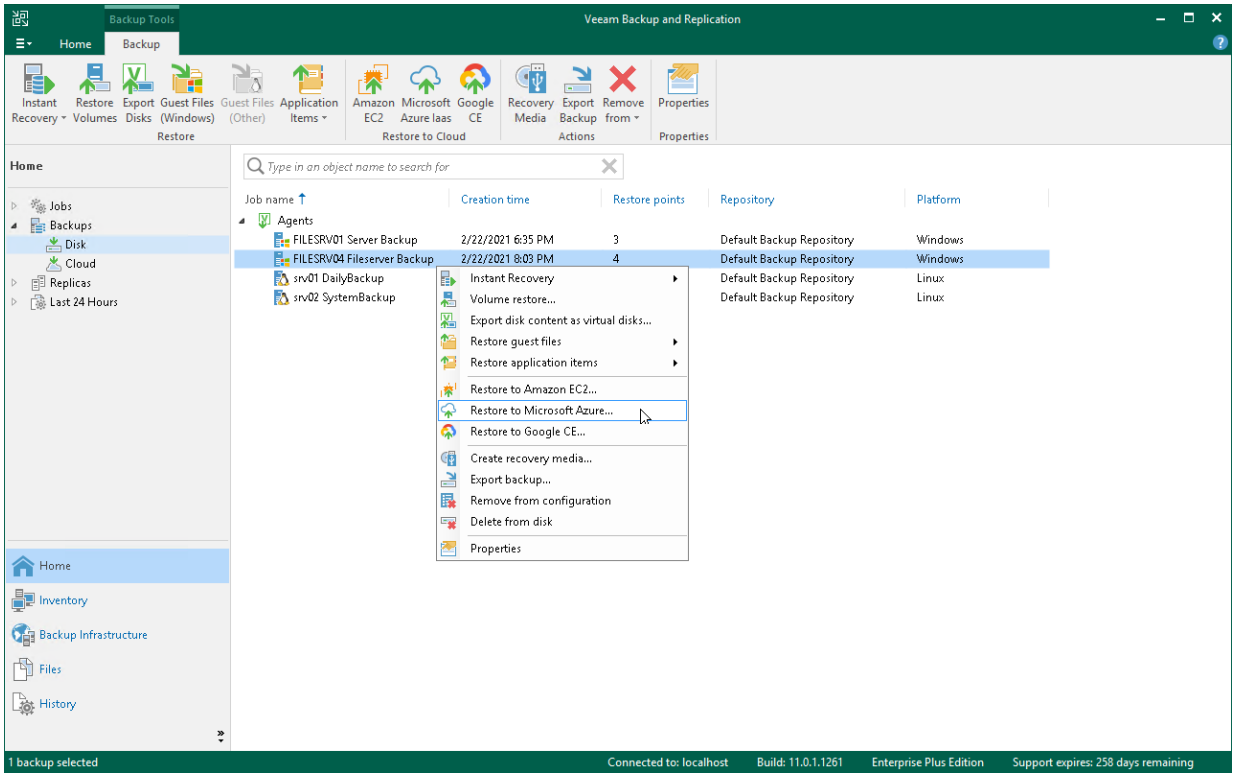
1. Review details for the disk to be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.



Restoring to Microsoft Azure

You can restore machines from backups created with Veeam Agent for Microsoft Windows to Microsoft Azure.

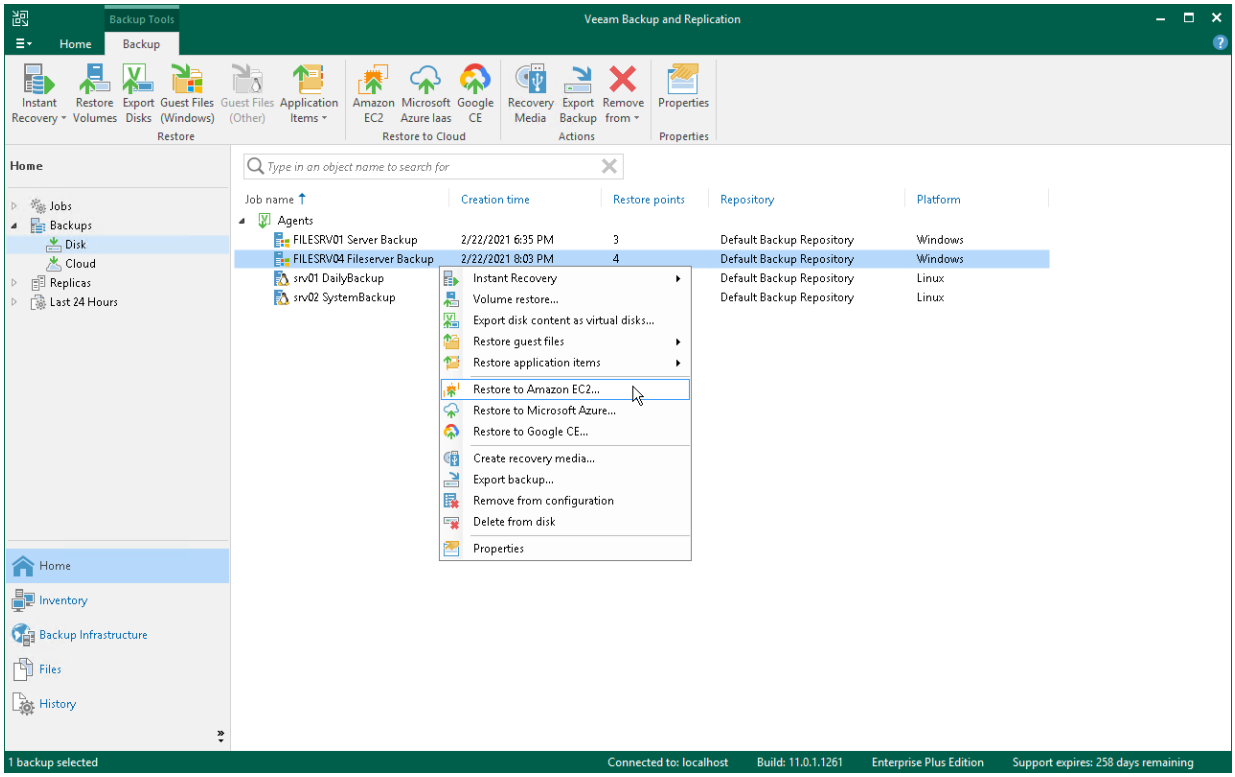
The procedure of restore to Microsoft Azure practically does not differ from a regular one. To learn more about restore to Microsoft Azure, see the Restore to Microsoft Azure section in the Veeam Backup & Replication User Guide.



Restoring to Amazon EC2

You can restore machines from backups created with Veeam Agent for Microsoft Windows to Amazon EC2.

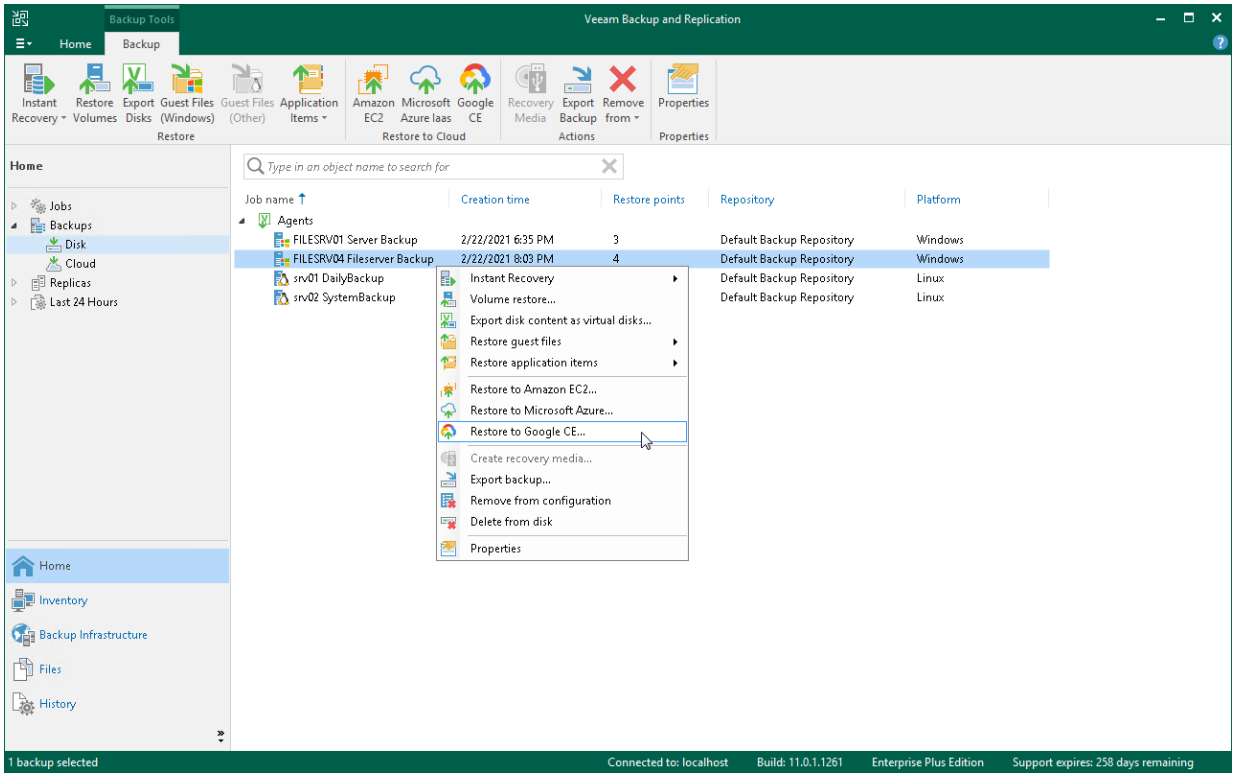
The procedure of restore to Amazon EC2 from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Amazon EC2, see the Restore to Amazon EC2 section in the Veeam Backup & Replication User Guide.



Restoring to Google Cloud Platform

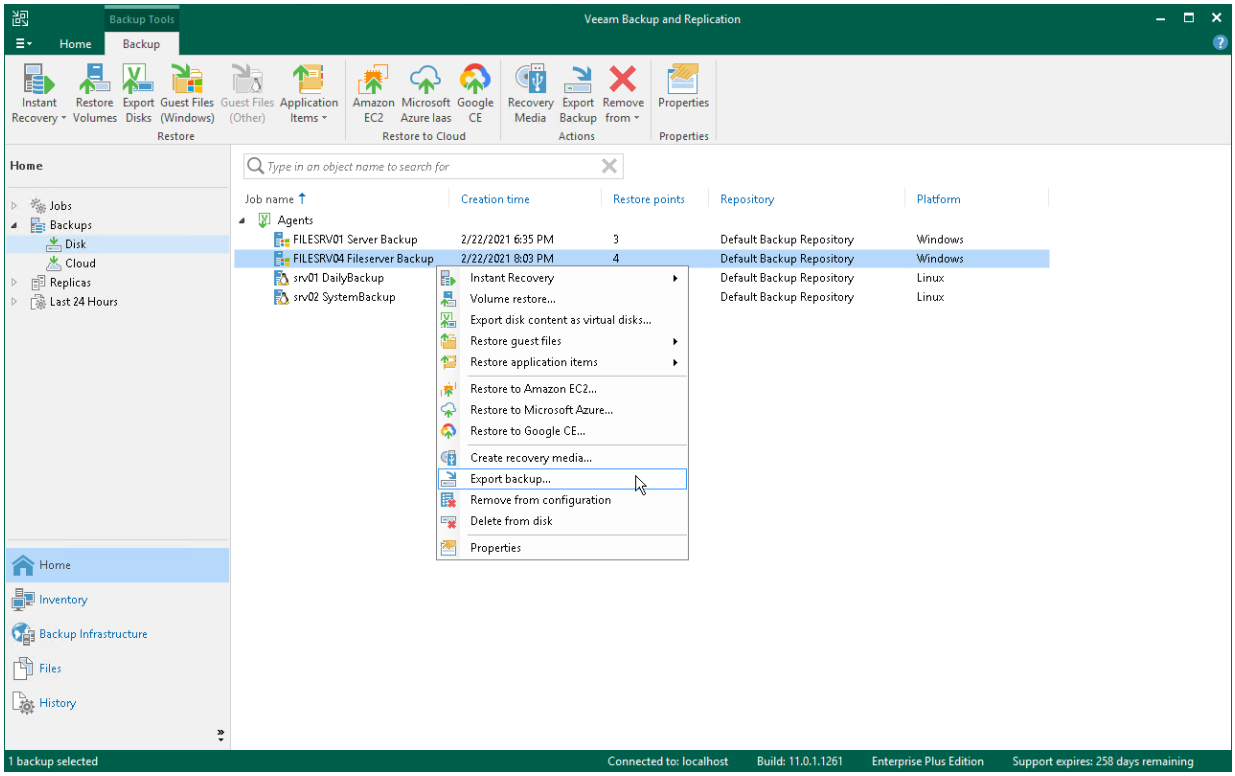
You can restore machines from backups created with Veeam Agent for Microsoft Windows to Google Cloud Platform. Only volume-level backups are supported.

The procedure of restore to Google Cloud Platform practically does not differ from a regular one. To learn more about restore to Google Cloud Platform, see the Restore to Google Cloud Platform section in the Veeam Backup & Replication User Guide.



Exporting Restore Point to Full Backup File

You can restore data from a specific restore point in a Veeam Agent backup and export this data to a standalone full backup file. The procedure of Veeam Agent backup export does not differ from the same procedure for a VM. To learn more, see the Exporting Backups section in the Veeam Backup & Replication User Guide.



Performing Administration Tasks

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

- Import Veeam Agent backups
- Enable and disable Veeam Agent backup jobs
- Delete Veeam Agent backup jobs
- View Veeam Agent backup job statistics
- Remove Veeam Agent backups
- View Veeam Agent backup properties
- Configure global settings
- Assign roles to users

Importing Veeam Agent Backups

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

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

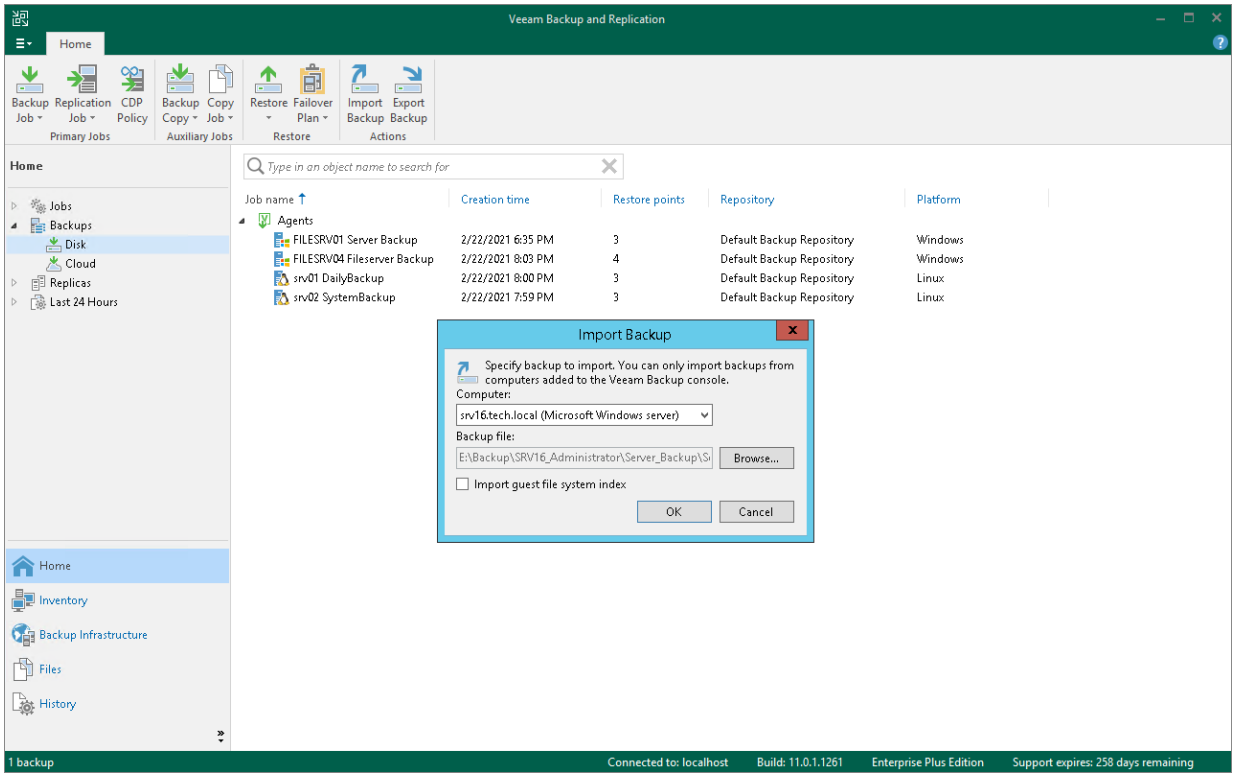
After importing, the Veeam Agent backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

Before importing a backup, check the following prerequisites:

- The computer or server from which you plan to import the backup must be added to Veeam Backup & Replication. Otherwise you will not be able to access backup files.
- To be able to restore data from previous backup restore points, make sure that you have all incremental restore points in the same folder where the full backup file resides.

To import a Veeam Agent backup:

1. In Veeam Backup & Replication, click **Import Backup** on the **Home** tab.
2. From the **Computer** list, select the computer or server on which the backup you want to import is stored.
3. Click **Browse** and select the necessary VBM or VBK file. If you select the VBM file, the import process will be notably faster. We recommend that you use the VBK files for import only if a corresponding VBM file is not available.
4. Click **OK**. The imported backup will become available in the **Home** view, under the **Backups** > **Disk (imported)** node in the inventory pane.



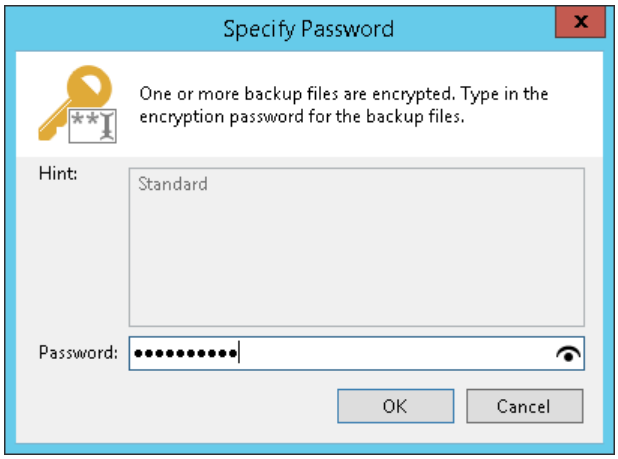
Importing Encrypted Backups

You can import Veeam Agent backups that were encrypted by Veeam Backup & Replication or Veeam Agent for Microsoft Windows.

To import an encrypted backup file:

1. On the **Home** tab, click **Import Backup**.
2. From the **Computer** list, select the host on which the backup you want to import is stored.
3. Click **Browse** and select the VBM or VBK file.
4. Click **OK**. The encrypted backup will appear under the **Backups** > **Disk (encrypted)** node in the inventory pane.
5. In the working area, select the imported backup and click **Specify Password** on the ribbon, or right-click the backup and select **Specify password**.
6. In the **Password** field, enter the password for the backup file. If you changed the password one or several times while the backup chain was created, you need to specify the latest password. For Veeam Agent backups, you can use the latest password to restore data form all restore points in the backup chain, including those restore points that were encrypted with an old password.

If you enter correct password, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups** > **Disk (imported)** node in the inventory pane.



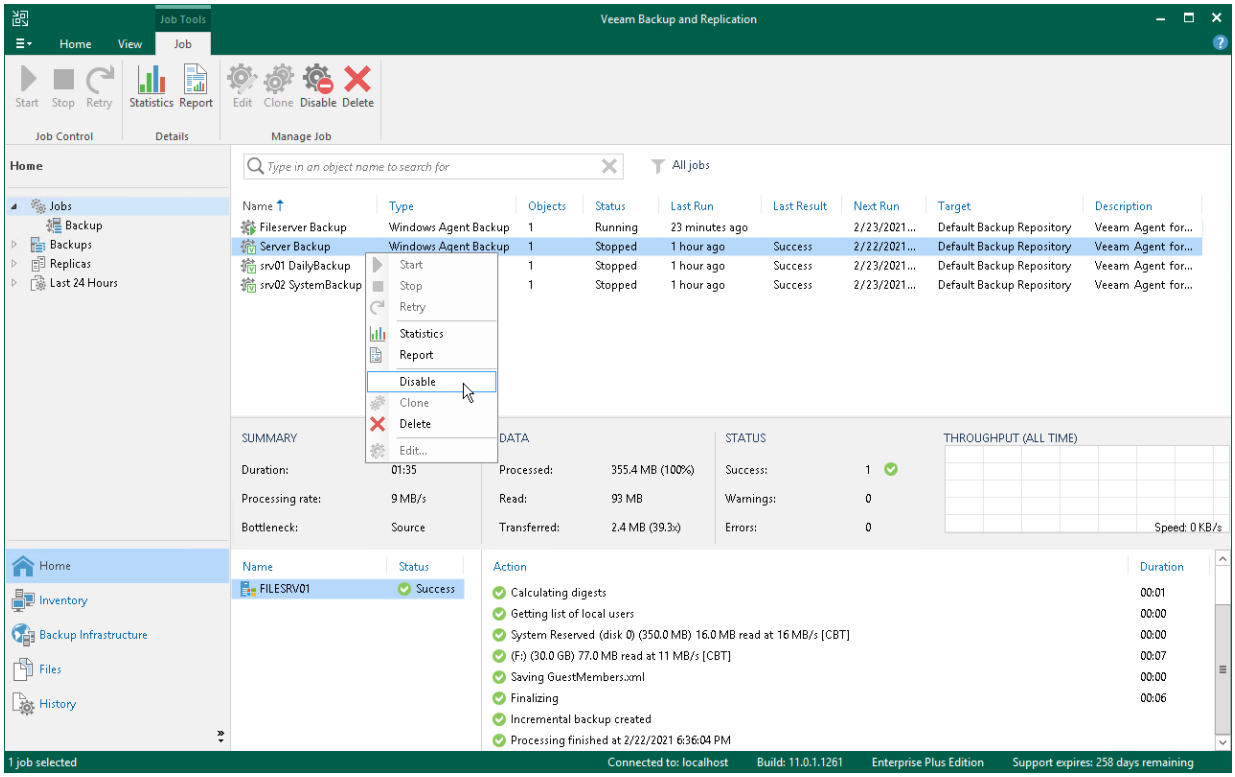
Enabling and Disabling Veeam Agent Backup Jobs

You can disable and enable Veeam Agent jobs in Veeam Backup & Replication.

When you disable the job, you prohibit the user to store the resulting backup to the backup repository. If the user starts a disabled job manually or the job starts by schedule, the job session will fail and report the "*The job has been disabled by the Veeam Backup & Replication administrator*" error. To let Veeam Agent for Microsoft Windows store backups to the backup repository again, you must enable the disabled job.

To disable or enable the scheduled backup job in Veeam Backup & Replication:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. Select the necessary job in the working area and click **Disable** on the ribbon, or right-click the necessary job in the working area and select **Disable**. To enable the disabled job, click **Disable** on the toolbar, or right-click the job and select **Disable** once again.



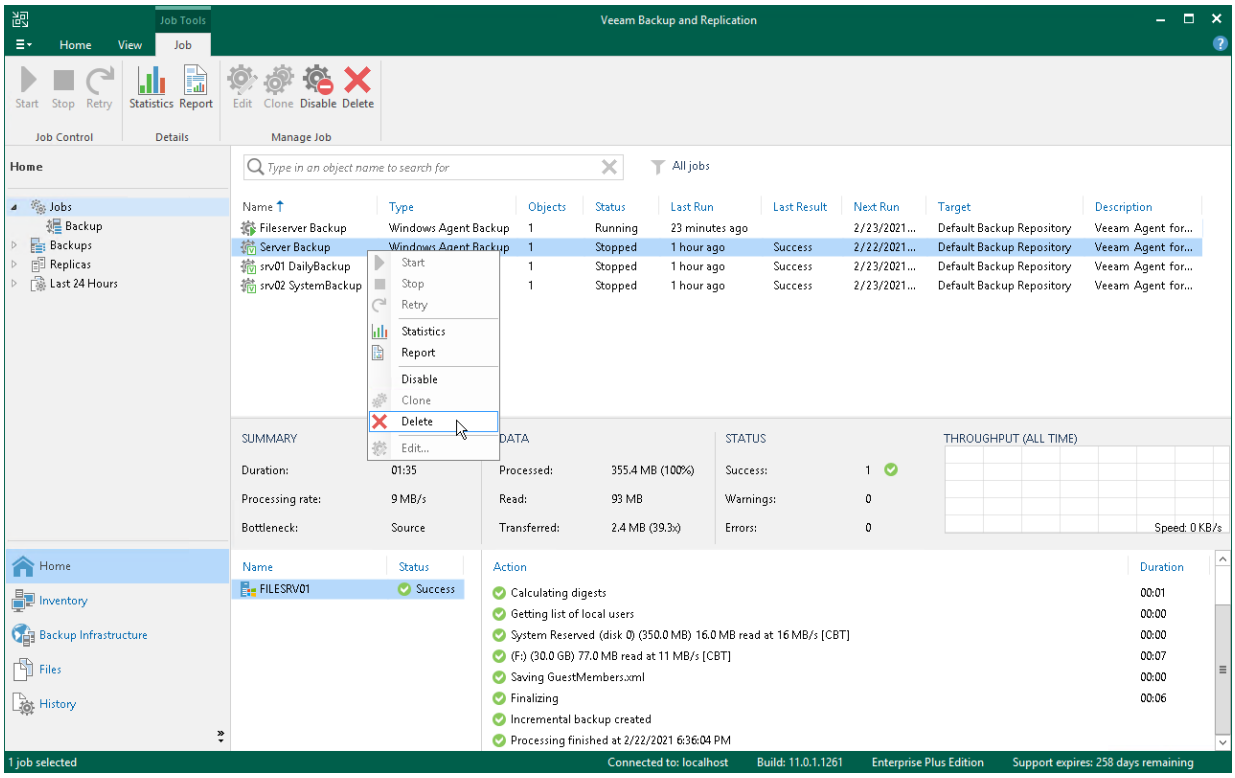
Deleting Veeam Agent Backup Jobs

You can delete Veeam Agent backup jobs.

When you delete a Veeam Agent backup job, Veeam Backup & Replication removes all records about the job from its database and console. When the user starts a new Veeam Agent backup job session manually or the job starts automatically by schedule, the job will appear in the Veeam Backup & Replication console again, and records about a new job session will be stored to the Veeam Backup & Replication database. To remove the job permanently, you must delete the job and unassign access rights permissions for this user from the backup repository.

To remove a job:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. Select the necessary job in the working area and click **Delete** on the ribbon, or right-click the necessary job in the working area and select **Delete**.

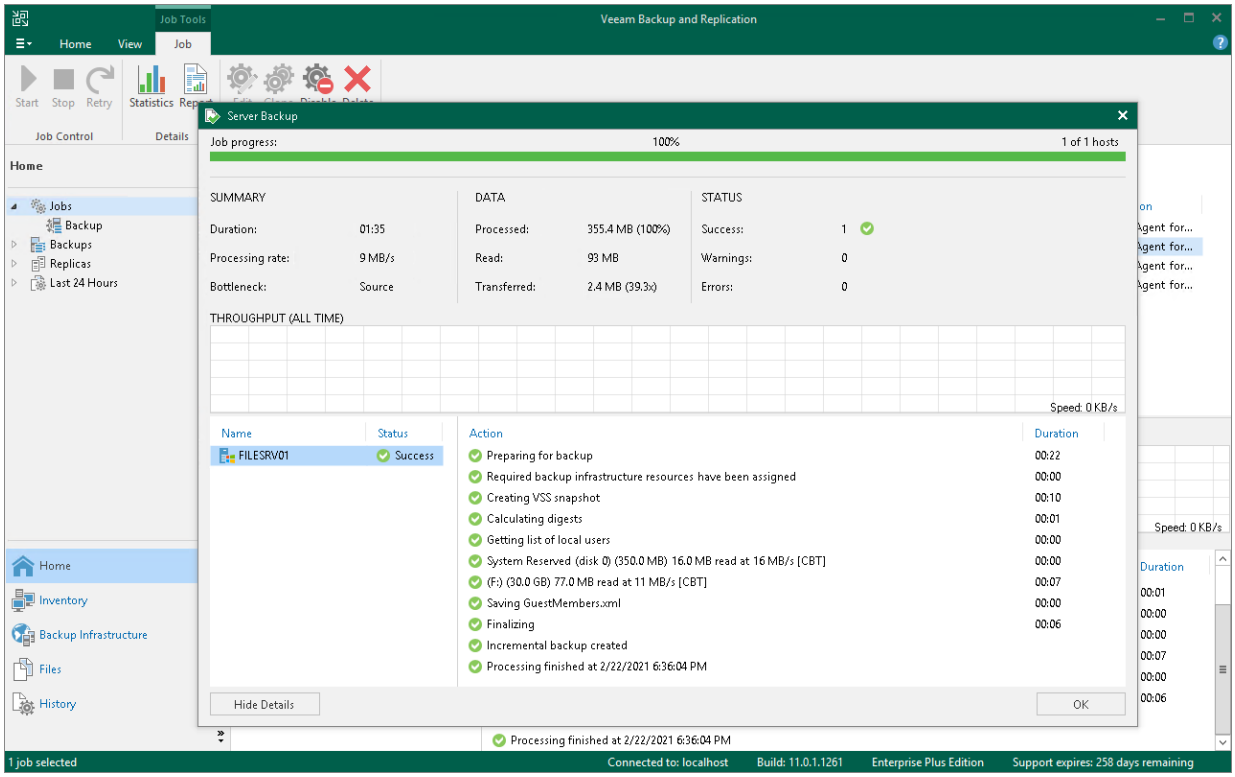


Viewing Veeam Agent Backup Job Statistics

You can view statistics about Veeam Agent backup jobs in the Veeam Backup & Replication console. Veeam Backup & Replication displays statistics for Veeam Agent backup jobs in the similar way as for regular backup jobs. The difference is that the list of objects included in the job contains a Veeam Agent machine instead of one or several VMs.

To view Veeam Agent backup job statistics:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary Veeam Agent backup job and click **Statistics** on the ribbon, or right-click the job and select **Statistics**.



Removing Veeam Agent Backups

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

Removing from Configuration

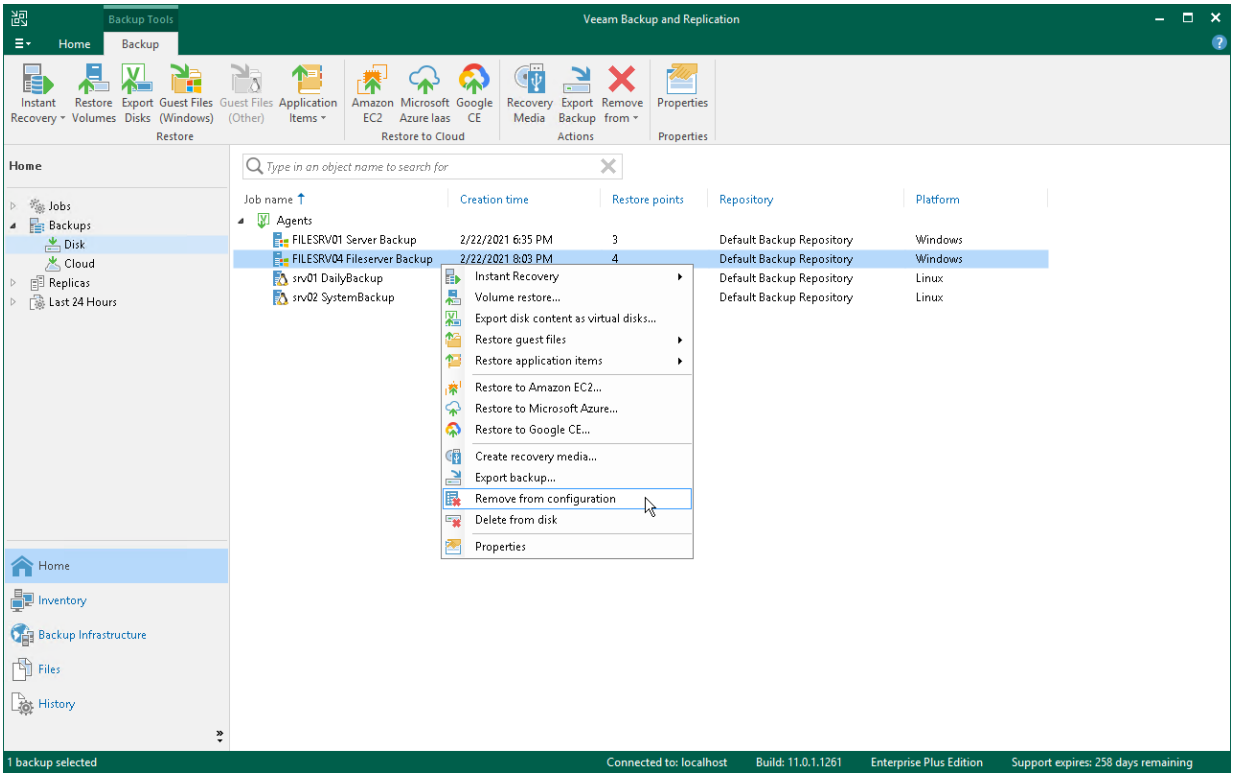
When you remove a Veeam Agent backup from configuration, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it. To learn more, see Importing Veeam Agent Backups.

To remove a Veeam Agent backup from configuration:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click **Disk** under the **Backups** node.
3. In the working area, expand the **Agents** node, select the necessary backup and click **Remove from > Configuration** on the ribbon, or right-click the backup and select **Remove from configuration.**

IMPORTANT

You should not remove a Veeam Agent backup from configuration if Veeam Agent for Microsoft Windows is set up to use the backup cache and the backup cache contains one or several restore points that are not uploaded to the target location yet. If you remove such backup and then import it in the Veeam Backup & Replication console, the backup will receive the new ID in the configuration database. As a result, Veeam Agent for Microsoft Windows will become unable to upload restore points from the backup cache to the target location and to create new restore points in the backup cache. To continue creating backups in the Veeam backup repository, you will need to delete restore points from the backup cache and run the backup job to create a new restore point in the backup repository.

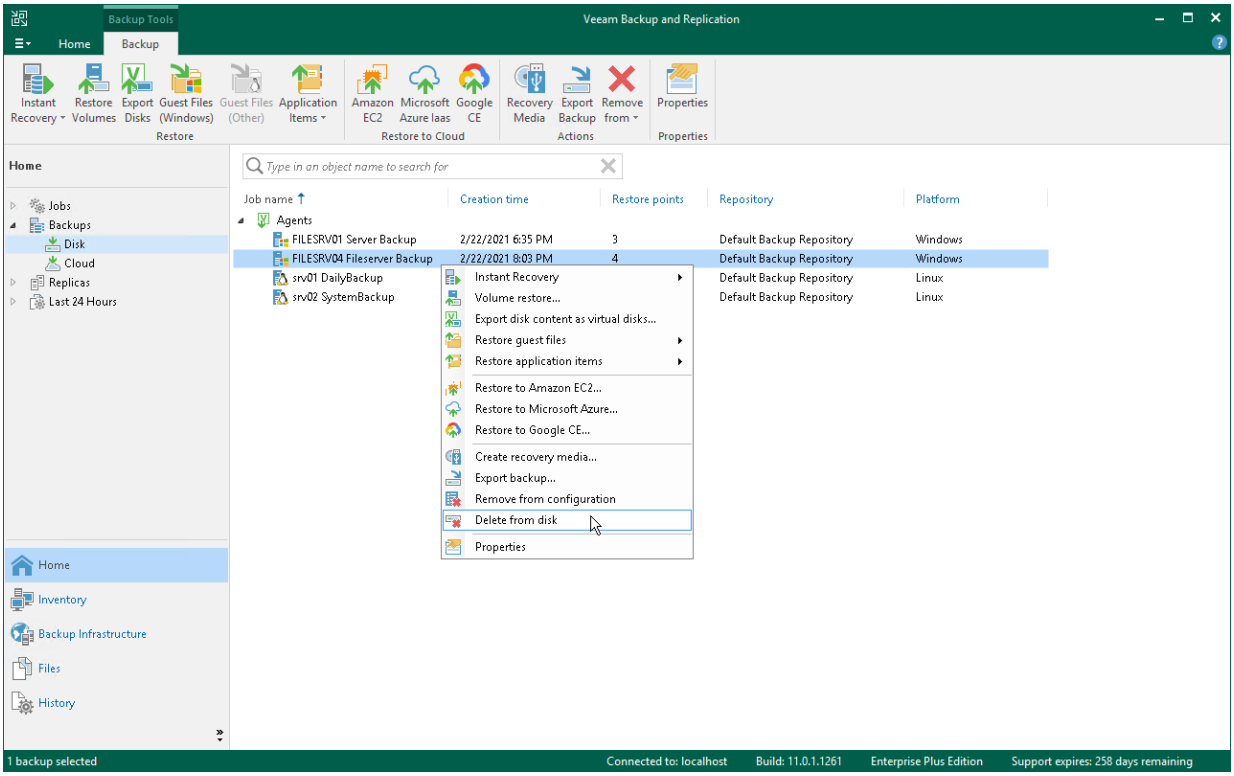


Removing from Backup Repository

When you remove a Veeam Agent backup from backup repository, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files are removed from the backup repository, too.

To remove a Veeam Agent backup from the backup repository:

1. In Veeam Backup & Replication, open the **Backup & Replication** view.
2. In the inventory pane, click **Disk** under the **Backups** node.
3. In the working area, expand the **Agents** node, select the necessary backup and click **Remove from > Disk** on the toolbar, or right-click the backup and select **Delete from disk.**

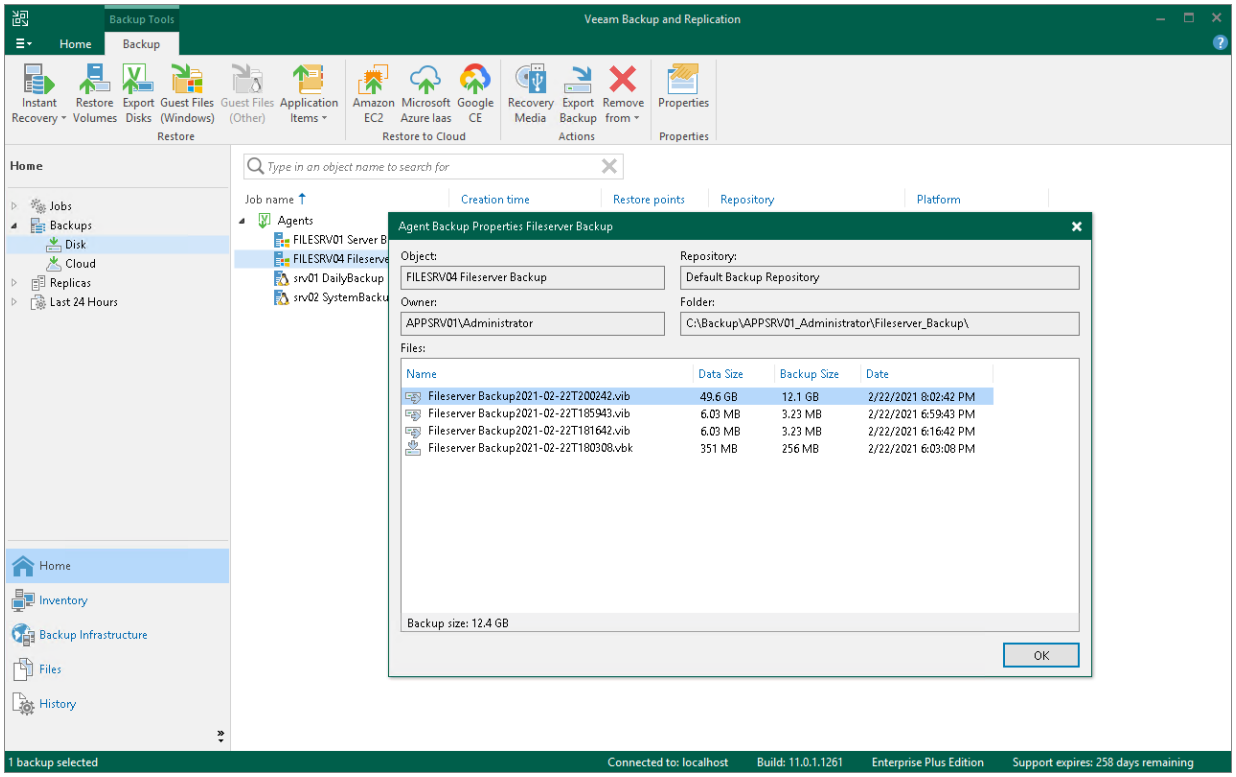


Viewing Veeam Agent Backup Properties

You can view statistics about Veeam Agent backups.

To view Veeam Agent backup statistics:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click **Disk** under the **Backups** node.
3. In the working area, expand the **Agents** node, select the necessary backup and click **Properties** on the ribbon, or right-click the backup and select **Properties**.



Configuring Global Settings

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

- Configure network throttling settings so that Veeam Agent backup job does not consume all network resources.
- Configure global email settings to get alerted about the Veeam Agent backup job results. Veeam Agent for Microsoft Windows sends email notifications on every type of backup tasks, such as backup job sessions started automatically by schedule, backup job sessions started from the command line and ad-hoc backup tasks.

To learn more, see Veeam Backup & Replication Documentation.

Assigning Roles to Users

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

To learn more, see the Roles and Users section in the Veeam Backup & Replication User Guide.

Automating Veeam Agent for Windows Operations

You can automate Veeam Agent for Microsoft Windows operations with Veeam Agent Configurator.

Veeam Agent Configurator is a tool that provides a command-line interface for Veeam Agent for Microsoft Windows. With Veeam Agent Configurator, you can perform data protection and administrative operations for Veeam Agent for Microsoft Windows from the command line, create custom scripts or integrate Veeam Agent for Microsoft Windows with third-party applications.

Veeam Agent Configurator is available in Workstation and Server editions of Veeam Agent for Microsoft Windows.

Veeam Agent Configurator comes with Veeam Agent for Microsoft Windows. The `Veeam.Agent.Configurator.exe` file is placed in the product folder on the computer protected with Veeam Agent for Microsoft Windows, by default, `C:\Program Files\Veeam\Endpoint Backup`.

For more information, see Veeam Agent Configurator Reference.

Appendix A. Veeam Agent Events

Veeam Agent for Microsoft Windows logs its events to event logs on the computer where the product is installed. Events can be used for monitoring the backup job activity and alerting about the backup status.

The table below lists all events logged by Veeam Agent for Microsoft Windows.

Event ID	Name	Description	Event Log	Source	Severity
110	Backup Job Started	Veeam Agent <jobname> has been started [by user <username>].	Veeam Agent	Veeam Agent	Information
115	Backup Job Resumed	Backup Job <jobname> has been resumed.	Veeam Agent	Veeam Agent	Information
190	Backup Job Finished	Veeam Agent <jobname> finished with <job status>. Job details: <additional information about the job results>[1].	Veeam Agent	Veeam Agent	Information Warning Error
191	Backup Job Retry	Veeam Agent <jobname> finished with Error and will be retried. Job details: <additional information about the job results>[1].	Veeam Agent	Veeam Agent	Warning
195	Synchronization Finished	Synchronization for cached restore points finished with <job status>. <Additional information about synchronized restore points>.	Veeam Agent	Veeam Agent	Information Warning Error
196	Destination Changed	Backup job destination has been switched from <target> to Backup Cache.	Veeam Agent	Veeam Agent	Information
197	Backup Cache Deleted	Backup cache has been deleted by <username>.	Veeam Agent	Veeam Agent	Information

Event ID	Name	Description	Event Log	Source	Severity
1074	Computer shut down[2]	The process C:\Windows\system32\Shutdown.exe (<jobname>) has initiated the shutdown of computer <jobname> on behalf of user NT AUTHORITY\SYSTEM for the following reason: No title for this reason could be found Reason Code: 0x800000ff Shutdown Type: shutdown Comment: Computer was shut down after successful backup by Veeam Agent for Microsoft Windows.	System	User32	Information
4010	License Installed	License key for Veeam Agent for Windows has been installed.	Veeam Agent	Veeam Agent	Information
4020	License Expiring	License key for Veeam Agent is about to expire in <number of days> of Days.	Veeam Agent	Veeam Agent	Warning
4030	License Expired	License key for Veeam Agent has expired.	Veeam Agent	Veeam Agent	Error
4025	License in Grace Period	Your license has expired and needs to be renewed. Veeam Agent will continue to operate for the duration of the grace period.	Veeam Agent	Veeam Agent	Error
4040	License Support Expiring	Support contract for Veeam Agent is about to expire in <number of days> of Days.	Veeam Agent	Veeam Agent	Warning
4050	License Support Expired	Support contract for Veeam Agent has expired. Contact Veeam sales representative to renew your support contract.	Veeam Agent	Veeam Agent	Error
4060	Product Edition Changed	Veeam Agent for Windows edition has been changed from <previousedition> to <currentedition>.	Veeam Agent	Veeam Agent	Information
10010	Restore Point Created	'<computername>' restore point has been created.	Veeam Agent	Veeam Agent	Information

Event ID	Name	Description	Event Log	Source	Severity
10050	Restore Point Removed	Restore point for '<computername>' has been removed according to the configured retention policy.	Veeam Agent	Veeam Agent	Information
23010	Backup Job Created	The <jobname> backup job has been created.	Veeam Agent	Veeam Agent	Information
23050	Backup Job Modified	The <jobname> backup job has been modified.	Veeam Agent	Veeam Agent	Information
23090	Backup Job Deleted	EndpointBackup <jobname> has been deleted.	Veeam Agent	Veeam Agent	Information
23051	Agent Modified	Veeam Agent option <optionname> has been changed.[3]	Veeam Agent	Veeam Agent	Information
23501	Agent Updated	Veeam Agent has been successfully updated.	Veeam Agent	Veeam Agent	Information
		Failed to update Veeam Agent.			Error
23110	Backup Mode Changed	The <jobname> backup mode has been changed from <previousmode> to <currentmode>.	Veeam Agent	Veeam Agent	Information
23120	Backup Source Updated	The <jobname> backup job source objects have been updated.	Veeam Agent	Veeam Agent	Information
26010	USB Device Ejected	Target USB device has been successfully ejected.	Veeam Agent	Veeam Agent	Information
178	Managed mode Enabled	Veeam Agent has been switched to managed mode.[4]	Veeam Agent	Veeam Agent	Information
179	Managed mode Disabled	Veeam Agent has been switched to free mode.[4]	Veeam Agent	Veeam Agent	Information
201	Read-only mode Enabled	Read only UI access has been enabled.[4]	Veeam Agent	Veeam Agent	Information
202	Read-only mode Disabled	Read only UI access has been disabled.[4]	Veeam Agent	Veeam Agent	Information

[1] Job details contain information about the reason for completing the job with the Warning or Error status.

[2] The event is triggered if the user has instructed Veeam Agent for Microsoft Windows to shut down the computer on successful backup.

[3] The event is triggered if the user has changed any Veeam Agent for Microsoft Windows setting other than backup job settings.

[4] The event can be triggered if Veeam Agent for Microsoft Windows is managed by a Remote Monitoring and Management platform, for example, LabTech.

Veeam Backup & Replication

Version 11

Veeam Agent Management Guide

January, 2022

© 2022 Veeam Software.

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

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

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE **8**
ABOUT THIS DOCUMENT **9**
OVERVIEW **10**
Veeam Agent Management Infrastructure 11
Protected Computers Discovery and Veeam Agent Deployment 15
Protection Groups 17
Rescan Job 22
Veeam Agent Backup Jobs and Policies 24
Backup Job 27
Backup Policy 29
Backup of Microsoft Windows Computers 35
Backup Cache 36
Storage Snapshots Support 38
Failover Cluster Support 43
Backup of Linux Computers 49
Backup Job and Snapshot Scripts 50
Backup of Database Systems 52
Backup of Unix Computers 53
Backup Job Scripts 54
Backup of macOS Computers 55
Backup to Veeam Cloud Connect Repository 56
PLANNING AND PREPARATION **58**
Considerations and Limitations 59
System Requirements 60
Licensing Requirements 72
Supported Applications 74
Supported Veeam Agents 77
Used Ports 80
GETTING STARTED **86**
CONFIGURING SECURITY SETTINGS **87**
Managing TLS Certificates 89
Generating Self-Signed Certificates 90
Importing Certificates from Certificate Store 93
Importing Certificates from PFX Files 95
Using Certificate Signed by Internal CA 97
Adding Computers to Trusted Hosts List 101

WORKING WITH PROTECTION GROUPS 103
Creating Protection Groups 104
Before You Begin 105
Step 1. Launch New Protection Group Wizard 107
Step 2. Specify Protection Group Name and Description 108
Step 3. Select Protection Group Type 109
Step 4. Specify Protection Scope 111
Step 5. Exclude Objects from Protection Group 119
Step 6. Specify Credentials 120
Step 7. Specify Discovery and Deployment Options 122
Step 8. Specify Advanced Protection Group Settings 124
Step 9. Review Components 129
Step 10. Assess Results 130
Step 11. Finish Working with Wizard 131
Deploying Veeam Agents Using Generated Setup Files 132
Deploying Veeam Agent for Microsoft Windows 133
Deploying Veeam Agent for Linux 137
Deploying Veeam Agent for Unix 139
Deploying Veeam Agent for Mac 141
Adding Protection Group to Backup Job 143
Editing Protection Group Settings 145
Rescanning Protection Group 146
Assigning Location to Protection Group 147
Disabling Protection Group 148
Removing Protection Group 150
WORKING WITH VEEAM AGENT BACKUP JOBS AND POLICIES 152
Creating Veeam Agent Backup Jobs 153
Creating Job for Windows Computers 154
Creating Job for Linux Computers 217
Creating Veeam Agent Backup Policies 274
Creating Policy for Windows Computers 275
Creating Policy for Linux Computers 276
Creating Policy for Unix Computers 277
Creating Policy for Mac Computers 306
Managing Veeam Agent Backup Jobs 337
Starting and Stopping Veeam Agent Backup Job 338
Retrying Veeam Agent Backup Job 340
Performing Active Full Backup 341
Editing Veeam Agent Backup Job Settings 342

Enabling and Disabling Veeam Agent Backup Job....343
Cloning Veeam Agent Backup Job.... 344
Removing Veeam Agent Backup Job....345
Managing Veeam Agent Backup Policies.... 346
Applying Backup Policy to Protected Computers....347
Starting and Stopping Backup.... 348
Performing Active Full Backup.... 350
Clearing Backup Cache.... 351
Editing Backup Policy Settings....352
Enabling and Disabling Backup Policy....353
Cloning Backup Policy....355
Removing Backup Policy....356
MANAGING PROTECTED COMPUTERS.... 357
Moving Unmanaged Computer to Protection Group....358
Adding Computer to Backup Job.... 360
Performing Quick Backup.... 361
Viewing Properties....362
Rescanning Protected Computer....363
Creating Veeam Recovery Media.... 364
Before You Begin....365
Step 1. Launch Create Recovery Media Wizard.... 366
Step 2. Specify Recovery Media Options....367
Step 3. Specify Path to ISO.... 368
Step 4. Review Recovery Image Settings.... 369
Step 5. Finish Working with Wizard....370
What You Do Next.... 371
Installing Veeam Agent....372
Upgrading Veeam Agent....373
Installing Veeam CBT Driver....377
Rebooting Protected Computer.... 380
Uninstalling Veeam Agent....381
Removing Computer from Protection Group....382
RESTORING DATA FROM VEEAM AGENT BACKUPS....386
Restoring Veeam Agent Backup to vSphere VM.... 388
Restoring Veeam Agent Backup to Hyper-V VM.... 389
Restoring Veeam Agent Backup to Nutanix AHV VM.... 390
Restoring to Microsoft Azure.... 391
Restoring to Amazon EC2....392
Restoring to Google Cloud Platform....393

Restoring Volumes 394
Before You Begin 395
Step 1. Launch Volume Level Restore Wizard 396
Step 2. Select Backup 397
Step 3. Select Restore Point 398
Step 4. Map Restored Disks 399
Step 5. Resize Restored Volumes 403
Step 6. Specify Secure Restore Settings 404
Step 7. Specify Restore Reason 405
Step 8. Complete Restore Process 406
Restoring Files and Folders 407
Restoring Application Items 408
Exporting Disks 409
Step 1. Launch Export Disk Wizard 410
Step 2. Select Backup 411
Step 3. Select Restore Point 412
Step 4. Select Disks 413
Step 5. Select Destination and Disk Format 414
Step 6. Specify Secure Restore Settings 416
Step 7. Specify Restore Reason 417
Step 8. Complete Restore Process 418
Exporting Restore Point to Full Backup File 419
MANAGING VEEAM AGENT BACKUPS 420
Creating Veeam Recovery Media from Backup 421
Removing Backup from Configuration 422
Deleting Backup from Disk 424
Viewing Backup Properties 425
REPORTING 427
Viewing Rescan Job Statistics 428
Viewing Rescan Job Report 429
Viewing Veeam Agent Backup Job Statistics 430
Viewing Veeam Agent Backup Job Report 431
Viewing Backup Policy Statistics 432
Viewing Backup Policy Report 434
Enabling Email Reporting 435
APPENDIX A. DEPLOYING HOTFIX ON PROTECTED COMPUTERS 436
Deployment Procedure for Windows Computers 439
Deployment Procedure for Linux Computers 440
APPENDIX B. RESTORING FILES FROM BACKUP WITHOUT ADMINISTRATOR PRIVILEGES 445

APPENDIX C. UPDATING PRE-INSTALLED VEEAM AGENTS..... 448
Update Procedure for Windows Computers 451
Update Procedure for Linux Computers..... 452
Update Procedure for Mac Computers..... 453

Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

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

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

About This Document

This guide describes how to use Veeam Backup & Replication to deploy and manage Veeam Agents. It provides a general overview of the Veeam Agent management functionality, as well as description of data protection and disaster recovery tasks available within the Veeam Agent management scenario. The document applies to Veeam Backup & Replication 11 and all subsequent versions until it is replaced by a new document.

Intended Audience

The guide is designed for anyone who wants to use Veeam Backup & Replication to automate data protection tasks performed on Veeam Agent computers. It is primarily aimed at backup administrators and other IT professionals managing Veeam Backup & Replication but can also be helpful for Veeam Agent computer users. The document assumes that you are familiar with basic concepts and operations that can be performed in Veeam Backup & Replication and Veeam Agents you need .

Related Documentation

The document should be regarded as a supplement to existing technical documentation for the following products:

- Veeam Backup & Replication
- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for IBM AIX
- Veeam Agent for Oracle Solaris
- Veeam Agent for Mac

The complete set of documentation for Veeam products can be found at https://www.veeam.com/documentation-guides-datasheets.html.

Overview

Veeam Backup & Replication lets you deploy and manage the following Veeam Agents on computers in your infrastructure:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for IBM AIX
- Veeam Agent for Oracle Solaris
- Veeam Agent for Mac

You do not need to install, set up and operate Veeam Agent on every computer whose data you want to protect. Instead, you can perform the whole set of deployment, administration, data protection and disaster recovery tasks on Veeam Agent computers remotely from the Veeam Backup & Replication console.

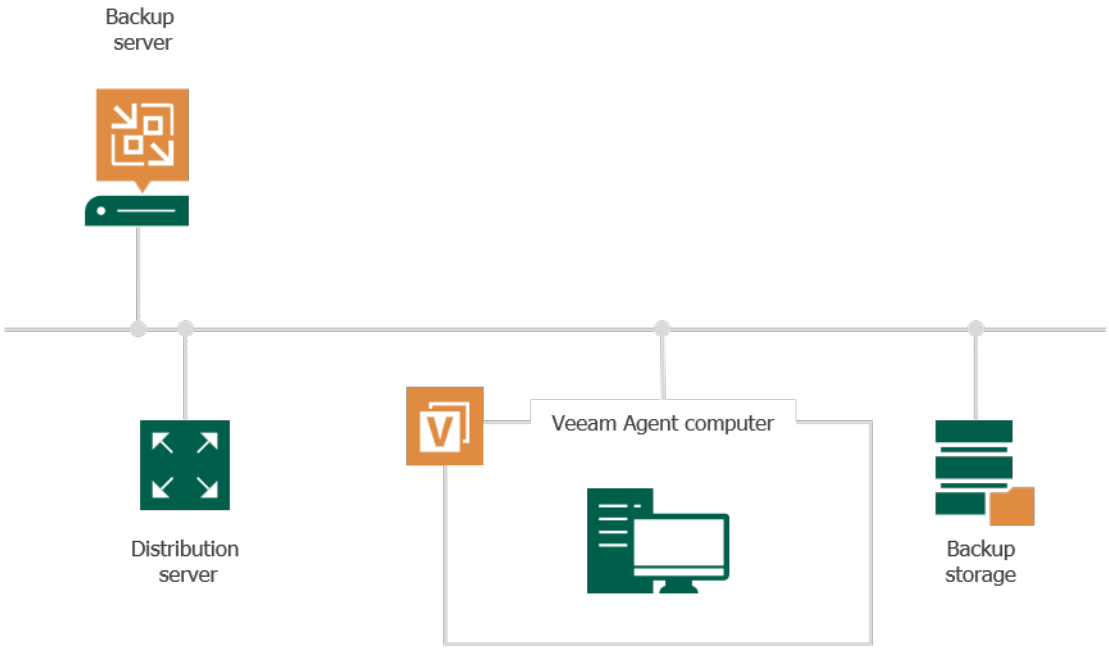
Veeam Backup & Replication offers the following Veeam Agent management capabilities:

- **Automated deployment and management of Veeam Agents**. You can set up Veeam Backup & Replication to automatically discover computers that you want to protect with Veeam Agent for Microsoft Windows and Veeam Agent for Linux. You can also manually deploy all supported Veeam Agents on computers you want to protect. Once Veeam Agent is deployed on protected computers, you can use the Veeam Backup & Replication console to administrate Veeam Agent on multiple computers.
- **Centralized configuration and management of Veeam Agent backup jobs on protected computers**. You can use the Veeam Backup & Replication console to create and manage Veeam Agent backup jobs on computers in your infrastructure whose data you want to protect.
- **Centralized management of backups created by Veeam Agent backup jobs**. If you choose to create Veeam Agent backups on a backup repository managed by the Veeam backup server, you can use the Veeam Backup & Replication console to restore data from these backups.

Veeam Agent Management Infrastructure

The Veeam Agent management infrastructure comprises the following components:

- Veeam backup server
- Veeam Agent computers
- Distribution server



Veeam Backup Server

The Veeam backup server is the core component in the backup infrastructure that fills the role of the "configuration and control center". To use the Veeam Agent management functionality offered by Veeam Backup & Replication, you can use the backup server that is already running in your backup infrastructure or deploy a separate backup server.

To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.

Veeam Agent Computers

To manage Veeam Agents on computers in your infrastructure, you must add computers that you want to protect to the inventory in the Veeam Backup & Replication console and deploy Veeam Agents. In Veeam Backup & Replication, protected computers are organized into protection groups. To learn more, see Protection Groups.

Veeam Backup & Replication lets you manage Veeam Agent on computers of the following types:

- Workstations, servers, and failover clusters running a Microsoft Windows OS
- Workstations and servers running a Linux OS
- Servers running a Unix OS
- Workstations and servers running a macOS

If you want to manage Veeam Agents installed on protected computers in Veeam Backup & Replication, you must set Veeam Agents in the managed mode. In this mode, all data protection and administration tasks are performed by a backup administrator in Veeam Backup & Replication. In some scenarios, a user can also perform a limited set of backup and disaster recovery tasks directly on a protected computer.

The following Veeam Agent configurations operate in the managed mode:

- Veeam Agent for Microsoft Windows and Veeam Agent for Linux deployed on remote computers by Veeam Backup & Replication automatically.

  Veeam Backup & Replication is set up to automatically discover computers added to the inventory and deploy Veeam Agent for Microsoft Windows and Veeam Agent for Linux on these computers. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.

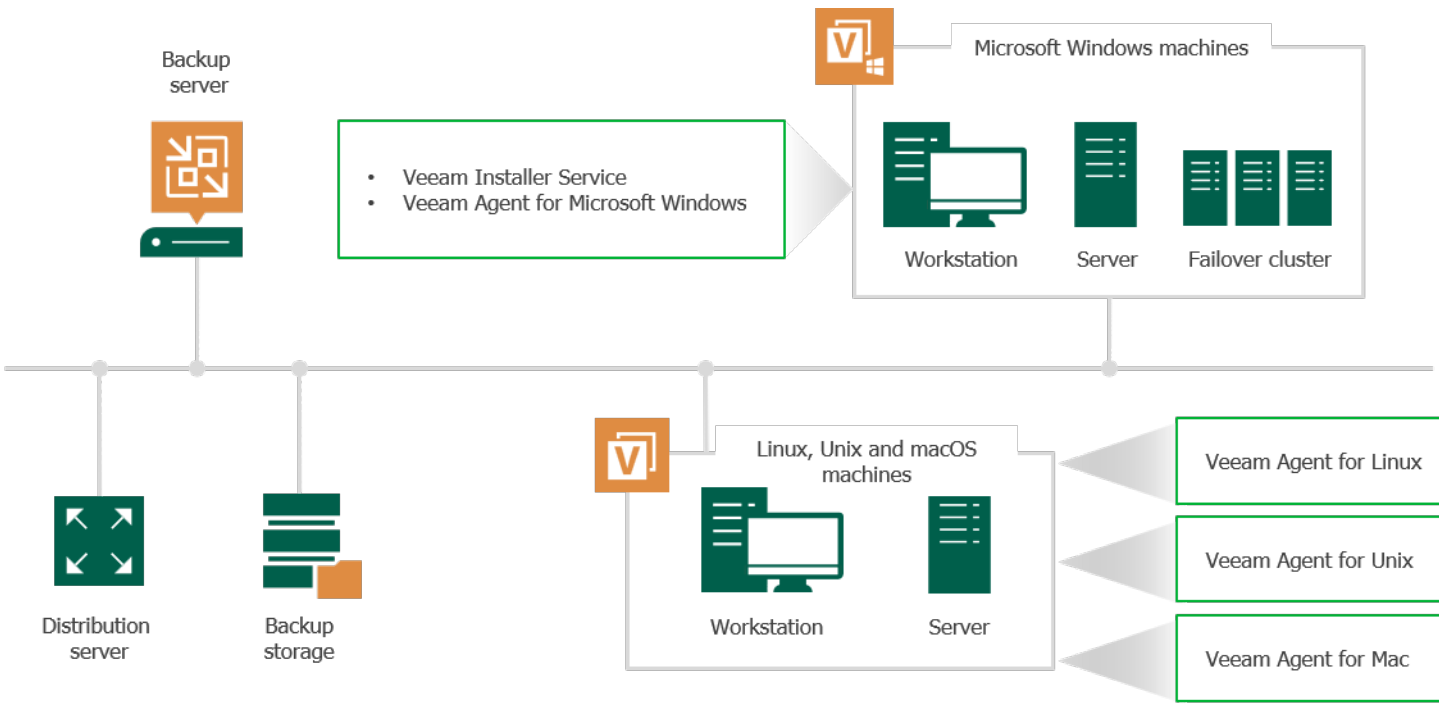
  On every Microsoft Windows computer added to the inventory, Veeam Backup & Replication installs the Veeam Installer Service. The service performs the following tasks:

  - Collects information about the protected computer and sends it to the Veeam backup server. The collected data includes details on the computer type, platform, host name, guest OS, BIOS UUID, IP address, and information about Veeam Agent (its presence on the computer, product version and license installed).
  - Downloads Veeam Agent setup files from the distribution server and installs Veeam Agent on the protected computer.

  On Linux computers, Veeam Backup & Replication does not install additional components for Veeam Agent deployment. Veeam Backup & Replication connects to a Linux computer via SSH and performs necessary operations on the computer. Keep in mind that to connect to Linux computer via SSH, this Linux computer must be added to the list of trusted hosts. To learn more, see Configuring Security Settings.

- Veeam Agents deployed on remote computers by user manually.

  On Unix and macOS computers, you must deploy Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris, or Veeam Agent for Mac on a computer you want to protect and set a connection to Veeam Backup & Replication. You can manually deploy Veeam Agent for Microsoft Windows and Veeam Agent for Linux as well. After that, you can use Veeam Backup & Replication to perform necessary operations on the computers. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.



Distribution Server

The distribution server is an architecture component in the Veeam Agent management infrastructure used for automated deployment of Veeam Agent setup files to protected computers. When you instruct Veeam Backup & Replication to install Veeam Agent on a protected computer, the Veeam backup server communicates to the distribution server, and Veeam Backup & Replication uploads Veeam Agent setup file from the distribution server to the target computer.

> **NOTE**
>
> Veeam Backup & Replication 11a (build 11.0.1.1261) with Cumulative Patch P20211211 installed deploys Veeam Agent for Microsoft Windows 5.0.2 and Veeam Agent for Linux 5.0.2 on protected computers.

By default, the role of the distribution server is assigned to the backup server itself. However, you can deploy a dedicated distribution server to reduce workload on the backup server. To deploy a distribution server, you need to add a Windows-based server to Veeam Backup & Replication. To learn more, see the Adding Microsoft Windows Servers section in the Veeam Backup & Replication User Guide. After you assigned the role of distribution server, you need to select this server in the properties of a protection group. To learn more, see Specify Discovery and Deployment Options.

A machine performing the role of the distribution server must meet the following requirements:

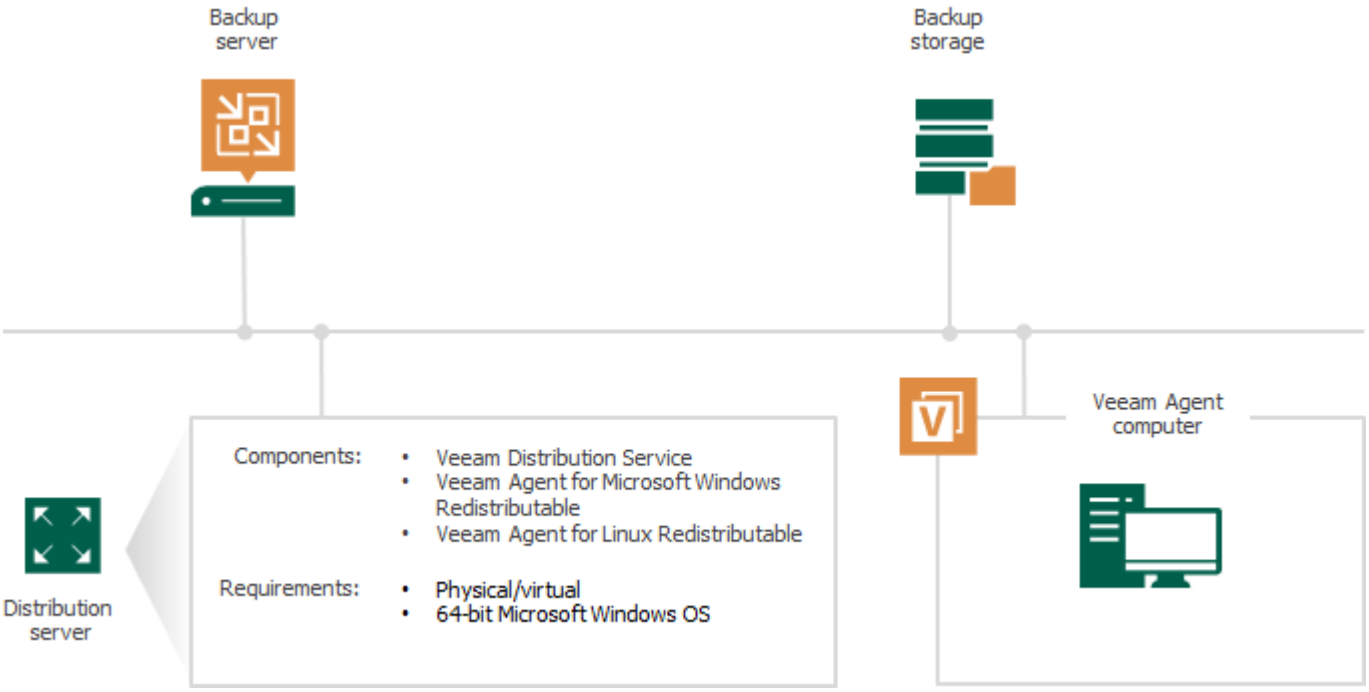
- The role of the distribution server can be assigned to a physical or virtual machine.
- The machine must run a 64-bit Microsoft Windows OS.
- You must add the machine to the Veeam Backup & Replication console as a managed server.

The distribution server comprises the following services and components:

- Veeam Distribution Service
- Veeam Agent for Microsoft Windows Redistributable
- Veeam Agent for Linux Redistributable

Keep in mind that Veeam Backup & Replication does not support automated deployment of Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris and Veeam Agent for Mac. You must deploy these Veeam Agent on computers using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

> **TIP**
>
> If you have several Microsoft Windows and Linux computers with Veeam Agent installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed Veeam Agent computers. To learn more, see Appendix A. Deploying Hotfix on Protected Computers.


Backup server
Backup storage
Veeam Agent computer
Components:
Veeam Distribution Service
Veeam Agent for Microsoft Windows Redistributable
Veeam Agent for Linux Redistributable
Requirements:
Physical/virtual
64-bit Microsoft Windows OS
Distribution server

Protected Computers Discovery and Veeam Agent Deployment

Veeam Backup & Replication supports automated and manual deployment of Veeam Agents on computers in your infrastructure:

- Automated and manual deployment from the Veeam backup console
- Manual deployment using external tools

Automated and Manual Deployment from Veeam Backup Console

You can deploy Veeam Agent for Microsoft Windows and Veeam Agent for Linux from the Veeam Backup & Replication console. To learn more about supported scenarios, see Supported Veeam Agents.

To deploy Veeam Agents, Veeam Backup & Replication needs to discover computers whose data you want to back up. To enable discovery, you organize your computers into one or more protection groups. Protection group settings define what Veeam Agent computers Veeam Backup & Replication will discover and how the discovery process will run. To learn more, see Protection Groups.

You can also disable automated Veeam Agent installation when configuring a protection group. In this case, you will need to use the Veeam Backup & Replication console to install Veeam Agent on every computer included in the protection group. To learn more, see Installing Veeam Agent.

Manual Deployment Using External Tools

You can manually deploy all supported Veeam Agents using external tools. To learn more about supported scenarios, see Supported Veeam Agents.

To deploy Veeam Agents using external tools, you need to perform the following operations:

1. Create a protection group for pre-installed Veeam Agents using Veeam Backup & Replication. To learn more about this type of protection groups, see Protection Group Types.

   After a new protection group is created, Veeam Backup & Replication generates a set of setup files required for the Veeam Agent deployment. This set of setup files includes an XML configuration file with a TLS certificate. This certificate is used to secure the first communication between Veeam Backup & Replication and Veeam Agents. It helps Veeam Agents identify themselves and make sure that computers connecting to the Veeam backup server are really the ones that they claim to be.

   To learn how to check information about the currently used certificate, see Configuring Security Settings.

   > **IMPORTANT**
   >
   > Veeam Backup & Replication generates the same TLS certificate for the first communication between Veeam Backup & Replication and all computers you want to include in protection groups for pre-installed Veeam Agents. So, it is strongly recommended that you securely store and share Veeam Agent setup files. Otherwise, any computer that has this certificate can connect to the Veeam backup server.

2. Using external tools, transfer Veeam Agent setup files to the computer you want to protect. Then, deploy Veeam Agent and connect it to Veeam backup server with an XML configuration file. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

   Once you connect Veeam Agent to the Veeam backup server, Veeam Backup & Replication discoveries the computer and replaces the TLS certificate for all Veeam Agent computers with another TLS certificate that is unique for each computer. After that, you can find the connected computer in the Veeam Backup & Replication console displayed as a member of the protection group.

Protection Groups

In Veeam Backup & Replication, computers that you want to protect with Veeam Agents are organized into protection groups. Technically, a protection group is a container in the Veeam Backup & Replication inventory aimed to combine protected computers of a specific type. For example, you can use a dedicated protection group for computers of the same type (for example, laptops, workstations or servers) or computers running the same OS type to simplify management of such computers. You can also use a separate protection group for a number of Veeam Agent computers that you want to manage in a different way from other machines in your infrastructure.

To start managing Veeam Agents in Veeam Backup & Replication, you need to create a protection group in the inventory and specify computers that you want to protect with Veeam Agents in the protection group settings. You can create one or more protection groups depending on the size and complexity of your infrastructure. Protection groups appear under the **Physical Infrastructure** node in the **Inventory** view of the Veeam Backup & Replication console.

> **NOTE**
>
> Mind the following:
>
> - The **Physical Infrastructure** node is not available if the Veeam Cloud Connect service provider license is installed on the backup server.
> - If you want to manage only a small number of Veeam Agent computers in Veeam Backup & Replication and do not want to create protection groups, you can add the necessary computers directly to a Veeam Agent backup job. Veeam Backup & Replication will automatically include such computers to the *Manually Added* protection group. To learn more, see Predefined Protection Groups.

Protection groups allow you to automate deployment and management of Veeam Agents on computers in your infrastructure. When you configure a protection group, you can specify scheduling options for protected computers discovery and Veeam Agent deployment. You do not need to perform administrative tasks individually for every computer that you want to protect with Veeam Agent — Veeam Backup & Replication will perform the specified operations automatically upon the defined schedule.

Veeam Backup & Replication connects to discovered computers using credentials of the account specified in the protection group settings. You can specify a master account that Veeam Backup & Replication will use to connect to all computers added to the protection group or specify separate accounts to connect to specific computers in the protection group.

After you create a protection group, Veeam Backup & Replication starts the rescan job session to connect to computers added to the protection group and perform the required operations on these computers. To learn more, see Rescan Job.

> **IMPORTANT**
>
> Keep in mind that protection groups for pre-installed Veeam Agents do not allow you to perform deployment and management tasks. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

Protection Group Types

Veeam Backup & Replication offers several methods to specify computers on which you want to install and manage Veeam Agent. You can create protection groups that include the following types of objects:

- **Individual computers**

  You can organize individual computers into a protection group by specifying the necessary computers in the protection group settings. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed.

- **Microsoft Active Directory objects**

  You can create protection groups that include one or more Microsoft Active Directory objects: entire domain, container, organization unit, group, computer or cluster. This allows you to manage Veeam Agents on computers being part of an Active Directory domain. Protection groups that include Active Directory domain, containers, groups and/or organization units are dynamic in their nature. For example, if a new computer is added to a container, Veeam Backup & Replication will automatically discover this computer and start managing this computer as specified in the protection group settings.

  You can specify a protection scope based on Active Directory objects in one of the following ways:

  - You can select individual Active Directory objects that you want to include in a protection group, for example, selected organization units and/or computers.
  - You can include in the protection group an entire domain or other Active Directory object (such as a container or organization unit) and exclude specific child objects being part of this object, for example, selected organization units and/or computers.

- **Computers listed in a CSV file**

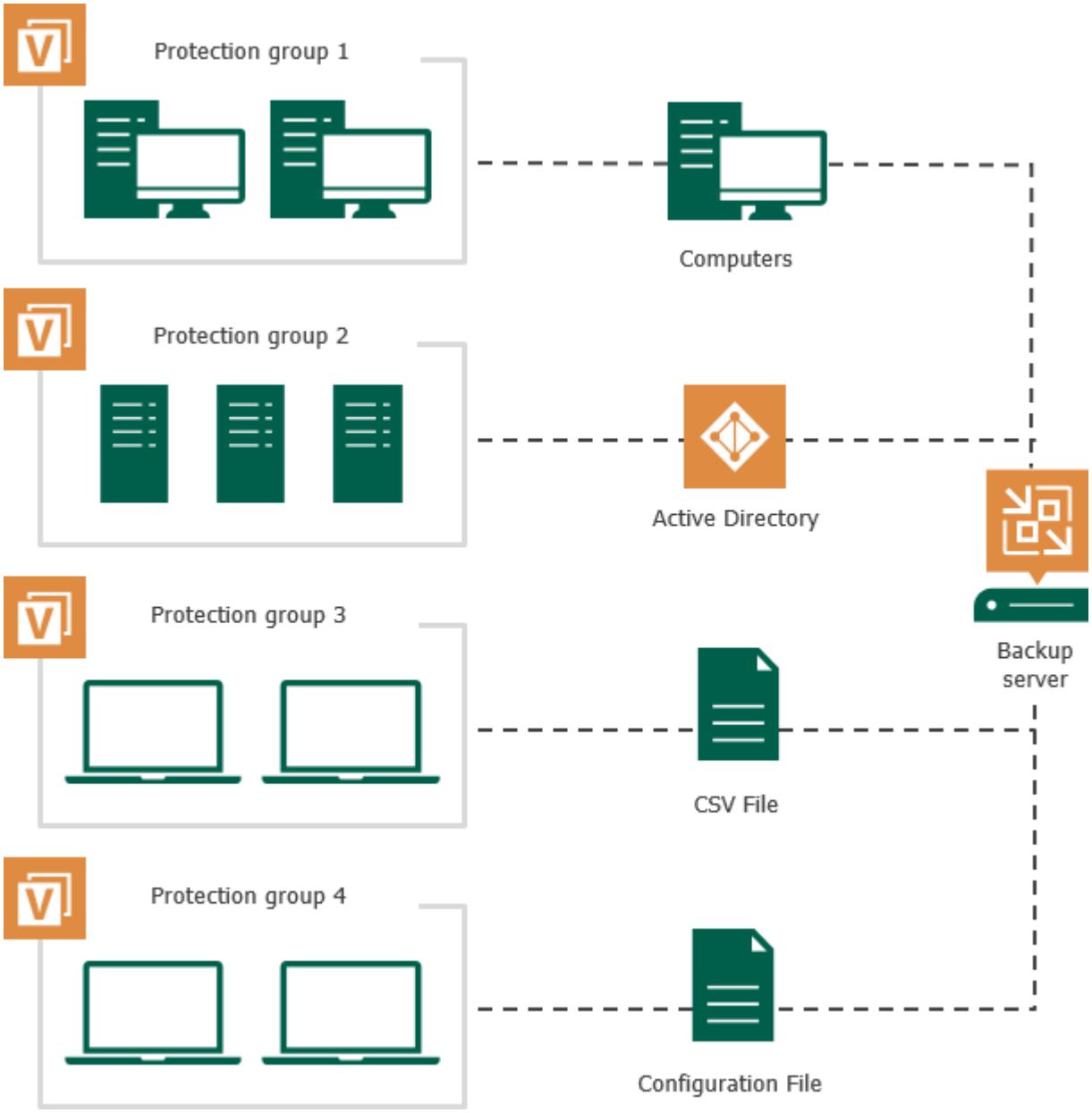
  You can add multiple computers to a protection group by importing a list of computers from a CSV file. Protection groups that include computers listed in a CSV file are also dynamic. If a new computer appears in a CSV file after the protection group is created, during the next protection group rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer.

- **Computers with pre-installed agents**

  You can create protection groups for pre-installed Veeam Agents. Protection groups for pre-installed Veeam Agents are empty just after they are created. You must deploy Veeam Agents on computers and configure Veeam Agents to connect to the Veeam backup server. After deployment and configuration, computers become members of the protection group.

  This option is recommended if you do not have the full list of computers that you want to protect when you create the protection group. This option also provides a convenient way to install agents using third-party software distribution solutions, when deploying them from the Veeam backup server is not possible due to security and network connectivity restrictions.

  Keep in mind that the **Computers with pre-installed agents** option is the only applicable option for Unix and macOS computers that you plan to protect with Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris, and Veeam Agent for Mac.



Predefined Protection Groups

In addition to protection groups created by a user, the Veeam Backup & Replication inventory may contain one or more predefined protection groups.

Manually Added

The *Manually Added* protection group contains individual computers added to Veeam Agent backup jobs configured in Veeam Backup & Replication. This protection group is aimed for scenarios when you want to manage a single Veeam Agent computer or a small number of Veeam Agent computers and do not want to create additional protection groups. Veeam Backup & Replication automatically adds a computer to the *Manually Added* protection group when you add this computer to a Veeam Agent backup job. To learn more, see Adding New Computers.

The *Manually Added* protection group has the following limitations:

- For the *Manually Added* protection group, you can change only a limited number of settings:
  - You can change discovery and deployment options. (Except for changing the distribution server. For the *Manually Added* protection group, the role of the distribution server is always assigned to the backup server.)
  - You can remove computers from this protection group. For example, you may want to remove a computer from a *Manually Added* protection group if you do not want to back up data of this computer any longer, and you have removed this computer from a Veeam Agent backup job.
  - You cannot change other settings, such as the name and type of this protection group.
- You cannot add the entire *Manually Added* protection group to a Veeam Agent backup job.

Unmanaged

The *Unmanaged* protection group acts as a filter to display unmanaged Veeam Agent computers, that is, computers that meet the following conditions:

1. Have Veeam Agent deployed and configured directly from a Veeam Agent computer or with Veeam Service Provider Console.
2. Run a Veeam Agent backup job targeted at a backup repository managed by Veeam Backup & Replication.

You cannot perform any operations with the *Unmanaged* protection group, as well as add computers included in this group to a Veeam Agent backup job. However, you can move such computers to a protection group that you created. To learn more, see Moving Unmanaged Computer to Protection Group.

After you move an unmanaged computer to a protection group, Veeam Backup & Replication will start managing Veeam Agent running on this computer according to discovery settings specified in the properties of the protection group. If the protection group is added to a Veeam Agent backup job, Veeam Backup & Replication will add the new computer to the job, too. You will no longer be able to manage Veeam Agent directly on the Veeam Agent computer or from Veeam Service Provider Console.

Out of Date

The *Out of Date* protection group is displayed when Veeam Backup & Replication discovers protected computers on which an outdated version of Veeam Agent is installed. For example, this may happen in a situation where you configure a protection group with Veeam Agent deployment options disabled, and Veeam Backup & Replication detects a newer version of Veeam Agent on the distribution server during discovery.

The *Out of Date* protection group lets you update Veeam Agent on multiple computers at once. To learn more, see Upgrading Veeam Agent on Multiple Computers.

Offline

The *Offline* protection group acts as a filter to display computers to which Veeam Backup & Replication could not connect during the latest rescan session.

Untrusted

The *Untrusted* protection group acts as a filter to display Linux-based computers whose fingerprints were not verified in Veeam Backup & Replication. For computers included in this protection group, you need to check and validate SSH fingerprints. To learn more, see Validating SSH Fingerprints.

Rescan Job

For automated discovery of protected computers, Veeam Backup & Replication uses the rescan job that runs on the backup server. Veeam Backup & Replication automatically creates this job once you create the first protection group in the inventory. The rescan job runs upon schedule defined individually for every protection group in the protection group settings. By default, Veeam Backup & Replication is set up to perform discovery at 9:00 PM daily. You can adjust daily schedule in the protection group settings or define periodic schedule.

The rescan job itself is not displayed in the Veeam Backup & Replication console. However, you can start and stop rescan job sessions manually for a specific protection group or individual computer in the inventory. This may be helpful, for example, if new computers appeared in your infrastructure, and you want to discover these computers without waiting for the next scheduled rescan job session start. To learn more, see Rescanning Protection Group and Rescanning Protected Computer.

You can view statistics for currently running and already performed rescan job sessions. To learn more, see Viewing Rescan Job Statistics.

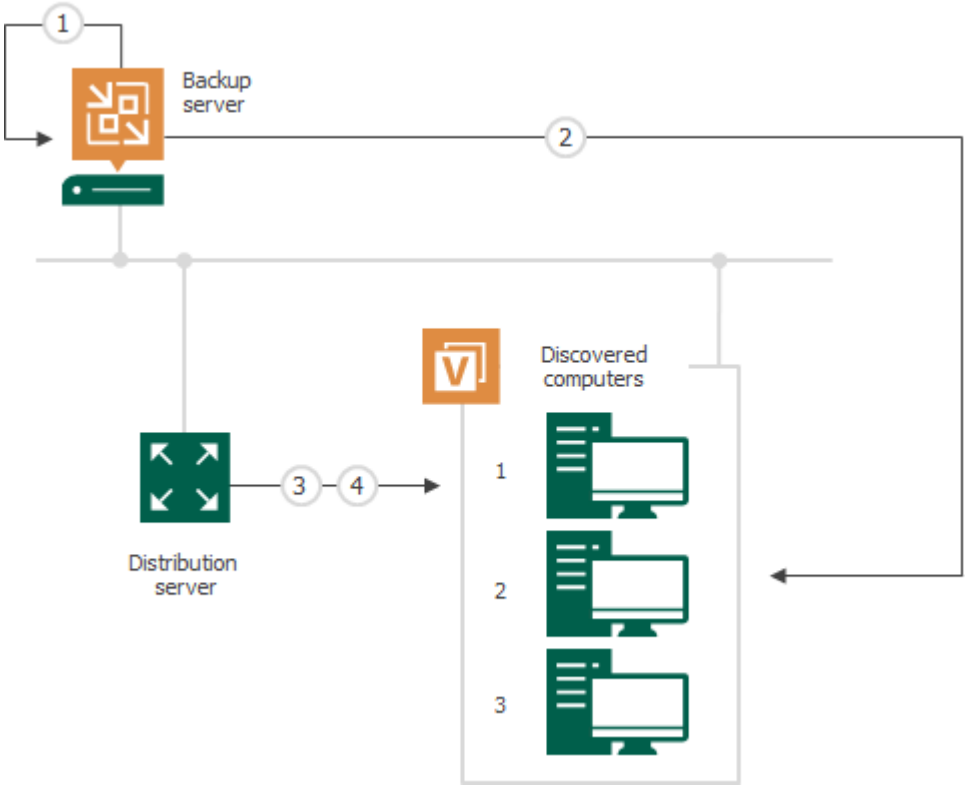
Keep in mind that rescan is not available for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in such protection groups synchronize with Veeam Backup & Replication every 6 hours and provide information about the Veeam Agent computer.

How It Works

When the rescan job is started — either automatically upon schedule or manually — Veeam Backup & Replication performs the following operations:

1. Obtains settings specified for the protection group from the configuration database. The settings include a list of computers to scan, an account for connecting to these computers, and so on.
2. Connects to each computer in the list under the specified account.
3. Deploys Veeam Installer Service on each newly discovered computer.
4. If the automatic Veeam Agent deployment option is enabled in the protection group settings, Veeam Backup & Replication also deploys Veeam Agent on discovered computers. As a part of this process, Veeam Backup & Replication performs the following operations:
    a. Veeam Installer Service running on the computer collects information about the computer and sends it to Veeam Backup & Replication. The collected data includes details on the computer type, platform, host name, guest OS, IP address, BIOS UUID, and information about Veeam Agent (its presence on the computer, product version and license installed).
    b. Veeam Backup & Replication uploads the Veeam Agent setup file from the distribution server to the discovered computer.

c. Veeam Installer Service installs Veeam Agent on the target computer.



Veeam Agent Backup Jobs and Policies

To back up data of your protected computers, you must configure a Veeam Agent backup job. The Veeam Agent backup job defines what data to back up, how, where and when to back up data. In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

- **Backup job**

  The backup job that processes Veeam Agent computers runs on the backup server in the similar way as a regular job for VM data backup. The backup job is intended for protected computers that have permanent connection to the backup server, such as standalone servers and failover clusters. You can use the backup job to create Veeam Agent backups in a backup repository or cloud repository.

  In Veeam Backup & Replication, the backup job of this type is also referred to as the *Veeam Agent backup job managed by the backup server*.

  To learn more, see Backup Job.

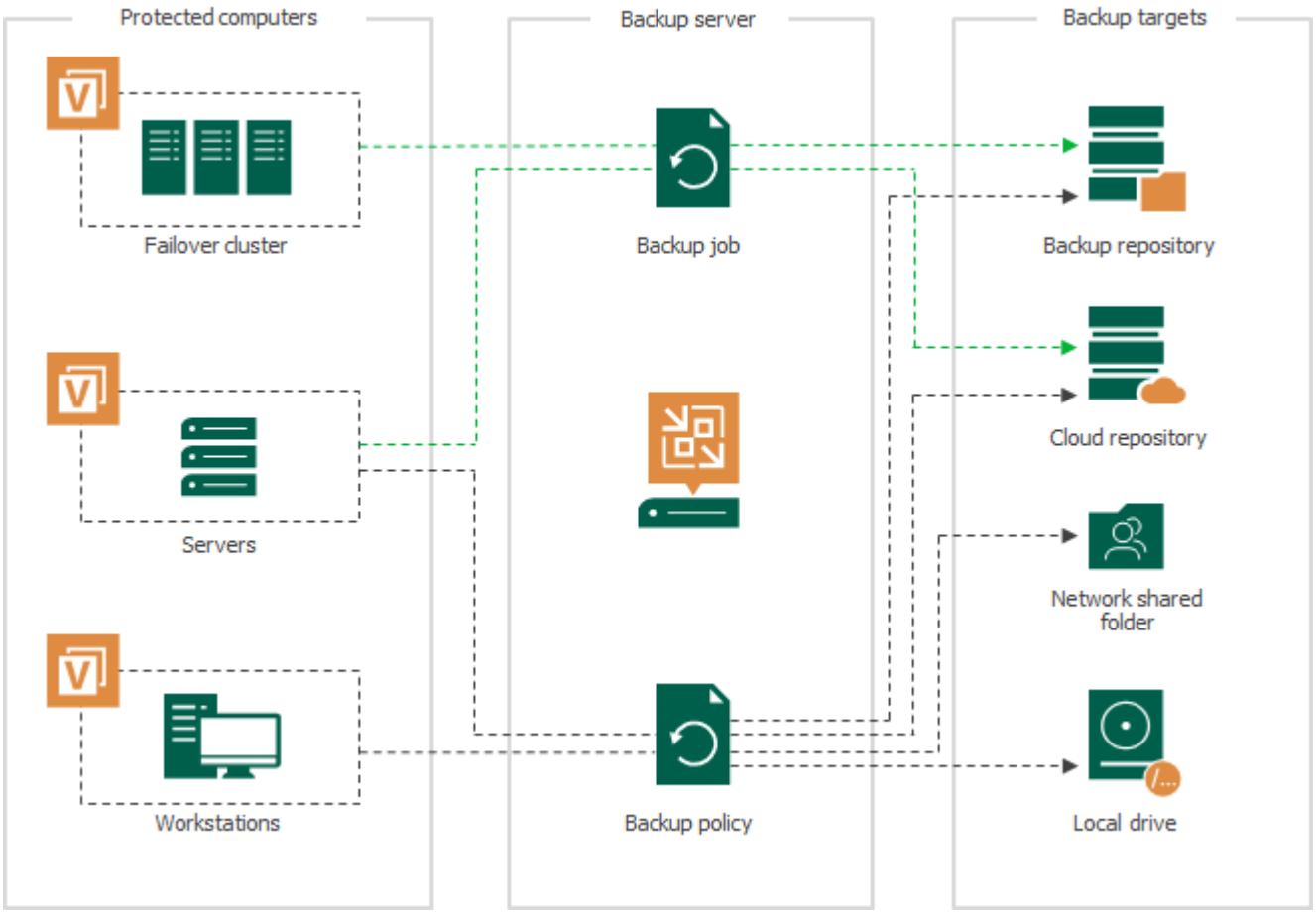
- **Backup policy**

  The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to Veeam Agents that run on computers specified in the backup policy. The backup policy is intended for protected computers that may have limited connection to the backup server, such as workstations, laptops and so on. You can choose to create Veeam Agent backups in a backup repository, cloud repository, network shared folder or on a local storage of a protected computer.

  Veeam Agent computers that are members of a protection group for pre-installed Veeam Agents can be processed only by backup policies. To learn more about protection group for pre-installed Veeam Agents, see Protection Group Types.

  In Veeam Backup & Replication, the backup policy is also referred to as the *Veeam Agent backup job managed by Veeam Agent*.

  To learn more, see Backup Policy.



Veeam Backup & Replication lets you create the following types of backup jobs and policies depending on the type of OS that runs on a protected computer:

- Backup jobs and policies that process Microsoft Windows computers. For such Veeam Agent backup jobs, Veeam Backup & Replication offers settings supported in Veeam Agent for Microsoft Windows.
- Backup jobs and policies that process Linux computers. For such Veeam Agent backup jobs, Veeam Backup & Replication offers settings supported in Veeam Agent for Linux.
- Backup policies that process Unix computers. For such Veeam Agent backup policies, Veeam Backup & Replication offers settings supported in Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris.

- Backup policies that process Mac computers. For such Veeam Agent backup policies, Veeam Backup & Replication offers settings supported in Veeam Agent for Mac.

If a protection group contains Microsoft Windows computers and Linux computers, you can add this protection group to a Veeam Agent backup job intended for any of these types of protected computers. Veeam Backup & Replication will automatically exclude computers of another type from the backup job and processes only those computers that run an OS of the same type.

For example, if you add a protection group that contains Microsoft Windows and Linux computers to a Veeam Agent backup job intended for Linux computers, Veeam Backup & Replication will exclude Microsoft Windows computers from this backup job and process only Linux computers within the job.

Processing One Computer with Multiple Jobs and Policies

The number of backup jobs and policies that can process the same protected computer depends on the computer type. A protected computer can be processed by more than one Veeam Agent backup job according to the following rules:

- You can include a computer of the *Server* type in more than one backup job managed by the backup server or more than one backup policy.
- You can include a computer of the *Workstation* type in one backup policy targeted at a local drive, network shared folder or Veeam backup repository plus unlimited number of backup policies targeted at a Veeam Cloud Connect repository.
- You cannot include the same computer in a backup job and backup policy simultaneously.

Backup Job

The backup job that processes Veeam Agent computers runs on the backup server in the similar way as a regular job for VM data backup. You can add one or more protection groups or individual computers to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or cloud repository. In terms of the Veeam Agent management scenario, the backup job of this type is also referred to as the Veeam Agent backup job managed by the backup server.

For a Veeam Agent backup job managed by the backup server, all job management tasks are performed on the Veeam Backup & Replication side: Veeam Backup & Replication starts the job upon the defined schedule, allocates backup infrastructure resources, and so on. Veeam Agent running on a protected computer operates under control from Veeam Backup & Replication and performs data backup operations only, such as creating a volume snapshot, reading the backed-up data and transferring backed-up data to the target location. To learn more, see How Veeam Agent Backup Job Works.

To configure a backup job, you must launch the **New Agent Backup Job** wizard and select the **Managed by backup server** option at the **Job mode** step of the wizard. For backup jobs of this type, Veeam Backup & Replication offers settings similar to settings of a VM backup job, as well as settings specific for Veeam Agents. To learn more, see Creating Veeam Agent Backup Jobs.

> **NOTE**
>
> To manage a Veeam Agent backup job managed by the backup server, you can use the Veeam Backup & Replication console only. On a computer added to a backup job of this type, the Veeam Agent user interface is not available, and you cannot perform operations with Veeam Agent directly on the protected computer.

How Veeam Agent Backup Job Works

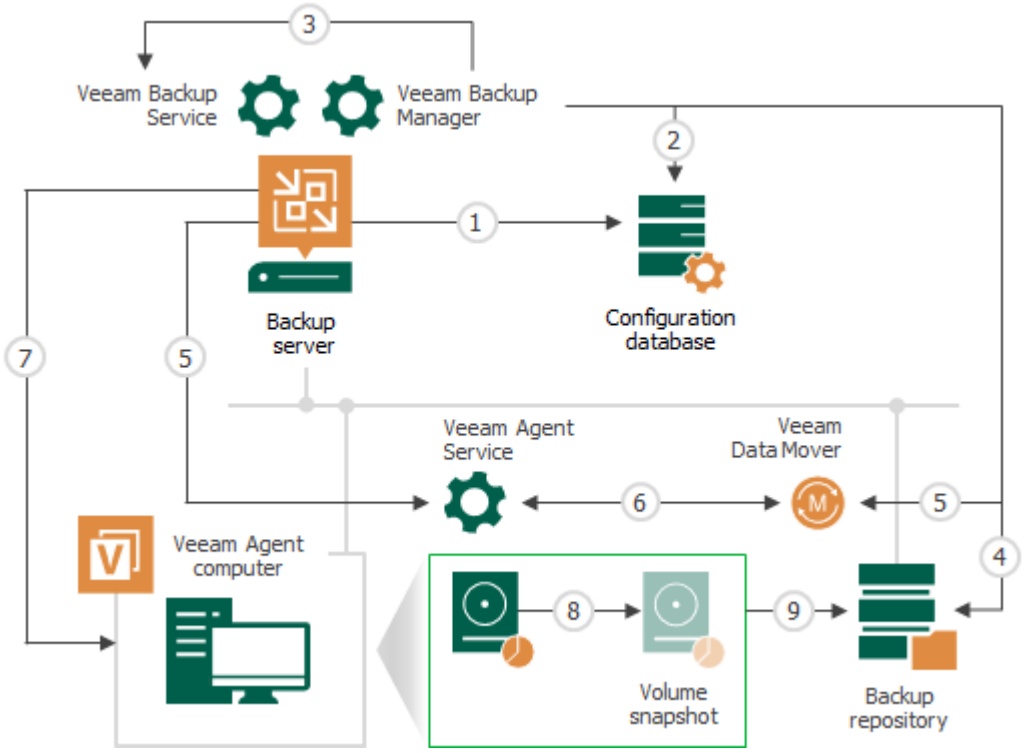
In the scenario where you use the backup job to create Veeam Agent backups, Veeam Backup & Replication performs backup in the following way:

1. When you create a Veeam Agent backup job in Veeam Backup & Replication, Veeam Backup & Replication saves the backup job settings in its database.
2. When a new backup job session starts, Veeam Backup & Replication starts the Veeam Backup Manager process on the backup server. Veeam Backup Manager reads job settings from the configuration database and creates a list of backup tasks to process. For every protected computer added to the job, Veeam Backup & Replication creates a new task.
3. Veeam Backup Manager connects to the Veeam Backup Service. The Veeam Backup Service includes a resource scheduling component that manages all tasks and resources in the backup infrastructure. The resource scheduler checks what backup infrastructure resources are available, and assigns backup repository to process job tasks.
4. Veeam Backup Manager connects to Veeam Transport Service on the backup repository. The Veeam Transport Service, in its turn, starts Veeam Data Mover. A new instance of Veeam Data Mover is started for every job task.
5. Veeam Backup Manager establishes a connection with Veeam Agent service that runs on the protected computer and Veeam Data Mover that runs on the backup repository, and sets a number of rules for data transfer, such as network traffic throttling rules and so on.
6. Veeam Agent service that runs on the protected computer and Veeam Data Mover that runs on the backup repository establish a connection with each other for data transfer.

7. If application-aware processing is enabled for the job, Veeam Backup & Replication connects to protected computers, establishes a connection with Veeam Agents running on protected computers and performs in-guest processing tasks.
8. Veeam Backup & Replication requests Veeam Agent to create a VSS snapshot or volume snapshot, depending on the type of OS running on the Veeam Agent computer. For Windows-based computers, Veeam Agent for Microsoft Windows leverages Microsoft VSS technology to create a VSS snapshot. For Linux-based computers, Veeam Agent for Linux uses the Veeam driver to create a volume snapshot.
9. Veeam Agent service that runs on the protected computer reads the backed-up data from the volume snapshot and transfers the data to the backup repository. During incremental job sessions, the Veeam Agent service uses CBT to retrieve only those data blocks that have changed since the previous job session. If CBT is not available, the Veeam Agent service interacts with the target Veeam Data Mover on the backup repository to obtain backup metadata, and uses this metadata to detect blocks that have changed since the previous job session.

   While transporting backed-up data, Veeam Agent running on a protected computer performs additional processing. It filters out zero data blocks, blocks of swap files and blocks of excluded files and folders. Veeam Agent compresses backed-up data and transports it to the target Veeam Data Mover.

   Veeam Backup & Replication stores backed-up data to the backup file in the backup repository.



Backup Policy

In some cases, the backup job managed by the backup server may be not suitable for data backup with Veeam Agents. For example, you may want use Veeam Agents to back up data of computers that reside in a remote location and have limited connection to the Veeam backup server and backup repository. For such scenarios, Veeam Backup & Replication offers the concept of the *backup policy*.

The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. You can add one or more protection groups or individual computers to the backup policy and instruct Veeam Agent to create backups in a Veeam backup repository, in a Veeam Cloud Connect repository, in a network shared folder or on a local storage of a protected computer. In terms of the Veeam Agent management scenario, the backup policy is also referred to as the Veeam Agent backup job managed by the Veeam Agent.

Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to protected computers. The resulting Veeam Agent backup jobs run on protected computers in the similar way as a regular backup job configured directly in Veeam Agent. All backup job management and data processing tasks are performed by Veeam Agent itself. This allows Veeam Agent to create backups of your data even if a connection to the backup server is unavailable. To learn more, see How Backup Policy Works.

Keep in mind that the backup policy is the only applicable approach to protect Mac and Unix computers as Veeam Agent for Mac, Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris do not support backup jobs managed by backup server.

To configure a backup policy, you must launch the **New Agent Backup Job** wizard and select the **Managed by agent** option at the **Job mode** step of the wizard. To learn more, see Creating Veeam Agent Backup Policies.

NOTE

- For computers specified in the backup policy, in addition to managing backup settings and performing backup tasks from the Veeam backup console, you can also perform selected operations directly on a protected computer. In particular, you can use the Veeam Agent control panel to start the backup job manually. This allows you to create ad-hoc backups of your data in addition to backups created upon schedule defined in the backup policy.
- The backup policy is the only approach to protect Mac computers as Veeam Agent for Mac does not support backup jobs managed by backup server.
- The backup policy is the only approach to protect members of a protection group for pre-installed Veeam Agents. To learn more, see Protection Group Types.

How Backup Policy Works

IMPORTANT

Mind that the way how backup policy works for computers included in protection groups for pre-installed Veeam Agents differs from the standard scenario. To learn more, see How Backup Policy Works With Computer Included In Protection Group for Pre-Installed Veeam Agents.

In the scenario where you use the backup policy to create Veeam Agent backups, Veeam Backup & Replication and Veeam Agents interact in the following way:

1. When you create a backup policy, Veeam Backup & Replication saves the backup policy settings in the following locations on the backup server:
    - In the Veeam Backup & Replication database.

- In the configuration file of the XML format.

2. Once the backup policy is created, Veeam Backup & Replication immediately applies the backup policy to Veeam Agents that run on protected computers.

   a. Veeam Backup & Replication reads the list of computers and protection groups specified in the backup policy and starts the discovery process for these computers.

   b. During the discovery process, Veeam Backup & Replication connects to each computer in the backup policy and uploads the XML file with backup policy settings to the target computer.

   c. Veeam Backup & Replication uses settings from the backup policy to configure the Veeam Agent backup job. This process differs depending on what OS and Veeam Agent the protected computer runs.

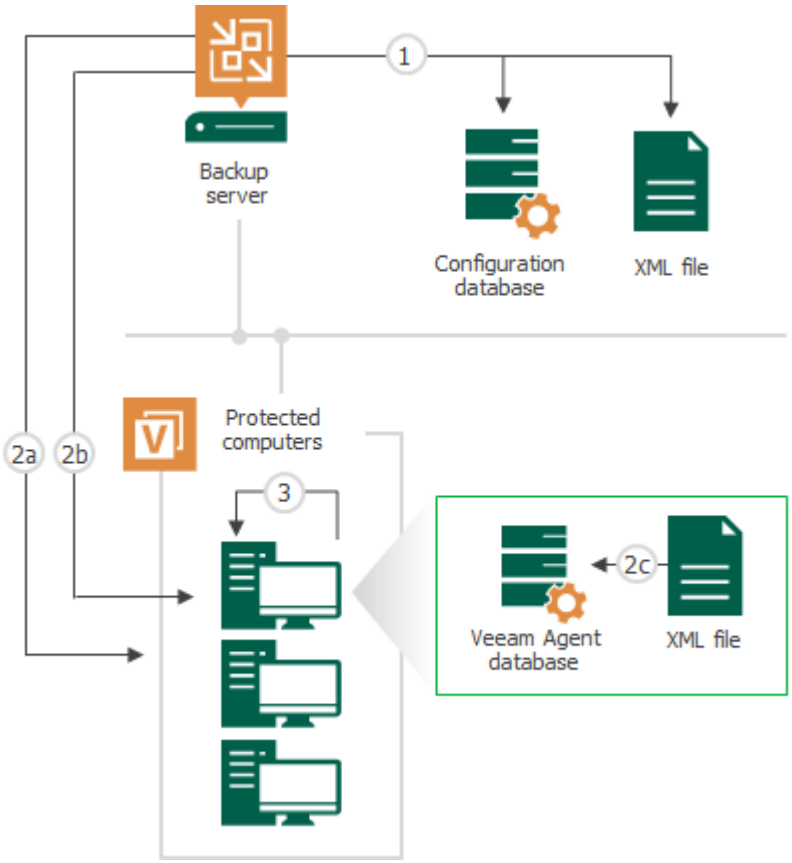
      - On Microsoft Windows computers, Veeam Backup & Replication creates the Veeam Agent backup job using the Veeam Agent for Microsoft Windows Configurator.
      - On Linux computers, Veeam Backup & Replication creates the Veeam Agent backup job using the Veeam Agent for Linux command line interface.

      Settings of the created backup job are saved to the Veeam Agent database on the protected computer.

   Veeam Backup & Replication regularly applies the backup policy to protected computers during rescan of protection groups added to the backup policy. To learn more, see Backup Policy Application Methods.

3. The created Veeam Agent backup job runs on the protected computer in the similar way as a regular Veeam Agent backup job configured directly on the Veeam Agent computer. To learn more, see the following sections:
   - How Backup Works section in the Veeam Agent for Microsoft Windows User Guide.
   - How Backup Works section in the Veeam Agent for Linux User Guide.

   Every 6 hours, Veeam Agent checks whether job settings obtained from the backup policy are up-to-date and do not differ from the current backup settings specified in the backup policy. If the settings differ, Veeam Agent updates backup job settings in its database. To learn more, see Backup Policy Application Methods.



How Backup Policy Works With Computer Included in Protection Group for Pre-Installed Veeam Agents

In the scenario where you use the backup policy to create Veeam Agent backups on Veeam Agent computer included in a protection group for pre-installed Veeam Agents, Veeam Backup & Replication and Veeam Agents interact in the following way:

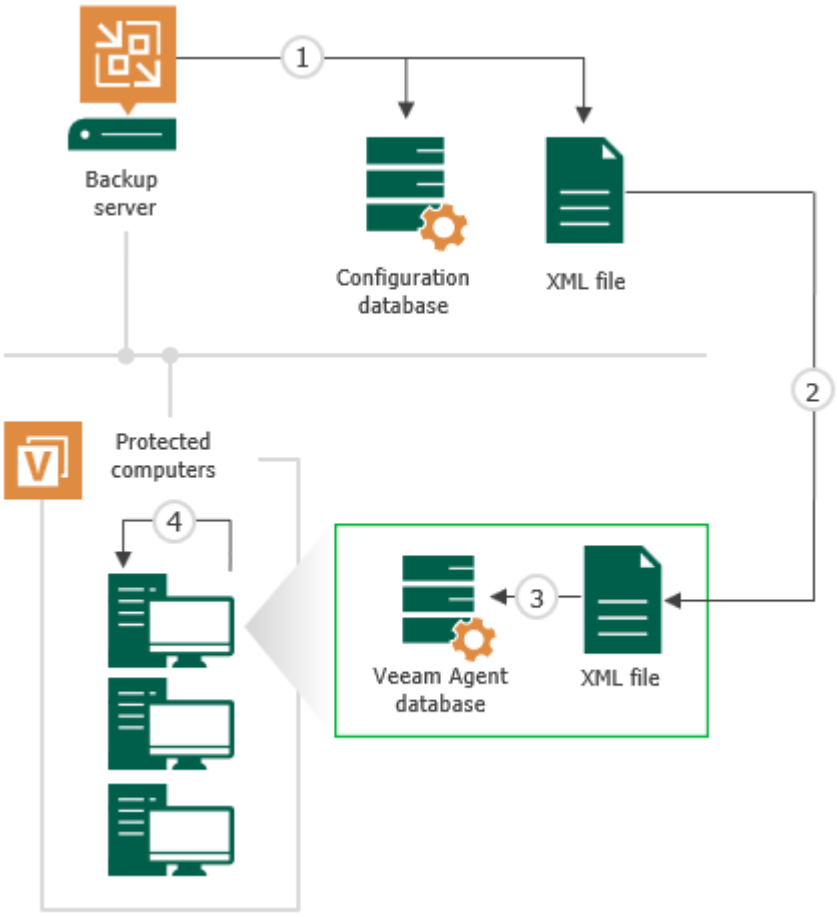
1. When you create a backup policy, Veeam Backup & Replication saves the backup policy settings in the following locations on the backup server:
   - In the Veeam Backup & Replication database.
   - In the configuration file of the XML format.
2. Veeam Agent connects to Veeam Backup & Replication and gets the configuration file.

IMPORTANT

Veeam Agent does not connect to Veeam Backup & Replication immediately after updated backup policy settings are saved. Veeam Agent checks whether Veeam Backup & Replication has any updates in the backup policy settings periodically. As a result, a time period between scenario steps 1 and 2 may take up to 6 hours.

3. Veeam Agent uses the backup policy settings from the configuration file to create a Veeam Agent backup job. Settings of the created backup job are saved to the Veeam Agent database on protected computer.
4. The created Veeam Agent backup job runs on the protected computer in the similar way as a regular Veeam Agent backup job configured directly on the Veeam Agent computer. To learn more, see the following sections:
   - How Backup Works section in the Veeam Agent for Microsoft Windows User Guide.
   - How Backup Works section in the Veeam Agent for Linux User Guide.
   - How Backup Works section in the Veeam Agent for Oracle Solaris User Guide.
   - How Backup Works section in the Veeam Agent for IBM AIX User Guide.
   - How Backup Works section in the Veeam Agent for Mac User Guide.

   Every 6 hours, Veeam Agent checks whether job settings obtained from the backup policy are up-to-date and do not differ from the current backup settings specified in the backup policy. If the settings differ, Veeam Agent updates backup job settings in its database.



Backup Policy Application Methods

To ensure that settings of Veeam Agent backup jobs on protected computers are up-to-date and do not differ from backup settings specified in the backup policy, Veeam Backup & Replication regularly applies the backup policy to protected computers.

> **TIP**
>
> You can also apply the backup policy to protected computers manually, if needed. To learn more, see Applying Backup Policy to Protected Computers.

There are two methods to start the policy application process:

- **By Veeam Backup & Replication**

  Veeam Backup & Replication applies the backup policy to protected computers at the following events:

  - At the time when the backup policy is created.
  - At the time when you start or stop the backup process manually in the Veeam Backup & Replication console.
  - At the time when Veeam Backup & Replication performs scheduled rescan of protection groups added to the backup policy. Veeam Backup & Replication automatically rescans a protection group upon schedule specified in the protection group settings.

  Keep in mind that Veeam Backup & Replication cannot apply backup policy to protection groups for pre-installed Veeam Agents and their members. For members of such protection groups, the policy application process can be started only by Veeam Agent.

- **By Veeam Agent**

  The Veeam Agent service running on a protected computer regularly synchronizes with Veeam Backup & Replication and checks whether job settings obtained from the backup policy are up-to-date and updates backup job settings, if necessary. Veeam Agent performs the synchronization every 6 hours.

  During the synchronization session, Veeam Agent performs the following operations:

  a. Connects to Veeam Backup & Replication and obtains from the Veeam Backup & Replication database information about backup policies to which the Veeam Agent computer was added.

  b. Compares obtained backup policy settings with backup job settings in the Veeam Agent database. If the settings differ, Veeam Agent performs the following tasks:

     - If backup policy settings and Veeam Agent backup job settings do not match, Veeam Agent updates backup job settings in its database.
     - If the protected computer was added to a new backup policy, Veeam Agent creates a new backup job on the protected computer.
     - If the protected computer was removed from the backup policy, Veeam Agent removes the Veeam Agent backup job on the protected computer.

Backup of Microsoft Windows Computers

To back up data of Microsoft Windows computers, you can use Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Backup Cache

Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication supports creating restore points in the backup cache — a temporary local storage where Veeam Agent creates backup files in case a remote backup location is unavailable at the time of backup. This may be helpful in the scenario where you create Veeam Agent backups using the backup policy: if some computers in the backup policy cannot access the remote location during scheduled backup, Veeam Agent creates backup files in the backup cache on these computers. When the target location becomes available, Veeam Agent uploads backup files from the backup cache to the remote storage so that the backup chain contains a sequence of restore points that precisely complies with the backup schedule.

In the Veeam Agent management scenario, the backup cache works in the similar way as in Veeam Agent operating in the standalone mode. To learn more, see the Backup Cache section in the Veeam Agent for Microsoft Windows User Guide.

In addition to backup cache features and limitations listed in the Veeam Agent for Microsoft Windows User Guide, the following applies to Veeam Agent operating in the managed mode:

- You can specify backup cache settings in the properties of backup policies targeted at the following types of backup location:
  - Veeam backup repository
  - Cloud repository
- To facilitate backup cache configuration on multiple Veeam Agent computers added to the backup policy, you can instruct Veeam Agent to automatically select location for the backup cache on each computer. To learn more, see How Automatic Backup Cache Placement Works.

How Automatic Backup Cache Placement Works

You can instruct Veeam Agent to automatically select location for the backup cache on each computer added to the backup policy. To do this, select the **Automatic selection** option at the **Backup Cache** step of the **New Agent Backup Job** wizard. For details, see Specify Backup Cache Settings.

With the **Automatic selection** option enabled in the backup cache settings, Veeam Agent for Microsoft Windows creates the backup cache according to the following rules:

1. Veeam Agent selects for the backup cache a non-system volume that has enough free space for the specified backup cache quota (that is, maximum backup cache size) and has the largest amount of free space.
2. On the selected volume, Veeam Agent creates the backup cache in the *Veeam Backup Cache* folder.

Mind the following:

- If the volume with the largest amount of free space is a system volume, Veeam Agent selects the volume that has enough space for the backup cache quota and has the second largest amount of free space.
- If the system volume is the only volume that has enough space for the backup cache quota, Veeam Agent creates the backup cache on the system volume.
- If no volumes have enough space for the backup cache quota, Veeam Agent selects the volume that has the largest amount of free space.

- Once Veeam Agent creates the *Veeam Backup Cache* folder on a protected computer, Veeam Agent does not change the location of this folder.

  For example, the system volume is the only volume that has enough space for the backup cache quota at the time when you create the backup policy. In this case, Veeam Agent creates the *Veeam Backup Cache* folder on the system volume. After disk configuration changes on the computer, a non-system volume becomes able to fit the backup cache quota. However, Veeam Agent will not move the *Veeam Backup Cache* folder to the non-system volume.

- Veeam Agent does not create the backup cache on external, removable or virtual disks.

Tasks with Backup Cache

For Veeam Agent operating in the managed mode, you can perform the same operations with the backup cache as for the standalone version of the product: you can monitor backup cache activity, pause backup cache synchronization and delete restore points from the backup cache. To do this, you must use the Veeam Agent control panel directly on the protected computer. For details, see the Managing Backup Cache section in the Veeam Agent for Microsoft Windows User Guide.

Note that Veeam Backup & Replication automatically deletes restore points from the backup cache on all computers added to the backup policy after you perform one of the following operations:

- Change the target location for backup files in the backup policy settings.
- Change the backup mode for the backup policy to the *File-level backup*.
- Enable or disable data encryption settings for the backup policy.
- Change backup cache location for the backup policy (in case it was specified manually).
- Disable the backup cache for the backup policy.
- Delete the backup policy.

You can also delete restore points from the backup cache manually in the Veeam backup console. To learn more, see Clearing Backup Cache.

Storage Snapshots Support

You can use Veeam Backup & Replication and Veeam Agent for Microsoft Windows operating in the managed mode (within the Veeam Agent management scenario) to create backups from native storage snapshots.

Native storage snapshots allow the following:

- Veeam Backup & Replication to use backup proxy servers to process storage systems.
- Veeam Agent to use hardware Volume Shadow Copy Service (VSS) provider and capabilities of native snapshots that are created on production storage systems to create backups.

This approach results in much less load on protected servers compared to the regular backup scenario that uses software VSS provider.

For general information about backup jobs that use storage snapshots as a data source, see the Integration with Storage Systems section in the Veeam Backup & Replication User Guide.

Getting Started

Before you configure a Veeam Agent backup job that will use a storage system snapshot as a data source, you must complete the following steps:

1. Configure the backup infrastructure for storage snapshots. For details, see the Backup Infrastructure for Storage Snapshots section in the Veeam Backup & Replication User Guide.

   Keep in mind that you must allow your storage to process Veeam Agent backups. To do this, select the **Block storage for Microsoft Windows servers** check box at the **Name** step of the **New Storage** wizard, then specify options for accessing the storage system at the **Agent Access** step of the wizard. For details, see the Adding Storage Systems section in the Veeam Backup & Replication User Guide.

   Veeam Agent for Microsoft Windows allows you to create backups from native snapshots with hardware VSS provider only. For the list of supported storage systems, see the Veeam Agent Integration section in the Veeam Backup & Replication User Guide.

2. Add a Microsoft Windows computer to the inventory and deploy Veeam Agent for Microsoft Windows on this computer using the Veeam Backup & Replication console. To learn more, see Creating Protection Groups.

Considerations and Limitations

Before you create a Veeam Agent backup from a storage system snapshot, check the following prerequisites:

- The backup proxy and the Veeam Agent computer must run Microsoft Windows Server OS versions. The backup proxy cannot run the OS version that is earlier than the Veeam Agent computer OS version.
- You must use the following product editions:
  - The Standard, Enterprise, or Enterprise Plus edition of Veeam Backup & Replication on the backup server with the backup proxy role.
  - The Server edition of Veeam Agent for Microsoft Windows on the Veeam Agent computer.

  You can check product editions in the **License Information** window of the Veeam Backup & Replication backup console. For details, see the Viewing License Information section in the Veeam Backup & Replication User Guide and the Assigning License to Veeam Agent section in the Veeam Agent for Microsoft Windows User Guide.
- At least one storage logical unit number (LUN) must be mapped to the Veeam Agent computer.

- At least one backup proxy must have access to all LUNs.
- You must use iSCSI or Fibre Channel protocol for your storage system:
  - You must use iSCSI or Fibre Channel protocol to connect LUNs to Veeam Agent computer and backup proxy to your storage system.
  - If you plan to use the iSCSI Protocol, the backup proxy and the Veeam Agent computer must have a Microsoft iSCSI Software initiator enabled.
  - If you plan to use the Fibre Channel Protocol, the backup proxy and the Veeam Agent computer must have a Fibre channel adapter installed and must have access to the storage system over Fibre Channel fabric.
- If a Veeam Agent computer has a storage system with disks that use the GUID Partition Table (GPT) as a partitioning scheme, each disk must contain a Microsoft Reserved (MSR) partition.

In addition to general limitations listed in the in the Veeam Backup & Replication User Guide, consider the following limitations for Veeam Agent backups from storage snapshots:

- If the Storage Replica feature is installed on the Veeam Agent computer, you cannot back up this computer using the hardware VSS provider. If you want to add this computer to the backup scope, you must allow Veeam Backup & Replication to fail over to the regular backup scenario that uses software VSS provider. To learn more, see Integration Settings. To learn more about Storage Replica, see this Microsoft article.
- The backup proxy and the Veeam Agent computer you want to back up cannot be the same computer.
- You cannot back up the following objects using the hardware VSS provider:
  - Volumes allocated to the RDM disk
  - Storage spaces

  With volumes allocated to RDM disks or storage spaces in the backup scope, Veeam Backup & Replication will fail over to the regular backup scenario even if failover is not allowed in storage integration settings.
- If your Veeam Agent computer has a disk that contains the storage spaces protective partition, you cannot back up volumes allocated to this disk using the hardware VSS provider. To back up such volumes, you must allow Veeam Backup & Replication to fail over to the regular backup scenario that uses software VSS provider. To learn more about failover, see Integration Settings.
- Volumes greater than 64 TB are supported with limitations. For details, see Storage Snapshots on Volumes Greater than 64 TB.
- BitLocker encrypted volumes are supported with limitations. For details, see Storage Snapshots on BitLocker Encrypted Volumes.

Backup from Storage Snapshots

To create a backup from a storage snapshot, Veeam Backup & Replication and Veeam Agent do the following:

1. Veeam Backup & Replication checks that the hardware VSS provider is installed on the Veeam Agent computer.

   If the hardware VSS provider is not installed, Veeam Backup & Replication rescans the Veeam Agent computer and installs the hardware VSS provider.

2. Veeam Backup & Replication starts a backup job session and sends a request to the storage system to create a native snapshot as a new LUN.

   If storage system fails to create a native snapshot within the time period allowed by VSS, Veeam Backup & Replication will behave according to the storage integration settings. Veeam Backup & Replication will complete the backup job with the *Failed* status or fail over to the regular backup scenario that uses software VSS provider.

   To learn more about VSS and its limitations, see this Microsoft article.

3. After a snapshot LUN is created, this LUN connects to Veeam Agent computer to finish VSS operations and record storage metadata.

4. Veeam Backup & Replication moves the snapshot LUN to the backup proxy.

5. Veeam Backup & Replication reads the snapshot LUN and transfers data from the backup proxy to the target repository.

   Keep in mind that if the snapshot LUN contains a dynamic volume, Veeam Backup & Replication reads all extents of this volume.

6. Veeam Backup & Replication completes the backup job session and deletes snapshot metadata from the storage and backup proxy.

After that, you can use backups created from storage snapshots for restore and administration tasks. For such Veeam Agent backups, Veeam Backup & Replication allows you to perform the same set of operations as for backups created with regular backup scenario that uses software VSS provider. To learn more, see Restoring Data from Veeam Agent Backups and Managing Veeam Agent Backups.

Storage Snapshots on Volumes Greater than 64 TB

By default, Veeam Agent can back up file systems that reside on a volume that is 64 TB or smaller, because Veeam Agent uses the Microsoft Software Shadow Copy Provider to create a volume shadow copy during the backup. But if you use Veeam Backup & Replication and Veeam Agent operating in the managed mode and you create backups from storage snapshots, you can back up volumes greater than 64 TB.

In addition to considerations and limitations listed in the Storage Snapshots Support, consider the following:

- You can back up volumes that are greater than 64 TB using only hardware VSS provider installed by Veeam Agent. In case of fail over to the regular backup scenario that uses software VSS provider, the backup job will fail.
- Your production system storage must support backup of the volume with the size that you plan to back up.
- We strongly do not recommend to back up Veeam Agent computer volumes (for example, system volume) together with volumes greater than 64 TB. Otherwise, the software VSS provider may locate the shadow copy storage area for Veeam Agent computer volumes on the volume greater than 64 TB. In this case, the backup job will fail and the OS running on the Veeam Agent computer may get a blue screen error.

Storage Snapshots on BitLocker Encrypted Volumes

You can use Veeam Backup & Replication and Veeam Agent for Microsoft Windows operating in the managed mode to create backups from storage snapshots located on volumes encrypted with Microsoft Windows BitLocker.

If volumes you want to back up are protected by Microsoft Windows BitLocker, do the following:

1. On the Veeam Agent computer, set BitLocker to automatically unlock volumes to which LUNs are mapped. For details, see this Veeam KB article.
2. On the backup proxy, perform the following operations:
    a. Connect volumes to which LUNs are mapped to the backup proxy.
    b. Set BitLocker to automatically unlock connected volumes on the backup proxy. For details, see this Veeam KB article.
    c. Disconnect volumes to which LUNs are mapped from the backup proxy.

If you plan to use several backup proxies, repeat step 2 for each backup proxy.

Consider the following:

- Automatic unlocking requires encryption of the system drive.
- If automatic unlocking is not set on the Veeam Agent computer, file indexing will not work during the backup process.
- If automatic unlocking is not set on the backup proxy, only volume-level restore to a new location is available. File-level restore and volume-level restore to the original location will fail.

Failover Cluster Support

You can use Veeam Agent for Microsoft Windows operating in the managed mode (within the Veeam Agent management scenario) to protect data processed by a failover cluster. Veeam Agent supports Windows Server Failover Clusters running on any of the supported Microsoft Windows Server OS versions. To learn the full list of versions, see System Requirements.

Veeam Agent supports data backup and restore for the following types of clusters:

- Windows File Server Failover Clusters
- Windows Server Failover Clusters that run the following applications:
  - Microsoft SQL Server 2008 SP4 or later

    Keep in mind that SQL Server Failover Cluster Instances and AlwaysOn Availability Groups are supported only for Microsoft SQL Server 2012 or later. For details about AlwaysOn Availability Groups, see Backup of AlwaysOn Availability Groups.
  - Microsoft Exchange Server 2010 or later

    Microsoft Exchange Database Availability Groups (DAGs) are supported. For details, see Backup of Database Availability Groups.

Limitations for Failover Cluster Support

Failover cluster support in Veeam Agent for Microsoft Windows has the following limitations:

- Backup of failover clusters is supported in Veeam Agent managed by Veeam Backup & Replication only. You cannot process a failover cluster by Veeam Agent operating in the standalone mode.
- Backup of CSV (Cluster Shared Volumes) is not supported. Cluster disks used as CSV are automatically excluded from backup.
- Active Directory-Detached Clusters are not supported.
- Backup of Storage Replica log volumes is not supported. Such volumes are automatically excluded from backup because of Microsoft VSS limitations. To learn more, see this Microsoft article.
- AlwaysOn Availability Groups based on SQL Server Failover Cluster Instances are not supported.
- AlwaysOn Clusterless Availability Groups are not supported.
- Distributed AlwaysOn Groups are not supported.

> **NOTE**
>
> Veeam Backup & Replication does not support simultaneous processing of Microsoft SQL Server transaction logs on SQL Server clustered instances with identical names. The limitation applies to clustered instances of different failover clusters as well.
>
> For example, you configure two backup jobs that process transaction logs of different clusters whose SQL clustered instances have identical names. In case these backup jobs run simultaneously, transaction logs will be processed only by the backup job that started first. The second backup job will not process transaction logs.

Backup and Restore of Failover Clusters

To process a cluster with Veeam Agent for Microsoft Windows, you must complete the following tasks:

1. In Veeam Backup & Replication, create a protection group that includes Active Directory objects and add to this protection group one of the following types of objects:
   - Cluster account of the failover cluster whose data you want to back up
   - Active Directory container that includes this cluster account

   To learn more, see Creating Protection Groups.
2. In Veeam Backup & Replication, configure a Veeam Agent backup job for a failover cluster. To add a failover cluster to the backup job, do the following:
   a. At the **Job Mode** step of the **New Agent Backup Job** wizard, select **Failover cluster**.
   b. At the **Computers** step of the wizard, add to the job the cluster account that you added to a protection group at the step 1. Alternatively, you can add to the job a container or protection group that includes this cluster account.

   To learn more, see Creating Agent Backup Job for Windows Computers.

IMPORTANT

- If a backup task within a Veeam Agent backup job that processes a failover cluster completes unsuccessfully or a new node is added to a cluster, Veeam Agent will create a full backup of all shared disks of the cluster during the next backup job run.
- You cannot create per-machine backup files with a Veeam Agent backup job that processes failover clusters because of cluster limitations. The backup job with failover clusters in the backup scope creates a separate backup file for each cluster.

Data Restore from Failover Cluster Backups

You can perform data restore tasks with failover cluster backups created by Veeam Agent. For example, you can restore entire volumes or individual folders and files from such backups.

Consider the following:

- When you restore data of a failover cluster, make sure that the cluster is added to the Veeam Backup & Replication inventory as part of a protection group.
- When you restore data of a clusters with shared disks, Veeam Agent does not restore data of a disk witness. During volume restore for shared disks of a cluster, the disk witness is not displayed at the **Disk Mapping** step of the **Volume Restore** wizard.

Backup Copy from Failover Cluster Backups

You can perform data copy tasks with failover cluster backups created by Veeam Agent to a secondary location.

When you copy failover cluster backups, consider the following:

- The network traffic will be higher compared to the traffic sent during the Veeam Agent backup job run.

- If you copy a failover cluster backup in the immediate mode, the job ignores the **Use per-machine backup files** option enabled for the backup repository and creates a single backup copy file for each cluster. If you copy a failover cluster backup in the periodic mode, the job will create backup copy files as set for the backup repository.

  To learn more, see the Per-Machine Backup Files section in the Veeam Backup & Replication User Guide.

To learn more about backup copy, see the Backup Copy section in the Veeam Backup & Replication User Guide.

Backup of Database Availability Groups

The procedure of adding a Microsoft Exchange Database Availability Group (DAG) to a Veeam Agent backup job differs depending on the type of the DAG that you want to process:

- For a regular DAG, the backup job configuration procedure is the same as for any failover cluster. To process a regular DAG, you must configure a Veeam Agent backup job for a failover cluster. To learn more, see Backup and Restore of Failover Clusters.
- For an IP Less DAG (a DAG without an Administrative Access Point), the backup job configuration procedure is similar to the same procedure for standalone servers. To process an IP Less DAG, you must create a protection group with all nodes of the IP Less DAG and add this protection group to the Veeam Agent backup job managed by the backup server. To learn more, see Creating Agent Backup Job for Windows Computers.

How It Works

During backup, Veeam Agent performs the following operations:

1. Veeam Agent detects Microsoft Exchange Server.

   Keep in mind that Veeam Agent performs the backup, but all pre-/post-backup operations are performed by the Exchange VSS Writer that is available on any Microsoft Exchange Server. To learn more about Exchange VSS Writer, see this Microsoft article.

   To learn more about Exchange data backups, see this Microsoft article.

2. Veeam Agent detects that server added to the backup scope is a part of a DAG.
   - For a regular DAG, Veeam Agent gets the list of all DAG servers and adds these servers to the backup job.

     If a set of servers included in a regular DAG changes between the job runs, Veeam Agent changes the backup scope accordingly.
   - For an IP less DAG, you must add all servers of an IP less DAG to the backup job manually.

     > **IMPORTANT**
     >
     > An IP less DAG does not have an Administrative Access Point. As a result, you must add all servers of an IP less DAG to the protection group manually. If a set of servers included in an IP less DAG changes between the job runs, you must update the backup scope manually as well. Otherwise, Veeam Agent will still back up all database files from all servers included into backup scope, but Microsoft Exchange Server will detect data inconsistency and skip the database processing.

3. Veeam Agent processes databases to prepare them for backup: Veeam Agent freezes databases, creates database snapshots, and returns databases to the initial state.

   DAG servers contain active and passive copies of each database. By default, the Exchange VSS Writer issues VSS freeze commands to passive database copies only. If all passive copies of the database are not available for some reason, the Exchange VSS Writer issues the VSS freeze command to the active copy of the database. This approach helps to ensure data consistency.

4. After the database processing is finished, Veeam Agent creates a transactionally consistent backup of all databases running on DAG servers. The backup will include all database files from all servers included into backup scope regardless of the database processing success.

   > **NOTE**
   >
   > Consider the following:
   >
   > - The Exhange VSS Writer cannot create a VSS snapshot of all databases at once. That is why Veeam Agent backs up DAG servers one by one.
   > - Veeam Agent backs up all active and passive copies of the database on all DAG servers. Otherwise, Veeam Agent will not be able to ensure data consistency as Microsoft Exchange transfers data from active copy to passive copies after some time.

5. Veeam Agent notifies the Exchange VSS Writer about successful backup. If required, the Exchange VSS Writer truncates logs on DAG servers.

   Log truncation is applied to all passive and active database copies. Veeam Agent uses the Exchange VSS Writer to truncate logs. However, you can set Veeam Agent to disable transaction logs or backup transaction logs with Veeam Agent in the backup job settings. To learn more, see Guest Processing Settings.

Backup of AlwaysOn Availability Groups

To process AlwaysOn Availability Group, you must complete the following tasks:

1. In Veeam Backup & Replication, create a protection group that includes Active Directory objects. Add to this protection group the cluster account of the failover cluster whose data you want to back up.
2. In Veeam Backup & Replication, configure a Veeam Agent backup job for a failover cluster. To add a failover cluster to the backup job, do the following:
   a. At the **Job Mode** step of the **New Agent Backup Job** wizard, select **Failover cluster**.
   b. At the **Computers** step of the wizard, add to the job the cluster account that you added to a protection group at the step 1. Alternatively, you can add to the job a container or protection group that includes this cluster account.
   c. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** option. Then click **Applications**. In the **Processing Settings** window, define processing settings. To learn more, see Application-Aware Processing.

   To learn more about the backup job configuration, see Creating Agent Backup Job for Windows Computers.

If you select to process transaction logs with the backup job in the **Processing Settings** window, Veeam Backup & Replication performs the following operations during an image-level backup:

1. Requests and analyzes information about databases that are included in the AlwaysOn Availability Groups.
2. Depending on the retrieved information, selects the VSS backup type for each computer: full backup (VSS_BT_FULL) or copy-only backup (VSS_BT_COPY). The copy-only backup is created if the computer represents a secondary node for at least one AlwaysOn Availability Group.

   To learn more about VSS backup types, see this Microsoft article.

Transaction Log Backup

You can enable transaction log backup in the **Processing Settings** window. To learn more, see Microsoft SQL Server Transaction Log Settings.

Transaction log backup can be performed only for those databases that were successfully backed up, on the primary or on the secondary node of AlwaysOn Availability Group. At each log processing interval, Veeam Backup & Replication chooses the AlwaysOn Availability Group node for which transaction logs will be backed up. Logs are backed up from one node of the AlwaysOn Availability Group.

To become a subject for a log backup, the node must meet the following criteria:

- The node is not subject to the limitations listed in Failover Cluster Support.
- The necessary Veeam Backup & Replication components must be installed on this node and the computer included in AlwaysOn Availability Group must be running. For more information on the necessary components, see How Microsoft SQL Server Log Backup Works.
- The database backup preferences settings must allow a backup of the node that you want to process. For example, if you want to back up the primary node, you must not exclude this node from a backup, or select the **Secondary only** option in the database backup preferences settings.
- Databases in the AlwaysOn Availability Groups for this node were successfully backed up for the last two processing intervals.

Backup of Linux Computers

To back up data of Linux computers, you can use Veeam Agent for Linux managed by Veeam Backup & Replication. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Backup Job and Snapshot Scripts

You can instruct Veeam Agent for Linux to run custom scripts within the backup job session. In contrast to the standalone version of the product that can run custom scripts on the Veeam Agent computer only, Veeam Agent for Linux operating in the managed mode supports the following types of scripts:

- Pre-freeze and post-thaw scripts executed on the Veeam Agent computer (for backup jobs that process servers)
- Pre-job and post-job scripts executed on the Veeam Agent computer
- Pre-job and post-job scripts executed on the backup server (for backup jobs managed by the backup server)

Pre-Freeze and Post-Thaw Scripts

Veeam Agent runs these scripts before and after creating a snapshot of the backed-up volume. For example, the pre-freeze script may quiesce the file system and application data to bring the Linux OS to a consistent state before Veeam Agent for Linux creates a snapshot. After the snapshot is created, the post-thaw script brings the file system and applications to their initial state.

You can specify pre-freeze and post-thaw script settings at the **Guest Processing** step of the **New Agent Backup Job** wizard. For details, see Backup Job and Snapshot Scripts.

During the backup job session, Veeam Backup & Replication uploads the scripts to each Veeam Agent computer added to the backup job and executes them on these computers. The scripts run in the same way as in the standalone version of Veeam Agent. To learn more, see the Backup Job Scripts section in the Veeam Agent for Linux User Guide.

Pre-Job and Post-Job Scripts on Veeam Agent Computer

Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to quiesce an application for the time when the backup job session runs on the Veeam Agent computer.

You can specify backup job script settings at the **Guest Processing** step of the **New Agent Backup Job** wizard. For details, see Backup Job and Snapshot Scripts.

During the backup job session, Veeam Backup & Replication uploads the scripts to each Veeam Agent computer added to the backup job and executes them on these computers. The scripts run in the same way as in the standalone version of Veeam Agent. To learn more, see the Backup Job Scripts section in the Veeam Agent for Linux User Guide.

Keep in mind that scripts of this type are supported for computers that run Veeam Agent for Linux 4.0 and later only. Earlier versions of Veeam Agent for Linux do not run pre-job and post-job scripts obtained from the backup server.

Pre-Job and Post-Job Scripts on Backup Server

Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to throttle activities of some resource-consuming services on the backup server during the backup process.

You can specify backup job script settings at the **Storage** step of the **New Agent Backup Job** wizard. For details, see Script Settings.

During the backup job session, Veeam Backup & Replication executes the scripts on the backup server. The scripts are executed on the backup server under the account under which the Veeam Backup Service runs (the local System account or account that has the local Administrator permissions on the backup server).

Script Execution Order

If you specify both pre-job and post-job scripts that run on the backup server and pre-job and post-job scripts that run on the Veeam Agent computer, the scripts will be executed in the following order:

1. Pre-job script on the backup server
2. Pre-job script on the Veeam Agent computer
3. Pre-freeze script
4. Post-thaw script
5. Post-job script on the Veeam Agent computer
6. Post-job script on the backup server

Backup of Database Systems

You can instruct Veeam Agent for Linux to create consistent backups of Veeam Agent computers that run one of the following database systems:

- Oracle database system
- MySQL database system
- PostgreSQL database system

To learn more, see the Backup of Database Systems section in the Veeam Agent for Linux User Guide.

Backup of Unix Computers

Starting from build 11.0.1.1261, you can use Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX managed by Veeam Backup & Replication to back up data of Unix computers. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Veeam Backup & Replication is required for the following tasks that are critical for the Unix computers protection:

- Configuration of the protection group for pre-installed Veeam Agents that is the only applicable group for Unix computers.
- Configuration of the backup policy for Veeam Agent for Unix.

Keep in mind that you must deploy Veeam Agent for Unix on the Unix computer using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

Backup Job Scripts

You can instruct Veeam Agent for Unix to run custom scripts within the backup job session.

Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to quiesce an application for the time when the backup job session runs on the Veeam Agent computer.

You can specify backup job script settings at the **Guest Processing** step of the **New Agent Backup Job** wizard. For details, see Backup Job Scripts.

During the backup job session, Veeam Backup & Replication uploads the scripts to each Veeam Agent computer added to the backup job and executes them on these computers. The scripts run in the same way as in the standalone version of Veeam Agent. To learn more, see the following sections:

- The Backup Job Scripts section in the Veeam Agent for IBM AIX User Guide.
- The Backup Job Scripts section in the Veeam Agent for Oracle Solaris User Guide.

Backup of macOS Computers

To back up data of macOS computers, you can use Veeam Agent for Mac together with Veeam Backup & Replication. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Veeam Backup & Replication is required for the following tasks that are critical for the macOS computer protection:

- Configuration of the protection group for pre-installed Veeam Agents that is the only applicable group for macOS computer.
- Configuration of the backup policy for Veeam Agent for Mac.

Keep in mind that you must deploy Veeam Agent for Mac on the macOS computer using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

Backup to Veeam Cloud Connect Repository

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

Getting Started

To back up Veeam Agent computer data to a cloud repository, you must complete the following steps:

1. Add the SP in the Veeam backup console. To do this, you must provide credentials of the tenant account that you obtained from the SP. For details, see the Connecting to Service Providers section in the Veeam Cloud Connect Guide.
2. Create Veeam Agent backup job or policy and specify a cloud repository as a target location for backup files. For details, see Creating Veeam Agent Backup Jobs.
3. In case some Veeam Agent computer data becomes missing or corrupted, you can restore the necessary data from the cloud. To learn more, see Restore Tasks with Veeam Agent Backups in Cloud Repository.

NOTE

Consider the following:

- In the Veeam Agent management scenario, you do not need to create subtenant accounts to connect Veeam Agent computers to the Veeam Cloud Connect infrastructure on the SP side. To learn more, see How It Works.
- If you plan to back up Veeam Agent computer data to the cloud using a backup policy, you must not connect to the SP using credentials of a vCloud Director tenant account. Veeam Backup & Replication does not support creating managed subtenant accounts for tenant accounts of this type.
- Veeam Agents must trust the TLS certificate obtained from the SP in the same way as Veeam Backup & Replication. If you accept the certificate as trusted in Veeam Backup & Replication, Veeam Agents will trust it automatically as well. If you set up the trust relationship on the Veeam backup server, you must also do this on all Veeam Agent computers that you plan to back up to the cloud repository.

How It Works

There are 2 scenarios for data backup to the cloud with Veeam Agent operating in the managed mode:

- Scenario 1: backup to the cloud with a backup job managed by the backup server. In this scenario, the backup process is similar to the same process for VM backup to a cloud repository.
- Scenario 2: backup to the cloud with a backup policy. In this scenario, the backup process is similar to the same process for Veeam Agent operating in the standalone mode.

Scenario 1. Backup to Cloud with Backup Job

In the scenario where you use a backup job managed by the backup server to back up Veeam Agent computer data to the cloud, backup is performed in the following way:

1. The tenant adds the SP in the Veeam backup console on the tenant backup server.

2. The tenant creates a Veeam Agent backup job managed by the backup server. The backup job is targeted at a cloud repository.
3. The backup job operates in the similar way as in the regular Veeam Cloud Connect Backup scenario. The difference is that Veeam Backup & Replication processes Veeam Agent computer data instead of VM data. To learn more about backup to a cloud repository, see the How Cloud Repository Works section in the Veeam Cloud Connect Guide.

Scenario 2. Backup to Cloud with Backup Policy

In the scenario where you use a backup policy to back up Veeam Agent computer data to the cloud, backup is performed in the following way:

1. The tenant adds the SP in the Veeam backup console on the tenant backup server.
2. The tenant creates a backup policy targeted at a cloud repository.
3. For each Veeam Agent computer added to the backup policy, Veeam Backup & Replication automatically creates a managed subtenant account. To learn more, see the Managed Subtenant Account section in the Veeam Cloud Connect Guide.
4. Backup jobs that run on Veeam Agent computers added to the backup policy operate in the similar way as in the standalone version of Veeam Agent. Veeam Agent connects to the SP under the managed subtenant account and transfers the backed-up data to the cloud repository.

Restore Tasks with Veeam Agent Backups in Cloud Repository

You can use the Veeam backup console to perform the following data restore tasks with Veeam Agent backups in a cloud repository:

- Restore computer volumes from a Veeam Agent backup (for backups of Microsoft Windows computers only).
- Restore individual files and folders from a Veeam Agent backup (for backups of Microsoft Windows computers only).
- Restore application items from a Veeam Agent backup with Veeam Explorers (for backups of Microsoft Windows computers only).
- Export computer disks as VMDK, VHD or VHDX disks.
- Export a specific restore point in a Veeam Agent backup to a full backup (VBK) file.

You cannot restore data from a Veeam Agent backup in the cloud repository to a VMware vSphere or Microsoft Hyper-V VM, Amazon EC2 and Microsoft Azure.

Limitations for Veeam Agent Backup to Cloud Repository

To learn about limitations for Veeam Cloud Connect Backup, see the Limitations for Cloud Repository section in the Veeam Cloud Connect Guide.

Planning and Preparation

Before you start using the Veeam Agent management functionality in Veeam Backup & Replication, make sure that the Veeam backup server and computers that you plan to protect with Veeam Agent for Microsoft Windows and/or Veeam Agent for Linux meet the system requirements and all required ports are open.

Considerations and Limitations

Before you start using the Veeam Agent management functionality in Veeam Backup & Replication, consider the following:

1. If you have already been using Veeam Agents with Veeam Backup & Replication, after you start managing this Veeam Agent with Veeam Backup & Replication, Veeam Agent will start a new backup chain on a target location. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
2. You cannot map a Veeam Agent backup job or backup policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.

System Requirements

Make sure that components in the Veeam Agent management infrastructure meet system requirements listed below.

Veeam Backup Server

To learn about system requirements for the Veeam backup server and other Veeam Backup & Replication components, see the System Requirements section in the Veeam Backup & Replication User Guide.

Veeam Agent Computer (Microsoft Windows)

A computer that you want to protect with Veeam Agent for Microsoft Windows must meet the following requirements:

Specification	Requirement
Hardware	CPU: x86-64 processor. Memory: 2 GB RAM or more. Memory consumption varies depending on number and size of processed disks. Disk Space: 200 MB for product installation. Network: 1 Mbps or faster[1]. System firmware: BIOS or UEFI. Drive encryption: Microsoft BitLocker (optional)[2]. [1] High latency and reasonably unstable WAN links are supported. [2] BitLocker encrypted volumes must be unlocked at the moment when Veeam Agent for Microsoft Windows starts the backup or restore operation. Only Microsoft BitLocker is supported for drive encryption. Other drive encryption products are not supported.

Specification	Requirement
OS	Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported[1,2,3]: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server Semi-Annual Channel (from version 1803 to version 20H2) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1[4] • Microsoft Windows 11 (version 21H2) • Microsoft Windows 10 Semi-Annual Channel (from version 1803 to version 21H2)[5] • Microsoft Windows 10 Long-Term Servicing Channel (versions 1507, 1607 and 1809) • Microsoft Windows 8.1 • Microsoft Windows 7 SP1 Each Veeam Agent computer that consumes a license installed in Veeam Backup & Replication must have a unique BIOS UUID. [1] Starting from Veeam Backup & Replication 11a (build 11.0.1.1261), support of the following OS versions is added: Microsoft Windows Server 2022, Microsoft Windows 10 version 21H1. For Veeam Backup & Replication 11a (build 11.0.1.1261) with Cumulative Patch P20211211) installed, support of Windows 10 version 21H2 and Windows 11 version 21H2 is added. [2] Running Veeam Agent on Insider versions of Microsoft Windows Client and Server OSes is not supported. [3] Server Core installations of Microsoft Windows Server OSes can be backed-up only by Veeam Agent backup jobs managed by the Veeam backup server. [4] Veeam CBT driver is supported only if Microsoft Windows update KB3033929 is installed on the Veeam Agent computer. [5] Microsoft Windows 10 Education is supported starting from build 10586 and later.
File System	Microsoft Windows FAT, NTFS, ReFS file systems are supported. The supported file system must reside on a volume that is 64 TB or smaller, because Veeam Agent uses the Microsoft Software Shadow Copy Provider to create a volume shadow copy during the backup. To learn more about the limitation, see this Microsoft article.

Specification	Requirement
Microsoft SQL Database	Microsoft SQL Server 2012 SP4 Express LocalDB Edition. Microsoft SQL Server is installed within the Veeam Agent deployment process only if you added the target computer to the backup policy. To learn more, see Backup Policy.
Software	The following required 3rd party software is included in the Veeam Agent for Microsoft Windows Redistributable. During the Veeam Agent deployment process, Veeam Backup & Replication checks whether all prerequisite software is available on the target computer. If some of the required software components are missing, Veeam Backup & Replication will install missing software automatically. • Microsoft .NET Framework 4.5.2 • Microsoft SQL Server 2012 Management Objects[1] • Microsoft SQL Server System CLR Types[1] • Windows Universal C Run-Time Library [1] The component is installed only together with Microsoft SQL Server.

Veeam Agent for Microsoft Windows works with only those hard drive types that are supported by the Microsoft Windows OS. Thus, Veeam Agent supports the 512 bytes and 4 KB sector hard drives only. Other hard drive types are not supported. To learn more, see this Microsoft article.

Veeam Agent Computer (Linux)

A computer that you want to protect with Veeam Agent for Linux must meet the following requirements:

Specification	Requirement
Hardware	CPU: x86-64 processor (i386 or later). Memory: 1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data. Disk Space: 100 MB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target. System firmware: BIOS or UEFI. Disk layout: MBR or GPT. For virtual machines: Only full virtualization type is supported. Containers and paravirtualized instances are not supported. Oracle VM virtual machines are supported with limitations.

Specification	Requirement
OS	**IMPORTANT!** Check considerations and limitations that apply to the list of supported OSes. Linux kernel version 2.6.32 or later is supported. Both 64-bit and 32-bit versions (if applicable) of the following distributions are supported[1]: • Debian 9.0 – 11.1 • Ubuntu 14.04, 16.04, 18.04, 20.04, 20.10, 21.04, 21.10 • RHEL 6.0 – 8.5 • CentOS 7.0 – 8.5 • Oracle Linux 6 – 8.5 (RHCK) • Oracle Linux 6 (starting from UEK R2) – Oracle Linux 8 (up to UEK R6 U2, kernel version 5.4.17-2102) • SLES 11 SP4, 12 SP2 – 15 SP3 • SLES for SAP 11 SP4, 12 SP2 – 15 SP3 • Fedora 33, 34, 35 • openSUSE Leap 15.2 – 15.3 • openSUSE Tumbleweed [1] Starting from Veeam Backup & Replication 11a (build 11.0.1.1261), support of the following OS versions is added: Debian 11, Ubuntu 21.04, RHEL 8.4, CentOS 8.4, Oracle Linux 8.4 (RHCK), Oracle Linux UEK R6 U1, UEK R6 U2 (up to kernel version 5.4.17-2102), SLES 15 SP3, SLES for SAP 15 SP3, Fedora 33, 34, openSUSE Leap 15.3. For Veeam Backup & Replication 11 (build 11.0.1.1261) with Cumulative Patch P20211211) installed, support of the following OS versions is added: Ubuntu 21.10, RHEL 8.5, CentOS 8.5, Oracle Linux 8.5 (RHCK), Fedora 35.

Specification	Requirement
File System	**IMPORTANT!** Check considerations and limitations that apply to the list of supported file systems. Veeam Agent for Linux supports consistent snapshot-based data backup for the following file systems[1]: • Btrfs (for OSes that run Linux kernel 3.16 or later) • Ext 2/3/4 • F2FS • FAT16 • FAT32 • HFS • HFS+ • JFS • NILFS2 • NTFS • ReiserFS • XFS The supported file system (except for Btrfs) can reside on a simple volume or LVM2 volume; volumes protected with encryption software such as dm-crypt are supported. Btrfs is supported only if it resides directly on a physical device with no additional abstraction layers (such as LVM, software RAID, dm-crypt and so on) below or above it. Data that resides on other file systems and volumes (including NFS and SMB shares) can be backed up using the snapshot-less mode. For details, see the Snapshot-Less File-Level Backup section in the Veeam Agent for Linux User Guide.

Specification	Requirement
Software	**IMPORTANT!** Check considerations and limitations that apply to the list of supported components. Protected computer must have the following components installed: • dkms • gcc • make • perl • linux-headers (for Debian-based systems) • kernel-headers (for RedHat-based systems) • kernel-devel (for RedHat-based systems) • libudev • libacl • libattr • lvm2 • libfuse • libncurses5 • dmidecode • libmysqlclient • libpq5 • python3 • efibootmgr (for UEFI-based systems) • isolinux (for Debian-based systems) • syslinux (for RedHat-based systems) • btrfs-progs (for backup of Btrfs file system) • mksquashfs (for custom Veeam Recovery Media) • unsquashfs (for custom Veeam Recovery Media) • wget (for custom Veeam Recovery Media) • xorriso (for custom Veeam Recovery Media with EFI support) For file system indexing, the following utilities are required: `mlocate`, `gzip` and `tar`. These utilities are provided along with the product in the product installation media.

Considerations and Limitations (Linux)

OS

- Linux kernel version 2.6.32 or later is supported as long as you use kernels supplied by your distribution. Consider the following limitations:
  - Fedora and openSUSE Tumbleweed are supported up to kernel 5.15.7.
  - Linux kernel 2.6.32-754.6.3 in RHEL and Oracle Linux (RHCK) is not supported.
  - If you work with the Veeam Agent for Linux 5.0 build earlier than 5.0.1.4493 and the protected computer is running Linux kernel version 5.8 or later, only snapshot-less file-level backup is supported.
- Only GA versions of the supported distributions that have been released before the current version of Veeam Agent for Linux are supported.
- The Linux OS must be set up to receive software updates from the default repositories enabled in the OS after installation.
- For cloud-based installations that use customized kernels (such as Linux distributions deployed from AWS Marketplace or Azure Marketplace), the `veeamsnap` kernel module has experimental support status. For details about experimental support, see this Veeam KB article.
- Automatic Veeam Agent deployment from the Veeam backup console is not supported for the following distributions:
  - Fedora 33, 34, 35
  - openSUSE Tumbleweed

  You need to install Veeam Agent for Linux directly on a target computer. For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.
- RHEL, CentOS, and Oracle Linux (RHCK) are supported up to certain kernel versions. For details, see this Veeam KB article.
- Ubuntu 21.10 minimal install is not supported.

File System

- Veeam Agent for Linux does not back up volumes that reside on USB devices and SD cards.
- Total size of all file systems included in a file-level backup must not exceed 218 TB. Size of a file included in a file-level backup must not exceed 16 TB.
- Veeam Agent supports backup of extended attributes with the following limitations:
  - Veeam Agent backs up extended attributes only with the following public namespaces: system, security, trusted, and user.
  - All extended attribute names and values of a file must not exceed 4096 bytes (size of a default ext4 file system block). Veeam Agent does not back up attributes exceeding the limit.

    For the kernel version 4.13 or later, if a value of extended attribute exceeds the limit, Veeam Agent uses the *ea_inodes* feature. Backups created using the *ea_inodes* feature cannot be mounted on kernel versions up to 4.12.
- Backup of file and directory attributes (for example, a — append only, c — compressed, and so on) is not supported.

- Each volume included in a backup must have a unique UUID.
- The `veeamsnap` module provides RAM-based changed block tracking (CBT) mechanism. Every time the module is unloaded or Veeam Agent for Linux computer is rebooted, CBT data is reset. As a result, Veeam Agent reads the entire data added to the backup scope to detect what blocks have changed since the last job session, and incremental backup requires greater time.
- You cannot back up an entire system image or specific volumes of computers used as cluster nodes. Only snapshot-less file-level backup of cluster nodes is supported. That includes backup of computers that use shared disks, clustered file systems, or clustered LVM.
- Certain limitations for EMC PowerPath configuration apply. To learn more, see this Veeam KB article.
- BFQ I/O scheduler is not supported.
- Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.

Software

> **IMPORTANT**
>
> Linux user account used to work with Veeam Agent for Linux installed on the protected computer must have the `/bin/bash` shell set as the default shell.

- To install Veeam Agent for Linux packages on a target computer, Veeam Backup & Replication uses the default package manager of the Linux distribution running on this computer. During the installation process, the package manager checks whether all prerequisite software is available on the computer. If some of the required software components are missing, the package manager will attempt to install the missing packages from a software repository configured in the OS.
- The following packages are not required for CentOS, RHEL and SLES distributions if a pre-built binary `veeamsnap` package is to be installed.
  - dkms
  - gcc
  - make
  - perl
  - kernel-headers (for RedHat-based systems)
  - kernel-devel (for RedHat-based systems)

  For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.
- Version of the following packages varies according to the Linux kernel version that you use:
  - linux-headers (for Debian-based systems)
  - kernel-headers (for RedHat-based systems)
  - kernel-devel (for RedHat-based systems)
- For openSUSE and SLES distributions, either of the following packages is required: `libncurses5` or `libncurses6`.

- The `dmidecode` package is required for Veeam Agent management — a valid BIOS UUID must be obtainable either from `dmidecode | grep -i uuid` or from `/sys/class/dmi/id/product_uuid`. Each Veeam Agent that consumes a license installed in Veeam Backup & Replication must have a unique BIOS UUID. If a valid UUID cannot be obtained, Veeam will generate it automatically.
- The `libmysqlclient` package is required to process MySQL database system located on the Veeam Agent server. Package version varies according to the MySQL database system version that you use.
- The `libpq5` package is required to process PostgreSQL database system located on the Veeam Agent server.
- The `python3` package or another RPM package providing a `/usr/bin/python3` binary is required for CentOS, RHEL 7.0 and later distributions if a pre-built binary `kmod-veeamsnap` package is to be installed.
- The `btrfs-progs` package version 3.16 or later is required.
- The `lvm2` package version up to 2.03.12 is required. Later versions are not supported.

Veeam Agent Computer (IBM AIX)

A computer that you want to protect with Veeam Agent for IBM AIX must meet the following requirements:

Specification	Requirement
Hardware	Memory: 1 GB RAM. For information about RAM requirements for backup of a great number of files, see the RAM Requirements for Large-Scale Environments section in the Veeam Agent for IBM AIX User Guide. Disk space: 1.5 GB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target.
OS	All versions of the IBM AIX operating system starting from IBM AIX 6.1 are supported. **Note:** • IBM AIX 6.1 is supported starting from Technology Level 5 (TL 5). • Backup of a Virtual I/O Server (VIOS) is not supported. • Only GA versions of the IBM AIX operating system that have been released before the Veeam Agent for IBM AIX 3.0 are are supported.
File System	All file systems supported by the supported operating systems. **Note:** • Total size of all file systems included in a file-level backup must not exceed 128 TB. • Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files. • JFS external snapshots are not supported.

Specification	Requirement
Software	For file system indexing, the following utilities are required: `mlocate`, `gzip` and `tar`. These utilities are provided along with the product in the product installation media.

Veeam Agent Computer (Oracle Solaris)

A computer that you want to protect with Veeam Agent for Oracle Solaris must meet the following requirements:

Specification	Requirement
Hardware	CPU: Oracle SPARC or Intel x86 processor. Memory: 1 GB RAM. For information about RAM requirements for backup of a great number of files, see the RAM Requirements for Large-Scale Environments section in the Veeam Agent for Oracle Solaris User Guide. Disk space: 150 MB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target.
OS	Oracle Solaris 10 – 11.4 operating systems on machines based on the SPARC and Intel x86 architecture are supported. **Note:** Only GA versions of the Oracle Solaris OS that have been released before the Veeam Agent for Oracle Solaris version 3.0 are supported.
File System	All file systems supported by the supported operating systems. **Note:** • Total size of all file systems included in a file-level backup must not exceed 218 TB. • Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.
Software	For file system indexing, the following utilities are required: `mlocate`, `gzip` and `tar`. These utilities are provided along with the product in the product installation media.

Veeam Agent Computer (macOS)

A computer that you want to protect with Veeam Agent for Mac must meet the following requirements:

Specification	Requirement
Hardware	The protected macOS computer must meet the following hardware requirements: • CPU: x64 or ARM Apple-branded hardware* • Disk Space: 200 MB free disk space for product installation • Network: 10 Mbps or faster network connection to a backup target * On a macOS computer with the ARM Apple-branded hardware, the product is running using the Rosetta Translation Environment.
OS	Veeam Agent supports the following macOS versions: • Big Sur 11.6.X • Catalina 10.15.X • Mojave 10.14.X • High Sierra 10.13.6
File System	Veeam Agent supports consistent data backup with snapshot for the APFS file system. The following file systems can be backed up in the snapshot-less mode: • HFS+ • MS-DOS (FAT) • exFAT • NTFS • FAT32 • SMB Consider the following: • Sortware RAID is not supported. • Total size of all file systems included in a file-level backup must not exceed 128 TB. Size of a file included in a file-level backup must not exceed 16 TB.

Backup Target

Backup can be performed to the following types of storage:

For Veeam Agent backup jobs managed by the backup server

- Veeam Backup & Replication 11 or later backup repository
- Veeam Cloud Connect 11 or later cloud repository

For Veeam Agent backup jobs managed by Veeam Agent

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

  > **IMPORTANT**
  >
  > [For Veeam Agent for Microsoft Windows] We do not recommend targeting a backup job at the storage device with the exFAT file system. If the protected computer runs Microsoft Windows 10 or Microsoft Windows Server 2019 and later, this configuration may lead to the backup data corruption caused by the exFAT file system issue.

- Network Attached Storage (NAS) able to represent itself as an SMB (CIFS) share
- Network Attached Storage (NAS) able to represent itself as an NFS share (for backups of Linux and Unix computers only)
- Veeam Backup & Replication 11 or later backup repository
- Veeam Cloud Connect 11 or later cloud repository (excluding backups of Unix computers)

Network

Consider the following:

- Veeam Agent should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Agent cannot work with Veeam Backup & Replication that is located behind the NAT gateway.
- Domain names of all managed servers added to the Veeam backup infrastructure and computers you want to back up must be resolvable into IPv4 addresses.

> **TIP**
>
> For Veeam Agent computers that are included in a protection group for pre-installed Veeam Agents, only Veeam Backup & Replication server must be resolvable into IPv4 address.

Licensing Requirements

The Veeam Agent management functionality is licensed by the number of instances. Instances are units (or tokens) that you can use to protect your computers (servers and workstations) with Veeam Agents. The number of instances that you can use depends on the type of license installed in Veeam Backup & Replication:

- *Per-instance license*. If you use a per-instance license in Veeam Backup & Replication, the number of servers and workstations that you can process with Veeam Agents depends on the edition of Veeam Backup & Replication and the number of instances in the license. For more information, see Veeam Licensing Policy.
- *Per-socket license*. If you use a perpetual per-socket license in Veeam Backup & Replication, the product allows you to use up to 6 instances to process Veeam Agents. If the number of sockets in your license is less than 6, you can use the number of instances that equals the number of sockets in the license. For example, if the number of sockets in the license is 5, you can use 5 instances. If the number of sockets in the license is 7, you can use 6 instances.

  Note that you can use Veeam Agents to protect VMs residing on a virtualization host that consumes a per-socket license. In this scenario, Veeam Agents will not consume instances in the license.
- *Community edition*. If you do not install a license in Veeam Backup & Replication, you can use the Community edition of the product. The Community edition of Veeam Backup & Replication allows you to use 10 instances. Functionality available in the Community edition of Veeam Backup & Replication is the same as in the Standard edition of the product.

  Keep in mind that you cannot use Veeam Agent for Unix to protect Unix computers with the Community edition of the product. To protect such computers, you must use Enterprise Plus edition of the product.

For more information on Veeam Backup & Replication licensing, see the Licensing section in the Veeam Backup & Replication User Guide.

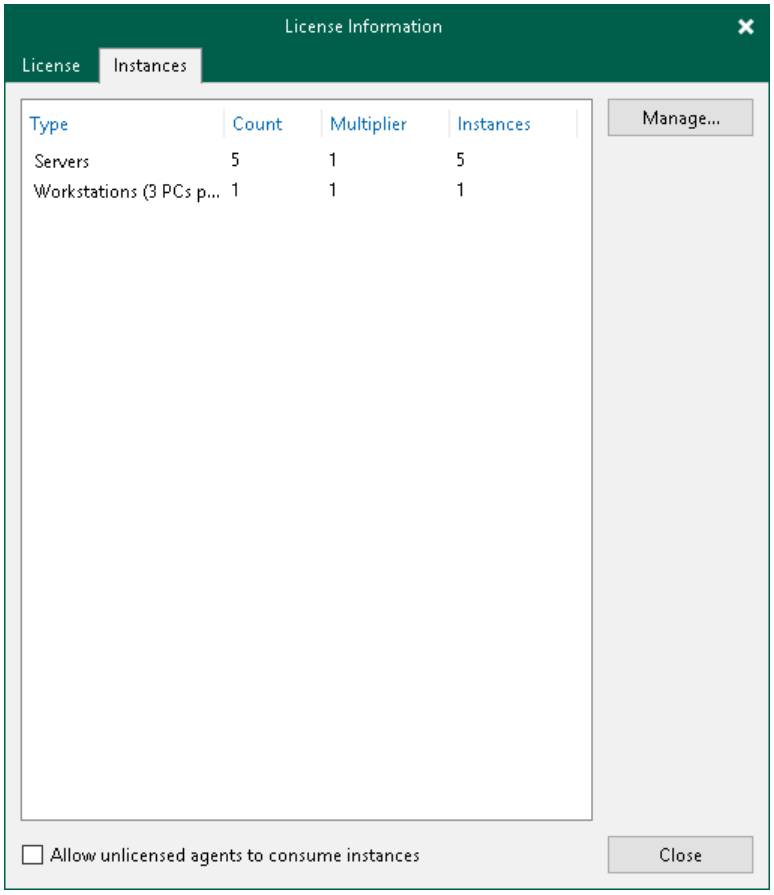
Managing Instance Consumption by Veeam Agents

After Veeam Agent connects to the Veeam backup server, Veeam Agent starts using instances in the license. You can restrict license consumption for Veeam Agents, for example, if you want to use Veeam Backup & Replication to process VMs and do not want Veeam Agents to use instances in the license.

To restrict instance consumption by Veeam Agents:

1. From the main menu, select **License**.
2. In the **License Information** window, click the **Instances** tab.
3. On the **Instances** tab, clear the **Allow unlicensed agents to consume instances** check box.

4. Click **Close**.



Supported Applications

Veeam Agent for Microsoft Windows

You can use Veeam Agent for Microsoft Windows operating in the managed mode to create transactionally consistent backups of servers running applications that support Microsoft VSS. System requirements for VSS-aware processing are listed in the following table.

Specification	Requirement
Microsoft Active Directory Domain Controllers	The following versions of Microsoft Active Directory Domain Services servers (domain controllers) are supported: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 Minimum supported domain and forest functional level is Windows 2003.
Microsoft Exchange	The following versions of Microsoft Exchange are supported: • Microsoft Exchange 2019 • Microsoft Exchange 2016 • Microsoft Exchange 2013 SP1 • Microsoft Exchange 2013 • Microsoft Exchange 2010 SP1 to SP3
Microsoft SharePoint	The following versions of Microsoft SharePoint are supported: • Microsoft SharePoint 2019 • Microsoft SharePoint 2016 • Microsoft SharePoint 2013 • Microsoft SharePoint 2010 All editions are supported (Foundation, Standard, Enterprise).

Specification	Requirement
Microsoft SQL Server	The following versions of Microsoft SQL Server are supported: • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2008 SP4 • Microsoft SQL Server 2005 SP4 All editions of Microsoft SQL Server except LocalDB are supported.
Oracle	Oracle Database versions 11g to 21c are supported for the following operating systems (32-bit and 64-bit architecture): • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 For information about OS requirements for particular Oracle Database versions, see Oracle documentation. **IMPORTANT!** • Automatic Storage Management (ASM) is not supported. • Oracle Real Application Clusters (RAC) are not supported. • Oracle Database systems running on Microsoft Windows Failover Clusters are not supported. • Oracle servers using Data Guard are not supported. • Oracle Database Express Edition is supported. • Configurations with different versions of Oracle Database deployed on the same server are not supported. • 32-bit Oracle running on 64-bit operating systems is not supported.

Veeam Agent for Linux

You can use Veeam Agent for Linux operating in the managed mode to create transactionally consistent backups of servers running Oracle database systems. System requirements for Oracle database processing are listed in the following table.

Specification	Requirement
Oracle	• Oracle Database versions 11g to 21c are supported for all operating systems supported by Veeam Agent for Linux. To learn more, see System Requirements. • Automatic Storage Management (ASM) is not supported. • Oracle Real Application Clusters (RAC) are not supported. • Oracle Grid Infrastructure is not supported. • Oracle Database Express Edition is not supported. • SAP on Oracle is not supported. • Oracle Database architectures with Data Guard and passive instances are not supported.
MySQL	• MySQL database system versions 5.6 to 8.0 are supported. • Configurations with multiple MySQL installations and/or instances on the same machine are not supported. • MySQL Cluster versions are not supported.
PostgreSQL	• PostgreSQL database system versions 9.5 to 14.0 are supported. • Configurations with multiple PostgreSQL installations and/or instances on the same server are not supported.

Supported Veeam Agents

The following tables describe what Veeam Agents are supported by the Veeam Backup & Replication depending on the product usage scenario.

Supported versions of Veeam Agents differs depending on the Veeam Backup & Replication version that you use:

- Veeam Backup & Replication 11a with Cumulative Patch P20211211
- Veeam Backup & Replication 11a
- Veeam Backup & Replication 11

Veeam Backup & Replication 11a (build 11.0.1.1261) with Cumulative Patch P20211211 installed supports the following Veeam Agents:

Scenario	Veeam Agent for Microsoft Windows Version	Veeam Agent for Linux Version	Veeam Agent for IBM AIX Version	Veeam Agent for Oracle Solaris Version	Veeam Agent for Mac Version	Description
Veeam Agent backup	4.0 and later	4.0 and later	3.0	3.0	1.0 and later	Veeam Backup & Replication 11a supports backup operations for these Veeam Agent versions.
Automated Veeam Agent deployment or upgrade from the Veeam backup console	5.0.2	5.0.2	N/A	N/A	N/A	If you set up Veeam Backup & Replication 11a to deploy or upgrade Veeam Agents on protected computers included in a protection group, these Veeam Agent versions are deployed. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.
Manual Veeam Agent deployment using external tools	5.0.2	5.0.2	3.0	3.0	1.0.1	If you set up Veeam Backup & Replication 11a to generate Veeam Agent setup files for a manual installation, setup files for these Veeam Agent versions are generated. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

Veeam Backup & Replication 11a (build 11.0.1.1261) supports the following Veeam Agents:

Scenario	Veeam Agent for Microsoft Windows Version	Veeam Agent for Linux Version	Veeam Agent for IBM AIX Version	Veeam Agent for Oracle Solaris Version	Veeam Agent for Mac Version	Description
Veeam Agent backup	4.0 and later	4.0 and later	3.0	3.0	1.0 and later	Veeam Backup & Replication 11a supports backup operations for these Veeam Agent versions.
Automated Veeam Agent deployment or upgrade from the Veeam backup console	5.0.1	5.0.1	N/A	N/A	N/A	If you set up Veeam Backup & Replication 11a to deploy or upgrade Veeam Agents on protected computers included in a protection group, these Veeam Agent versions are deployed. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.
Manual Veeam Agent deployment using external tools	5.0.1	5.0.1	3.0	3.0	1.0.1	If you set up Veeam Backup & Replication 11a to generate Veeam Agent setup files for a manual installation, setup files for these Veeam Agent versions are generated. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

If you work with Veeam Backup & Replication 11 build earlier than 11.0.1.1261, Veeam Backup & Replication supports the following Veeam Agents:

Scenario	Veeam Agent for Microsoft Windows Version	Veeam Agent for Linux Version	Veeam Agent for Mac Version	Description
Veeam Agent backup	4.0 and later	4.0 and later	1.0 and later	Veeam Backup & Replication 11 supports backup operations for these Veeam Agent versions.
Automated Veeam Agent deployment or upgrade from the Veeam backup console	5.0	5.0	N/A	If you set up Veeam Backup & Replication 11 to deploy or upgrade Veeam Agents on protected computers included in a protection group, these Veeam Agent versions are deployed. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.

Scenario	Veeam Agent for Microsoft Windows Version	Veeam Agent for Linux Version	Veeam Agent for Mac Version	Description
Manual Veeam Agent deployment using external tools	5.0	5.0	1.0	If you set up Veeam Backup & Replication 11 to generate Veeam Agent setup files for a manual installation, setup files for these Veeam Agent versions are generated. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

Used Ports

The following tables describe network ports that must be opened to ensure proper communication of components in the Veeam Agent management infrastructure.

Veeam Backup & Replication Connections

For information about network ports that must be opened to ensure proper communication of the backup server with backup infrastructure components, see the Used Ports section in the Veeam Backup & Replication User Guide.

For information about ports that must be opened to ensure communication of the backup server with Veeam Cloud Connect infrastructure components, see the Used Ports section in the Veeam Cloud Connect Guide.

In addition to general port requirements applicable to a Veeam backup server, the backup server used in the Veeam Agent management scenario must have the following ports opened:

From	To	Protocol	Port	Notes
Veeam Backup Server	Veeam Agent Computer (Microsoft Windows)	TCP	6184+	Default port used for communication with theVeeam Agent for Microsoft Windows Service. If port 6184 is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.
		TCP UDP	135, 137 to 139, 445, 6160, 11731	Default ports used for communication with the Veeam Installer Service. Port 135 is used for WMI queries. WMI queries are mandatory to back up failover clusters and perform file-level restore and optional to provide faster Veeam Agent deployment. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS. Ports 137 to 139 and 445 are used during restore started from the Veeam Backup & Replication console. Ports 6160 and 11731 are used to deploy Veeam Agent on the computer and to provide faster restore. If the backup repository server role and the mount server role are assigned to different servers in your infrastructure, you must open ports described in the Mount Server Connections subsection of the Veeam Backup & Replication User Guide.

From	To	Protocol	Port	Notes
		TCP	2500 to 3300	[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer.
		TCP	6167, 2500 to 3300	[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer operating as part of a failover cluster with SQL Server AlwaysOn Availability Groups.
		TCP	6211	[For storage snapshots support] Port used for communication with the hardware VSS provider. For more information, see Storage Snapshots Support.
		TCP	6160, 11731	Port port used for the volume-level restore.
	Veeam Agent Computer (Linux)	TCP	22	Default port used as a control channel from the Veeam Backup Server to the Veeam Agent computer.
		TCP	6162	Default port used by the Veeam Data Mover.
		TCP	2500 to 3300	Default range of ports used for communication between Veeam Agent components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned.
	Distribution Server	TCP UDP	135, 137 to 139, 445, 6160, 11731	Ports on a Microsoft Windows server used for deploying the Distribution Server component. Port 135 is optional. This port is used to provide faster Veeam Agent deployment. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS. Ports 6160 and 11731 are used by the Veeam Installer Service. These ports together with port 445 are mandatory to deploy the Distribution Server component.

From	To	Protocol	Port	Notes
		TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.
		TCP	9380	Default port used for communication with the Veeam Distribution Service.
	Backup Proxy	TCP	6211	[For storage snapshots support] Port used for communication with the hardware VSS provider. For more information, see Storage Snapshots Support.
Distribution Server	Veeam Agent Computer (Microsoft Windows)	TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article. The port range is required for communication with the Veeam Installer Service.
		TCP UDP	6160, 11731	Ports on the Veeam Agent computer used for deploying Veeam Agent.
	Veeam Agent Computer (Linux)	TCP	22	Default port used to establish an SSH connection for the purpose of Veeam Agent packages transmission and deployment control.

Veeam Agent Computer Connections

From	To	Protocol	Port	Notes
Veeam Agent Computer (Microsoft Windows)	Veeam Backup Server	TCP	10005	Default port used by Veeam Agent for Microsoft Windows operating in the managed mode for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.

From	To	Protocol	Port	Notes
	Veeam Agent Computer (Microsoft Windows)	TCP	9395+, 6183+	Ports used locally on the Veeam Agent computer for communication between Veeam Agent components and Veeam Agent for Microsoft Windows Service. If port 9395 or 6183 is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.
Veeam Agent Computer (Linux, Unix, macOS)	Veeam Backup Server	TCP	10006	Default port used for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.
	Veeam Agent Computer (Linux, Unix, macOS)	TCP	2500 to 3300	Default range of ports used for communication between Veeam Agent components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned.
Communication with Veeam Backup & Replication Repositories				
Veeam Agent Computer	Linux server performing the role of a backup repository	TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
	Microsoft Windows server performing the role of a	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see this Microsoft KB article.

From	To	Protocol	Port	Notes
	backup repository	TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
	Shared folder CIFS (SMB) share	TCP UDP	137 to 139, 445	Ports used as a transmission channel from the Veeam Agent computer to the target CIFS (SMB) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.
	Gateway Microsoft Windows server	TCP UDP	137 to 139, 445	If a CIFS (SMB) share is used as a backup repository and a Microsoft Windows server is selected as a gateway server for this CIFS share, these ports must be opened on the gateway Microsoft Windows server. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.
		TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.
		TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Communication with Veeam Cloud Connect Repositories				
Veeam Agent Computer (Microsoft Windows, Linux, macOS)	Cloud gateway	TCP	6180	Port on the cloud gateway used to transport Veeam Agent data to the Veeam Cloud Connect repository.

From	To	Protocol	Port	Notes
	Certificate Revocation Lists	TCP	80 or 443 (most popular)	Veeam Agent computer needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the Veeam Cloud Connect service provider. Generally, information about CRL locations can be found on the CA website.

Getting Started

To start using the Veeam Agent management functionality in Veeam Backup & Replication, you must perform the following operations:

1. Deploy Veeam Backup & Replication.

   To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.

2. Configure security settings.

   By default, Veeam Backup & Replication offers the following settings to establish a secure connection between the backup server and protected computers:

   - To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed certificate.
   - Veeam Backup & Replication allows all new Linux hosts to establish a connection to the backup server.

   You can use the default security settings or change them if needed. To learn more, see Configuring Security Settings.

3. Add computers that you want to protect with Veeam Agents to the Veeam Backup & Replication inventory.

   In Veeam Backup & Replication, computers that you want to protect with Veeam Agents are organized into protection groups. You can use the Veeam Backup & Replication console to create one or more protection groups that include individual computers, Microsoft Active Directory objects or list of computers imported from a CSV file. To learn more, see Creating Protection Groups.

4. Discover protected computers and deploy Veeam Agents.

   Veeam Backup & Replication is set up to automatically discover protected computers and install Veeam Agent on a discovered computer. By default, these operations are performed immediately after you create a protection group. You can change Veeam Agent discovery and deployment options in the protection group settings, if needed. You can also run discovery and deployment operations manually for an entire protection group, individual Active Directory object in a protection group or individual computer in a protection group. To learn more, see Specify Discovery and Deployment Options, Working with Protection Groups and Managing Protected Computers.

5. Configure Veeam Agent backup job settings.

   You can configure one or more Veeam Agent backup jobs and add to these jobs one or more protection groups, Active Directory objects and/or individual computers. In Veeam Backup & Replication, you can configure the following types of Veeam Agent backup jobs:

   - Veeam Agent backup job managed by the Veeam backup server
   - Veeam Agent backup job managed by Veeam Agent, or Veeam Agent backup policy

   To learn more, see Creating Veeam Agent Backup Jobs.

6. Manage Veeam Agent backup jobs and policies.

   You can start, stop, enable and disable Veeam Agent backup jobs and policies to administer data protection operations on protected computers. To learn more, see Working with Veeam Agent Backup Jobs and Policies.

7. In case of a disaster, you can restore data from a Veeam Agent backup.

   To learn more, see Restoring Data from Veeam Agent Backups.

Configuring Security Settings

When you configure the Veeam Agent management infrastructure in Veeam Backup & Replication, you can specify what security settings Veeam Backup & Replication will use to establish a secure connection between the backup server and protected computers. By default, Veeam Backup & Replication offers the following security settings:

- To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed TLS certificate.
- Veeam Backup & Replication allows all computers that run a Linux OS to establish a connection to the backup server using the SSH fingerprint.

Keep in mind that default security settings are only for testing and evaluation purposes. To prevent potential security issues, you can change security settings. For example, you can use a custom TLS certificate and verification of Linux host SSH fingerprints.

To specify the security settings, do the following:

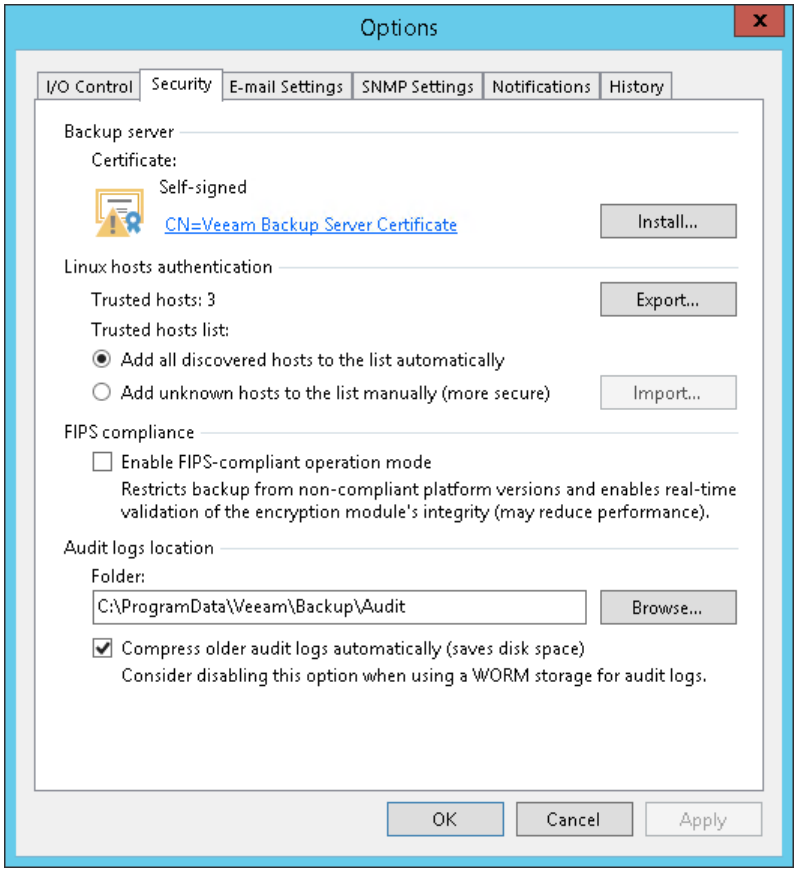
1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Certificate** section, check information about the currently used certificate. By default, Veeam Backup & Replication uses a self-signed TLS certificate generated during the Veeam Backup & Replication installation process. If you want to use a custom certificate, click **Install** and specify a new certificate. To learn more, see Managing TLS Certificates.

4. In the **Linux hosts authentication** section, specify how Veeam Backup & Replication will add Linux-based protected computers to the list of trusted hosts. You can select one of the following options:
   - **Add all discovered hosts to the list automatically** — with this option enabled, Veeam Backup & Replication allows all discovered computers that run a Linux OS to connect to the backup server. This scenario is recommended for demo environments only.
   - **Add unknown hosts to the list manually (more secure)** — with this option enabled, only the following Linux-based computers can connect to the backup server:
     - Protected computers that have already established a connection to the backup server and have their fingerprints stored in the Veeam Backup & Replication database. Veeam Backup & Replication displays the number of such computers in the **Trusted hosts** field. You can export the list of trusted Linux computers to a *known_hosts* file. To do this, click **Export** and specify a path to the folder to save the file.
     - Protected computers specified in the *known_hosts* file imported to Veeam Backup & Replication. To import a *known_hosts* file, click **Import** and specify a path to the folder where the file resides.
     - Protected computers added to the list of trusted hosts in the Veeam Backup & Replication console. To learn more, see Adding Computers to Trusted Hosts List.

   Computers that are not in the list of trusted hosts cannot connect to the Veeam backup server and download Veeam Agent for Linux installation packages during discovery.
5. Click **OK**.

TIP

To learn more about other security settings available on the **Security** tab, see the Configuring Security Settings section in the Veeam Backup & Replication User Guide.



Managing TLS Certificates

When you configure the Veeam Agent management infrastructure, you can specify what TLS certificate must be used to establish a secure connection between the backup server and protected computers. Veeam Backup & Replication offers the following options for TLS certificates:

- You can choose to keep the default self-signed TLS certificate generated by Veeam Backup & Replication.
- You can use Veeam Backup & Replication to generate a new self-signed TLS certificate. To learn more, see Generating Self-Signed Certificates.
- You can select an existing TLS certificate from the certificates store. To learn more, see Importing Certificates from Certificate Store.
- You can import a TLS certificate from a file in the PFX format. To learn more, see Importing Certificates from PFX Files.

> **NOTE**
>
> If you plan to use a certificate issued by your own Certificate Authority (CA), make sure that the certificate meets the requirements. To learn more, see Using Certificate Signed by Internal CA.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Agent management infrastructure.

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the Veeam backup server. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

- User who created the TLS certificate
- LocalSystem user account
- Local Administrators group

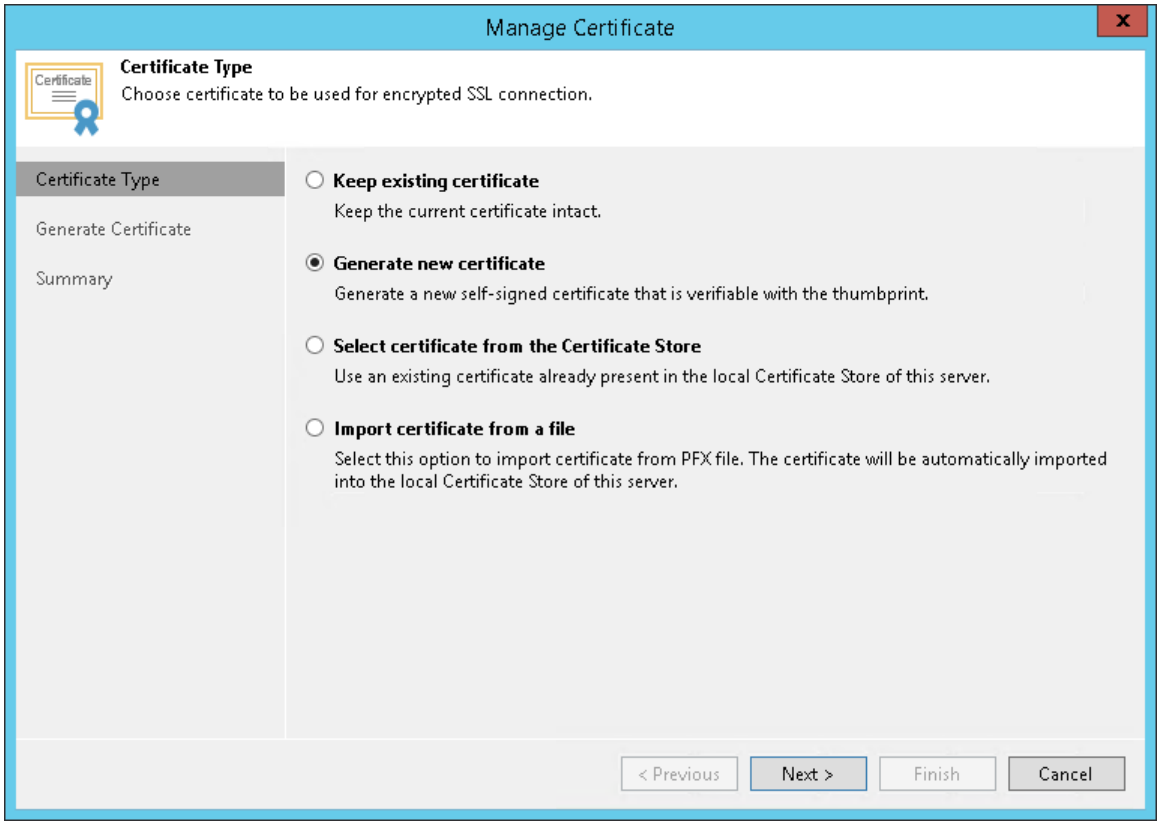
If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on a protected computer. When Veeam Backup & Replication discovers a protected computer, a matching TLS certificate with a public key is installed on the protected computer automatically. During discovery, Veeam Installer Service deployed on the protected computer retrieves the TLS certificate with a public key from the backup server and installs a TLS certificate with a public key on the protected computer.

> **NOTE**
>
> When you generate a self-signed TLS certificate with Veeam Backup & Replication, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam Backup & Replication license installed on the Veeam backup server.

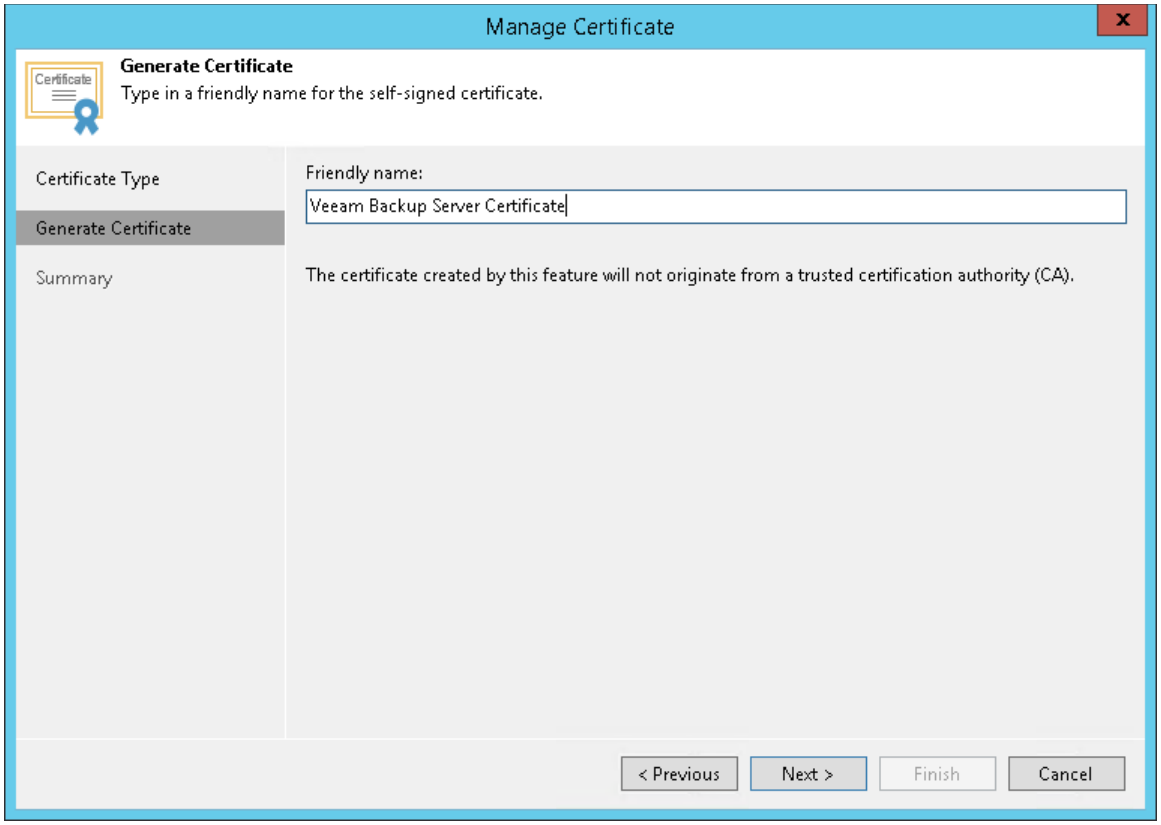
To generate a self-signed TLS certificate:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.

4. At the **Certificate Type** step of the wizard, select **Generate new certificate**.

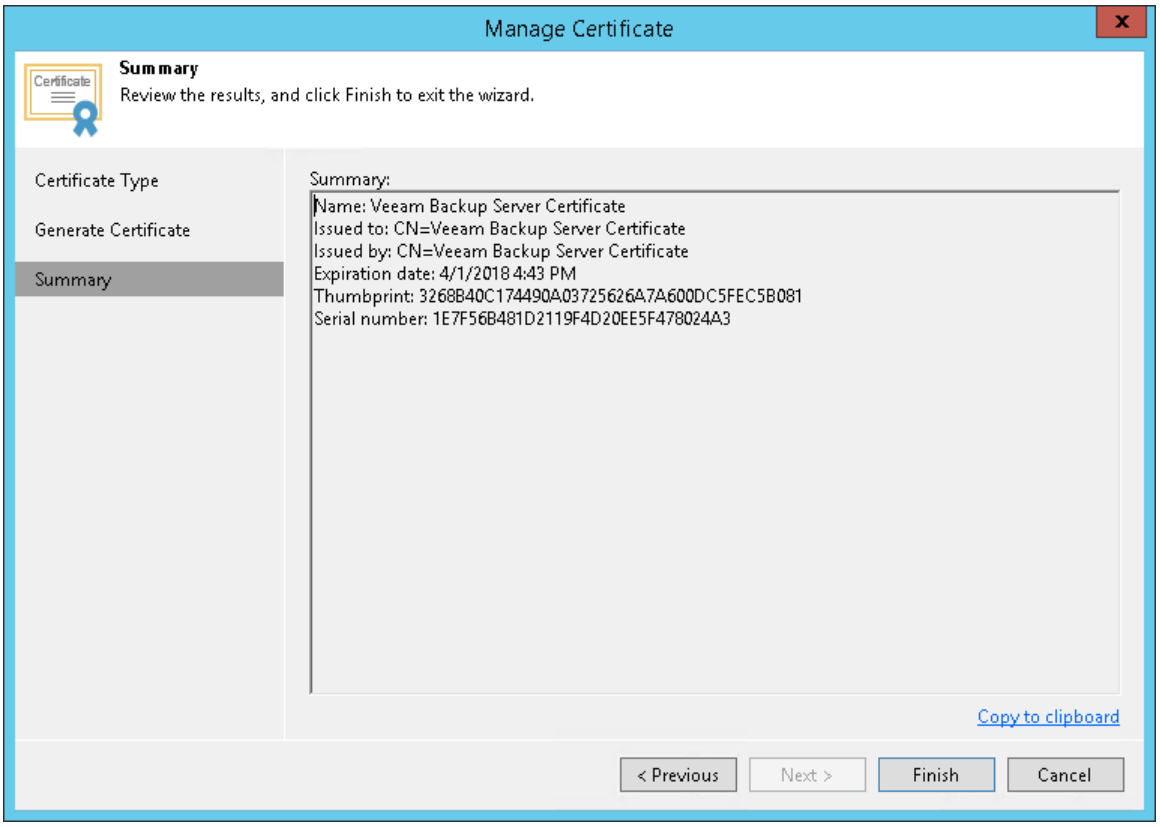


5. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.



6. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the generated TLS certificate. You will be able to use the copied information to verify the TLS certificate with the certificate thumbprint.

7. Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the Veeam backup server.

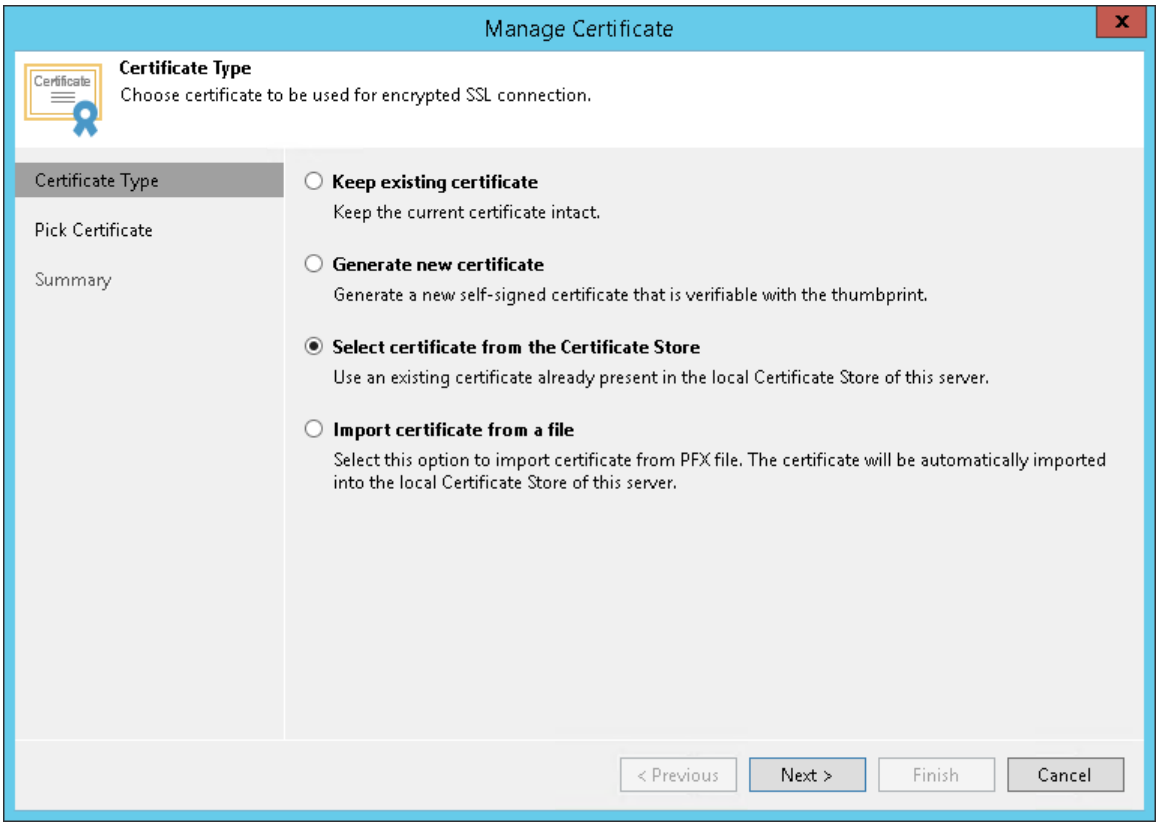


Importing Certificates from Certificate Store

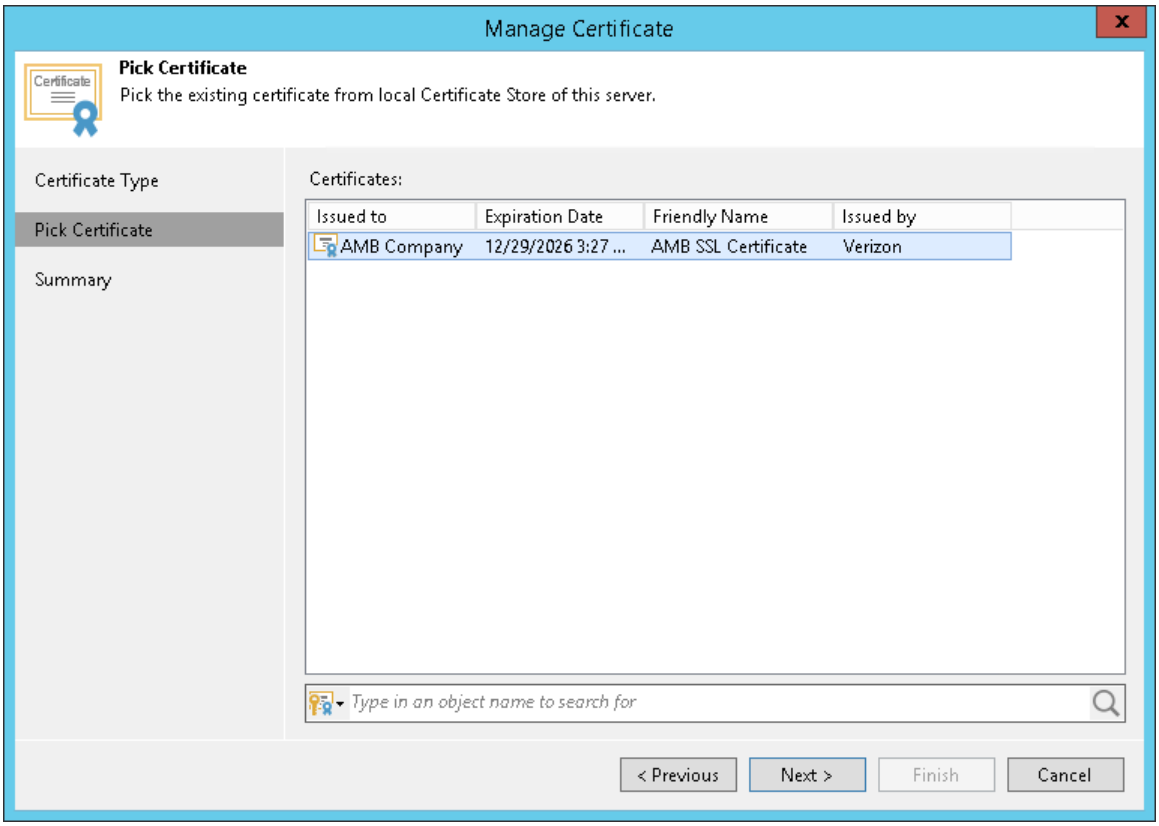
If your organization has a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows Certificate store, you can use this certificate for authenticating parties in the Veeam Agent management infrastructure.

To select a certificate from the Microsoft Windows Certificate store:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Select certificate from the Certificate Store**.



5. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.



6. At the **Summary** step of the wizard, review the certificate properties.
7. Click **Finish** to apply the certificate.

Importing Certificates from PFX Files

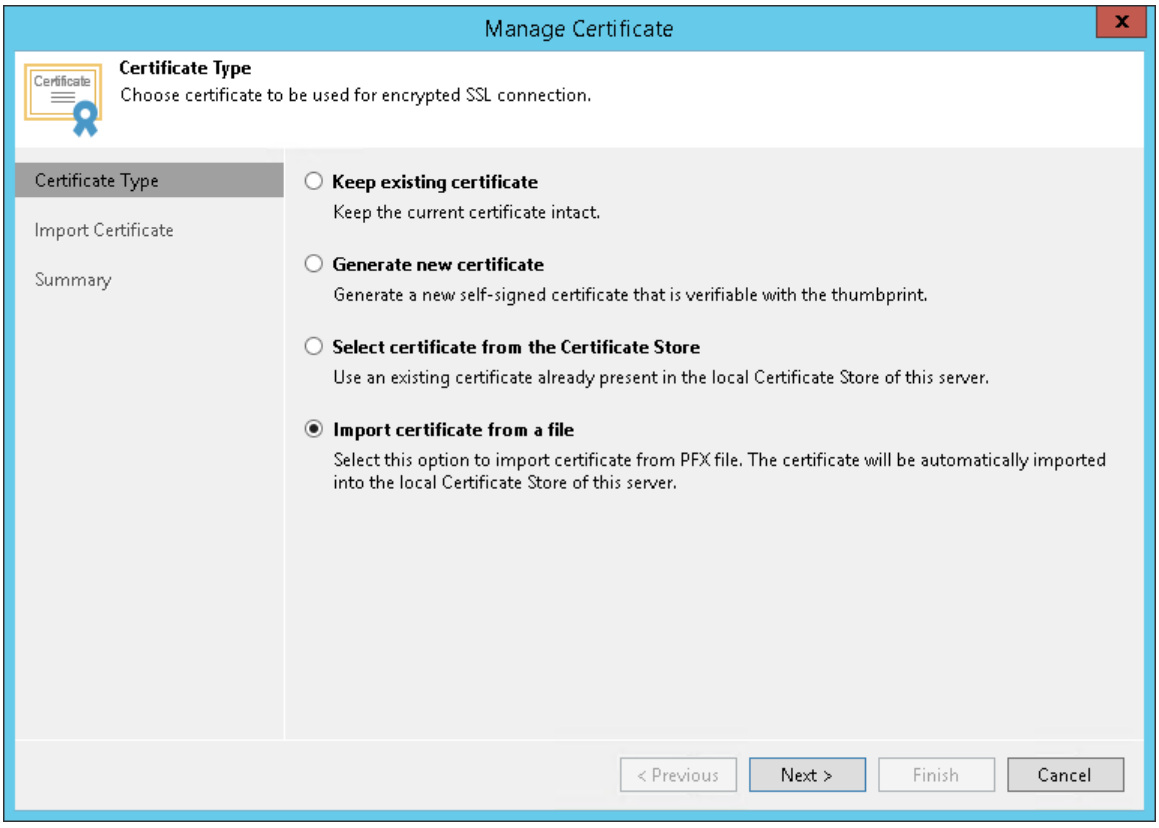
You can import a TLS certificate in the following situations:

- Your organization uses a TLS certificate signed by a CA and you have a copy of this certificate in a file of PFX format.
- You have generated a self-signed TLS certificate in the PFX format with a third-party tool and you want to import it to Veeam Backup & Replication.

> **IMPORTANT**
>
> The TLS certificate must pass validation on the Veeam backup server. In the opposite case, you will not be able to import the TLS certificate.

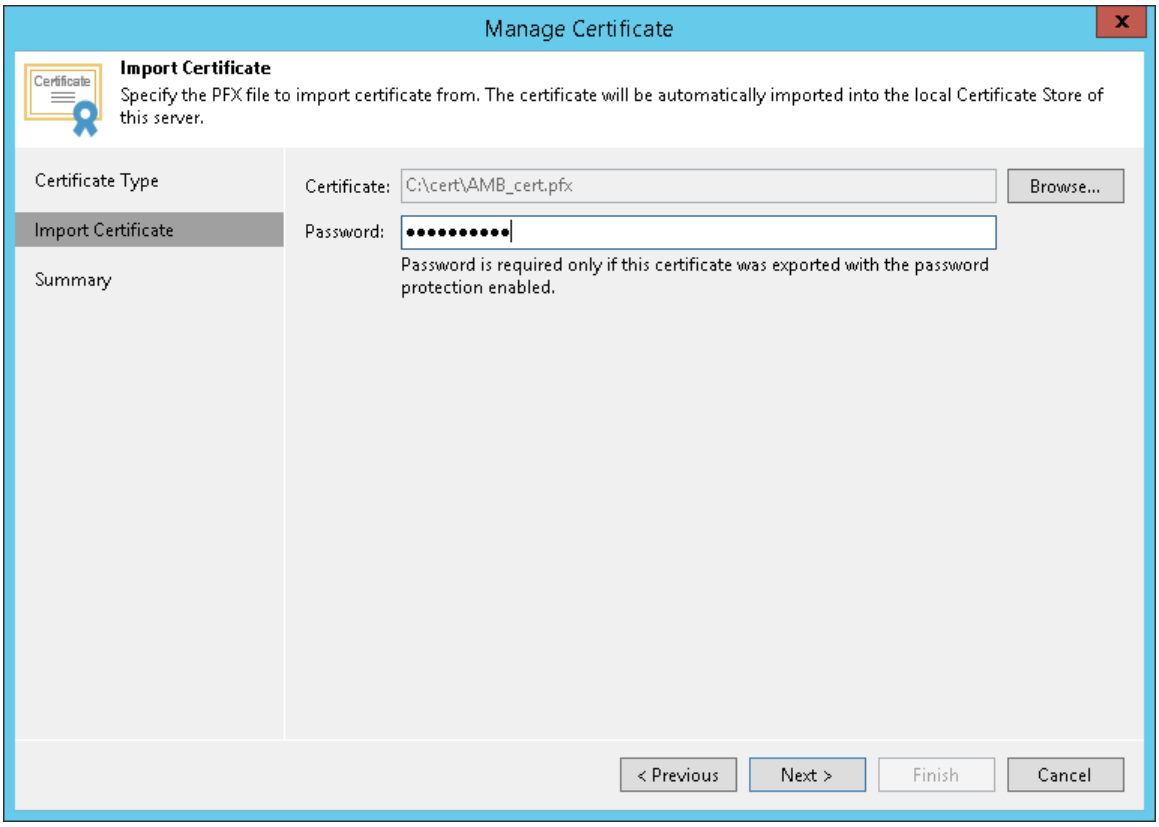
To import a TLS certificate from a PFX file:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.



5. At the **Import Certificate** step of the wizard, specify a path to the PXF file.

6. If the PFX file is protected with a password, specify the password in the field below.



7. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the TLS certificate. You can use the copied information on a protected computer to verify the TLS certificate with the certificate thumbprint.

8. Click **Finish** to apply the certificate.

Using Certificate Signed by Internal CA

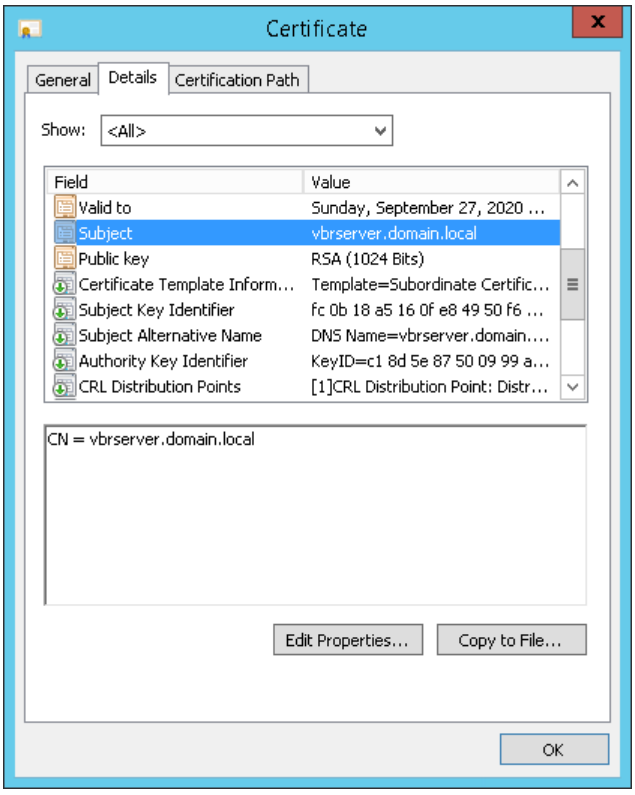
To establish a secure connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. By default, Veeam Backup & Replication uses a self-signed certificate. Veeam Backup & Replication generates this certificate when you install the product on the Veeam backup server.

If you want to use a certificate signed by your internal Certification Authority (CA), make sure that the following requirements are met:

- Veeam Agents and Veeam Backup & Replication must trust the CA. That is, the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the Veeam backup server and Veeam Agent computers.
- Certificate Revocation List (CRL) must be accessible from the Veeam backup server and Veeam Agent computers.
- [For Linux-based Veeam Agent computers] OpenSSL version 1.0 or later must be installed on the Veeam Agent computer.

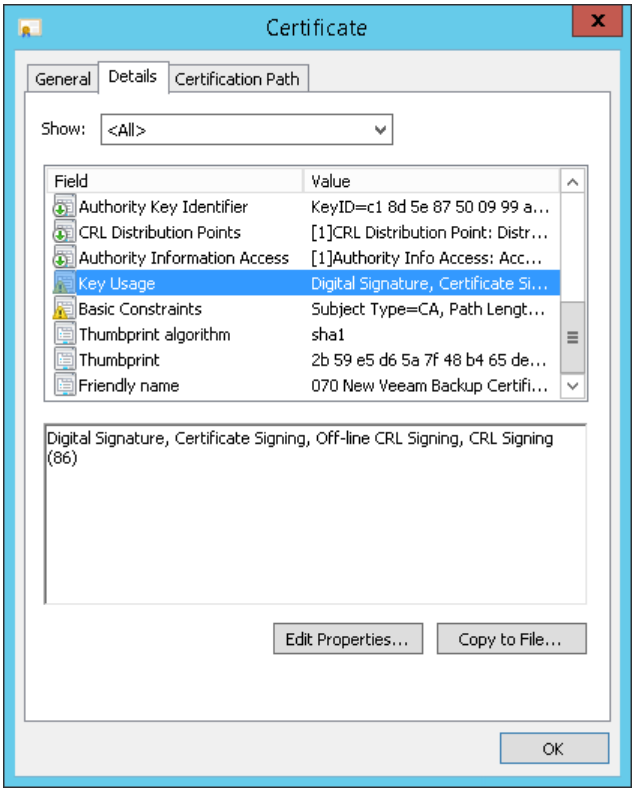
A certificate signed by a CA must meet the following requirements:

1. The certificate subject must be equal to the fully qualified domain name of the Veeam backup server. For example: *vbrserver.domain.local*.



2. The following key usage extensions must be enabled in the certificate to sign and deploy child certificates for Veeam Agent computers:
   - Digital Signature
   - Certificate Signing
   - Off-line CRL Signing
   - CRL Signing (86)

   If you use Windows Server Certification Authority, it is recommended that you issue a Veeam Backup & Replication certificate based on the built-in "Subordinate Certification Authority" template or templates similar to it.



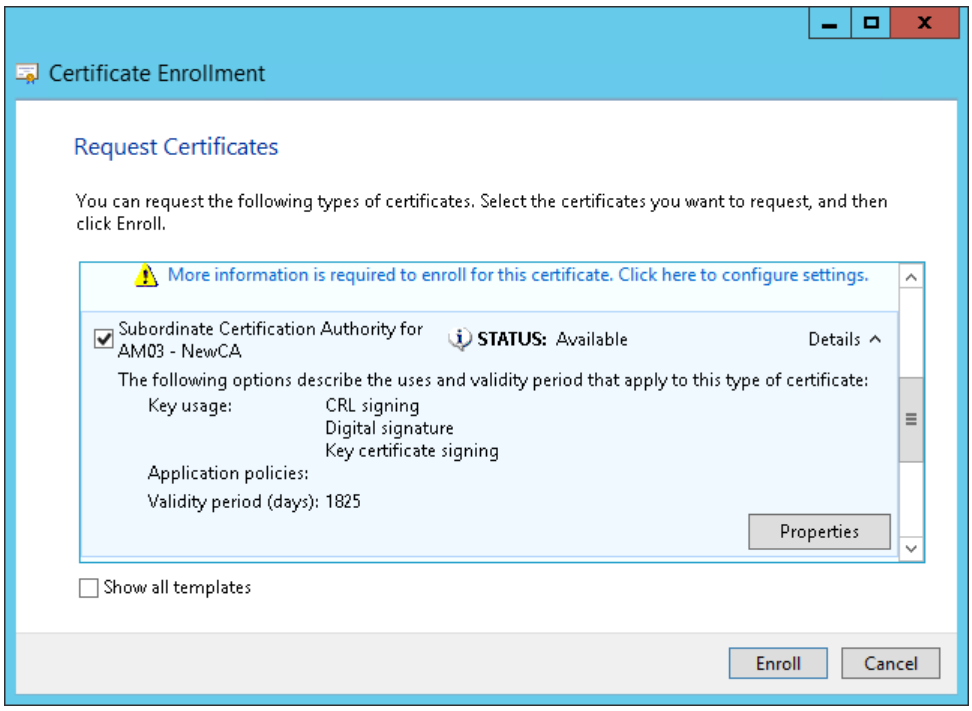
3. It is highly recommended to add "pathLen=0" to Basic Constraints.

   If you use Windows Server Certification Authority, to do this, enable the **Do not allow subject to issue certificates to other CAs** option in the certificate template.

4. The key type in the certificate must be set to *Exchange*.

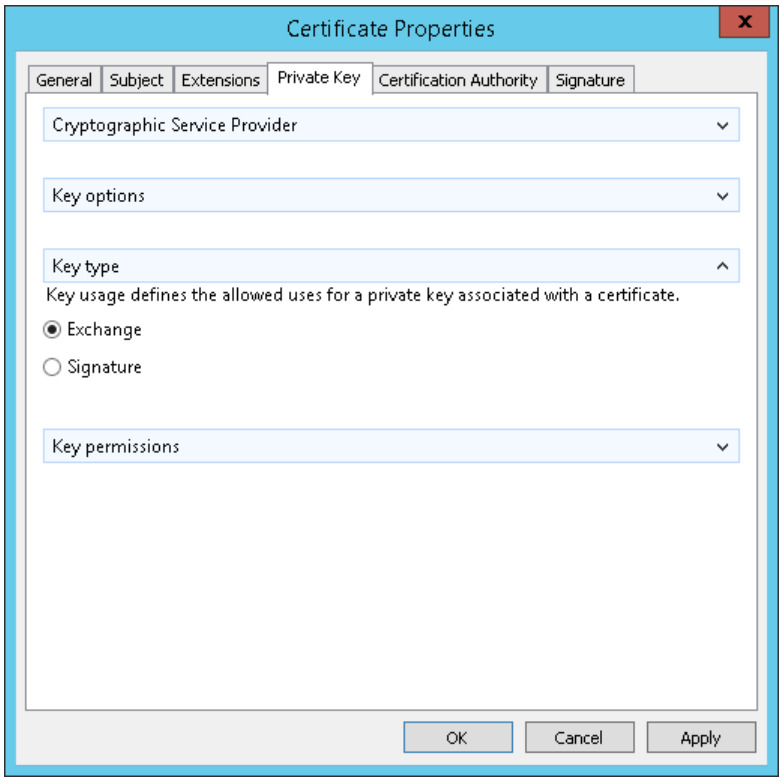
   If you create a certificate request using the Windows MMC console, to specify the key type, do the following:

   a. At the **Request Certificates** step of the **Certificate Enrollment** wizard, select a check box next to the necessary certificate template and click **Properties**.



   b. In the **Certificate Properties** window, click the **Private Key** tab.

   c. In the **Key Type** section, select **Exchange**.



To start using the signed certificate, you must select it from the certificates store on the Veeam backup server. To learn more, see Importing Certificates from Certificate Store.

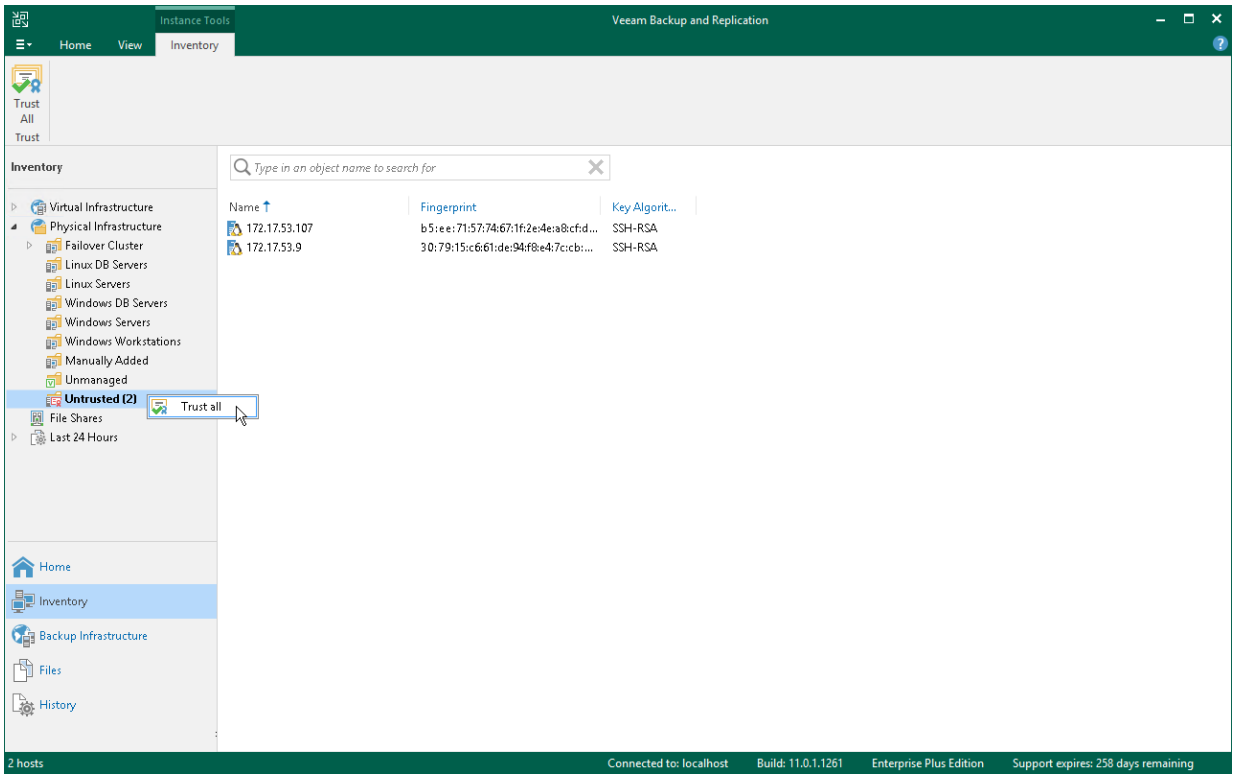
After you specify the signed certificate in Veeam Backup & Replication, during the next backup job session Veeam Agents will receive child certificates from the Veeam backup server.

Adding Computers to Trusted Hosts List

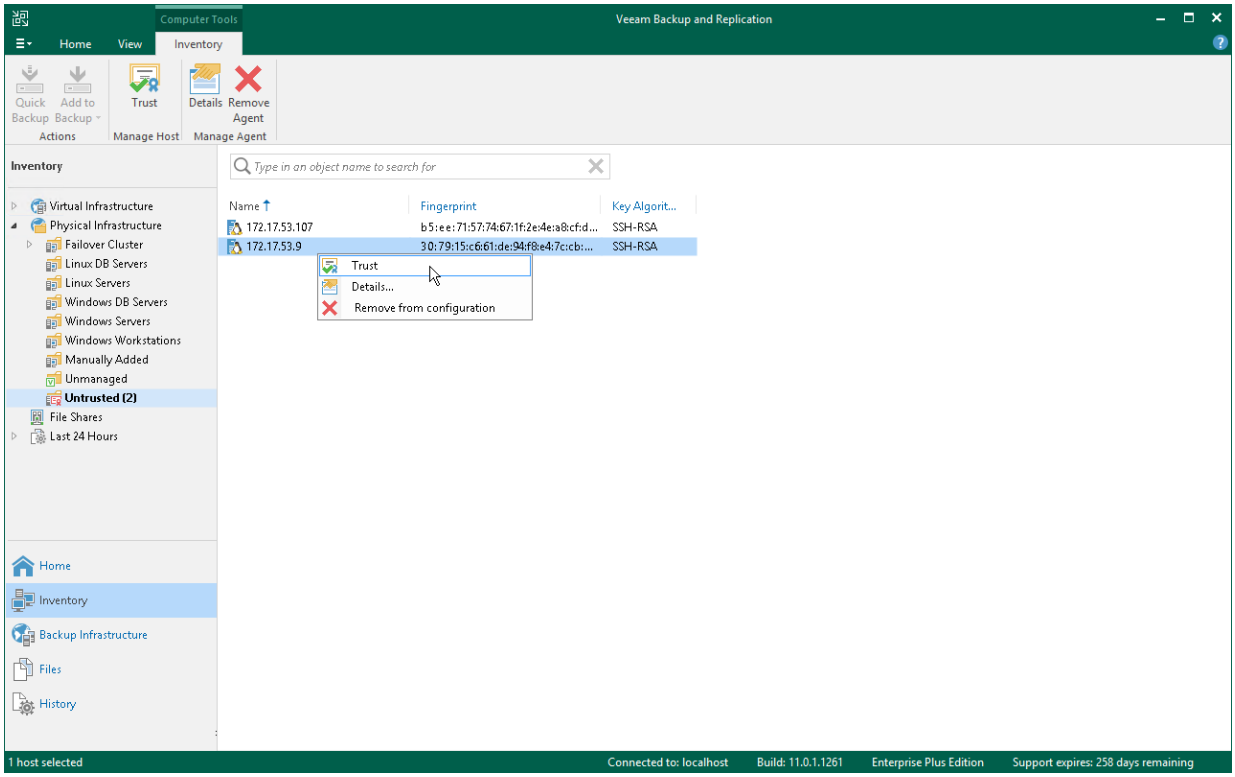
After you enable the **Add unknown hosts to the list manually (more secure)** option in Veeam Backup & Replication settings, Linux-based computers whose SSH fingerprints are not stored in the Veeam Backup & Replication database become unable to communicate to the Veeam backup server. During discovery, Veeam Backup & Replication puts such computers to the *Untrusted* protection group. To start managing an untrusted computer, you must manually validate the SSH fingerprint and add the to the list of trusted hosts in the Veeam Backup & Replication console.

To add a computer to the list of trusted hosts:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and click **Untrusted**.
3. In the working area, Veeam Backup & Replication will display discovered computers that you can add to the list of trusted hosts. Check SSH fingerprints of the computers and add them to the list of trusted hosts in one of the following ways:
   - To add all computers at once to the list of trusted hosts, select the **Untrusted** node in the inventory pane and click **Trust All** on the ribbon or right-click the **Untrusted** node and select **Trust all**.



- To add a specific computer to the list of trusted hosts, select the necessary computer in the working area and click **Trust** on the ribbon or right-click the computer and select **Trust**.



Working with Protection Groups

> **IMPORTANT**
>
> Protection groups for pre-installed Veeam Agents offer a limited set of operations. To learn more, see Working with Protection Groups for Pre-Installed Veeam Agents.

In Veeam Backup & Replication, Veeam Agent computers are organized into protection groups. You can perform the following operations with protection groups:

- Create a protection group.
- Add a protection group to a Veeam Agent backup job.
- Edit protection group settings.
- Rescan a protection group.
- Assign location to a protection group.
- Disable a protection group.
- Remove a protection group.

Working with Protection Groups for Pre-Installed Veeam Agents

A protection group for pre-installed Veeam Agents offers a limited set of operations. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

For protection groups for pre-installed Veeam Agents, you can perform the following operations:

- Create a protection group.
- Add a protection group to a Veeam Agent backup job.
- Edit protection group settings.
- Disable a protection group.
- Remove a protection group.

Creating Protection Groups

You must add computers that you plan to protect with Veeam Agents to the inventory in the Veeam Backup & Replication console. In Veeam Backup & Replication, protected computers are organized into protection groups. You can create one or more protection groups that contain computers of different types or offer different discovery and deployment options.

> **TIP**
>
> If you do not want to create protection groups, for example, if you plan to manage only a small number of computers in your infrastructure, you can add the necessary computers directly to a Veeam Agent backup job. Veeam Backup & Replication will automatically add such computers to the *Manually Added* protection group. To learn more, see Adding Computers to Backup Job and Predefined Protection Groups.

Before You Begin

Before creating a protection group, consider the following prerequisites and limitations:

1. [Not applicable to protection groups for pre-installed Veeam Agents] When Veeam Backup & Replication performs discovery of protected computers, Veeam Backup & Replication connects to every computer added to the protection group. If you instruct Veeam Backup & Replication to perform discovery immediately after the protection group is created, make sure that all computers added to the protection group are powered on and may be accessed over the network. Otherwise, Veeam Backup & Replication will be unable to connect to a protected computer and perform the required operations on this computer.
2. A protection group for pre-installed Veeam Agents is the only protection group that allows to protect the following computers:
   - Unix computers with Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris installed
   - macOS computers with Veeam Agent for Mac installed
3. A protection group for pre-installed Veeam Agents offers a limited set of deployment and management operations. To learn more, see Working with Protection Groups for Pre-Installed Veeam Agents and Managing Protected Computers Added to Protection Group for Pre-Installed Veeam Agents.
4. A protection group that includes Microsoft Active Directory objects can include objects from one domain only. To add to the inventory computers that reside in another domain, you need to create a separate protection group and include in this protection group the necessary objects from that domain.
5. Veeam Backup & Replication automatically excludes from the protection scope Active Directory objects of the Group type that exist in a parent Active Directory object (organization unit, container or entire domain) specified in the protection group settings. To instruct Veeam Backup & Replication to process a group, you must select this group explicitly in the protection group settings.
6. You cannot add and/or exclude universal and domain local groups to/from protection groups that include Microsoft Active Directory objects. Only global groups are supported.
7. [Not applicable to protection groups for pre-installed Veeam Agents] It is recommended that you do not add a computer to a protection group by specifying a dynamic IP address assigned to this computer. If such computer receives another IP address from a DHCP server, Veeam Backup & Replication will be unable to discover the computer and perform on this computer operations defined in the protection group settings.
8. [Not applicable to protection groups for pre-installed Veeam Agents] It is recommended that you do not add a computer to a protection group by specifying a public IP address assigned to this computer. If you add such computer to a backup policy targeted at a cloud repository, the name of the subtenant account created for the computer can contain the public IP address. This IP address will be visible to the Veeam Cloud Connect service provider who has access to subtenant account settings.
9. We recommend that you include each computer in one protection group only. For example, if you have added an Active Directory container to a protection group, it is not recommended to add a computer that exists in this container to another protection group. Adding computers to multiple protection groups with different computer discovery and Veeam Agent deployment settings will result in additional load on the backup server.
10. You can add a cluster only to a protection group that includes Microsoft Active Directory objects. You cannot add clusters to protection groups that include individual computers or computers specified in a CSV file.
11. When you configure a protection group for a cluster, do not exclude nodes of this cluster from a protection scope. Otherwise, Veeam Backup & Replication will not have complete information about all clustered servers.

12. [Not applicable to protection groups for pre-installed Veeam Agents] To deploy Veeam Installer Service and Veeam Agent for Microsoft Windows on a protected computer, Veeam Backup & Replication uses the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the administrative share.

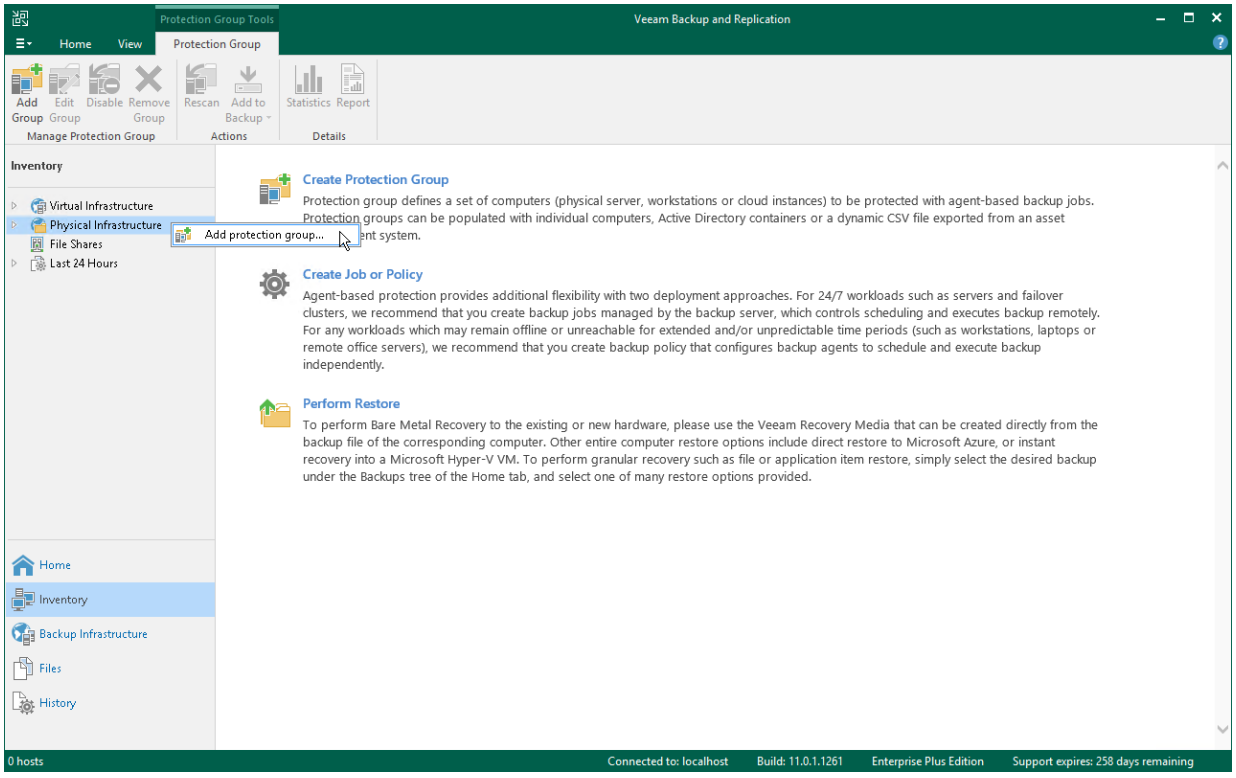
    Note that in client Microsoft Windows OSes access to the administrative share is forbidden by default for local accounts. You can enable this option with a registry key. For details, see this Microsoft KB article.

13. Veeam Backup & Replication does not support usage of a Linux account for which system settings modify shell output results to connect to a computer included in the protection group. For example, this includes Linux accounts with the modified *PS1* shell variable.

Step 1. Launch New Protection Group Wizard

To launch the **New Protection Group** wizard, do one of the following:

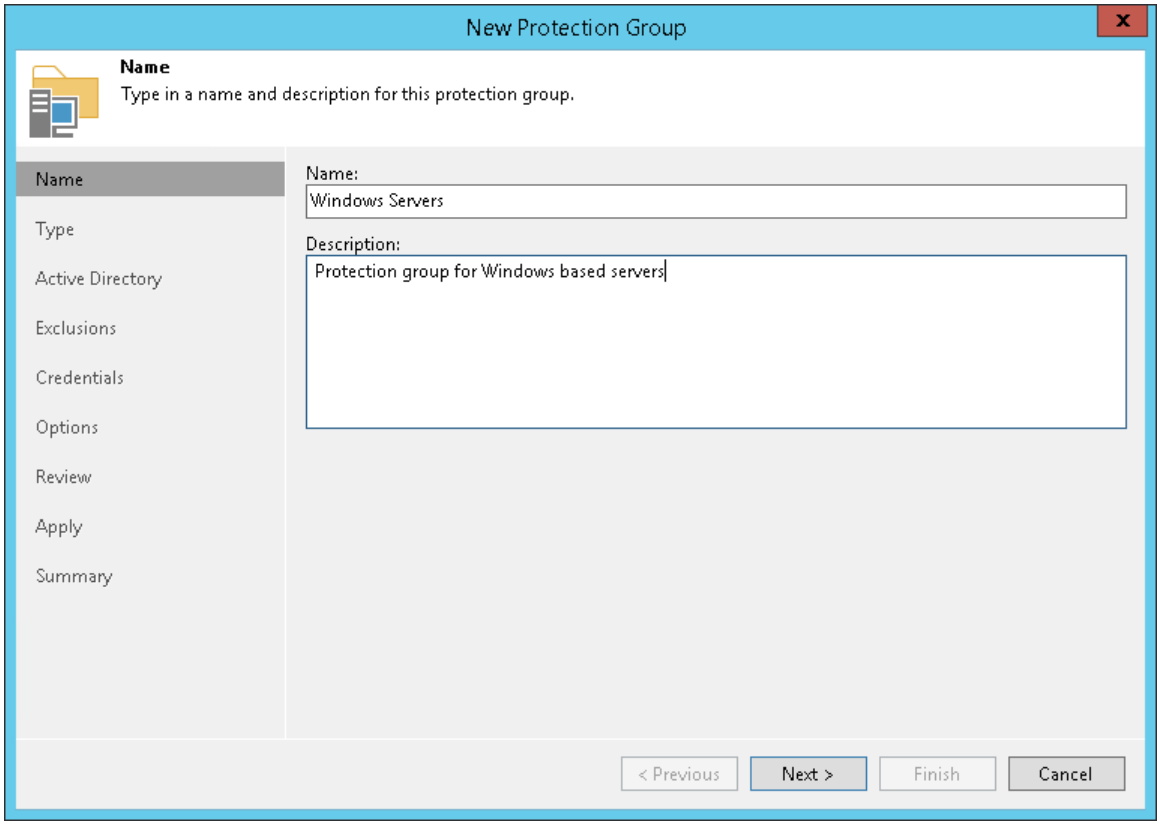
- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Add Group** on the ribbon.
- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Create Protection Group** in the working area.
- Open the **Inventory** view. Right-click the **Physical Infrastructure** node in the inventory pane and select **Add protection group**.



Step 2. Specify Protection Group Name and Description

At the **Name** step of the wizard, specify a name and description for the protection group.

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



Step 3. Select Protection Group Type

At the **Type** step of the wizard, select the type of the protection group.

> **NOTE**
>
> You can add a Microsoft failover cluster to a protection group based on Microsoft Active Directory objects only. To do this, you must select the **Microsoft Active Directory objects** option and then add a cluster account or an AD object containing this account at the Active Directory step of the wizard.

You can select one of the following types:

- **Individual computers** — select this option if you want to define a static protection scope by adding specific computers to the protection group. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed.

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

- **Microsoft Active Directory objects** — select this option if you want to add to the protection group one or several Active Directory objects: entire domain, container, organization unit, group, computer or cluster. Protection groups that include Active Directory containers and/or organization units are dynamic in their nature. If a new computer is added to a container or organization unit that you have specified in the protection group settings, during the next rescan session, Veeam Backup & Replication will discover this computer and (optionally) deploy Veeam Agent on this computer.

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

- **Computers from CSV file** — select this option if you want to add to the protection scope computers listed in a CSV file that resides in a local folder on the backup server or in a network shared folder. As well as protection groups that include Active Directory containers, protection groups of this type are also dynamic. If a new computer appears in a CSV file after the protection job is created, within the next rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer.

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

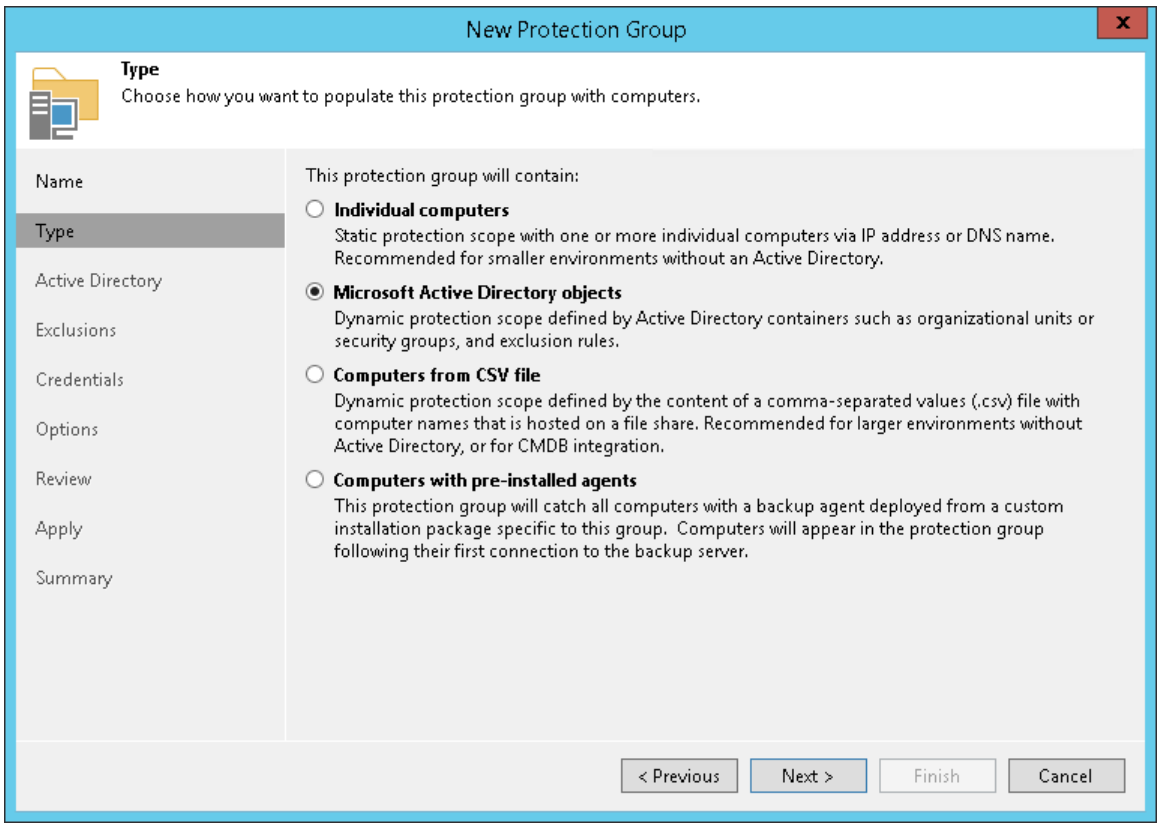
- **Computers with pre-installed agents** — select this option if you want to create a protection group for pre-installed Veeam Agents. This protection group will include any number of computers that use a certain certificate ID to connect to the Veeam backup server. Certificate ID is a unique identification number generated for each protection group that is available among other connection settings in a configuration file. You will obtain the configuration file along with Veeam Agent setup files after the protection group is created. Using these setup files, you must deploy Veeam Agent and apply connection settings from the configuration file on the Veeam Agent computer. After that, Veeam Agent connects to the Veeam backup and Veeam Backup & Replication includes the Veeam Agent computer in the protection group.

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

  To learn more about Veeam Agents deployment, see Deploying Veeam Agents Using Generated Setup Files.

NOTE

- The **Computers with pre-installed agents** option is the only applicable option for Unix computers that you plan to protect with Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX and Mac computers that you plan to protect with Veeam Agent for Mac.
- You can add a protection group of the **Computers with pre-installed agents** type only to a Veeam Agent backup job managed by Veeam Agent. Veeam Agent backup jobs managed by the backup server are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.



Step 4. Specify Protection Scope

Specify protection scope for the created protection group:

- Specify computers — if you have selected the **Individual computers** option at the Type step of the wizard.
- Specify Microsoft Active Directory objects — if you have selected the **Microsoft Active Directory objects** option at the Type step of the wizard.
- Specify a CSV file — if you have selected the **Computers from CSV file** option at the Type step of the wizard.
- Specify packages — if you have selected the **Computers with pre-installed agents** option at the Type step of the wizard.

Specifying Computers

The **Computers** step of the wizard is available if you have chosen the **Individual computers** option at the Type step of the wizard.

At this step of the wizard, specify computers that you want to add to the protection group.

To add a computer to a protection group:

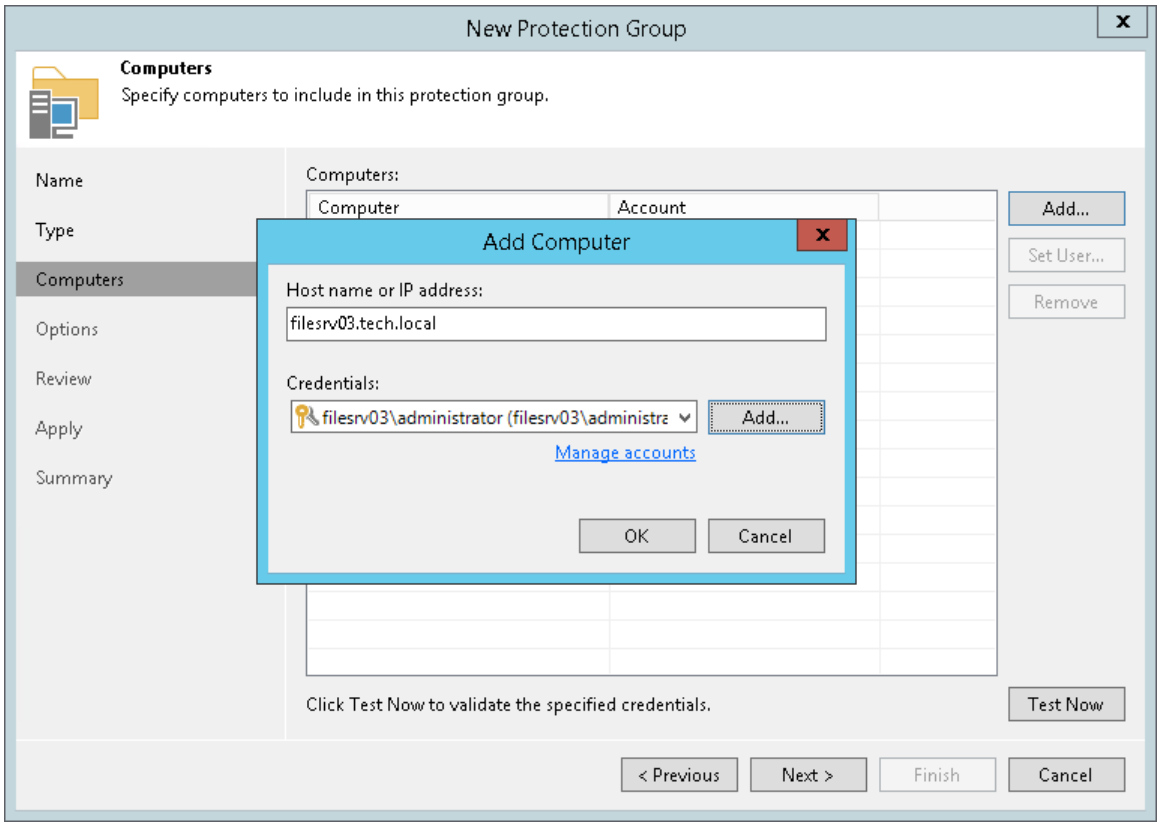
1. Click **Add**.
2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name, NetBIOS name or IP address of the computer that you want to add to the protection group.
3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the protection group. Veeam Backup & Replication will use this account to connect to the protected computer and perform the necessary operations on the computer: upload and install Veeam Agent, and so on.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

   Keep in mind that the username must be specified in the down-level logon name format. For example, DOMAIN\UserName or HOSTNAME\UserName. Use the full domain or hostname name. Do not replace them with a dot.
4. Repeat steps 1–3 for every computer that you want to add to the protection group.
5. To check if Veeam Backup & Replication can communicate with computers added to the protection group, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all computers in the list.

NOTE

If you chose to manually add Linux-based computers to the list of trusted hosts in Veeam Backup & Replication, when you test credentials for an unknown Linux-based computer in the protection group settings, the test operation will complete with the *Failed* status. This happens because Veeam Backup & Replication cannot connect to the untrusted computer before you add this computer to the list of trusted hosts. To learn more, see Adding Computers to Trusted Hosts List.



Specifying Active Directory Objects

The **Active Directory** step of the wizard is available if you have chosen the **Microsoft Active Directory objects** option at the Type step of the wizard.

At this step of the wizard, select Active Directory objects that you want to add to the protection group. You can add to a protection group the following types of Active Directory objects: domain, organization unit, container, computer, cluster, or group.

To add Active Directory objects to a protection group:

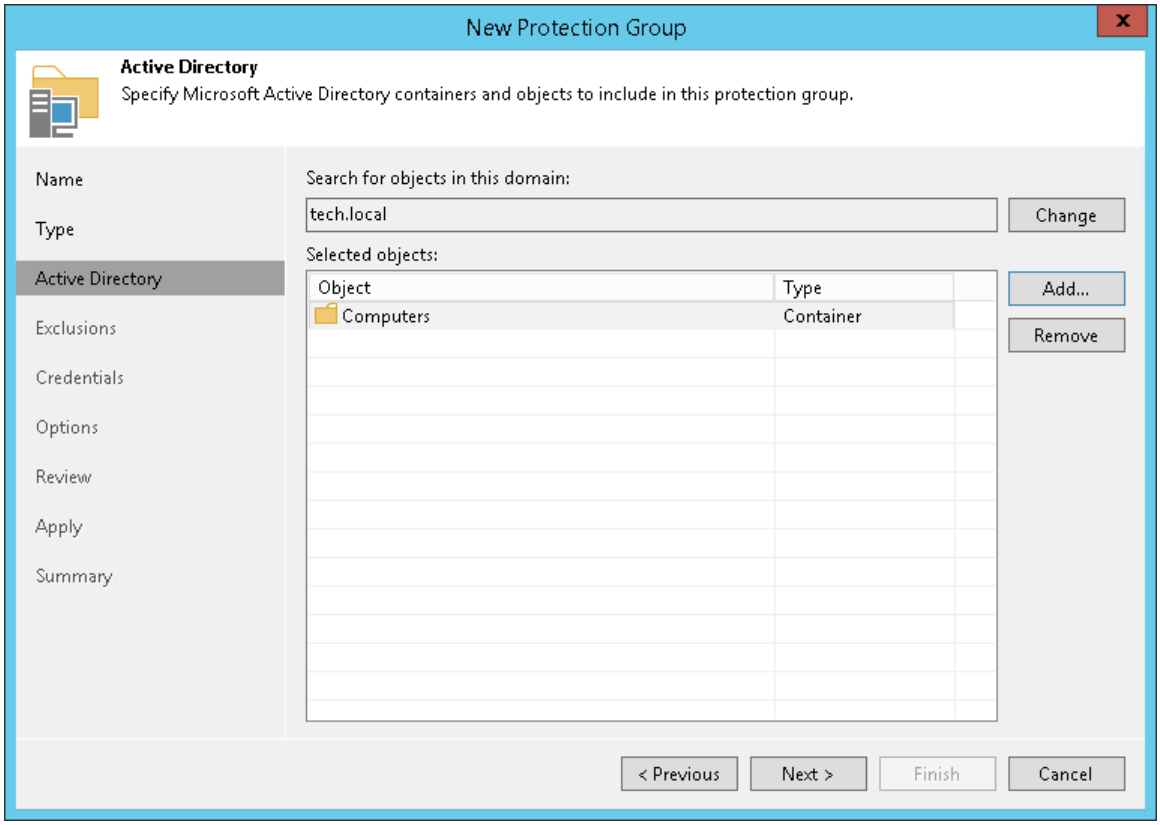
1. In the **Search for objects in this domain** field, click **Change**.
2. In the **Specify Domain** window, specify settings of the domain whose objects you want to include in the protection group:
   a. In the **Domain controller or domain DNS name** field, type a name of the domain controller or domain whose objects you want to include in the protection group.
   b. In the **Port** field, specify a port number over which Veeam Backup & Replication must communicate with the domain controller. By default, Veeam Backup & Replication uses port 389.
   c. From the **Account** list, select a user account that is a member of the *DOMAIN\Administrators* group. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.
   d. Click **OK** to close the **Specify Domain** window.

   > **NOTE**
   >
   > If you want to include a large number of computers in the protection group but do not want to use an account with domain administrator permissions in the protection group settings, consider configuring a protection group based on a list of computers imported from a CSV file. To learn more, see Select Protection Group Type.

3. In the **Selected objects** field, click **Add**.
4. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

   To quickly find the necessary object, you can use the search field at the bottom of the **Add Objects** window.
   a. Click the button to the left of the search field and select the necessary type of object to search for: *Everything*, *Computer*, *Cluster*, *Organization Unit*, *Container* or *Group*.
   b. Enter the object name or a part of it in the search field.

c. Click the **Start search** button on the right or press **[ENTER]**.



Specifying CSV File

The **CSV File** step of the wizard is available if you have chosen the **Computers from CSV file** option at the Type step of the wizard.

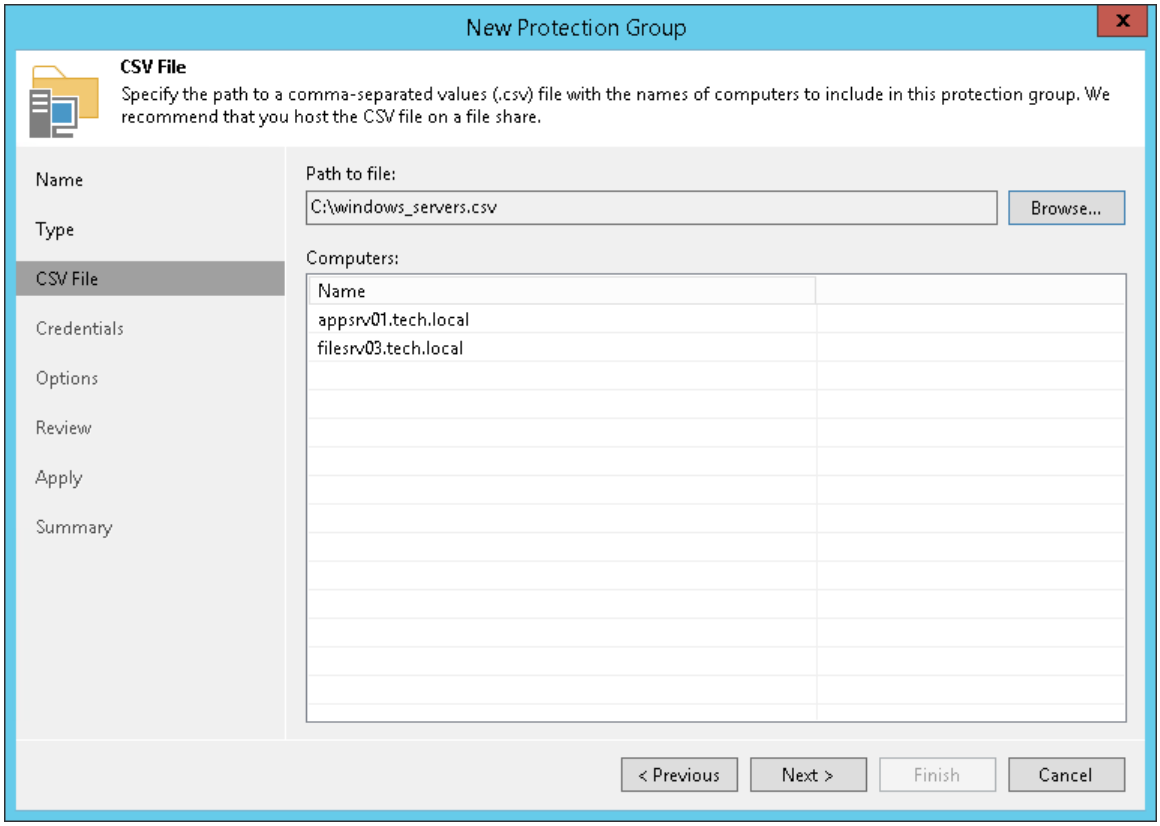
At this step of the wizard, specify a file that defines a list of computers that you want to add to the protection group. You must specify a list of computers in a file of the CSV or TXT format. The file must be created beforehand. To learn more, see Preparing CSV File.

To specify a CSV file:

1. In the **Path to file** field, click **Browse** and specify a path to a CSV file that contains a list of IP addresses or domain names of computers that you want to add to the protection group. The CSV file can reside in a folder on the local drive of the Veeam backup server or in a network shared folder accessible from the backup server.
2. In the **Computers** field, review the list of IP addresses or domain names imported from the CSV file.

NOTE

After you finish configuring the protection group, Veeam Backup & Replication will perform discovery of computers listed in the CSV file upon schedule defined in the protection group settings. If Veeam Backup & Replication is unable to read the CSV file (for example, after the file was moved or deleted from the specified location), the rescan job will use the list of computers imported from the CSV file during the previous rescan job session.



Preparing CSV File

To define a dynamic protection scope based on a list of computers, you must create a CSV file with a list of IP addresses or domain names to scan during discovery. Veeam Backup & Replication supports IP addresses of the IPv4 format only.

Delimit IP addresses or domain names in the list with commas (',') or semicolons (';'). For example:

```
172.17.53.16,172.17.53.19,172.17.53.31,172.17.53.40
```

Alternatively, you can delimit IP addresses or domain names in the list with the newline character:

```
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40
```

Specifying Packages

The **Package** step of the wizard is available if you have chosen the **Computers with pre-installed agents** option at the Type step of the wizard.

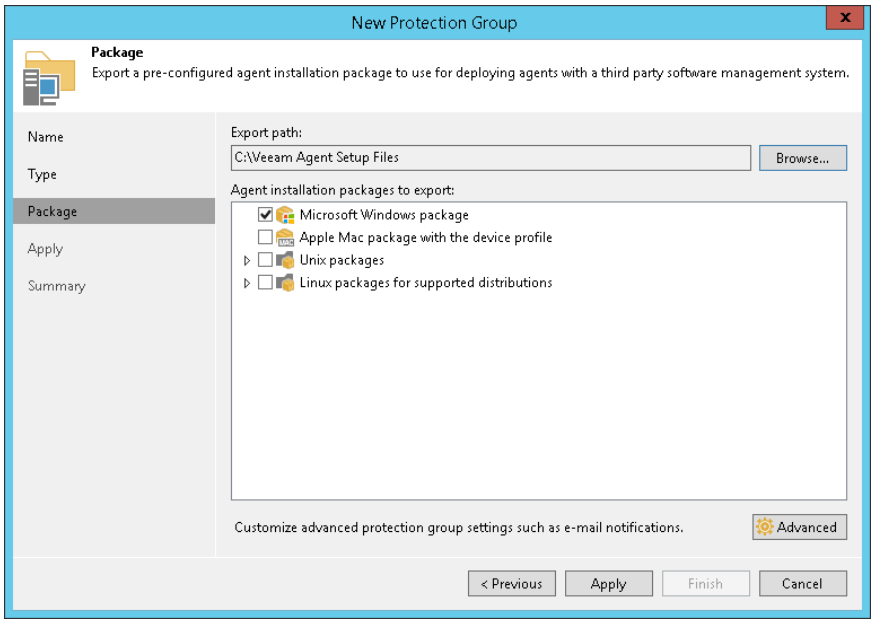
At this step of the wizard, specify what setup files you want to obtain to deploy Veeam Agents. Veeam Backup & Replication will export the specified setup files to the specified folder. Then, you must use these setup files to deploy Veeam Agents on computers you plan to protect. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

To specify setup files to export:

1. In the **Export path** field, click **Browse**.
2. In the **Select Folder** window, specify a path to the folder to which Veeam Backup & Replication will export Veeam Agent setup files. Setup files can be exported to a folder on the local drive of the Veeam backup server or to a network shared folder accessible from the backup server.
3. In the **Agent installation packages to export** field, select setup files depending on the type of the OS that runs on computers you plan to add to the protection group.
   a. If you plan to protect Windows computers, select the **Microsoft Windows package** option
   b. If you plan to protect Mac computers, select the **Apple Mac package with the device profile** option
   c. If you plan to protect Unix computers, expand the **Unix Packages** option and select options depending on the distributions you need.

      If you select the **Unix Packages** option, Veeam Backup & Replication will export setup files for all Unix distributions supported by Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris.
   d. If you plan to protect Linux computers, expand the **Linux packages for supported distributions** option and select options depending on the distributions you need.

      If you select the **Linux packages for supported distributions** option, Veeam Backup & Replication will export setup files for all Linux distributions supported by Veeam Agent for Linux.
4. Click **Advanced** to specify advanced settings for the protection group. To learn more, see Specify Advanced Protection Group Settings.



Step 5. Exclude Objects from Protection Group

The **Exclusions** step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects.

At this step of the wizard, you can specify which objects you want to exclude from the protection group. You can exclude the following types of objects:

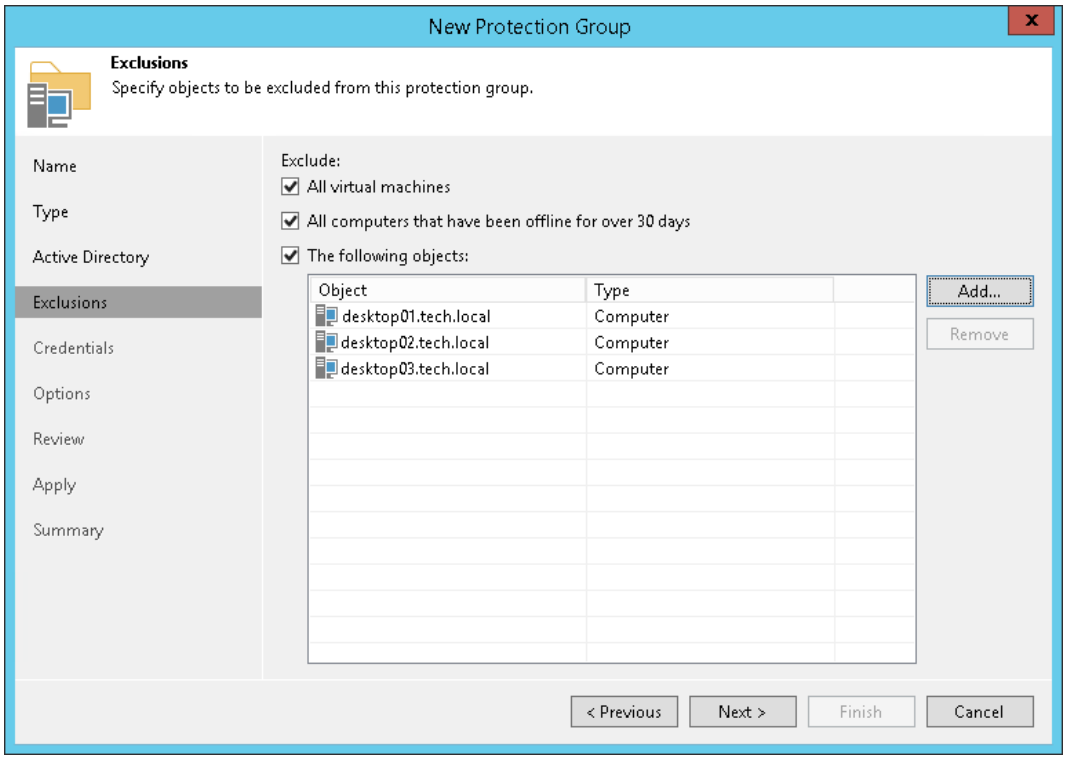
- All virtual machines — all VMs residing in the domain. You can select this option, for example, if you do not want to protect VMs with Veeam Agents and want to back up VM data with Veeam Backup & Replication instead.
- All computers that have been offline for over 30 days — all computers in the domain that have not logged on to Active Directory for more than 30 days.
- Individual Active Directory objects — specific Active Directory objects: computers, clusters, groups, organization units and/or containers. With this option selected, you must specify Active Directory objects that you want to exclude from the protection group.

To exclude Active Directory objects:

1. In the **Exclude** section, select the **The following objects** check box.
2. Click **Add**.
3. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, you can use the search field at the bottom of the **Add Objects** window.

1. Click the button to the left of the search field and select the necessary type of object to search for: *Everything*, *Computer*, *Cluster*, *Group*, *Organization Unit* or *Container*.
2. Enter the object name or a part of it in the search field.
3. Click the **Start search** button on the right or press **[ENTER]**.



Step 6. Specify Credentials

The **Credentials** step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects or computers specified in a CSV file.

At this step of the wizard, specify credentials to connect to computers included in the protection group:

1. If you want to use the same credentials for all computers in the protection group, select the necessary user account from the **Master account** list. The account must have local administrator permissions on all computers that you have added to the protection group.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

2. By default, Veeam Backup & Replication uses credentials specified in the **Master account** field for all computers in the protection group. If some computer requires a different user account, do the following:

   a. Select the **Use custom credentials for the following objects** check box,

   b. Click **Add** next to the list of objects and select the necessary object in the **Add Objects** window:

      - If you configure a protection group that includes Active Directory objects, objects that you have added to the protection group at the **Active Directory** step or the wizard are already displayed in the **Use custom credentials for the following objects** list. In the **Add Objects** window, you can also select child objects for which you want to specify custom credentials. For example, you may want to specify separate credentials for different organization units, containers, groups or individual computers within the entire domain added to the protection group.

      - If you configure a protection group that includes computers specified in a CSV file, you can select in the **Add Objects** window one or more computers listed in a CSV file and add them to the **Use custom credentials for the following objects** list.

   c. In the **Use custom credentials for the following objects** list, select the necessary object, click **Edit** and select custom credentials for the object. Credentials must be specified in the following format:

      - For Active Directory accounts — *DOMAIN\Username*

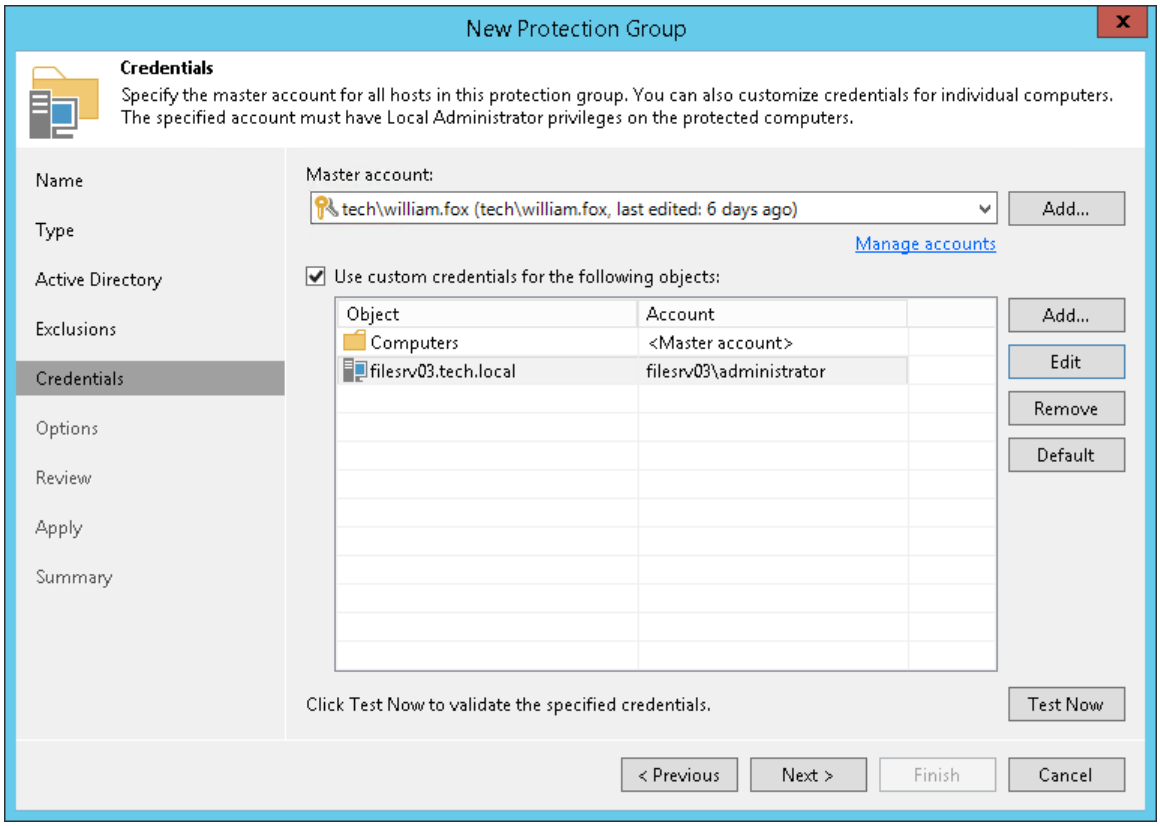
      - For local accounts — *Username* or *HOST\Username*

NOTE

Consider the following:

- Veeam Backup & Replication supports user account names in the SAM-Account-Name format (*DOMAIN\Username*). The User-Principal-Name (UPN) format (*username@domain*) is not supported. If you specify credentials in the UPN format, Veeam Backup & Replication will successfully connect to computers added to the protection group during the *Test Now* operation. However, the subsequent protection group rescan operations will fail.
- The account that you use to connect to a Linux computer must have a home directory on this computer.
- If you configure a protection group that includes dynamic Active Directory objects, such as domain, organization unit, container or group, the master account or custom account specified for an object must be a member of the DOMAIN\Administrators group.
- If you plan to back up Oracle databases that run on Linux computers, the OS account used to connect to the computer must be a member of the group that owns configuration files of the Oracle database (for example, the oinstall group).

To check if Veeam Backup & Replication can connect to computers added to the protection group, click **Test Now**. Veeam Backup & Replication will form a list of computers to connect and use the specified credentials to connect to computers in the list.



Step 7. Specify Discovery and Deployment Options

The **Options** step of the wizard is available if you have chosen to define a protection scope that includes individual computers, Microsoft Active Directory objects, or computers specified in a CSV file.

At this step of the wizard, specify settings for protected computers discovery and Veeam Agent deployment.

Veeam Backup & Replication regularly connects to protected computers according to the schedule defined in the protection group settings. At this step of the wizard, you can define the discovery schedule and specify operations that Veeam Backup & Replication must perform on discovered computers. You can also select which server in your backup infrastructure should act as a distribution server for Veeam Agents.

To specify discovery and deployment options:

1. In the **Discovery** section, define schedule for automatic computer discovery within the scope of the protection group:
   - To run the rescan job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the rescan job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the rescan job. In the **Start time within an hour** field, specify the exact time when the job must start.
   - To run the rescan job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new rescan job session will start as soon as the previous rescan job session finishes.

   > **NOTE**
   >
   > You cannot create a protection group without defining schedule for automatic discovery. However, you can disable automatic discovery for a specific protection group, if needed. To learn more, see Disabling Protection Group.

2. In the **Deployment** section, from the **Distribution server** list, select a Microsoft Windows server that you plan to use as a distribution server. Veeam Backup & Replication will use the distribution server to upload Veeam Agent setup files to computers added to the protection group. By default, Veeam Backup & Replication assigns the distribution server role to the backup server. To learn more, see Distribution Server.
3. If you want to instruct Veeam Backup & Replication to automatically deploy Veeam Agents on all discovered computers in the protection group, in the **Deployment** section, make sure that the **Install backup agent automatically** check box is selected.

   You can also choose to disable automated Veeam Agent installation. In this case, you will need to install Veeam Agent on every computer included in the protection group and discovered by Veeam Backup & Replication. To learn more, see Installing Veeam Agent.

   > **NOTE**
   >
   > Veeam Backup & Replication installs the Veeam Installer Service on every computer added to the protection group even if the **Install backup agent automatically** check box is not selected in the protection group settings.

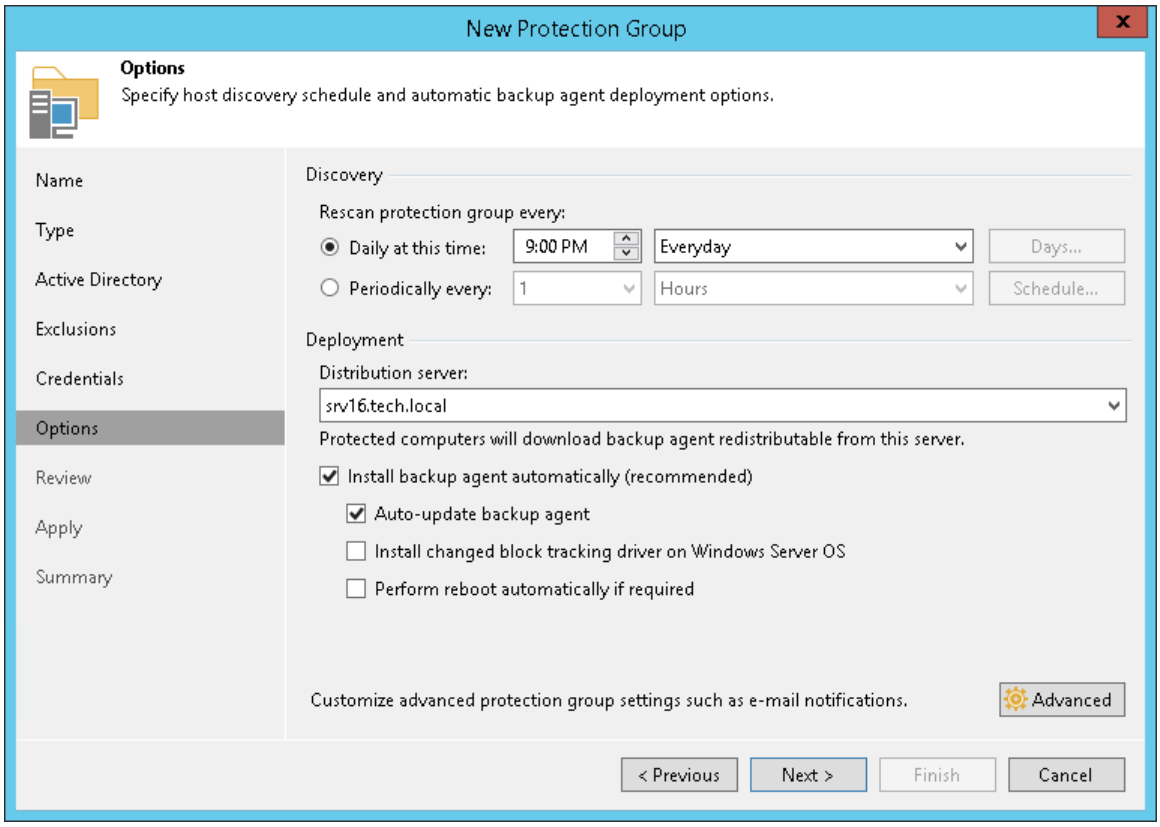
4. If you want to instruct Veeam Backup & Replication to automatically upgrade Veeam Agent on discovered computers when a new version of Veeam Agent appears on the distribution server, in the **Deployment** section, make sure that the **Auto-update backup agent** check box is selected.

5. [For protection groups that include Microsoft Windows servers] Select the **Install changed block tracking driver on Windows Server OS** check box if you want to install the advanced changed block tracking (CBT) driver on servers protected with Veeam Agent for Microsoft Windows. To learn more, see the Veeam Changed Block Tracking Driver section in the Veeam Agent for Microsoft Windows User Guide.

   If you included workstations and servers in the created protection group, Veeam Backup & Replication will install the Veeam CBT driver on servers only.

6. Select the **Perform reboot automatically if required** check box to allow Veeam Backup & Replication to reboot a protected computer. In particular, the reboot operation is required as part of the Veeam CBT driver installation process.

7. Click **Advanced** to specify advanced settings for the protection group. To learn more, see Specify Advanced Protection Group Settings.



Step 8. Specify Advanced Protection Group Settings

In the **Advanced Settings** window, specify advanced settings for the protection group:

- Veeam Agent for Microsoft Windows settings
- Notification settings

> **TIP**
>
> After you specify necessary settings for the protection group, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new protection group, Veeam Backup & Replication will automatically apply the default settings to the new protection group.

Veeam Agent for Microsoft Windows Settings

You can specify the following settings for Veeam Agent for Microsoft Windows that will be deployed on computers included in the protection group:

- **Network usage settings**. You can limit bandwidth consumption and restrict network connections usage for Veeam Agent for Microsoft Windows backup jobs. Limiting bandwidth consumption prevents jobs from utilizing the entire bandwidth available in your environment and makes sure that enough traffic is provided for other network operations. In addition to limiting bandwidth consumption, you can choose whether to allow backup over metered connections and VPN connections. For Microsoft Windows workstations that run Veeam Agent, you can also specify one or more wireless networks over which Veeam Agent is allowed to perform backup or restrict usage over any wireless networks.

  To learn more, see the Restricting Network Connections Usage section in the Veeam Agent for Microsoft Windows User Guide.

- **Throttling settings**. You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup. The throttling option can help you avoid situations when backup tasks performed by Veeam Agent for Microsoft Windows consume all available hard disk resources and hinder work of other applications and services on a protected computer. With throttling enabled, Veeam Backup & Replication sets low priority for Veeam Agent components running on protected computers and engaged in the backup process. If this option is not enabled, Veeam Agent components have normal priority.

- **Security settings**. You can allow user accounts that do not have administrative privileges on a Veeam Agent computer to perform file-level restore on this computer.

Veeam Backup & Replication applies the specified settings to Veeam Agent that runs on a protected computer added to a backup policy. Veeam Backup & Replication applies the settings during the protection group rescan process. Settings are saved to the Veeam Agent for Microsoft Windows database on the protected computer.

> **IMPORTANT**
>
> Network usage, throttling, and security settings are not applied to protected computers added to a Veeam Agent backup job managed by the backup server.

To specify settings for Veeam Agent for Microsoft Windows:

1. At the **Options** step of the wizard, click **Advanced**.
2. If you want to limit bandwidth consumption for Veeam Agent backup jobs, on the **Agent for Windows** tab, in the **Network** section, select the **Limit bandwidth consumption to** check box. Then specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.
3. By default, backup over metered connections is disabled for Veeam Agent for Microsoft Windows. Veeam Agent automatically detects metered connections and does not perform backup when your computer is on such connection. To enable backup over metered connections, clear the **Restrict metered connections usage** check box.

   > **NOTE**
   >
   > Mind the following limitations and requirements:
   >
   > - Veeam Agent for Microsoft Windows disables backup over metered Internet connections only on computers that run Microsoft Windows 8 and later. If the computer runs an earlier version of Microsoft Windows, this option is not applicable.
   > - You must specify which connections are metered in Microsoft Windows. To learn more, see this Microsoft webpage.

4. If you want to disable backup over VPN connections, select the **Restrict VPN connections usage** check box. Veeam Agent for Microsoft Windows will automatically detect VPN connections and will not perform backup when the Veeam Agent computer is on such connection.
5. If you want to restrict usage of wireless networks for Veeam Agent running on Microsoft Windows workstations, do the following:
   a. Select the **Restrict Wi-Fi usage to these networks only** check box and click **Add**.
   b. In the **Wi-Fi Network** window, specify the SSID of the Wi-Fi network over which Veeam Agent will be allowed to perform backup, and click **OK**.

   Veeam Backup & Replication will add the specified network to the list of allowed Wi-Fi networks. Backup over other wireless networks will be disabled for Veeam Agent.

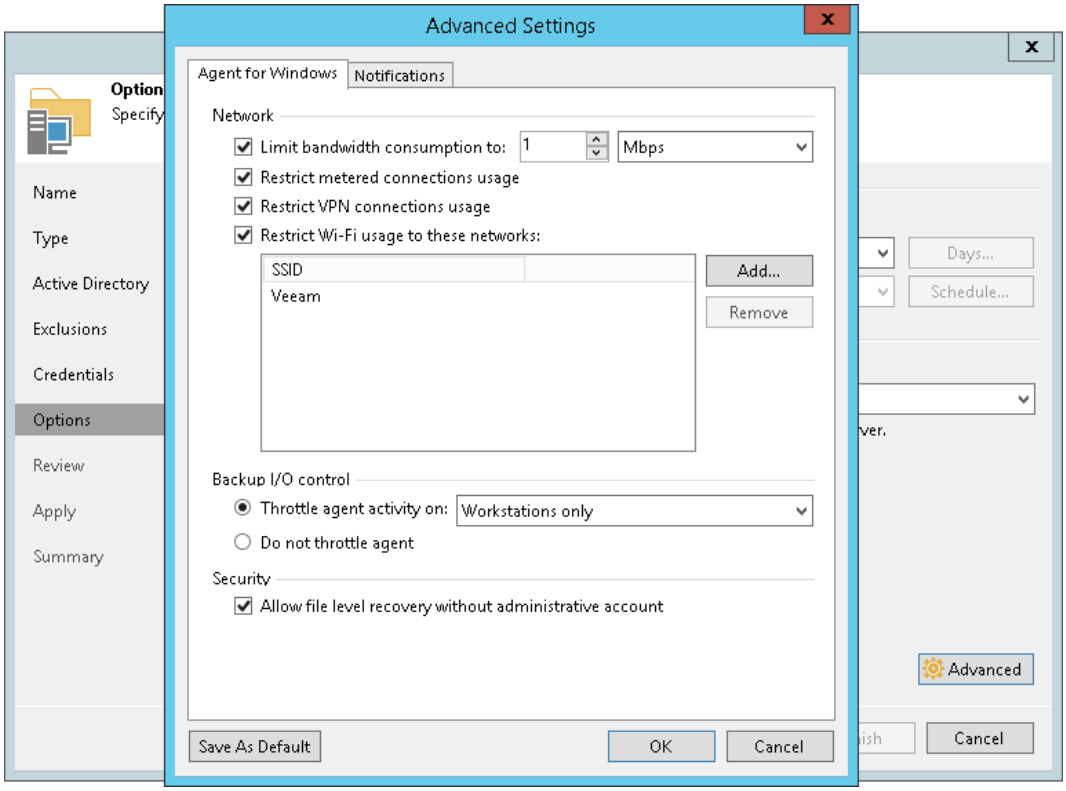
   > **TIP**
   >
   > If you want to restrict usage over any wireless networks, select the **Restrict Wi-Fi usage to these networks only** check box and do not add any networks to the list.

6. If you want to throttle Veeam Agent activities during backup, in the **Backup I/O control** section, make sure that the **Throttle agent activity on** option is selected. Then select the type of computers on which to throttle Veeam Agent backup activities: *Workstations only*, *Servers only* or *All hosts*.

   If you do not want to throttle backup activities for Veeam Agent, select **Do not throttle agent**.
7. In the **Security** section, select the **Allow file level recovery without administrative account** check box. With this option enabled, Veeam Agent computer users who work under accounts that do not have administrative privileges will be able to perform file-level restore on the Veeam Agent computer.

   In this case, access rights to files and folders are managed by Veeam Agent computer OS. If user cannot access the folder in the original location, this user cannot browse or restore the content of this folder as well.

   To learn more, see Appendix B. Restore Files from Backup without Administrator Privileges.



Notification Settings

You can specify email notification settings for the protection group. If you enable notification settings, Veeam Backup & Replication will send a daily email report with protection group statistics to a specified email address. The report contains cumulative statistics for rescan job sessions performed for the protection group within the last 24-hour period.

> **NOTE**
>
> Email reports with protection group statistics will be sent only if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the protection group, in addition to reports sent according to the global email notification settings, Veeam Backup & Replication will send reports with the protection group statistics to email addresses specified in the protection group settings. This allows you to fine-tune email notifications in Veeam Backup & Replication: while one or more backup administrators receive email notifications according to the global settings, other backup administrators can receive reports for specific protection groups only.
>
> If you do not enable global email notification settings in Veeam Backup & Replication, notification settings for the protection group will not be sent even if you enable them in the protection group settings.

To specify notification settings for the protection group:

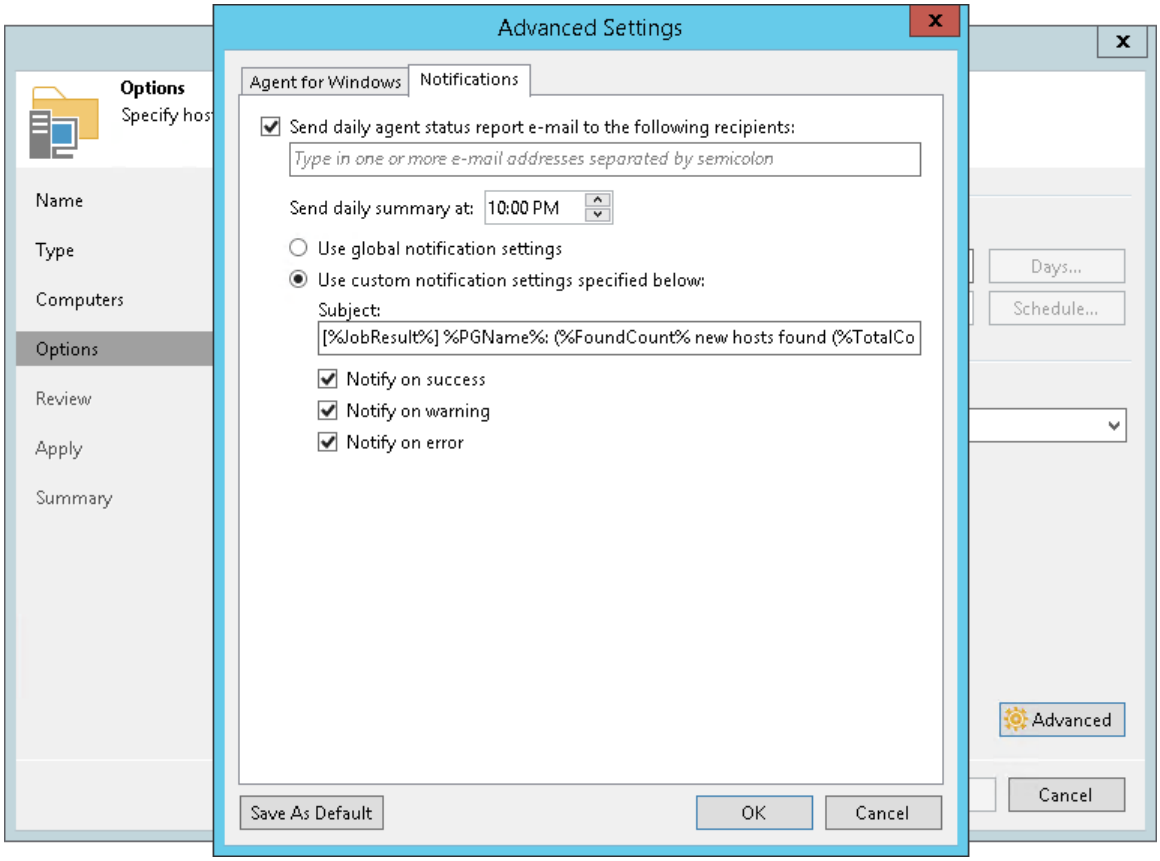
1. At the **Options** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send daily agent status report e-mail to the following recipients** check box and specify a recipient's email address. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.
5. You can choose to use global notification settings or specify custom notification settings.

   To receive a typical notification for the protection group, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the protection group global email notification settings specified for the backup server.

   To configure a custom notification for the protection group, select **Use custom notification settings specified below**. You can specify the following notification settings:

   - In the **Subject** field, specify a notification subject. You can use the following variables in the subject:
     - *%JobResult%* — rescan job result.
     - *%PGName%* — protection group name.
     - *%FoundCount%* — number of new computers discovered within the last 24-hour period.
     - *%TotalCount%* — total number of computers in the protection group.
     - *%SeenCount%* — number of computers in the protection group that were online for the last 24 hours. A computer is considered to be online if Veeam Backup & Replication successfully connected to this computer during the last rescan session.

- Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.

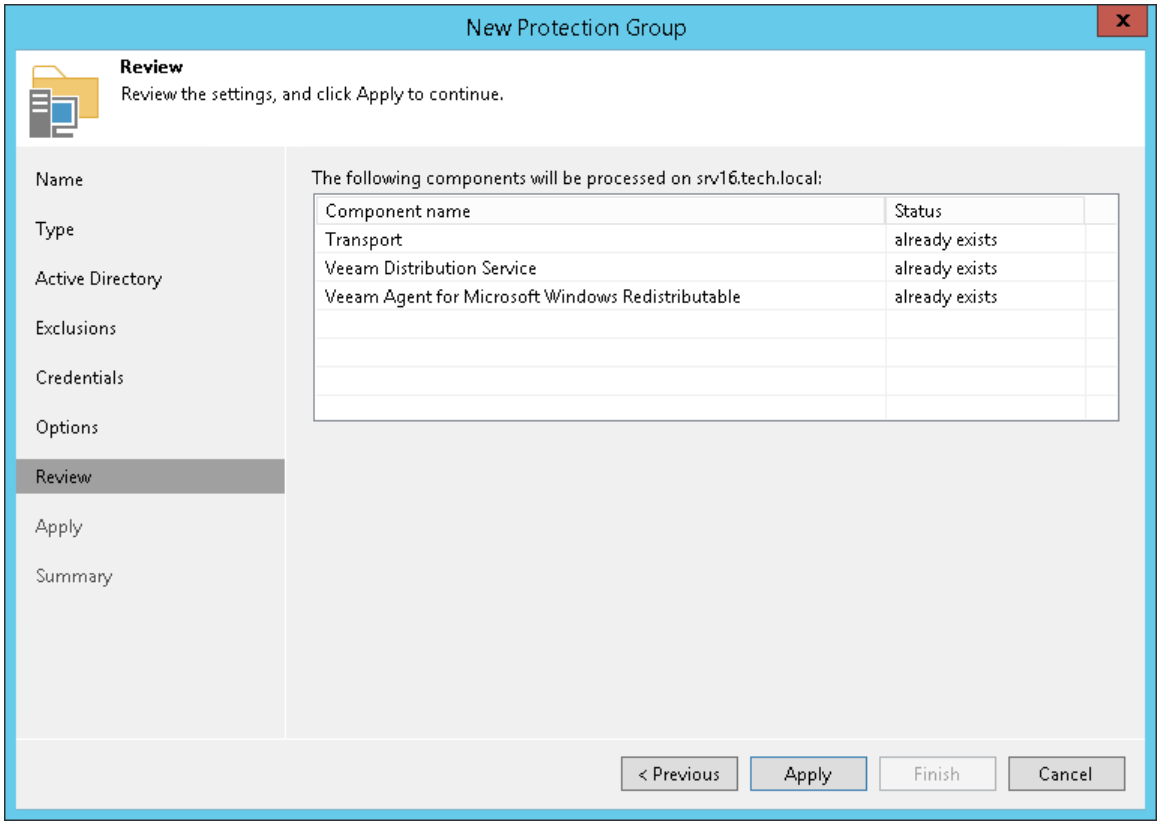


Step 9. Review Components

The **Review** step of the wizard is available if you have chosen to define a protection scope that includes individual computers, Microsoft Active Directory objects, or computers specified in a CSV file.

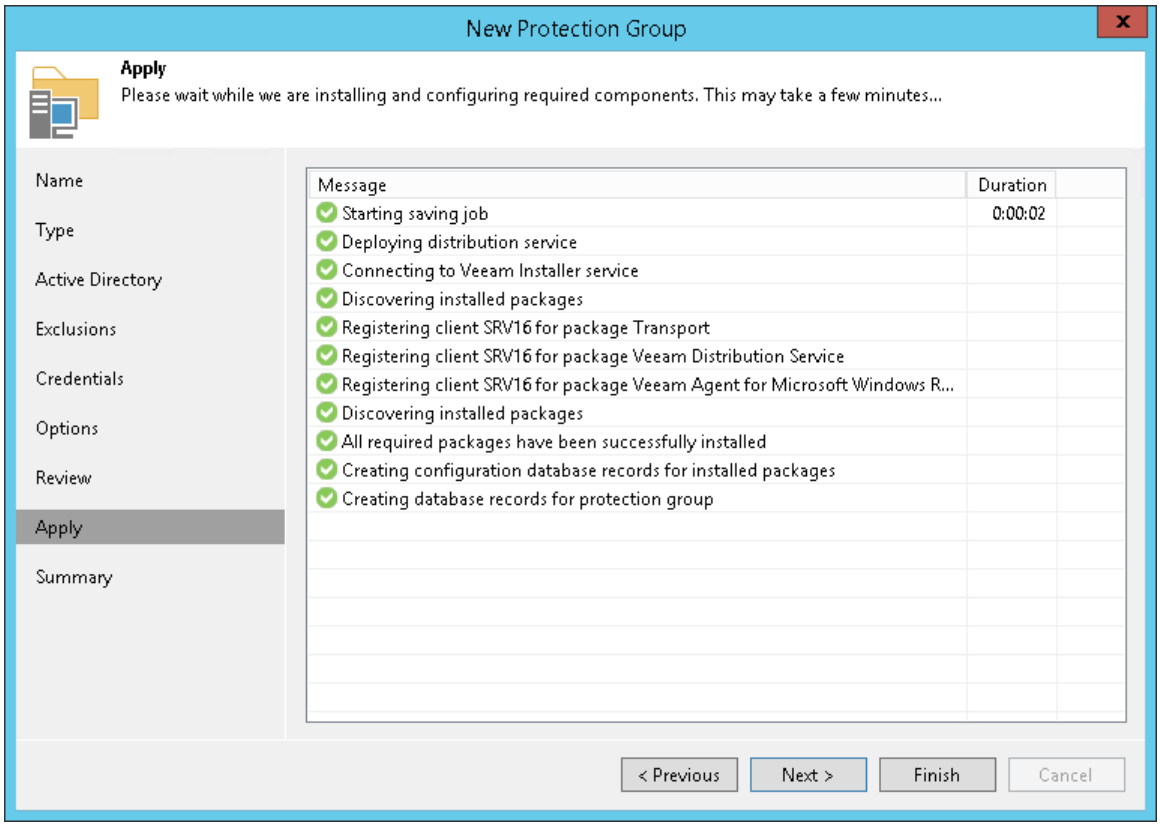
At this step of the wizard, review what Veeam Backup & Replication components are already installed on the distribution server specified for the protection group and what components will be installed.

1. Review the components.
2. Click **Apply** to add the configured protection group to the inventory.



Step 10. Assess Results

At the **Apply** step of the wizard, Veeam Backup & Replication will create the configured protection group. Wait for the operation to complete and click **Next** to continue.

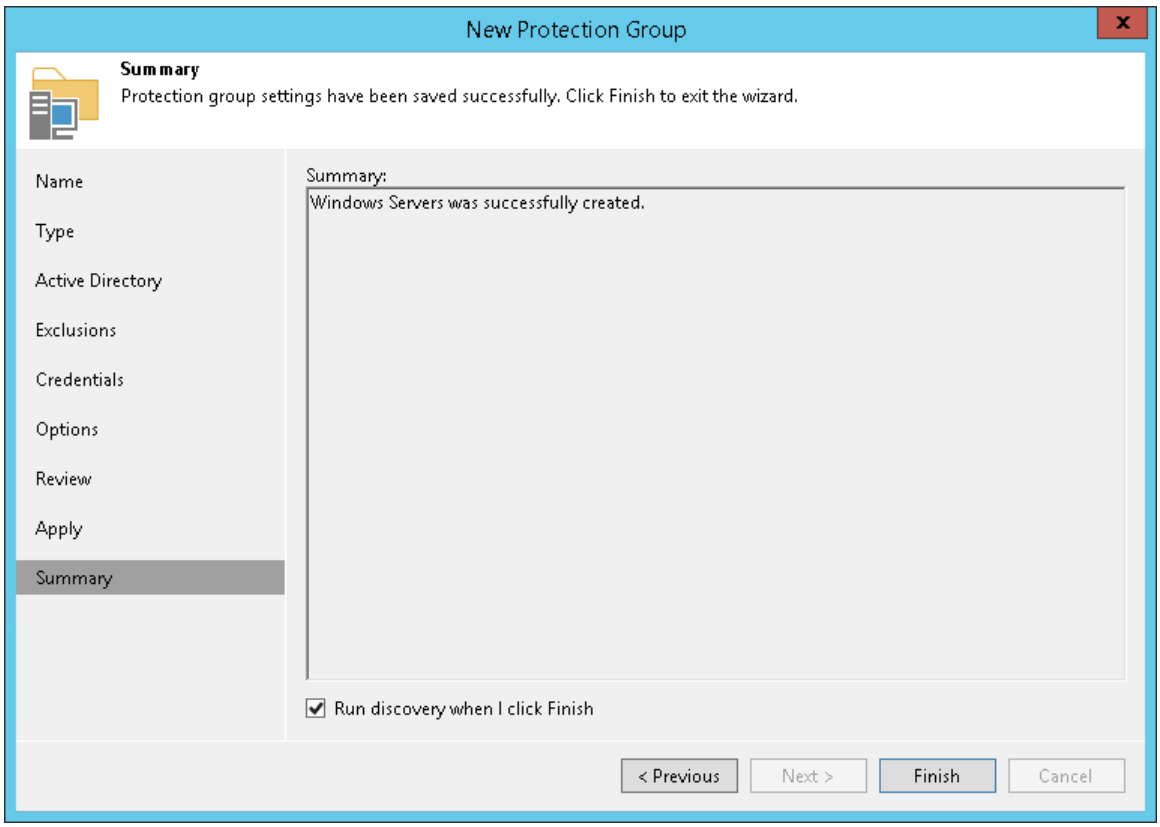


Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, complete the protection group configuration process.

1. Review information about the created protection group.
2. To start the rescan job after you close the wizard, make sure that the **Run discovery when I click Finish** option is selected.

   If you want to perform computer discovery later, you can clear the **Run discovery when I click Finish** check box. In this case, the rescan job will start automatically upon the defined schedule. You can also start the rescan job manually at any time you need. To learn more, see Starting Protection Group Discovery.
3. Click **Finish to close the wizard**.



Deploying Veeam Agents Using Generated Setup Files

When you configure the Veeam Agent management infrastructure in Veeam Backup & Replication, you can create protection groups of the Computers with pre-installed agents type. If you selected this protection group type, you must deploy Veeam Agents on the computers that you plan to protect.

> **IMPORTANT**
>
> Mind the following:
>
> - The deployment operation must take place on the Veeam Agent computer side.
> - You must use only those Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.
> - If any other version of Veeam Agent is already installed on the computer you plan to protect, you must uninstall it first.
> - If you uninstall Veeam Agent for Microsoft Windows added to the protection group of the Computers with pre-installed agents type and then re-install it on the same computer, Veeam Agent will not connect to the Veeam backup server automatically. To connect Veeam Agent, you must repeat the configuration step of the Veeam Agent deployment scenario.

Deployment scenario depends on the Veeam Agent you work with:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Unix
- Veeam Agent for Mac

Deploying Veeam Agent for Microsoft Windows

To deploy Veeam Agent for Microsoft Windows using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Microsoft Windows and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect. Then navigate to the folder where you have saved setup files.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. To install the .NET Framework 4.5.2, double-click the `NDP452-KB2901907-x86-x64-AllOS-ENU.exe` file located in the `<path_to_setup_files>/Windows/5.0.2.4680` folder.

   If a later version of the .NET Framework is already installed on the computer, you can skip this step.

3. To install Windows Universal C Runtime (CRT), find and double-click the file depending on your computer OS architecture and version:

OS Architecture	OS Version	File Location	File Name
32-bit	Windows 7 or Windows Server 2008 R2	`<path_to_setup_files>/Windows/5.0.2.4680/VAW/x86/CRT`	`Windows6.1-KB2999226-x86.msu`
	Windows 8 or Windows Server 2012		`Windows6.1-KB2999226-x64.msu`
	Windows 8.1 or Windows Server 2012 R2		`Windows8-RT-KB2999226-x86.msu`
64-bit	Windows 7 or Windows Server 2008 R2	`<path_to_setup_files>/Windows/5.0.2.4680/VAW/x64/CRT`	`Windows8-RT-KB2999226-x64.msu`
	Windows 8 or Windows Server 2012		`Windows8.1-KB2999226-x86.msu`

OS Architecture	OS Version	File Location	File Name
	Windows 8.1 or Windows Server 2012 R2		`Windows8.1-KB2999226-x64.msu`

4. To install Microsoft SQL Server components, use one of the following file sets depending on the architecture of your computer OS:

   For 32-bit Windows

   - Double-click the following files located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW/x86` folder:
     - SharedManagementObjects.msi
     - SqlLocalDB.msi
     - SQlSysClrTypes.msi

   For 64-bit Windows

   - Double-click the following files located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW/x64` folder:
     - SharedManagementObjects.msi
     - SqlLocalDB.msi
     - SQlSysClrTypes.msi

5. To install Veeam Agent for Microsoft Windows, use one of the following files depending on the architecture of your computer OS:

   For 32-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x86.msi` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder

   For 64-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder

6. To install the Veeam Installer Service, double-click the `VeeamInstallerSvc` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder.

   If an earlier version of the Veeam Installer Service is already installed on the computer, uninstall it first.

Configuration

To configure Veeam Agent for Microsoft Windows, you must apply connection settings from the configuration file. You obtained this file together with other setup files when the protection group for pre-installed Veeam Agents was created. To do configure Veeam Agent, execute the following command from the folder where Veeam Agent setup files are located:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -setVBRse
ttings /p:"<protection_group_name>.xml"
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `/p` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. After you apply new backup policy settings in the Veeam Backup & Replication console, Veeam Agent will get these settings during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -syncnow
```

Deploying Veeam Agent for Linux

To deploy Veeam Agent for Linux using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Linux and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the installation of the Veeam Agent for Linux in the offline mode. For details, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.

   Keep in mind that if you use the APT package manager and the installation command reports that some dependencies for package not installed, run the following command instead:

   ```
   apt-get install -f
   ```

   After that, repeat the Veeam Agent installation procedure.

Configuration

To configure Veeam Agent for Linux, you must apply connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. To do this, run the following command from the directory where Veeam Agent setup files are located:

```
veeamconfig mode setVBRsettings --cfg <protection_group_name>.xml
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `--cfg` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. After you apply new backup policy settings in the Veeam Backup & Replication console, Veeam Agent will get these settings during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Deploying Veeam Agent for Unix

To deploy Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Unix and all the required components, do the following:

1. Upload the installation archive to a directory that can be accessed from the computer where you want to install the product and extract setup files from this archive.

   Keep in mind that you must use the Veeam Agent installation archive that is generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have extracted setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Unix. For details, see the following sections:

   - For Veeam Agent for Oracle Solaris, see the Installing Veeam Agent section in the Veeam Agent for Oracle Solaris User Guide.
   - For Veeam Agent for IBM AIX, see the Installing Veeam Agent section in the Veeam Agent for IBM AIX User Guide.

Configuration

To configure Veeam Agent for Unix, you must apply connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. To do this, run the following command from the folder where Veeam Agent setup files are located:

```
veeamconfig mode setVBRsettings --cfg <protection_group_name>.xml
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `--cfg` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with the Veeam backup server every 6 hours. After you apply the connection settings, Veeam Agent will use them to connect to backup server during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Deploying Veeam Agent for Mac

To deploy Veeam Agent for Mac using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Mac and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Mac. For details, see the Installing Veeam Agent section in the Veeam Agent for Mac User Guide.

3. Grant full disk access to Veeam Agent for Mac. For details, see the Granting Full Disk Access section in the Veeam Agent for Mac User Guide.

Alternatively, you use install Veeam Agent and grant full disk access using a Mobile Device Management (MDM) solution. For details, see the Installation and Configuration with MDM Solution section in the Veeam Agent for Mac User Guide.

Configuration

To configure Veeam Agent for Mac, you must import connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. For details, see the Importing Configuration section in the Veeam Agent for Mac User Guide.

If you use the MDM solution to install Veeam Agent, you must deploy the configuration file as a device profile. For details, see Installation and Configuration with MDM Solution in the Veeam Agent for Mac Use Guide.

Keep in mind that you may need one of the following configuration files depending on the solution that you use:

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

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

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with the Veeam backup server every 6 hours. After you apply the connection settings, Veeam Agent will use them to connect to backup server during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Adding Protection Group to Backup Job

You can quickly add an entire protection group to a Veeam Agent backup job configured in Veeam Backup & Replication.

NOTE

- You can add a protection group for pre-installed Veeam Agents only to a Veeam Agent backup job managed by Veeam Agent. Veeam Agent backup jobs managed by the backup server are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.
- You can add only a protection group for pre-installed Veeam Agents to a backup job for Unix and macOS computers. Other protection groups are not supported for computers running these OSes. To learn more, see Protection Group Types.
- If you add a protection group that contains computers running different OSes to a Veeam Agent backup job for computers running a certain OS, Veeam Backup & Replication will automatically exclude computers running other OSes from this backup job.

  For example, if you add protection group that contains Microsoft Windows, Linux, and Mac computers to a Veeam Agent backup job for Linux computers, Veeam Backup & Replication will automatically exclude Microsoft Windows and Mac computers from this backup job.

To add a protection group to a Veeam Agent backup job:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and do one of the following:

   For Microsoft Windows computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Windows** > *name of the job* on the ribbon.
   - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Windows** > *name of the job*.

   For Linux computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Linux** > *name of the job* on the ribbon.
   - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Linux** > *name of the job*.

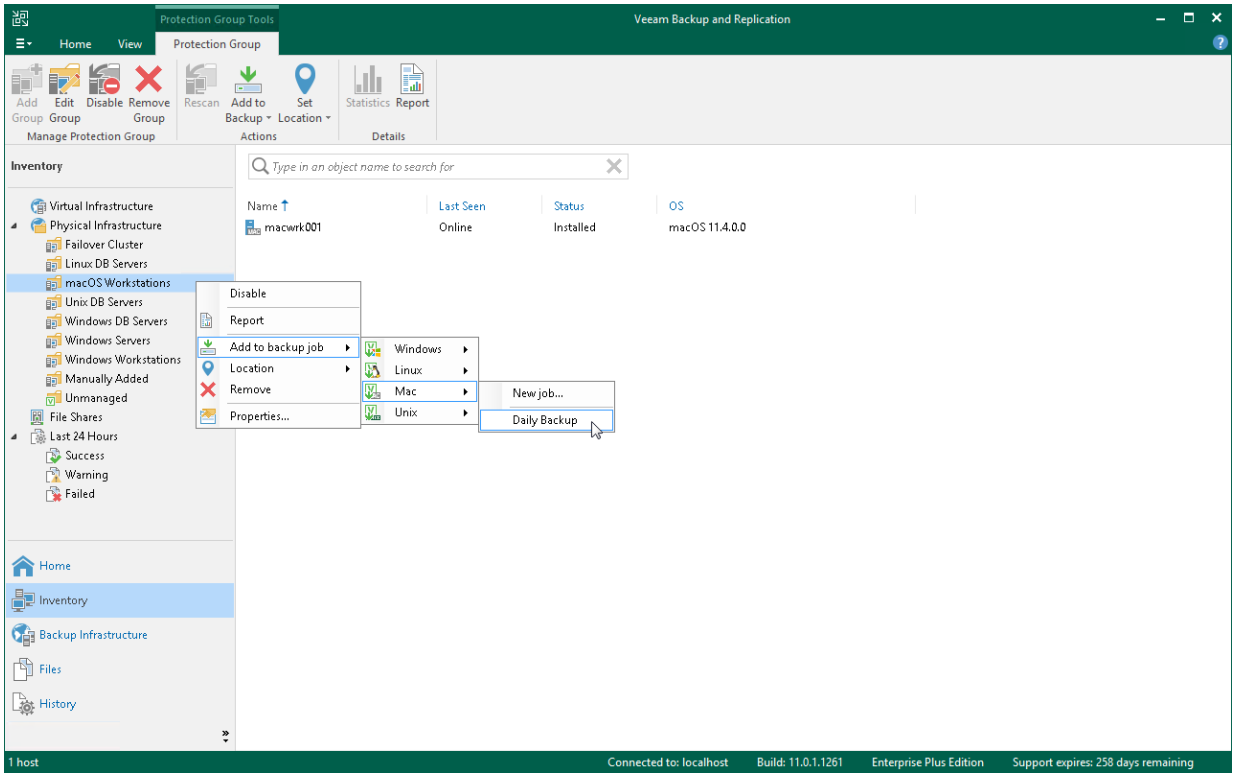
   [For protection groups for pre-installed Veeam Agents] For Unix computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Unix** > *name of the job* on the ribbon.
   - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Unix** > *name of the job*.

   [For protection groups for pre-installed Veeam Agents] For Mac computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Mac** > *name of the job* on the ribbon.

- In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Mac** > *name of the job*.



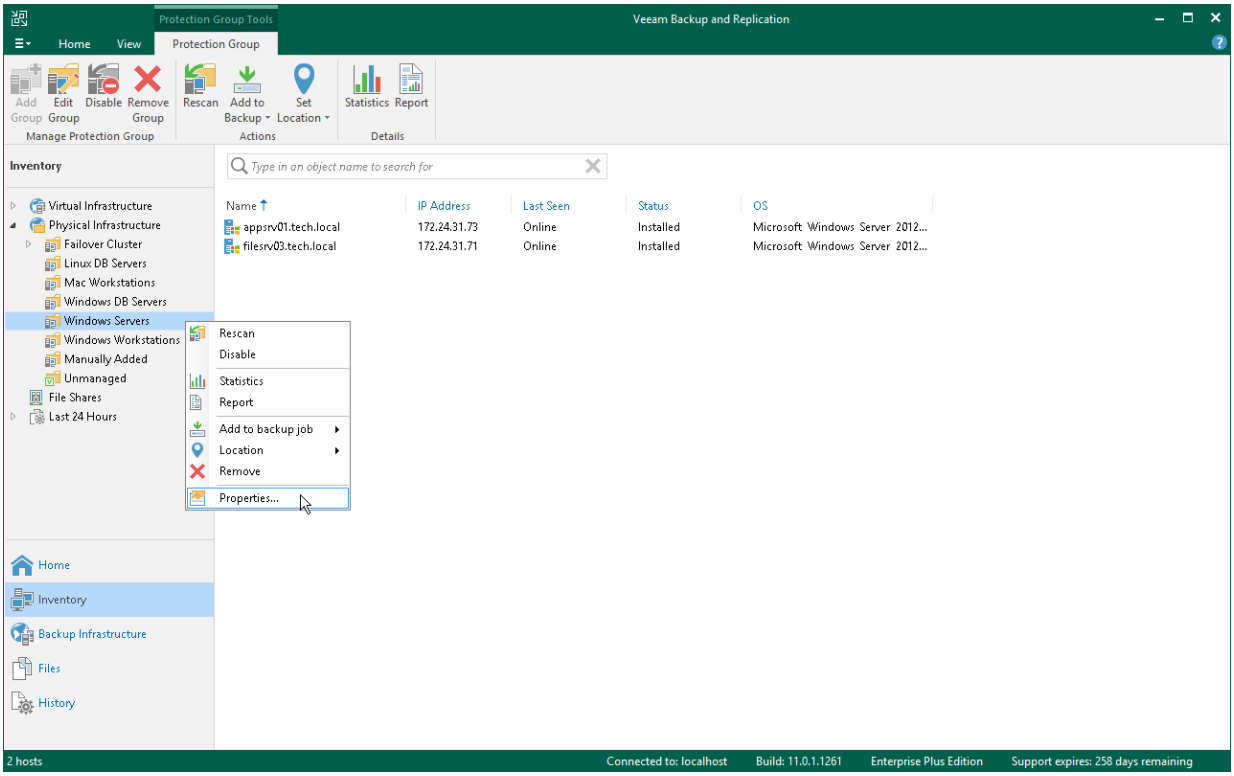
Editing Protection Group Settings

You can edit settings of a protection group. This operation may be required, for example, if you want to add/remove computers to/from a protection group or change settings for protected computers discovery and Veeam Agent deployment defined in the properties of the protection group.

> **NOTE**
>
> Consider the following:
>
> - You cannot change the type of a protection group when editing protection group settings.
> - For the *Manually Added* protection group, you can change only a limited number of settings. In particular, you can edit protected computers discovery and Veeam Agent deployment options (except for changing the distribution server for the protection group). You can also remove from this protection group computers that are no longer included in a Veeam Agent backup job.
> - You cannot edit settings of default protection groups that act as filters used to display protected computers of a specific type: *Unmanaged*, *Out of Date*, *Offline* and *Untrusted*.

To edit protection group settings:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the protection group that you want to edit and click **Edit Group** on the ribbon or right-click the protection group that you want to edit and select **Properties**.
4. Edit protection group settings as required.



Rescanning Protection Group

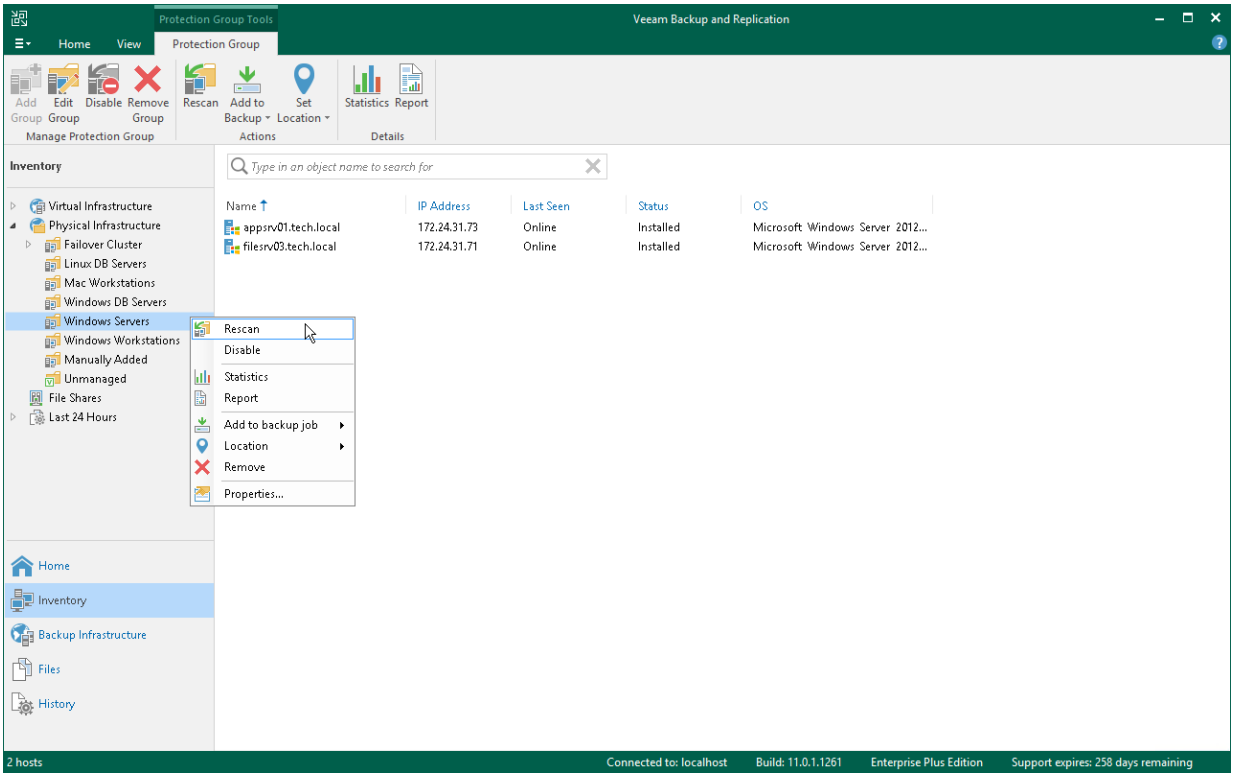
You can rescan a protection group configured in the inventory. When you perform protection group rescan, you manually start the discovery process for the protection group. This operation may be required, for example, if you want to discover new computers added to the protection group without waiting for the next scheduled start of the rescan job.

> **NOTE**
>
> You cannot rescan a protection group for pre-installed Veeam Agents. To learn more, see Protection Group Types.

During the rescan operation, Veeam Backup & Replication starts the rescan job in the same way as in case of scheduled discovery. The rescan job connects to computers included in the protection group and performs on these computers operations specified in the protection group settings. For example, if Veeam Backup & Replication is set up to automatically install Veeam Agent on protected computers during discovery, you can use the rescan operation to deploy Veeam Agent to computers that have appeared in the protection group after the previous scheduled rescan job session finished.

To rescan a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.

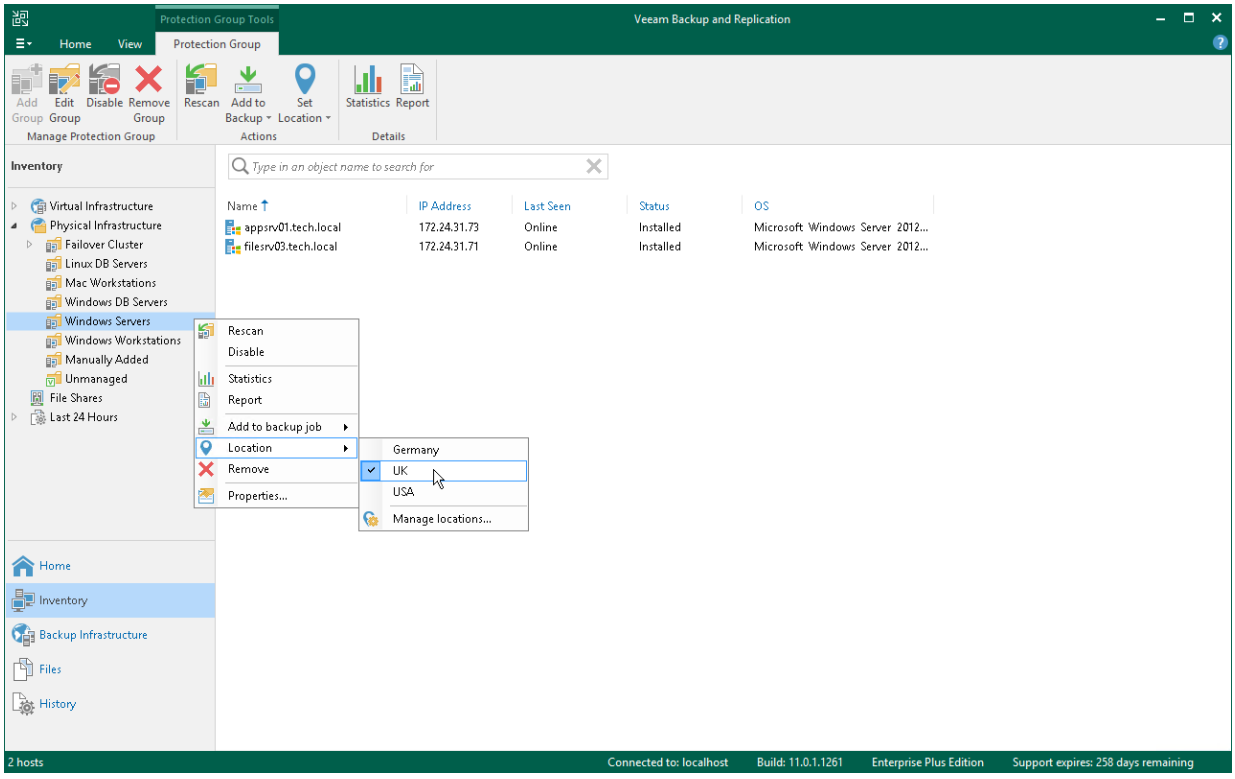


Assigning Location to Protection Group

You can assign a location to a protection group configured in Veeam Backup & Replication. To assign a location:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Location** > *<Location name>* on the ribbon or right-click the necessary protection group and select **Location** > *<Location name>*.

To learn more about locations, see the Locations section in the Veeam Backup & Replication User Guide.



Disabling Protection Group

You can temporary disable a protection group configured in the inventory. When you disable a protection group, you disable scheduled discovery of protected computers added to this protection group. This may be required, for example, if a new version of Veeam Agent appears on a distribution server, and you do not want to deploy Veeam Agent to all protected computers at once. Instead, you can disable the protection group, test the deployment process on a specific computer in this group, and then enable the protection group to let Veeam Backup & Replication deploy Veeam Agent to remaining computers.

When you disable a protection group, Veeam Backup & Replication does not start the rescan job upon schedule defined in the protection group settings. However, you can start the discovery process manually if needed. To learn more, see Rescanning Protection Group.

Disabling a protection group does not affect processing of Veeam Agent computers included in this protection group. If a protected computer is added to a Veeam Agent backup job, and the backup job is scheduled to start at the time when the protection group is in the disabled state, the backup job will run as usual.

> **NOTE**
>
> You cannot disable default protection groups that act as filters used to display protected computers of a specific type: *Unmanaged*, *Out of Date*, *Offline* and *Untrusted*.

To disable automatic discovery for the protection group:

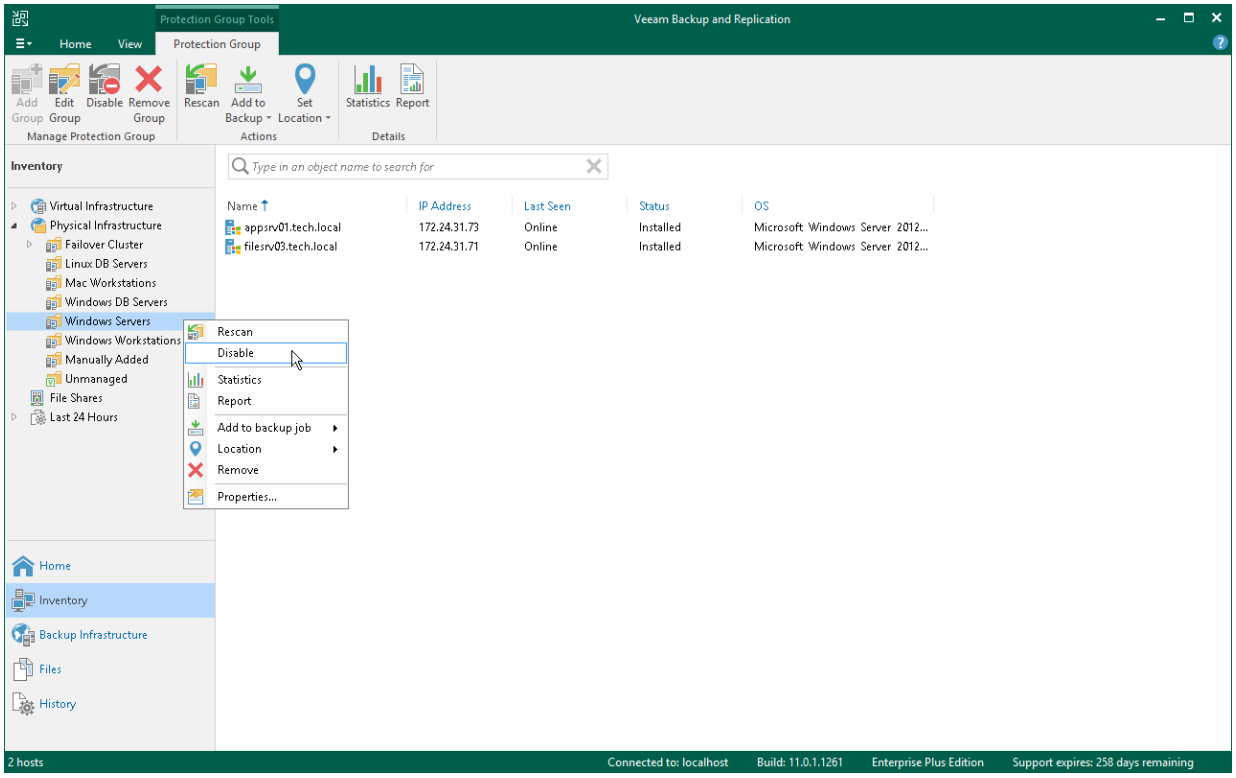
1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.

To enable automatic discovery for the protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.

TIP

After you disable a protection group for pre-installed Veeam Agents, Veeam Backup & Replication does not add new members to this protection group. If the Veeam Agent computer user tries to connect to the Veeam backup server with the configuration file, the user will get an error message. To learn more about protection group types, see Protection Group Types.



Removing Protection Group

You can remove a protection group that you configured.

When you remove a protection group, you can instruct Veeam Backup & Replication to remove Veeam Agents from all protected computers included in this protection group, too. The protection group is removed permanently. You cannot undo this operation.

Backups created for computers that were included in the removed protection group remain intact in the backup location. You can delete this backup data manually later if needed.

NOTE

Consider the following:

- You cannot remove a protection group if the entire protection group or a separate computer included in this protection group is added to a Veeam Agent backup job.
- You cannot remove default protection groups, such as *Manually Added*, *Unmanaged*, and so on.

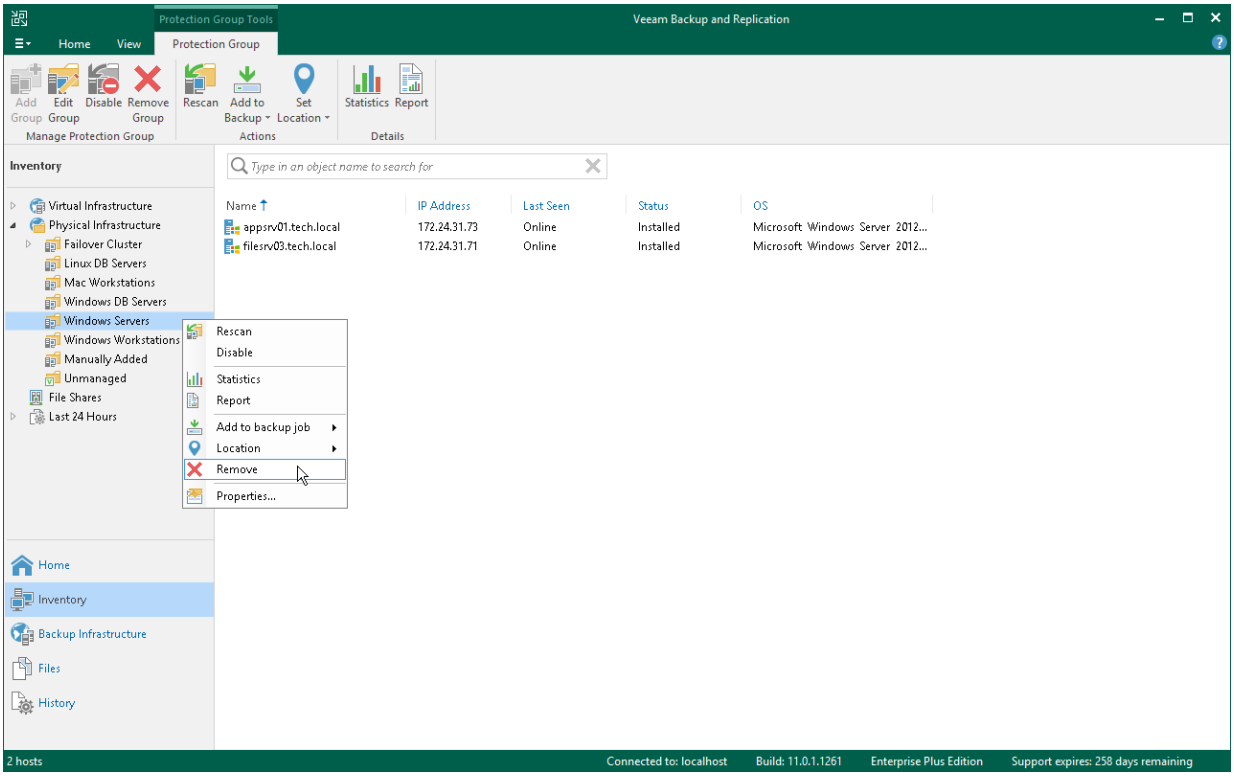
TIP

You can also remove separate computers from protection groups. To learn more, see Removing Computer from Protection Group.

To remove a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the protection group that you want to remove and click **Remove Group** on the ribbon or right-click the protection group and select **Remove**.
4. If you want to remove Veeam Agent deployed on protected computers, in the displayed window, select the **Uninstall Agents** check box. With this option selected, Veeam Backup & Replication will remove the protection group from the configuration database and, in addition, uninstall Veeam Agent and Veeam Installer Service from every computer in the deleted protection group.

5. In the displayed window, click **Yes**.



Working with Veeam Agent Backup Jobs and Policies

To back up data of your protected computers, you must configure a Veeam Agent backup job in Veeam Backup & Replication. The Veeam Agent backup job defines what data to back up, how, where and when to back up data. One Veeam Agent backup job can be used to process one or more protected computers.

In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

- *The backup job* that runs on the backup server in the similar way as a regular job for VM data backup. The backup job is intended for protected computers that have permanent connection to the backup server. To learn more, see Backup Job.
- *The backup policy* that describes configuration of individual Veeam Agent backup jobs that run on protected computers. Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to Veeam Agents that run on computers added to the backup policy. The backup policy is intended for protected computers that may have limited connection to the backup server. To learn more, see Backup Policy.

To learn more, see Veeam Agent Backup Jobs and Policies.

After you configured a Veeam Agent backup job in Veeam Backup & Replication, you can manage it in Veeam Backup & Replication as well. Operations available for a Veeam Agent backup job depend on the job mode specified in the job properties:

- For a Veeam Agent backup jobs managed by the backup server, Veeam Backup & Replication allows you to perform a set of operations similar to a regular backup job for VM data backup. To learn more, see Managing Veeam Agent Backup Jobs.
- For a Veeam Agent backup job managed by Veeam Agent, or backup policy, Veeam Backup & Replication allows you to perform a set of operations similar to a regular Veeam Agent backup job configured on a Veeam Agent computer. To learn more, see Managing Veeam Agent Backup Policies.

One protected computer may be processed with one or more Veeam Agent backup jobs. To learn more, see Processing One Computer with Multiple Jobs and Policies.

Creating Veeam Agent Backup Jobs

To create a Veeam Agent backup job, you must create a Veeam Agent backup job in Veeam Backup & Replication with the **Managed by backup server** option selected in the job settings.

Veeam Backup & Replication lets you create backup jobs for the following types of protected computers:

- Microsoft Windows computers protected with Veeam Agent for Microsoft Windows
- Linux computers protected with Veeam Agent for Linux

If you want to protect a computer running Unix or macOS, you must create a Veeam Agent backup policy. For details, see Creating Policy for Unix Computers and Creating Agent Backup Policy for Mac Computers.

Creating Job for Windows Computers

To back up data of a computer protected with Veeam Agent for Microsoft Windows, you must configure a Veeam Agent backup job in Veeam Backup & Replication.

Before You Begin

Before you create a Veeam Agent backup job in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup job.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the job must be configured in advance.
- [For backup jobs targeted at the cloud repository] The Veeam Cloud Connect service provider must be added in the Veeam backup console.

Veeam Agent backup jobs have the following limitations:

- For Veeam Agent backup job managed by backup server, you can create Veeam Agent backups on a Veeam backup repository and Veeam Cloud Connect repository. If you want to save backups in other target locations, you must configure a Veeam Agent backup job managed by Veeam Agent (backup policy). To learn more, see Veeam Agent Backup Jobs and Policies.
- [For Veeam Agent backup job managed by Veeam Agent] You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent for Microsoft Windows does not support file-level backup for backup jobs that include clusters.
- Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.
- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup job settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- The backup cache is supported only for Veeam Agent backup jobs managed by Veeam Agent.
- You cannot use a Microsoft OneDrive storage as a target for a Veeam Agent backup job configured in Veeam Backup & Replication.
- Veeam Agent does not support creating transaction log backups in a cloud repository. You cannot enable transaction log backup options in the properties of the backup job targeted at a cloud repository.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job for protected computers that run a Microsoft Windows OS in one of the following ways:

- Create a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.
- Add a protection group to a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.
- Add individual computers to a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.

Launching Backup Job Wizard

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

- On the **Home** tab, click **Backup Job** > **Windows computer**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Windows computer** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Windows computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Windows** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup job and click **Add to Backup** > **Windows** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the job. You can add other protection groups and (or) individual computers to the job later on, when you pass through the wizard steps.

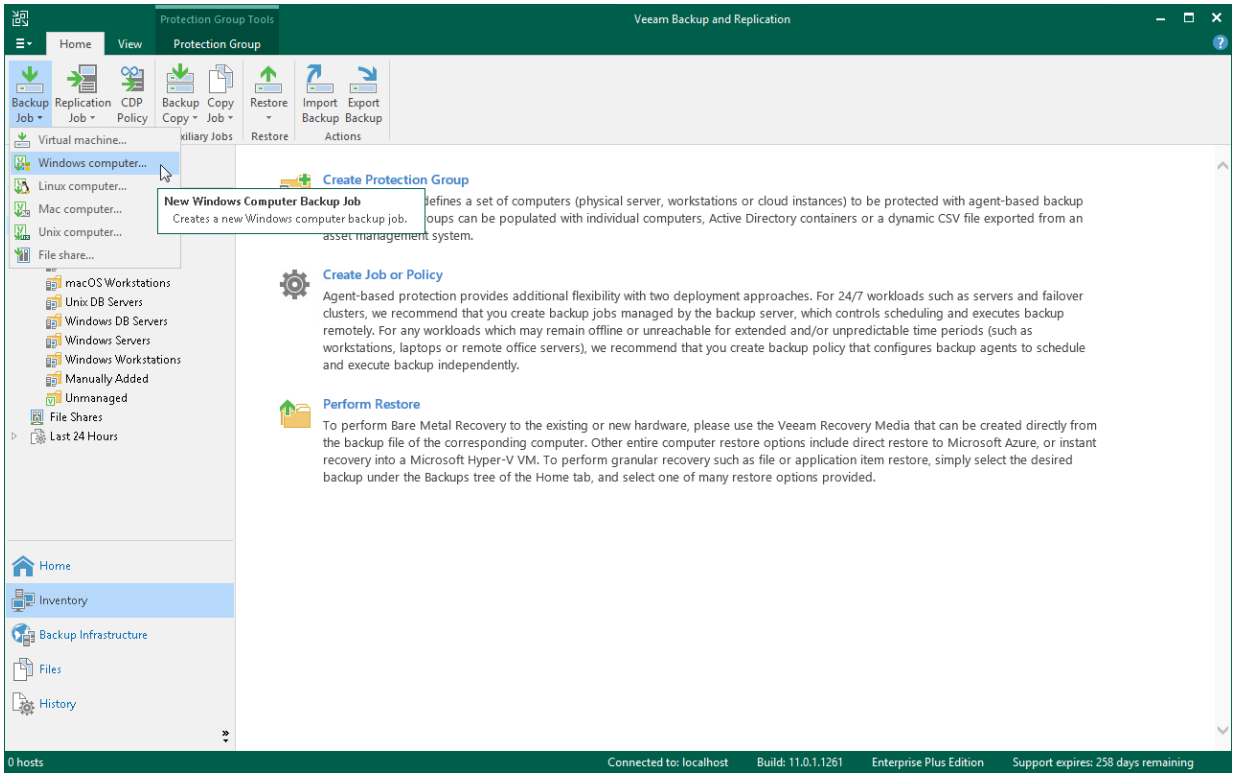
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job, right-click the selected computer and select **Add to backup job** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job and click **Add to Backup** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the job. You can add other computers and (or) protection groups to the job later on, when you pass through the wizard steps.

> **TIP**
>
> Consider the following:
>
> - You can press and hold **[CTRL]** to select multiple computers at once.
> - You can add an individual computer or protection group to a Veeam Agent backup job that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.



Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the backup job:

1. Select the type of protected computers whose data you want to back up with Veeam Agents.
2. If you choose to back up data pertaining to servers, select the job mode.

   The job mode defines the type of the created Veeam Agent backup job: the backup job (backup job managed by the backup server) or backup policy (backup job managed by Veeam Agent).

Selecting Protected Computer Type

At the **Job Mode** step of the wizard, in the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents. The selected type defines what modes will be available for the configured backup job and what job settings will be available at subsequent steps of the wizard. You can select one of the following computer types:

- **Workstation** — select this option if you want to back up data pertaining to workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  For backup jobs that process workstations, Veeam Backup & Replication offers settings similar to the settings of the backup job available in the *Workstation* edition of Veeam Agent for Microsoft Windows. To learn more, see Veeam Agent for Microsoft Windows User Guide.

  With this option selected, the backup job will be managed by Veeam Agent installed on the protected computer — you do not need to select the job mode.

- **Server** — select this option if you want to back up data pertaining to standalone servers. This option is suitable for computers that have permanent connection to the backup server.

  For backup jobs that process servers, Veeam Backup & Replication offers settings similar to the settings of the backup job available in the *Server* edition of Veeam Agent for Microsoft Windows. To learn more, see Veeam Agent for Microsoft Windows User Guide.

  With this option selected, you can also select the job mode. To learn more, see Selecting Job Mode.

- **Failover cluster** — select this option if you want to back up data pertaining to a failover cluster.

  For backup jobs that process failover clusters, Veeam Backup & Replication offers practically the same backup job settings as for servers.

  With this option selected, the backup job will be managed by the Veeam backup server — you do not need to select the job mode.

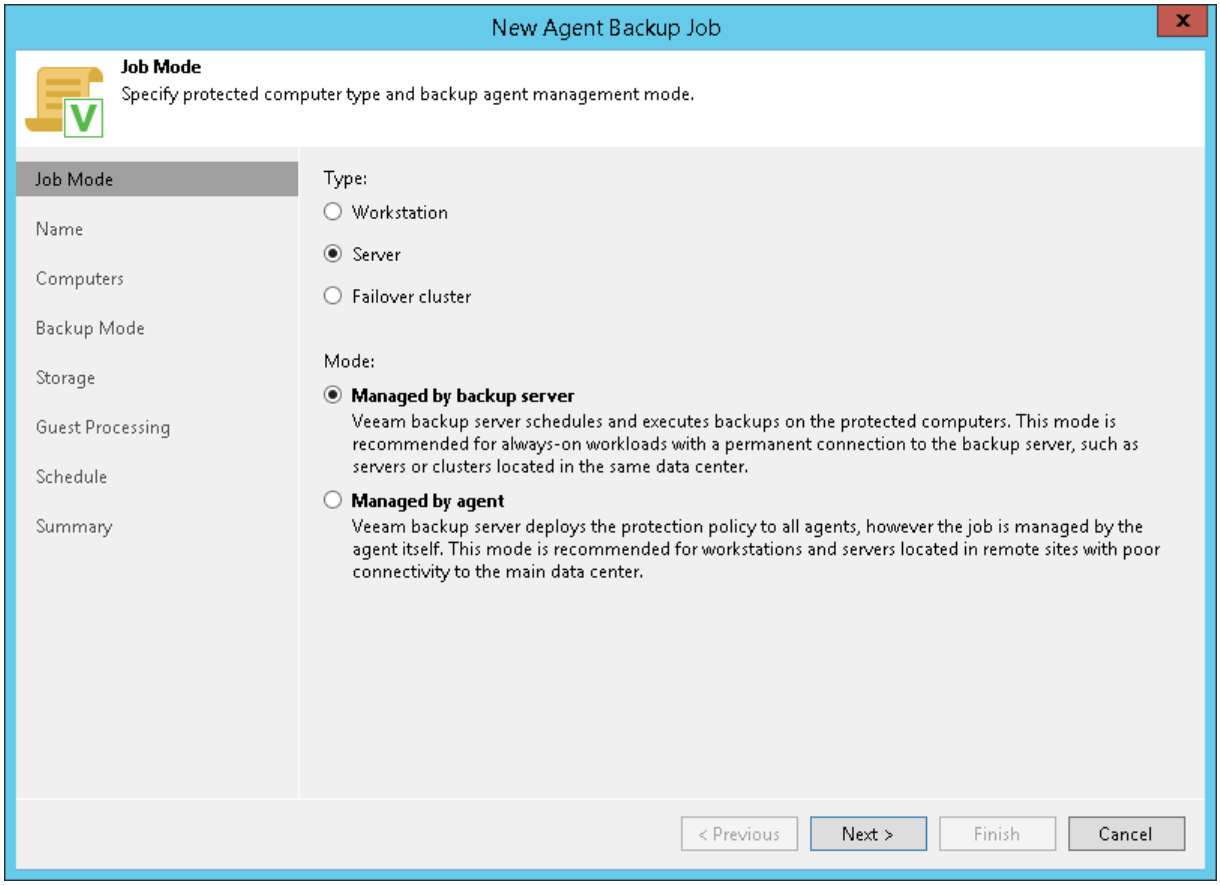
Selecting Job Mode

If you selected the **Server** computer type in the Type field, in the **Mode** field, select the job mode. You can select one of the following modes:

- **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job. With this option selected, you will be able to add one or more individual computers and/or protection groups to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or Veeam Cloud Connect repository. The Veeam Agent backup job will run on the backup server in the similar way as a regular job for VM data backup. To learn more, see Backup Job.
- **Managed by agent** — select this option if you want to configure the backup policy. The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers, and acts as a saved template. With this option selected, you will be able to add one or more individual computers and/or protection groups to the backup policy, and instruct Veeam Agent to create backups on a local disk of a protected computer, in a network shared folder, Veeam backup repository or Veeam Cloud Connect repository. To learn more, see Backup Policy.

NOTE

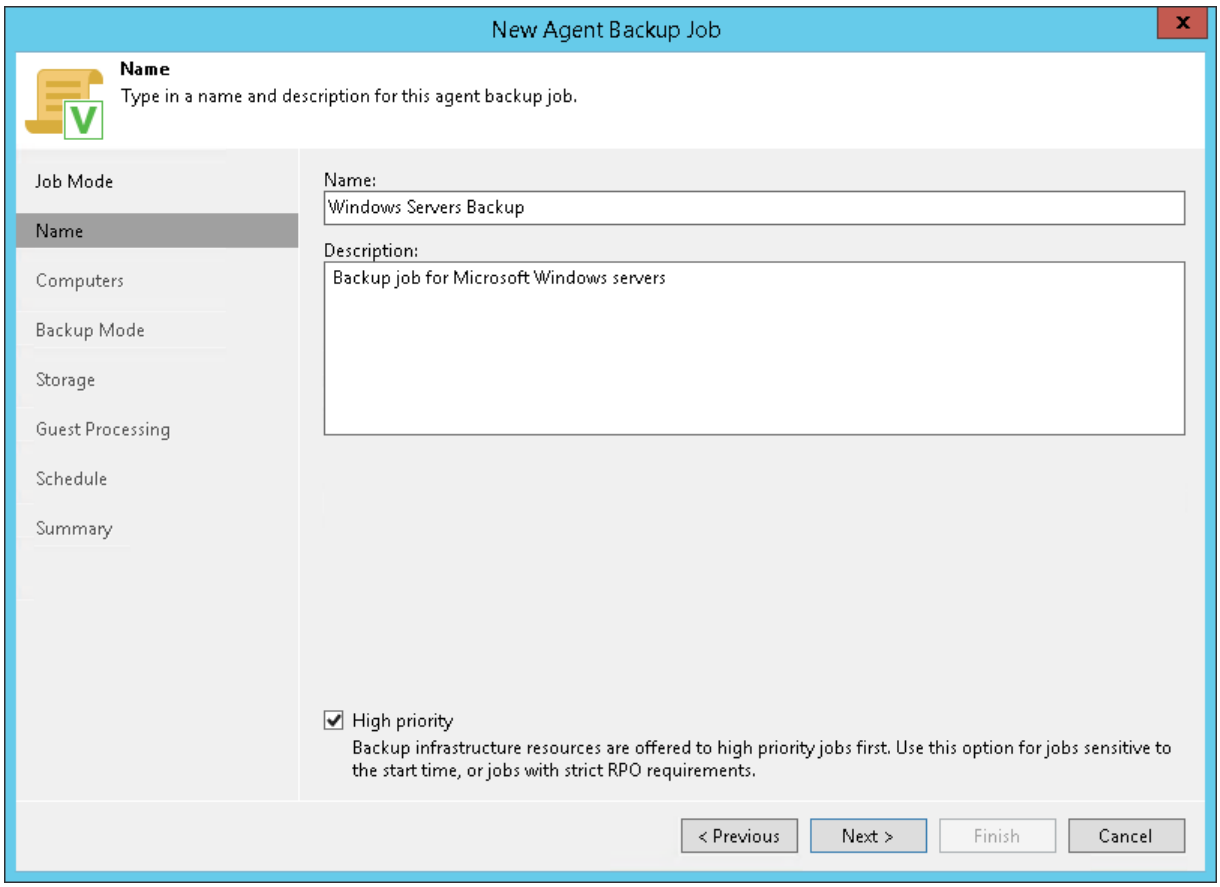
- The **Managed by backup server** option is available for servers and failover clusters. For failover clusters, this is the only available option. This option is not available for workstations.
- The **Managed by agent** option is available for workstations and servers. For workstations, this is the only available option. This option is not available for failover clusters.
- You must select the **Managed by agent** option if you want to use the backup job to protect computers with pre-installed Veeam Agents. To learn more, see Select Protection Group Type.



Step 3. Specify Job Name and Description

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

1. In the **Name** field, enter a name for the backup job.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the job, date and time when the job was created.
3. [For backup job managed by backup server] Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. To learn more, see the Job Priorities section in the Veeam Backup & Replication User Guide.



Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers whose data you want to back up.

You can add to the Veeam Agent backup job one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. You can also add to the job computers that are not added to inventory yet. Veeam Backup & Replication will add such computers to the job and also add them to the *Manually Added* protection group.

Jobs with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup job is created, Veeam Backup & Replication will automatically update the job settings to include the added computer.

NOTE

- If you used the **Add to backup job** > **Windows** > **New job** option to launch the **New Agent Backup Job** wizard, the **Protected computers** list will already contain computers that you have selected to add to the job. You can remove some computers from the job or add new computers to the job, if necessary.
- Veeam Backup & Replication displays protection groups for pre-installed Veeam Agents and their members only if you selected the **Managed by Agent** option at the **Job Mode** step of the wizard. You cannot add protection groups for pre-installed Veeam Agents to backup jobs managed by backup server. To learn more, see Selecting Job Mode.

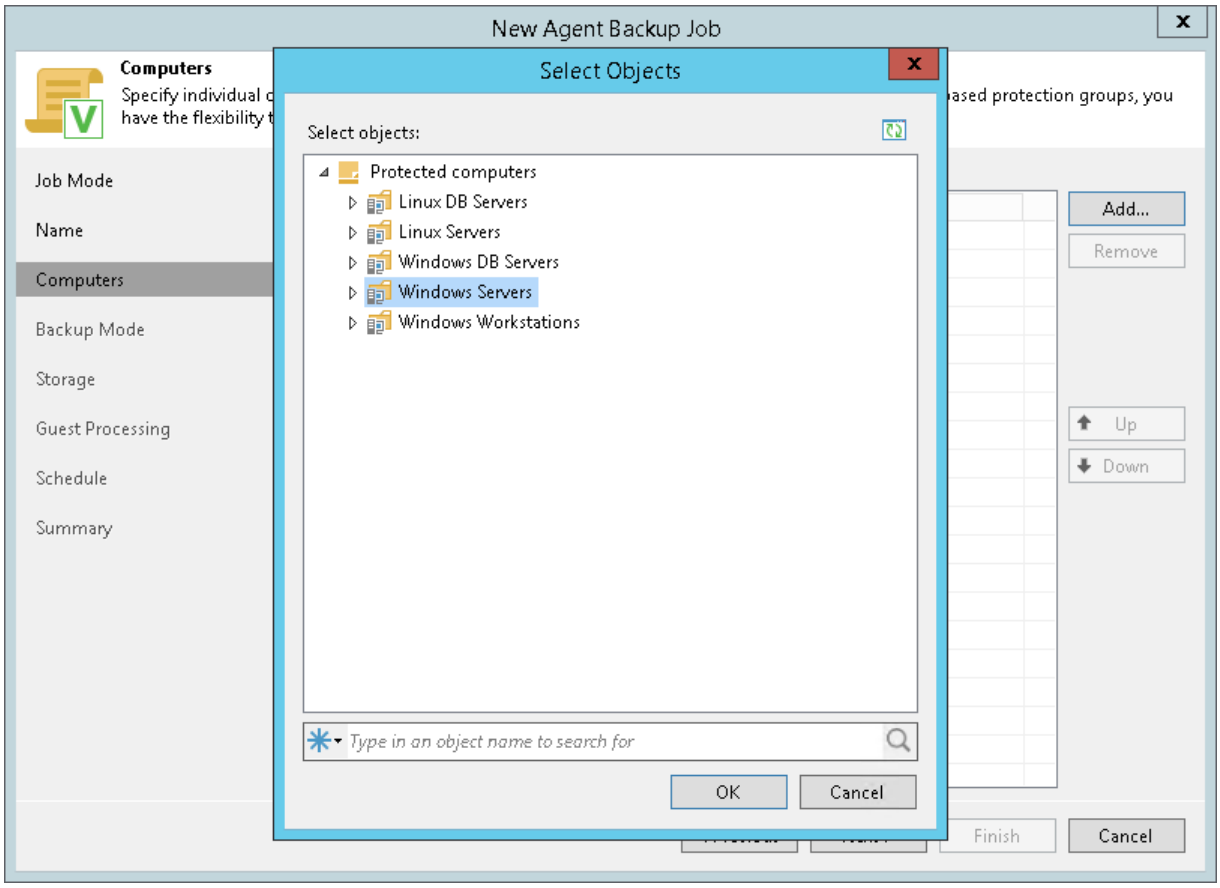
Adding Protection Groups and Computers from Inventory

To add protection groups and/or individual computers to the Veeam Agent backup job:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and/or computers in the list and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

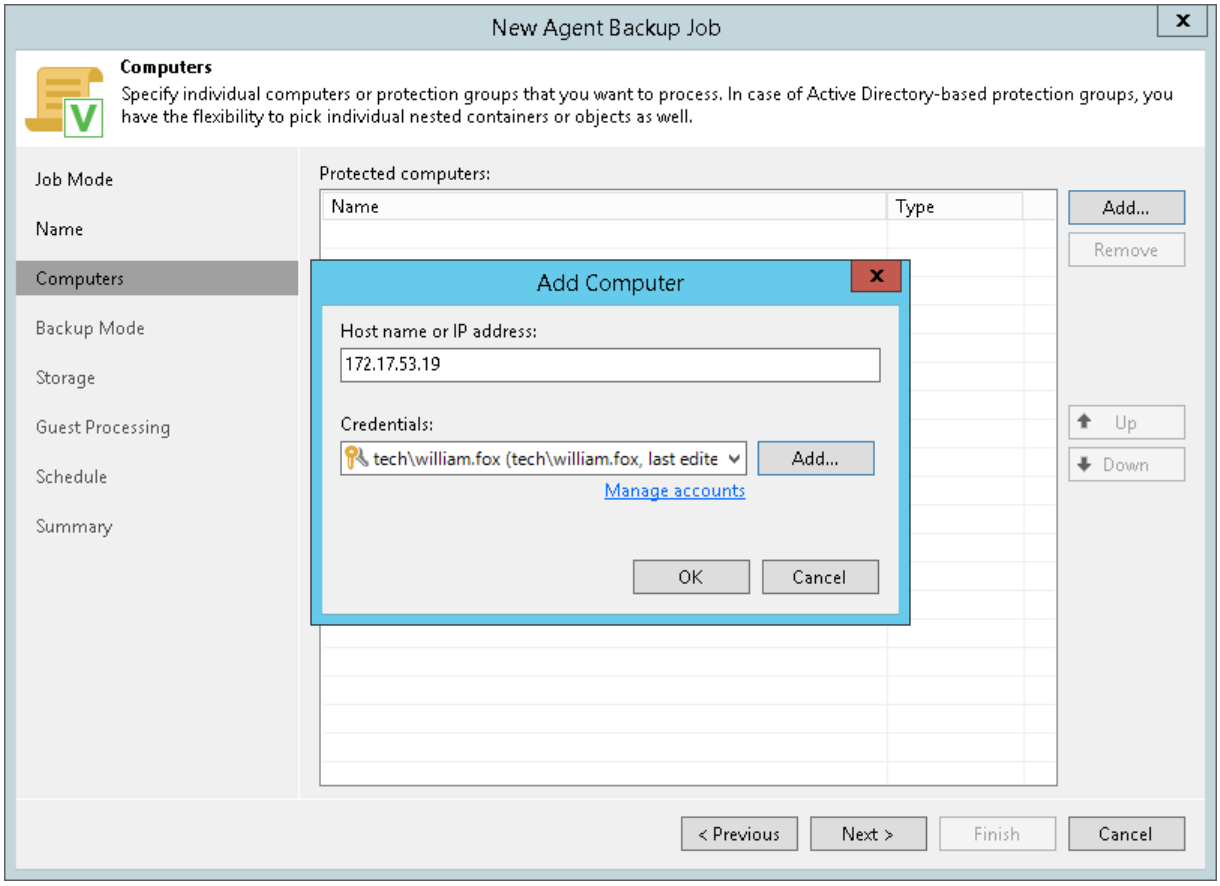
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Adding New Computers

To add to the Veeam Agent backup job new computers that do not exist in the inventory:

1. Click **Add** > **Individual computer**.
2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name or IP address of the computer that you want to add to the job.
3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the job. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.



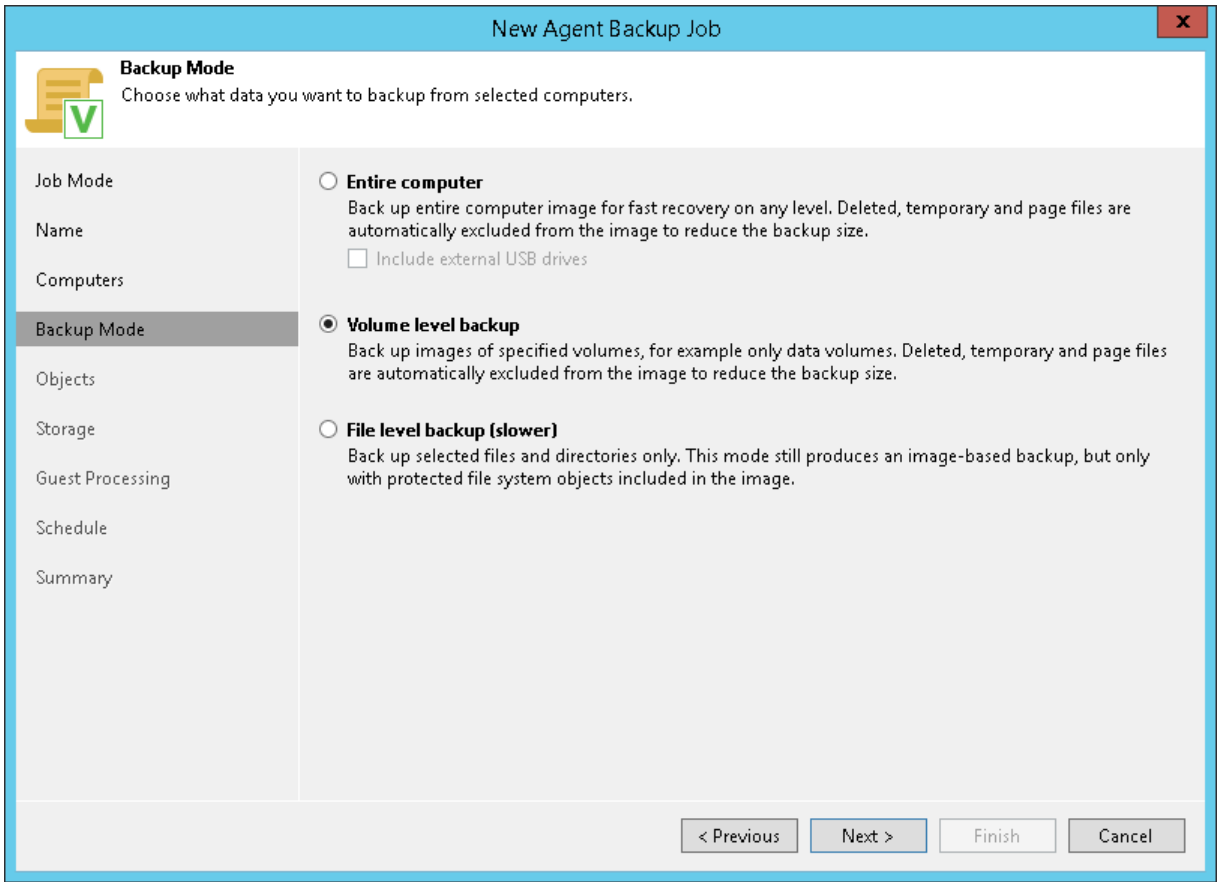
Step 5. Select Backup Mode

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

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:
   - **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on. With this option selected, you will pass to one of the following steps of the wizard:
     - Storage — if you have selected the **Managed by backup server** option at the Job Mode step of the wizard.
     - Destination — if you have selected the **Managed by agent** option at the Job Mode 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 Objects 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 Objects step of the wizard.
2. [For entire computer backup] If you want to include in the backup one or more external USB drives, select the **Include external USB drives** check box. With this option selected, Veeam Agent will include in the backup all external USB drives that are connected to the Veeam Agent computer at the time when the backup job starts. To learn more, see the Backup of External Drives section in the Veeam Agent for Microsoft Windows User Guide.

NOTE

- The **File level backup** option is not available if you have selected the **Failover cluster** option at the Job Mode step of the wizard.
- File-level backup is typically slower than volume-level backup. Depending on the performance capabilities of your computer and backup environment, the difference between file-level and volume-level backup job performance may increase significantly. If you plan to back up all folders with files on a specific volume or back up large amount of data, it is recommended that you configure volume-level backup instead of file-level backup.



Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you chose to create volume-level or file-level Veeam Agent backups. Specify backup scope for the Veeam Agent backup job:

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

Specifying Volumes to Back Up

The **Objects** step of the wizard is available if you have selected the **Volume level backup** option at the Backup Mode step of the wizard.

At this step of the wizard, you must specify the backup scope — define what volumes you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified volume does not exist on one or more computers in the job, the job will skip such volume on those computers and back up only existing ones.

To specify the backup scope, you can select the **Backup the following volumes only** option and add necessary objects.

Alternatively, you can back up the whole Veeam Agent computer. To do this, select the **Backup all volumes except the following** option. With this option selected, you can exclude objects that you do not need from the backup scope.

You can include or exclude the following objects:

- *OS volume* — data pertaining to the OS installed on a protected computer. This object includes the Microsoft Windows system partition and boot partition of your computer. For GPT disks on Microsoft Windows 8.1, 10, 2012, 2012 R2, 2016 and 2019, the object additionally includes the recovery partition. To learn more, see the System State Data Backup section in the Veeam Agent for Microsoft Windows User Guide.

  To include or exclude the OS volume, in the necessary wizard section, click **Add** and select the **OS volume** option.

- *Individual volumes.*

  To include or exclude individual volumes:

  a. In the necessary wizard section, click **Add** and select the **Volume name** option.

  b. In the **Add Object** window, type the drive letter of a volume that you want to back up, for example, `C:\`, and click **OK**.

  c. Repeat steps a-b for all volumes that you want to back up.

- *Individual mount points.*

  To include or exclude individual mount points:

  a. In the necessary wizard section, click **Add** and select the **Volume name** option.

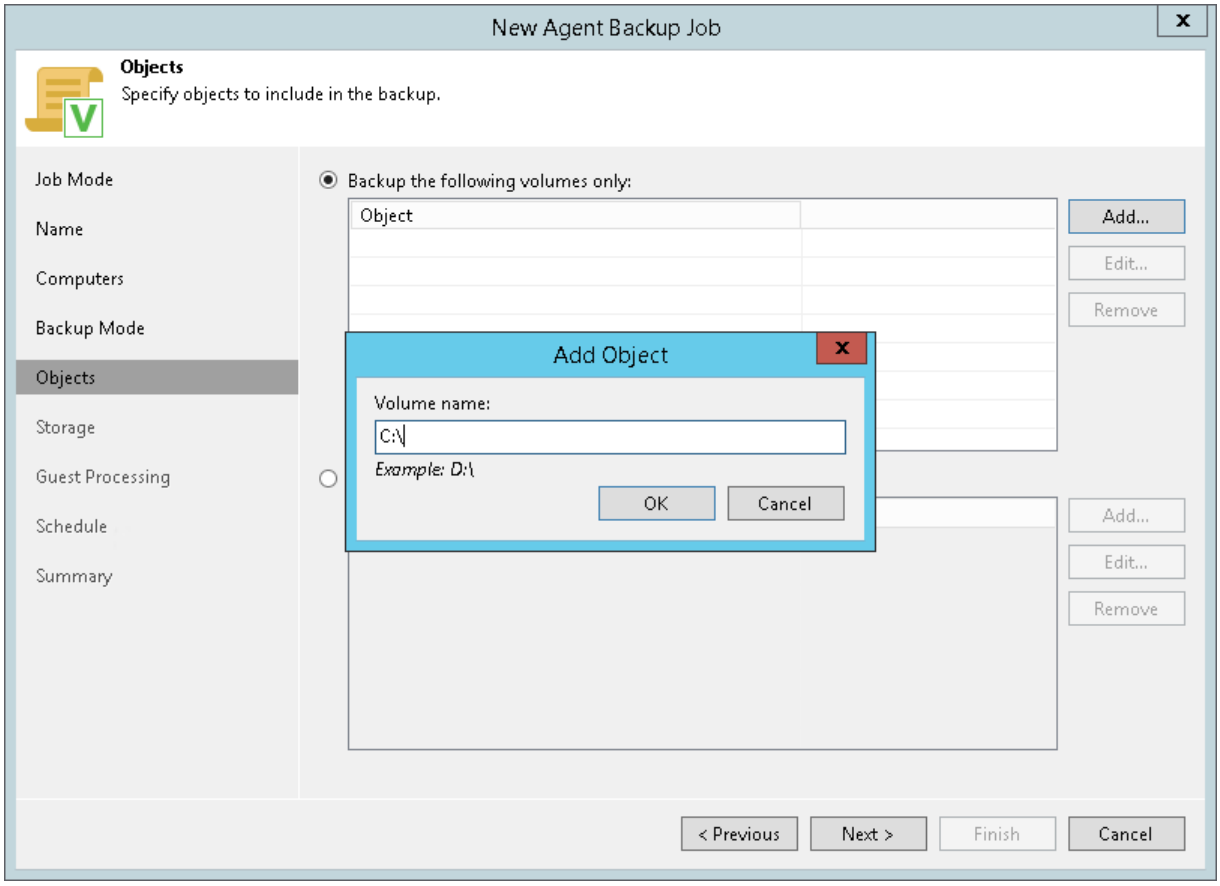
  b. In the **Add Object** window, type the path to a folder that is an entry point to the mounted volume you want to back up, for example, `C:\Data`, and click **OK**.

  c. Repeat steps a-b for all mount points that you want to back up.

NOTE

Mind the following:

- If you include a system volume in the volume-level backup, Veeam Agent for Microsoft Windows automatically includes the System Reserved/UEFI or other system partitions in the backup too.
- Veeam Agent for Microsoft Windows automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.



Specifying Folders to Back Up

The **Objects** step of the wizard is available if you have selected the **File level backup** option at the Backup Mode step of the wizard.

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

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

At this step of the wizard, you must specify the backup scope — define what folders with files or entire volumes you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified object does not exist on one or more computers in the job, the job will skip such object on those computers and back up existing ones.

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

- *Operating system* — data related to the OS installed on a protected computer. To learn more, see the System State Data Backup section in the Veeam Agent for Microsoft Windows User Guide.
- *Personal files* — data related to user profiles. With this option enabled, Veeam Backup & Replication will include in the backup scope settings and data related to Veeam Agent computer user profiles. To learn more, see the Personal Data Backup section in the Veeam Agent for Microsoft Windows User Guide.
- *Individual file system objects* — folders, mount points, and volumes of a protected computer.

To specify individual folders to back up:

1. Select the **The following file system objects** check box and click **Add**.
2. In the **Add Object** window, type the path to a folder, mount point folder, or volume that you want to back up, for example, `D:\Reports` or `D:\`, and click **OK**.

   To specify the backup scope, you can use system environment variables such as *%ProgramFiles%* or *%WinDir%*. This may be useful, for example, in case computers added to the backup job run different versions of Microsoft Windows OSes, and actual paths to directories that contain data of the same type differ on these computers.

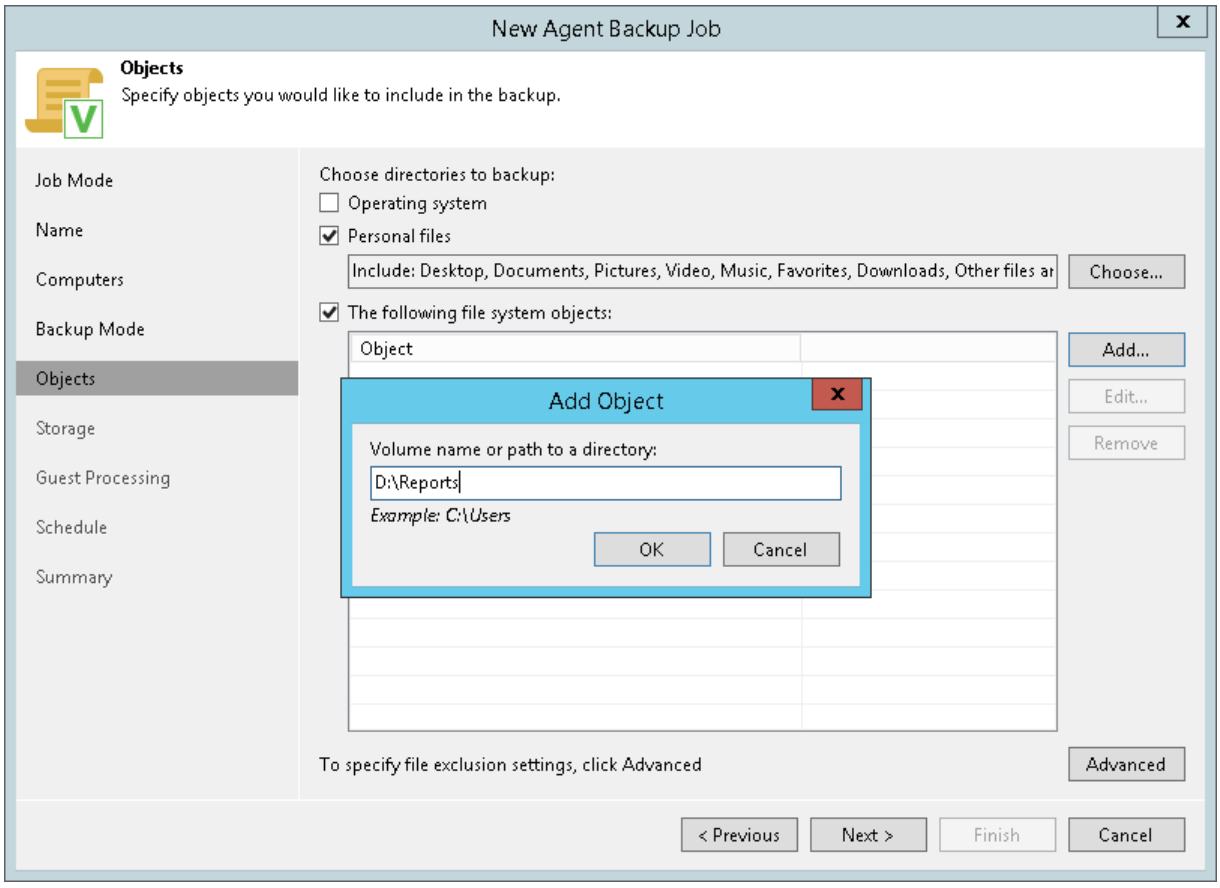
   Consider the following:

   - You can use only system environment variables — variables defined for the Local System account on computers added to the backup job. User-dependent environment variables are not supported.
   - Environment variables that contain multiple values (such as the *%PATH%* variable) are not supported.
   - Environment variables that contain other environment variables are not supported.
3. Repeat steps 1-2 for all items that you want to back up.

NOTE

Mind the following:

- If you include a system volume in the file-level backup, Veeam Agent does not automatically include the System Reserved/UEFI or other system partitions in the backup. These volumes are automatically included in the backup only if you select the *Operating system* option to specify the backup scope.
- Veeam Agent automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.
- You can exclude Microsoft OneDrive folders from the backup scope in the File Filters window.



Configuring Filters

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

> **NOTE**
>
> Consider the following:
>
> - If you include a specific folder in the file-level backup, Veeam Agent applies filters to files in specific folders that you include in the backup. Filters are not applied to computer volumes, mount points, and folders selected for backup. If you plan to create a hybrid backup that will contain volumes, mount points, and folders, filters will be applied to files in folders only.
> - If you include a whole volume in the file-level backup, you cannot apply filters to include or exclude files of a specific type in/from the backup. You can only exclude specific folders that reside on the volume.
> - You cannot apply filters to files and folders that reside on the mount point.

To configure a filter:

1. At the **Objects** step of the wizard, click **Advanced**.
2. Specify what files you want to back up:
   - If you include a specific folder in the file-level backup, in the **Include masks** field, specify file names and/or masks for file types that you want to back up, for example, `MyReport.pdf`, `*filename*`, `*.docx`. The resulting Veeam Agent backup will contain only selected files. Other files will not be backed up.

     You cannot specify include masks if you add an entire volume in the backup.
   - In the **Exclude masks** field, specify files that you do not want to back up in the following ways:
     - If you include an entire volume in the file-level backup, in the **Exclude masks** field, specify paths to folders that contain files that you do not want to back up. The resulting Veeam Agent backup will contain all folders that reside on the backed-up volume except the files in the specified folders.

       For example, you include the `D:\` volume in the backup and specify the `D:\Reports\OldReports` folder in the **Exclude masks** field. The resulting backup will contain all folders and files that reside on the volume except files that reside in the `D:\Reports\OldReports` folder.
     - If you include a specific folder in the file-level backup, in the **Exclude masks** field, specify file names and/or masks for file types that you do not want to back up, for example, `OldReports.rar`, `*.temp`, `*.tmp`, `*.back`. The resulting Veeam Agent backup will contain all files except files whose names match the specified names or masks.

     Keep in mind that depending on the backup type, Veeam Agent excludes files and folders from the backup scope differently:

     - For the volume-level backup, content of folders you do not want to back up is excluded from the VSS snapshot with the FilesNotToSnapshot registry key.

- For the file-level backup, folders and files are excluded by Veeam Agent after the VSS snapshot is created.

As a result, some objects may be excluded or not excluded from the backup scope depending on the type of the created backup. For example, if you configure a volume-level backup, the objects that you excluded may stay in the backup scope due to the FilesNotToSnapshot registry key limitations. To learn more, see this Microsoft article.

3. Click **Add**.
4. Repeat steps 2–3 for each mask that you want to add.

TIP

You can also use system environment variables to specify include and exclude masks. In this case, you must type the back slash (\) symbol in the beginning of the mask. For example: *\%appdata%*.

Consider the following:

- To specify include and exclude masks, you can use only system environment variables — variables defined for the Local System account on computers added to the backup job, and cannot use user environment variables. For example, if you specify the *\%appdata%* exclude mask, Veeam Agent will exclude the `C:\Windows\system32\config\systemprofile\AppData\Roaming` folder from the backup. Application data directories for other user accounts (for example, `C:\Users\Administrator\AppData\Roaming`) will not be excluded from the backup.
- You cannot use environment variables that contain multiple values or other environment variables to specify include and exclude masks.

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

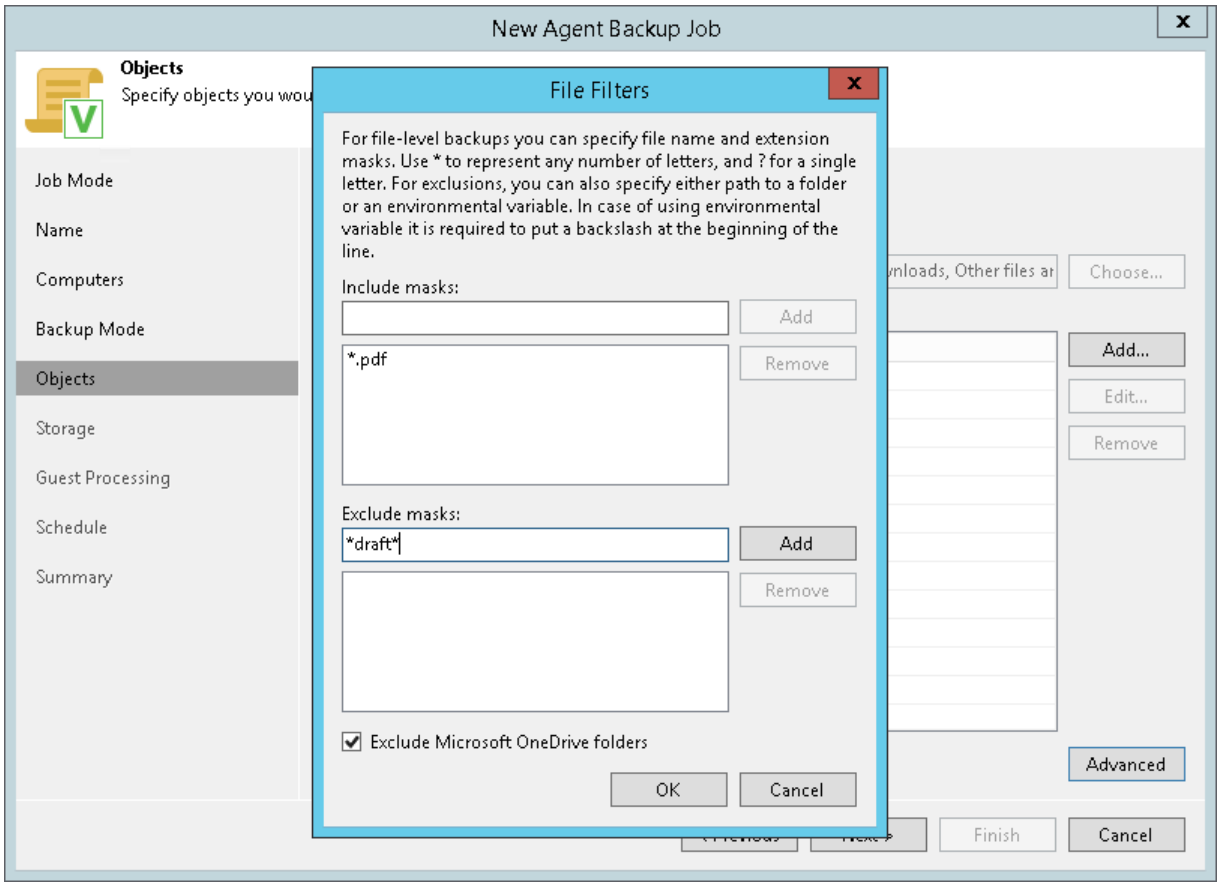
The resulting Veeam Agent backup will contain all files of the PDF format that do not contain *draft* in their names.

Additionally, you can specify how Veeam Agent for Microsoft Windows will process Microsoft OneDrive folders. Select the **Exclude Microsoft OneDrive folders** option to exclude Microsoft OneDrive folders and their content from the backup scope.

Consider the following limitation:

- Veeam Agent excludes Microsoft OneDrive folders only in file-level backups. If you include an entire volume in the backup, Veeam Agent will not exclude Microsoft Onedrive folders from this volume.

- Due to the OS limitations, the **Exclude Microsoft OneDrive folders** option behaves properly only on Veeam Agent computers running Microsoft Windows 10. If your Veeam Agent computers run other OS versions, we recommend to exclude Microsoft OneDrive folders manually.



Step 7. Select Backup Destination

The **Destination** step of the wizard is available if you have selected the **Managed by agent** option at the Job Mode step of the wizard.

At this step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

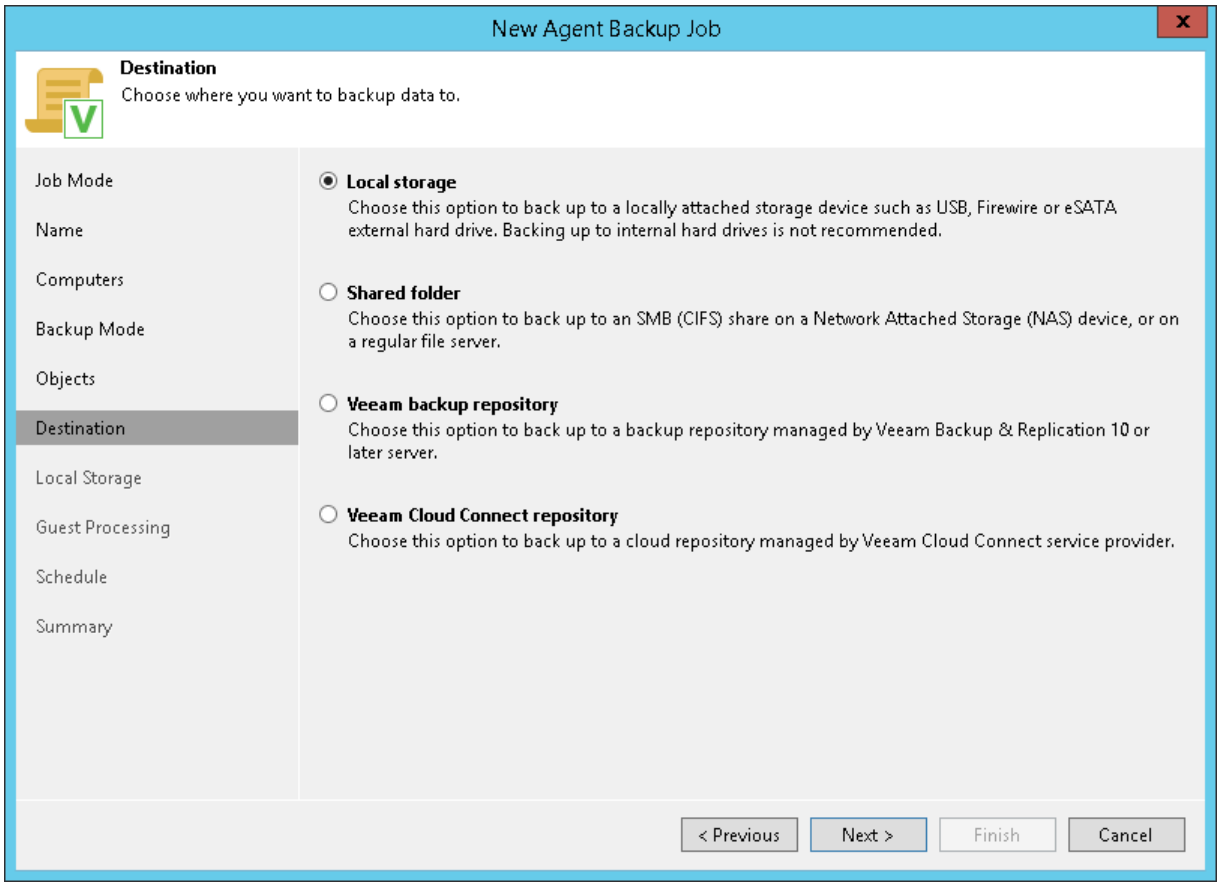
You can store backup files in one of the following locations:

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

> **IMPORTANT**
>
> Consider the following:
>
> - It is strongly recommended that you store backups in the external location like USB storage device or shared network folder. You can also keep your backup files on the separate non-system local drive.
> - If you select to store the backup on a local folder included in the backup scope, Veeam Agent for Microsoft Windows will automatically exclude this folder from the backup.

- **Shared folder** — select this option if you want to save a backup in a network shared folder. With this option selected, you will pass to the Shared folder step of the wizard.
- **Veeam backup repository** — select this option if you want to save a backup on a backup repository managed by the Veeam backup server of which the Veeam Agent backup job is configured. With this option selected, you will pass to the Backup Server step of the wizard.

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



Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- If you have selected the **Managed by backup server** mode at the Job Mode step of the wizard, you can create Veeam Agent backups only on a backup repository managed by this Veeam backup server or on a cloud repository exposed to you by a Veeam Cloud Connect service provider. Specify backup repository settings at the Storage of the wizard.
- If you have selected the **Managed by agent** mode at the Job Mode step of the wizard, specify backup storage settings at one of the following steps of the wizard:
  - Local storage settings — if you have selected the **Local storage** option at the Destination step of the wizard.
  - Shared folder settings — if you have selected the **Shared folder** option at the Destination step of the wizard.
  - Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
  - Cloud repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.

Backup Storage Settings

The **Storage** step of the wizard is available if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store Veeam Agent backups. You can select from the following types of backup repositories:
   - Veeam backup repository configured on the backup server that will manage the created backup job.
   - Cloud repository allocated to your tenant account by a Veeam Cloud Connect service provider.

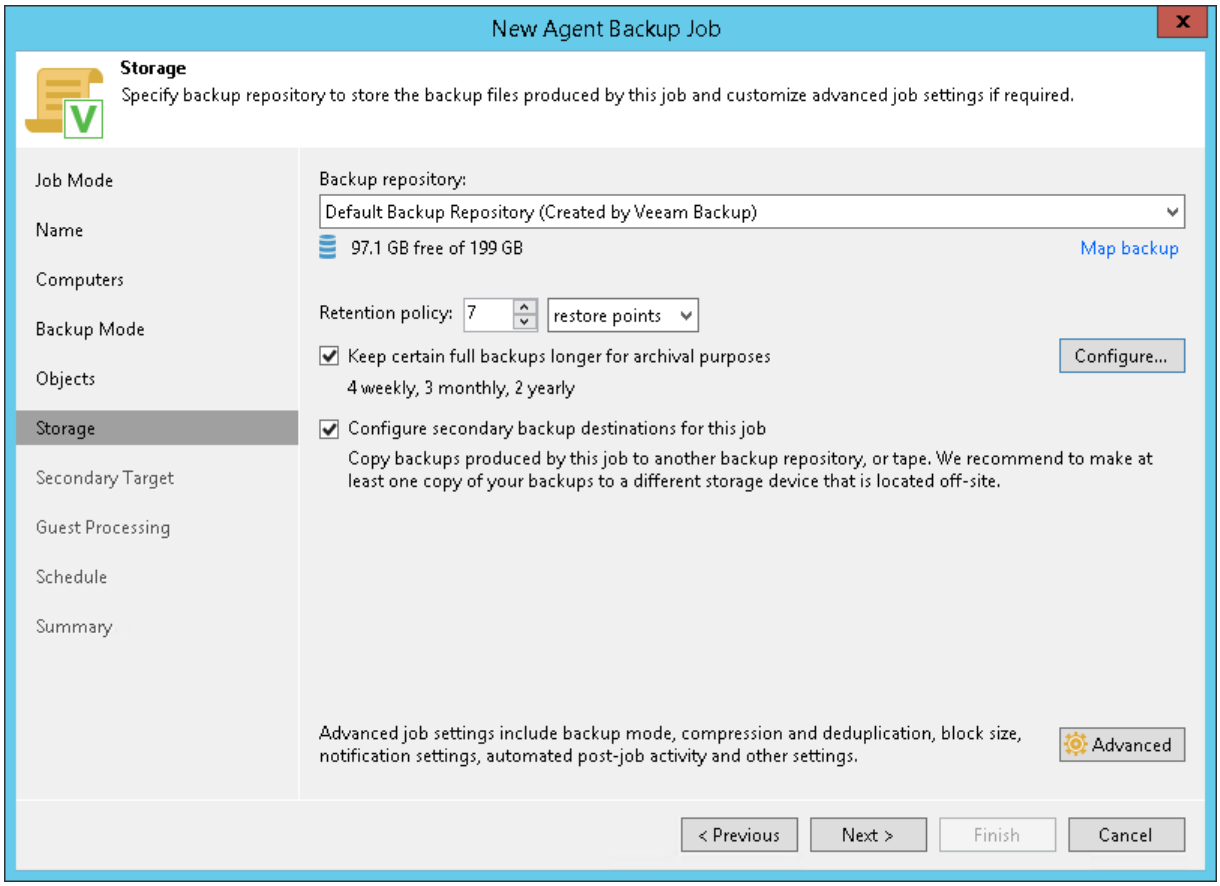
   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. You can map the job to a specific backup stored on the backup repository. Backup job mapping can be helpful if you have moved backup files to a new backup repository and want to point the job to existing backups on this new backup repository. You can also use backup job mapping if the configuration database got corrupted and you need to reconfigure backup jobs.

   To map the job to a backup, click the **Map backup** link and select the backup on the backup repository. Backups can be easily identified by job names. To find the backup, you can also use the search field at the bottom of the window.

   > **NOTE**
   >
   > Mind the following:
   >
   > - Backup job mapping is available only for a Veeam Agent backup job managed by the backup server.
   > - You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created by Veeam Agent operating in the standalone mode.

3. Specify short-term backup retention policy settings in one of the following ways:
   - From the **Retention policy** list, select *restore points* and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the **Retention policy** list, select *days* and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.
5. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — **Secondary Target**. At the **Secondary Target** step of the wizard, you can link the backup job to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.
6. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



Local Storage Settings

The **Local Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save the backup on a local drive of your computer.

Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent for Microsoft Windows will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup job settings to this computer.

   > **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.

2. Specify short-term backup retention policy settings in one of the following ways:

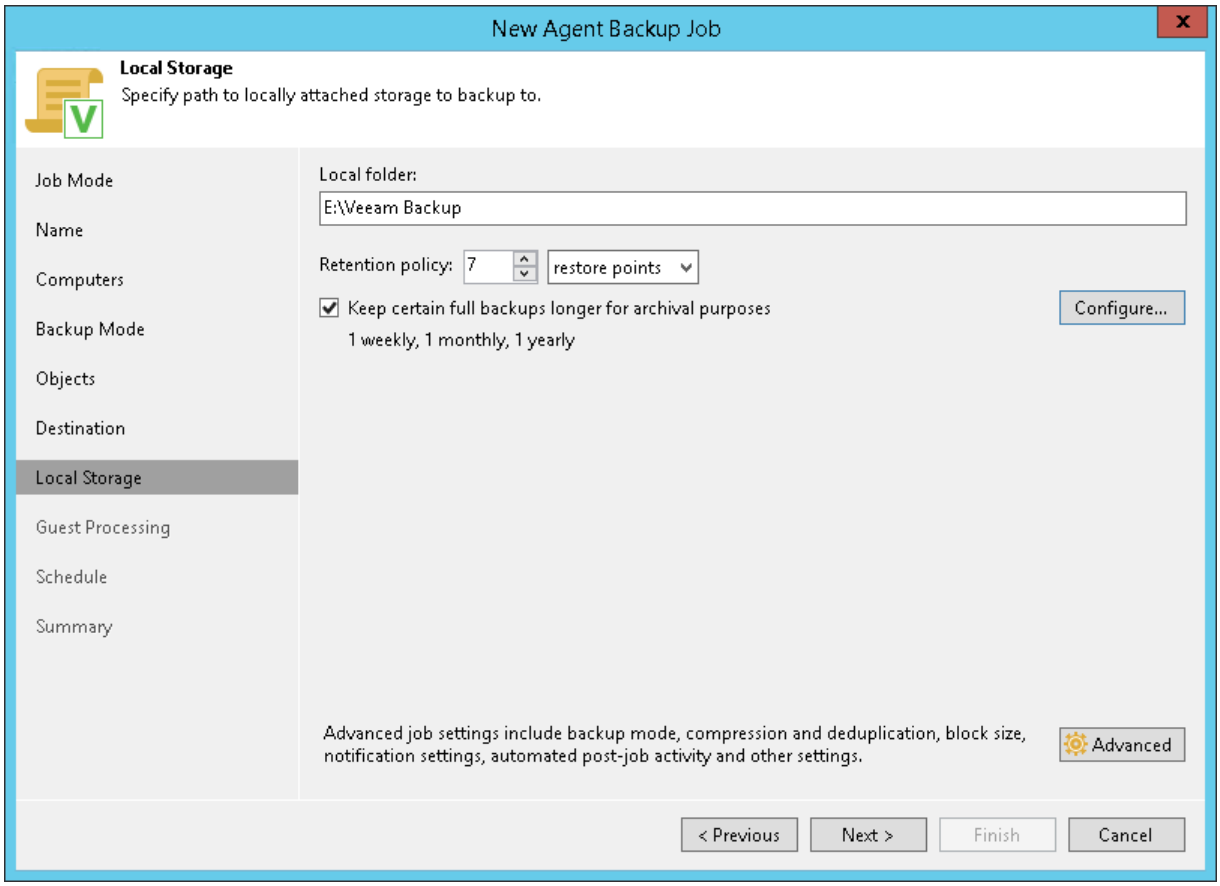
   - From the **Retention policy** list, select restore points and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the **Retention policy** list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   > **NOTE**
   >
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   >
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent retains restore points for a certain number of days or retains the number of latest restore points.

3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

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



Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and 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 select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. The user name must be specified in the *DOMAIN\USERNAME* format.

   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the *NT AUTHORITY\SYSTEM* account of the computer where the product is installed. You can use this scenario if the Veeam Agent computer is joined to the Active Directory domain. In this case, you can simply grant *Full Control* access on the shared folder and underlying file system to the computer account *(DOMAIN\COMPUTERNAME$)*.
3. Specify short-term backup retention policy settings in one of the following ways:
   - From the **Retention policy** list, select restore points and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

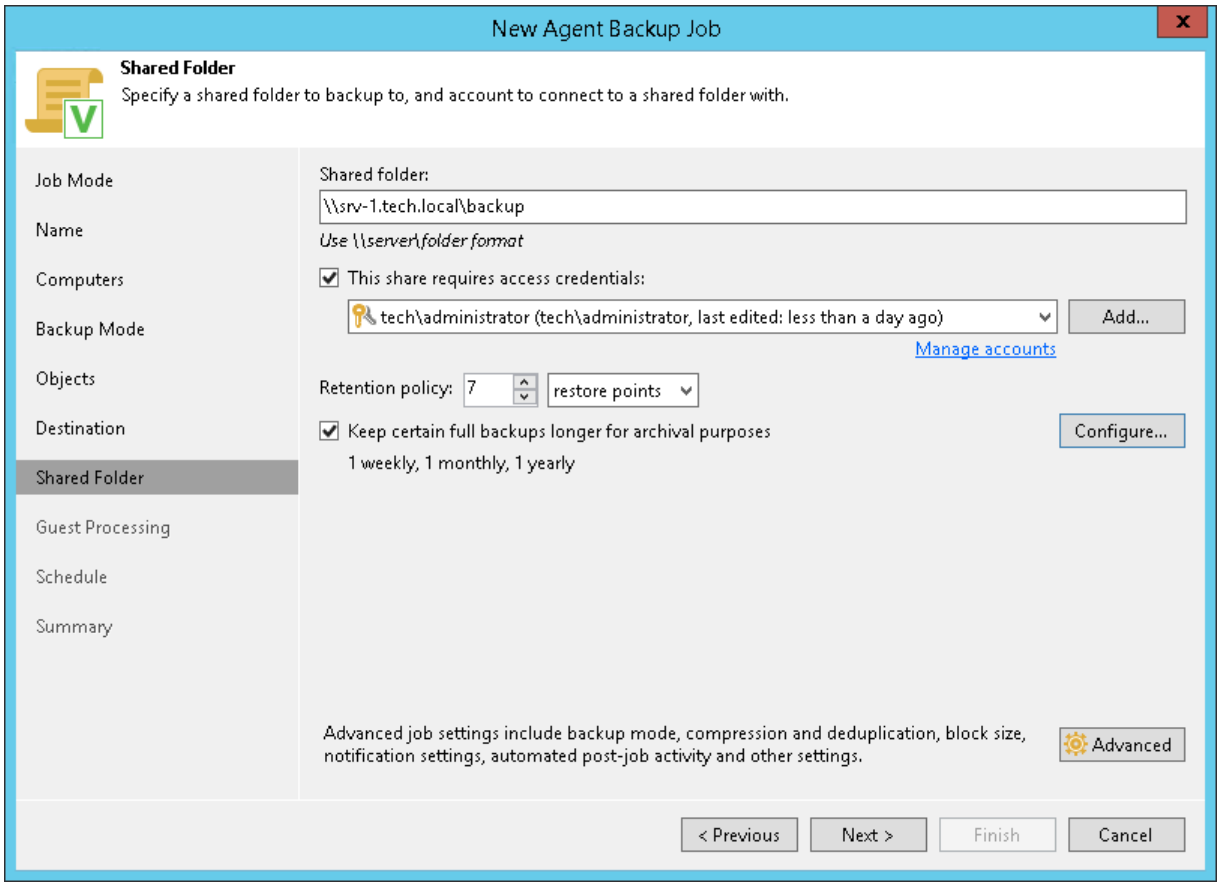
- From the **Retention policy** list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

  Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

> **NOTE**
>
> The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
>
> - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
> - The Retention Policy in Server Edition section about retention policy using that Veeam Agent retains restore points for a certain number of days or retains the number of latest restore points.

4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

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



Veeam Backup Repository Settings

If you have selected the **Managed by agent** mode for the backup job and chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

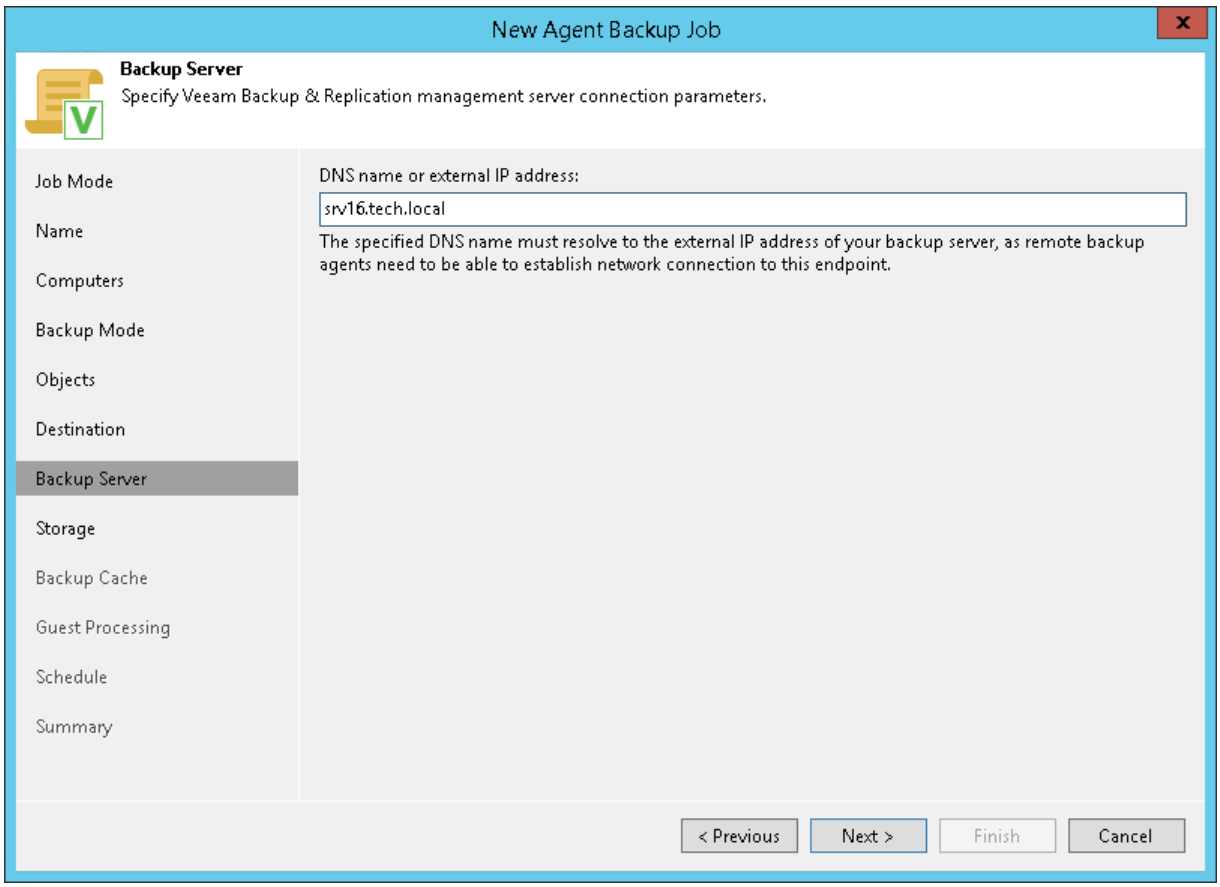
Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to store backup files on a Veeam backup repository.

In the **DNS name or external IP address field**, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup job. The specified DNS name or IP address must be accessible from Veeam Agent computers.

NOTE

Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.



Selecting Backup Repository

The **Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam backup repository.

NOTE

You cannot map a Veeam Agent backup job managed by Veeam Agent (backup policy).

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. Specify short-term backup retention policy settings in one of the following ways:
   - From the **Retention policy** list, select restore points and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the **Retention policy** list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

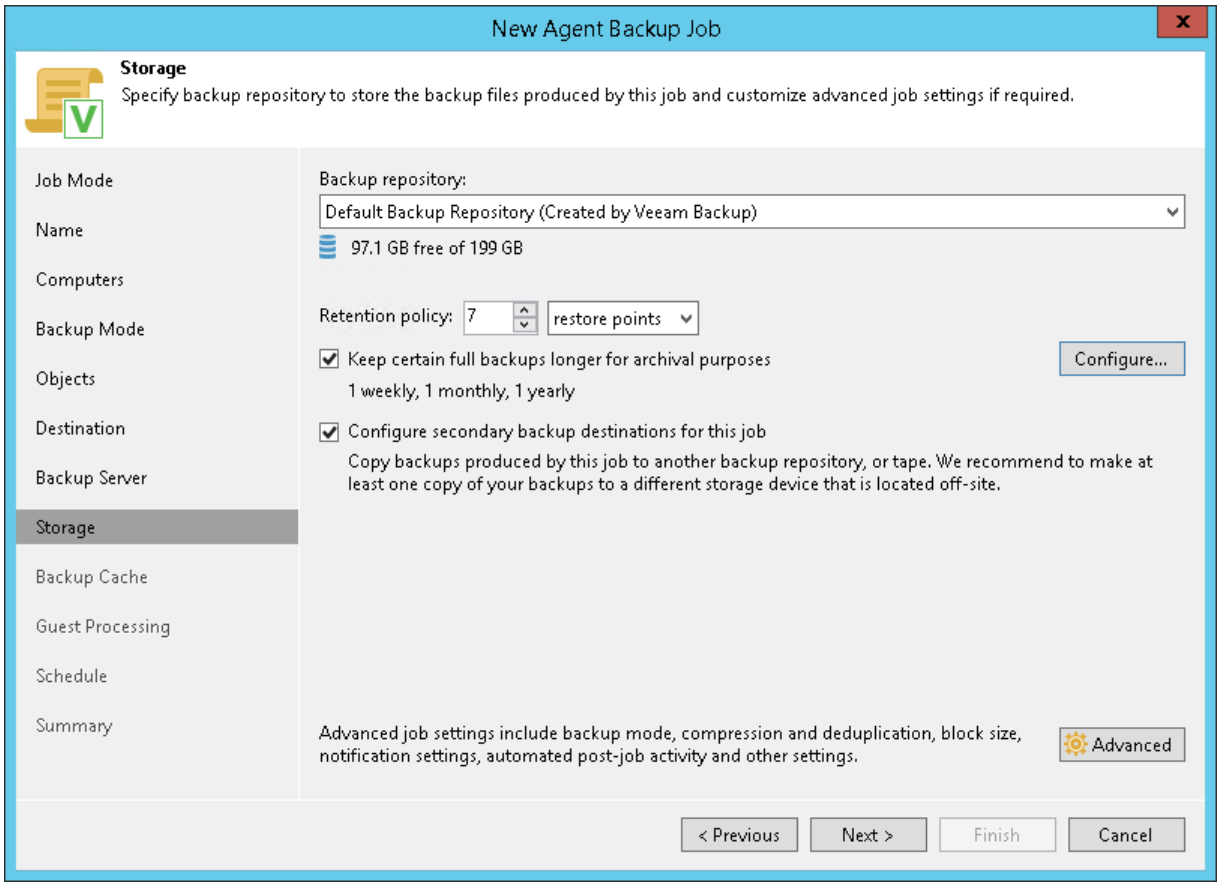
     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   > **NOTE**
   >
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   >
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent restore points for a certain number of days or retains the number of latest restore points.

3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.
4. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary Target. At the **Secondary Target** step of the wizard, you can link the backup job to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.

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



Cloud Repository Settings

The **Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam Cloud Connect repository.

> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

Specify settings for the cloud repository:

1. From the **Backup repository** list, select a cloud repository where you want to store created backups. The **Backup repository** list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication automatically checks how much free space is available on the repository.

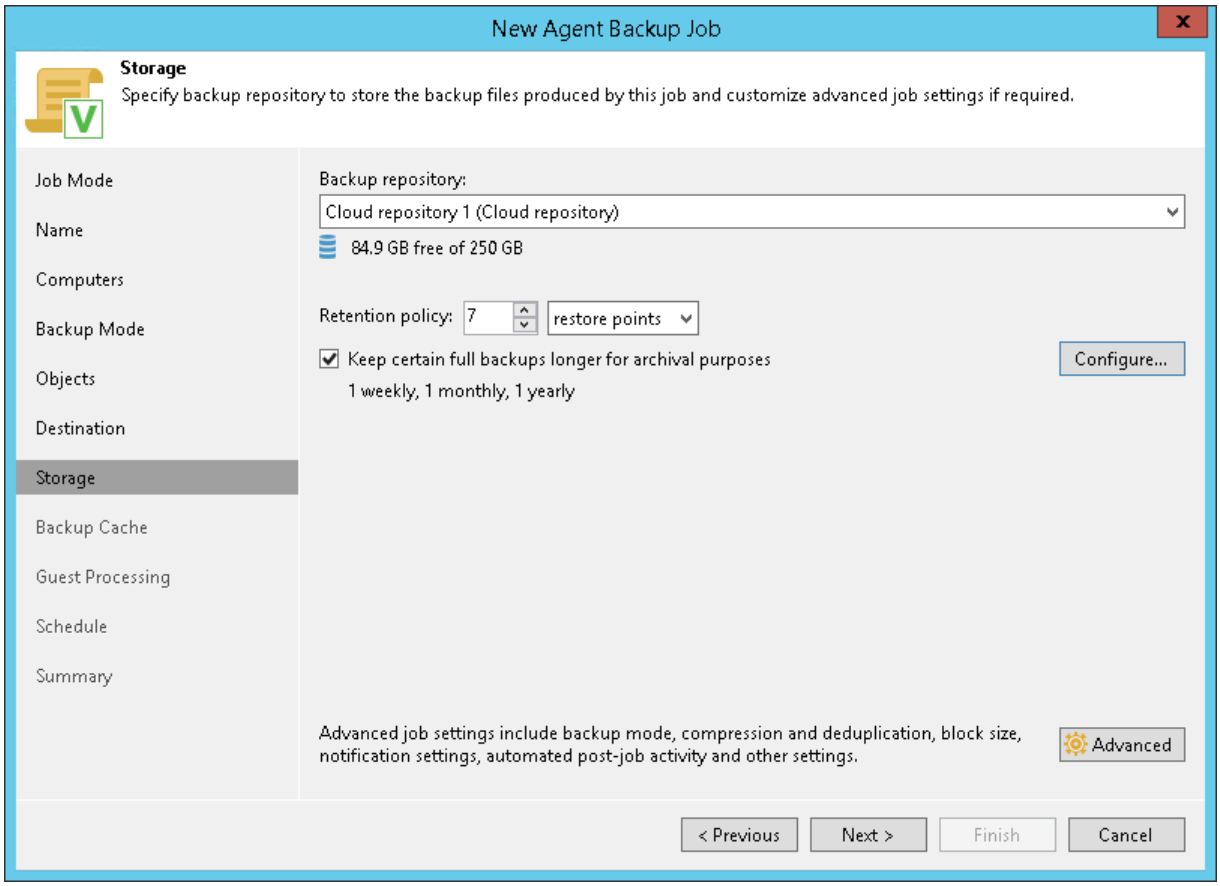
2. Specify short-term backup retention policy settings in one of the following ways:
   - From the **Retention policy** list, select restore points and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the **Retention policy** list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   > **NOTE**
   >
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   >
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent restore points for a certain number of days or retains the number of latest restore points.

3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

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



Step 9. Specify Advanced Backup Settings

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

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings
- [For Veeam Agent jobs managed by the backup server] Integration settings
- [For Veeam Agent jobs managed by the backup server] Script settings

> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup job, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Backup Settings

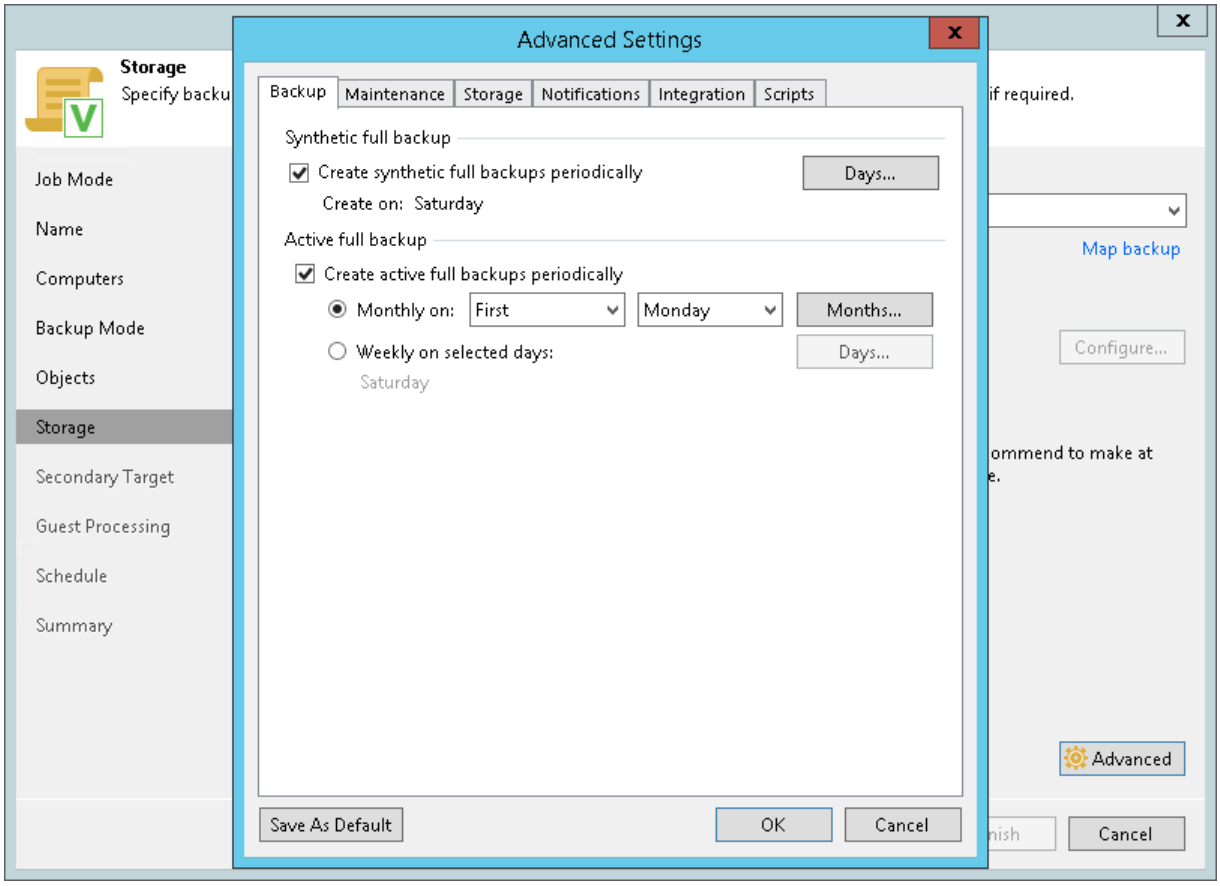
To specify settings for a backup chain created with the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. If you want to periodically create synthetic full backups, on the **Backup** tab, select the **Create synthetic full backups periodically** check box and click **Days** to schedule synthetic full backups on the necessary week days.
3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

NOTE

Consider the following:

- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location. For more information about periodic full backups, see the Active Full Backup and Synthetic Full Backup sections in the Veeam Agent for Microsoft Windows User Guide.
- If you schedule the active full backup and synthetic full backup on the same day, Veeam Agent for Microsoft Windows will perform only active full backup. Synthetic full backup will be skipped.



Maintenance Settings

You can specify maintenance settings for a backup chain created with the Veeam Agent backup job. Maintenance operations help make sure that the backup chain remains valid and consistent.

Maintenance settings are available for the following types of Veeam Agent backup jobs that process Microsoft Windows computers:

- Backup job managed by the backup server.
- Backup job managed by Veeam Agent (backup policy).

To specify maintenance settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. In the **Advanced Settings** window, click the **Maintenance** tab.
3. To periodically perform a health check for the latest restore point in the backup chain, in the **Storage-level corruption guard** section, select the **Perform backup files health check** check box and specify the schedule for the health check.

   An automatic health check can help you avoid a situation where a restore point gets corrupted, making all dependent restore points corrupted, too. If during the health check Veeam Agent for Microsoft Windows or Veeam Backup & Replication detect corrupted data blocks in the latest restore point in the backup chain (or the restore point before the latest one if the latest restore point is incomplete), it will start the health check retry and transport valid data blocks from the Veeam Agent computer to the target location. The transported data blocks are stored to a new backup file or the latest backup file in the backup chain, depending on the data corruption scenario.

   For Veeam Agent backup jobs managed by the backup server, the health check process is similar to the one for backup jobs that process VMs. For more information, see the Health Check for Backup Files section in the Veeam Backup & Replication User Guide.

   For Veeam Agent backup jobs managed by Veeam Agent, the health check process is the same as for Veeam Agent backup jobs configured directly on a Veeam Agent computer. For more information, see the Health Check for Backup Files section in the Veeam Agent for Microsoft Windows User Guide.
4. [For backup jobs and policies targeted at a Veeam backup repository or cloud repository] Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup job in the target location.
   - For backup jobs managed by the backup server, deleted items retention policy is similar to retention policy for deleted VMs. After you remove a protection group or individual computer from a Veeam Agent backup job, Veeam Backup & Replication will keep its data on the backup repository for the period that you have specified. When this period is over, backup data of this computer will be removed from the backup repository. For more information, see the Retention Policy for Deleted VMs section in the Veeam Backup & Replication User Guide.
   - For backup jobs managed by Veeam Agent, if Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location. For more information, see the Retention Policy for Outdated Backups section in the Veeam Agent for Microsoft Windows User Guide.

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

   > **NOTE**
   >
   > The **Remove deleted items data after** option is not available if you configure a backup job managed by Veeam Agent (backup policy) and have selected the **Local storage** or **Shared folder** option at the Destination step of the wizard.

5. To periodically compact a full backup, select the **Defragment and compact full backup file** check box and specify the schedule for the compact operation. During the compact operation, data blocks from the full backup file are copied to a new empty file. As a result, the full backup file gets defragmented, and the speed of reading from and writing to the backup file increases.

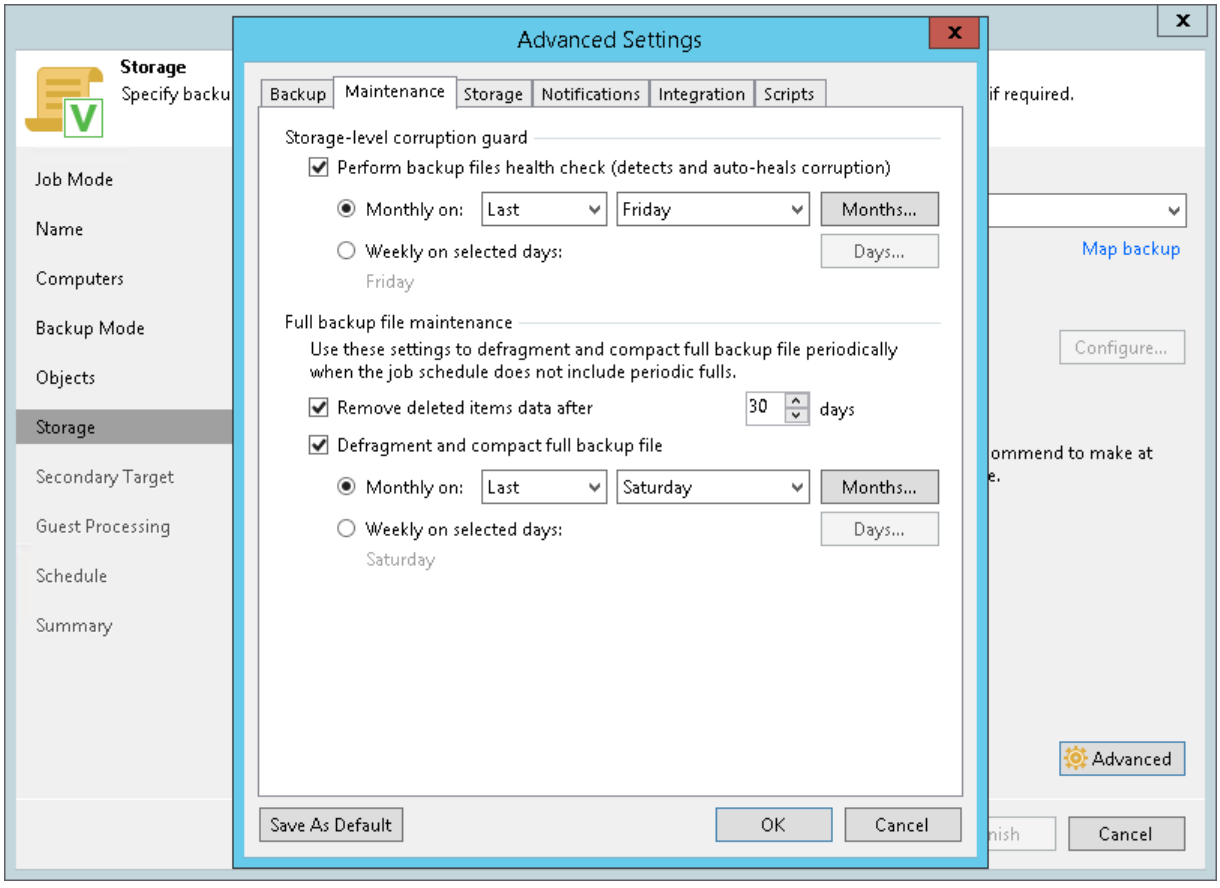
   The compact operation differs depending on the type of the backup job.

   - For Veeam Agent backup jobs managed by the backup server, the compact operation is similar to the compact operation performed for VM backup jobs. If the full backup file contains data blocks for deleted items (protection groups or individual computers that were removed from the backup job), Veeam Backup & Replication will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Backup & Replication User Guide.
   - For Veeam Agent backup jobs managed by Veeam Agent, if the full backup file contains data blocks for deleted drives, Veeam Agent for Microsoft Windows will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Agent for Microsoft Windows User Guide.

   NOTE

   Consider the following:

   - If you want to periodically compact a full backup, you must make sure that you have enough free space in the target location. For the compact operation, the amount of free space must be equal to or more that the size of the full backup file.
   - In contrast to the compact operation for a VM backup, during compact of a full Veeam Agent backup file, Veeam Backup & Replication does not perform the data take out operation. If the full backup file contains data for a computer that has only one restore point and this restore point is older than 7 days, Veeam Backup & Replication will not extract data for this computer to a separate full backup file.



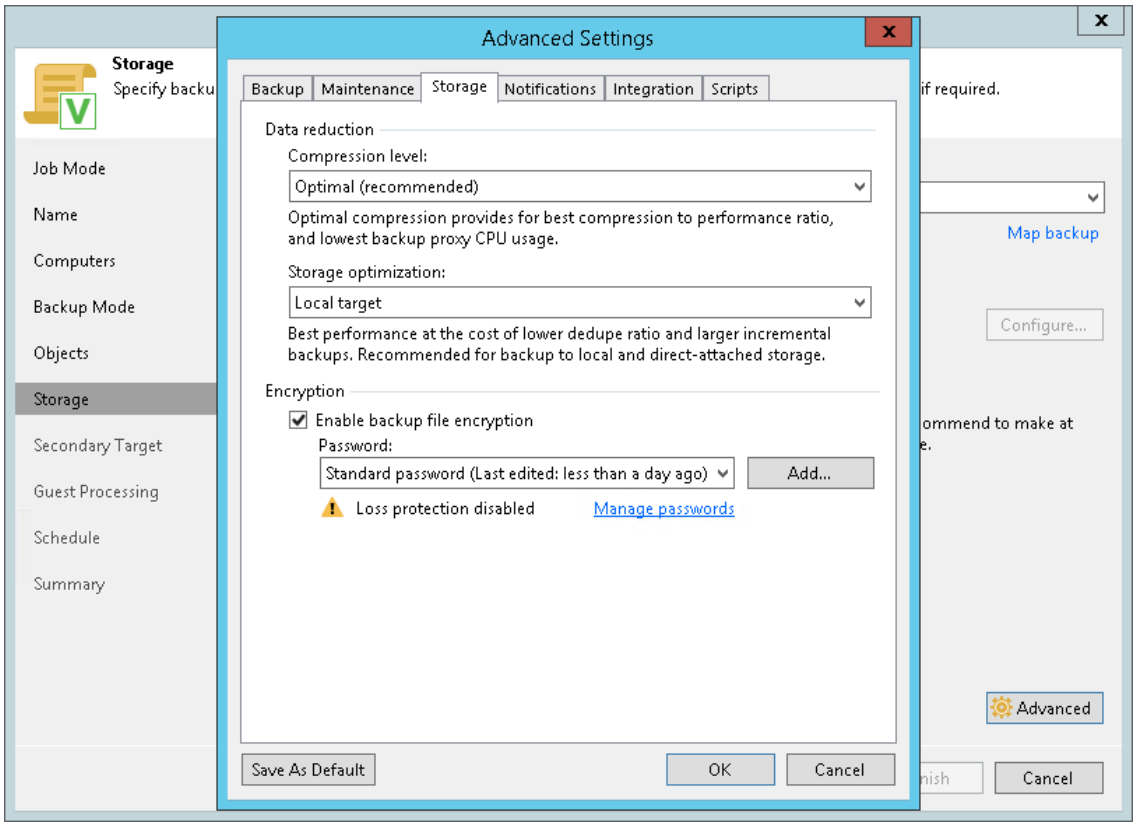
Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Storage** tab.
3. [For a failover cluster backup job] By default, Veeam Backup & Replication deduplicates failover cluster data before storing it on the backup repository. Data deduplication provides a smaller size of the backup file but may reduce the backup job performance. You can disable data deduplication if necessary, for example, if you use a deduplication storage appliance as a backup repository. To disable data deduplication, clear the **Enable inline data deduplication** check box.

   > **NOTE**
   >
   > The **Enable inline data deduplication** option is unavailable if you selected the **Workstation** or **Server** option at the Job Mode step of the wizard.

4. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
5. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Agent for Microsoft Windows will use data blocks of different size to optimize the size of backup files and job performance.



6. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see the Password Manager section in the Veeam Backup & Replication User Guide..

   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.

   NOTE

   Consider the following:

   - Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer, at a network shared folder, or at a cloud repository. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.
   - If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.
   - If you enable encryption for an existing Veeam Agent backup, during the next job session Veeam Agent for Microsoft Windows will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.
   - Encryption is not retroactive. If you enable encryption for an existing backup job, Veeam Agent for Microsoft Windows will encrypt the backup chain starting from the next restore point created with this job.
   - [For backup policies targeted at a local drive, network shared folder or cloud repository] When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

     This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

   To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.

Notification Settings

You can specify notification settings for Veeam Agent backup jobs configured in Veeam Backup & Replication. Notification options differ depending on the job mode that you have selected at the Job Mode step of the wizard:

- **Managed by backup server**. To learn more, see Notification Settings for Veeam Agent Backup Job.
- **Managed by agent**. To learn more, see Notification Settings for Backup Policy.

Notification Settings for Veeam Agent Backup Job

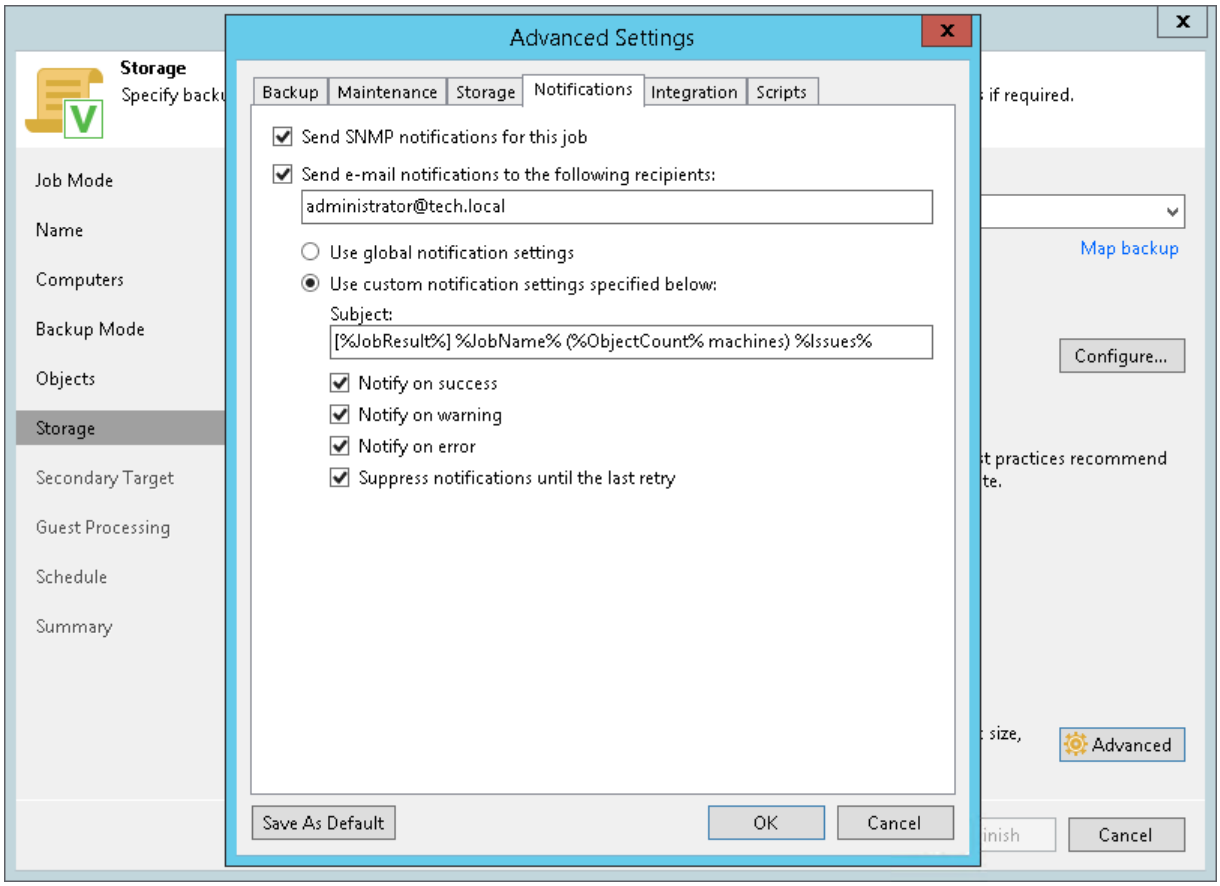
To specify notification settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

   SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

   Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

5. You can choose to use global notification settings or specify custom notification settings.
    - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server.
    - To configure a custom notification for the job, select **Use custom notification settings specified below**. You can specify the following notification settings:
        - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the *Warning* or *Failed* status).
        - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.
        - Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.



Notification Settings for Backup Policy

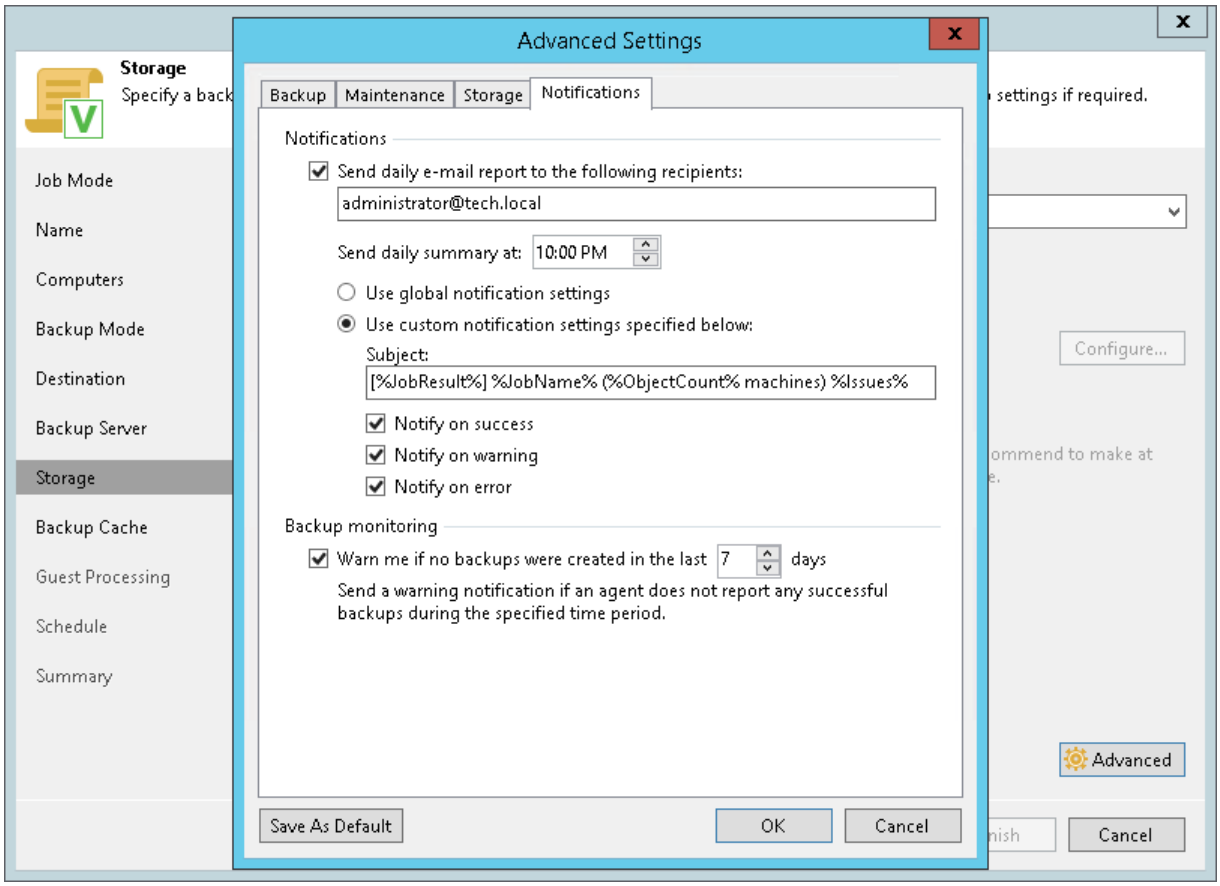
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

> **NOTE**
>
> Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the backup policy, Veeam Backup & Replicationwill send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will send the report daily at the specified time.
5. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server.
   - To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the backup policy) and *%Issues%* (number of machines in the backup policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.

6. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



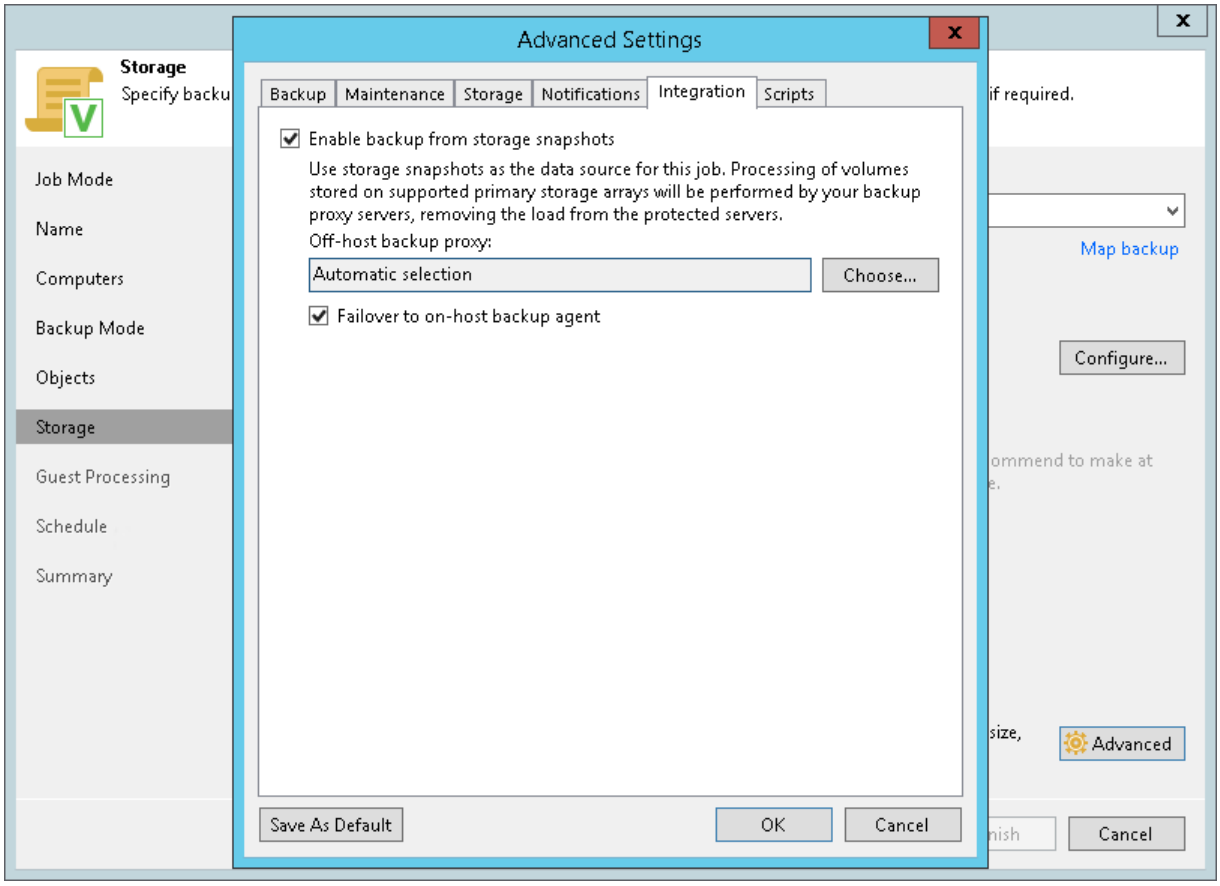
Integration Settings

You can specify storage integration settings for the job if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

To specify storage integration settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Integration** tab.
3. If you select the **Enable backup from storage snapshots** check box, Veeam Backup & Replication will use native storage snapshots to create Veeam Agent backups. To learn more about storage snapshots support, see Storage Snapshots Support.
4. To transfer a snapshot from storage to the target repository, Veeam Backup & Replication uses off-host backup proxies. You can allow Veeam Backup & Replication to use any suitable backup proxies or you can select specific backup proxies. To learn more, see Selecting Off-Host Backup Proxy.
5. If Veeam Backup & Replication fails to create a storage snapshot or backup proxy is unavailable, you can fail over to the regular backup scenario that uses the software VSS provider. To do this, select the **Failover to on-host backup agent** check box.

   To learn more about regular backup scenario, see the How Backup Works section in the Veeam Agent for Microsoft Windows User Guide.



Selecting Off-Host Backup Proxy

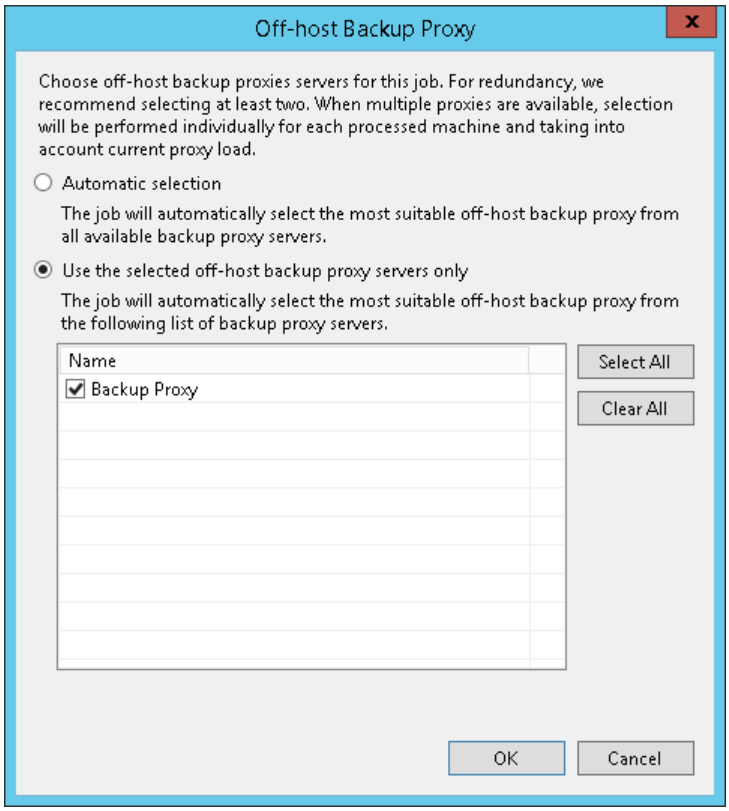
You can select what backup proxies Veeam Backup & Replication will use during the backup process. The following options are available:

- If you want Veeam Backup & Replication to use any suitable backup proxies, select the **Automatic selection** option. In this case, the number of backup proxies that Veeam Backup & Replication uses for data transfer depends on the backup scope.

  > **IMPORTANT**
  >
  > If you use the NetApp Element storage system and you have 4 or more backup proxies set in your Veeam Backup & Replication infrastructure, you cannot use automatic selection. You must manually select up to 3 backup proxies.

- If you want to select backup proxies manually, select the **Use the selected off-host backup proxy servers only** option and select check boxes near backup proxies you plan to use.

Keep in mind that Veeam Backup & Replication displays only those backup proxies that run Microsoft Windows Server OS. For more information about backup proxy requirements, see Storage Snapshots Support.



Script Settings

You can specify script settings for the job if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

To specify script settings for the backup job:

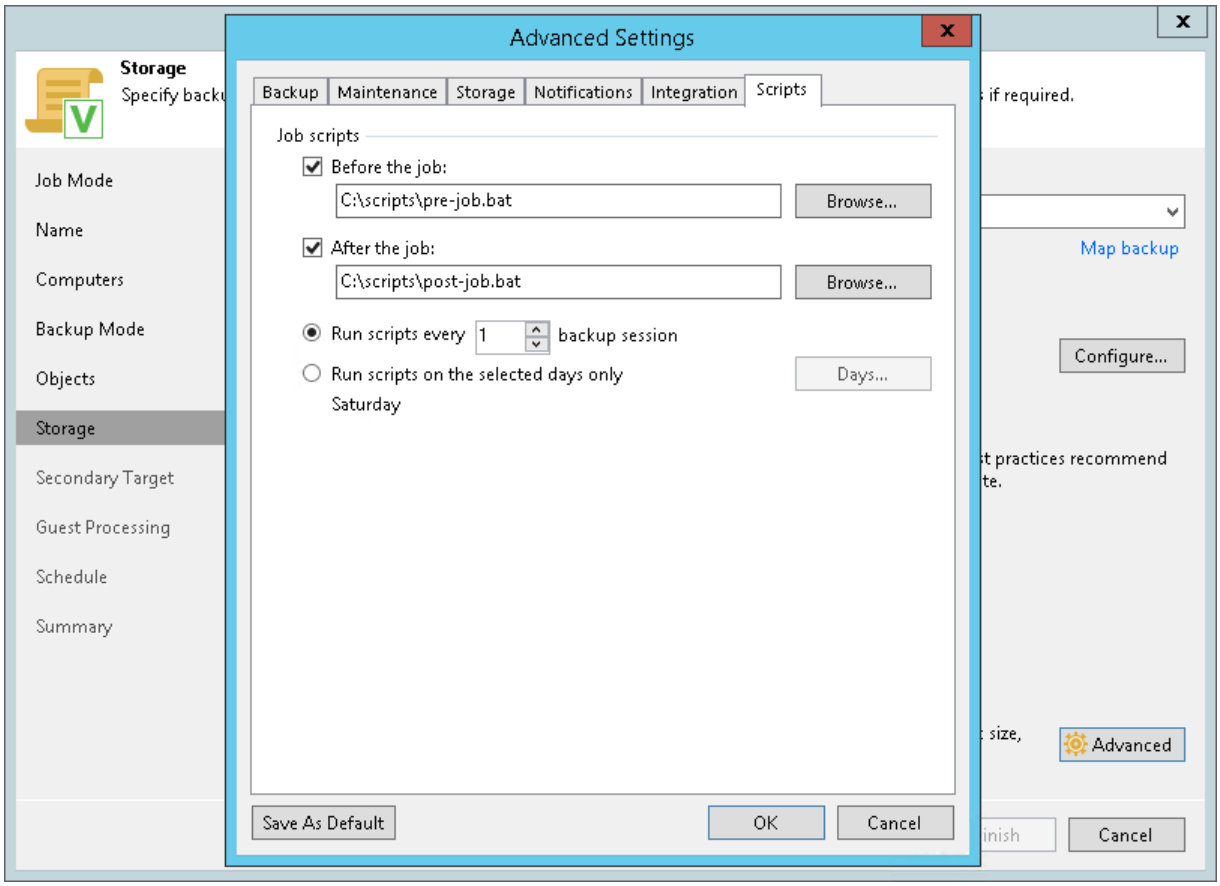
1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before and/or after the backup job, select the **Before the job** and **After the job** check boxes and click **Browse** to choose executable files from a local folder on the backup server. The scripts are executed on the backup server.

   You can select to execute pre- and post-backup actions after a number of backup sessions or on specific week days.

   - If you select the **Run scripts every <N> backup session** option, specify the number of the backup job sessions after which the scripts must be executed.
   - If you select the **Run scripts on the selected days only** option, click **Days** and specify week days on which the scripts must be executed.

NOTE

Custom scripts that you define in the advanced job settings relate to the backup job itself, not the OS quiescence process on protected computers. To add pre-freeze and post-thaw scripts for Veeam Agent computer OS quiescence, use the **Guest Processing** step of the wizard.



Step 10. Specify Secondary Target

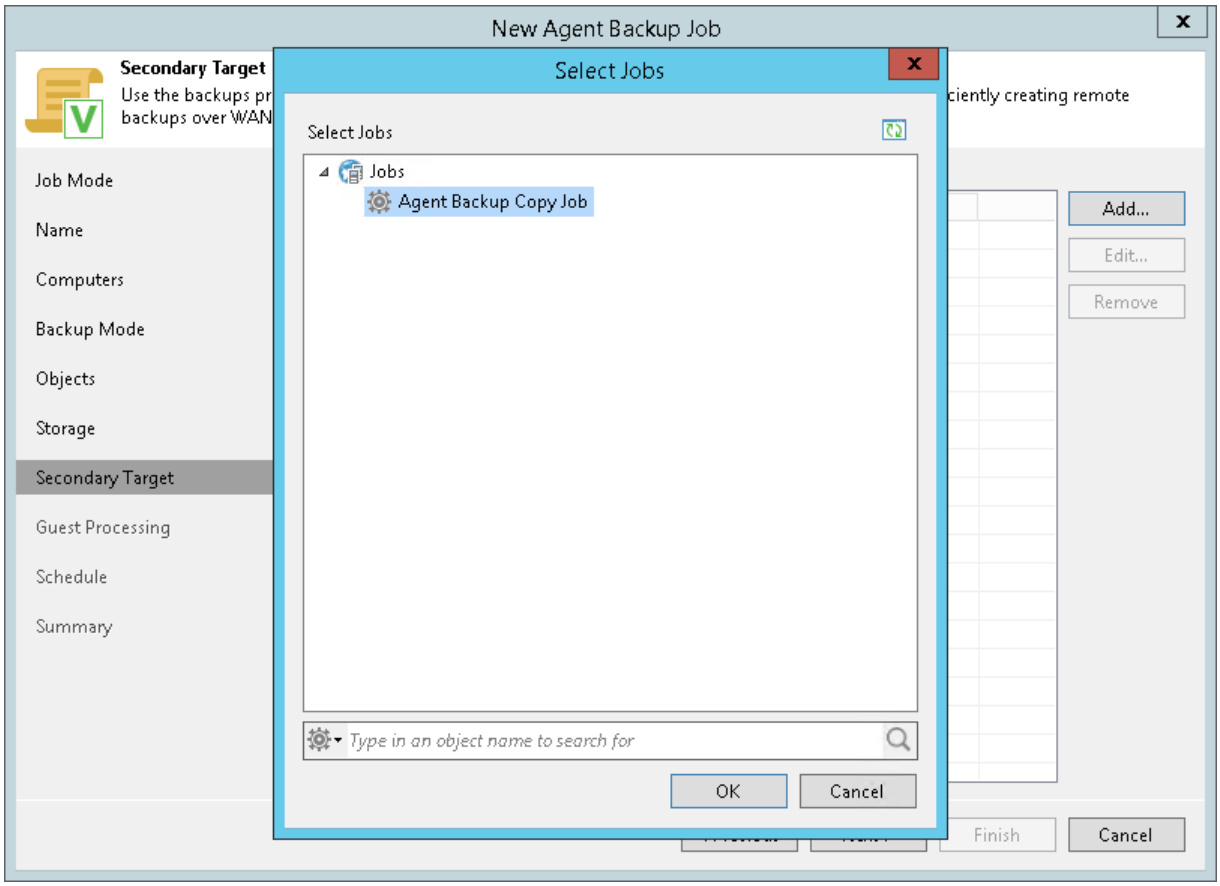
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup job to a backup to tape or backup copy job. As a result, the backup job will be added as a source to the backup to tape or backup copy job. Backup files created with the backup job will be archived to tape or copied to the secondary backup repository according to the secondary jobs schedule. For more information, see the Linking Backup Jobs to Backup Copy Jobs and Linking Backup Jobs to Backup to Tape Jobs sections in the Veeam Backup & Replication User Guide.

The backup to tape job or backup copy job must be configured beforehand. You can create these jobs with an empty source. When you link the Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent backup job as a source for these jobs.

To link jobs:

1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom of the wizard.



Step 11. Specify Backup Cache Settings

The **Backup Cache** step of the wizard is available if you selected the following options at the previous steps of the wizard:

1. Selected the **Managed by agent** mode at the Job Mode step of the wizard.
2. Selected the **Veeam backup repository** or **Veeam Cloud Connect repository** option at the Destination step of the wizard.

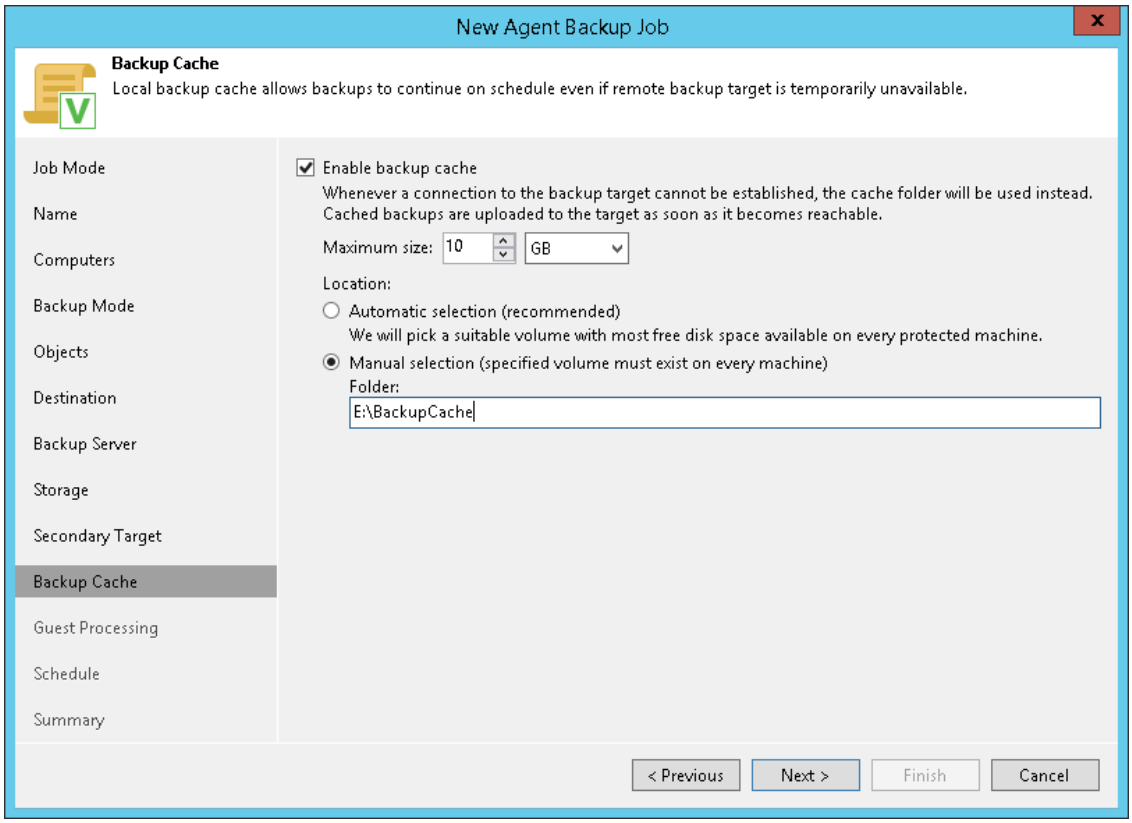
To specify backup cache settings:

1. Select the **Enable backup cache** check box.
2. In the **Maximum size** field, specify the size for the backup cache.

   When defining the size of the backup cache, assume the following:

   - Each full backup file may consume about 50% of the backed-up data size.
   - Each incremental backup file may consume about 10% of the backed-up data size.
3. In the **Location** section, specify where Veeam Agent for Microsoft Windows will create the backup cache. You can select from the following options:

   - **Automatic selection** — select this option if you want to let Veeam Agent pick a location for the backup cache automatically. On every computer added to the backup policy, Veeam Agent will detect a volume with the largest amount of free disk space and create the backup cache in the *Veeam Backup Cache* folder on this volume. To learn more, see Backup Cache.
   - **Manual selection** — select this option if you want to specify a location for the backup cache manually. If you select this option, in the **Folder** field, specify a path to the folder on a protected computer in which backup files must be stored.

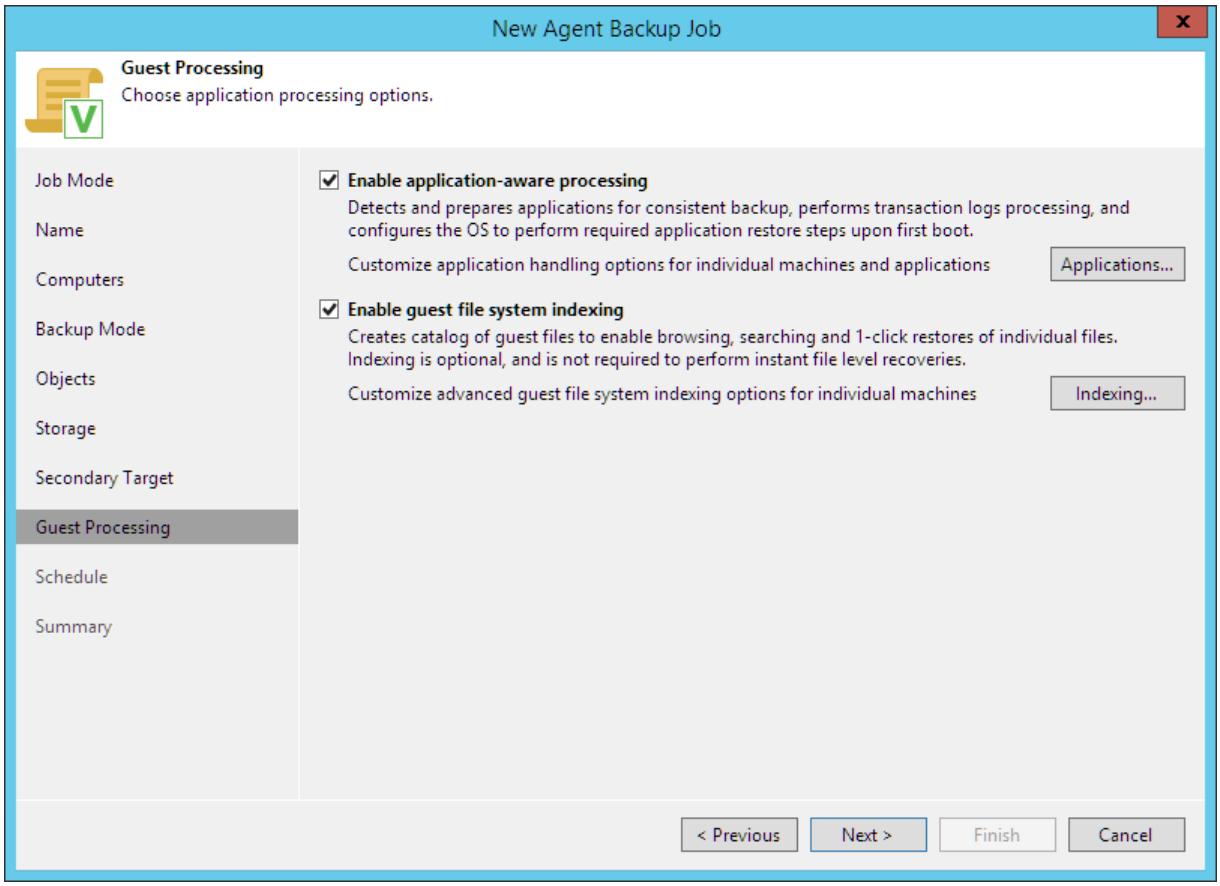


Step 12. Specify Guest Processing Settings

The **Guest Processing** step of the wizard is available if you have selected the **Server** or **Failover cluster** option at the Job Mode step of the wizard.

For a Veeam Agent backup job that includes Windows-based computers, you can enable the following guest OS processing settings:

- Application-aware processing
- Transaction log handling for Microsoft SQL Server
- Archived log handling for Oracle databases
- SharePoint account settings
- Use of pre-freeze and post-thaw scripts
- File indexing



Application-Aware Processing

If your computer runs VSS-aware applications, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of applications without data loss.

To enable application-aware processing:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, make sure that the **Enable application-aware processing** check box is selected.

   You can clear this check box, for example, if you want to disable application-aware processing for a specific computer added to the backup job as a part of a protection group.

   [For Microsoft SQL Server] If you disable application-aware processing, Veeam Agent will not include information about databases in the backup. However, you can use Veeam Explorer for Microsoft SQL to locate a database file in the backup and restore the database.
5. [For Microsoft Exchange, Microsoft SQL Server and Oracle] In the **Transaction logs** section, specify if Veeam Agent for Microsoft Windows running on a protected computer must process transaction logs or copy-only backups must be created.

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

     [For Microsoft Exchange] With this option selected, Veeam Agent for Microsoft Windows will wait for backup to complete successfully, and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.

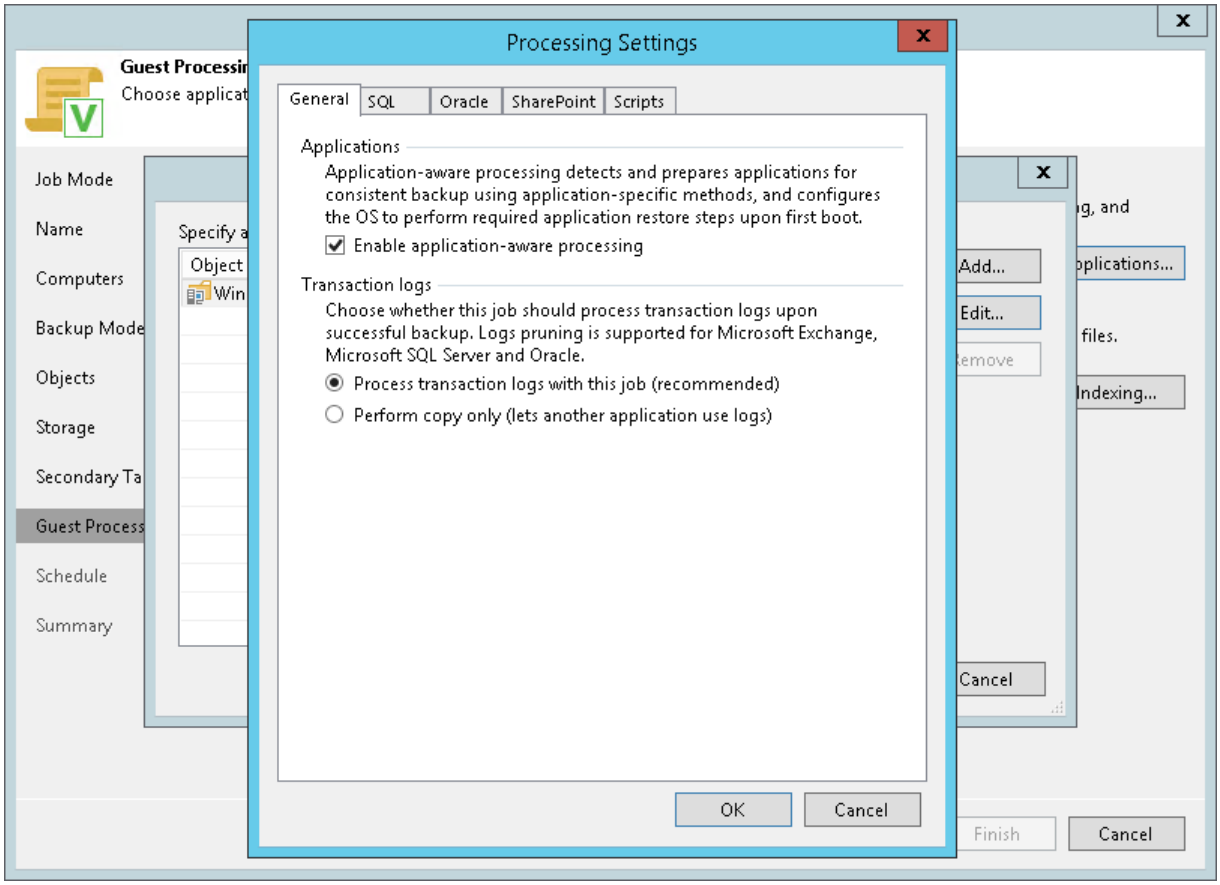
     [For Microsoft SQL Server and Oracle] You will have to specify settings for database log handling on the **SQL** and **Oracle** tabs of the **Processing Settings** window. For more information, see Microsoft SQL Server Transaction Log Settings and Oracle Archived Log Settings.

   - Select **Perform copy only** if you use another tool to maintain consistency of the database state. Veeam Agent for Microsoft Windows will create a copy-only backup. The copy-only backup preserves the chain of full/differential backup files and transaction logs. After a copy-only backup, Veeam Agent does not trigger truncation of transaction logs. For more information, see this Microsoft article.

IMPORTANT

Consider the following:

- [For Microsoft Exchange] Veeam Agent for Microsoft Windows performs truncation of Microsoft Exchange transaction logs only if all disks that contain the Microsoft Exchange database are included in a volume-level backup job.
- [For Microsoft SQL Server and Oracle] If both Microsoft SQL Server and Oracle Server are installed on one guest OS, and log backup is enabled for both applications, Veeam Agent for Microsoft Windows will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.



Microsoft SQL Server Transaction Log Settings

If you back up Microsoft SQL Server, you can specify how Veeam Agent for Microsoft Windows must process database transaction logs:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **Processing Settings** window, click the **SQL** tab.

6. To specify a user account that Veeam Agent for Microsoft Windows will use to connect to the Microsoft SQL Server, select from the **Specify Microsoft SQL Server account with database admin privileges** list a user account that has access permissions on the database. To connect to the Microsoft SQL Server, you must use a Microsoft Windows user account that has sysadmin privileges on the Microsoft SQL Server. You cannot use Microsoft SQL Server accounts (for example, the SA account) to connect to the database.

   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the Microsoft SQL Server under the account that you have specified for the protected computer in the protection group settings.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

7. Specify how transaction logs must be processed. You can select one of the following options:

   - Select **Truncate logs** to truncate transaction logs after successful backup. Veeam Agent for Microsoft Windows will wait for the backup to complete successfully and then truncate transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.
   - Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Agent for Microsoft Windows will not truncate transaction logs.

     It is recommended that you enable this option for databases that use the *Simple* recovery model. If you enable this option for databases that use the *Full* or *Bulk-logged* recovery model, transaction logs may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs him-/herself.
   - Select **Backup logs periodically** to back up transaction logs with Veeam Agent for Microsoft Windows. Veeam Agent for Microsoft Windows will periodically copy transaction logs to the backup location and store them together with the image-level backup. During the backup job session, transaction logs will be truncated.

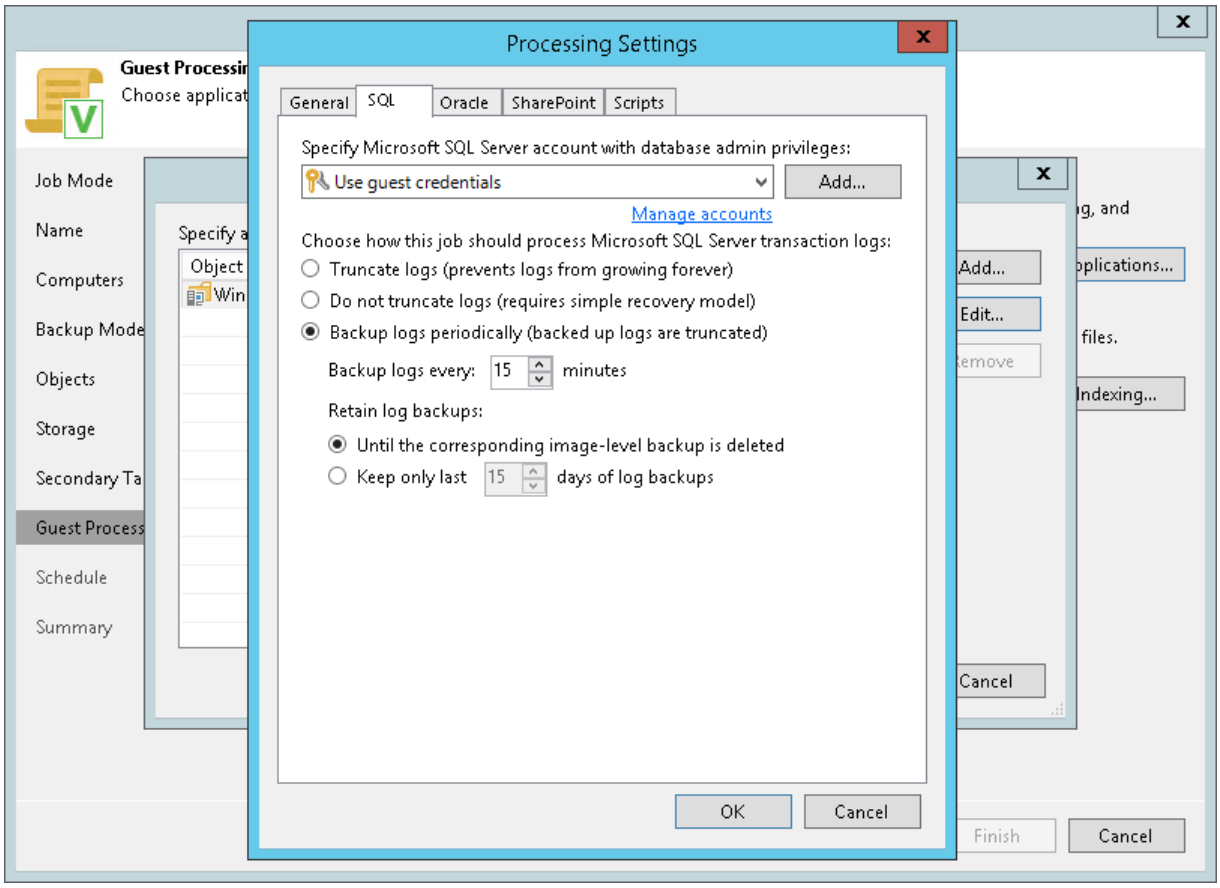
     For more information, see the Microsoft SQL Server and Oracle Logs Backup section in the Veeam Agent for Microsoft Windows User Guide.

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

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

IMPORTANT

Veeam Agent for Microsoft Windows automatically excludes its configuration database from application-aware processing during backup. Transaction logs for the configuration database are not backed up.



Oracle Archived Log Settings

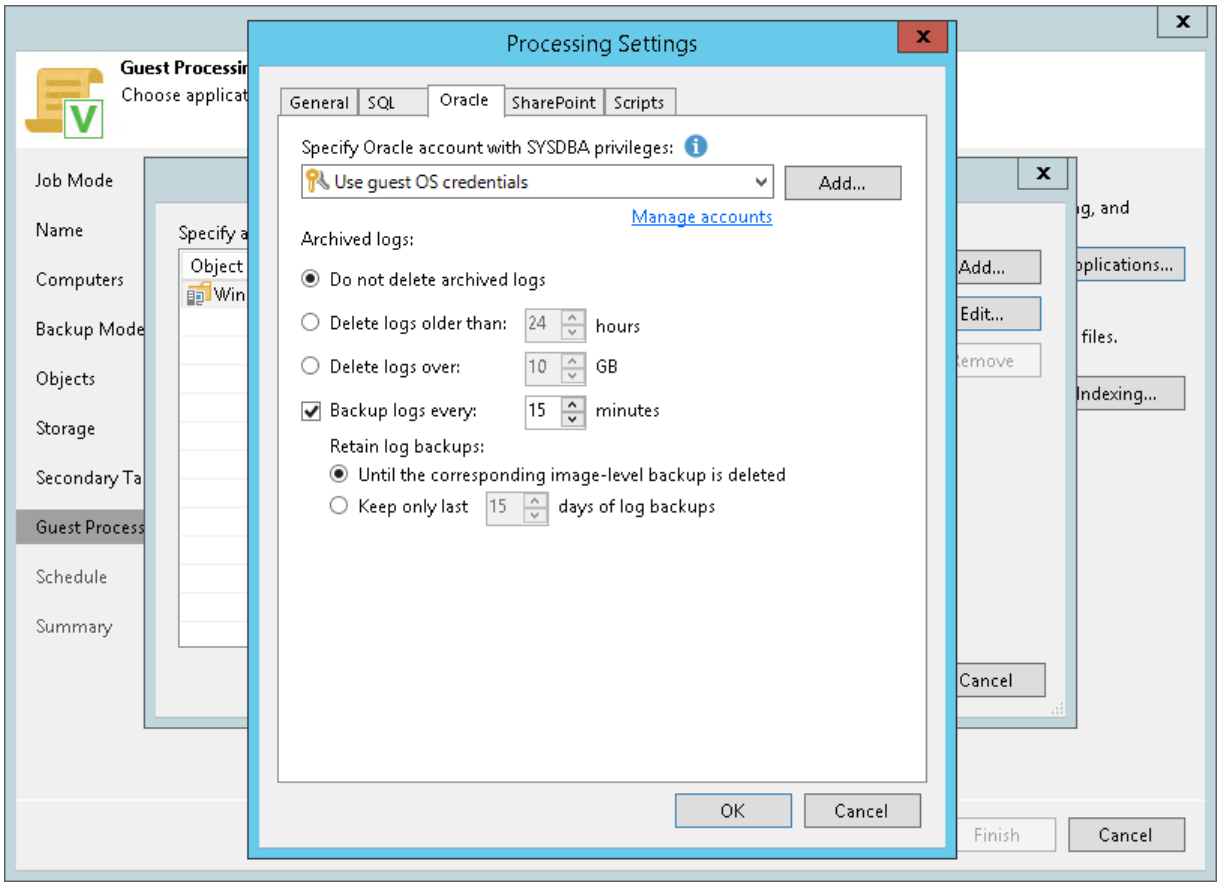
If you back up an Oracle database, you can specify how Veeam Agent for Microsoft Windows must process archived logs:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **Processing Settings** window, click the **Oracle** tab.
6. To specify a user account that Veeam Agent for Microsoft Windows will use to connect to the Oracle database, select from the **Specify Oracle account with SYSDBA privileges** list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   By default, the **Use guest OS credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the Oracle database under the account that you have specified for the protected computer in the protection group settings.

7. In the **Archived logs** section, specify if Veeam Agent for Microsoft Windows must delete archived logs on the Oracle database:
   - Select **Do not delete archived logs** if you want Veeam Agent for Microsoft Windows to preserve archived logs. When the backup job completes, Veeam Agent for Microsoft Windows will not delete archived logs.

     It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.
   - Select **Delete logs older than <N> hours** or **Delete logs over <N> GB** if you want Veeam Agent for Microsoft Windows to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent for Microsoft Windows will wait for the backup to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.
8. To back up Oracle archived logs with Veeam Agent for Microsoft Windows, select the **Backup log every <N> minutes** check box and specify the frequency for archived logs backup. By default, archived logs are backed up every 15 minutes. The minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.
9. In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for Veeam Agent backups and archived log backups.
   - Select **Keep only last <n> days of log backups** to keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the Veeam Agent backups. For more information, see the Retention for Database Log Backups section in the Veeam Agent for Microsoft Windows User Guide.

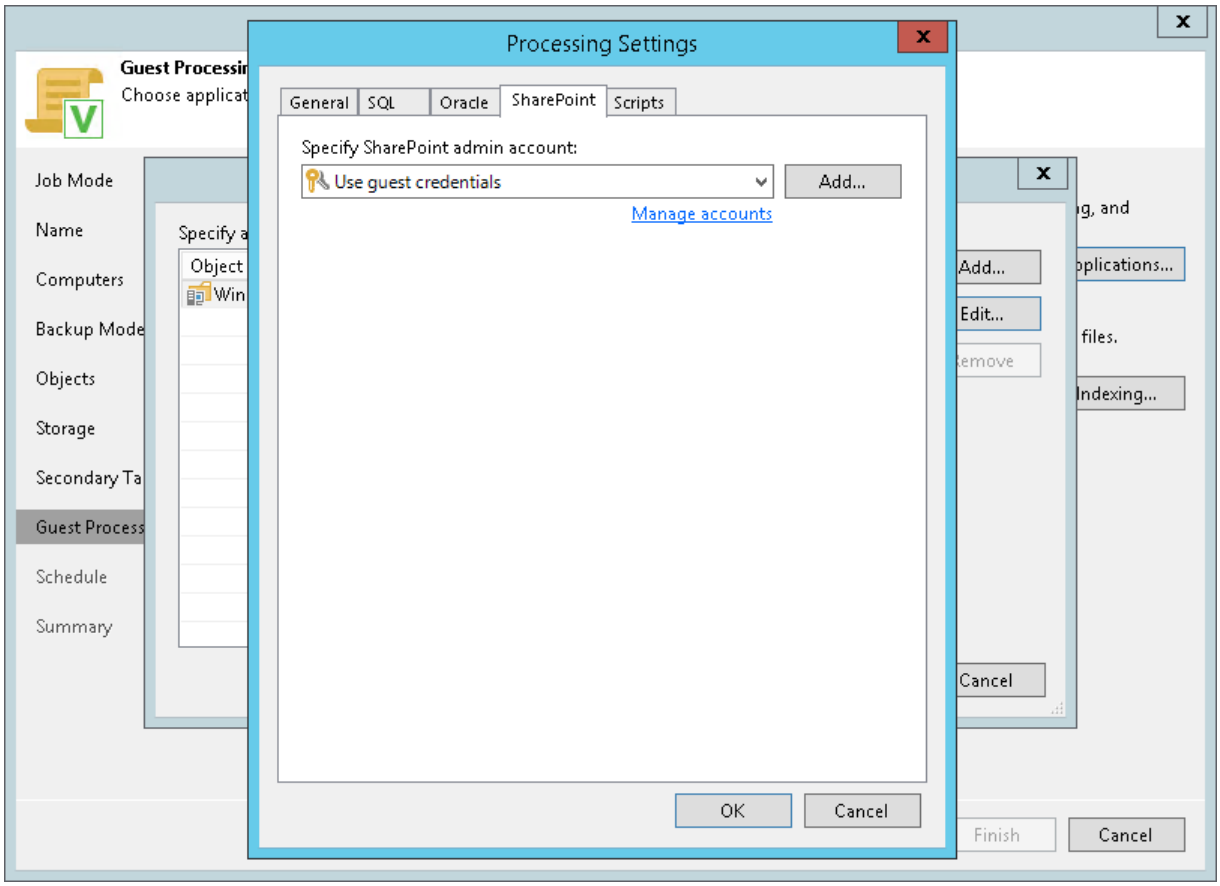


Microsoft SharePoint Account Settings

If you back up Microsoft SharePoint, you must specify a user account that has enough permissions on the application:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Processing Settings** window, click the **SharePoint** tab.
5. From the **Specify SharePoint admin account** list, select a user account that Veeam Agent for Microsoft Windows will use to connect to the SharePoint application. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the SharePoint application under the account that you have specified for the protected computer in the protection group settings.



Pre-Freeze and Post-Thaw Scripts

If you plan to back up data of applications that do not support VSS, you can specify what scripts Veeam Agent for Microsoft Windows must use to quiesce the OS on the protected computer. The pre-freeze script quiesces the file system and application data to bring the OS to a consistent state before Veeam Agent for Microsoft Windows creates a VSS snapshot. After the VSS snapshot is created, the post-thaw script brings the file system and applications to their initial state.

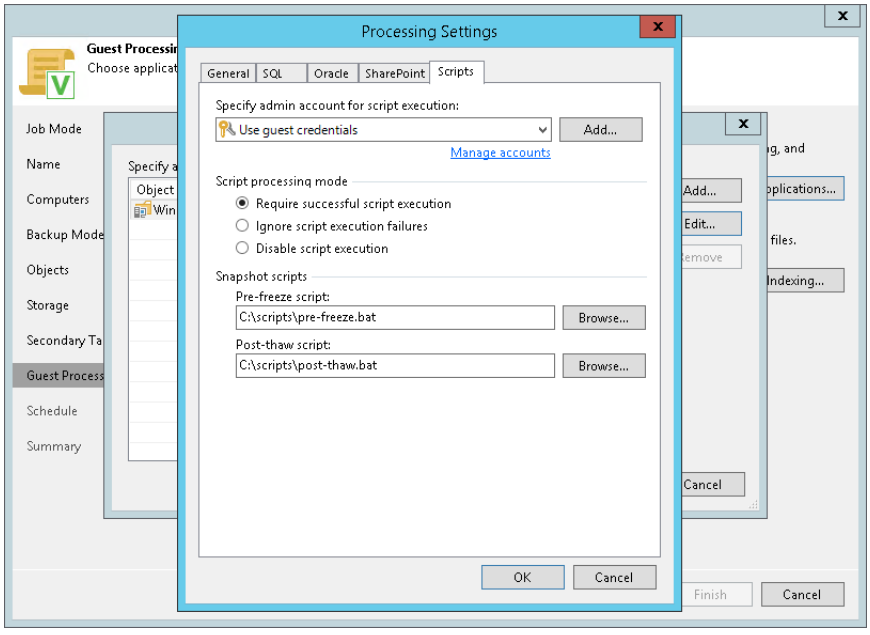
To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Processing Settings** window, click the **Scripts** tab.
5. From the **Specify admin account for script execution** list, select a user account that Veeam Agent for Microsoft Windows will use to run pre-freeze and post-thaw scripts. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will run pre-freeze and post-thaw scripts under the account that you have specified for the protected computer in the protection group settings.
6. In the **Script processing mode** section, specify the scenario for scripts execution:
   - Select **Require successful script execution** if you want Veeam Agent for Microsoft Windows to stop the backup process if the script fails.
   - Select **Ignore script execution failures** if you want to continue the backup process even if script errors occur.
   - Select **Disable script execution** if you do not want to run scripts.
7. In the **Pre-freeze script** and **Post-thaw script** fields, click **Browse** to choose executable files from a local folder on the backup server. During the backup job session, Veeam Backup & Replication will upload the scripts to Veeam Agent computers added to the job and execute them on these computers.

   Veeam Agent for Microsoft Windows supports the following types of scripts:
   - Program files in the EXE, BAT and CMD format
   - Windows script files in the JS, VBS and WSF format
   - PowerShell script files in the PS1 format

   You can use scripts of other formats as well, but we cannot guarantee correct processing of such scripts.



File Indexing

You can instruct the backup job to create an index of files and folders on the protected computer OS during backup. If you enable the file indexing option, you will be able to search for individual files inside Veeam Agent backups and perform 1-click restore in Veeam Backup Enterprise Manager.

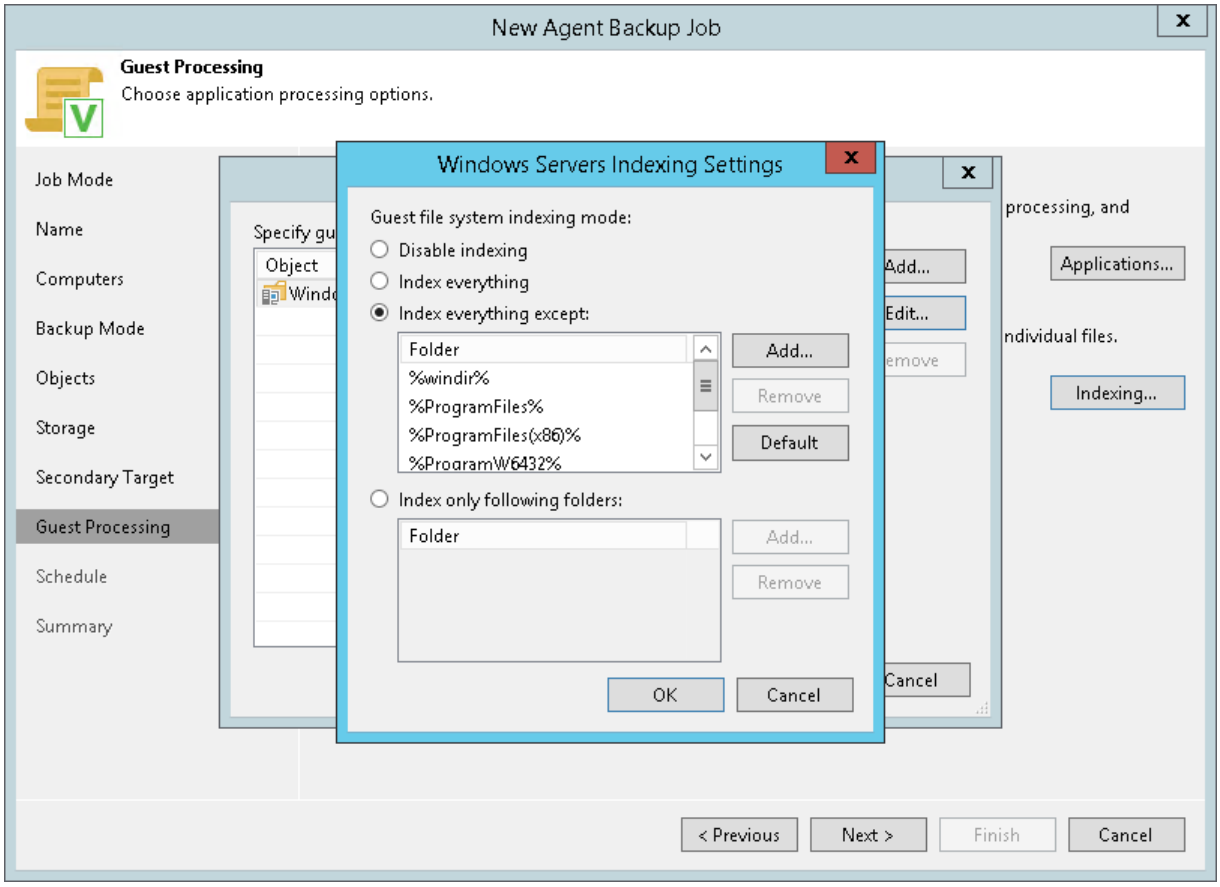
> **NOTE**
>
> File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the Preparing for File Browsing and Restore section in the Veeam Backup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

To specify file indexing options:

1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

4. In the **Windows indexing settings** window, specify the indexing scope:
   - Select **Index everything** if you want to index all files within the backup scope that you have specified at the Backup mode step of the wizard. Veeam Agent for Microsoft Windows will index all files that reside:
     - On the protected computer OS (for entire computer backup)
     - On the volumes that you have specified for backup (for volume-level backup)
     - In the folders that you have specified for backup (for file-level backup)
   - Select **Index everything except** if you want to index all files on the protected computer OS except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders using the **Add** and **Remove** buttons on the right. You can also use system environment variables to form the list, for example: *%windir%*, *%Program Files%* and *%Temp%*.

     To reset the list of folders to its initial state, click **Default**.
   - Select **Index only following folders** to define folders that you want to index. You can add or delete folders to index using the **Add** and **Remove** buttons on the right. You can also use system environment variables to form the list, for example: *%windir%*, *%Program Files%* and *%Temp%*.



Step 13. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup. Backup job scheduling options differ depending on the platform and job mode that you have selected at the Job Mode step of the wizard:

- Scheduling Settings for Workstations
- Scheduling Settings for Servers and Failover Clusters

> **NOTE**
>
> If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.

Scheduling Settings for Workstations

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

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 backup job to perform backup automatically at specific events.
2. If you have selected the *On these days* option, click the **Days** button and clear check boxes for the days when the job must not start.
3. Select the action that Veeam Agent for Microsoft Windows must perform in case the protected computer is powered off at the time when the scheduled backup job must start.
   - *Backup once powered on* — select this option if you want Veeam Agent for Microsoft Windows to start the scheduled backup job when the protected computer is powered on.
   - *Skip backup* — select this option if you want Veeam Agent for Microsoft Windows not to start the scheduled backup job when the computer is powered on. Veeam Agent for Microsoft Windows will perform backup at the next scheduled time.

4. If you want Veeam Agent for Microsoft Windows to perform a finalizing action after the backup job completes successfully, select the necessary action:
   - *Keep running* — select this option if the computer must keep on working.
   - *Sleep* — select this option if you want Veeam Agent for Microsoft Windows to bring the computer to the standby mode.
   - *Shutdown* — select this option if you want Veeam Agent for Microsoft Windows to shut down the computer.
   - *Hibernate* — select this option if you want Veeam Agent for Microsoft Windows to bring the computer to the hibernate mode. This option is available if the hibernate mode is enabled on the protected computer. To learn more, see this Microsoft KB article.

   When the backup job completes, Veeam Agent for Microsoft Windows will prompt a dialog with a countdown to the selected post-job action. You can select to proceed to the action immediately or to cancel the action. To learn more, see the Controlling Backup Post-Job Action section in the Veeam Agent for Microsoft Windows User Guide.
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 backup job when the user locks the Veeam Agent computer.
   - Select the **Log off** check box if you want to start the 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 backup job when the backup storage becomes available (for example, when the computer connects to a local network and the target shared folder is accessible).
   - Select the **Eject removable storage once backup is completed** check box if you want Veeam Agent for Microsoft Windows to unmount the storage device after the backup job completes successfully. With this option selected, backup files on the removable storage will be protected from encrypting ransomware, such as CryptoLocker.

     Veeam Agent applies this setting only to backup jobs triggered by the *When backup target is connected* event. In case of backup jobs triggered by other computer events or started periodically at specific time, Veeam Agent will ignore this setting, and the storage device will not be unmounted after the backup job completes successfully.

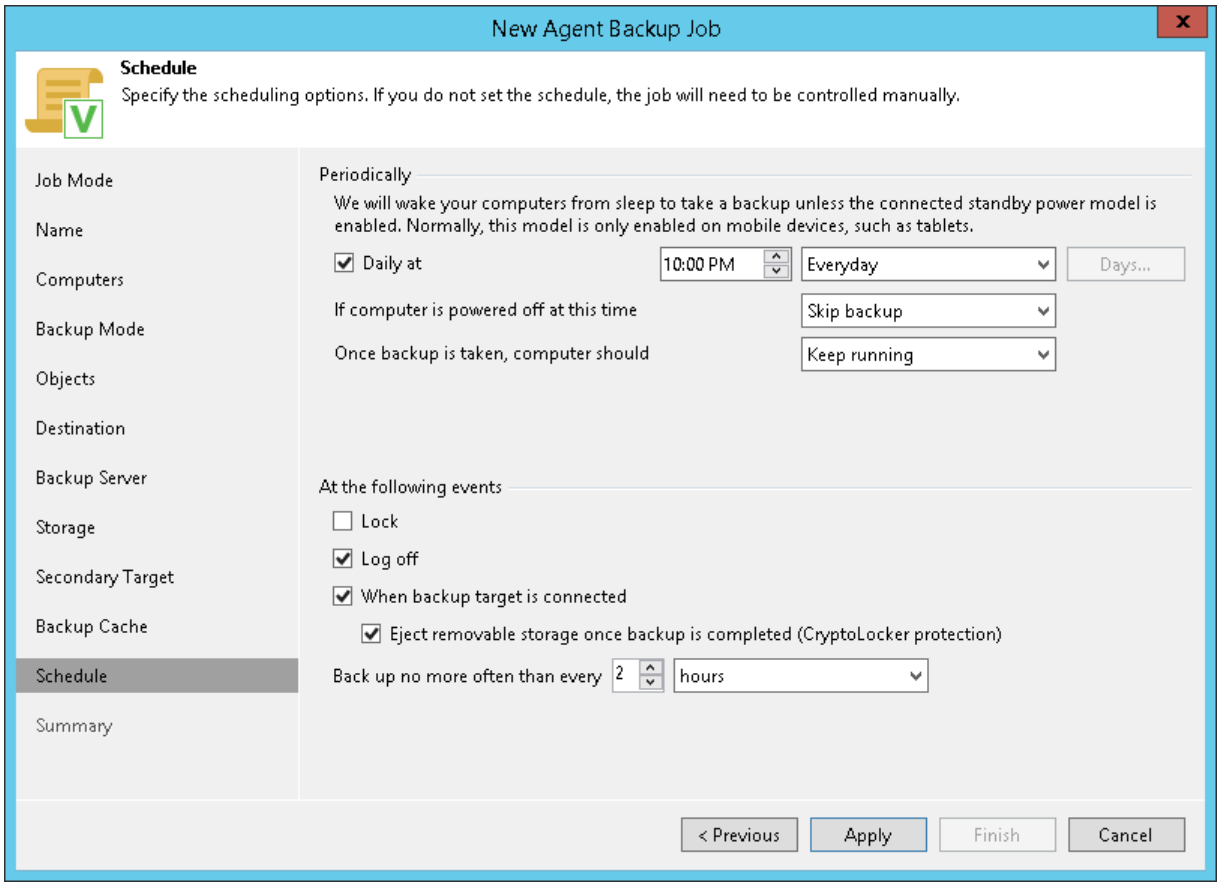
     > **IMPORTANT**
     >
     > The *Eject removable storage once backup is completed* option does not guarantee a bulletproof protection against ransomware. To ensure your backups are safe, keep the OS up to date and regularly scan your backup repository for virus threats using modern antivirus software.

   - Use the **Back up no more often than every <N> <time units>** field to restrict the frequency of backup job sessions. Specify a minutely, hourly or daily interval between the backup job sessions.

     The *Back up no more often than every <N> <time units>* option is applied only to job sessions started at specific events. Daily backups are performed according to defined schedule regardless of the time interval specified for this setting.

IMPORTANT

If the power scheme on the Veeam Agent computer does not allow using wake up timers, Veeam Agent for Microsoft Windows will not be able to wake your computer from sleep for backup. You can manually change the power scheme settings on the Veeam Agent computer. To do this, navigate to **Control Panel** > **All Control Panel Items** > **Power Options** > **Edit Plan Settings**.



Scheduling Settings for Servers and Clusters

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

A repeatedly run job is started by the following rules:

- The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
- If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

- To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.
- [For Managed by backup server mode only] To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list.

> **NOTE**
>
> Mind the following:
>
> - The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
> - The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Agent for Microsoft Windows (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Agent for Microsoft Windows retries the job for the defined number of times without any time intervals between the job runs.

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

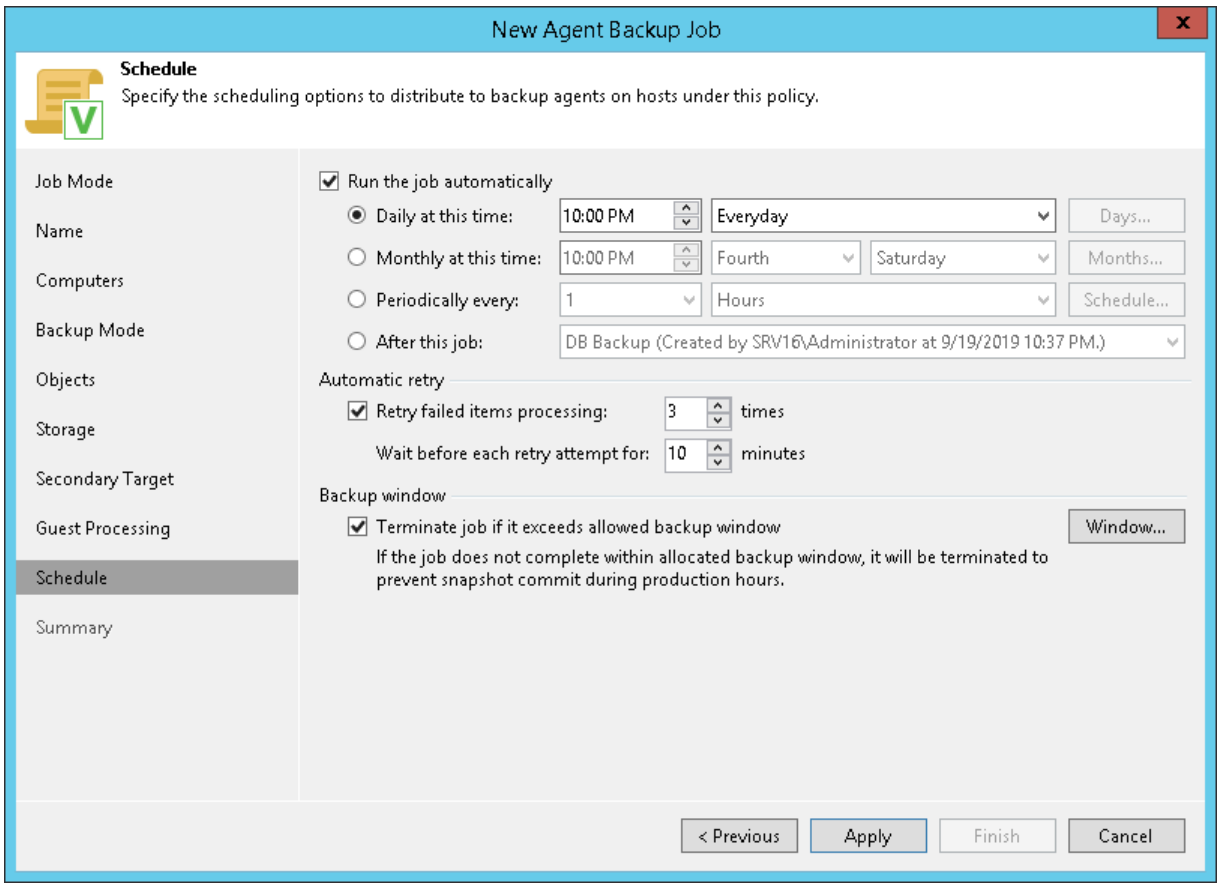
4. In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:

   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup.

      If the job exceeds the allowed window, it will be automatically terminated. In this case, data transport and backup chain transformation processes are stopped. Keep in mind that this behavior differs from a VM backup job where backup window affects data transport process and heath check operations only.

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



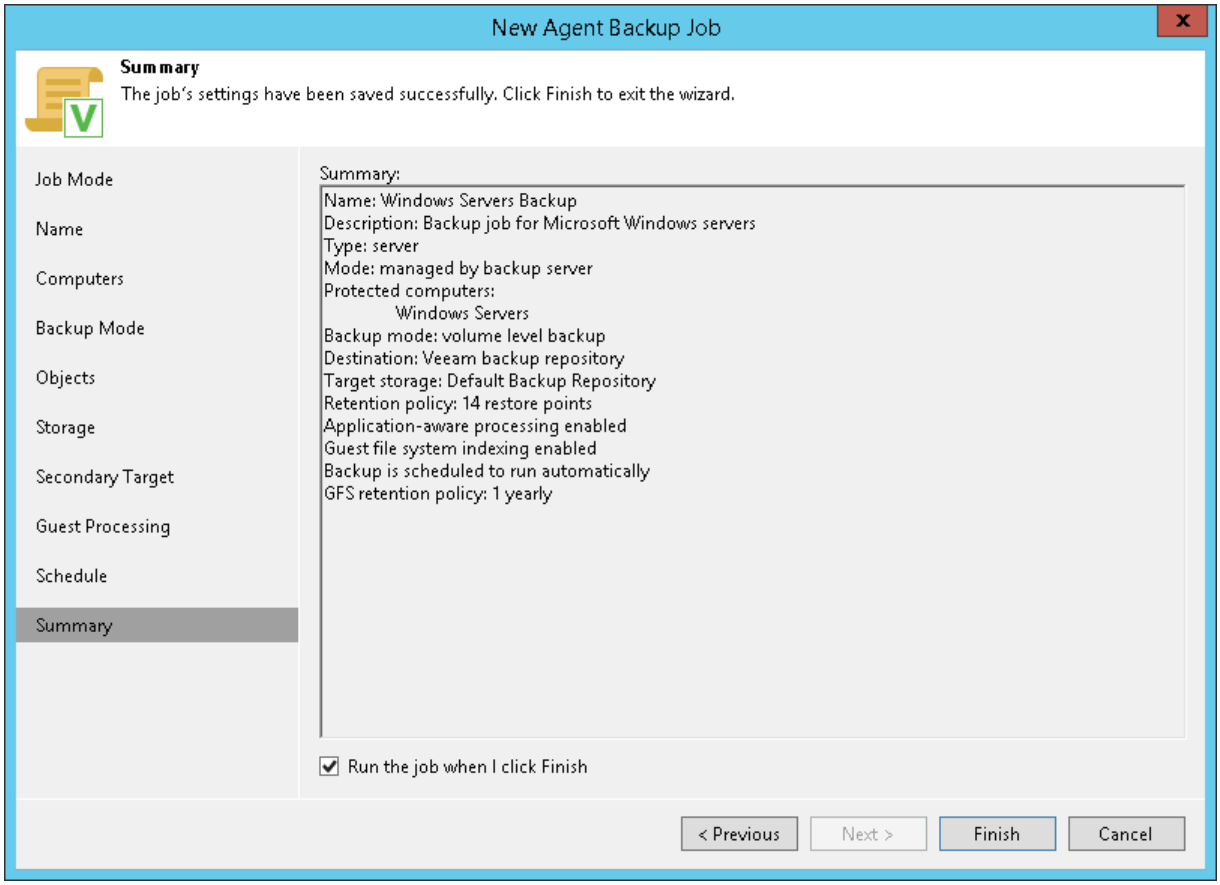
Step 14. Review Backup Job Settings

At the **Summary** step of the wizard, complete the backup job configuration process.

1. Review settings of the configured Veeam Agent backup job.
2. [For backup job managed by backup server] Select the **Run the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.

[For backup job managed by Veeam Agent] Keep in mind that Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Microsoft Windows Configuration.



Creating Job for Linux Computers

To back up data of a computer protected with Veeam Agent for Linux, you must configure a Veeam Agent backup job in Veeam Backup & Replication.

Before You Begin

Before you create a Veeam Agent backup job in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup job.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the job must be configured in advance.
- [For backup jobs targeted at the cloud repository] The Veeam Cloud Connect service provider must be added in the Veeam backup console.

Veeam Agent backup jobs have the following limitations:

- For Veeam Agent backup job managed by backup server, you can create Veeam Agent backups on a Veeam backup repository and Veeam Cloud Connect repository. If you want to save backups in other target locations, you must configure a Veeam Agent backup job managed by Veeam Agent (backup policy). To learn more, see Veeam Agent Backup Jobs and Policies.
- [For Veeam Agent backup job managed by Veeam Agent] 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.
- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup job settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Agent does not support creating transaction log backups in the cloud repository. You cannot enable transaction log backup options in the properties of the backup job targeted at the cloud repository.
- If you plan to create a Veeam Agent backup job for computers with Veeam Agents installed using the `veeam-nosnap` package, consider the limitations and system requirements in the Appendix A. Requirements for veeam-nosnap section of the Veeam Agent for Linux User Guide.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job for protected computers that run a Linux OS in one of the following ways:

- Create a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.
- Add a protection group to a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.
- Add individual computers to a new backup job — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.

Launching Backup Job Wizard

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

- On the **Home** tab, click **Backup Job** > **Linux computer**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Linux computer** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Linux computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Linux** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup job and click **Add to Backup** > **Linux** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the job. You can add other protection groups and (or) individual computers to the job later on, when you pass through the wizard steps.

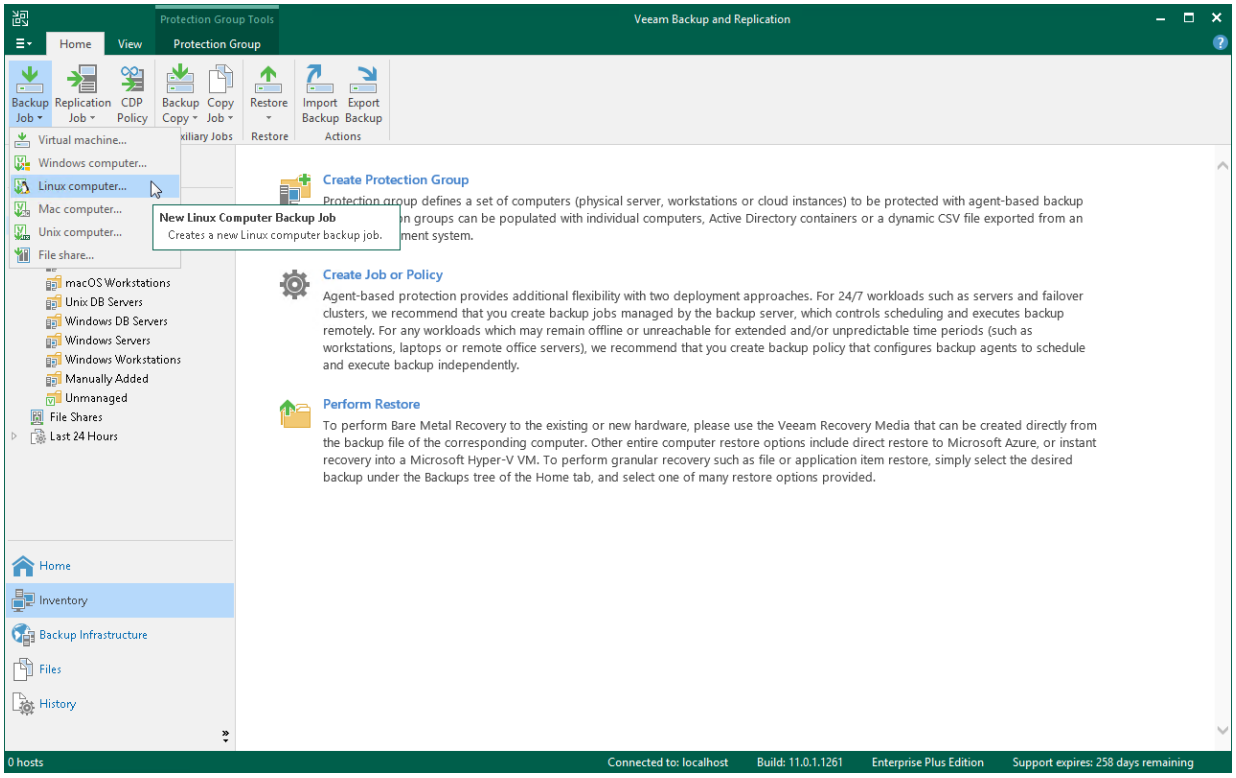
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job, right-click the selected computer and select **Add to backup job** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job and click **Add to Backup** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the job. You can add other computers and (or) protection groups to the job later on, when you pass through the wizard steps.

> **TIP**
>
> Consider the following:
>
> - You can press and hold **[CTRL]** to select multiple computers at once.
> - You can add an individual computer or protection group to a Veeam Agent backup job that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.



Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the backup job:

1. Select the type of protected computers whose data you want to back up with Veeam Agents.
2. If you choose to back up data pertaining to servers, select the job mode.

   The job mode defines the type of the created Veeam Agent backup job: the backup job (backup job managed by the backup server) or backup policy (backup job managed by Veeam Agent).

Selecting Protected Computer Type

At the **Job Mode** step of the wizard, in the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents. The selected type defines what settings will be available for the configured backup job and the job mode. You can select one of the following computer types:

- **Workstation** — select this option if you want to back up data pertaining to Linux-based workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  For backup jobs that process workstations, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent for Linux operating in the *Workstation* mode. To learn more, see the Product Editions section in the Veeam Agent for Linux User Guide.

  With this option selected, the backup job will be managed by Veeam Agent installed on the protected computer — you do not need to select the job mode.

- **Server** — select this option if you want to back up data pertaining to Linux-based servers. This option is suitable for computers that have permanent connection to the backup server.

  For backup jobs that process servers, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent for Linux operating in the Server mode. To learn more, see Veeam Agent for Linux User Guide.

  With this option selected, you can also select the job mode. To learn more, see Selecting Job Mode.

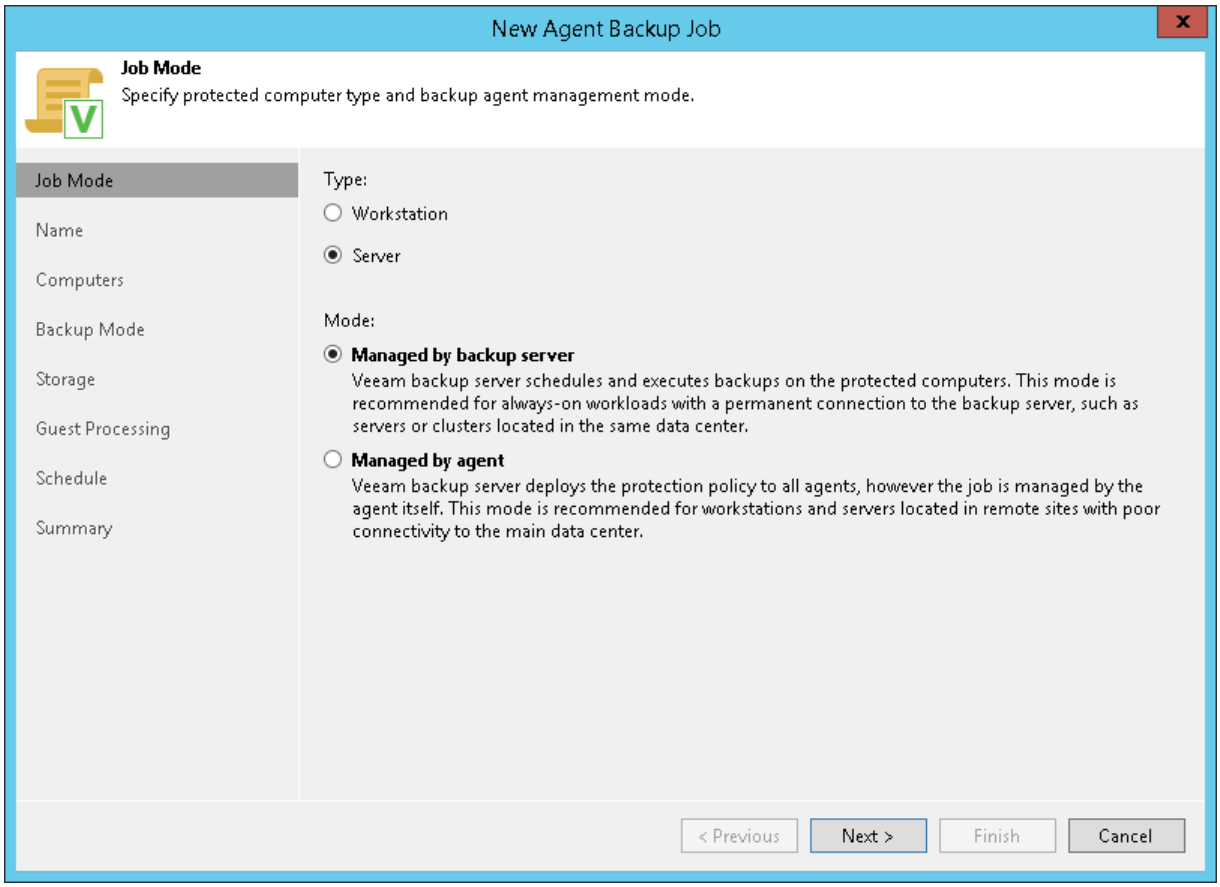
Selecting Job Mode

If you selected the **Servers** computer type in the Type field, in the **Mode** field, select the job mode. You can select one of the following modes:

- **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job. With this option selected, you will be able to add one or more individual computers and/or protection groups to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or Veeam Cloud Connect repository. The Veeam Agent backup job will run on the backup server in the similar way as a regular job for VM data backup. To learn more, see Backup Job.
- **Managed by agent** — select this option if you want to configure the backup policy. The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers, and acts as a saved template. With this option selected, you will be able to add one or more individual computers and/or protection groups to the backup policy, and instruct Veeam Agent to create backups on a local disk of a protected computer, in a network shared folder, Veeam backup repository or Veeam Cloud Connect repository. To learn more, see Backup Policy.

NOTE

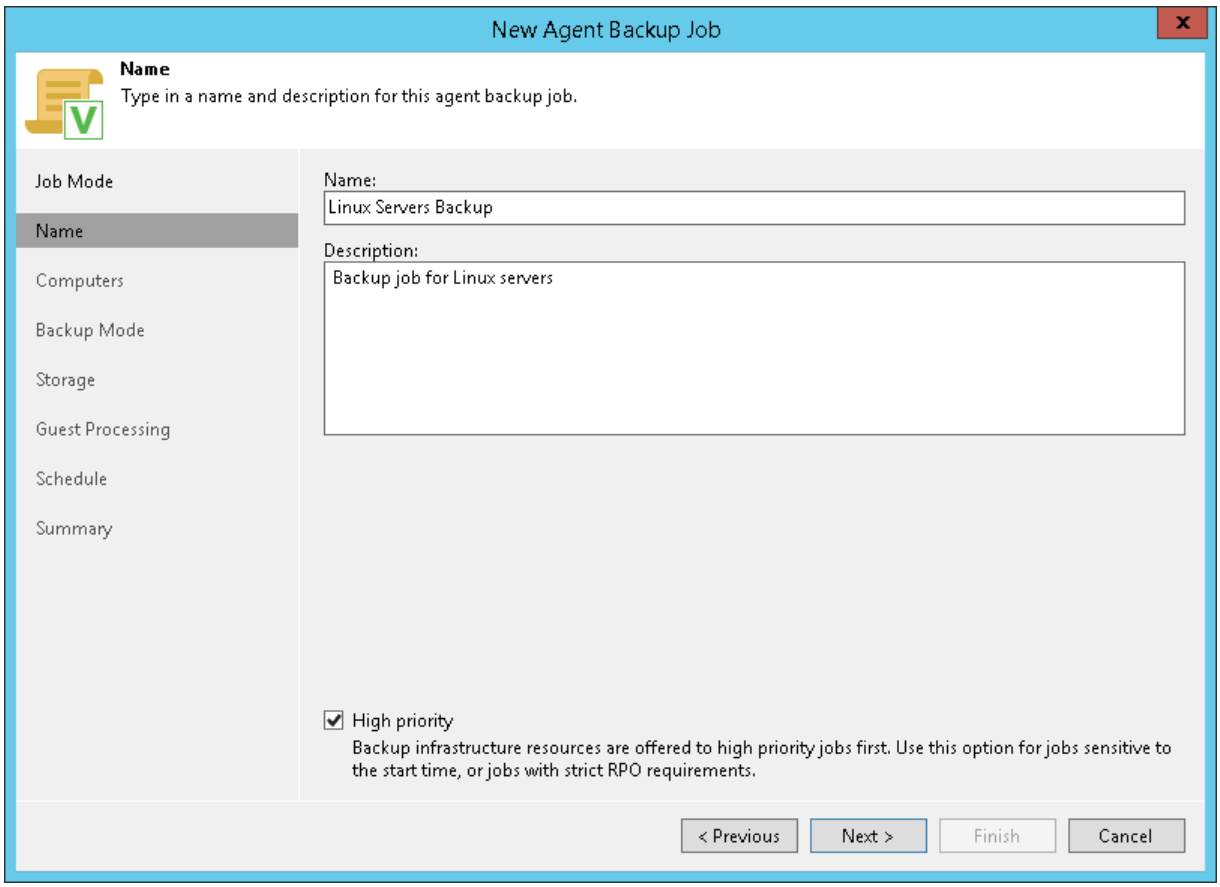
You must select the **Managed by agent** option if you want to use the backup job to protect computers included in protection groups for pre-installed Veeam Agents. To learn more, see Select Protection Group Type.



Step 3. Specify Job Name and Description

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

1. In the **Name** field, enter a name for the backup job.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the job, date and time when the job was created.
3. [For backup job managed by backup server] Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. To learn more, see the Job Priorities section in the Veeam Backup & Replication User Guide.



Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers that you want to back up.

You can add to the Veeam Agent backup job one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. You can also add to the job computers that are not added to inventory yet. Veeam Backup & Replication will add such computers to the job and also add them to the **Manually Added** protection group.

Jobs with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup job is created, Veeam Backup & Replication will automatically update the job settings to include the added computer.

NOTE

- If you used the **Add to backup job** > **Linux** > **New job** option to launch the **New Agent Backup Job** wizard, the **Protected computers** list will already contain computers that you have selected to add to the job. You can remove some computers from the job or add new computers to the job, if necessary.
- Veeam Backup & Replication displays protection groups for pre-installed Veeam Agents and their members only if you selected the **Managed by Agent** option at the **Job Mode** step of the wizard. You cannot add protection groups for pre-installed Veeam Agents to backup jobs managed by backup server. To learn more, see Selecting Job Mode.

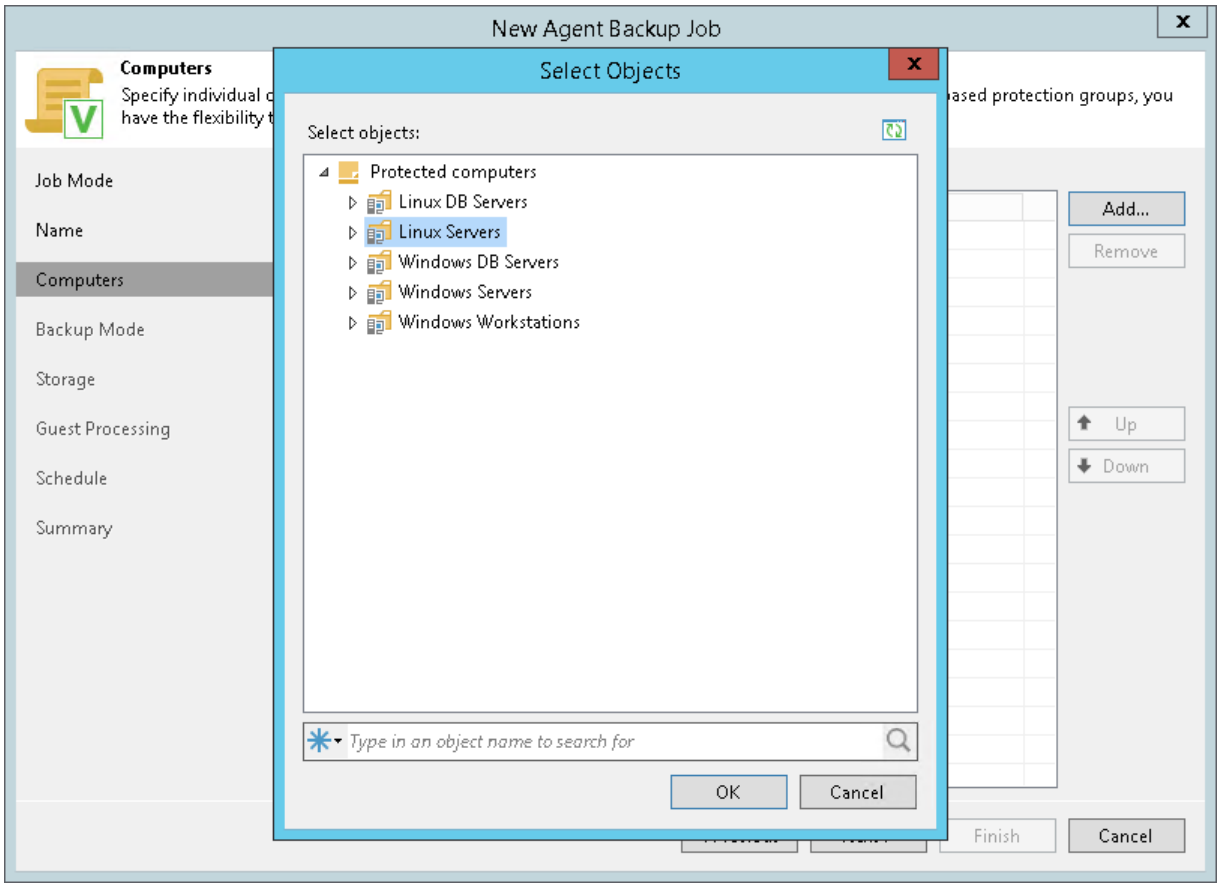
Adding Protection Groups and Computers from Inventory

To add protection groups and/or individual computers to the Veeam Agent backup job:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and/or computers in the list and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

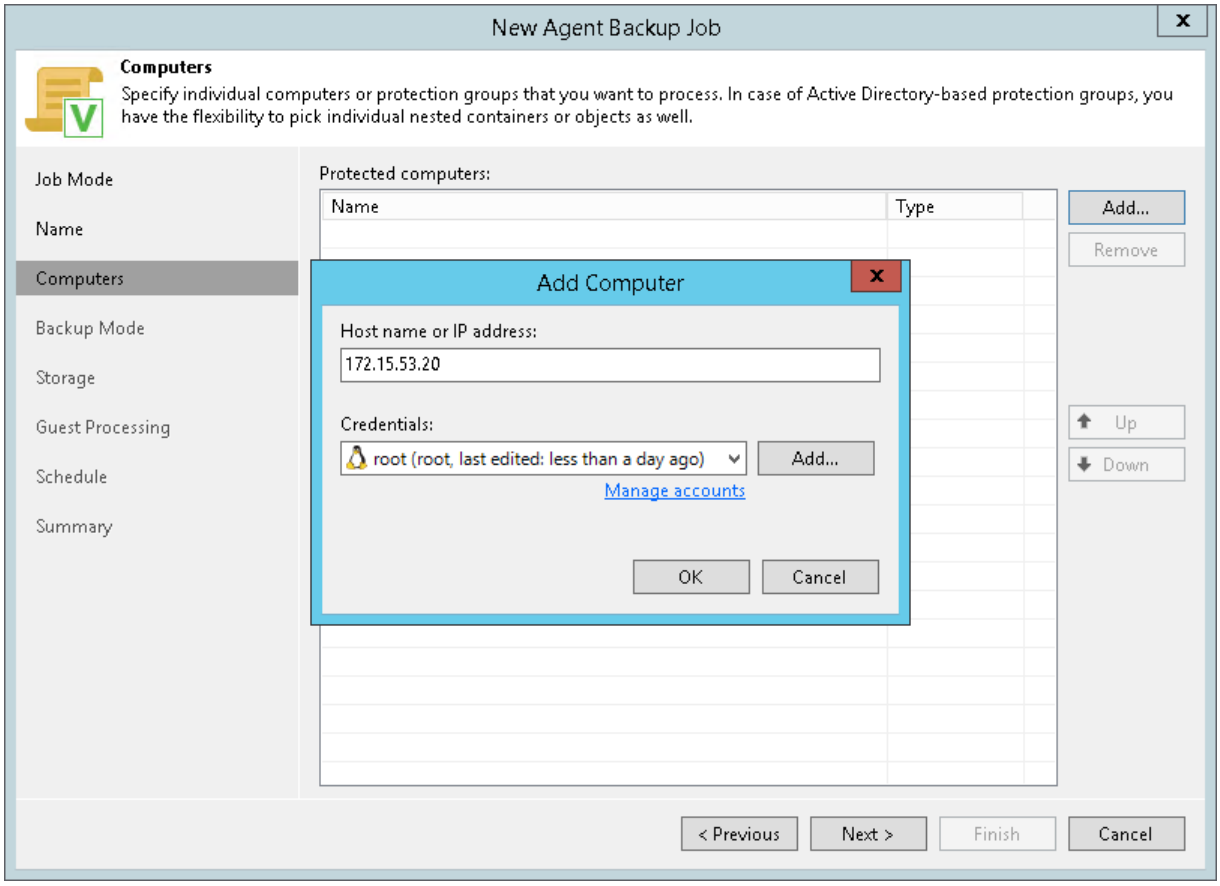
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Adding New Computers

To add to the Veeam Agent backup job new computers that do not exist in the inventory:

1. Click **Add** > **Individual computer**.
2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name or IP address of the computer that you want to add to the job.
3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the job. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.



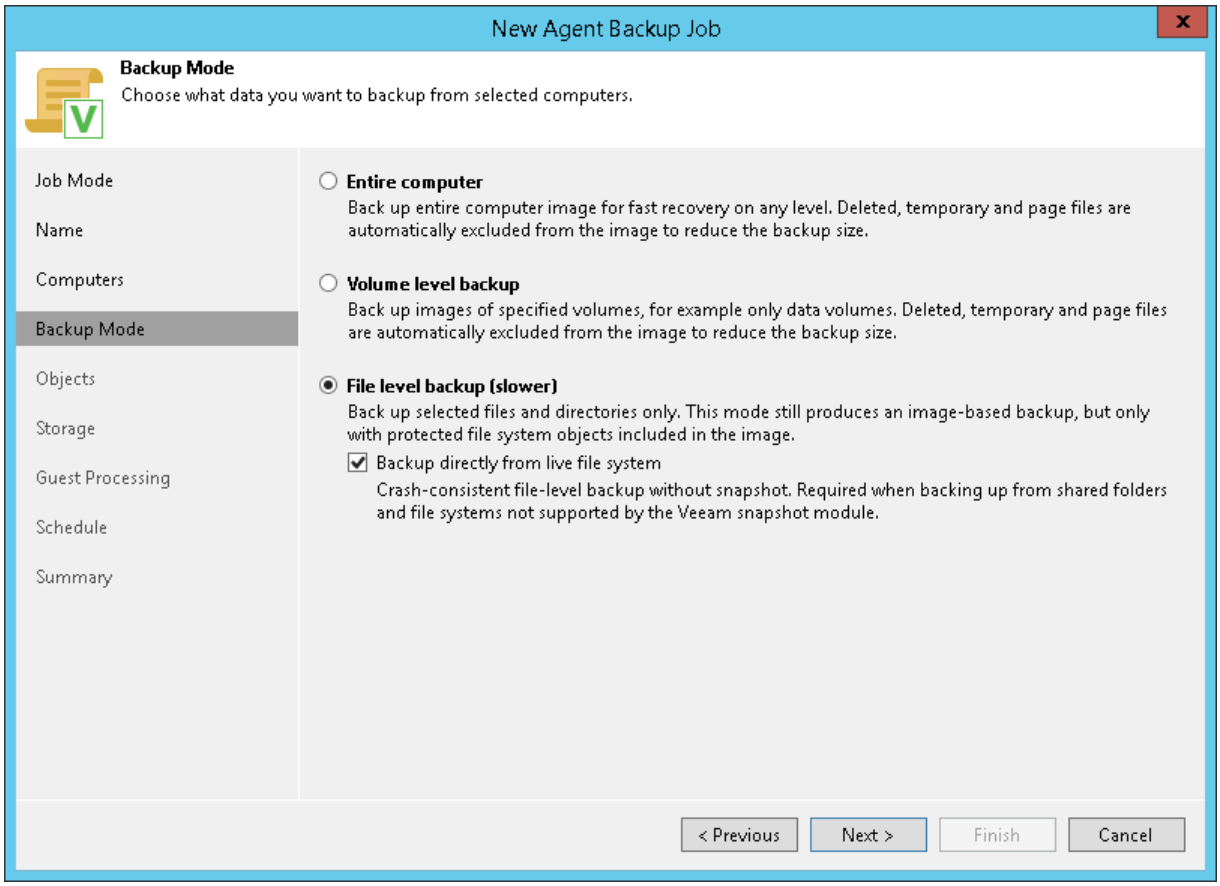
Step 5. Select Backup Mode

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

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:
   - **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, directories, application data and so on. With this option selected, you will pass to one of the following steps of the wizard:
     - Storage — if the Managed by backup server option was selected at the Job Mode step of the wizard.
     - Destination — if the Managed by agent option was selected at the Job Mode step of the wizard.
   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, the system volume. When you restore data from such backup, you will be able to recover data on these volumes only: files, directories, application data and so on. With this option selected, you will pass to the Objects step of the wizard.
   - **File level backup** — select this option if you want to create a backup of individual directories on your computer. With this option selected, you will pass to the Objects step of the wizard.
2. [For file-level backup] If you want to perform backup in the snapshot-less mode, select the **Backup directly from live file system** check box. With this option selected, Veeam Agent for Linux will not create a snapshot of a backed-up volume during backup. This allows Veeam Agent to back up data residing in file systems that are not supported for snapshot-based backup with Veeam Agent for Linux. To learn more, see the Snapshot-Less File-Level Backup section in the Veeam Agent for Linux User Guide.

TIP

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



Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you chose to create volume-level or file-level Veeam Agent backups. Specify backup scope for the backup job:

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

Specifying Volumes to Back Up

The **Objects** step of the wizard is available if you have chosen to create 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. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified volume does not exist on one or more computers in the job, the job will skip such volumes on those computers and back up only existing ones.

To specify the backup scope:

1. In the **Objects to backup** field, click **Add** and select the type of object that you want to include in the backup: *Device*, *Mount point*, *LVM* or *BTRFS*.
2. In the **Add Object** window, specify the object that you want to back up and click **OK**.

   You can specify the following objects to back up:

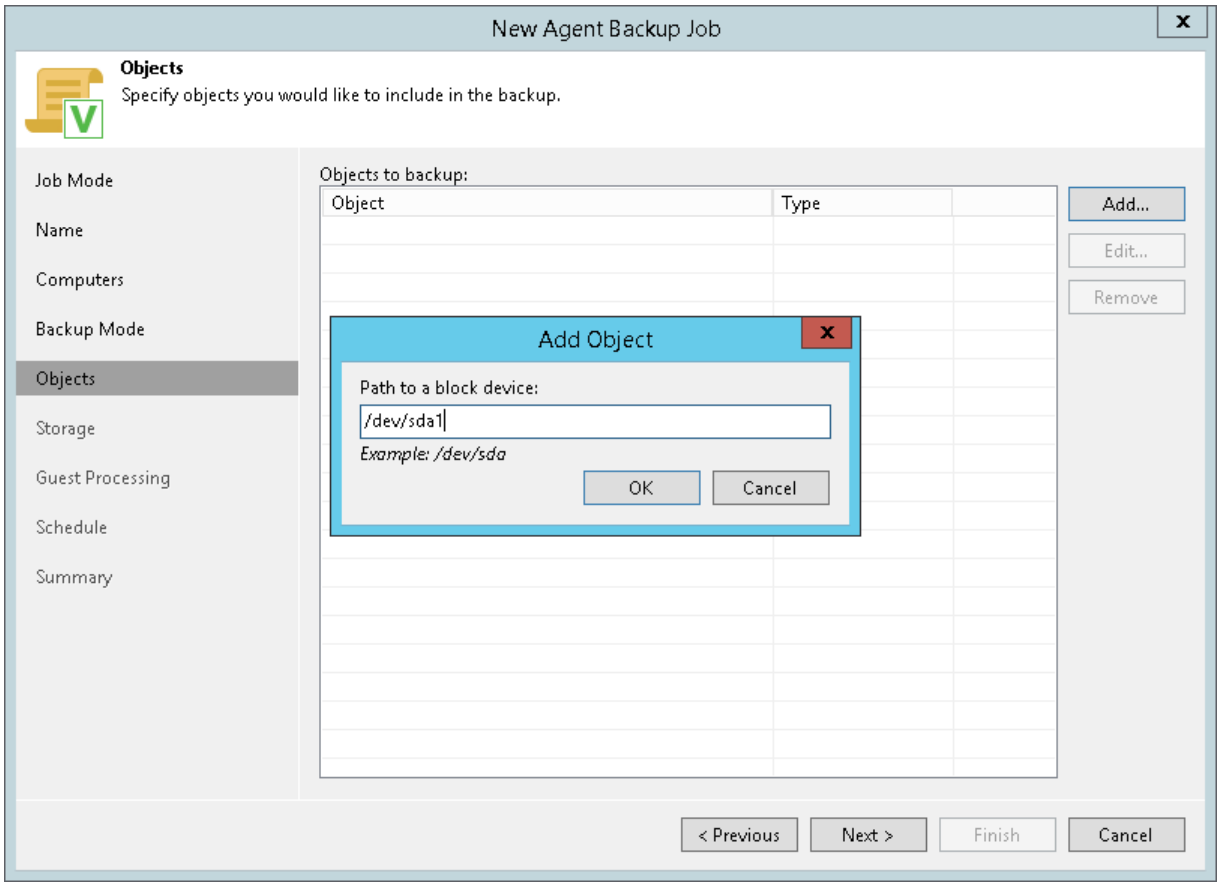
   - *Block devices*. You can include in the backup scope all volumes on a computer disk or individual volumes of a protected computer:
     - To include all volumes on a computer disk in the backup, type the path to a block device that represents the disk whose volumes you want to back up. For example: /dev/*sda*.
     - To include a specific volume of a protected computer in the backup, type the path to a block device that represents the volume that you want to back up. For example: */dev/sda1*.

     > **NOTE**
     >
     > If you include a block device in the backup, and this block device is a physical volume assigned to an LVM volume group, Veeam Agent will include the whole LVM volume group in the backup.

   - *Mount points*. You can include in the backup scope individual volumes of a protected computer. Type the path to a mount point of the volume that you want to back up. For example: / or /home.
   - *LVM volumes*. You can include in the backup scope entire LVM volume groups or individual LVM logical volumes of a protected computer. Type the path to a mount point or a block device that represents the volume group or logical volume that you want to back up. For example: */dev/vg* or */dev/vg/lv1*.
   - *Btrfs subvolumes*. You can include in the backup scope all Btrfs subvolumes of a Btrfs storage pool or specific Btrfs subvolumes.
     - To include all subvolumes of a Btrfs pool in the backup, type the path to a block device that represents the Btrfs pool. For example: */dev/sda1*.
     - To include a specific Btrfs subvolume in the backup, type the path to a mount point of this subvolume. For example: */sub1*.

3. Repeat steps 1–2 for all objects that you want to back up.

If you have created several system partitions, for example, a separate partition for the `/boot` directory, make sure that you include all of these partitions in the backup. Otherwise, Veeam Agent for Linux does not guarantee that the OS will boot properly when you attempt to recover from such backup.



Specifying Directories to Back Up

The **Objects** 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 directories with files you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified directory does not exist on one or more computers in the job, the job will skip such folder on those computers and back up existing ones.

To specify directories to back up:

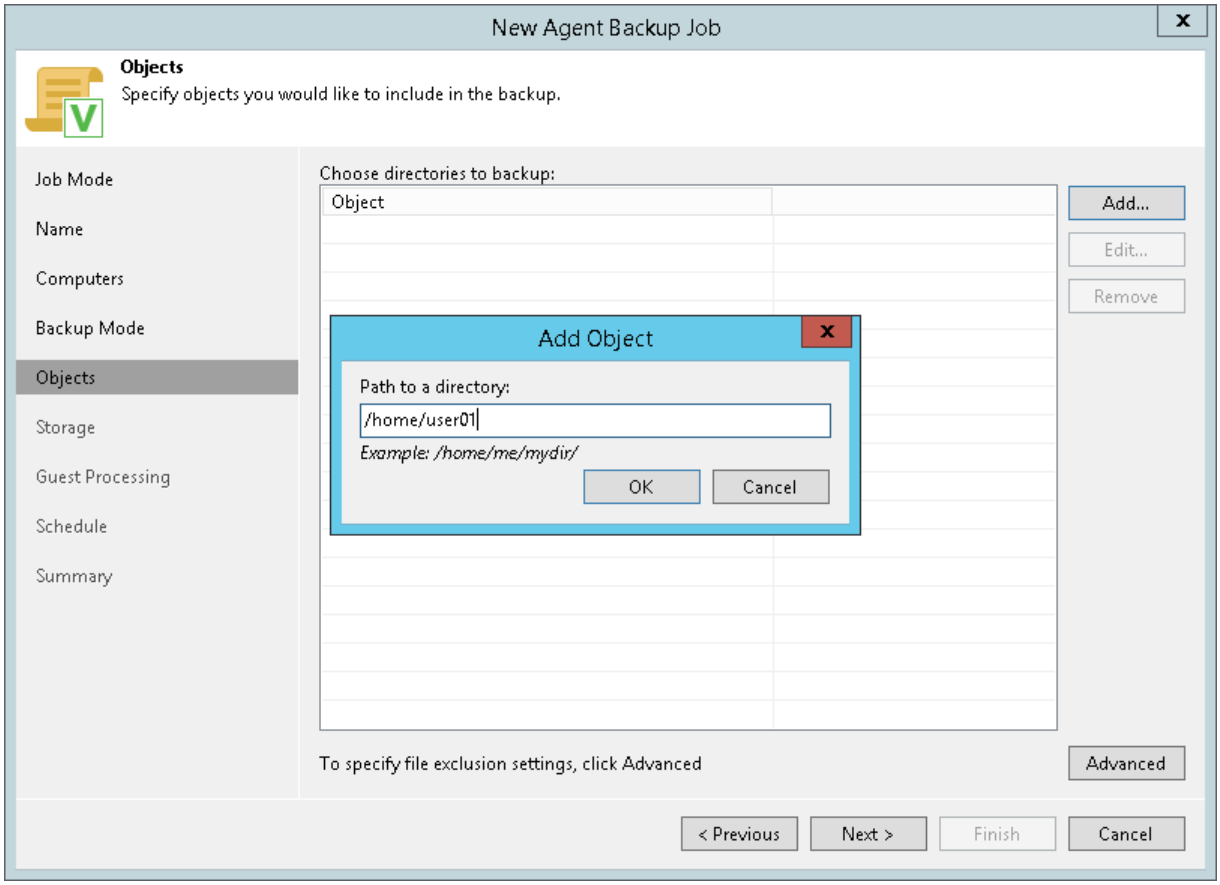
1. In the **Choose directories to backup** field, click **Add**.
2. In the **Add Object** window, type the path to a directory that you want to back up, for example, */home/user01*, and click **OK**.
3. Repeat steps 1–2 for all directories that you want to back up.

TIP

If you want to back up the root directory and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.

For example, you have a file system mounted to the `/home/media` directory. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root directory and the mounted file system, add the following objects to the backup scope:

- `/`
- `/home/media`



Configuring Filters

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

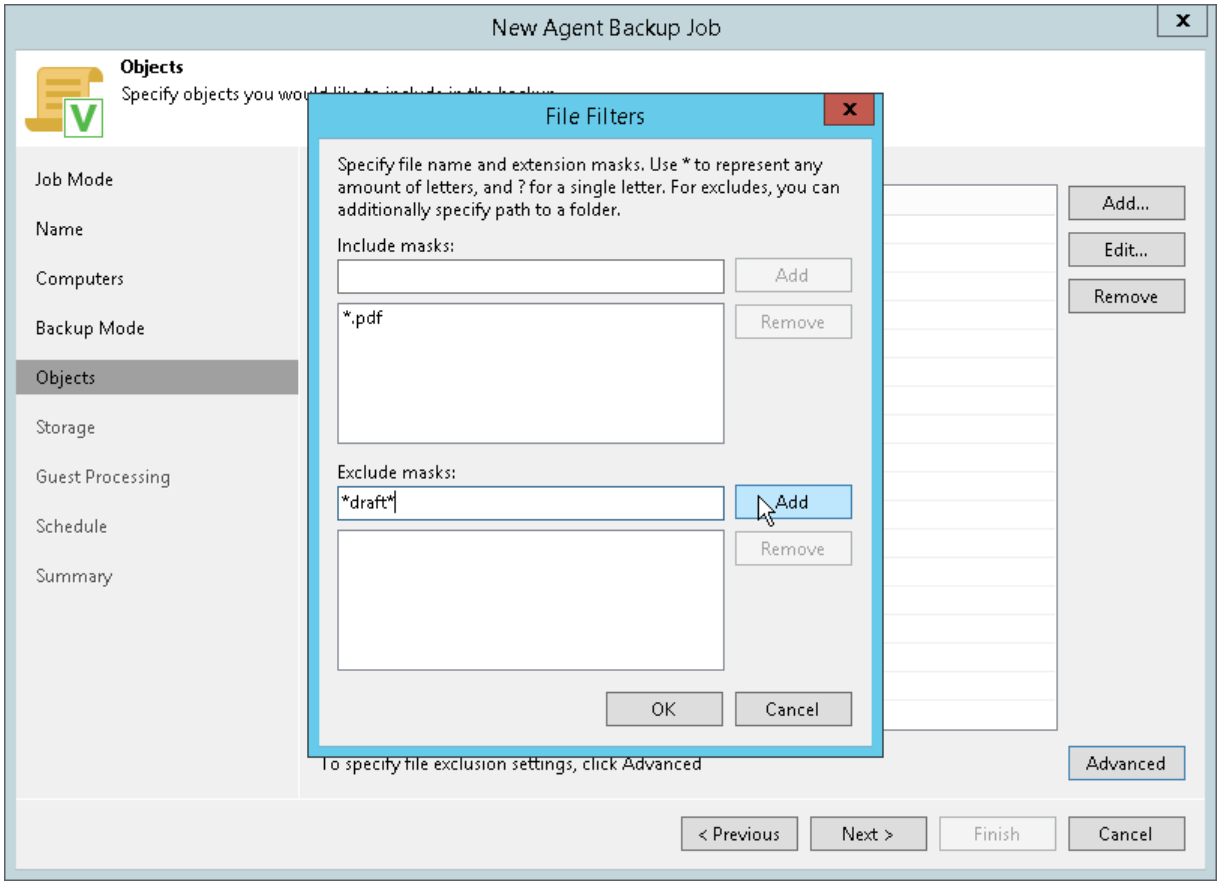
To configure a filter:

1. At the **Objects** 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, *Report.pdf* or **filename**. Veeam Agent for Linux 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, *OldReports.tar.gz* or **.odt*. Veeam Agent for Linux 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: **.pdf*
- Exclude mask: **draft**

Veeam Agent for Linux will include in the backup all files of the PDF format that do not contain *draft* in their names.



Step 7. Select Backup Destination

The **Destination** step of the wizard is available if you have selected the **Managed by agent** option at the Job Mode step of the wizard.

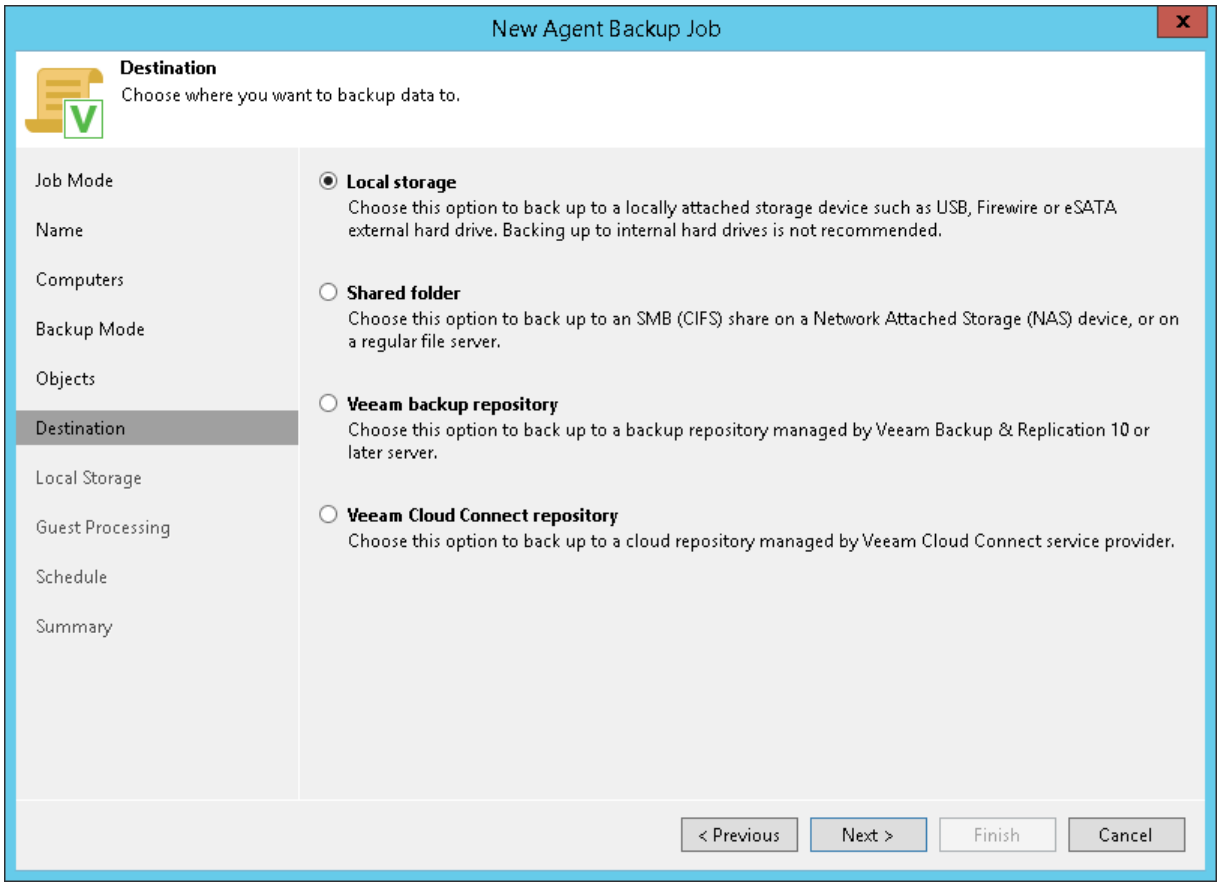
At this step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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

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

> **IMPORTANT**
>
> It is 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.

- **Shared folder** — select this option if you want to save a backup in a network shared folder. With this option selected, you will pass to the Shared folder step of the wizard.
- **Veeam backup repository** — select this option if you want to save a backup on a backup repository managed by a Veeam backup server. With this option selected, you will pass to the Backup Server step of the wizard.
- **Veeam Cloud Connect repository** — select this option if you want to save a backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the Storage step of the wizard.



Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- If you have selected the **Managed by backup server** mode at the Job Mode step of the wizard, you can create Veeam Agent backups on a backup repository managed by this Veeam backup server. Specify Veeam backup repository settings at the Storage of the wizard.
- If you have selected the **Managed by agent** mode at the Job Mode step of the wizard, specify backup storage settings at one of the following steps of the wizard:
  - Local storage settings — if you have selected the **Local storage** option at the Destination step of the wizard.
  - Shared folder settings — if you have selected the **Shared folder** option at the Destination step of the wizard.
  - Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
  - Cloud repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.

Backup Storage Settings

The **Storage** step of the wizard is available if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

Specify settings for the target backup repository managed by the same backup server that manages the Backup Job:

1. From the **Backup repository** list, select a backup repository where you want to store Veeam Agent backups. You can select from the following types of backup repositories:
   - Veeam backup repository configured on the backup server that will manage the created backup job.
   - Cloud repository allocated to your tenant account by a Veeam Cloud Connect service provider.

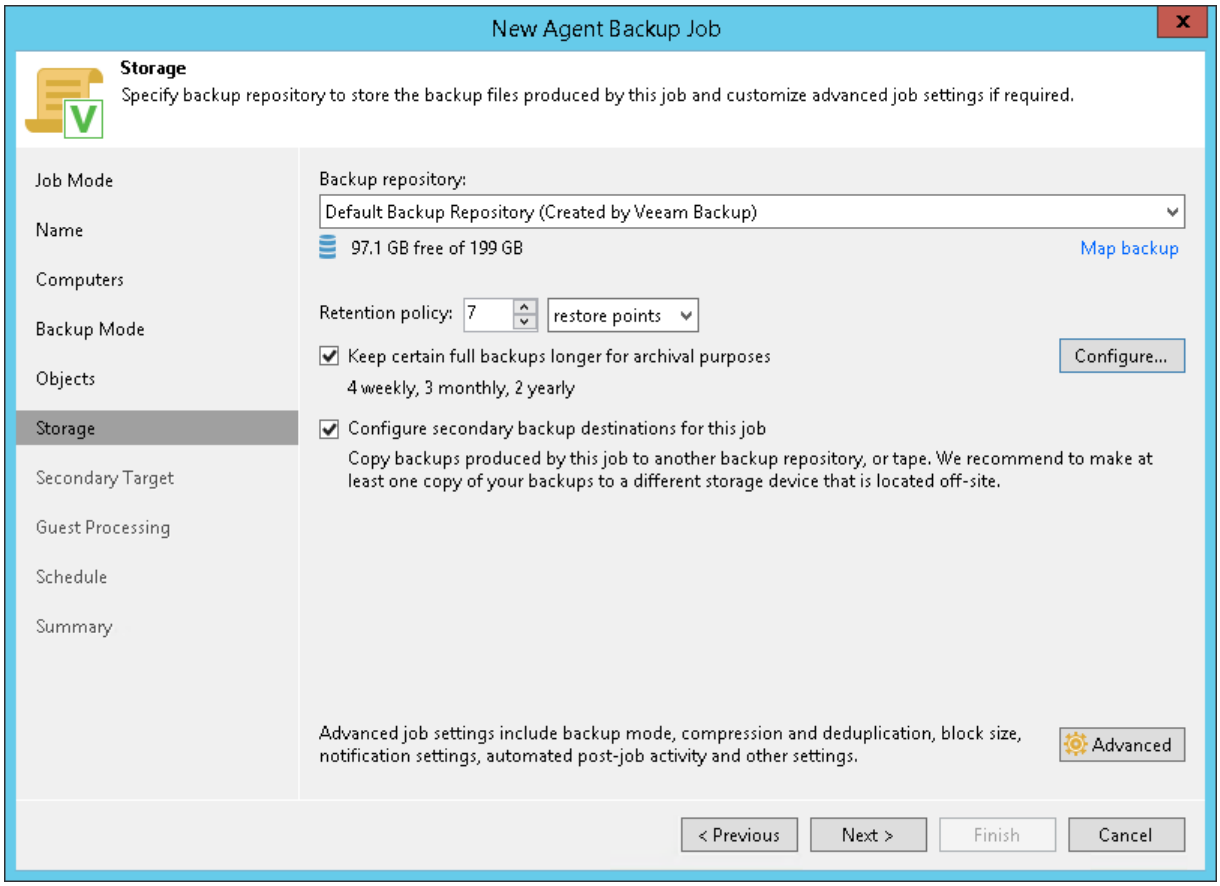
   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. You can map the job to a specific backup stored on the backup repository. Backup job mapping can be helpful if you have moved backup files to a new backup repository and want to point the job to existing backups on this new backup repository. You can also use backup job mapping if the configuration database got corrupted and you need to reconfigure backup jobs.

   To map the job to a backup, click the **Map backup** link and select the backup on the backup repository. Backups can be easily identified by job names. To find the backup, you can also use the search field at the bottom of the window.

   > **NOTE**
   >
   > Mind the following:
   >
   > - Backup job mapping is available only for a Veeam Agent backup job managed by the backup server.
   > - You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created on a backup repository by Veeam Agent operating in the standalone mode.

3. Specify backup retention policy settings:
   - From the **Retention policy** list, select *restore points* and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the **Retention policy** list, select *days* and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep some periodic full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.
5. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary Target. At the **Secondary Target** step of the wizard, you can link the backup job to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.
6. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



Local Storage Settings

The **Local Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save the backup on a local drive of your computer.

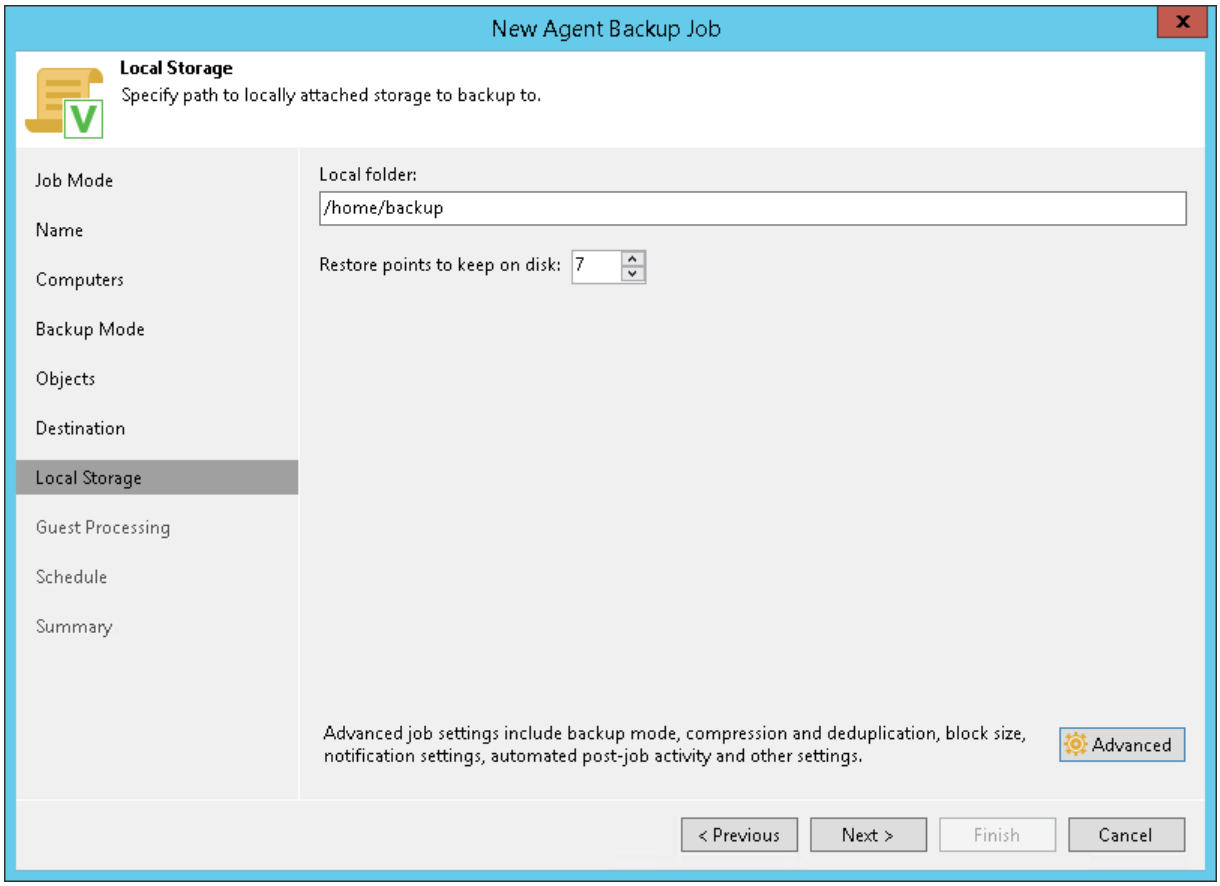
Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent for Linux will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup job settings to this computer.

   > **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.

2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

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



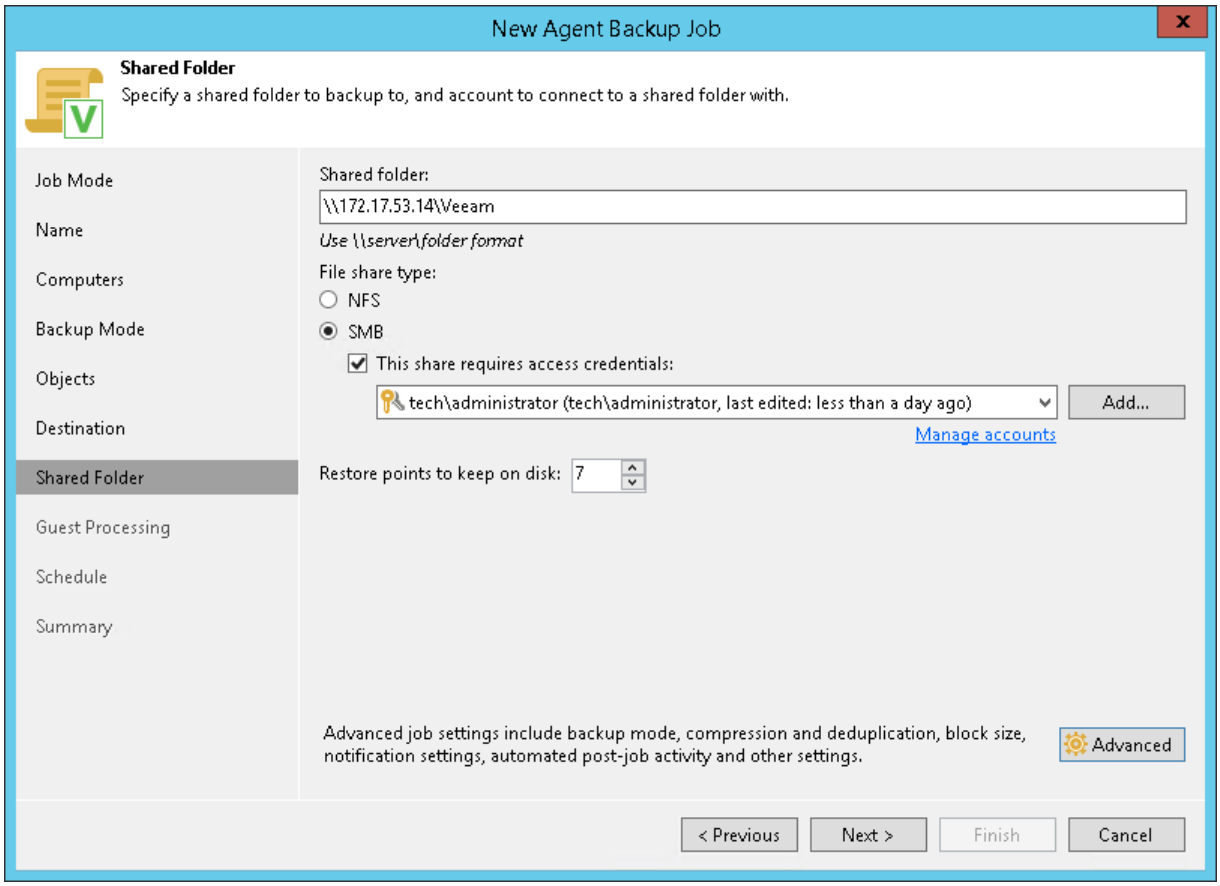
Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save the backup in a network shared folder.

Specify shared folder settings:

1. In the **File share type** section, select the type of a network shared folder:
   - **NFS** — to connect to a network shared folder using the NFS protocol.
   - **SMB** — to connect to a network shared folder using the SMB (CIFS) protocol.
2. In the **Shared folder** field, type a name of the network shared folder in which you want to store backup files.
   - [For an NFS shared folder] Specify a name of the network shared folder in the *SERVER://DIRECTORY* format.
   - [For an SMB shared folder] Specify a UNC name of the network shared folder. Keep in mind that the UNC name always starts with two back slashes (\\).
3. [For an SMB shared folder] If the network shared folder requires authentication, select the **This share requires access credentials** check box and select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. The user name must be specified in the *DOMAIN\USERNAME* format.
4. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

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



Veeam Backup Repository Settings

If you have selected the **Managed by agent** mode for the backup job and chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

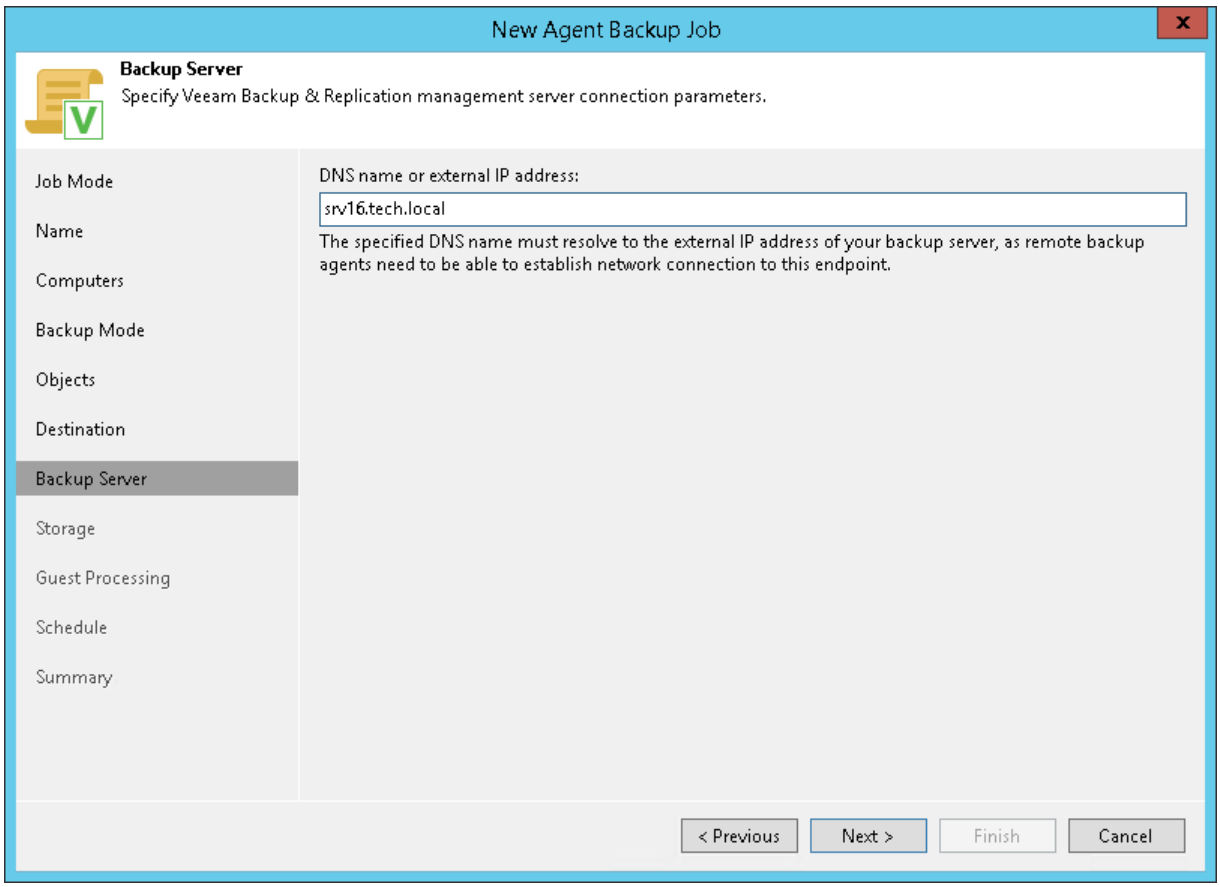
Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to store backup files on a Veeam backup repository.

In the **DNS name or external IP address field**, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup job. The specified DNS name or IP address must be accessible from the network to which Veeam Agent computers are connected.

NOTE

Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.



Selecting Backup Repository

The **Backup Repository** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam backup repository.

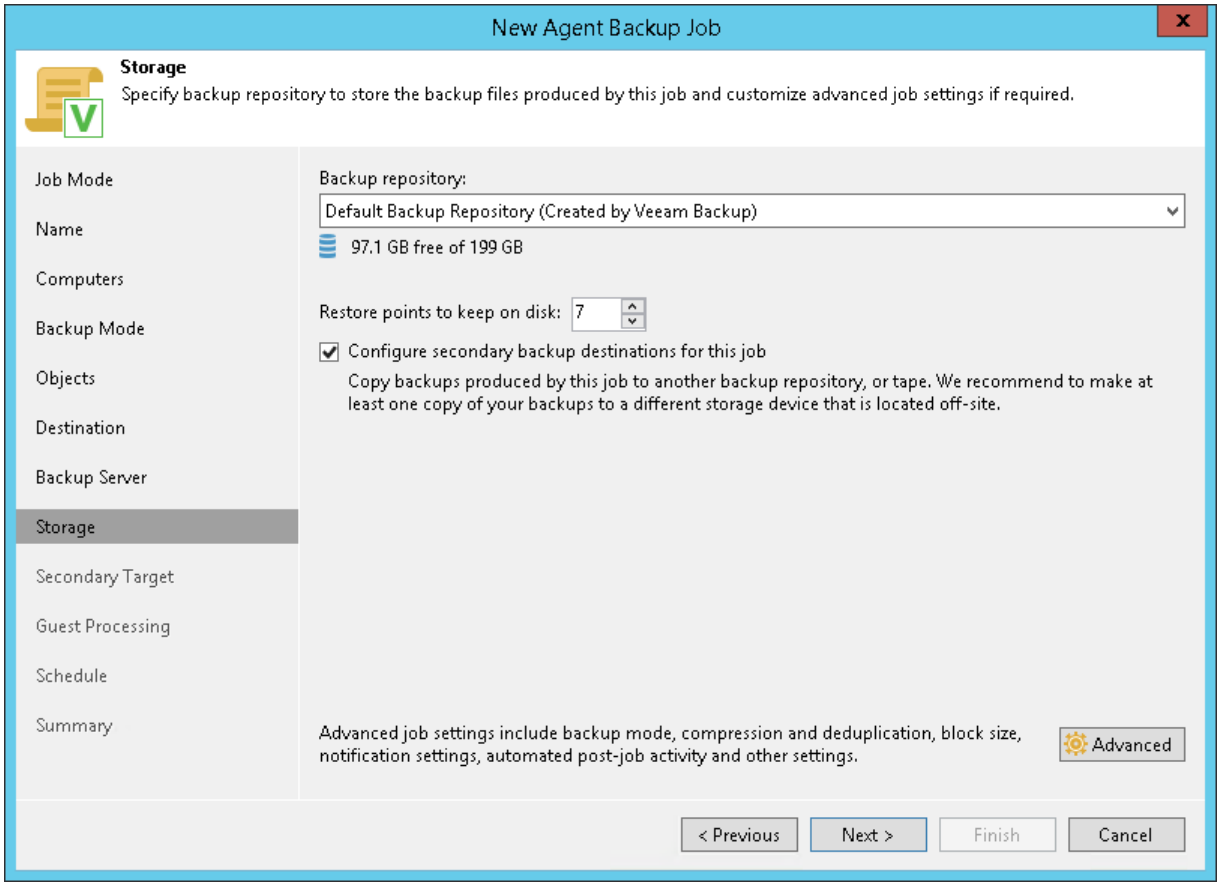
Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

3. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary Target. At the **Secondary Target** step of the wizard, you can link the backup job to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.

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



Cloud Repository Settings

The **Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam Cloud Connect repository.

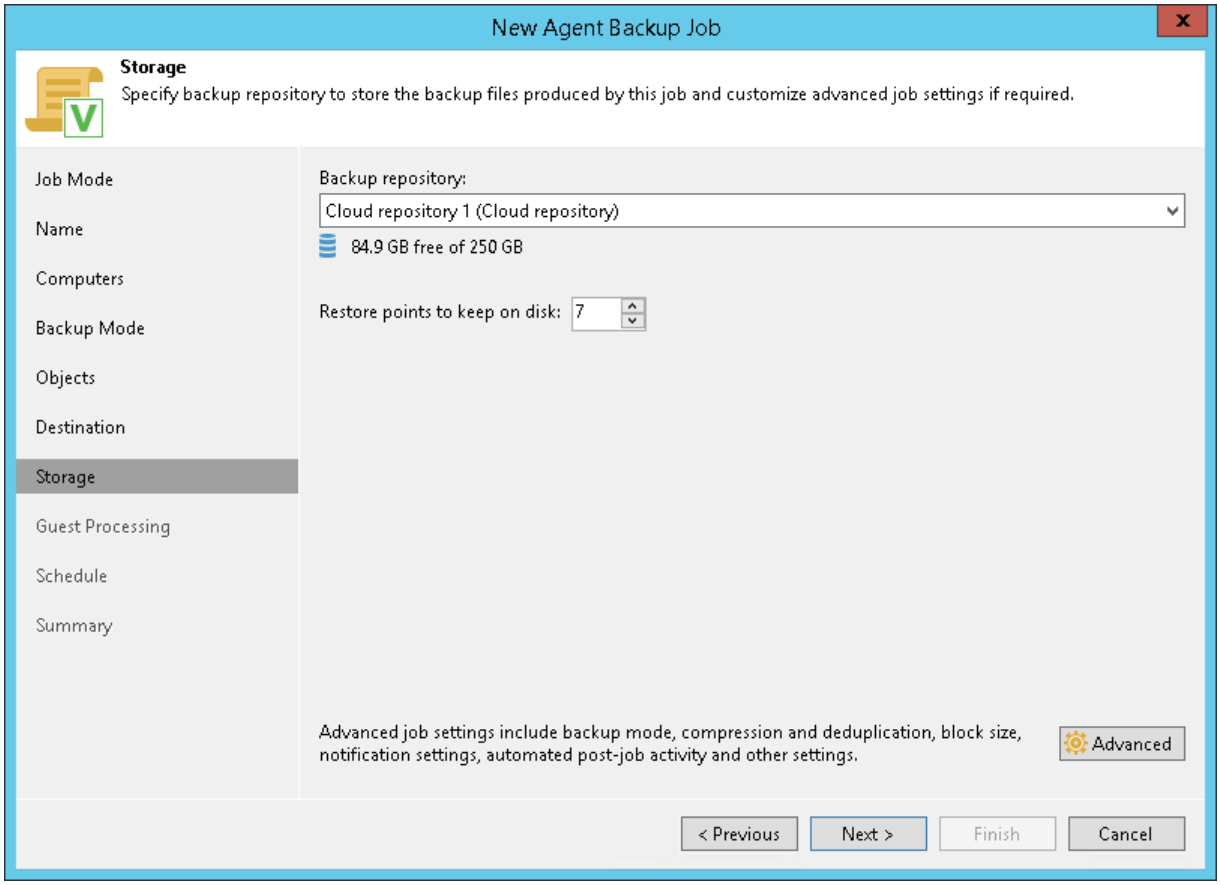
> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

Specify settings for the cloud repository:

1. From the **Backup repository** list, select a cloud repository where you want to store created backups. The **Backup repository** list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication automatically checks how much free space is available on the repository.

2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

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



Step 9. Specify Advanced Backup Settings

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

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings
- [For Veeam Agent jobs managed by the backup server] Script settings

> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup job, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Backup Settings

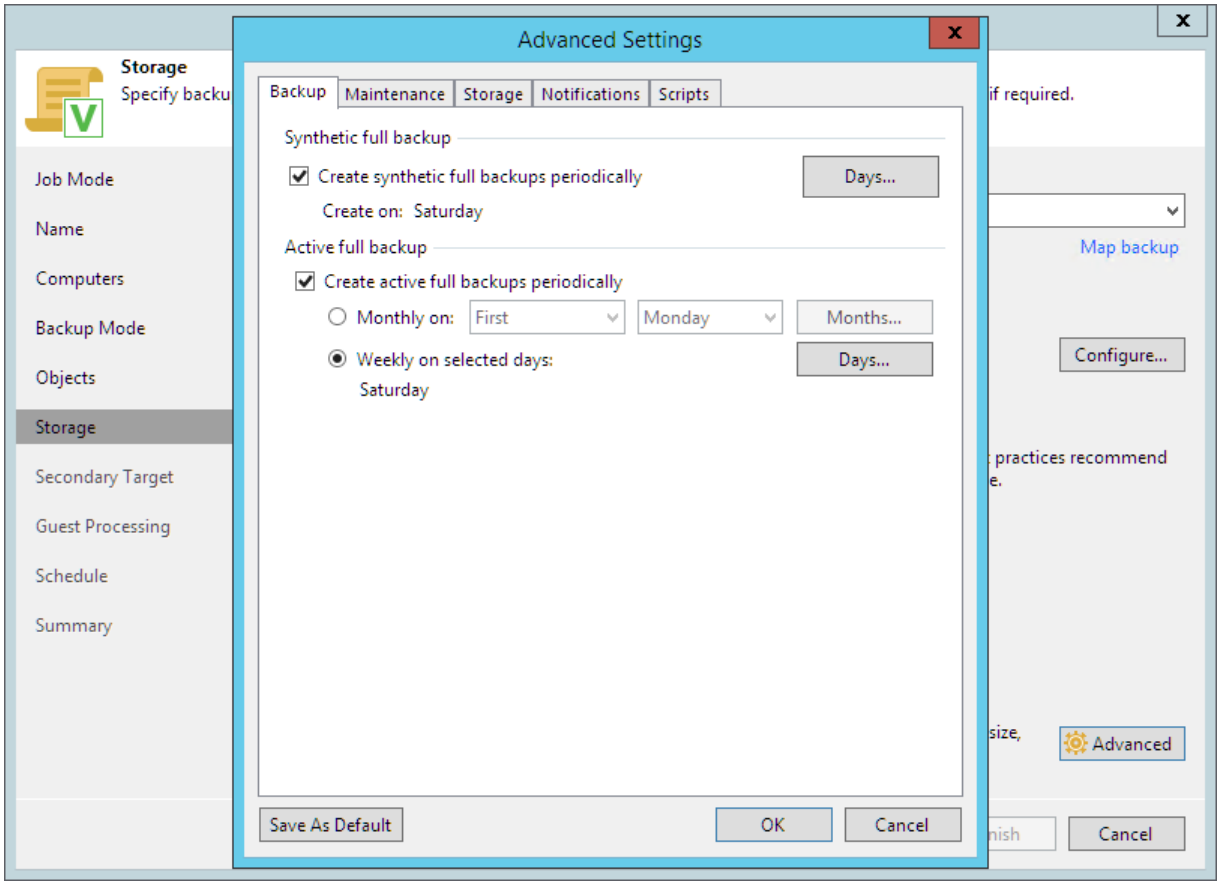
To specify settings for a backup chain created with the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. [For Veeam Agent jobs managed by the backup server] If you want to periodically create synthetic full backups, on the **Backup** tab, select the **Create synthetic full backups periodically** check box and click **Days** to schedule synthetic full backups on the necessary week days.
3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

NOTE

Consider the following:

- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.
- If you schedule the active full backup and synthetic full backup on the same day, Veeam Backup & Replication will perform only active full backup. Synthetic full backup will be skipped.



Maintenance Settings

You can specify maintenance settings for a backup chain created with the Veeam Agent backup job. Maintenance operations help make sure that the backup chain remains valid and consistent.

Maintenance settings are available for the following types of Veeam Agent backup jobs that process Linux computers:

- Backup job managed by the backup server.
- Backup job managed by Veeam Agent (backup policy). For backup jobs of this type, maintenance settings are available only if the job is targeted at a Veeam backup repository.

To specify maintenance settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. [For backup jobs managed by the backup server] To periodically perform a health check for the latest restore point in the backup chain, in the **Storage-level corruption guard** section select the **Perform backup files health check** check box and specify the time schedule for the health check.

   An automatic health check can help you avoid a situation where a restore point gets corrupted, making all dependent restore points corrupted, too. If during the health check Veeam Backup & Replication detects corrupted data blocks in the latest restore point in the backup chain (or the restore point before the latest one if the latest restore point is incomplete), it will start the health check retry and transport valid data blocks from the protected computer to the Veeam backup repository. The transported data blocks are stored to a new backup file or the latest backup file in the backup chain, depending on the data corruption scenario. For more information, see the Health Check for Backup Files section in the Veeam Backup & Replication User Guide.
4. Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup job in the target location.

   - For backup jobs managed by the backup server, deleted items retention policy is similar to retention policy for deleted VMs. After you remove a protection group or individual computer from a Veeam Agent backup job, Veeam Backup & Replication will keep its data on the backup repository for the period that you have specified. When this period is over, backup data of this computer will be removed from the backup repository. For more information, see the Retention Policy for Deleted VMs section in the Veeam Backup & Replication User Guide.
   - For backup jobs managed by Veeam Agent, if Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location. For more information, see the Veeam Agent for Linux User Guide.

   By default, the deleted items data retention period is 30 days. Do not set the deleted items retention period to 1 day or a similar short interval. In the opposite case, the backup job may work not as expected and remove data that you still require.
5. [For backup jobs managed by the backup server] To periodically compact a full backup, select the **Defragment and compact full backup file** check box and specify the schedule for the compact operation.

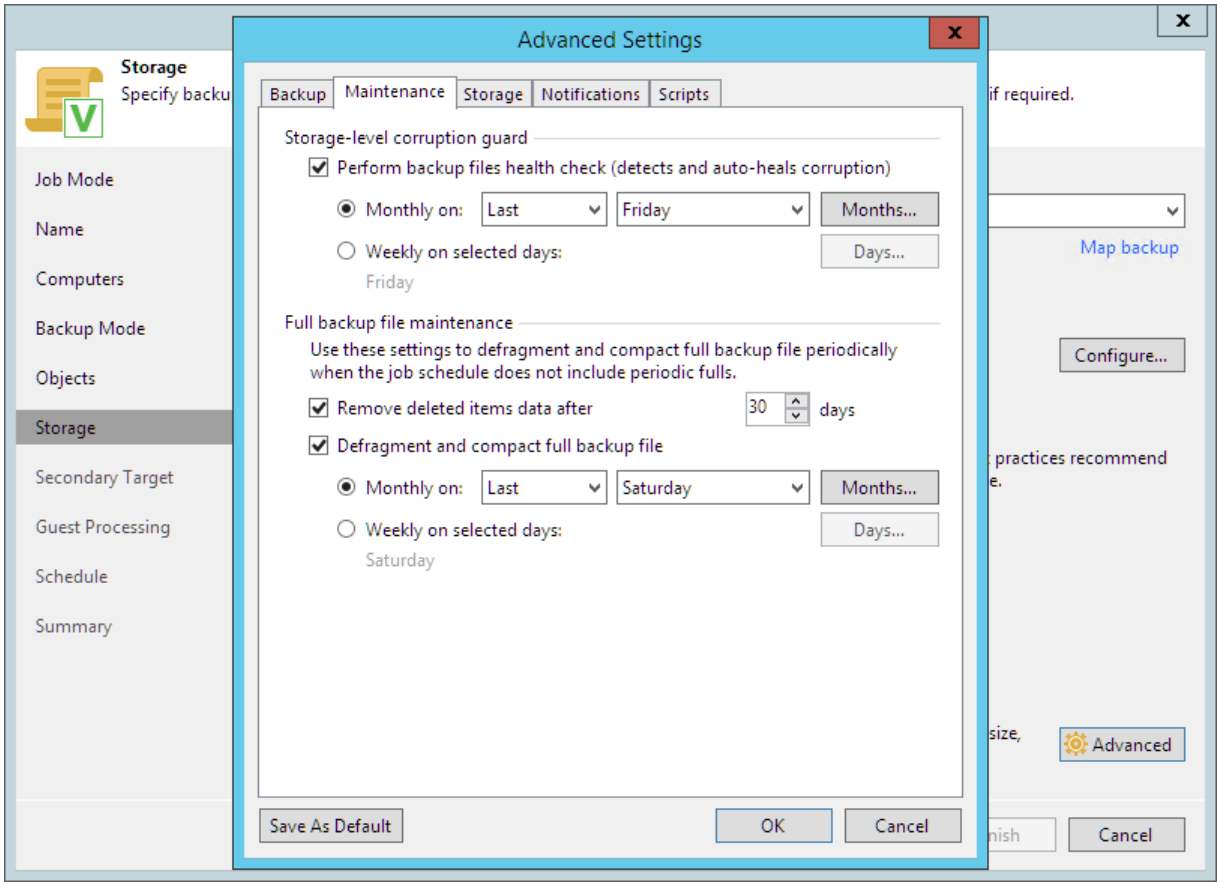
   During the compact operation, Veeam Backup & Replication creates a new empty file and copies to it data blocks from the full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from/to the backup file increases.

   If the full backup file contains data blocks for deleted items (protection groups or individual computers), Veeam Backup & Replication will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Backup & Replication User Guide.

NOTE

Consider the following:

- If you want to periodically compact a full backup, you must make sure that you have enough free space in the target location. For the compact operation, the amount of free space must be equal to or more that the size of the full backup file.
- In contrast to the compact operation for a VM backup, during compact of a full Veeam Agent backup file, Veeam Backup & Replication does not perform the data take out operation. If the full backup file contains data for a machine that has only one restore point and this restore point is older than 7 days, Veeam Backup & Replication will not extract data for this machine to a separate full backup file.

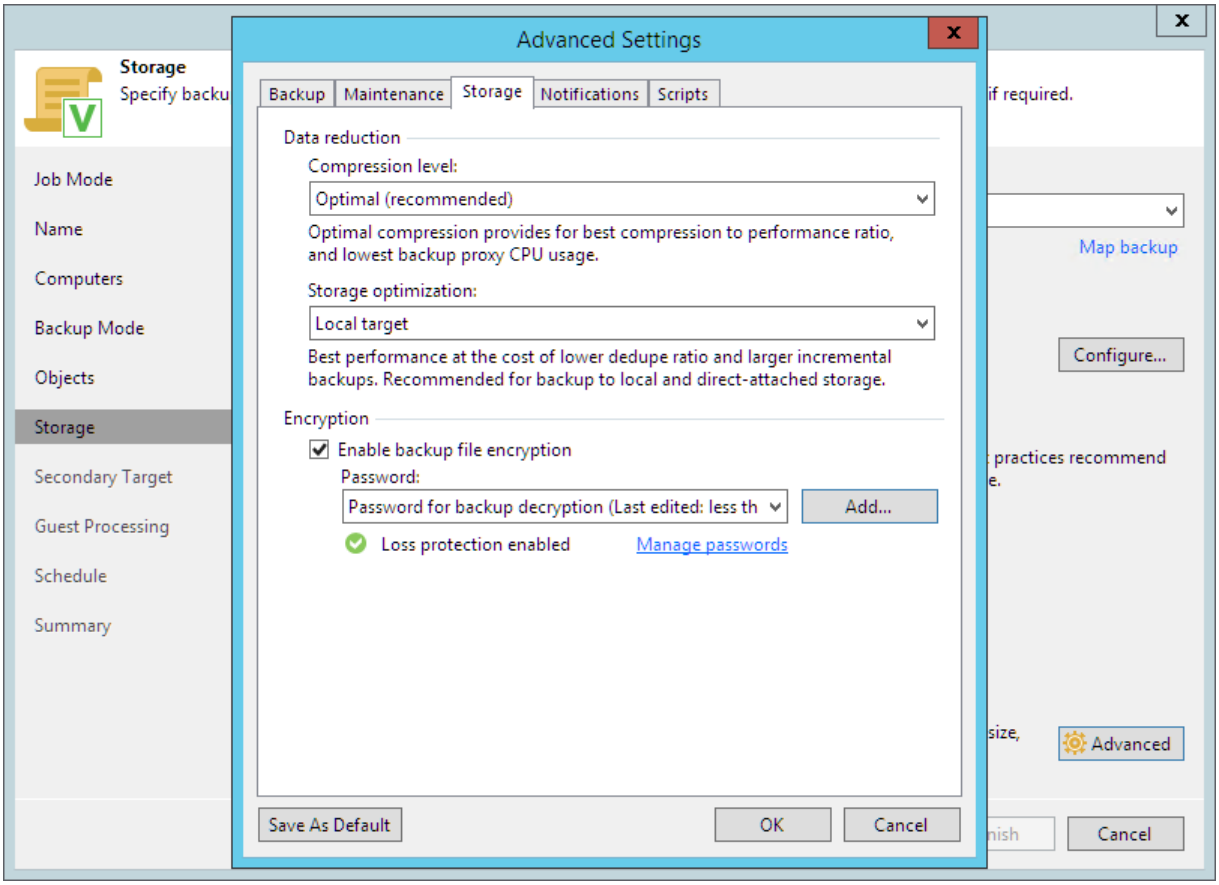


Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Storage** tab.
3. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
4. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Agent for Linux will use data blocks of different size to optimize the size of backup files and job performance.
5. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see the Password Manager section in the Veeam Backup & Replication User Guide.

   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.



NOTE

Consider the following:

- Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer or at a network shared folder. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.
- If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.
- If you enable encryption for an existing Veeam Agent backup, during the next job session Veeam Agent for Linux will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.
- Encryption is not retroactive. If you enable encryption for an existing backup job, Veeam Agent for Linux will encrypt the backup chain starting from the next restore point created with this job.
- [For backup policies targeted at a local drive, network shared folder or cloud repository] When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

  This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.

Notification Settings

You can specify notification settings for Veeam Agent backup jobs configured in Veeam Backup & Replication. Notification options differ depending on the job mode that you have selected at the Job Mode step of the wizard:

- **Managed by backup server**. To learn more, see Notification Settings for Veeam Agent Backup Job.
- **Managed by agent**. To learn more, see Notification Settings for Backup Policy.

Notification Settings for Veeam Agent Backup Job

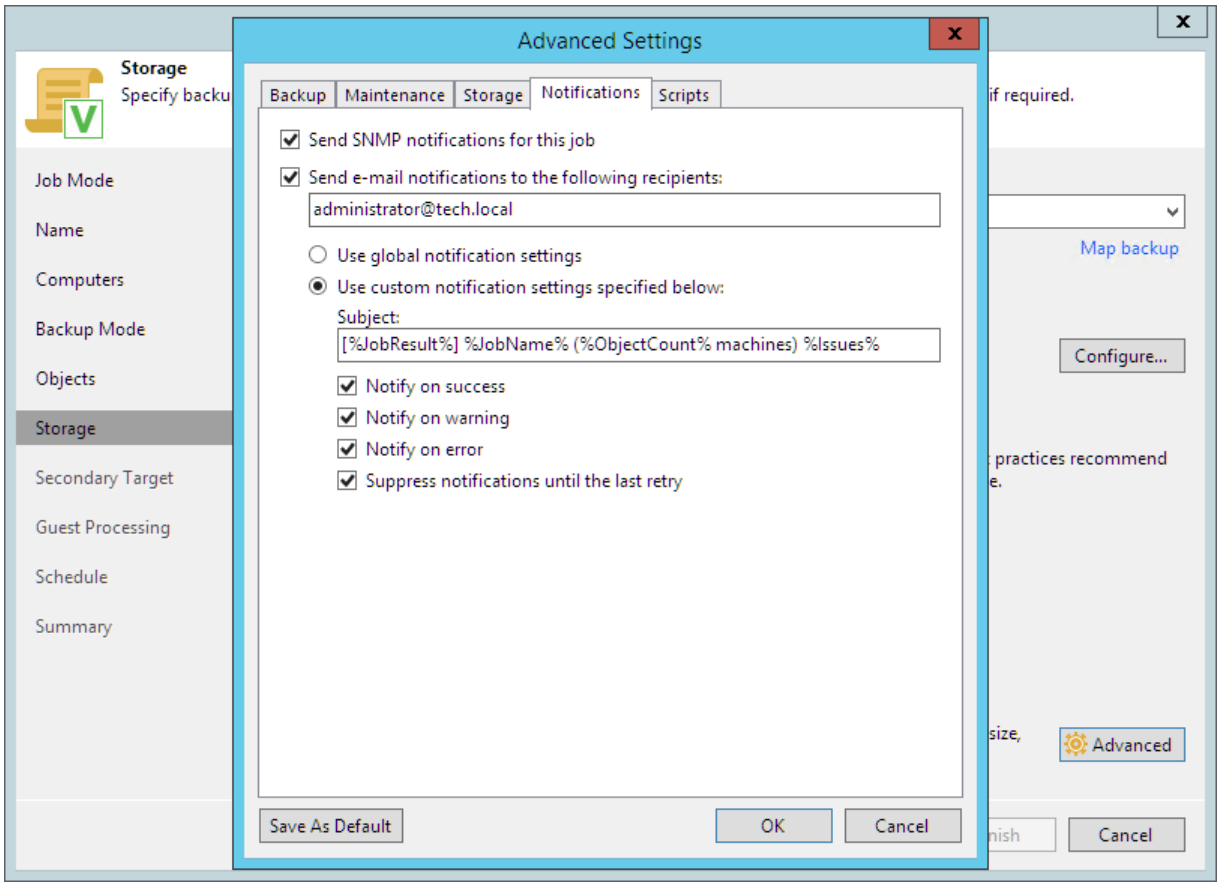
To specify notification settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

   SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

   Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

5. You can choose to use global notification settings or specify custom notification settings.
    - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server.
    - To configure a custom notification for the job, select **Use custom notification settings specified below**. You can specify the following notification settings:
        - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the *Warning* or *Failed* status).
        - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.
        - Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.



Notification Settings for Backup Policy

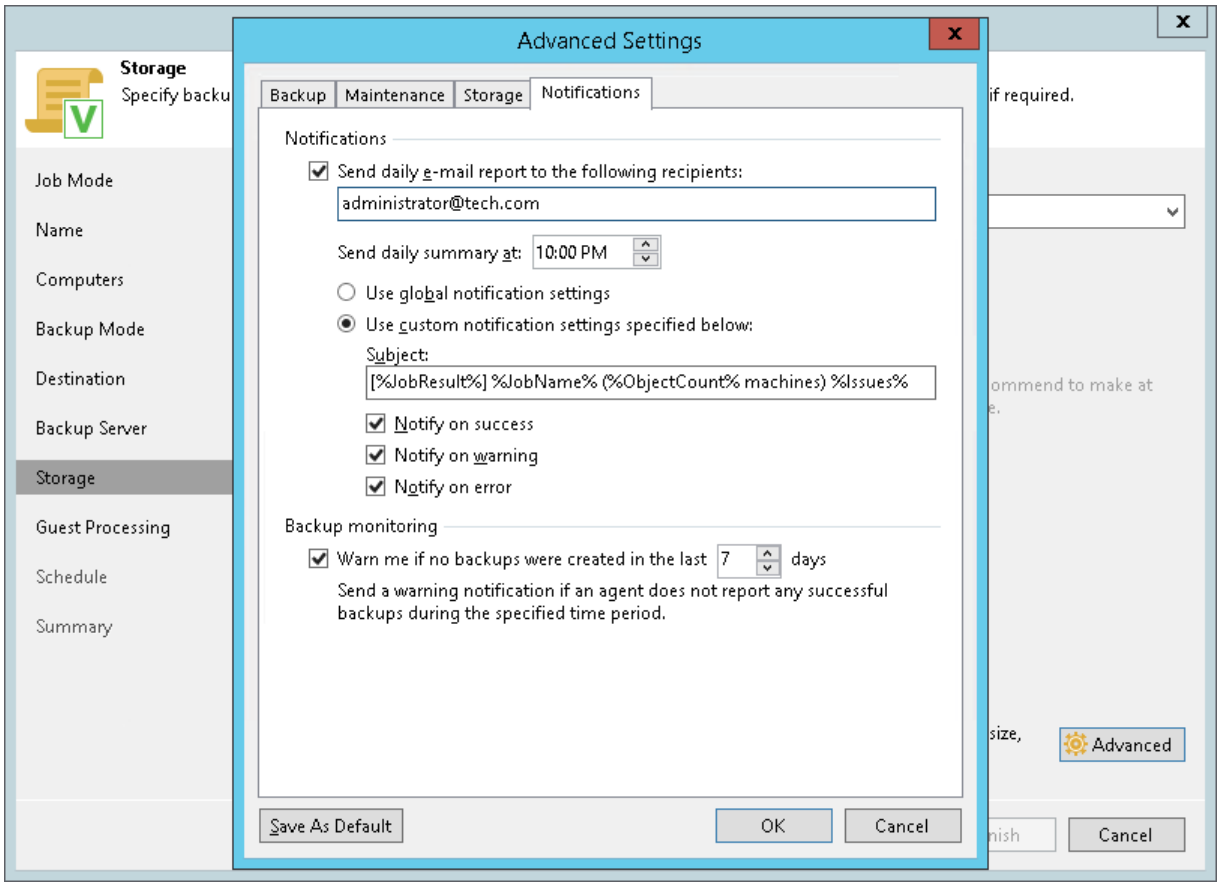
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

> **NOTE**
>
> Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the backup policy, Veeam Backup & Replication will send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will sent the report daily at the specified time.
5. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing backup policy statistics at 8:00 AM daily.
   - To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the backup policy) and *%Issues%* (number of machines in the backup policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Script Settings

You can specify what scripts Veeam Backup & Replication will execute on the backup server before and after the backup job session. This option is available if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

To specify script settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before and/or after the backup job, select the **Before the job** and **After the job** check boxes and click **Browse** to choose executable files from a local folder on the backup server. The scripts are executed on the backup server under the account under which the Veeam Backup Service runs (the local System account or account that has the local Administrator permissions on the backup server).

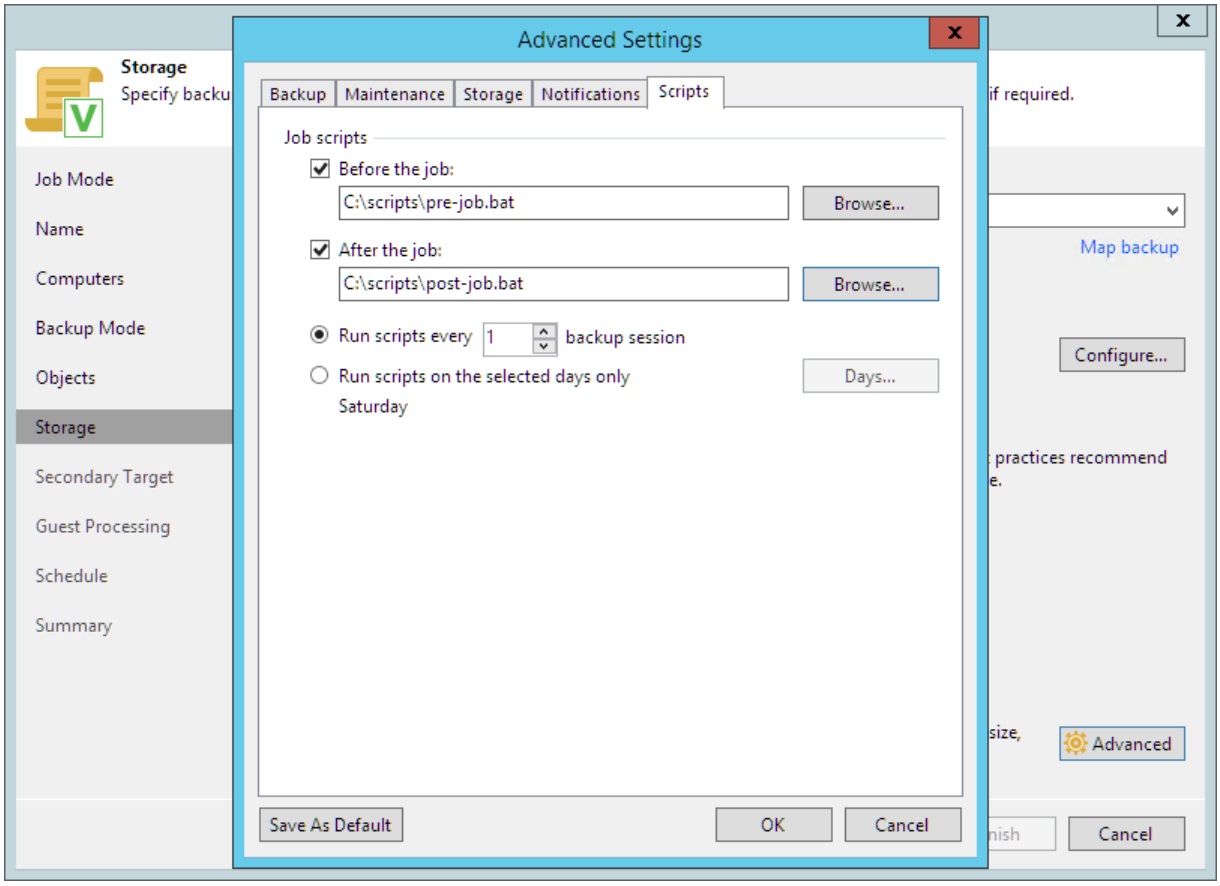
   You can select to execute pre- and post-backup actions after a number of backup sessions or on specific week days.

   - If you select the **Run scripts every <N> backup session** option, specify the number of the backup job sessions after which the scripts must be executed.
   - If you select the **Run scripts on the selected days only** option, click **Days** and specify week days on which the scripts must be executed.

TIP

Consider the following:

- Custom scripts that you define in the advanced job settings relate to the backup job itself, not the OS quiescence process on protected computers. To add pre-freeze and post-thaw scripts for Veeam Agent computer OS quiescence, use the Guest Processing step of the wizard.
- You can also specify what scripts will be executed on a Veeam Agent computer before and/or after the backup job session. To learn more, see Backup Job and Snapshot Scripts.



Step 10. Specify Secondary Target

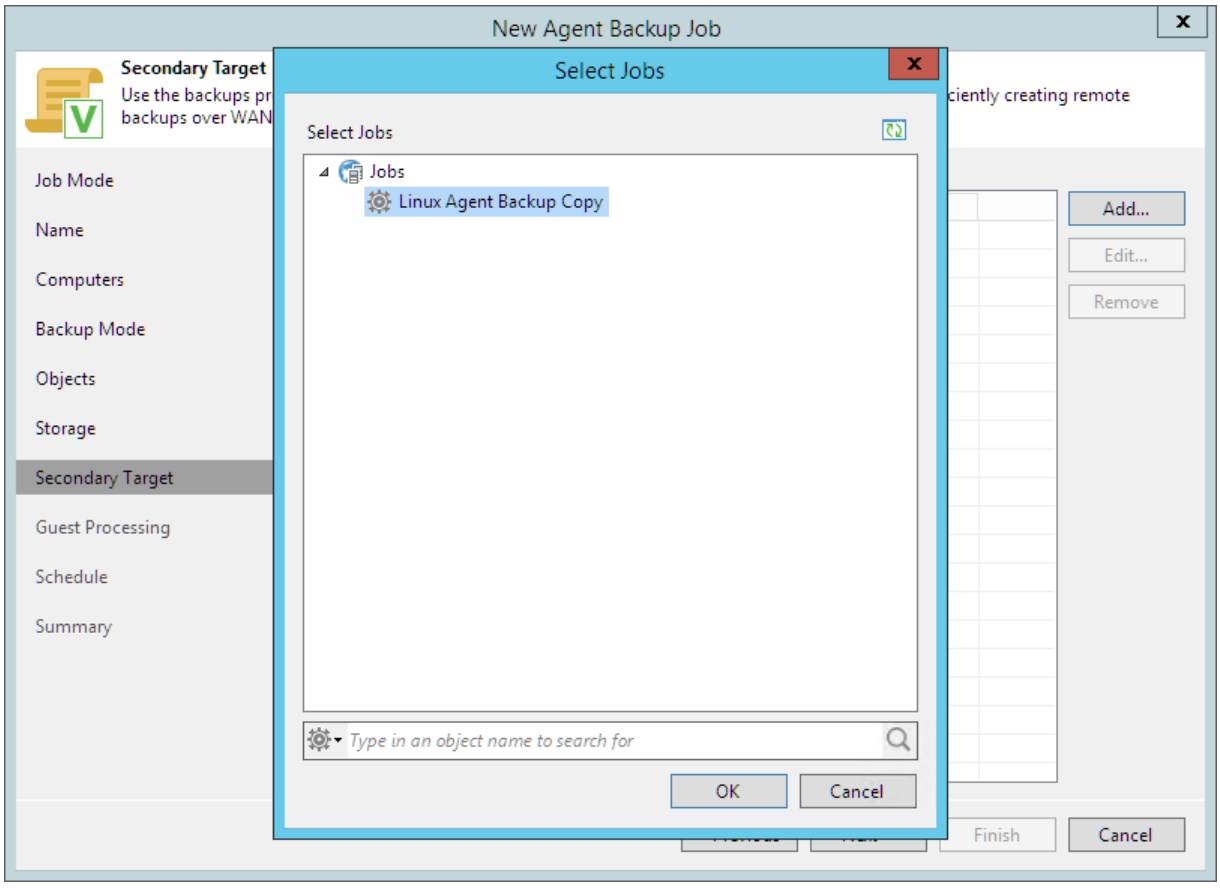
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup job to a backup to tape or backup copy job. As a result, the backup job will be added as a source to the backup to tape or backup copy job. Backup files created with the backup job will be archived to tape or copied to the secondary backup repository according to the secondary jobs schedule. For more information, see Linking Backup Jobs to Backup Copy Jobs and Linking Backup Jobs to Backup to Tape Jobs in the Veeam Backup & Replication User Guide.

The backup to tape job or backup copy job must be configured beforehand. You can create these jobs with an empty source. When you link the Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent backup job as a source for these jobs.

To link jobs:

1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom of the wizard.



Step 11. Specify Guest Processing Settings

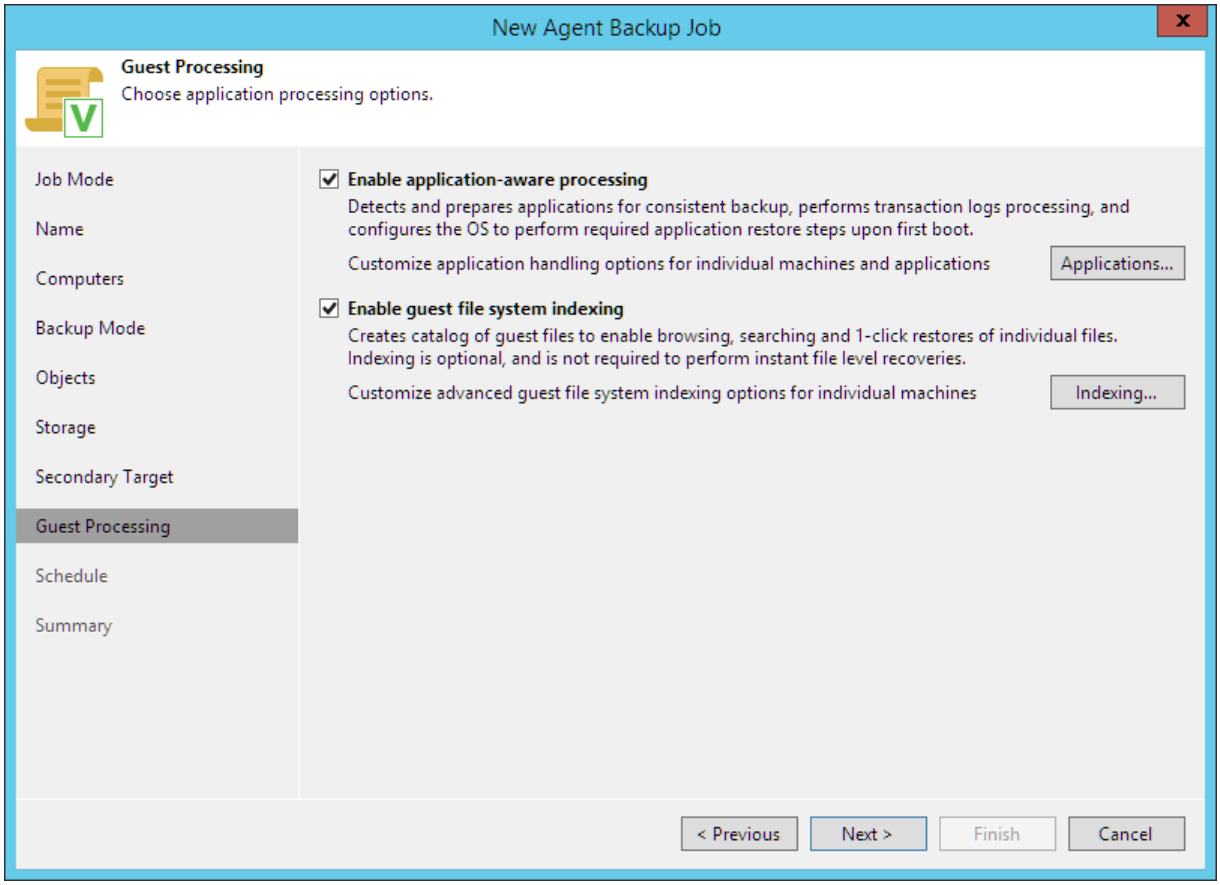
At the **Guest Processing** step of the wizard, you can enable the following guest OS processing settings for a Veeam Agent backup job that includes Linux-based computers:

- Application-aware processing
- Processing of Oracle databases
- Processing of MySQL databases
- Processing of PostgreSQL databases
- Use of backup job and snapshot scripts
- File indexing

NOTE

Consider the following:

- Application-aware processing and database processing options are available if you have selected the **Server** option at the Job Mode step of the wizard.
- Application-aware processing and database processing options are available if you have selected the **Entire computer** or **Volume level backup** option at the Backup Mode step of the wizard.
- Available script settings depend on the options that you have selected at the Job Mode and Backup Mode steps of the wizard. To learn more, see Backup Job and Snapshot Scripts.
- Veeam Agent for Linux does not support processing of multiple database systems on one Veeam Agent computer.



Application-Aware Processing

If a computer protected with Veeam Agent for Linux runs an Oracle, MySQL or PostgreSQL database system, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of databases without data loss.

To enable application-aware processing:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.

4. On the **General** tab, in the **Applications** section, specify the behavior scenario for application-aware processing:

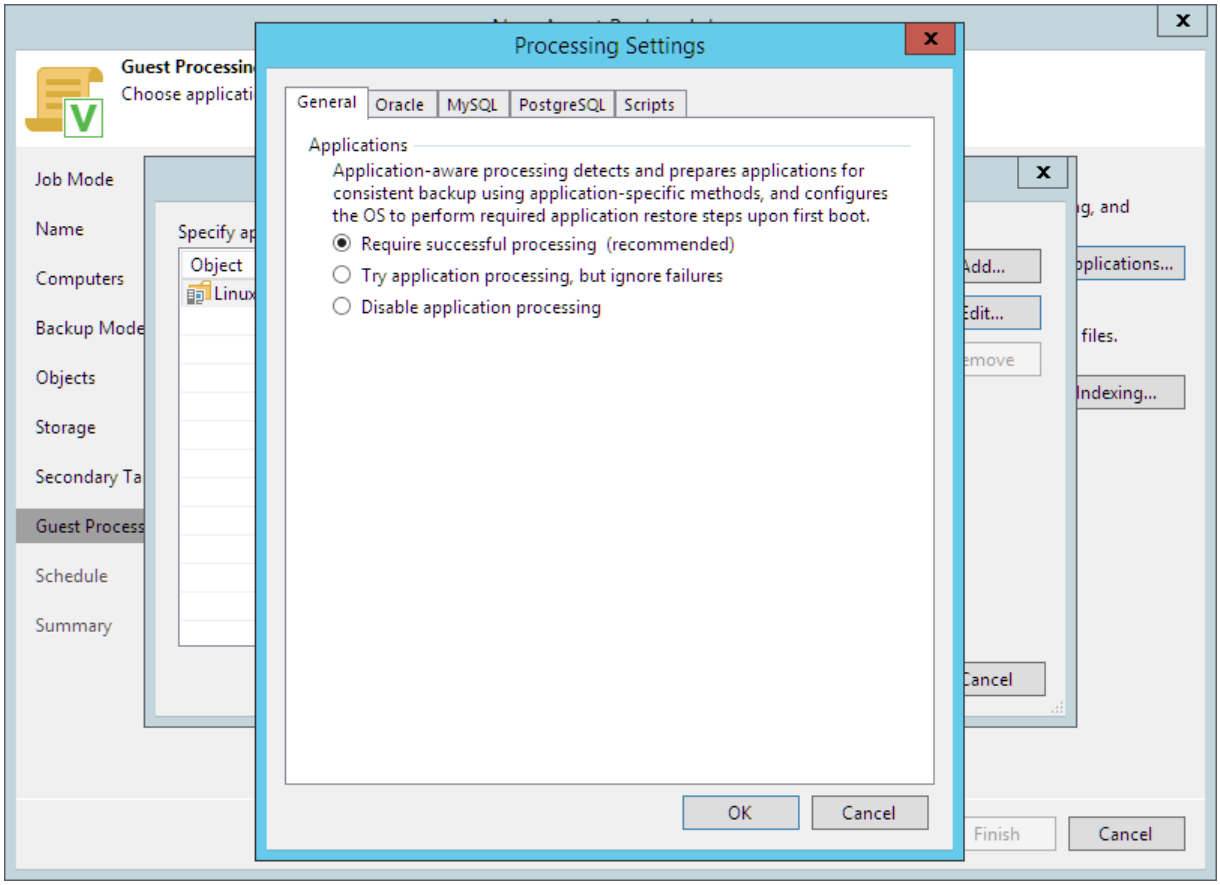
   - Select **Require successful processing** if you want Veeam Agent for Linux to process databases. With this option selected, if an error occurs when processing a database, Veeam Agent for Linux will stop the backup process.

     If you select this option, you will need to specify database processing settings. For more information, see Oracle Processing Settings, MySQL Processing Settings and PostgreSQL Processing Settings.

   - Select **Try application processing, but ignore failures** if you want Veeam Agent for Linux to process databases. With this option selected, if an error occurs when processing a database, Veeam Agent for Linux will not stop the backup process. Instead, Veeam Agent for Linux will skip this database and proceed to the next one. Information about the skipped database will be displayed in a warning message in the job session statistics. After the backup process completes, you will be able to restore data from the backup and restore databases that were successfully processed during backup.

     If you select this option, you will need to specify database processing settings. For more information, see Oracle Processing Settings, MySQL Processing Settings and PostgreSQL Processing Settings.

   - Select **Disable application processing** if you do not want Veeam Agent for Linux to process databases. If you select this option, the **Oracle**, **MySQL** and **PostgreSQL** tabs of the **Processing Settings** window will become unavailable. You will be able to specify script settings for the job on the **Scripts** tab of the window.



Oracle Processing Settings

If you back up an Oracle database, you can specify how Veeam Agent for Linux must process archived logs:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

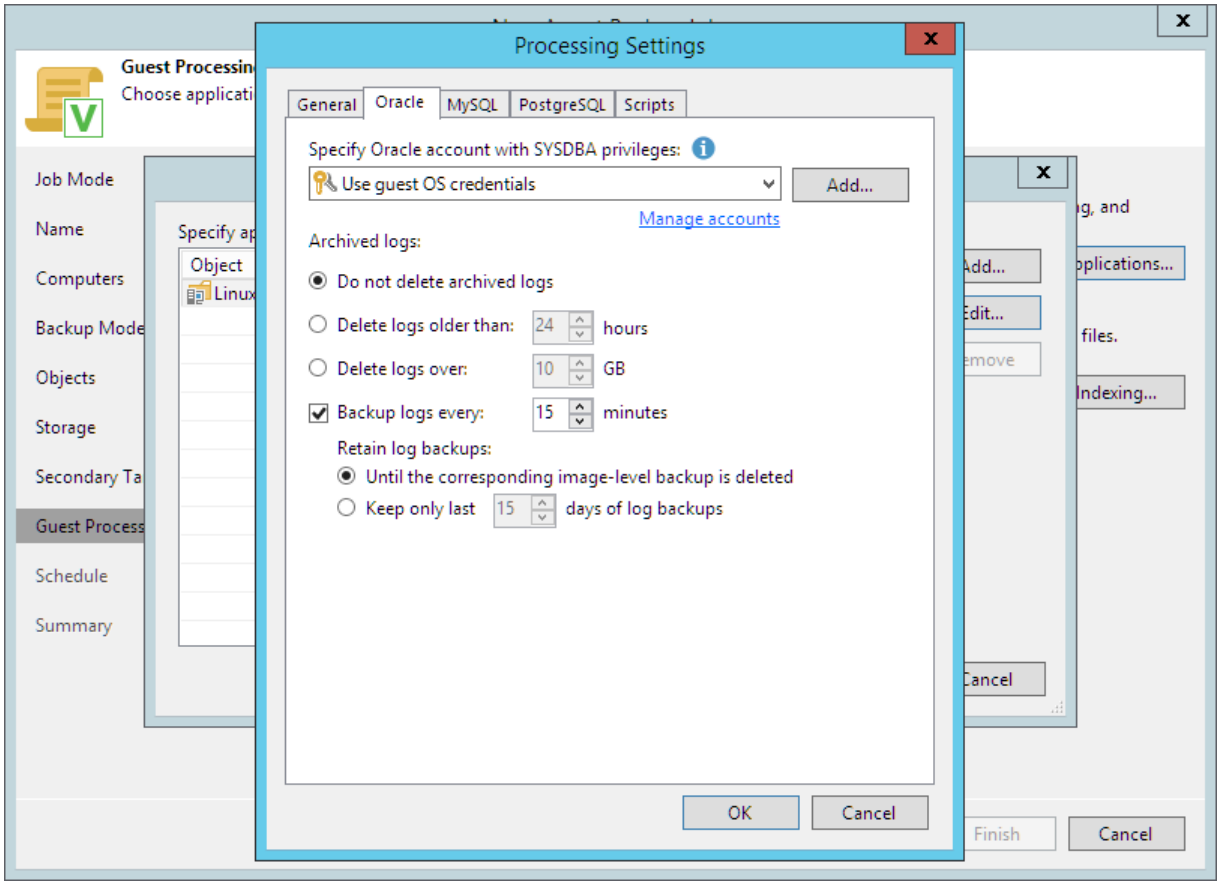
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, select **Require successful processing** or **Try application processing, but ignore failures**.
5. In the **Processing Settings** window, click the **Oracle** tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the Oracle database, select from the **Specify Oracle account with SYSDBA privileges** list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Linux will connect to the Oracle database under the account that you have specified for the protected computer in the protection group settings.

   > **NOTE**
   >
   > Veeam Agent for Linux always uses the root account to connect to the Oracle database. This includes the following cases:
   >
   > - An Oracle account with the SYSDBA rights is selected in the **Specify Oracle account with SYSDBA privileges** list, and the database is set to use database authentication.
   > - A non-root OS account added to the group that owns configuration files for the Oracle database (for example, the oinstall group) is selected in the **Specify Oracle account with SYSDBA privileges** list, and the database is set to use authentication by the operating system.
   >
   > Thus, to perform database processing successfully, the root account must always have privileges to connect to the Oracle database system.
7. In the **Archived logs** section, specify if Veeam Agent for Linux must delete archived logs on the Oracle database:
   - Select **Do not delete archived logs** if you want Veeam Agent for Linux to preserve archived logs. When the backup job completes, Veeam Agent for Linux will not delete archived logs.

     It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.
   - Select **Delete logs older than <N> hours** or **Delete logs over <N> GB** if you want Veeam Agent for Linux to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent for Linux will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.

8. [For Veeam Agent jobs managed by the backup server] To back up Oracle archived logs with Veeam Agent for Linux, select the **Backup log every <N> minutes** check box and specify the frequency for archived logs backup. By default, archived logs are backed up every 15 minutes. The minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.
9. [For Veeam Agent jobs managed by the backup server] In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for Veeam Agent backups and archived log backups.
   - Select **Keep only last <n> days** to keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the Veeam Agent backups. The maximum time period to keep archived logs is 60 days.



MySQL Processing Settings

You can specify how Veeam Agent for Linux must process a MySQL database:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

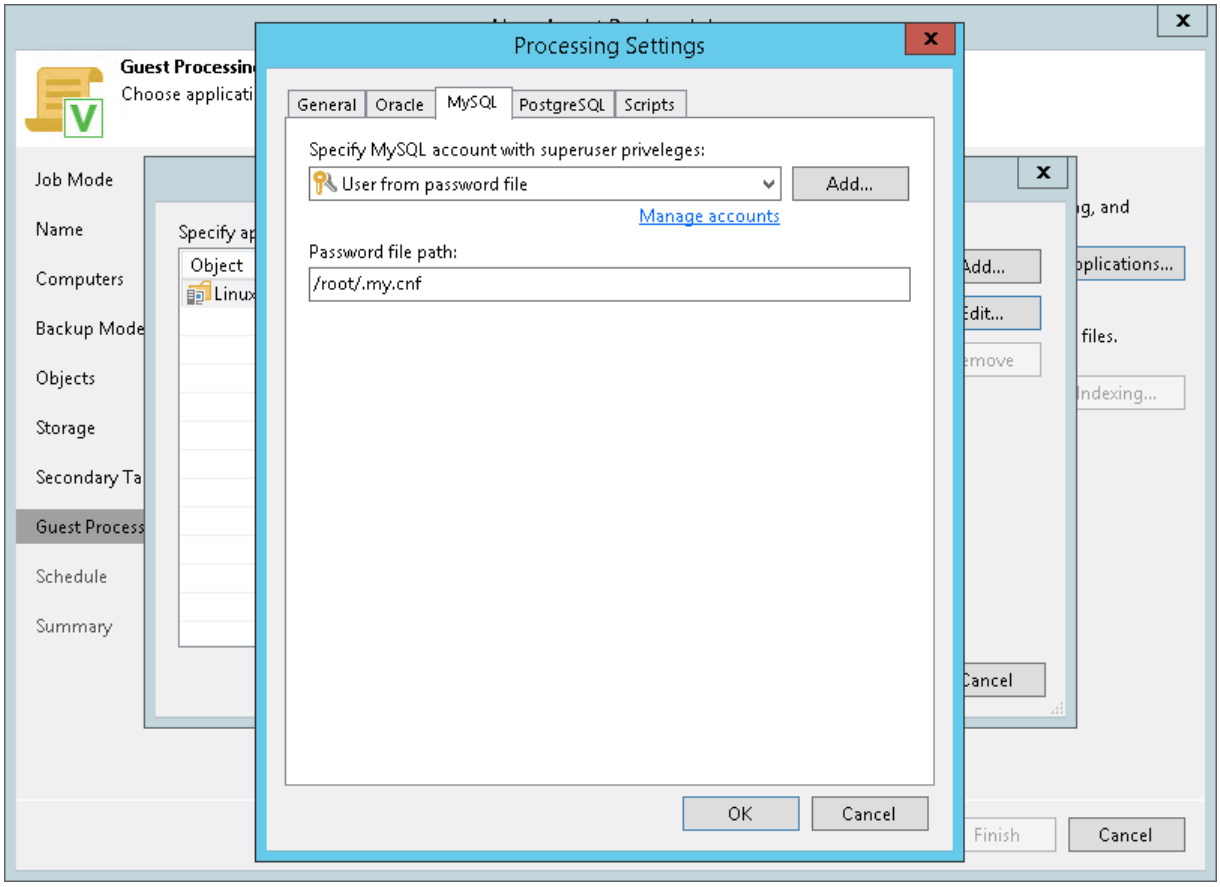
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, select **Require successful processing** or **Try application processing, but ignore failures**.
5. In the **Processing Settings** window, click the **MySQL** tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the MySQL database, from the **Specify MySQL account with superuser privileges** list, select a user account that has the following privileges on the database:
   - SELECT for all tables. If the account does not have the SELECT privilege for the table, Veeam Agent will not be able to access the table metadata. Thus, Veeam Agent will not process the table. To learn more, see MySQL documentation.
   - LOCK TABLES. If the account does not have this privilege, Veeam Agent will not process tables based on the MyISAM storage engine.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   By default, the **User from password file** option is selected in the list. With this option selected, Veeam Agent for Linux will connect to the MySQL database under the account specified in the password file on the Veeam Agent computer. The default location for the password file is `/root/.my.cnf`. For information about the password file format, see the Preparing Password File for MySQL Processing section in the Veeam Agent for Linux User Guide.

7. If you want to specify a custom path to the password file, specify a full path in the **Password file path** field. Specifying relative paths is not supported.

For information on how Veeam Agent for Linux processes the MySQL database system, see the MySQL Backup section in the Veeam Agent for Linux User Guide.



PostgreSQL Processing Settings

You can specify how Veeam Agent for Linux must process a PostgreSQL database:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

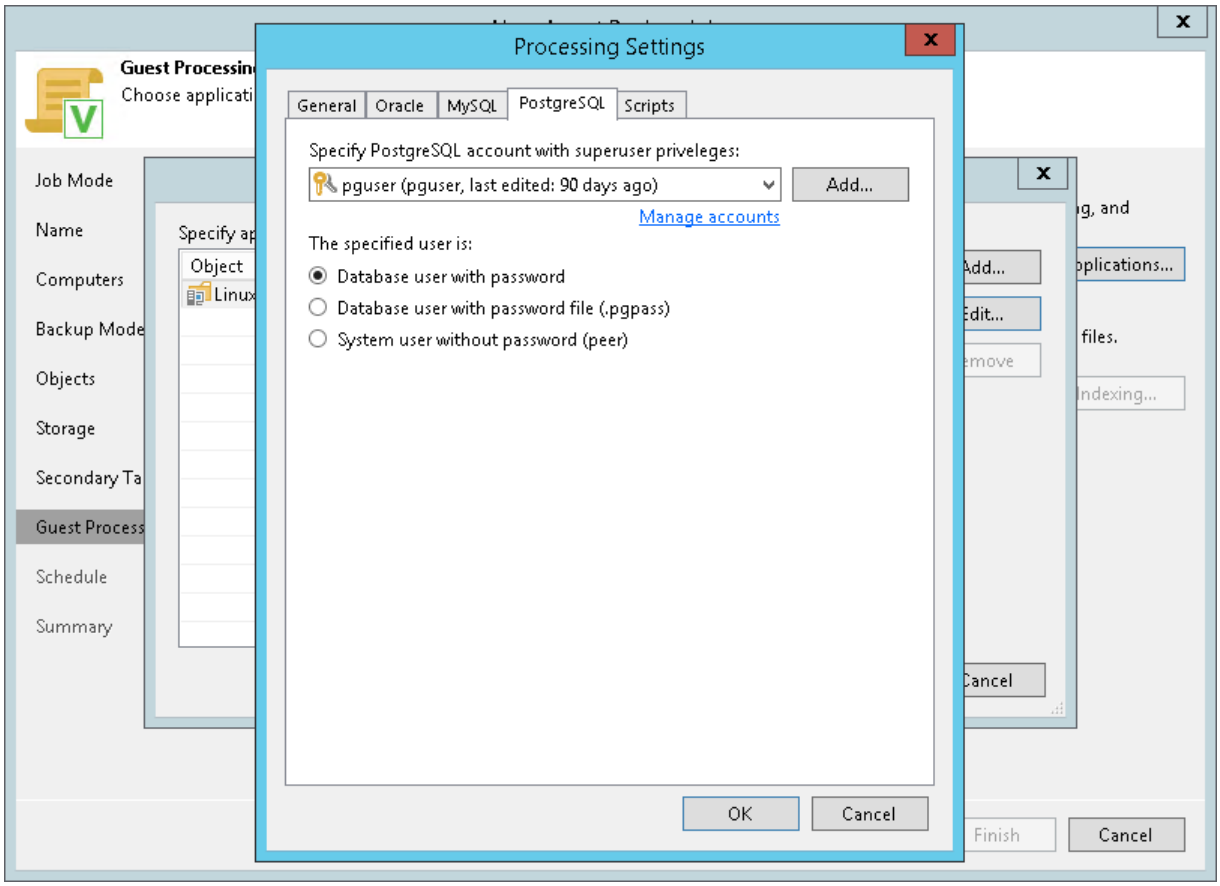
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, select **Require successful processing** or **Try application processing, but ignore failures**.
5. In the **Processing Settings** window, click the **PostgreSQL** tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the PostgreSQL database, select the account from the **Specify PostgreSQL account with superuser privileges** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

   Note that if you plan to select the peer authentication method at the step 7 of this procedure, you can add a user account in the Credentials Manager without specifying the password for the account.

   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent will connect to the PostgreSQL database under the account that you have specified for the protected computer in the protection group settings.

7. In the **The specified user is** field, specify how Veeam Agent for Linux will connect to the PostgreSQL database:
   - Select **Database user with password** if the account that you specified at the step 6 is a PostgreSQL account, and you entered the password for this account in the Credentials Manager.
   - Select **Database user with password file** if the password for the account that you specified at the step 6 is defined in the `.pgpass` configuration file on the Veeam Agent computer. For information about the `.pgpass` file format, see the Password File for PostgreSQL Processing section in the Veeam Agent for Linux User Guide.
   - Select **System user without password** if you want Veeam Agent to use the peer authentication method. In this case, Veeam Agent will apply the Veeam Agent computer OS account as the PostgreSQL account.

For more information on how Veeam Agent for Linux processes the PostgreSQL database system, see the PostgreSQL Backup section in the Veeam Agent for Linux User Guide.



Backup Job and Snapshot Scripts

You can specify custom scripts that will be executed within the backup job session on Linux computers. Veeam Agent for Linux supports the following types of scripts:

- *Backup job scripts* — pre-job and post-job scripts that run on the Veeam Agent computer before and after the backup job session.
- *Snapshot scripts* — pre-freeze and post-thaw scripts that run on the Veeam Agent computer before and after the volume snapshot is created.

To learn more, see Backup Job Scripts.

Veeam Backup & Replication offers 2 scenarios for specifying script settings:

- Scenario 1. Specify backup job scripts and snapshot scripts.

  You can specify both backup job scripts and snapshot scripts for the backup job if the following conditions are met:

  a. You selected the **Server** option at the Job Mode step of the wizard.

  b. You did not select the **Backup directly from live file system option** at the Backup Mode step of the wizard.

- Scenario 2. Specify backup job scripts only.

  In one of the following conditions, you can specify only backup job scripts that will be executed on Linux computers:

  - If you selected the **Server** option at the Job Mode step of the wizard and selected the **Backup directly from live file system** option at the Backup Mode step of the wizard.
  - If you selected the **Workstation** option at the Job Mode step of the wizard.

> **TIP**
>
> You can also specify custom scripts that will be executed on the backup server before and/or after the backup job session. To learn more, see Script Settings.

Specifying Backup Job and Snapshot Scripts

To specify custom scripts for the job:

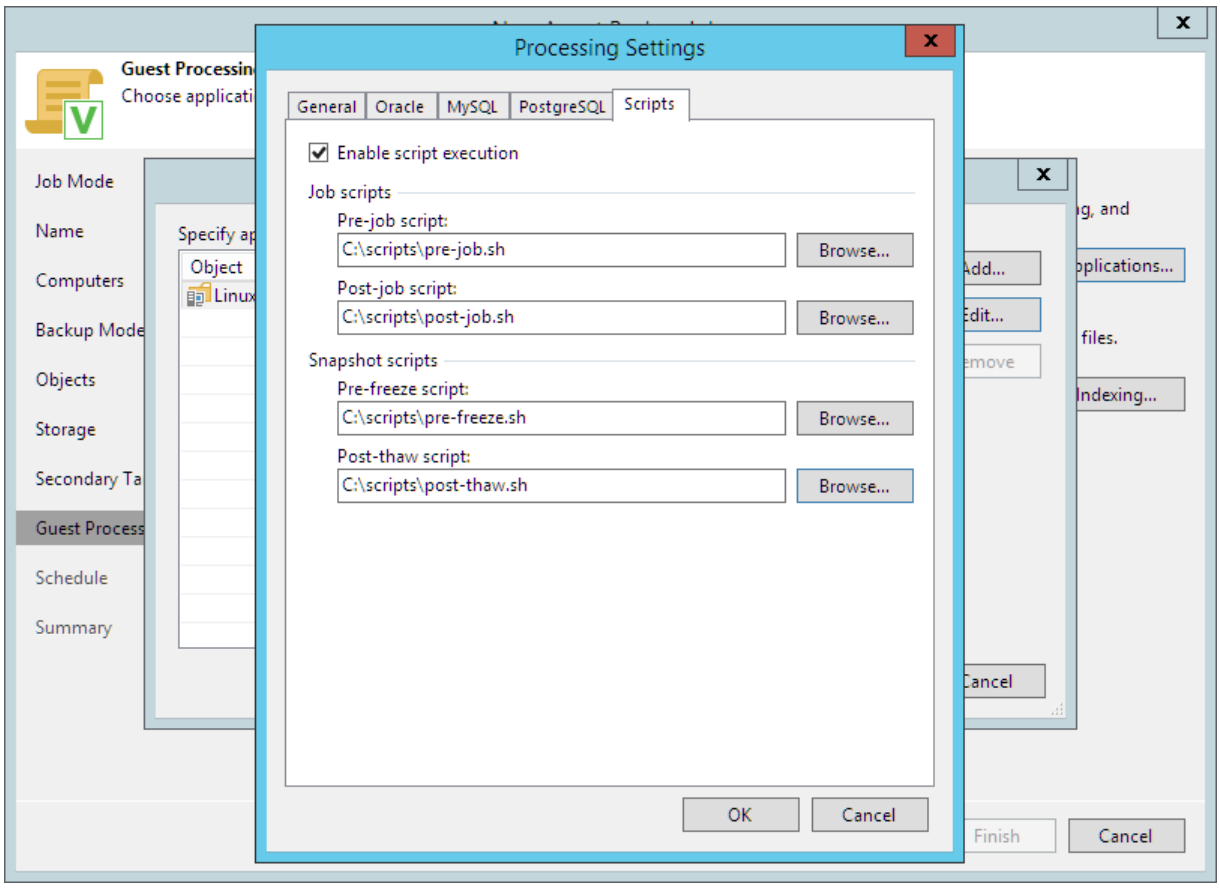
1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. [For an entire computer backup or volume-level backup job] In the **Processing Settings** window, click the **Scripts** tab.

> **NOTE**
>
> For a file-level backup job, application-aware processing and database processing options are not available, and no tabs are displayed in the **Processing Settings** window.

5. Select the **Enable script execution** check box.
6. In the **Job scripts** section, specify custom scripts that you want to execute before and/or after the backup job session. To do this, in the **Pre-job script** and **Post-job script** fields, click **Browse** and choose executable files from a local folder on the backup server.
7. In the **Snapshot scripts** section, specify custom scripts that you want to execute before Veeam Agent for Linux creates a snapshot of the backed-up volume and/or after the snapshot is created. To do this, in the **Pre-freeze script** and **Post-thaw script** fields, click **Browse** and choose executable files from a local folder on the backup server.

Veeam Agent for Linux supports scripts in the SH file format. During the backup job session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the backup job and execute them on these computers.



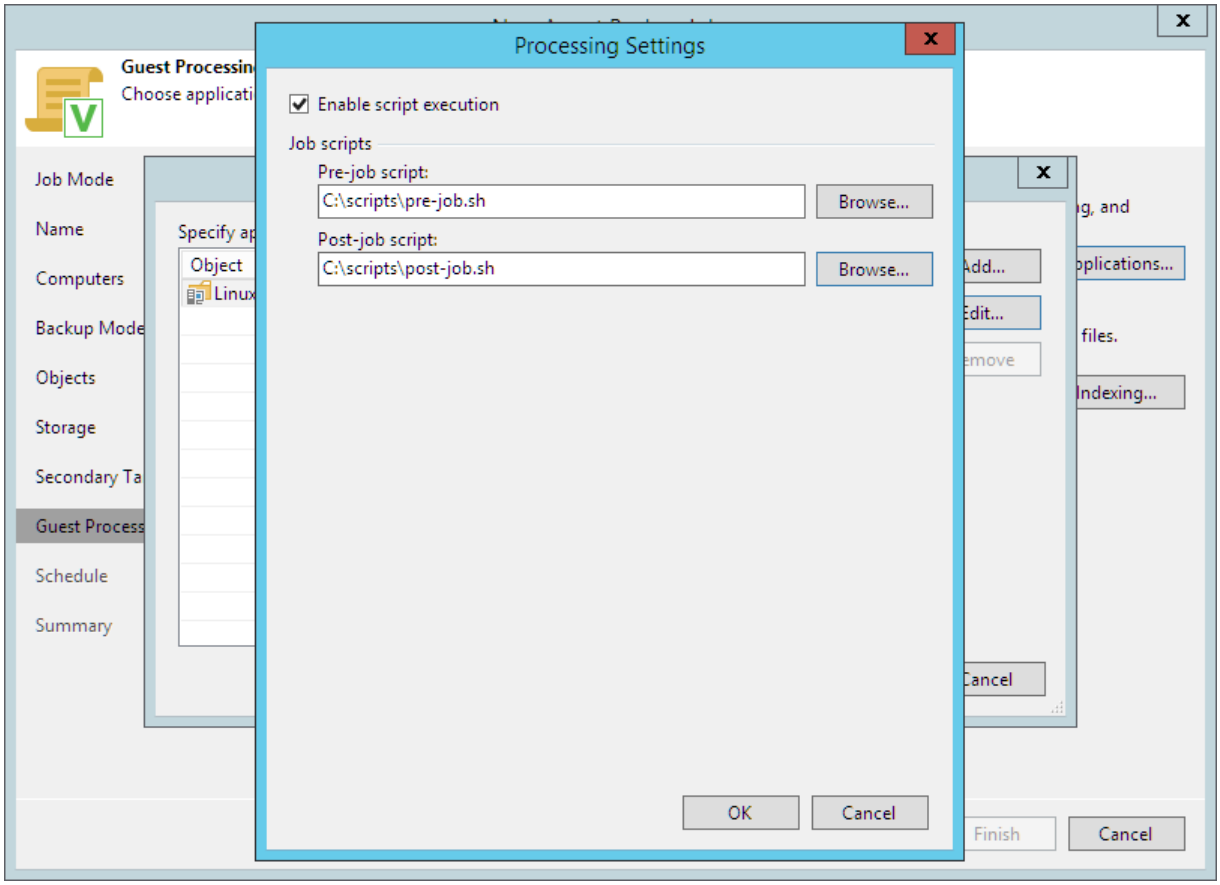
Specifying Backup Job Scripts

To specify custom scripts for the job:

1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Processing Settings** window, select the **Enable script execution** check box.
5. In the **Pre-job script** and **Post-job script** fields, click **Browse** to choose executable files from a local folder on the backup server.

Veeam Agent for Linux supports scripts in the SH file format. During the backup job session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the job and execute them on these computers.



File Indexing

To specify file indexing options:

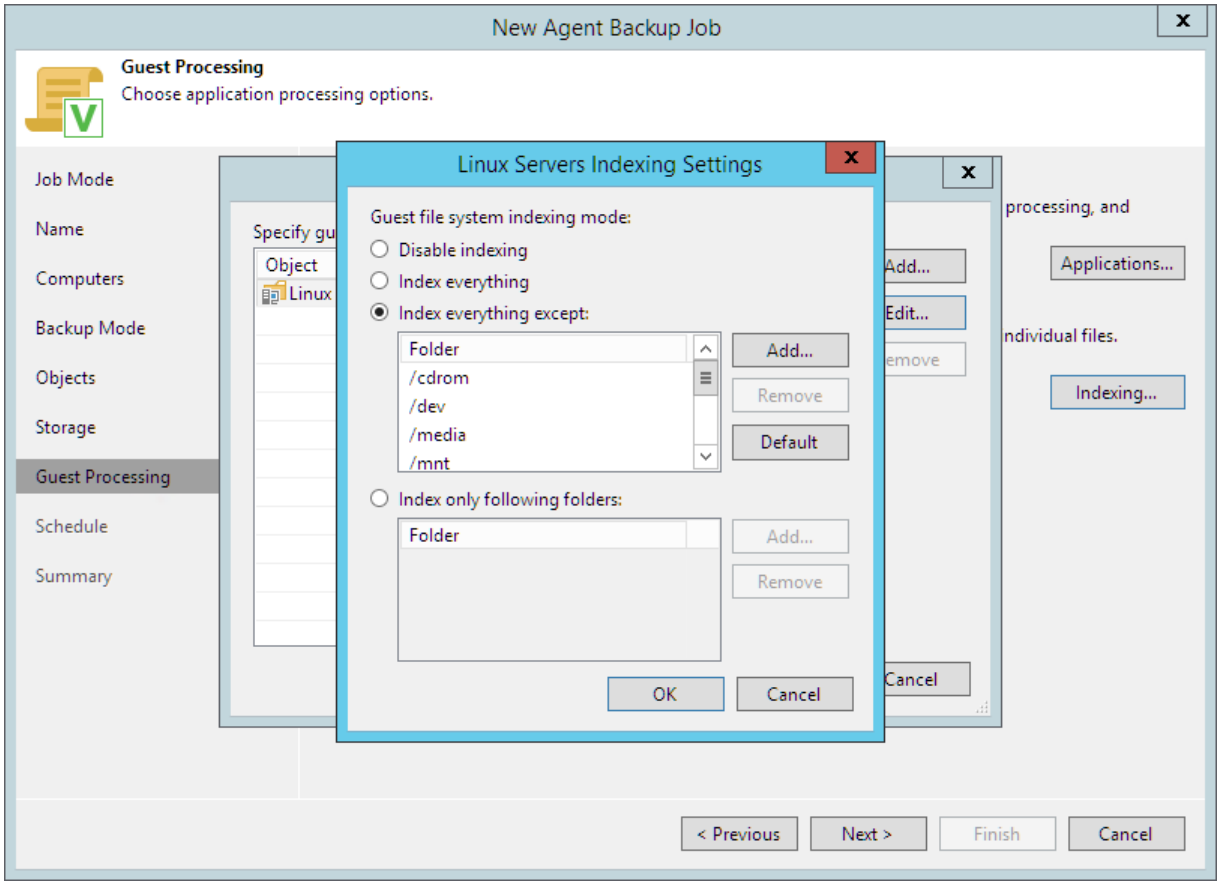
1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select the protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Indexing Settings** window, specify the indexing scope:
   - Select **Index everything** if you want to index all files within the backup scope that you have specified at the Backup mode step of the wizard. Veeam Agent for Linux will index all files that reside:
     - On the protected computer OS (for entire computer backup)
     - On the volumes that you have specified for backup (for volume-level backup)
     - In the directories that you have specified for backup (for file-level backup)
   - [For volume-level backup only] Select **Index everything except** if you want to index all files on your computer OS except those defined in the list. By default, system directories `/cdrom`, `/dev`, `/media`, `/mnt`, `/proc`, `/tmp` and `/lost+found` are excluded from indexing. You can add or delete folders using the **Add** and **Remove** buttons on the right.

     To reset the list of folders to its initial state, click **Default**.
   - [For volume-level backup only] Select **Index only following folders** to define directories that you want to index. You can add or delete directories to index using the **Add** and **Remove** buttons on the right.

NOTE

You can specify a custom indexing scope only in for a volume-level backup job. For a file-level backup job that processes Linux-based computers, only the **Index everything** option is available.



Step 12. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.
   - [For backup job managed by backup server] To define the permitted time window for the job, click **Schedule** and use the time table. In the **Start time within an hour** field, specify the exact time when the job must start.

     A repeatedly run job is started by the following rules:

     - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
     - If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

     For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.
   - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.
   - [For backup job managed by backup server] To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list.

NOTE

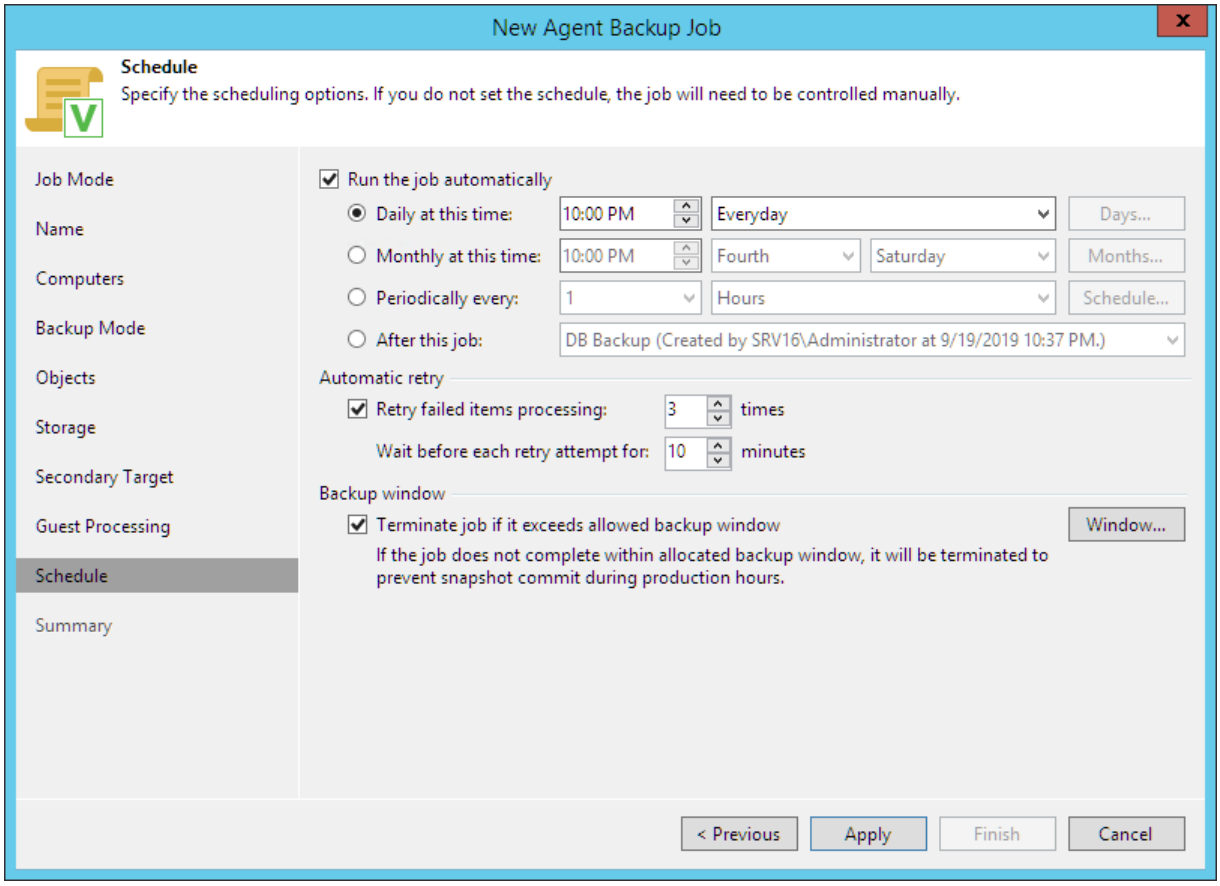
Mind the following:

- The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
- The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Agent for Linux (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Agent for Linux will retry the job for the defined number of times without any time intervals between the job runs.
4. [For backup job managed by backup server] In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:
   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.
   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

NOTE

If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.



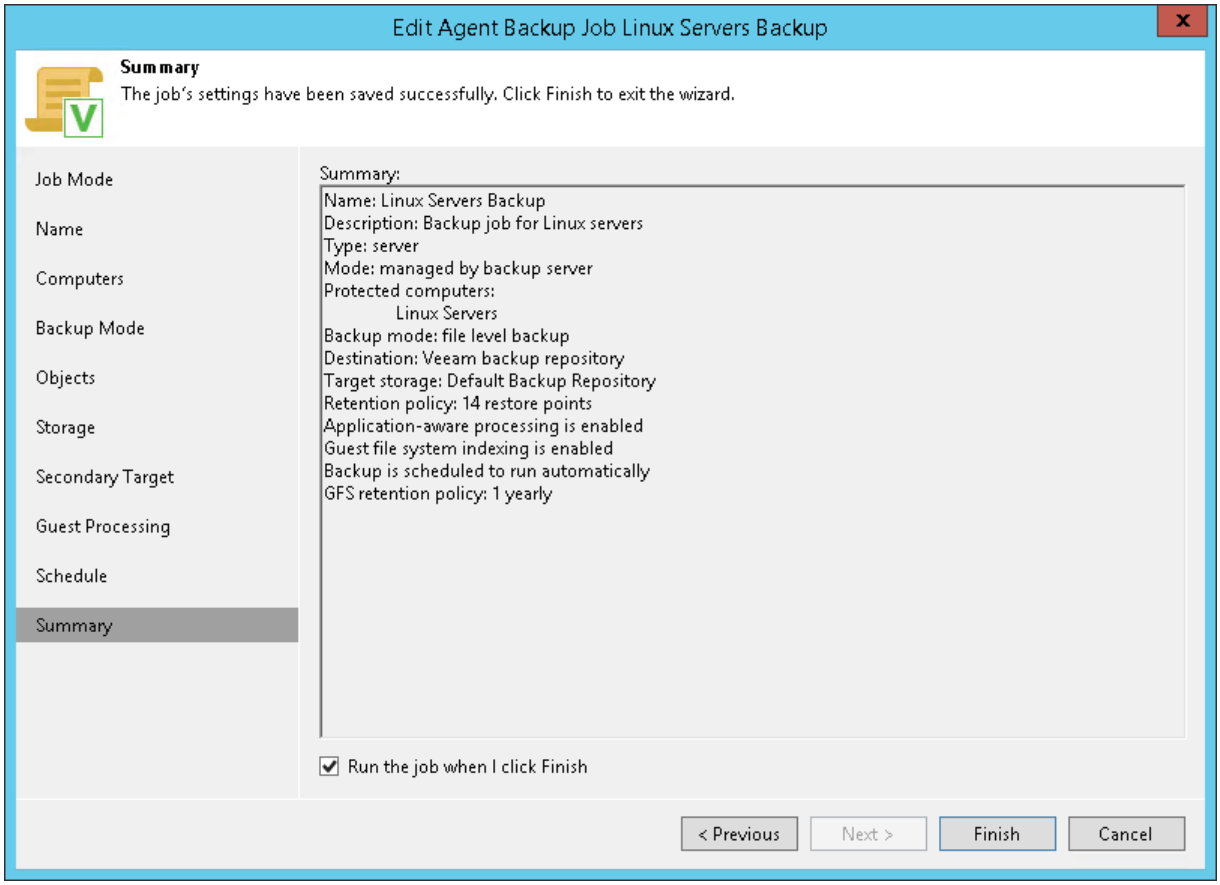
Step 13. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup job configuration process.

1. Review settings of the configured backup job.
2. [For backup job managed by backup server] Select the **Run the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.

[For backup job managed by Veeam Agent] Keep in mind that Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Linux Configuration.



Creating Veeam Agent Backup Policies

To create a Veeam Agent backup policy, you must create a Veeam Agent backup job in Veeam Backup & Replication with the **Managed by agent** option selected in the job settings. In contrast to a Veeam Agent backup job managed by the backup server that is similar to a regular backup job for VM backup, a backup policy acts as a template that describes settings of individual Veeam Agent backup jobs running on protected computers.

Veeam Backup & Replication lets you create backup policies for the following types of protected computers:

- Microsoft Windows computers protected with Veeam Agent for Microsoft Windows
- Linux computers protected with Veeam Agent for Linux
- Unix computers protected with Veeam Agent for Unix
- macOS computers protected with Veeam Agent for Mac

After you create a backup policy, Veeam Backup & Replication connects to protected computers added to the backup policy and applies settings specified in the policy to configure the Veeam Agent backup job on each computer.

Keep in mind that Veeam Backup & Replication does not connect to the protected computers added to the protection group for pre-installed Veeam Agents. In case of this protection group, computers connect to the Veeam backup server and become members of the protection group after Veeam Agent deployment. To learn more, see Protection Group Types.

Creating Policy for Windows Computers

Backup jobs and policies for Microsoft Windows computers protected with Veeam Agent for Microsoft Windows are configured in the same **New Agent Backup Job** wizard. When you select the **Managed by agent** option in the wizard, the subsequent steps of the wizard will automatically change to offer backup settings available in Veeam Agent for Microsoft Windows. For details, see Creating Agent Backup Job for Windows Computers.

Creating Policy for Linux Computers

Backup jobs and policies for Linux computers protected with Veeam Agent for Linux are configured in the same **New Agent Backup Job** wizard. When you select the **Managed by agent** option in the wizard, the subsequent steps of the wizard will automatically change to offer backup settings available in Veeam Agent for Linux. For details, see Creating Agent Backup Job for Linux.

Creating Policy for Unix Computers

To back up data of a computer protected with Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX, you must configure a Veeam Agent backup policy in Veeam Backup & Replication. This backup policy will be applied to Veeam Agent computers to create individual backup jobs. Using these jobs, Veeam Agents will perform backup operations.

Before configuring a backup policy, check prerequisites. Then use the **New Agent Backup Job** wizard to define settings for the backup policy.

1. Launch the New Agent Backup Job wizard.
2. Select the type of protected computers.
3. Specify policy name and description.
4. Select computers to back up.
5. Select backup mode.
6. Specify backup scope.
7. Select backup destination.
8. Specify backup storage settings.
9. Specify advanced backup settings.
10. Specify secondary backup target.
11. Specify guest processing settings.
12. Specify the backup schedule.
13. Review backup policy settings.

Before You Begin

Before you create a Veeam Agent backup policy in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.
- Protection groups that you want to add to the job must be of the **Computer with pre-installed agents** type. To learn more, see Protection Group Types.

Veeam Agent backup policies have the following limitations:

- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup policy settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will be updated on the Veeam Agent computer at the next start of the backup session. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

  Keep in mind, that you can immediately update settings of the backup policy from the Veeam Agent computer. To learn more, see Deploying Veeam Agent for Unix.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup policy for protected computers that run a Unix OS in one of the following ways:

- Create a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.
- Add a protection group to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.
- Add individual computers to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.

Launching Backup Job Wizard

To launch the New Agent Backup Job wizard, do one of the following:

- On the **Home** tab, click **Backup Job** > **Unix computers**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Unix computers** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Unix computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup policy, do one of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup policy and select **Add to backup job** > **Unix** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup policy and click **Add to Backup** > **Unix** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the policy. You can add other protection groups and (or) individual computers to the policy later on, when you pass through the wizard steps.

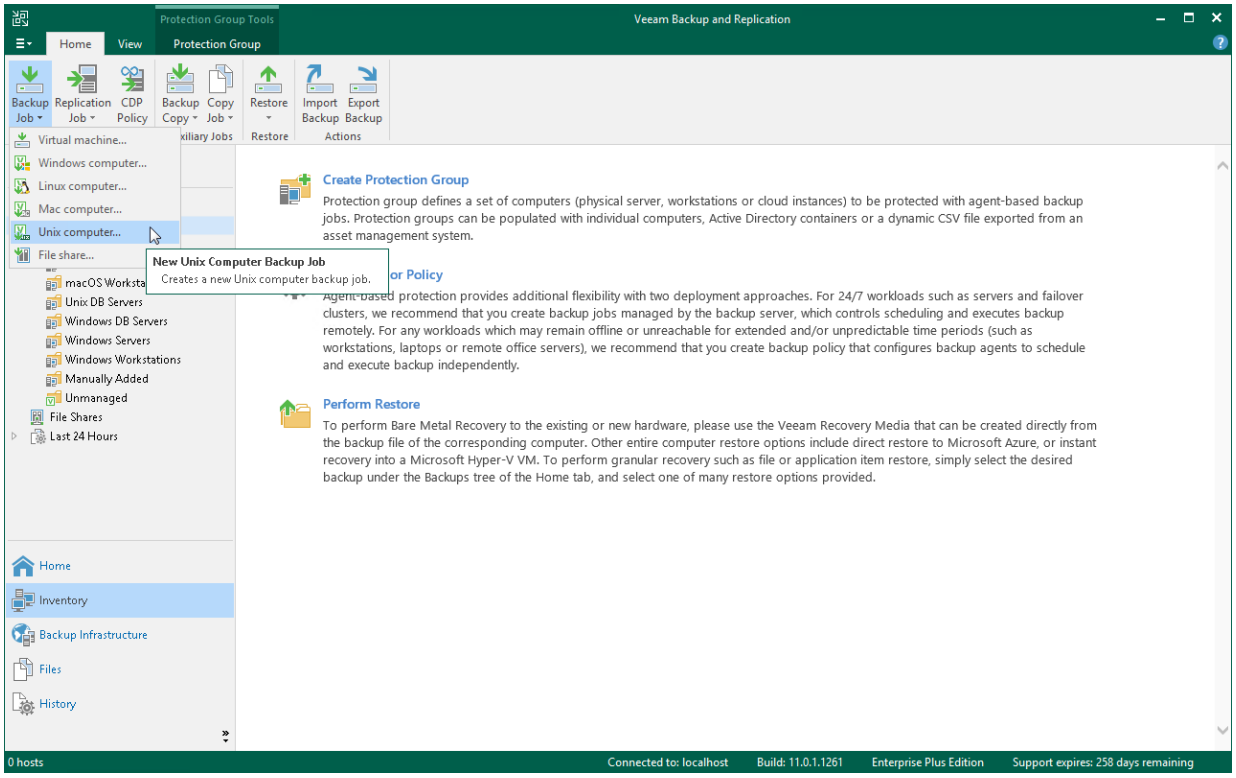
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup policy, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy, right-click the selected computer and select **Add to backup job** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy and click **Add to Backup** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the policy. You can add other computers and (or) protection groups to the policy later on, when you pass through the wizard steps.

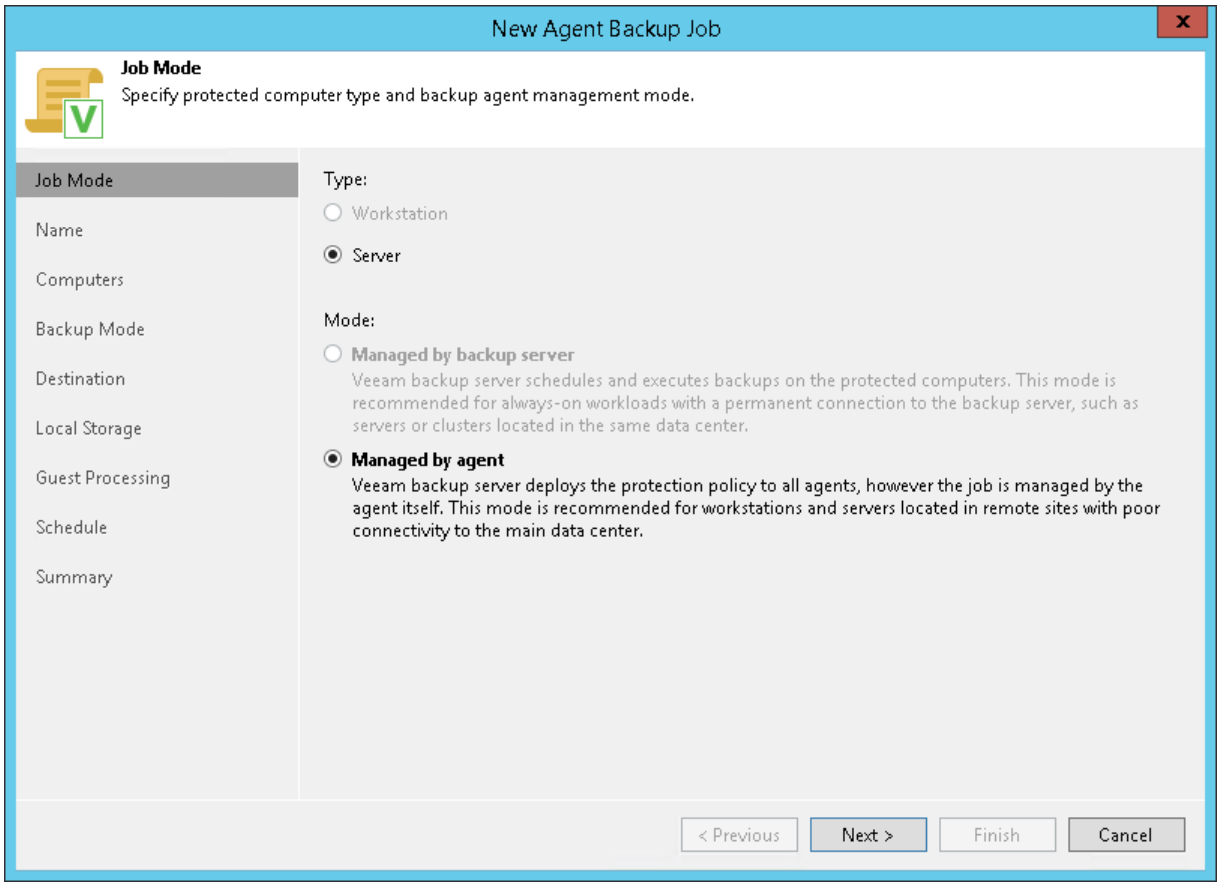
> **TIP**
>
> Consider the following:
>
> - You can press and hold **[CTRL]** to select multiple computers at once.
> - You can add an individual computer or protection group to a Veeam Agent backup policy that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.



Step 2. Select Job Mode

At the **Job Mode** step of the wizard, click **Next**.

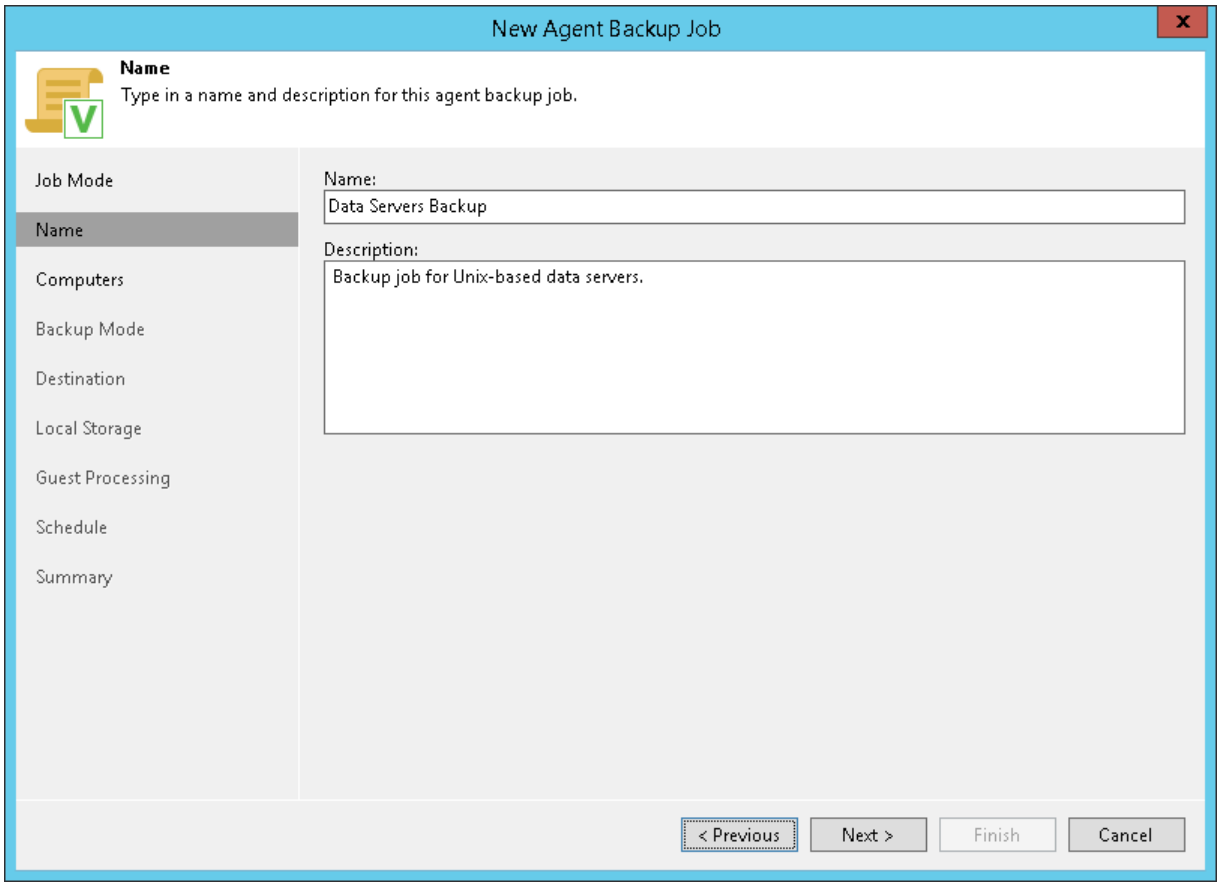
You do not need to select the job type and mode. Unix computers can be added only as servers and only to Veeam Agent backup jobs managed by Veeam Agent.



Step 3. Specify Policy Name and Description

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

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



Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers that you want to back up.

You can add to the Veeam Agent backup policy one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

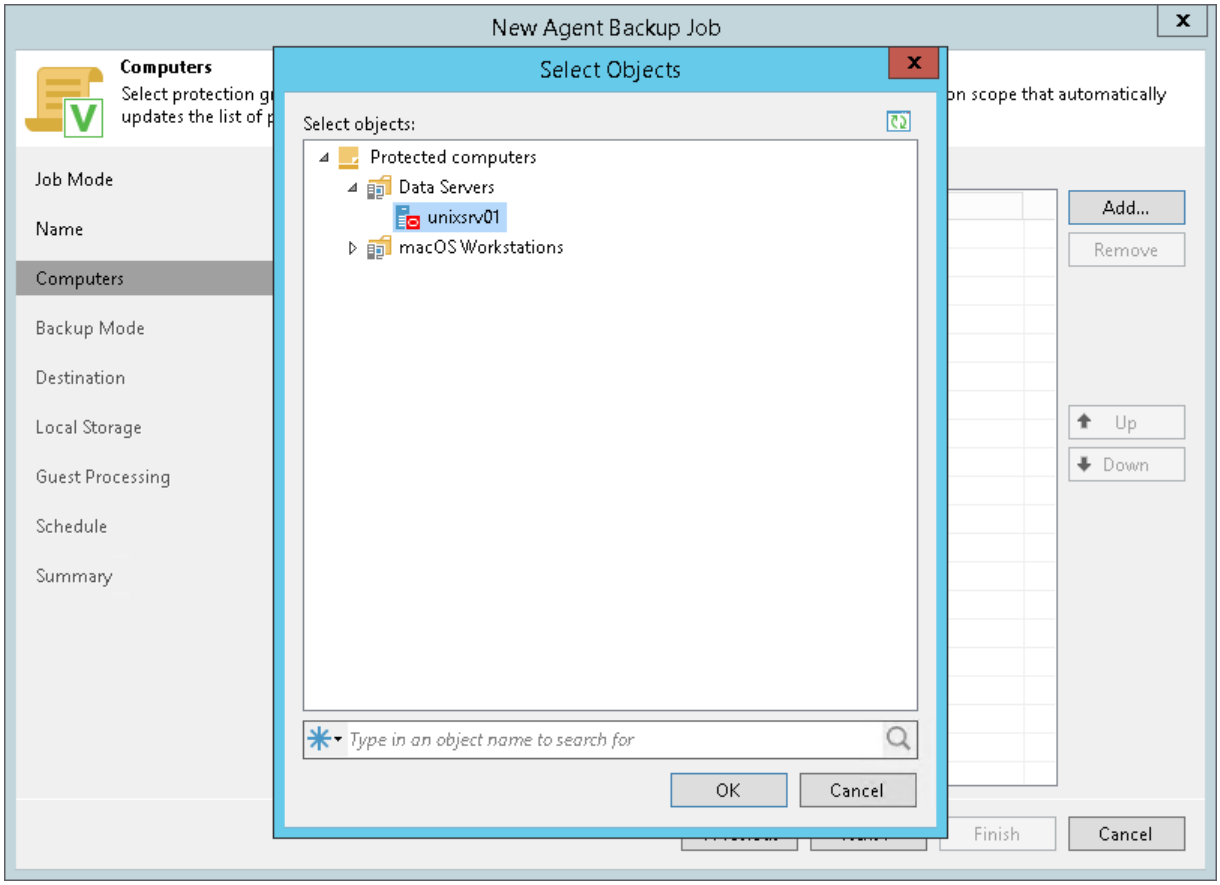
> **NOTE**
>
> If you used the **Add to backup job** > **Unix** > **New job** option to launch the New Agent Backup Job wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers to the policy, if necessary.

To add protection groups and/or individual computers to the Veeam Agent backup policy:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and/or computers in the list and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Step 5. Select Backup Mode

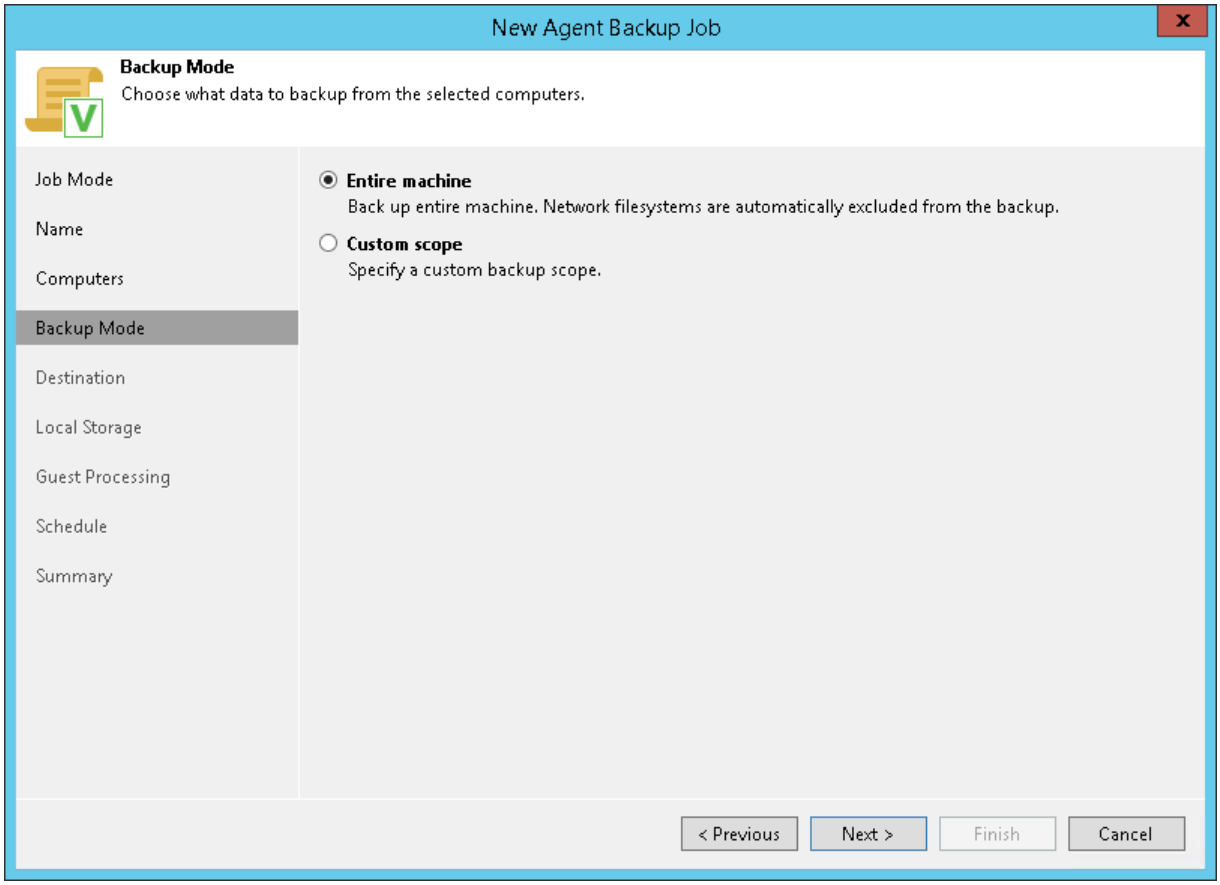
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup. You can select one of the following options:

- **Entire machine** – select this option if you want to create a backup of all files and directories available on the protected Unix computer.

  Mind that in the Entire machine mode, Veeam Agent excludes network shared folders from the backup scope. To back up network shared folders, use the Custom scope mode.

- **Custom scope** – select this option if you want to create a backup of individual directories on your computer. With this option selected, you will pass to the Objects step of the wizard.

  > **TIP**
  >
  > If you plan to back up a network shared folder, you must select the **Custom scope** option and add this network shared folder as an individual object to the backup scope at the **Objects** step of the wizard.



Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you have chosen the **Custom scope** mode at the Backup Mode step of the wizard.

At this step of the wizard, you must specify the backup scope — define what directories with files you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup policy. If a specified directory does not exist on one or more computers in the policy, the policy will skip such directory on those computers and back up existing ones.

To specify directories to back up:

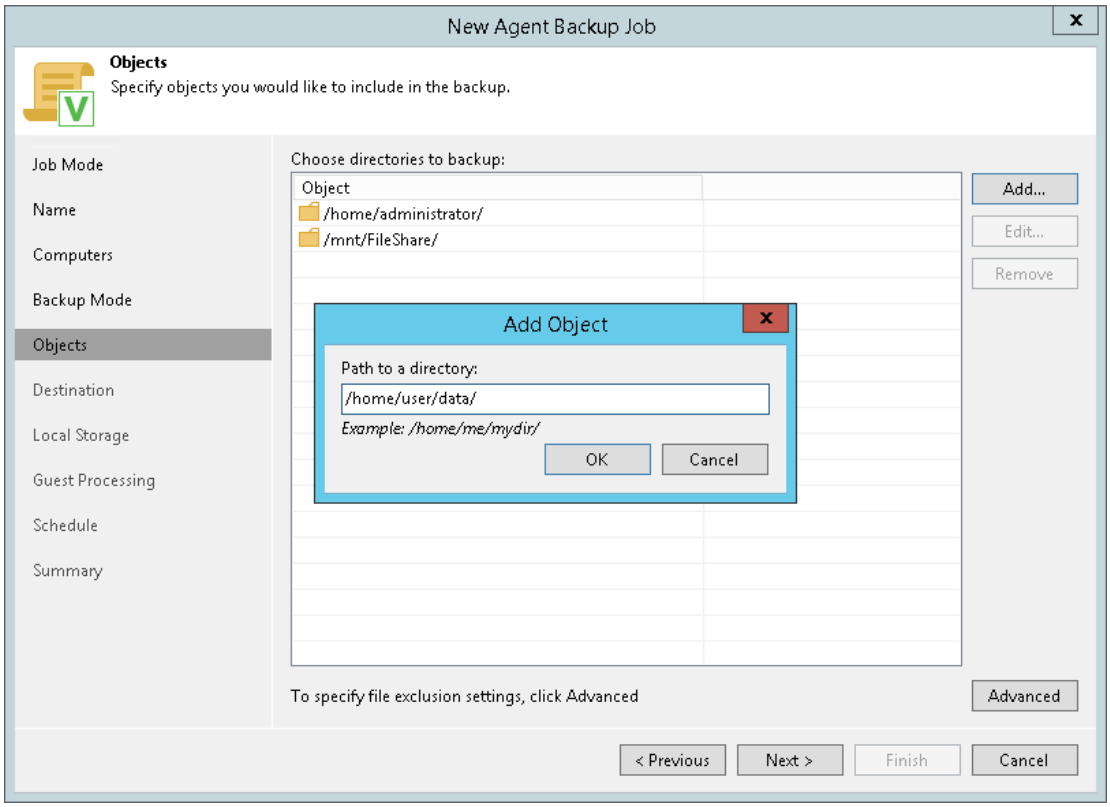
1. In the **Choose directories to backup** field, click **Add**.
2. In the **Add Object** window, type the path to a directory that you want to back up, for example, `/home/user01`, and click **OK**.
3. Repeat steps 1-2 for all directories that you want to back up.

TIP

If you want to back up the root directory and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.

For example, you have a file system mounted to the `/Library/Media` directory. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root directory and the mounted file system, add the following objects to the backup scope:

- `/`
- `/Library/Media`



Configuring Filters

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

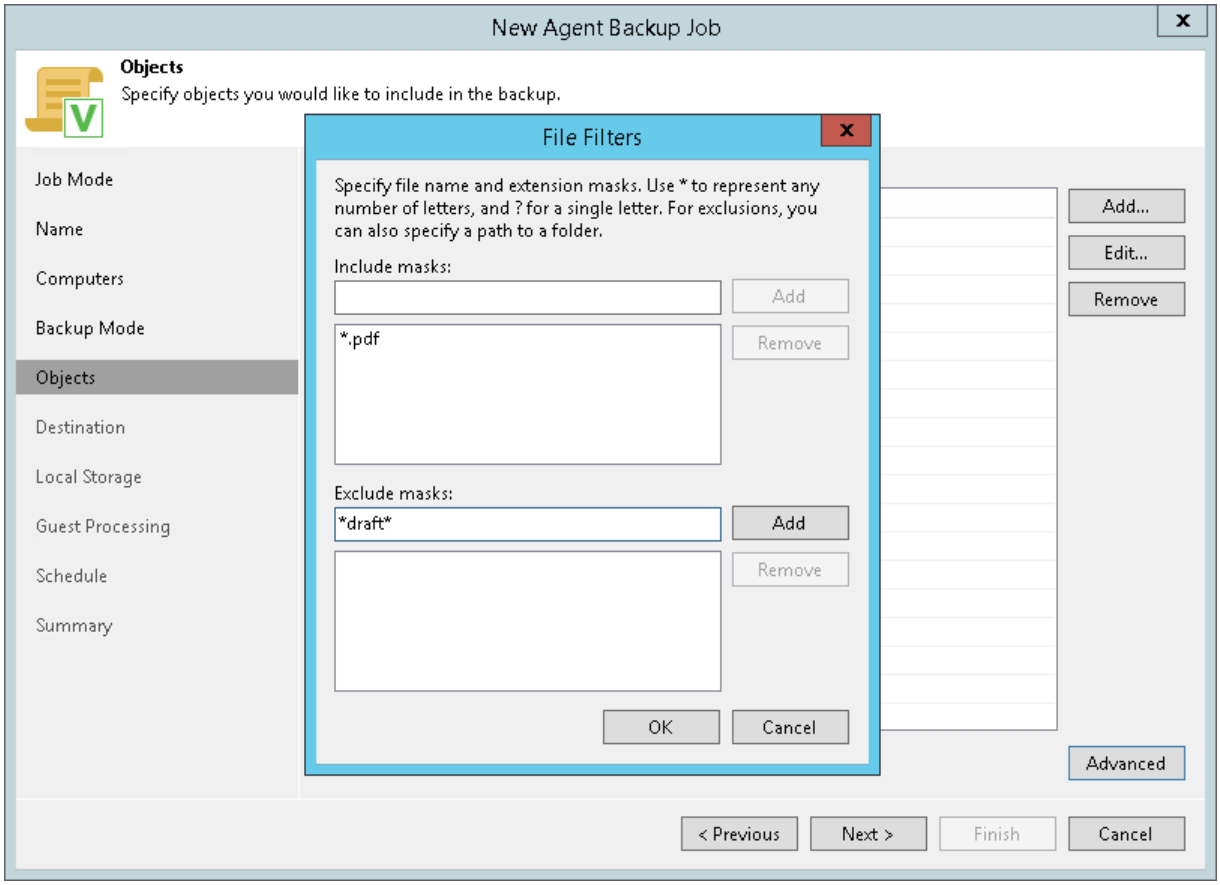
To configure a filter:

1. At the **Objects** 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, `Report.pdf` or `*filename*`. Veeam Agent will create a backup only for selected files. Other files will not be backed up.
   - In the **Exclude masks** field, specify file names and/or masks for file types that you do not want to back up, for example, `OldReports.tar.gz` or `*.odt`. Veeam Agent will back up all files except files of the specified type.
3. Click **Add**.
4. Repeat steps 2–3 for each mask that you want to add.

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

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

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



Step 7. Select Backup Destination

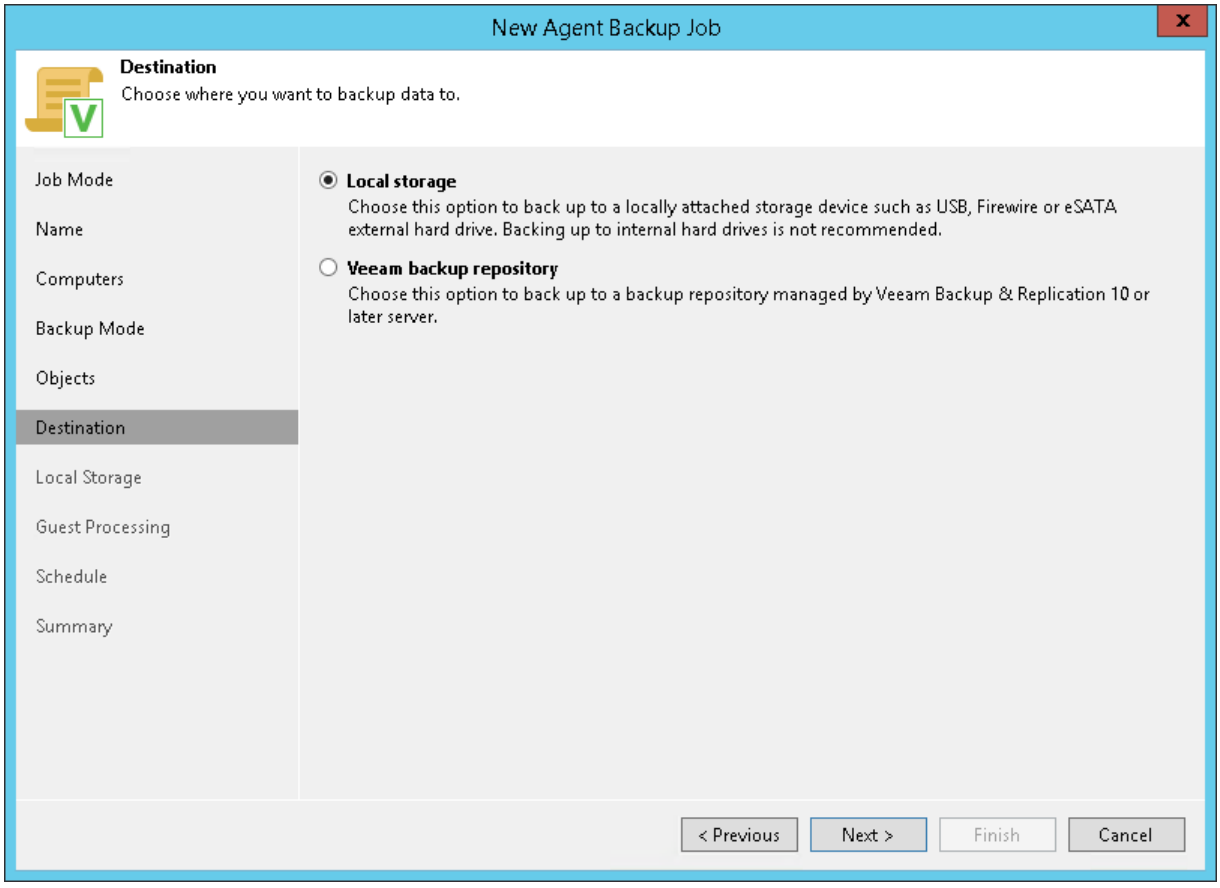
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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

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

  > **IMPORTANT**
  >
  > It is 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.

- **Veeam backup repository** — select this option if you want to save a backup 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 8. Specify Backup Storage Settings

Specify backup storage settings for the backup policy at one of the following steps of the wizard:

- Local storage settings — if you have selected the **Local storage** option at the Destination step of the wizard.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.

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.

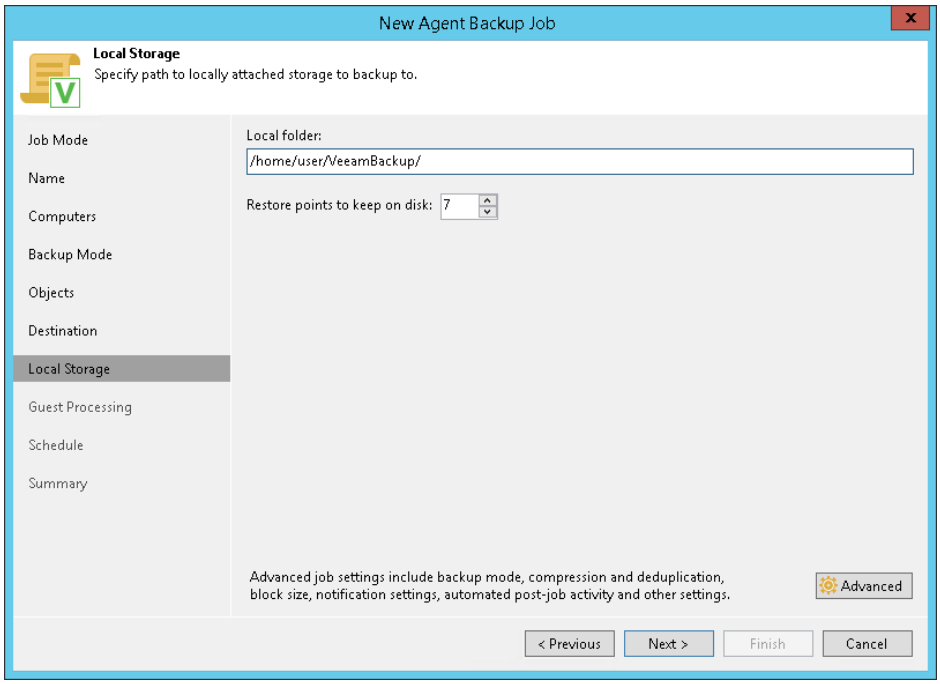
Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup policy settings to this computer.

   > **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.

2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



Veeam Backup Repository Settings

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

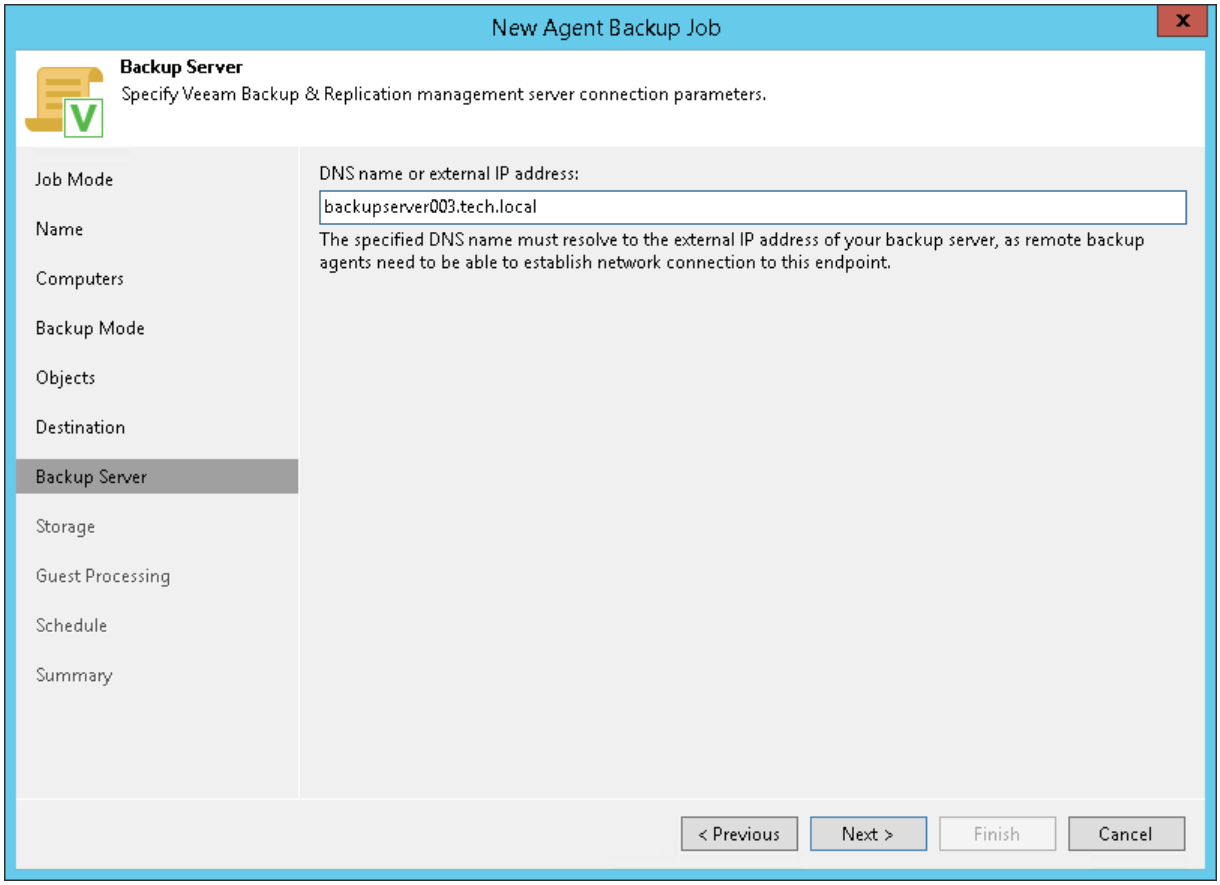
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

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

In the **DNS name or external IP address field**, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup policy. The specified DNS name or IP address must be accessible from the network to which Veeam Agent computers are connected.

> **NOTE**
>
> Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.

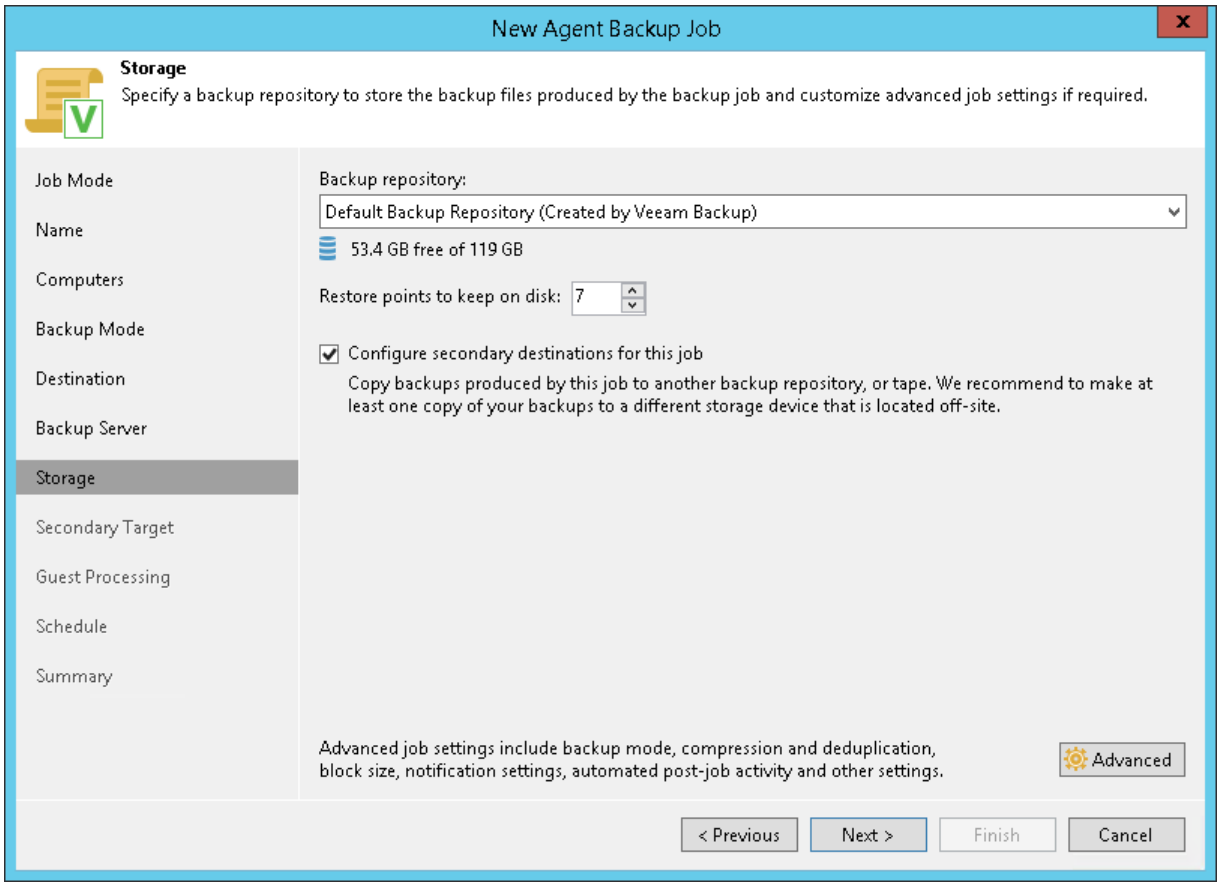


Selecting Backup Repository

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.
3. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary Target. At the **Secondary Target** step of the wizard, you can link the backup policy to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.
4. Click **Advanced** to specify advanced settings for the backup policy. To learn more, see Specify Advanced Backup Settings.



Step 9. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the Veeam Agent backup policy:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings

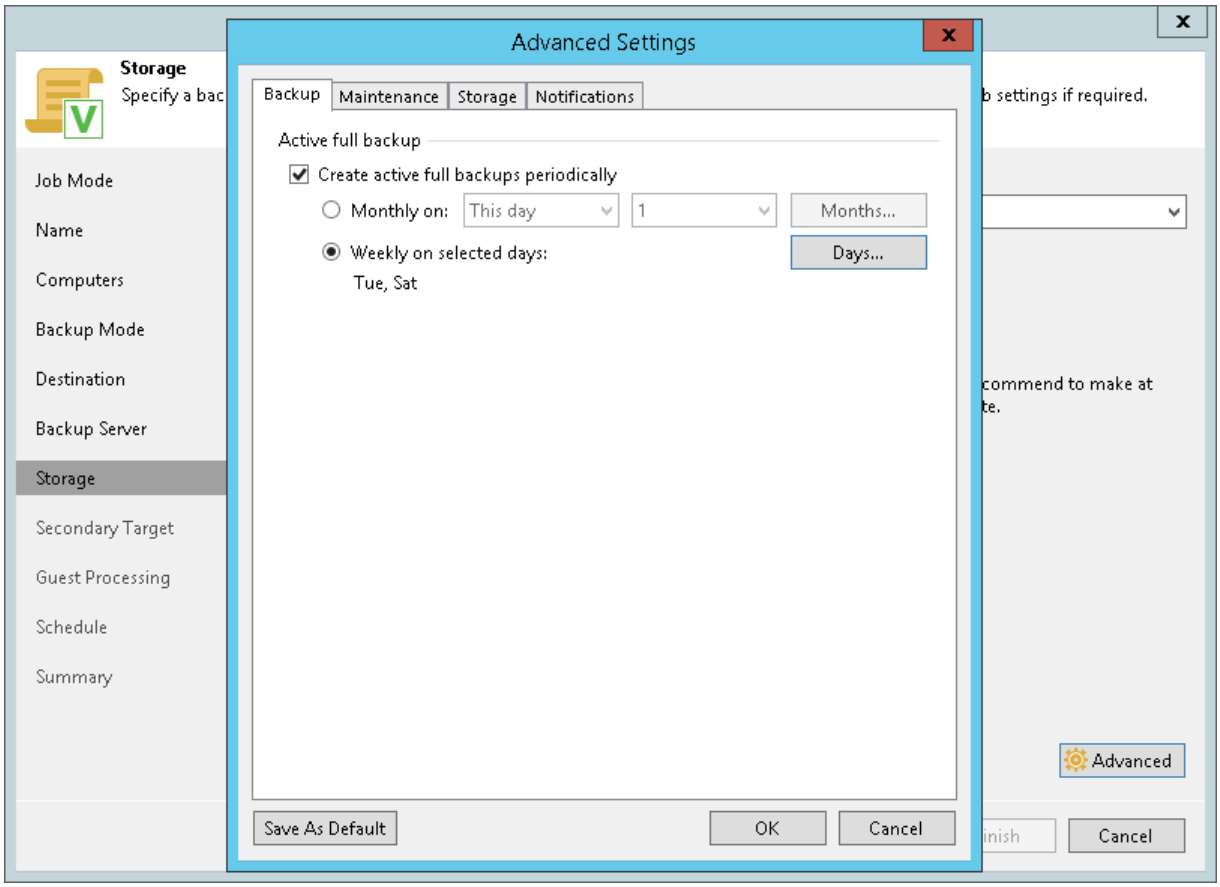
> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

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

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
2. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

> **NOTE**
>
> Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.



Maintenance Settings

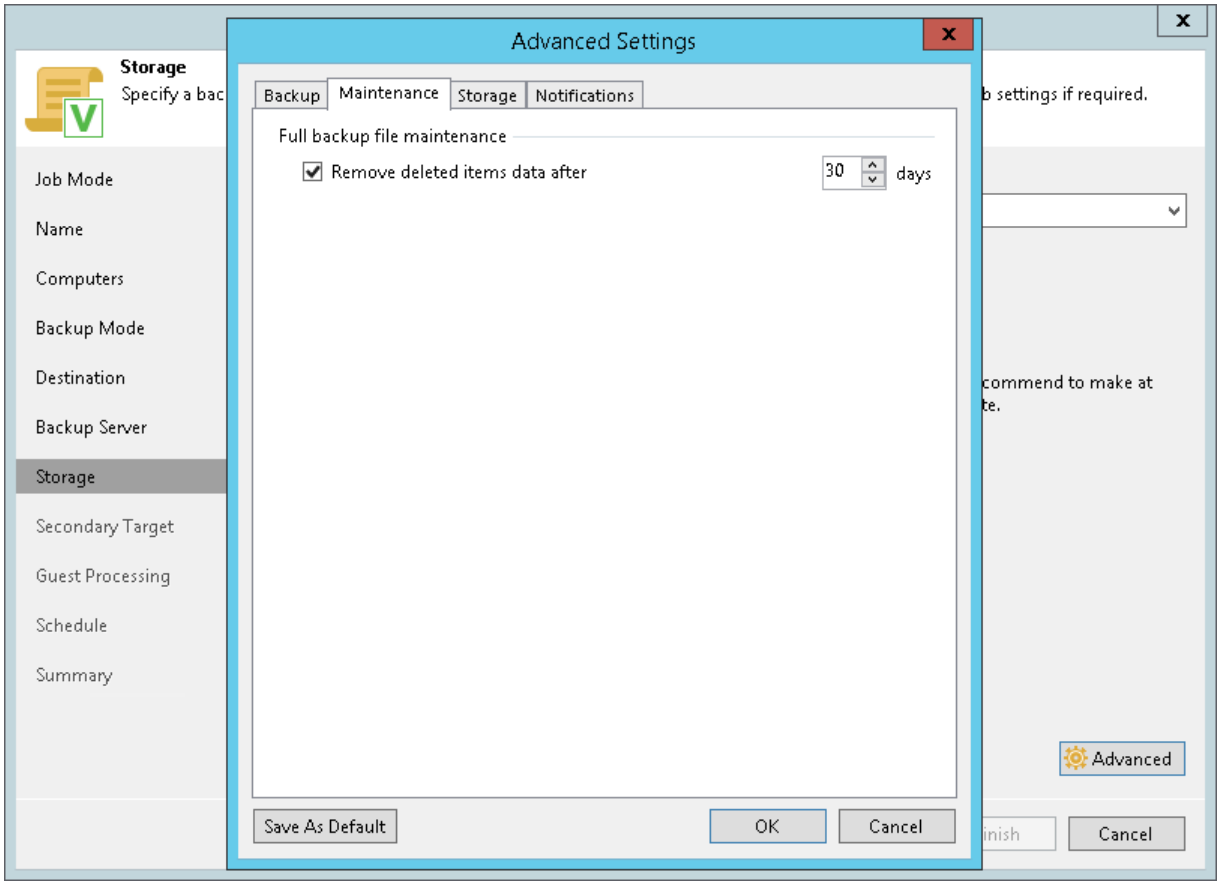
You can specify maintenance settings for a backup policy targeted at a Veeam backup repository. Maintenance operations help make sure that the backup chain remains valid and consistent.

To specify maintenance settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup policy in the target location.

   If Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location.

   By default, the deleted items data retention period is 30 days. Do not set the deleted items retention period to 1 day or a similar short interval. Otherwise, the backup policy may not work as expected and remove data that you still require.

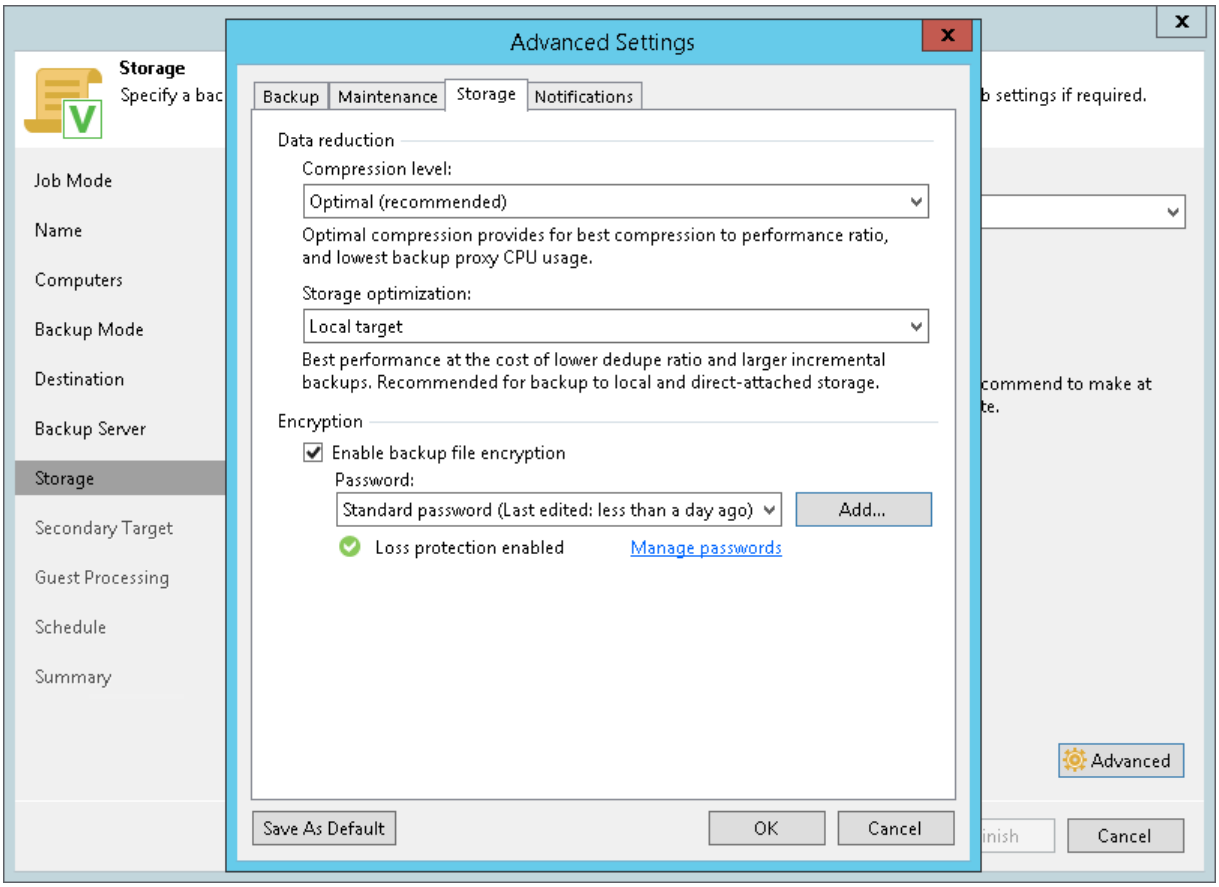


Storage Settings

To specify storage settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
2. Click the **Storage** tab.
3. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
4. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Agent will use data blocks of different size to optimize the size of backup files and policy performance.
5. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see the Password Manager section in the Veeam Backup & Replication User Guide.

   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.



NOTE

Consider the following:

- Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer or at a network shared folder. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.
- If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.
- If you enable encryption for an existing Veeam Agent backup job or policy, during the next session Veeam Agent will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.
- Encryption is not retroactive. If you enable encryption for an existing backup job or policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this job.
- When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

  This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.

Notification Settings

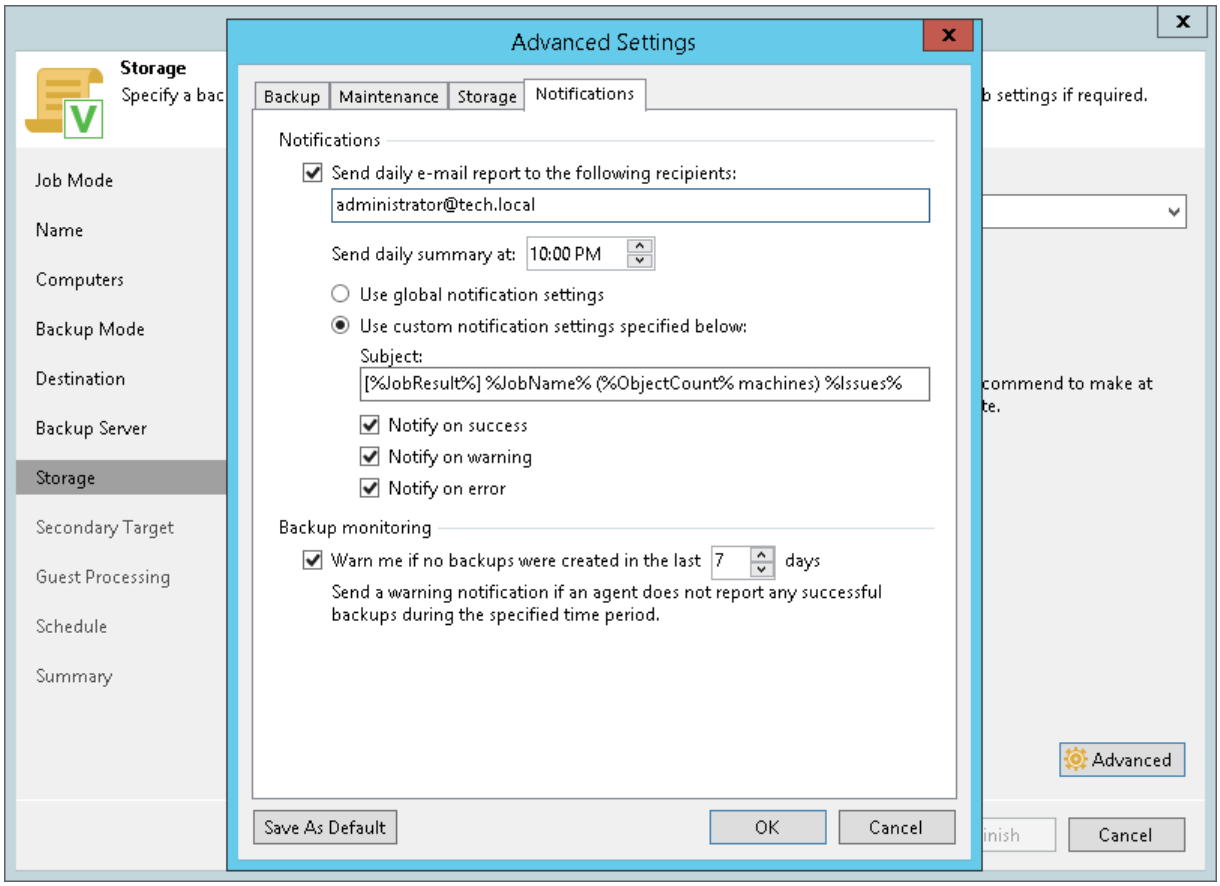
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup policy sessions performed for the last 24-hour period on computers to which the backup policy is applied.

> **NOTE**
>
> Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the backup policy, Veeam Backup & Replication will send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will send the report daily at the specified time.
5. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing backup policy statistics at 8:00 AM daily.
   - To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the backup policy) and *%Issues%* (number of machines in the backup policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the policy completes successfully, completes with a warning or fails.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Step 10. Specify Secondary Target

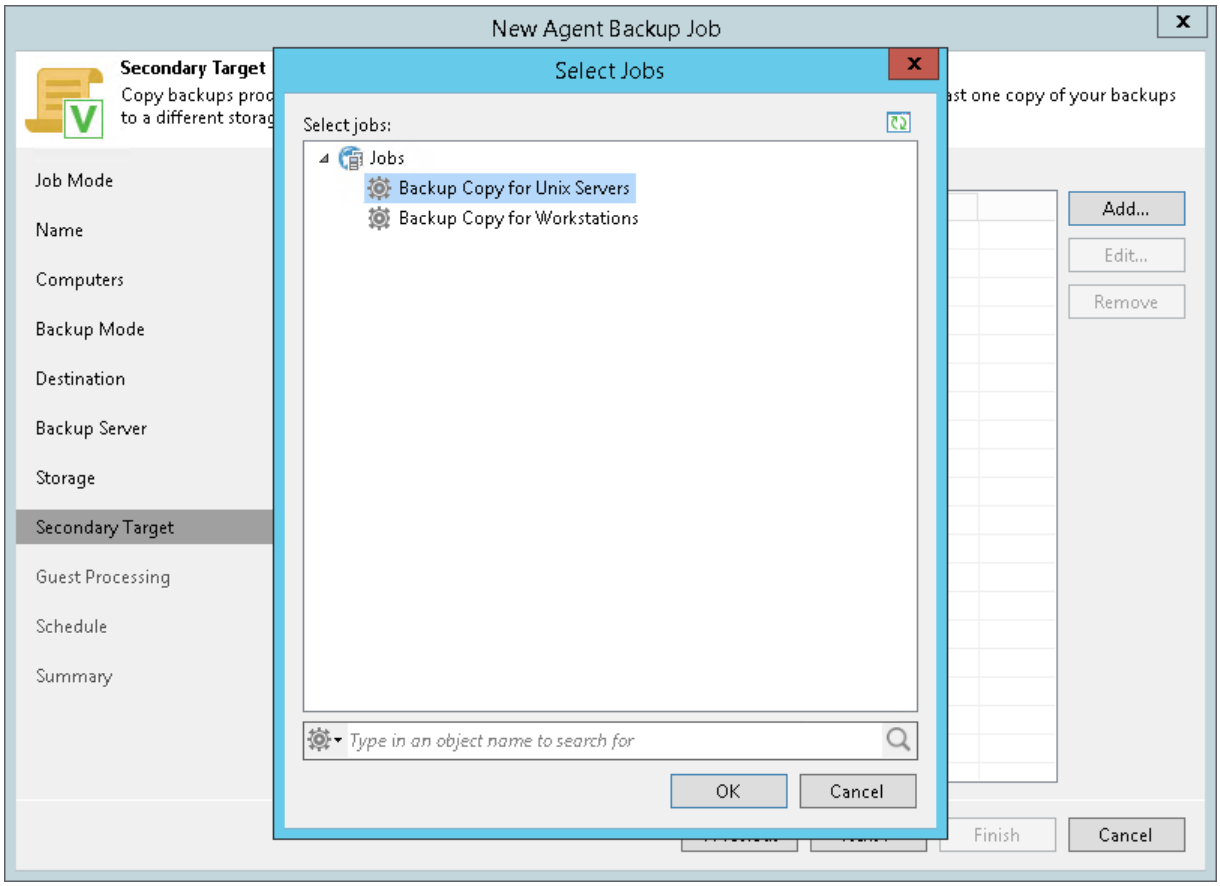
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup job to a backup to tape or backup copy job. As a result, the backup job will be added as a source to the backup to tape or backup copy job. Backup files created with the backup job will be archived to tape or copied to the secondary backup repository according to the secondary jobs schedule. For more information, see Linking Backup Jobs to Backup Copy Jobs and Linking Backup Jobs to Backup to Tape Jobs in the Veeam Backup & Replication User Guide.

The backup to tape job or backup copy job must be configured beforehand. You can create these jobs with an empty source. When you link the Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent backup job as a source for these jobs.

To link jobs:

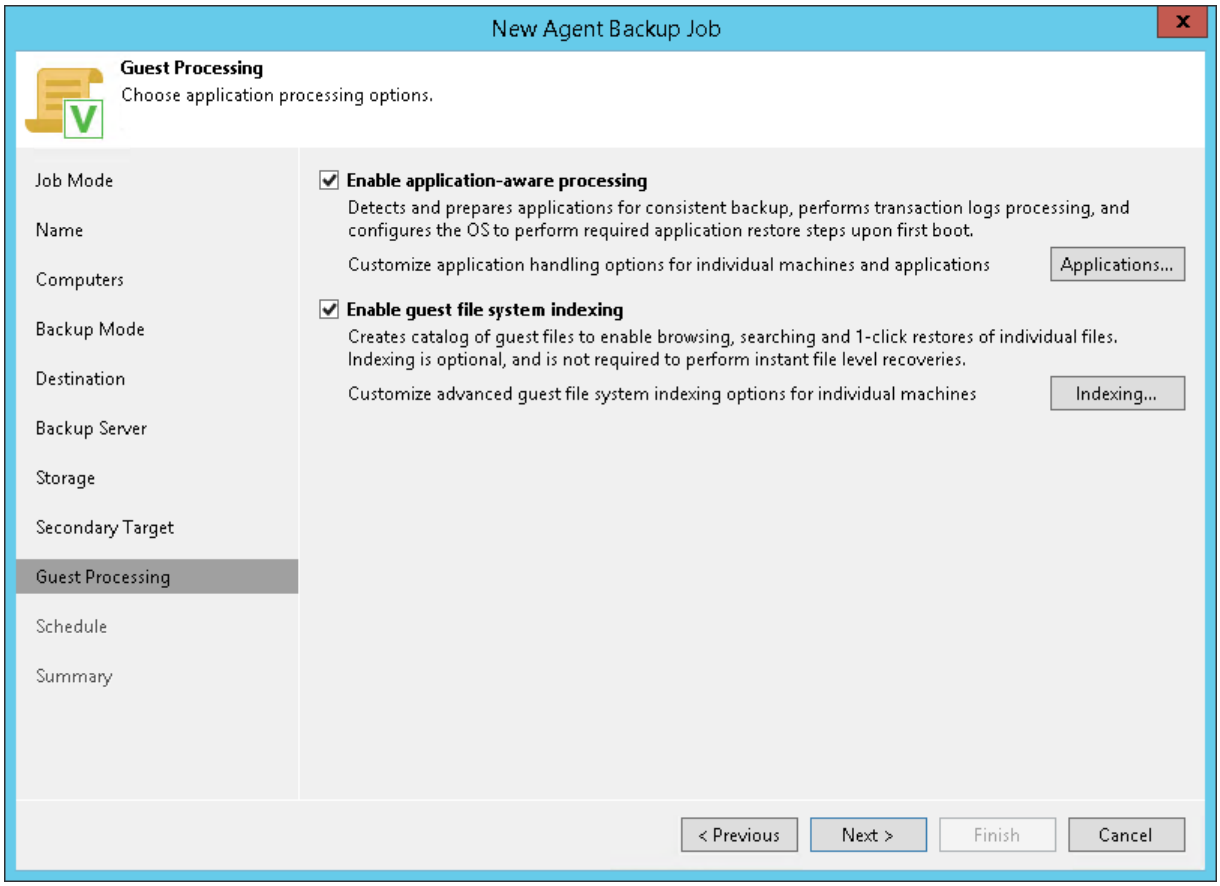
1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom of the wizard.



Step 11. Specify Guest Processing Settings

At the **Guest Processing** step of the wizard, you can enable the following guest OS processing settings for a Veeam Agent backup job that includes Unix-based computers:

- Use of backup job and snapshot scripts
- File indexing



Backup Job Scripts

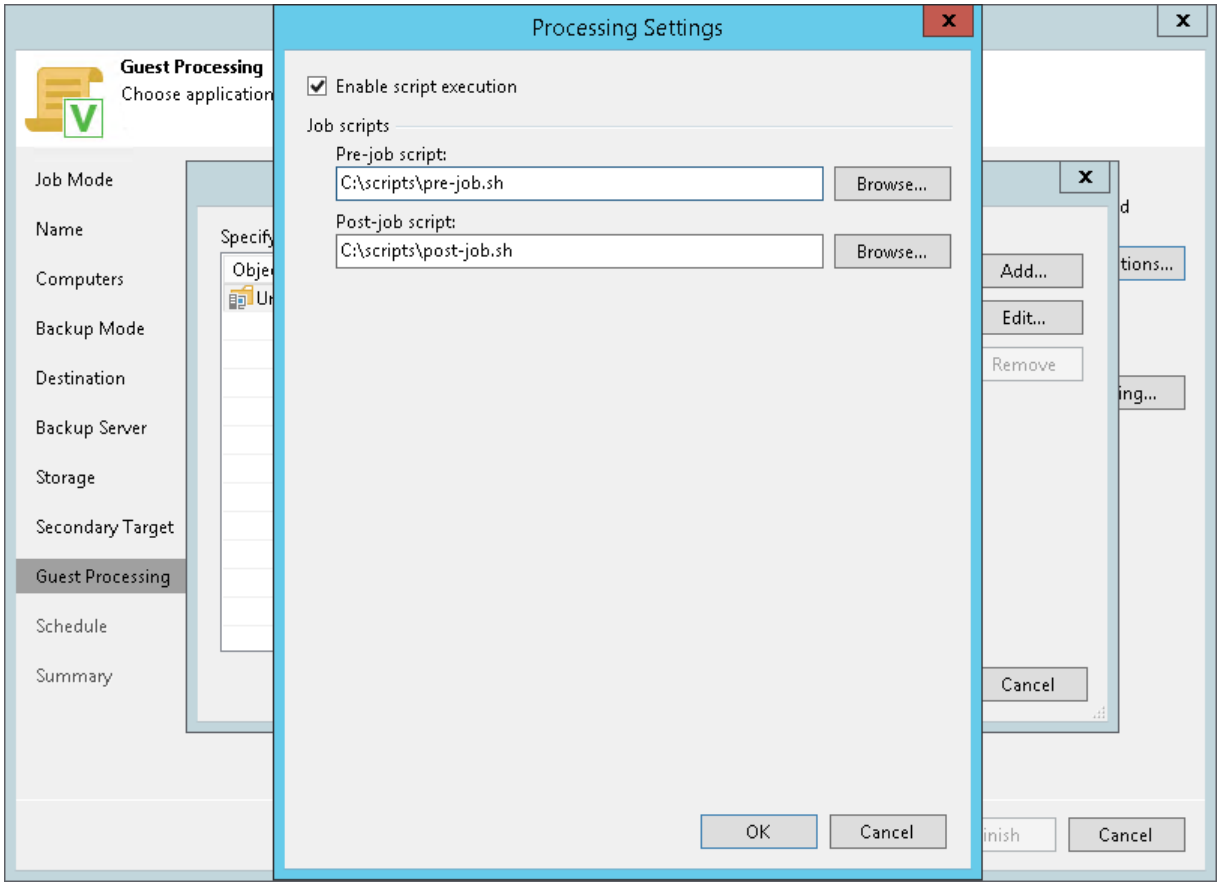
You can specify custom backup job scripts that will be executed within the backup job session on Unix computers. Veeam Agent supports pre-job and post-job scripts that run on the Veeam Agent computer before and after the backup job session. To learn more, see Backup Job Scripts.

To specify custom scripts for the job:

1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Processing Settings** window, select the **Enable script execution** check box.
5. In the **Pre-job script** and **Post-job script** fields, click **Browse** to choose executable files from a local folder on the backup server.

Veeam Agent supports scripts in the SH file format. During the backup job session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the job and execute them on these computers.



File Indexing

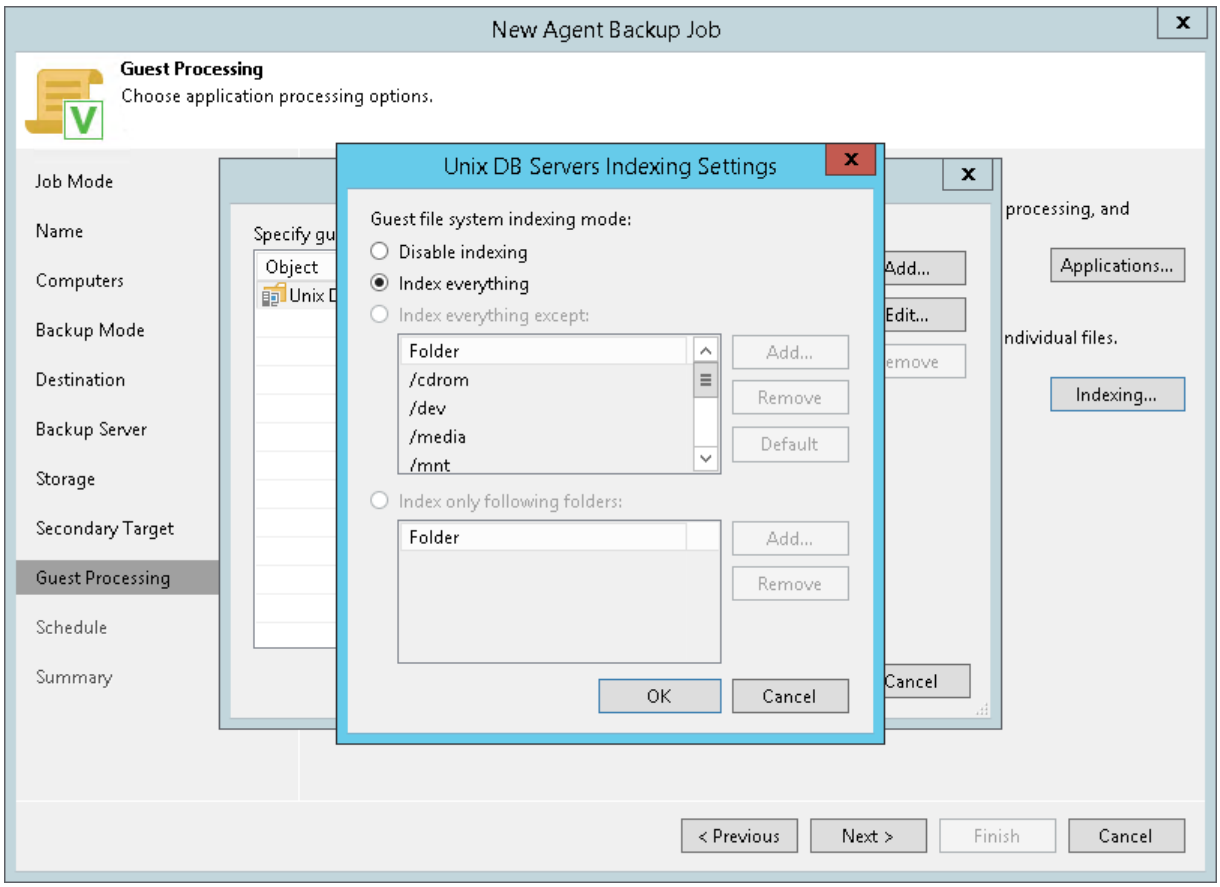
To specify file indexing options:

1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select the protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Indexing Settings** window, select **Index everything** if you want to index all files within the backup scope that you have specified at the [TBD} Unix Source step of the wizard.

NOTE

You cannot specify a custom indexing scope for Unix computers. For a file-level backup job that processes Unix computers, only the **Index everything** option is available.



Step 12. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

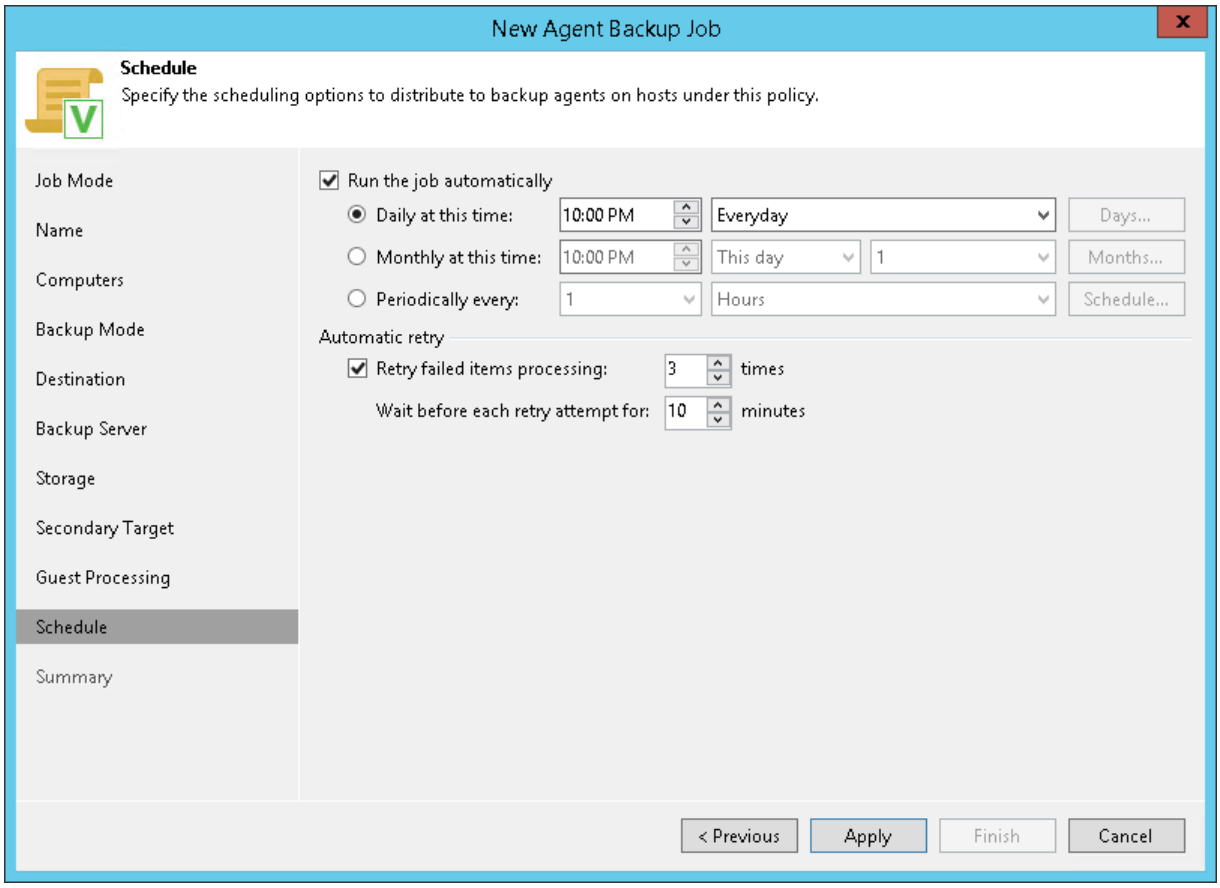
     A repeatedly run job is started by the following rules:

     - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
     - If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

     For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

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

3. In the **Automatic retry** section, define whether Veeam Agent must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Agent for Mac will retry the job for the defined number of times without any time intervals between the job runs.



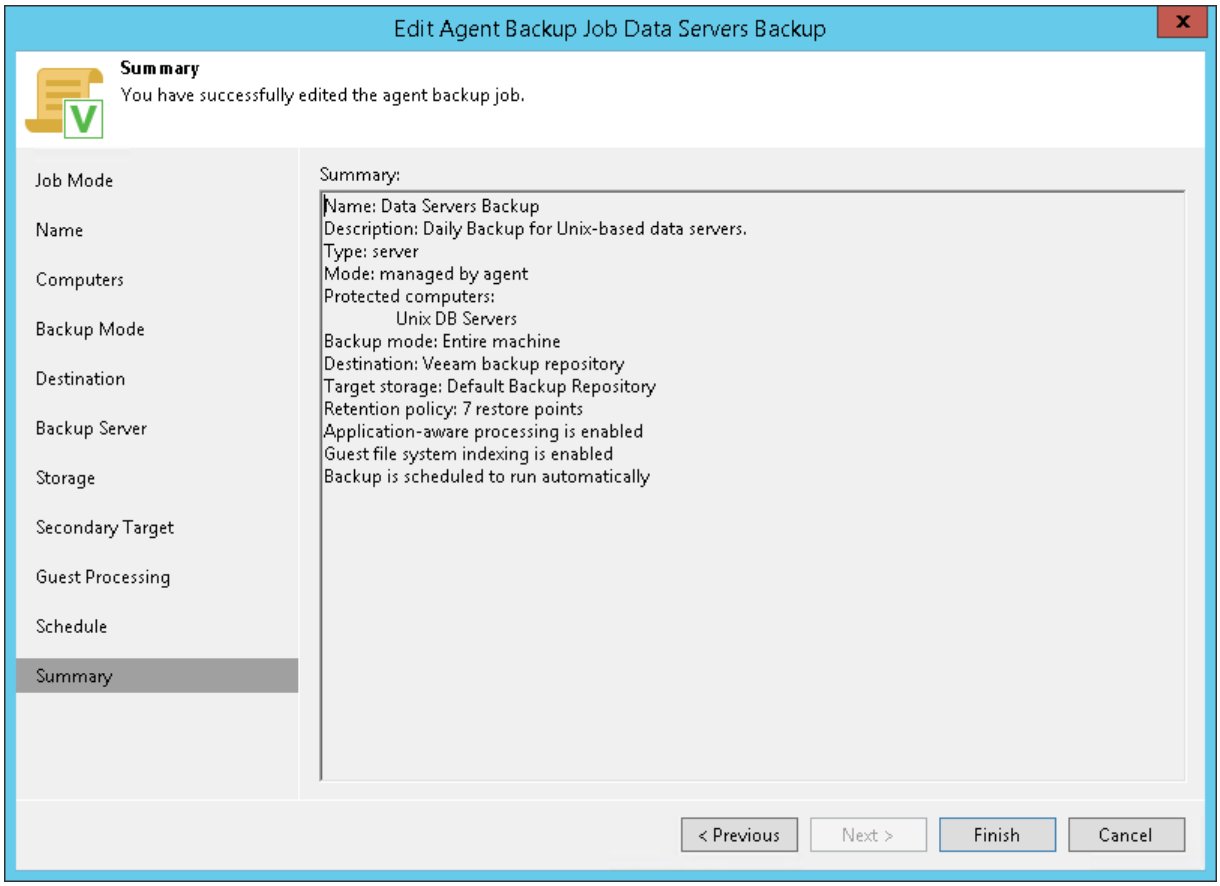
Step 13. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup policy configuration process.

1. Review settings of the configured backup policy.
2. Click **Finish** to close the wizard.

Keep in mind that Veeam Backup & Replication does not apply backup policy to Unix computers immediately. Veeam Agents installed on Unix computers connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Unix Configuration.



Creating Policy for Mac Computers

To back up data of a computer protected with Veeam Agent for Mac, you must configure a Veeam Agent backup policy in Veeam Backup & Replication. This backup policy will be applied to Veeam Agent computers to create individual backup jobs. Using these jobs, Veeam Agents will perform backup operations.

Before configuring a backup policy, check prerequisites. Then use the **New Agent Backup Job** wizard to define settings for the backup policy.

1. Launch the New Agent Backup Job wizard.
2. Select the type of protected computers.
3. Specify policy name and description.
4. Select computers to back up.
5. Select backup mode.
6. Specify backup scope.
7. Select backup destination.
8. Specify backup storage settings.
9. Specify advanced backup settings.
10. Specify secondary backup target.
11. Specify the backup schedule.
12. Review backup policy settings.

Before You Begin

Before you create a Veeam Agent backup policy in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.
- Protection groups that you want to add to the job must be of the **Computer with pre-installed agents** type. To learn more, see Protection Group Types.
- [For backup jobs targeted at the cloud repository] The Veeam Cloud Connect service provider must be added in the Veeam backup console.

Veeam Agent backup policies have the following limitations:

- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup policy settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will be updated on the Veeam Agent computer at the next start of the backup session. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

  Keep in mind, that you can immediately update settings of the backup policy from the Veeam Agent computer. To learn more, see Deploying Veeam Agent for Mac.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup policy for protected computers that run a macOS in one of the following ways:

- Create a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.
- Add a protection group to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.
- Add individual computers to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.

Launching Backup Job Wizard

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

- On the **Home** tab, click **Backup Job** > **Mac computer**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Mac computer** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Mac computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup policy, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup policy and select **Add to backup job** > **Mac** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup policy and click **Add to Backup** > **Mac** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the policy. You can add other protection groups and (or) individual computers to the policy later on, when you pass through the wizard steps.

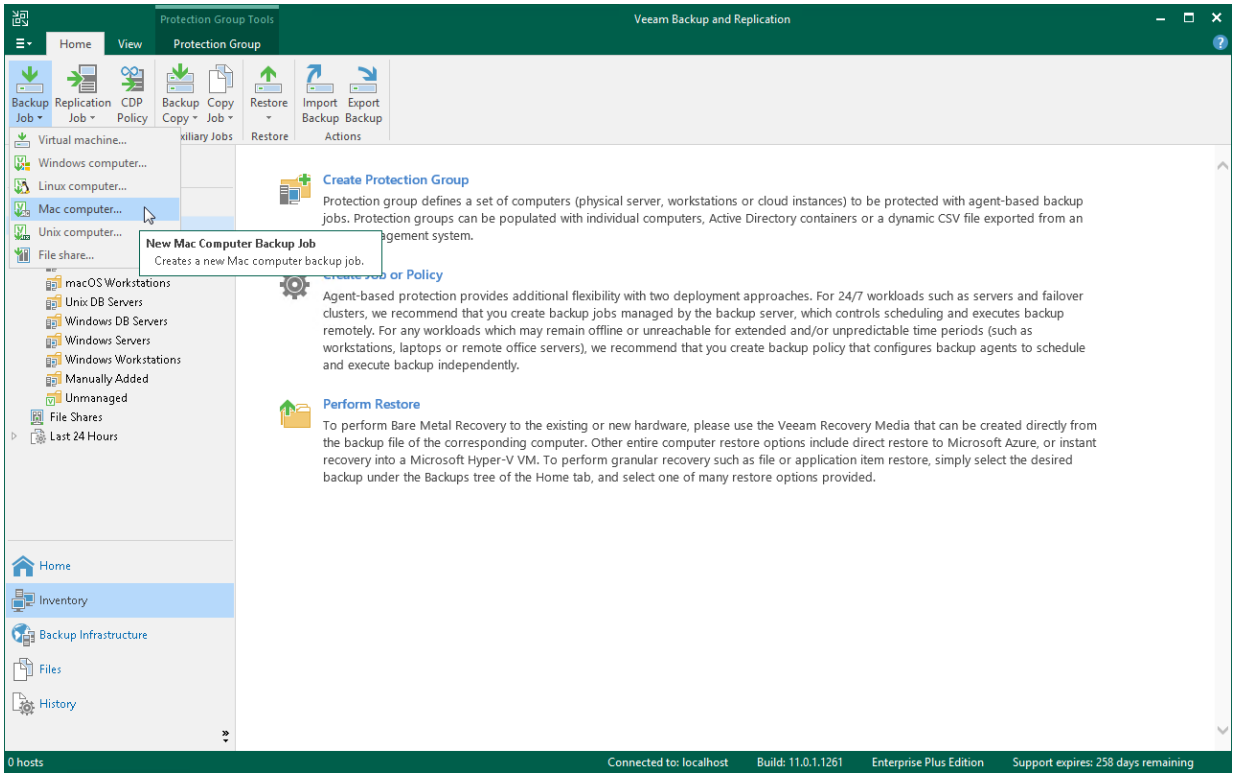
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup policy, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy, right-click the selected computer and select **Add to backup job** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy and click **Add to Backup** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the policy. You can add other computers and (or) protection groups to the policy later on, when you pass through the wizard steps.

> **TIP**
>
> Consider the following:
>
> - You can press and hold **[CTRL]** to select multiple computers at once.
> - You can add an individual computer or protection group to a Veeam Agent backup policy that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.



Step 2. Select Job Mode

At the **Job Mode** step of the wizard, in the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents.

The selected type defines what settings will be available for the configured backup policy. You can select one of the following computer types:

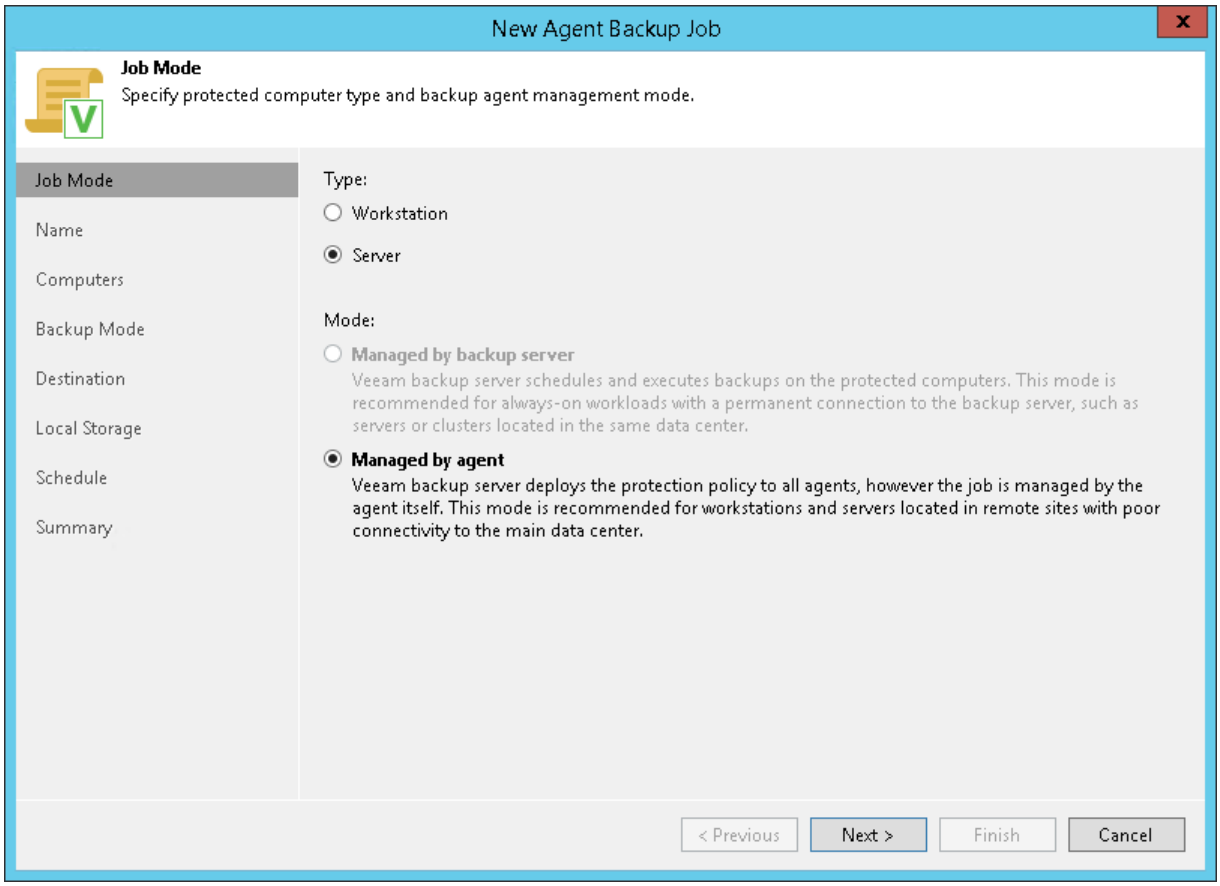
- **Workstation** — select this option if you want to back up data pertaining to macOS workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  For backup jobs that process workstations, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent operating in the *Workstation* mode. To learn more, see the Product Editions section in the Veeam Agent for Mac User Guide.

- **Server** — select this option if you want to back up data pertaining to macOS servers. This option is suitable for computers that have permanent connection to the backup server.

  For backup jobs that process servers, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent operating in the Server mode. To learn more, see the Product Editions section in the Veeam Agent for Mac User Guide.

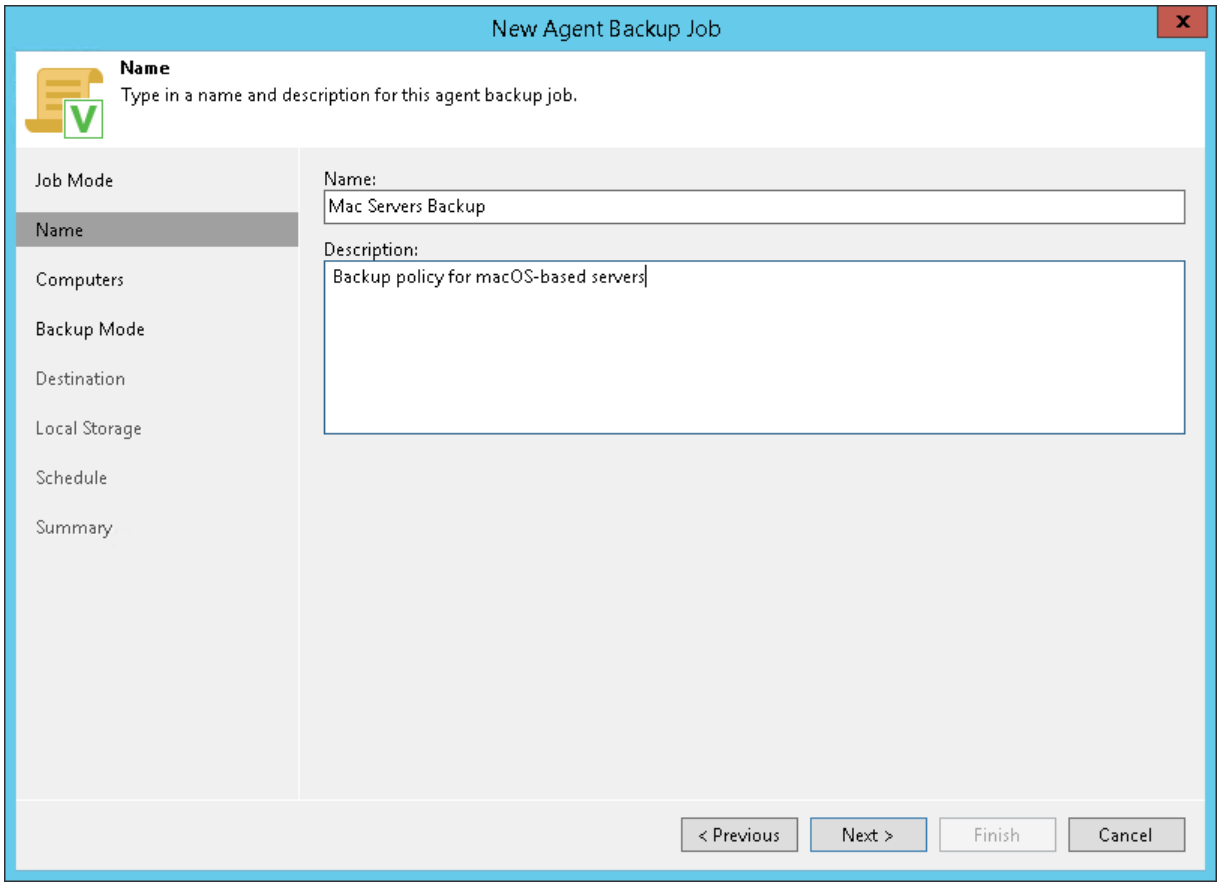
You do not need to select the job mode. Mac computers can be added only to Veeam Agent backup jobs managed by Veeam Agent.



Step 3. Specify Policy Name and Description

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

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



Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers that you want to back up.

You can add to the Veeam Agent backup policy one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

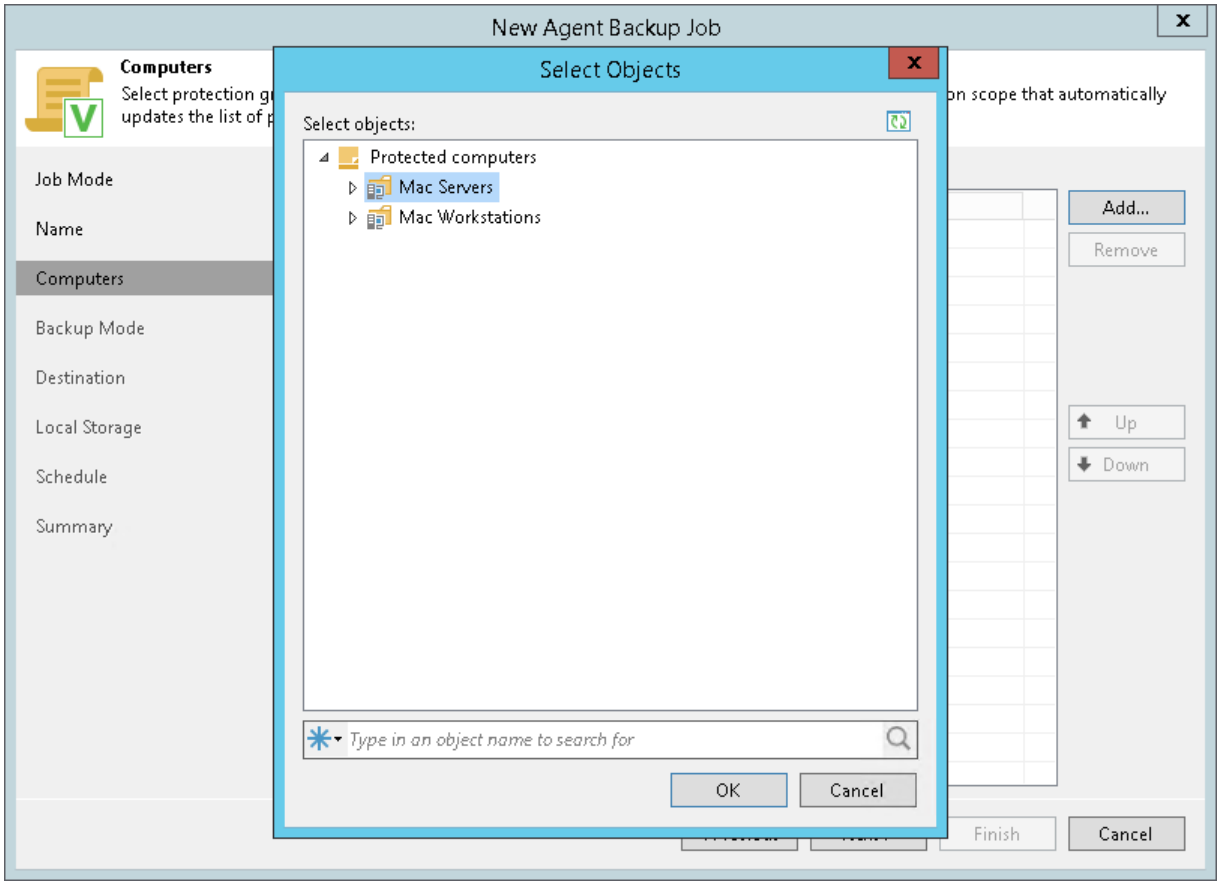
> **NOTE**
>
> If you used the **Add to backup job** > **Mac** > **New job** option to launch the New Agent Backup Job wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers to the policy, if necessary.

To add protection groups and/or individual computers to the Veeam Agent backup policy:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and/or computers in the list and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Step 5. Select Backup Mode

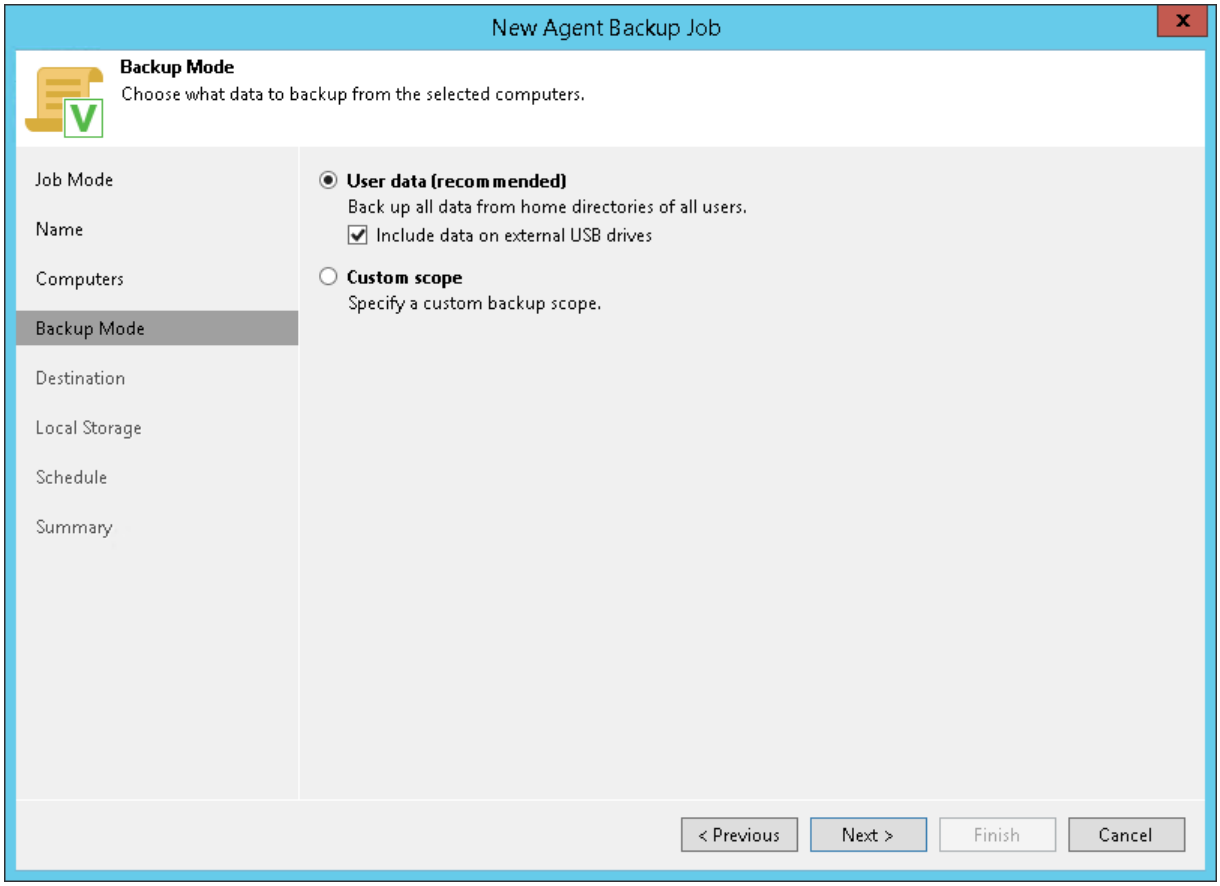
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup.

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:
   - **User data** — select this option if you want to create a backup of the *Users* folder that contains the **Home** folders of all users.

     Mind that in the **User data** mode, Veeam Agent excludes network shared folders from the backup scope. To back up network shared folders, use the **Custom scope** mode.
   - **Custom scope** — 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 Objects step of the wizard.

   > **TIP**
   >
   > If you plan to back up a network shared folder, you must select the **Custom scope** option and add this network shared folder as an individual object to the backup scope at the **Objects** step of the wizard.

2. [For the **Users data** backup mode] If you want to include in the backup one or more external USB drives, select the **Include external USB drives** check box. With this option selected, Veeam Agent will include in the backup all external USB drives that are connected to the Veeam Agent computer at the time when the backup job starts on the protected computer.



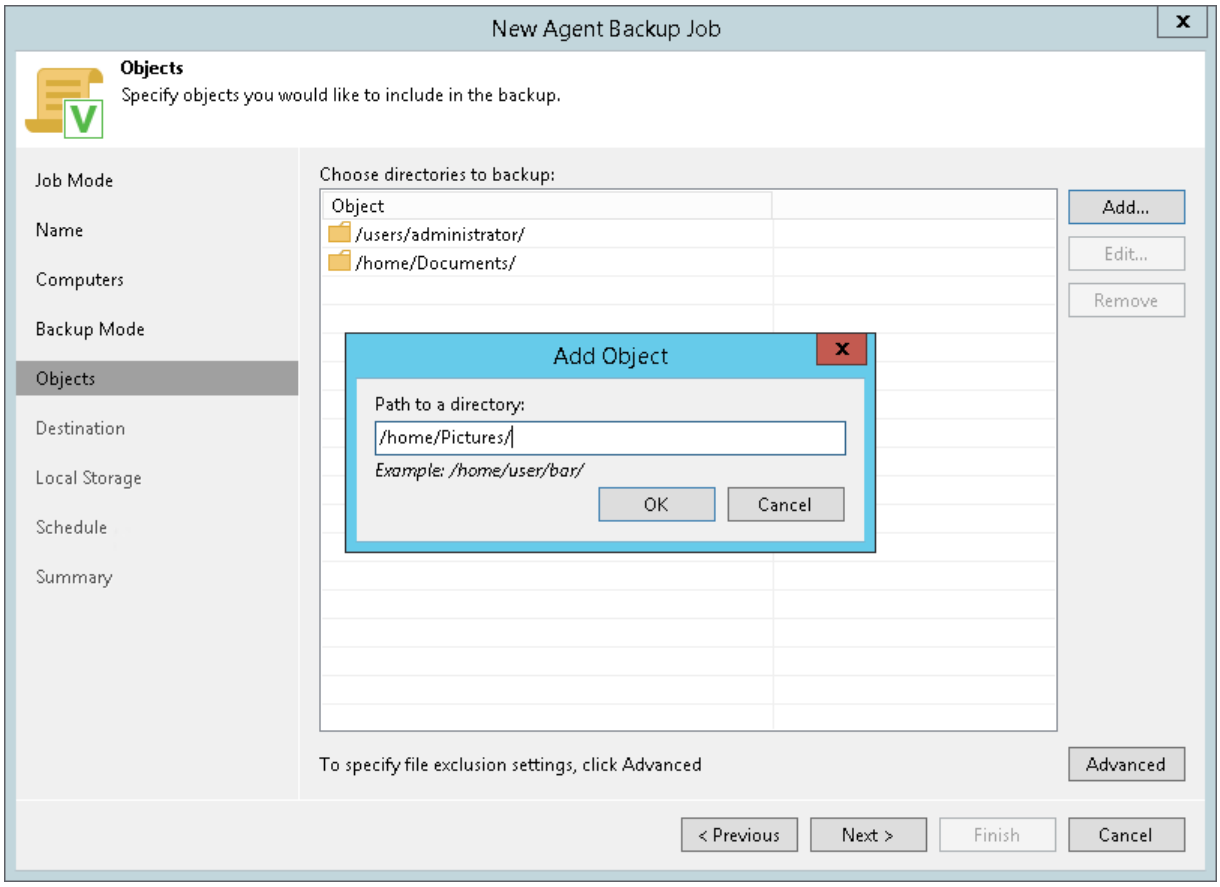
Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you have chosen the **Custom scope** mode at the Backup Mode step of the wizard.

At this step of the wizard, you must specify the backup scope — define what folders with files you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup policy. If a specified folder does not exist on one or more computers in the policy, the policy will skip such folder on those computers and back up existing ones.

To specify folders to back up:

1. In the **Choose directories to backup** field, click **Add**.
2. In the **Add Object** window, type the path to a folder that you want to back up, for example, `/home/user01`, and click **OK**.
3. Repeat steps 1-2 for all folders that you want to back up.



TIP

If you want to back up the root folder and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.

For example, you have a file system mounted to the `/Library/Media` folder. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root folder and the mounted file system, add the following objects to the backup scope:

- `/`
- `/Library/Media`

Configuring Filters

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

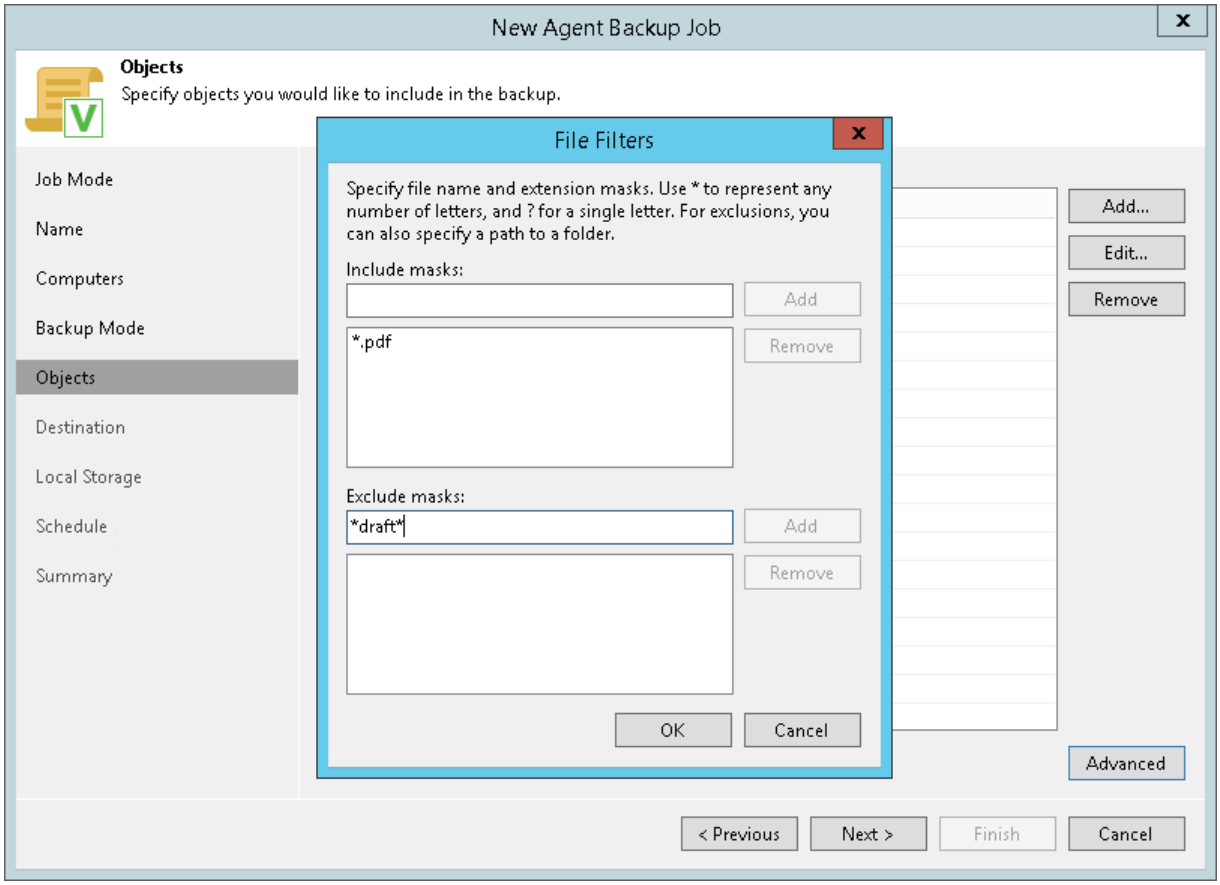
To configure a filter:

1. At the **Objects** 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, `Report.pdf` or `*filename*`. Veeam Agent will create a backup only for selected files. Other files will not be backed up.
   - In the **Exclude masks** field, specify file names and/or masks for file types that you do not want to back up, for example, `OldReports.tar.gz` or `*.odt`. Veeam Agent will back up all files except files of the specified type.
3. Click **Add**.
4. Repeat steps 2–3 for each mask that you want to add.

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

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

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



Step 7. Select Backup Destination

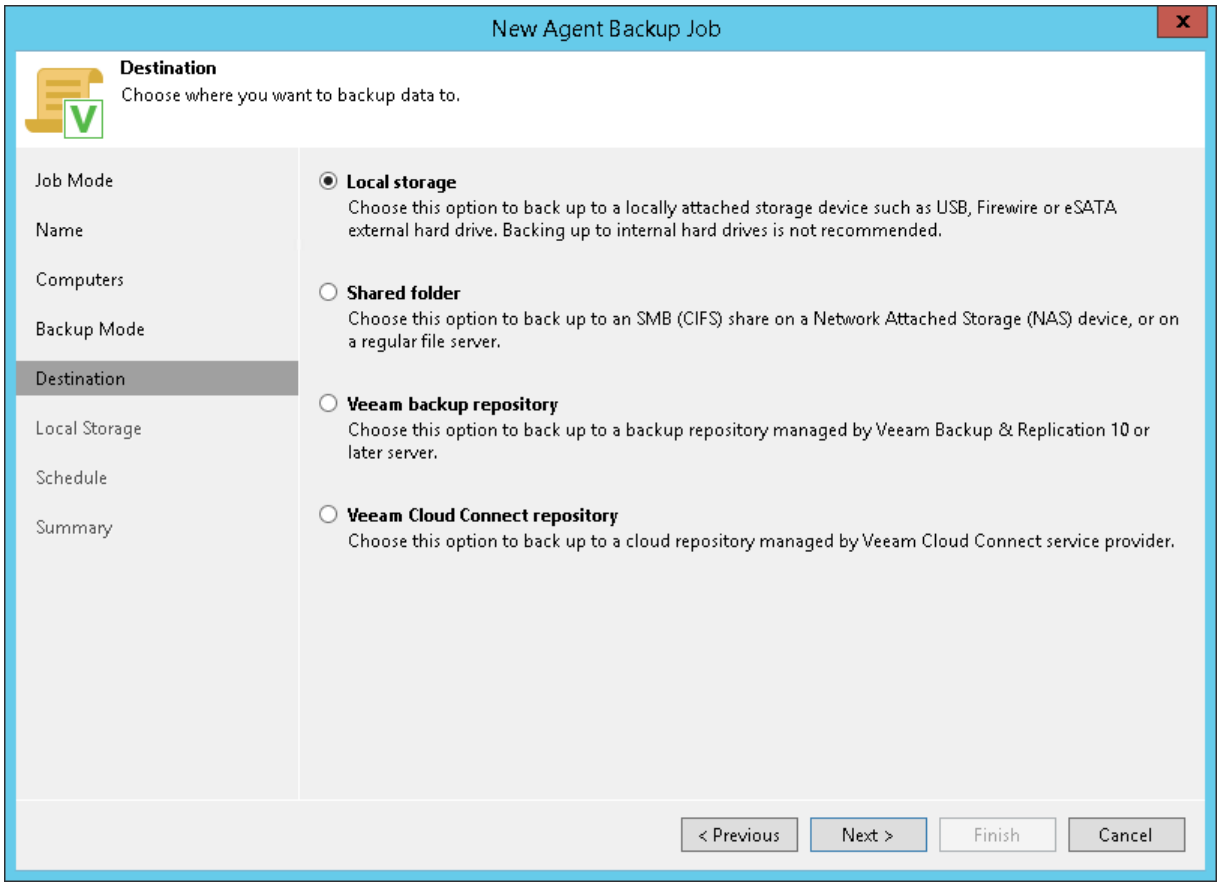
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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

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

  > **IMPORTANT**
  >
  > It is 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.

- **Shared folder** — select this option if you want to save a backup in a network shared folder. With this option selected, you will pass to the Shared folder step of the wizard.
- **Veeam backup repository** — select this option if you want to save a backup on a backup repository managed by a Veeam backup server. With this option selected, you will pass to the Backup Server step of the wizard.
- **Veeam Cloud Connect repository** — select this option if you want to save a backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the Storage step of the wizard.



Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup policy at one of the following steps of the wizard:

- Local storage settings — if you have selected the **Local storage** option at the Destination step of the wizard.
- Shared folder settings — if you have selected the **Shared folder** option at the Destination step of the wizard.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.
- Cloud repository settings — if you have selected the **Veeam Cloud Connect repository** option at the Destination step of the wizard.

Local Storage Settings

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

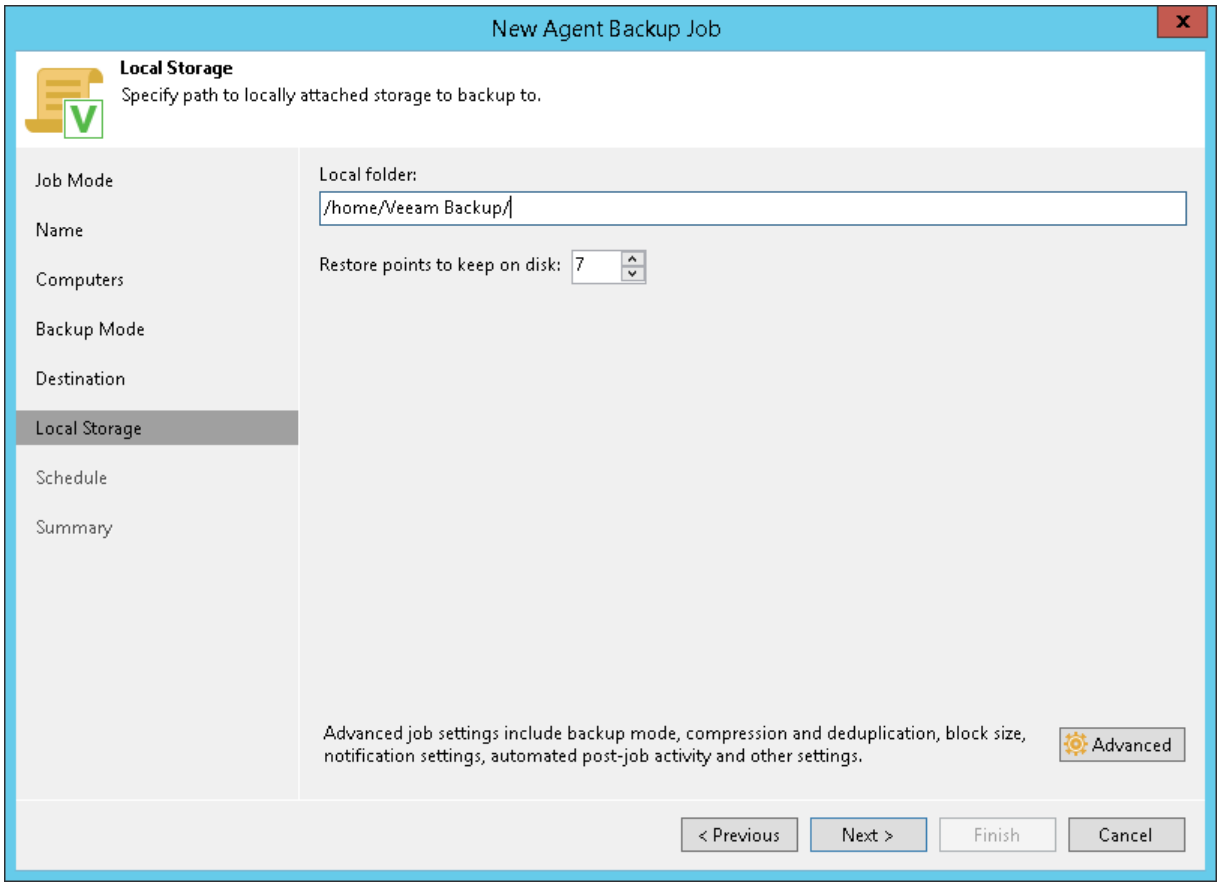
Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup policy settings to this computer.

   > **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.

2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



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:

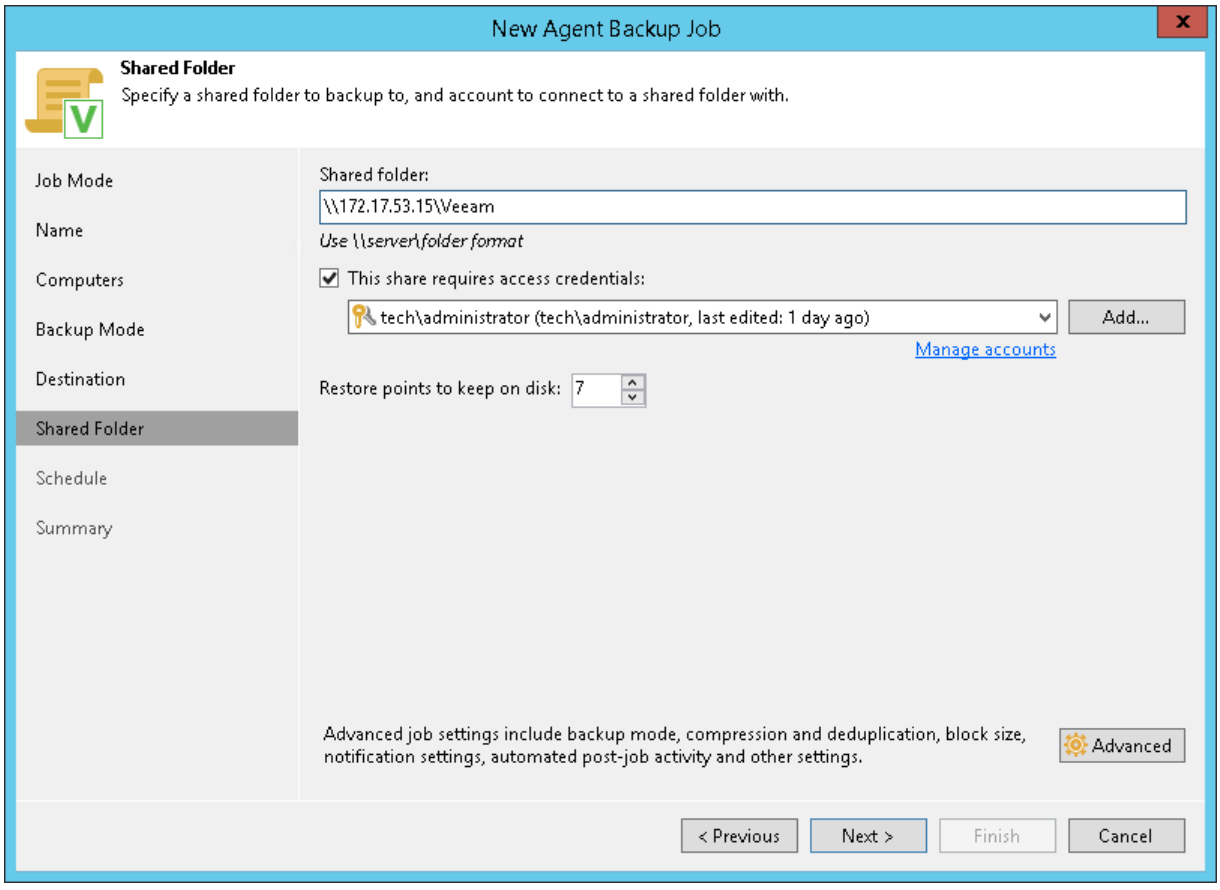
1. In the **Shared folder** field, specify a UNC name of the SMB network shared folder. The UNC name always starts with two back slashes (\\).

   Mind that Veeam Backup & Replication does not support the NFS shares for Mac computers.

2. If the SMB network shared folder requires authentication, select the **This share requires access credentials** check box and select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. The user name must be specified in the *DOMAIN\USERNAME* format.

3. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



Veeam Backup Repository Settings

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

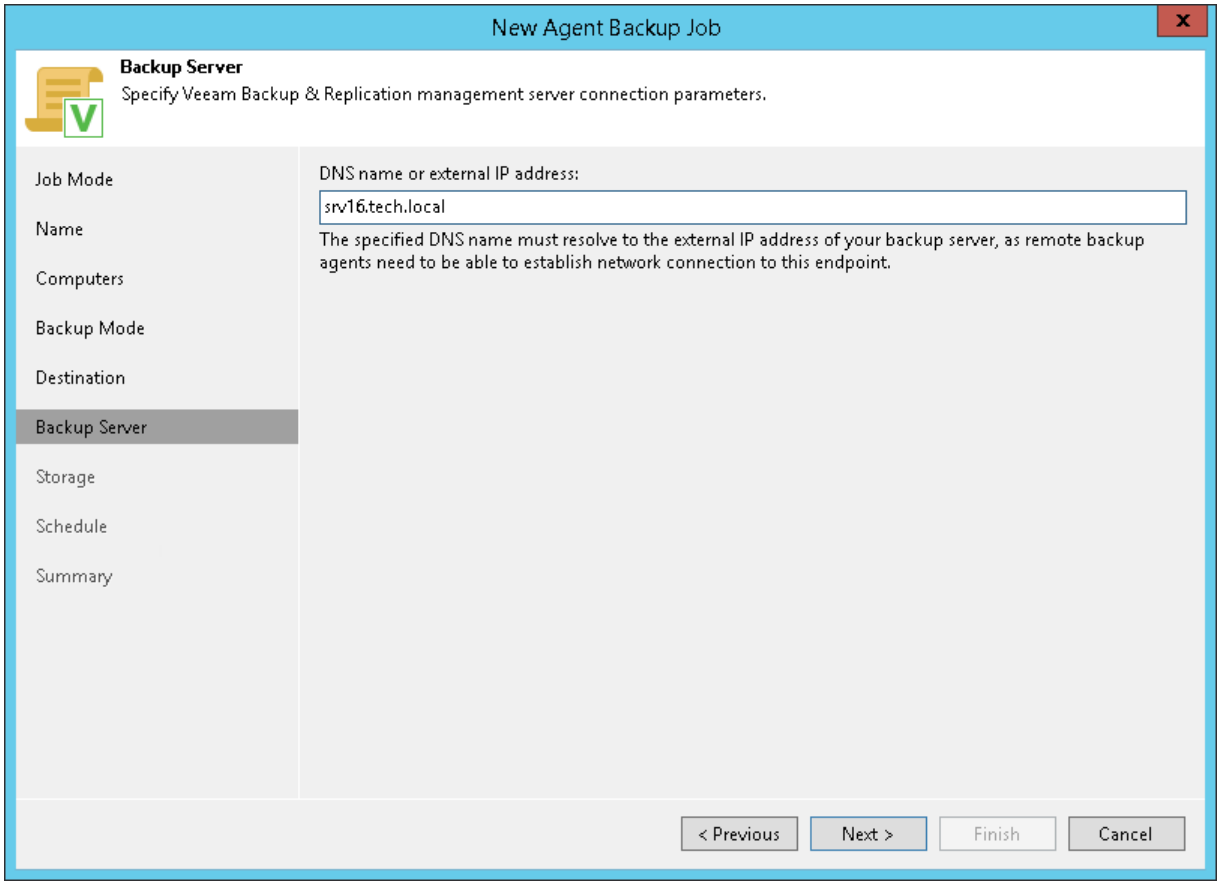
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

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

In the **DNS name or external IP address field**, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup policy. The specified DNS name or IP address must be accessible from the network to which Veeam Agent computers are connected.

> **NOTE**
>
> Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.

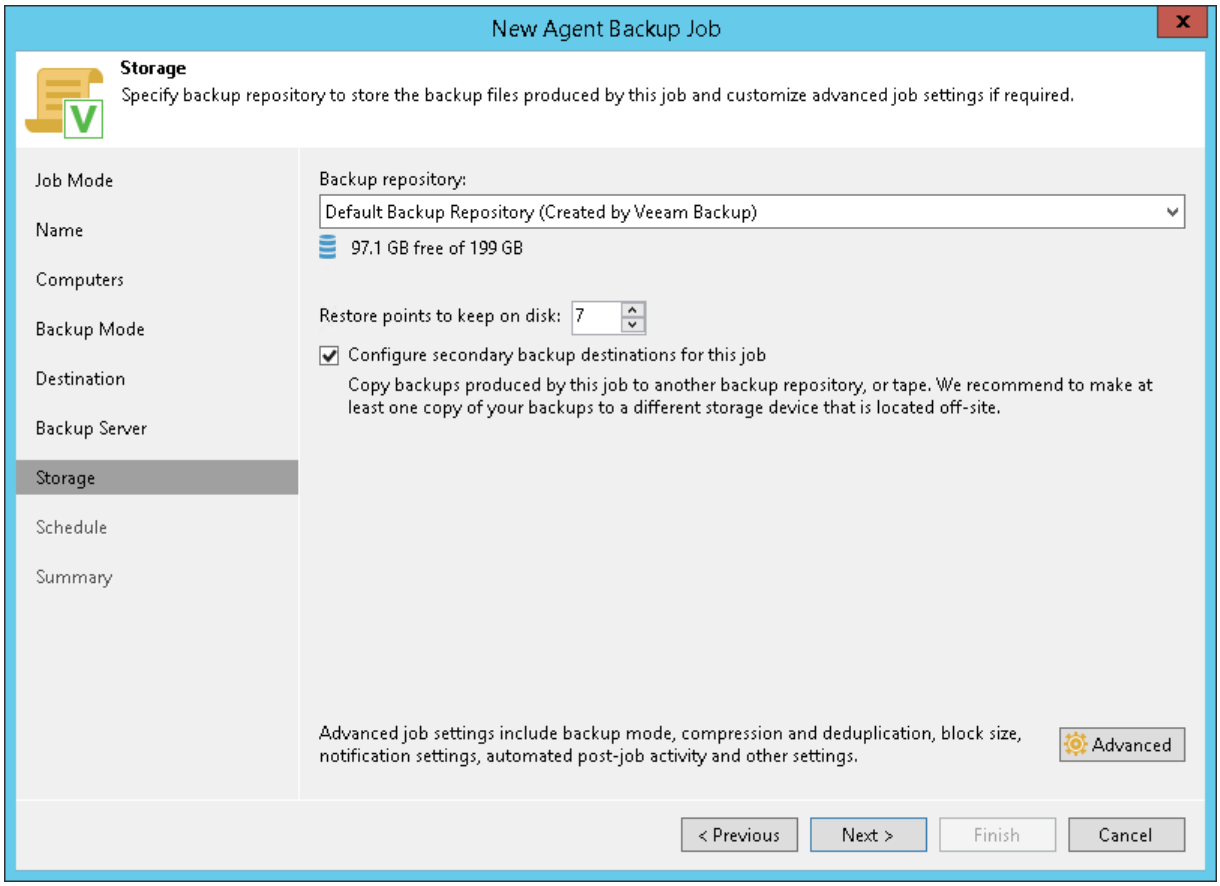


Selecting Backup Repository

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.
3. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary Target. At the **Secondary Target** step of the wizard, you can link the backup policy to the backup copy job or backup to tape backup job.

   You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.
4. Click **Advanced** to specify advanced settings for the backup policy. To learn more, see Specify Advanced Backup Settings.



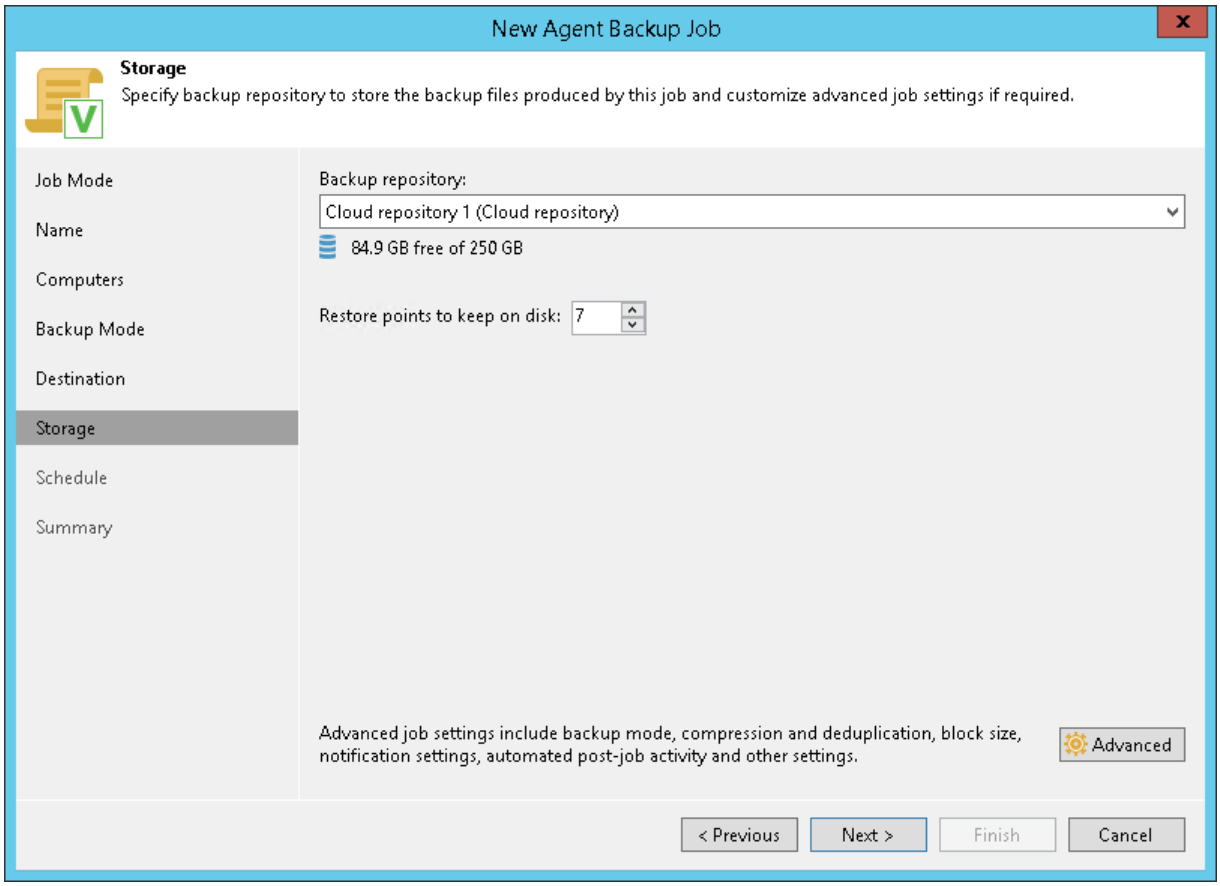
Cloud Repository Settings

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

> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

Specify settings for the cloud repository:

1. From the **Backup repository** list, select a cloud repository where you want to store created backups. The **Backup repository** list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication automatically checks how much free space is available on the repository.
2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.
3. Click **Advanced** to specify advanced settings for the backup policy. To learn more, see Specify Advanced Backup Settings.



Step 9. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the Veeam Agent backup policy:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings

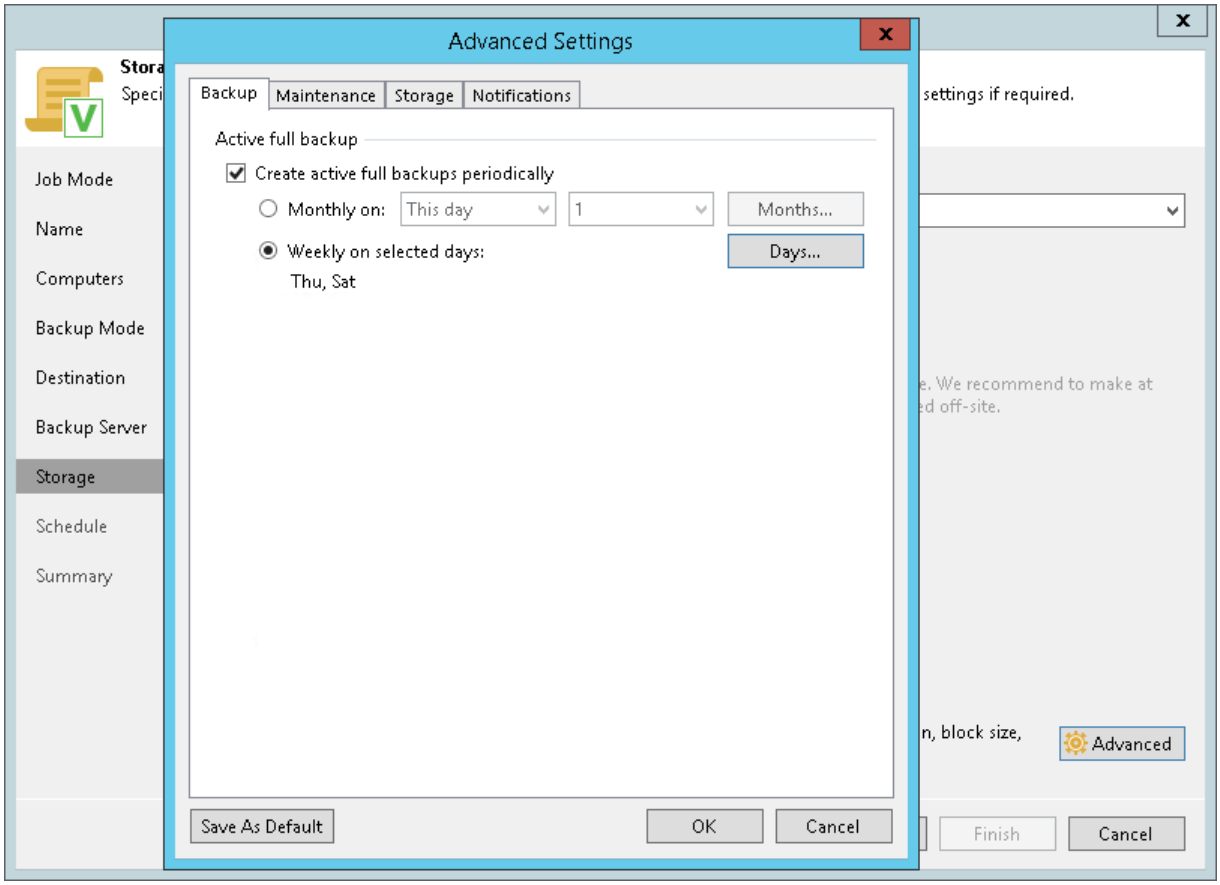
> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

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

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
2. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

> **NOTE**
>
> Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.



Maintenance Settings

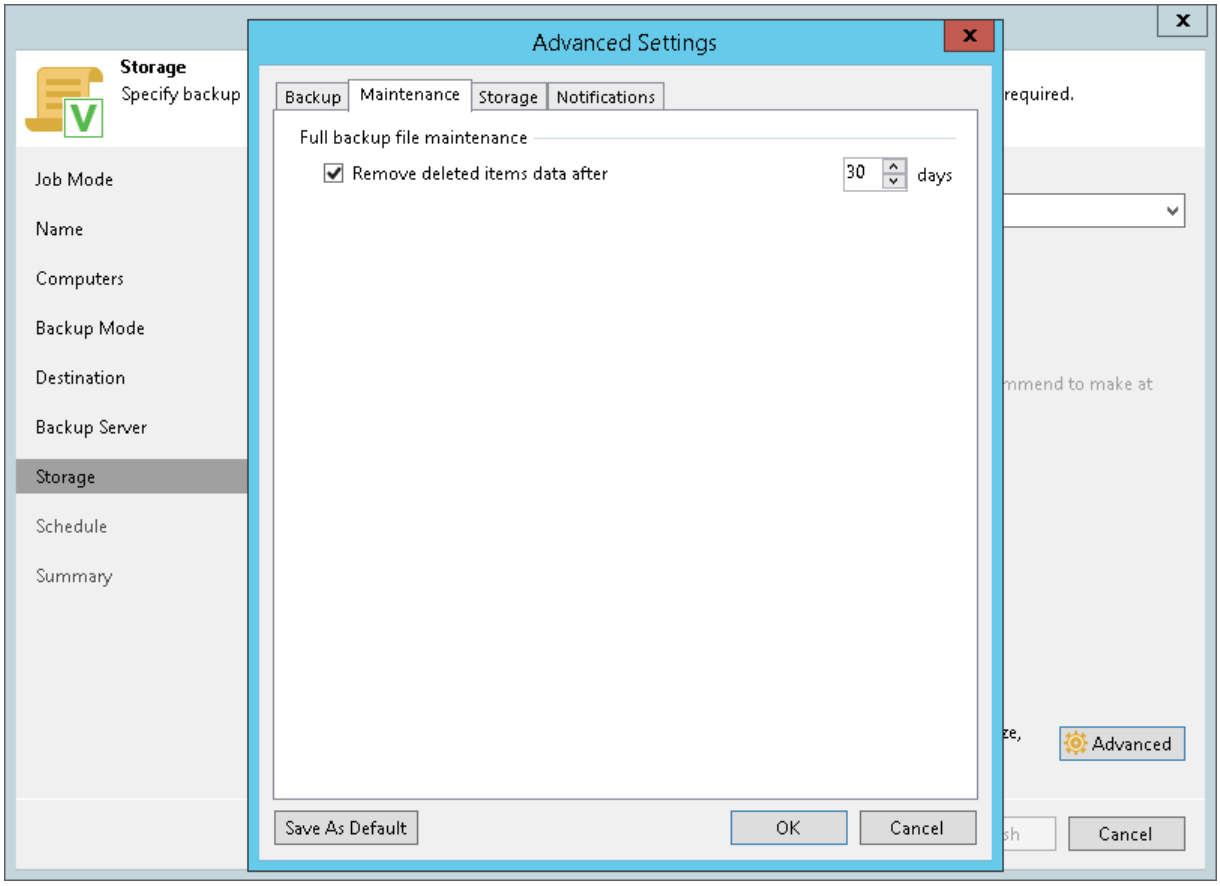
You can specify maintenance settings for a backup policy targeted at a Veeam backup repository. Maintenance operations help make sure that the backup chain remains valid and consistent.

To specify maintenance settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup policy in the target location.

   If Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location.

   By default, the deleted items data retention period is 30 days. Do not set the deleted items retention period to 1 day or a similar short interval. Otherwise, the backup policy may not work as expected and remove data that you still require.

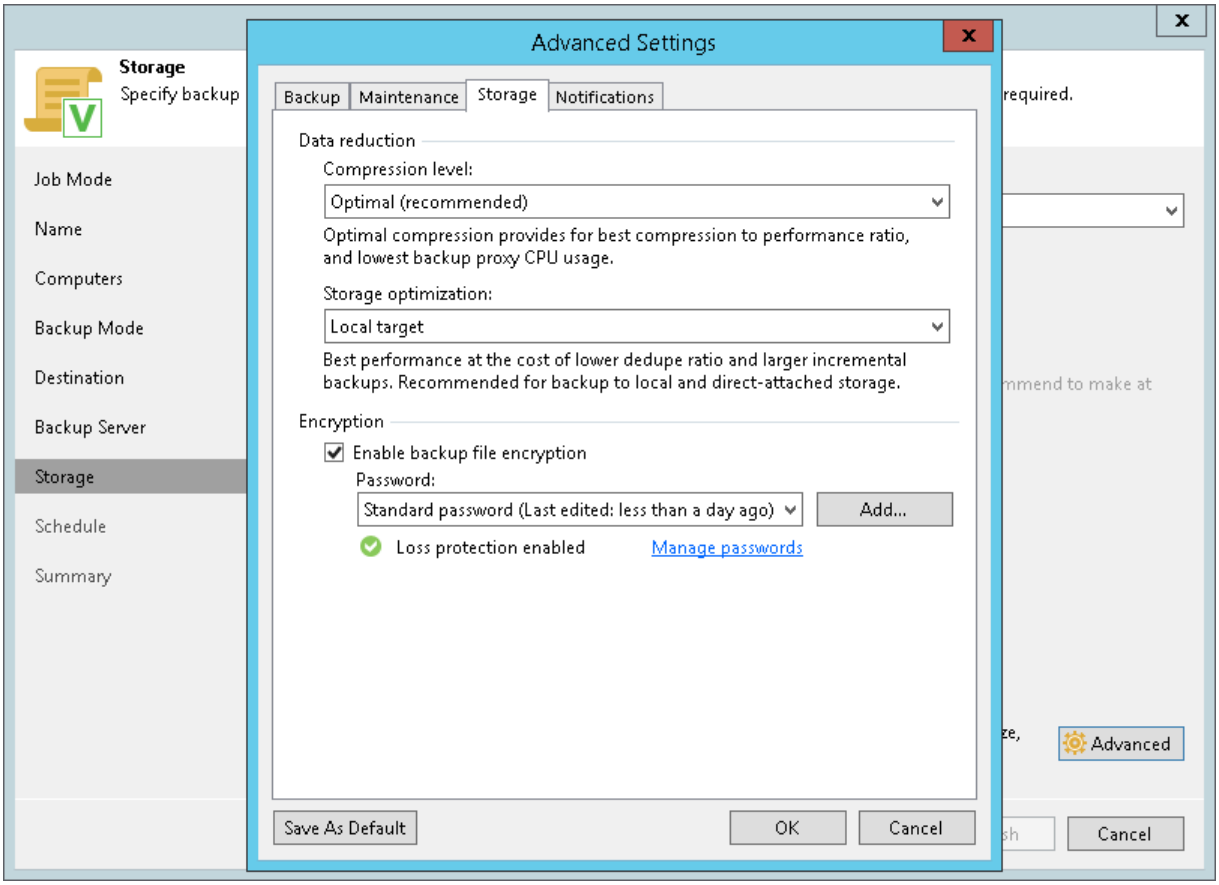


Storage Settings

To specify storage settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
2. Click the **Storage** tab.
3. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
4. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Agent will use data blocks of different size to optimize the size of backup files and policy performance.
5. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see the Password Manager section in the Veeam Backup & Replication User Guide.

   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.



NOTE

Consider the following:

- Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer or at a network shared folder. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.
- If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.
- If you enable encryption for an existing Veeam Agent backup job or policy, during the next session Veeam Agent will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.
- Encryption is not retroactive. If you enable encryption for an existing backup job or policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this job.
- When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

  This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.

Notification Settings

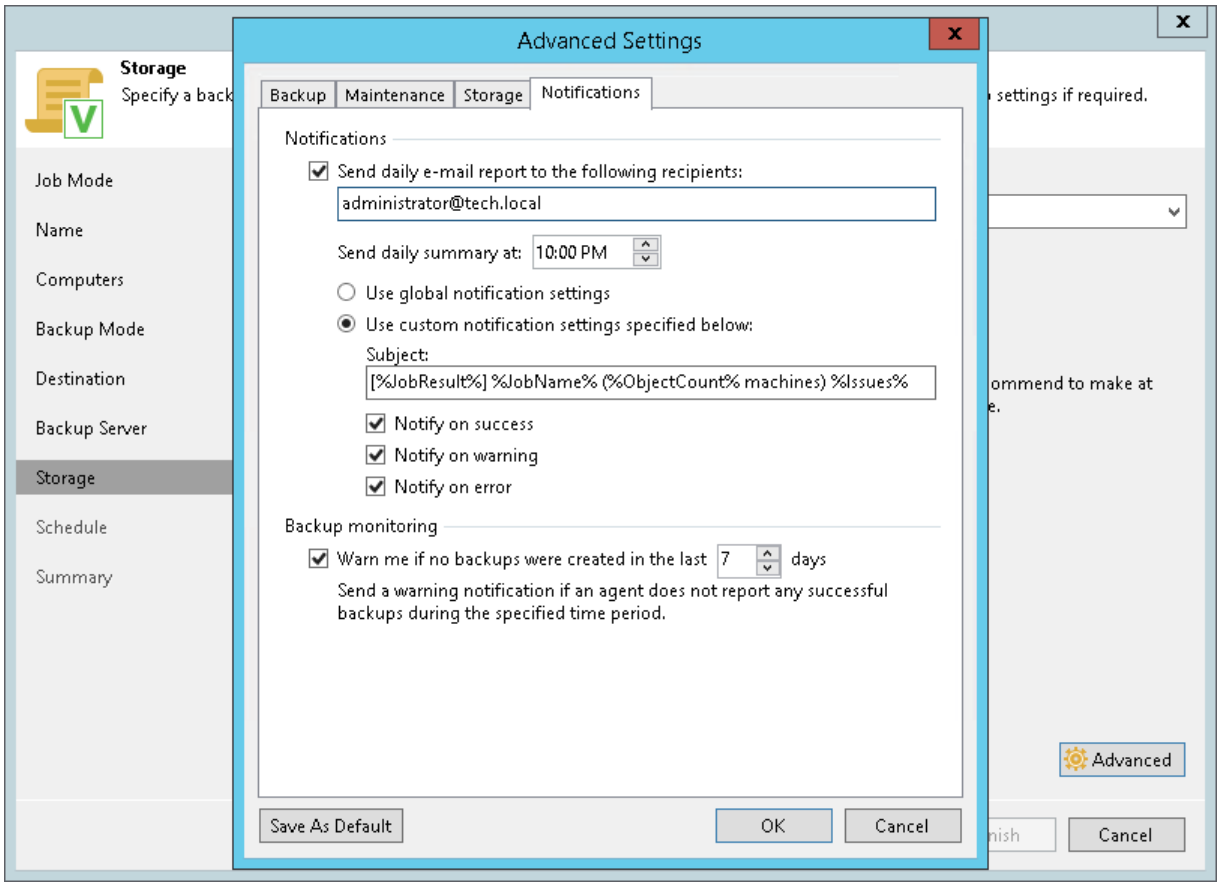
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup policy sessions performed for the last 24-hour period on computers to which the backup policy is applied.

> **NOTE**
>
> Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the backup policy, Veeam Backup & Replicationwill send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will sent the report daily at the specified time.
5. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing backup policy statistics at 8:00 AM daily.
   - To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the backup policy) and *%Issues%* (number of machines in the backup policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the policy completes successfully, completes with a warning or fails.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Step 10. Specify Secondary Target

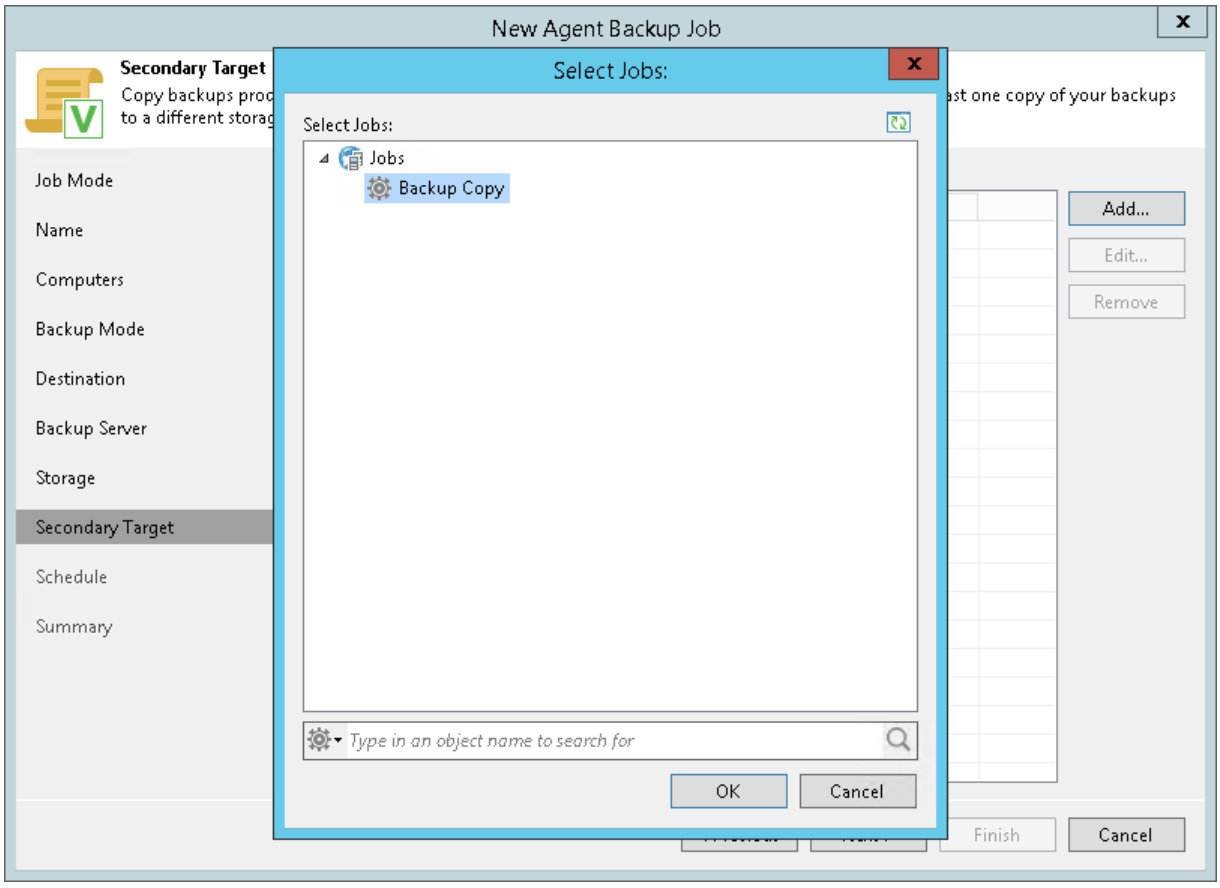
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup job to a backup to tape or backup copy job. As a result, the backup job will be added as a source to the backup to tape or backup copy job. Backup files created with the backup job will be archived to tape or copied to the secondary backup repository according to the secondary jobs schedule. For more information, see Linking Backup Jobs to Backup Copy Jobs and Linking Backup Jobs to Backup to Tape Jobs in the Veeam Backup & Replication User Guide.

The backup to tape job or backup copy job must be configured beforehand. You can create these jobs with an empty source. When you link the Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent backup job as a source for these jobs.

To link jobs:

1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom of the wizard.



Step 11. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup. Backup job scheduling options differ depending on the job mode that you have selected at the Job Mode step of the wizard:

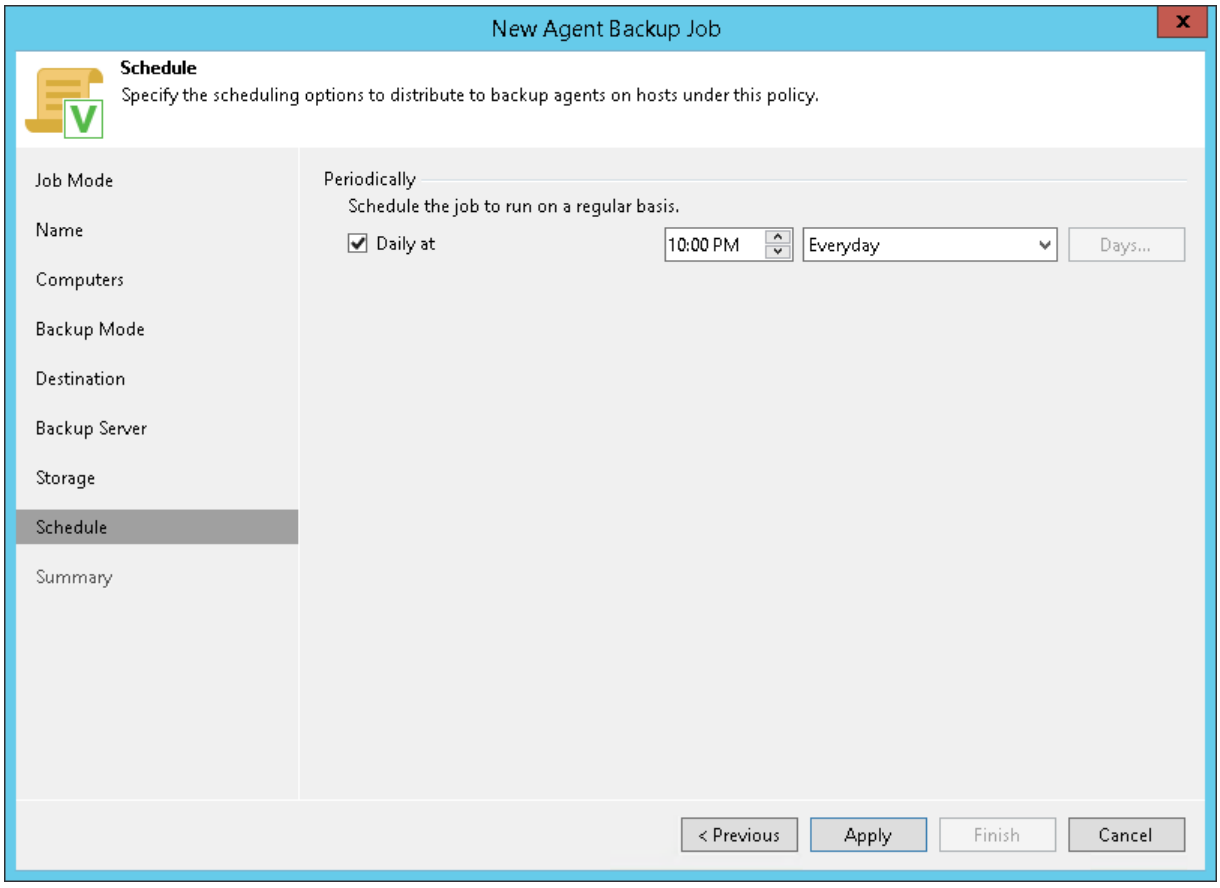
- Scheduling Settings for Workstations
- Scheduling Settings for Servers

Scheduling Settings for Workstations

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

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.

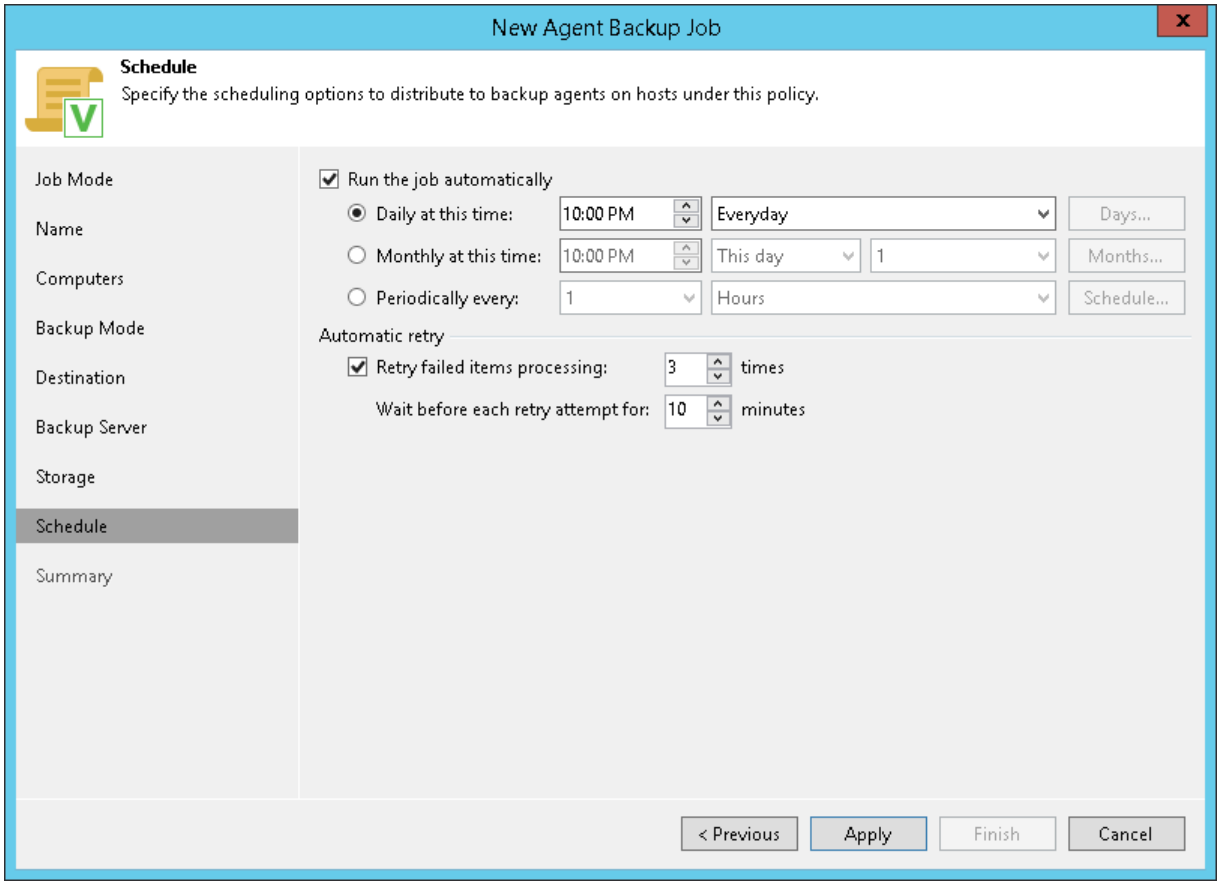


Scheduling Settings for Servers

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.
3. In the **Automatic retry** section, define whether Veeam Agent must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Agent for Mac will retry the job for the defined number of times without any time intervals between the job runs.



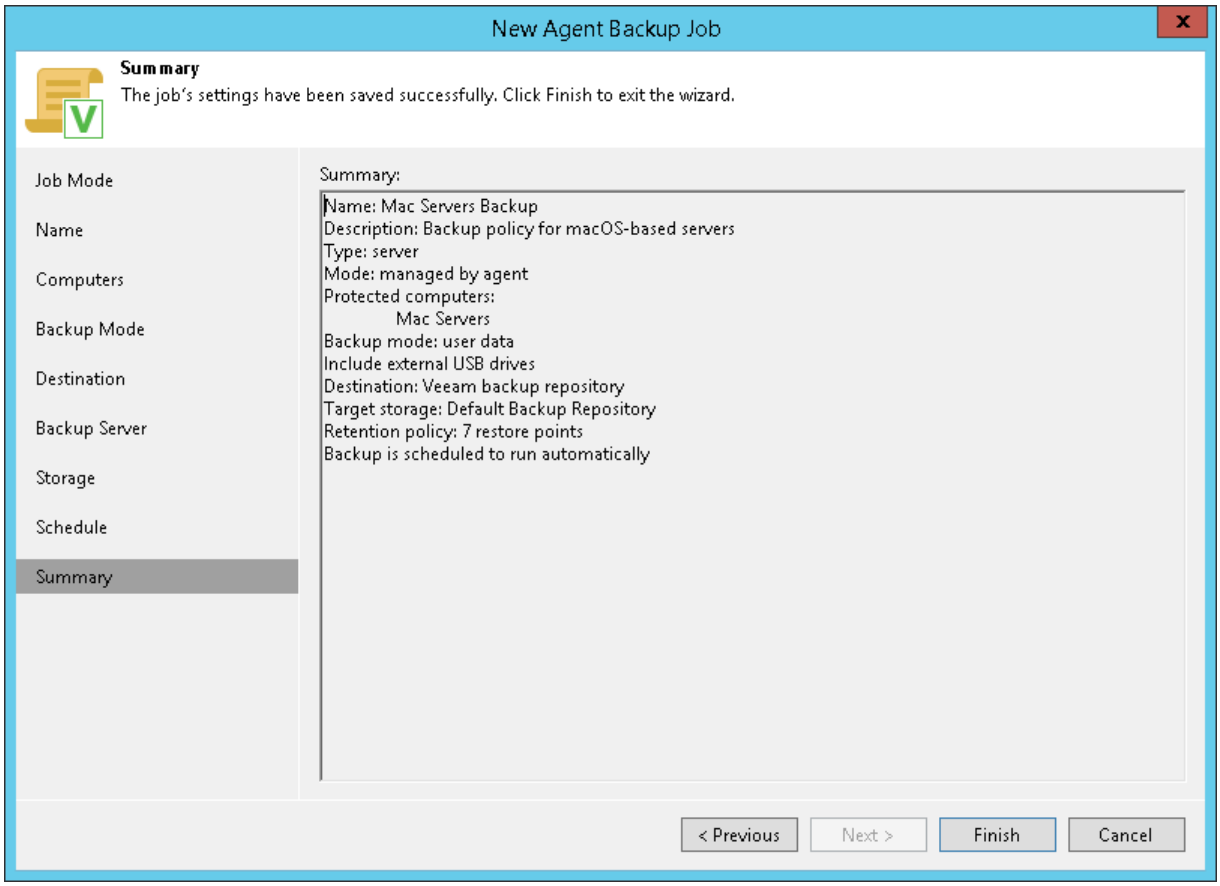
Step 12. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup policy configuration process.

1. Review settings of the configured backup policy.
2. Click **Finish** to close the wizard.

Keep in mind that Veeam Backup & Replication does not apply backup policy to Mac computers immediately. Veeam Agents installed on Mac computers connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Mac Configuration.



Managing Veeam Agent Backup Jobs

You can use the Veeam Backup & Replication console to perform the following operations with a Veeam Agent backup job managed by the backup server:

- Start and stop a Veeam Agent backup job.
- Retry a Veeam Agent backup job.
- Perform active full backup.
- Edit Veeam Agent backup job settings.
- Enable and disable a Veeam Agent backup job.
- Clone a Veeam Agent backup job.
- Remove a Veeam Agent backup job.

Starting and Stopping Veeam Agent Backup Job

You can start a Veeam Agent backup job manually, for example, if you want to create an additional restore point in the backup chain and do not want to change the job schedule. You can also stop a job, for example, if processing of a Veeam Agent computer is about to take long, and you do not want the job to produce workload on the production environment during business hours.

Starting Jobs

To start a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Start** on the ribbon or right-click the job and select **Start**.

Stopping Jobs

You can stop a Veeam Agent backup job in one of the following ways:

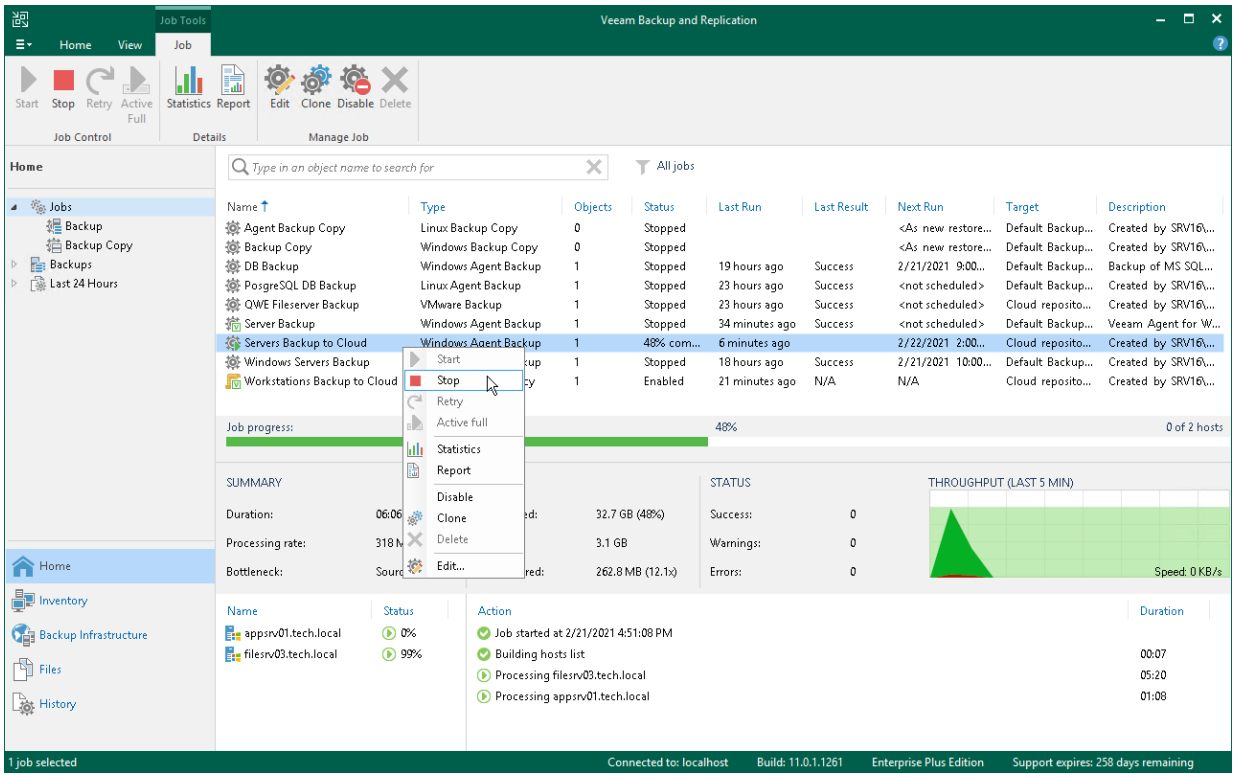
- Stop job immediately. In this case, Veeam Backup & Replication will produce a new restore point only for those computers in the job that have already been processed by the time you stop the job.
- Stop job gracefully. In this case, Veeam Backup & Replication will produce a new restore point only for those computers in the job that have already been processed and for computers that are being processed at the moment.

To stop a job immediately:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Stop** on the ribbon or right-click the job and select **Stop**. In the displayed window, click **Immediately**.

To stop a job gracefully:

1. Open the **Home** view.
2. In the inventory pane, click **Jobs**.
3. In the working area, right-click the job and select **Stop**. In the displayed window, click **Gracefully**.

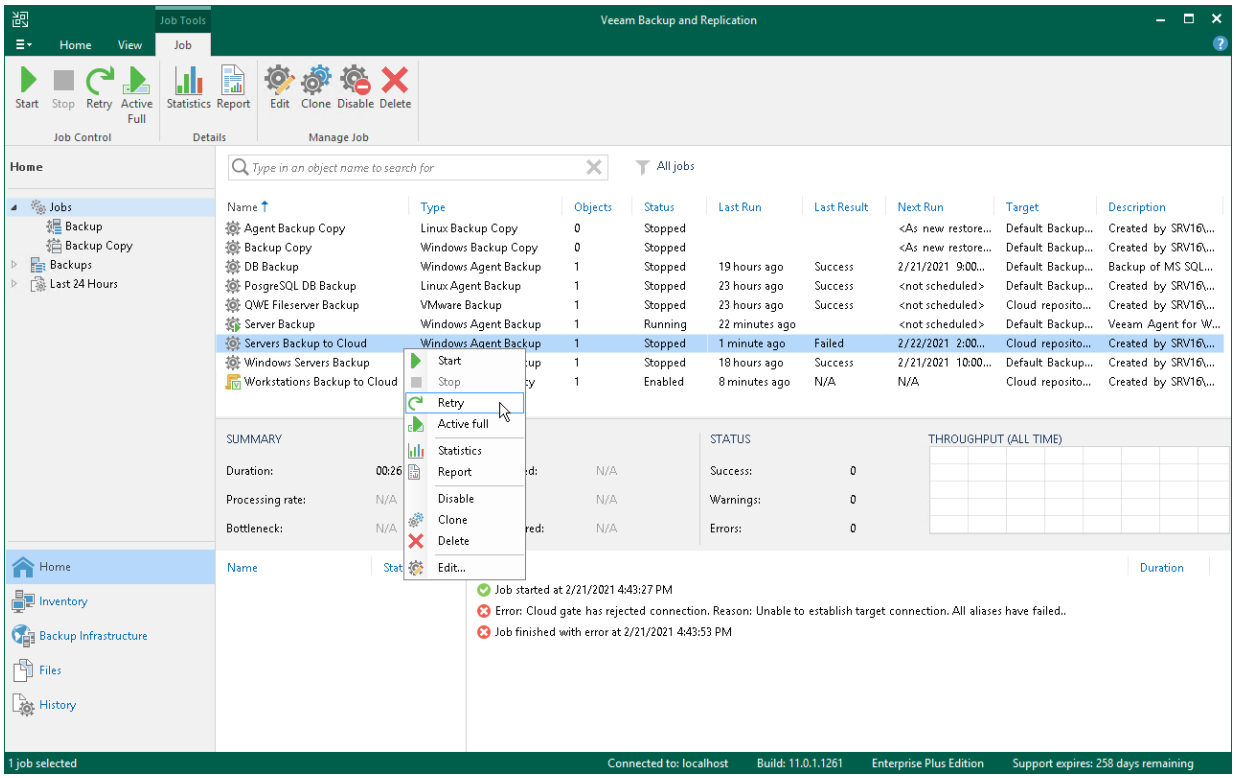


Retrying Veeam Agent Backup Job

You can manually retry a Veeam Agent backup job configured in Veeam Backup & Replication if the job failed during the previous job session. When you retry a Veeam Agent backup job, Veeam Backup & Replication processes only those computers in the job that were not processed successfully during the previous job session.

To retry a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Retry** on the ribbon or right-click the job and select **Retry**.

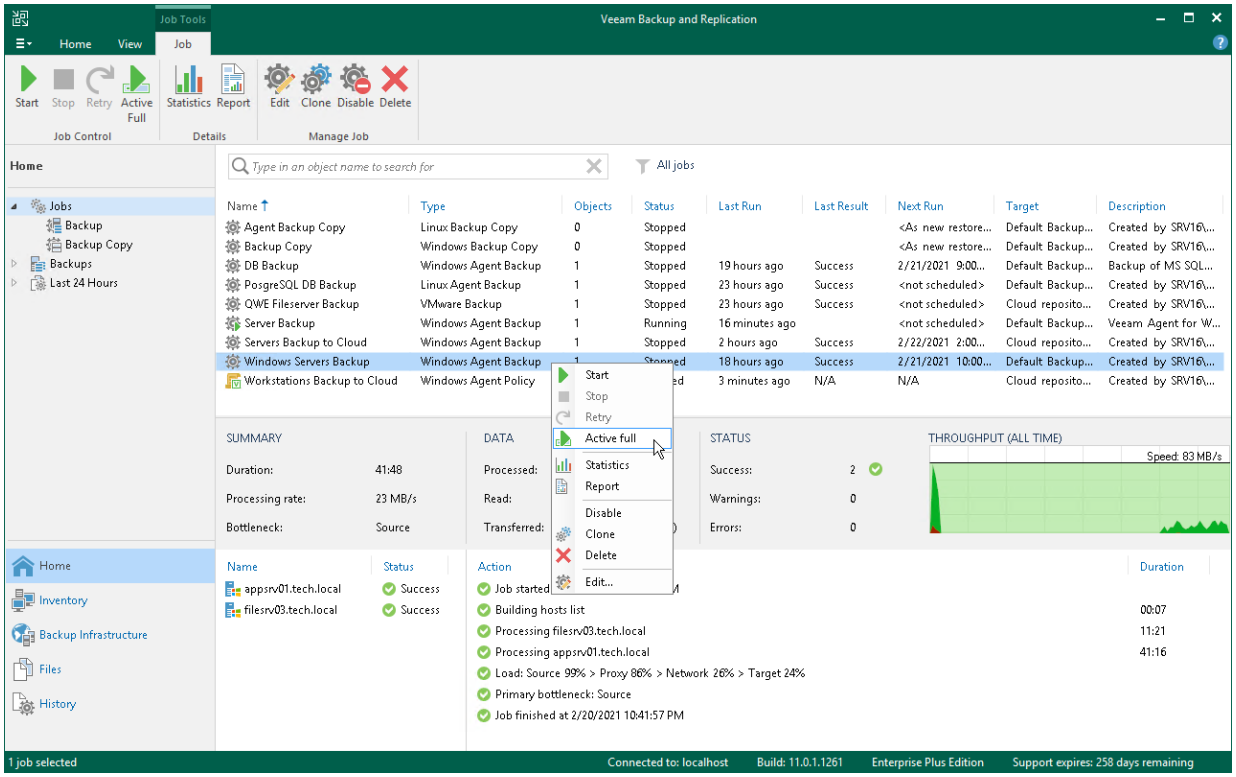


Performing Active Full Backup

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

To perform active full backup:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Active Full** on the ribbon or right-click the job and select **Active Full**.



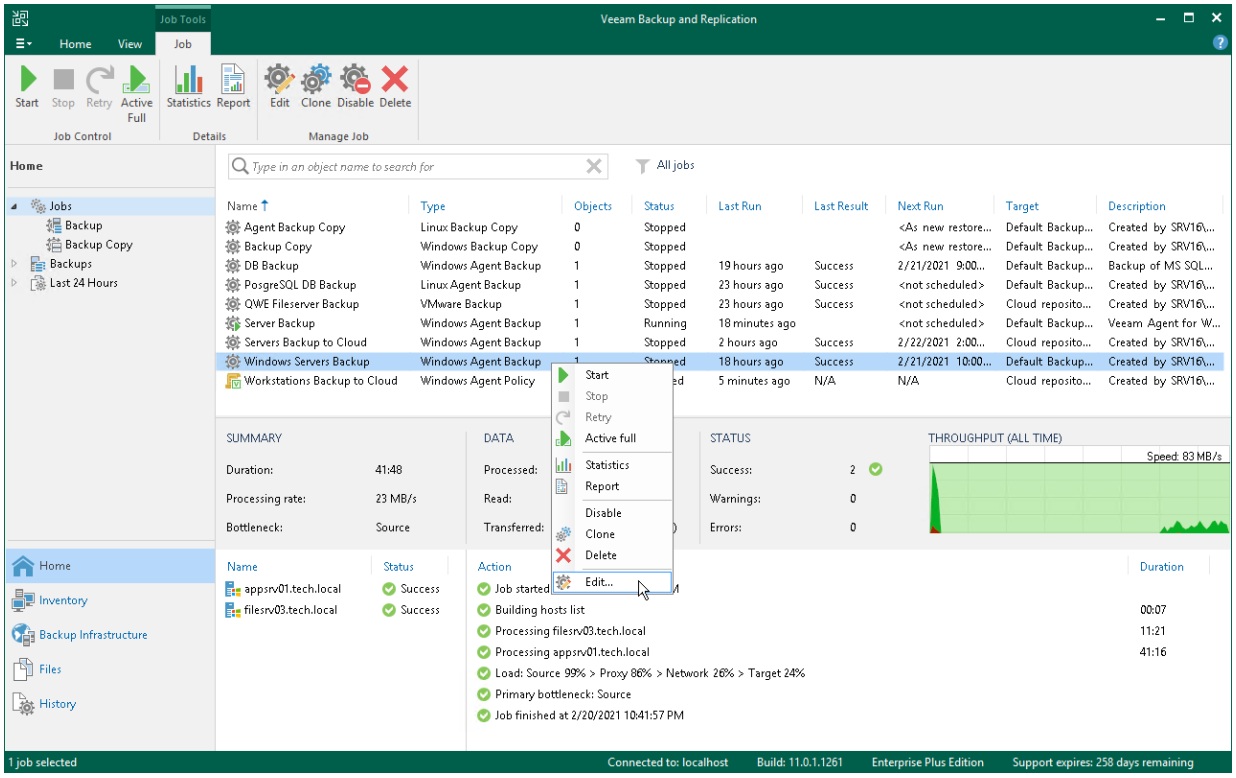
Editing Veeam Agent Backup Job Settings

You can edit Veeam Agent backup jobs configured in Veeam Backup & Replication at any time. For example, you may want to edit a backup job to change the backup scope, target location or job scheduling settings.

> **NOTE**
>
> Mind the following:
>
> - You cannot change the type of protected computers added to the job and the job mode (that is, change a Veeam Agent backup job to a backup policy and vice versa).
> - If you want to specify another backup repository as a target for backups created by the job, you must delete backups from the old repository or move backups to the new repository prior to changing a backup repository in the job settings.
> - [For Veeam Agent backup jobs for Linux computers] You cannot change the backup mode from file-level to volume-level and vice versa.

To edit job settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Edit** on the ribbon or right-click the job and select **Edit**.
4. Complete the steps of the **Edit Agent Backup Job** wizard to change the job settings as required.



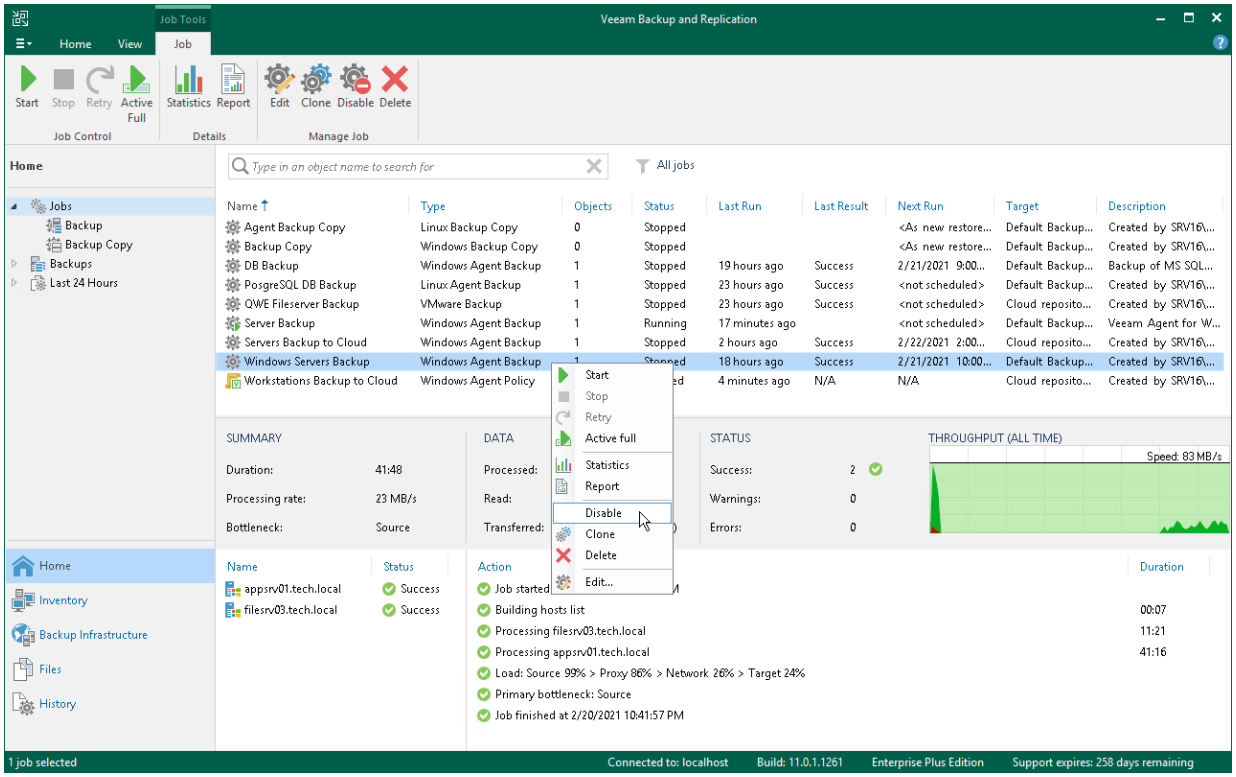
Enabling and Disabling Veeam Agent Backup Job

You can temporary disable Veeam Agent backup jobs configured in Veeam Backup & Replication. When you disable a job, Veeam Backup & Replication does not start the job by the specified schedule. You can start a disabled job manually at any time you need. You can also enable a disabled job at any time.

To disable a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Disable** on the ribbon or right-click the job and select **Disable**.

To enable a disabled job, select it in the list and click **Disable** on the ribbon once again.



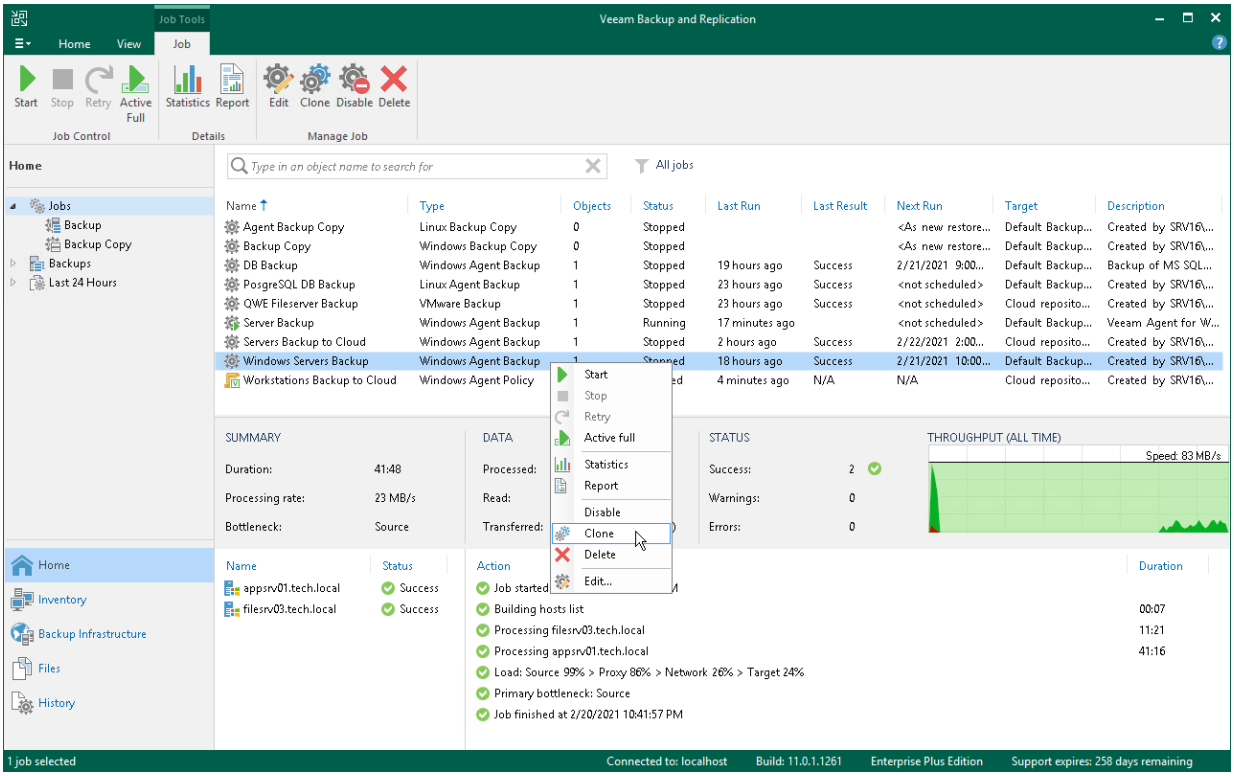
Cloning Veeam Agent Backup Job

You can clone Veeam Agent backup jobs configured in Veeam Backup & Replication. For example, you may want to configure a Veeam Agent backup job that will be used as a 'job template', and use this job to create multiple jobs with similar settings.

To clone a Veeam Agent backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Clone** on the ribbon or right-click the job and select **Clone**.
4. After a job is cloned, you can edit all its settings, including the job name.

> **NOTE**
>
> The job cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

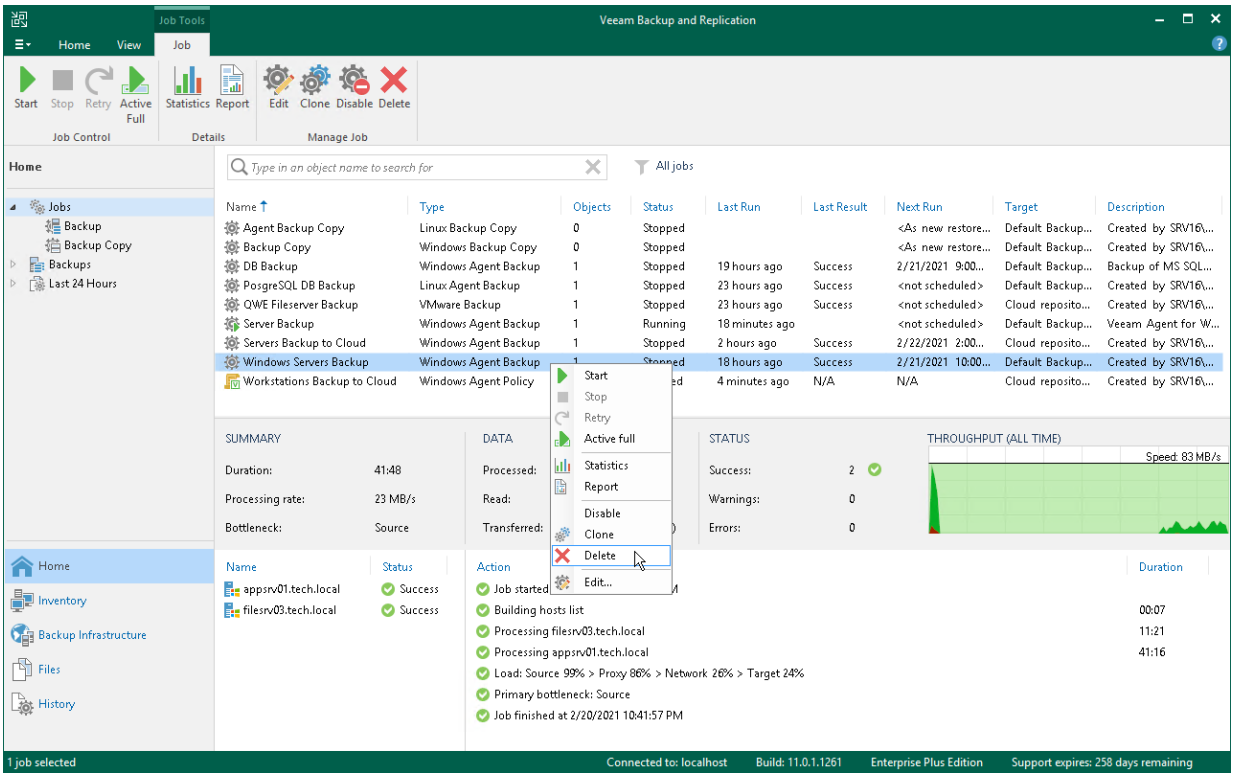


Removing Veeam Agent Backup Job

You can permanently remove a Veeam Agent backup job from Veeam Backup & Replication. When you remove a job, Veeam Agent backups created by this job remain intact on the backup repository. In the Veeam Backup & Replication console, such backups are displayed in the **Home** view, under the **Backups** > **Imported** node in the inventory pane.

To remove a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Delete** on the ribbon or right-click the job and select **Delete**.



Managing Veeam Agent Backup Policies

You can use the Veeam Backup & Replication console to perform the following operations with a Veeam Agent backup job managed by Veeam Agent (a Veeam Agent backup policy):

- Apply backup policy to Veeam Agent computers.
- Start and stop Veeam Agent backup jobs on computers added to the backup policy.
- Perform active full backup on computers added to the backup policy.
- Clear the backup cache on computers added to the backup policy.
- Edit backup policy settings.
- Enable and disable a backup policy.
- Clone a backup policy.
- Remove a backup policy.

Applying Backup Policy to Protected Computers

To configure individual Veeam Agent backup jobs on protected computers added to a backup policy, Veeam Backup & Replication applies settings of the backup policy to these computers. This operation is performed automatically at the time when the backup policy is created and at the process of automatic protection group rescan. You can also apply backup policy settings manually at any time. This may be required, for example, in case one or more protected computers could not be accessed over the network at the time when the backup policy was created.

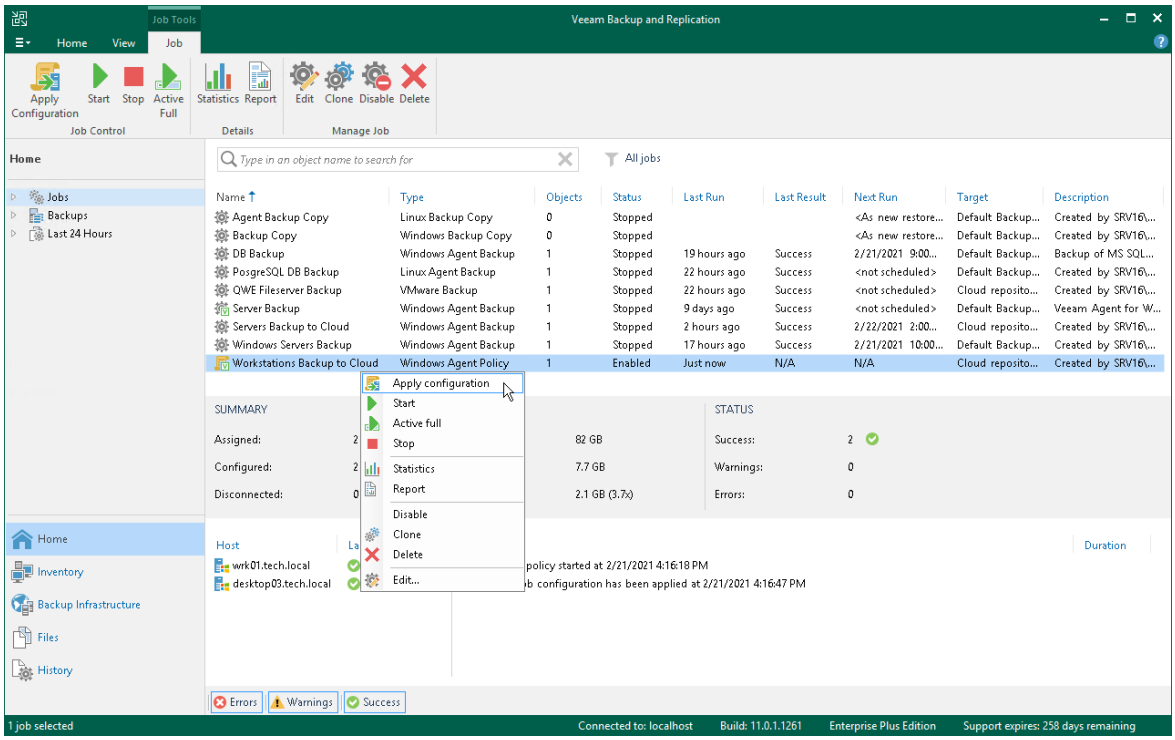
To assign a backup policy to protected computers:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Apply Configuration** on the ribbon or right-click the policy and select **Apply configuration**.

   Keep in mind that Veeam Backup & Replication does not apply backup policy to protection groups for pre-installed Veeam Agents and their members immediately. Veeam Agents installed on computers included in such protection groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If a backup policy is targeted at the Veeam backup server and the backup policy session is scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next session start.

   If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see one of the following sections depending on the Veeam Agent you use:

   - Veeam Agent for Microsoft Windows Configuration
   - Veeam Agent for Linux Configuration
   - Veeam Agent for Unix Configuration
   - Veeam Agent for Mac Configuration



Starting and Stopping Backup

You can manually start backup on Veeam Agent computers added to the backup policy, for example, if you want to create an additional restore point in the backup chain and do not want to change the backup schedule. You can also stop the backup process, for example, if processing of a Veeam Agent computer is about to take long, and you do not want the backup process to produce workload on the production environment during business hours.

When you start the backup process for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to start backup jobs on these computers.

When you stop the backup process for a backup policy, Veeam Backup & Replication does not apply the policy to Veeam Agent computers and immediately sends a command to stop backup jobs on these computers.

Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the start or stop operation will be performed only on those computers that received the command from the backup server.

Keep in mind that you cannot start or stop the backup process for protection groups for pre-installed Veeam Agents and their members. Veeam Agent computers included in such protection groups will be skipped and Veeam Backup & Replication will display a warning message in a backup policy session statistics.

Starting Backup

To start backup on Veeam Agent computers added to the backup policy:

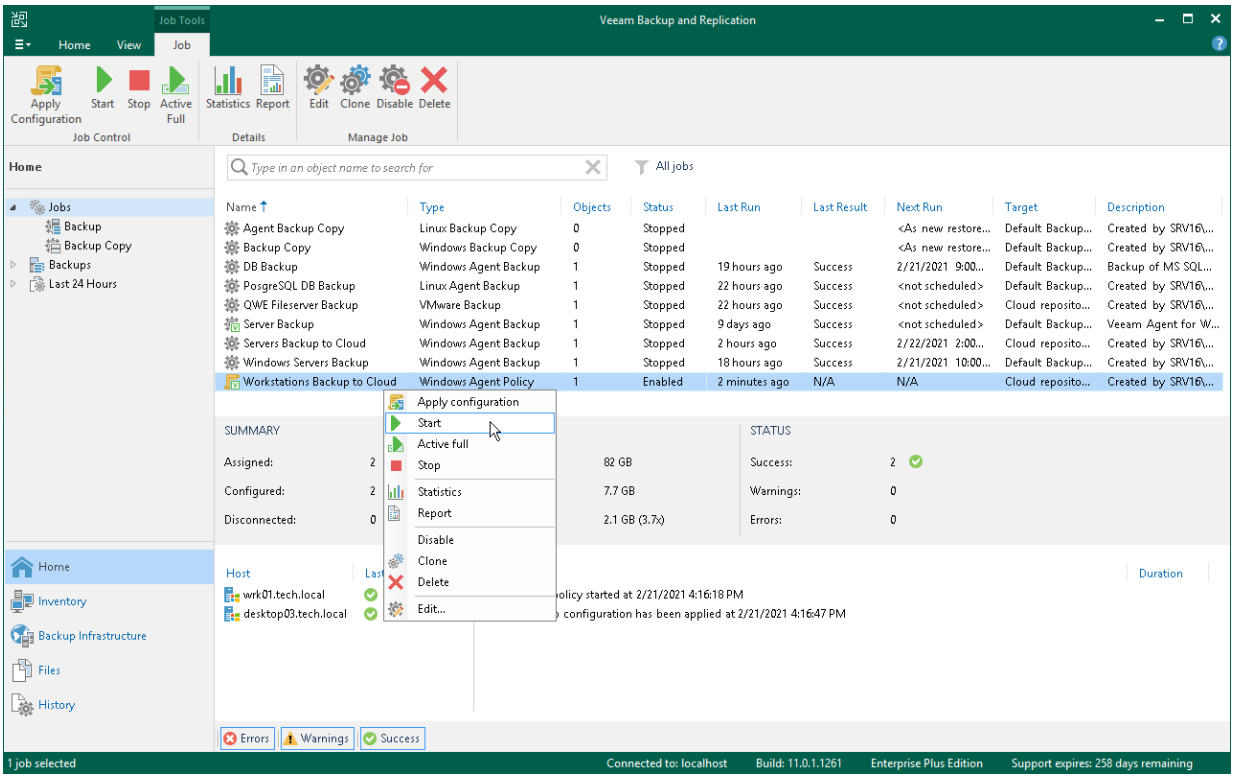
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Start** on the ribbon or right-click the job and select **Start**.

> **TIP**
>
> You can also start a Veeam Agent backup job directly on a protected computer from the Veeam Agent user interface.

Stopping Backup

To stop backup on Veeam Agent computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Stop** on the ribbon or right-click the job and select **Stop**. In the displayed window, click **Yes**.



Performing Active Full Backup

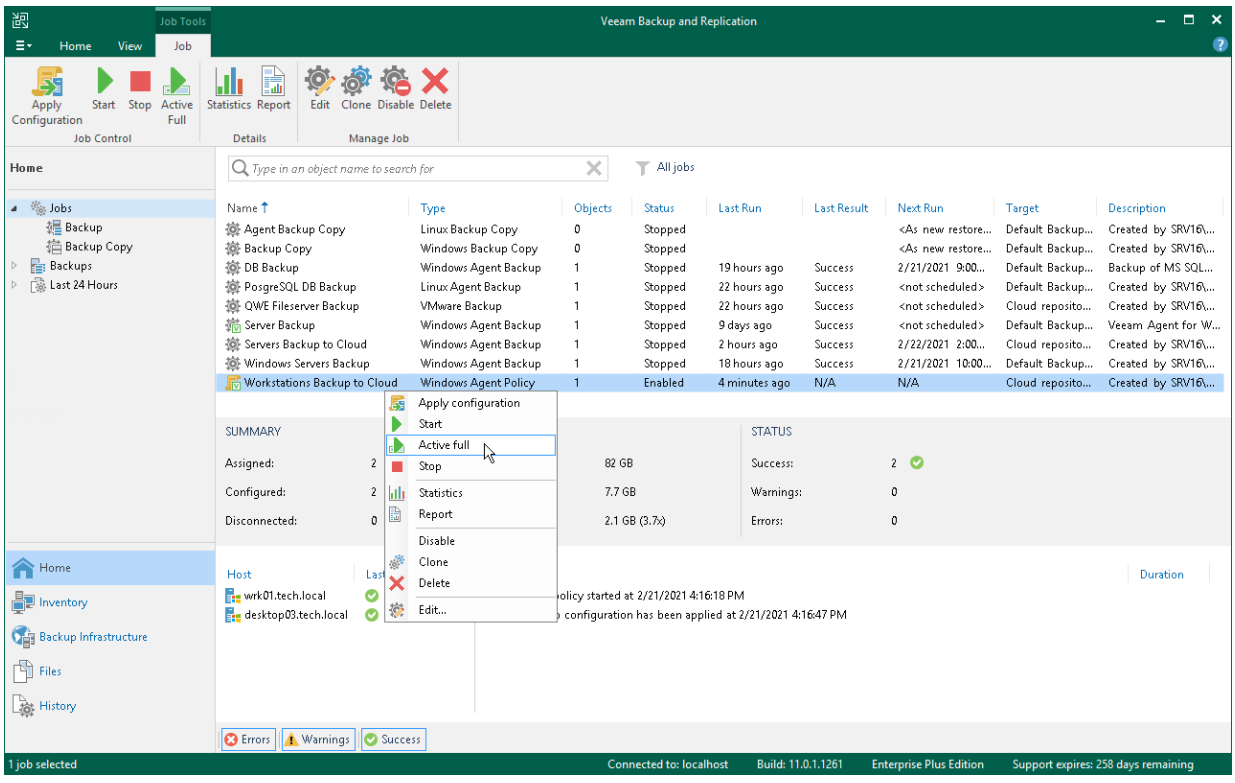
You can create an ad-hoc full backup — active full backup, and add it to the backup chain on the backup repository. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the backup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

When you start active full backup for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to perform active full backup on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the active full backup operation will be performed only on those computers that received the command from the backup server.

Keep in mind that you cannot start active full backup for protection groups for pre-installed Veeam Agents and their members. Veeam Agent computers included in such protection groups will be skipped and Veeam Backup & Replication will display a warning message in a backup policy session statistics.

To perform active full backup on Veeam Agent computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Active Full** on the ribbon or right-click the job and select **Active full**.



Clearing Backup Cache

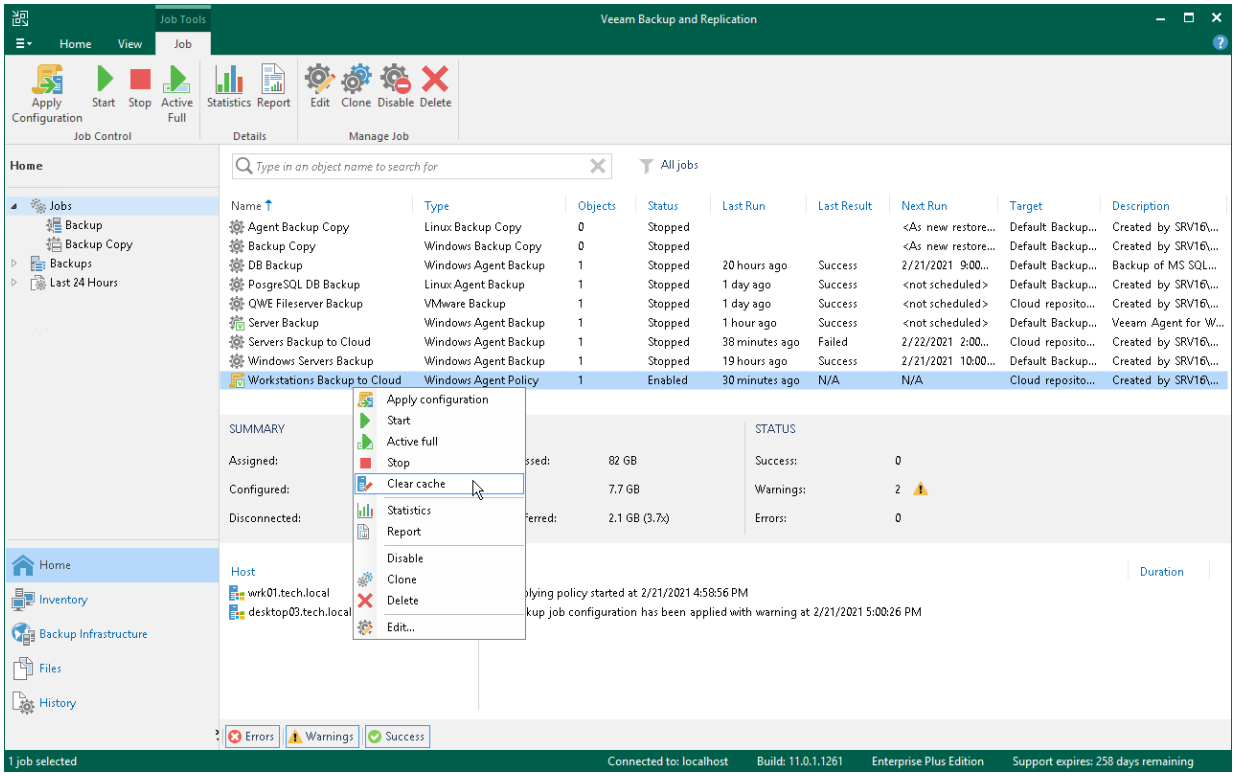
You can use the Veeam backup console to delete restore points from the backup cache on computers added to the backup policy. This operation may be required, for example, if the backup cache contains one or more restore points, and the backup chain in the target location has changed prior to the time when Veeam Agent for Microsoft Windows starts uploading restore points to the target location.

Keep in mind that the clear cache operation is available only for computers that are protected with Veeam Agent for Microsoft Windows and are members of any protection group excluding protection group for pre-installed Veeam Agents.

When you perform the clear cache operation, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to delete restore points from the backup cache on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the operation will be performed only on those computers that received the command from the backup server.

To clear the backup cache on Veeam Agent computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, press and hold the **[CTRL]** key, right-click the backup policy and select **Clear cache**.



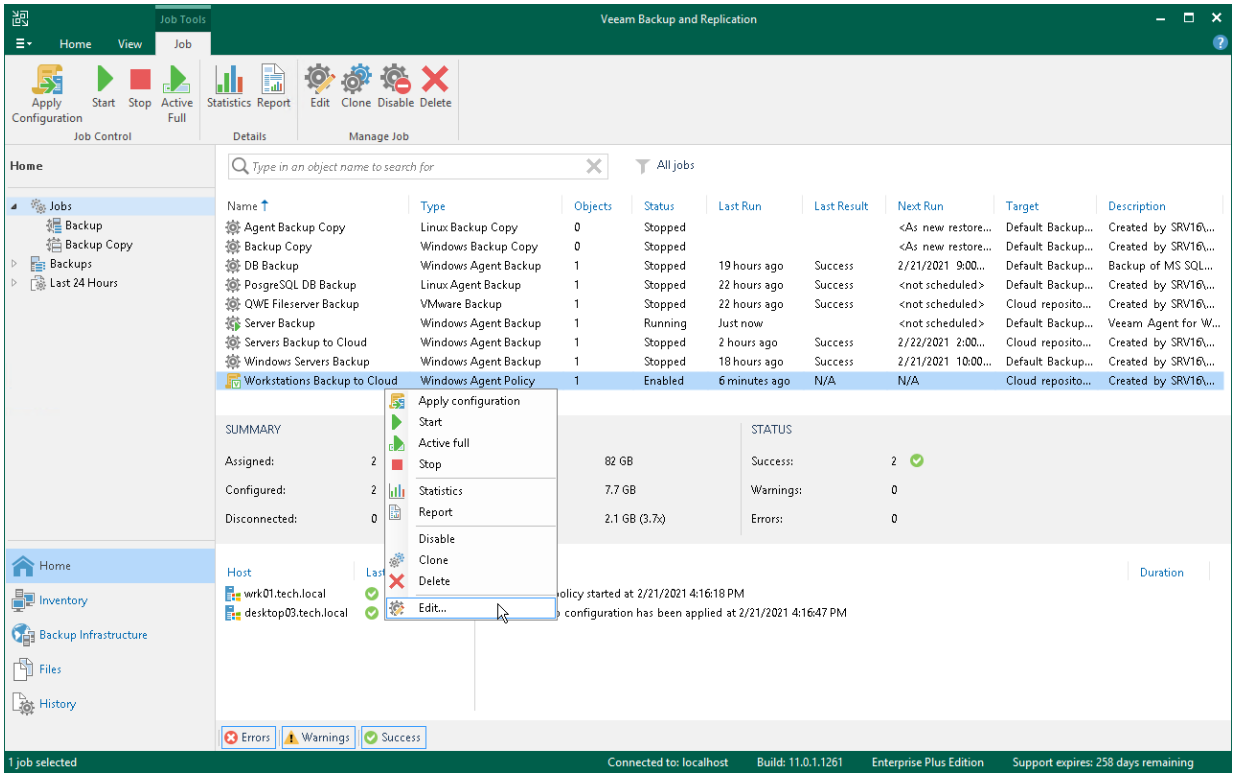
Editing Backup Policy Settings

You can edit settings of a Veeam Agent backup policy at any time. For example, you may want to change the backup scope, target location or scheduling settings for Veeam Agent backup jobs running on protected computers. After you change settings of the backup policy, Veeam Backup & Replication applies the specified settings to Veeam Agent backup jobs configured on protected computers added to the policy.

> **NOTE**
>
> Mind the following:
>
> - You cannot change the type of protected computers added to the job and the job mode (that is, change a Veeam Agent backup job to a backup policy and vice versa).
> - [For Veeam Agent backup jobs for Linux computers] You cannot change the backup mode from file-level to volume-level and vice versa.
> - If you change a password for data encryption without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.

To edit backup policy settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Edit** on the ribbon or right-click the policy and select **Edit**.
4. Complete the steps of the **Edit Agent Backup Job** wizard to change the job settings as required.



Enabling and Disabling Backup Policy

You can temporary disable Veeam Agent backup policies configured in Veeam Backup & Replication. While a backup policy is in the disabled state, the following operations are not performed in the Veeam Agent management infrastructure:

- Veeam Backup & Replication does not apply backup policy settings to Veeam Agent computers.
- Veeam Agent running on a protected computer does not create backups on the backup repository.

  If a user of a protected computer starts the Veeam Agent backup job manually or if the job starts by schedule, the job session will fail and report the *"The job has been disabled by the Veeam Backup & Replication administrator"* error. To let Veeam Agent for Microsoft Windows store backups to the backup repository again, you must enable the disabled policy and apply it to protected computers. To learn more, see Applying Backup Policy to Protected Computers.

> **NOTE**
>
> Disabling a backup policy does not affect performance of Veeam Agent backup jobs if a local drive or network shared folder is specified as a target location for backups in the policy settings.

To disable a Veeam Agent backup policy:

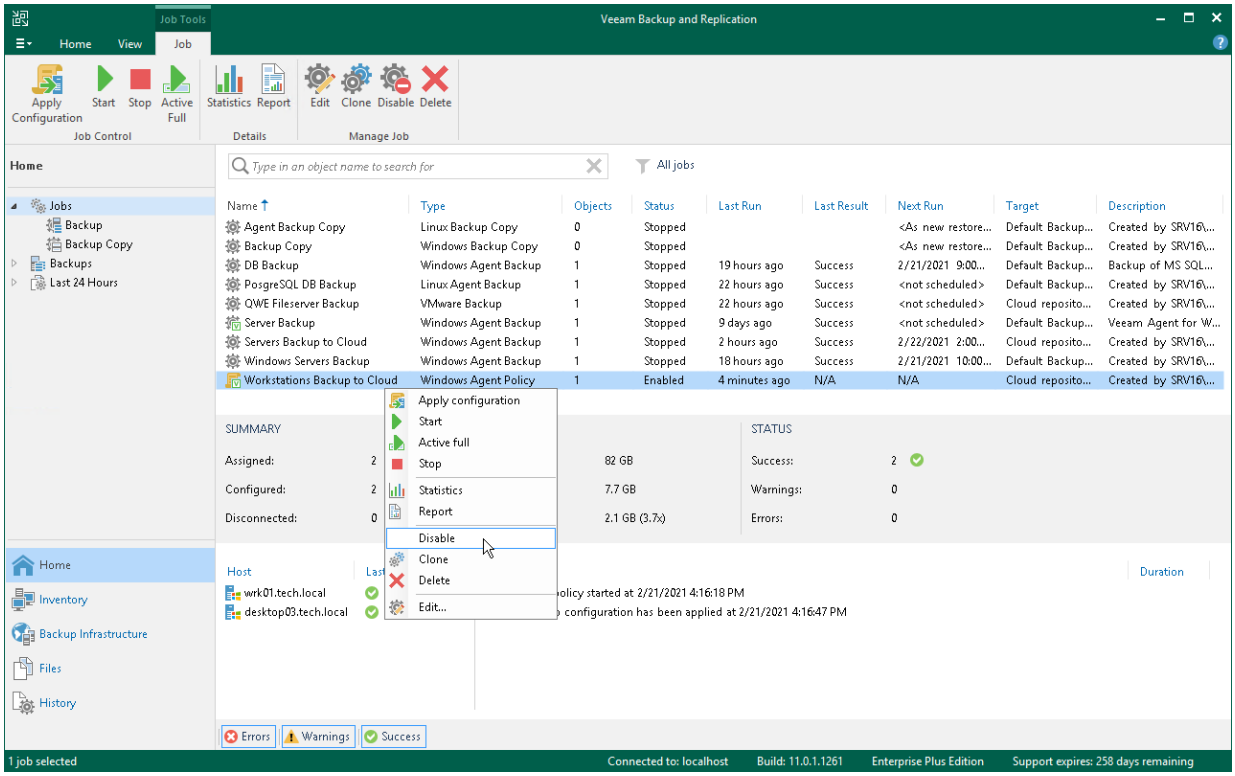
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup policy and click **Disable** on the ribbon or right-click the policy and select **Disable**.

   Keep in mind that Veeam Backup & Replication does not immediately disable a backup policy for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If a backup policy is targeted at the Veeam backup server and the next backup policy session is scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next session start.

   If you disabled a backup policy in the Veeam Backup & Replication console and this backup policy starts a new backup session targeted at the Veeam backup server before the next connection to Veeam Backup & Replication, this backup session and all automatic retries of this session will fail.

   If you want to disable backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Microsoft Windows Configuration, Veeam Agent for Linux Configuration, or Veeam Agent for Mac Configuration.

To enable a disabled policy, select it in the list and click **Disable** on the ribbon once again.



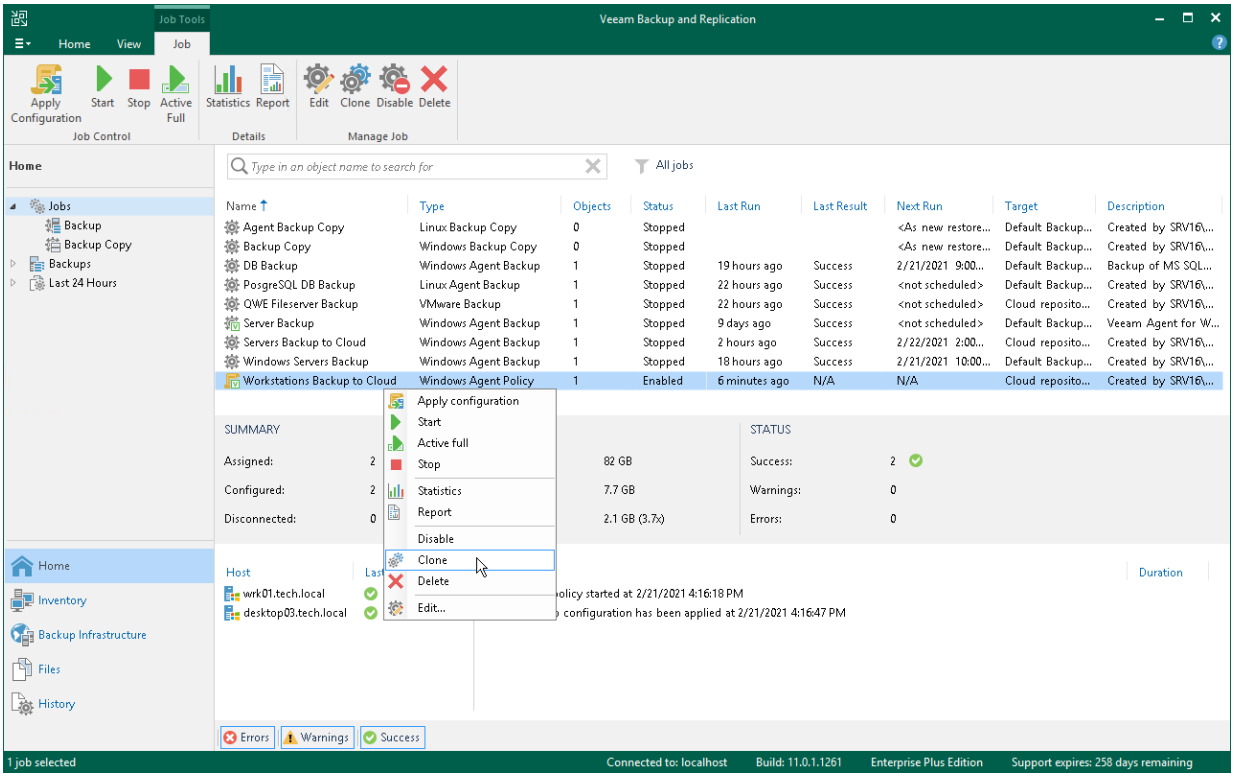
Cloning Backup Policy

You can clone backup policies configured in Veeam Backup & Replication. For example, you may want to configure a backup policy that will be used as a 'policy template', and use this policy to create multiple policies with similar settings.

To clone a backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Clone** on the ribbon or right-click the backup policy and select **Clone**.
4. After a backup policy is cloned, you can edit all its settings, including the job name.

> **NOTE**
>
> The backup policy cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

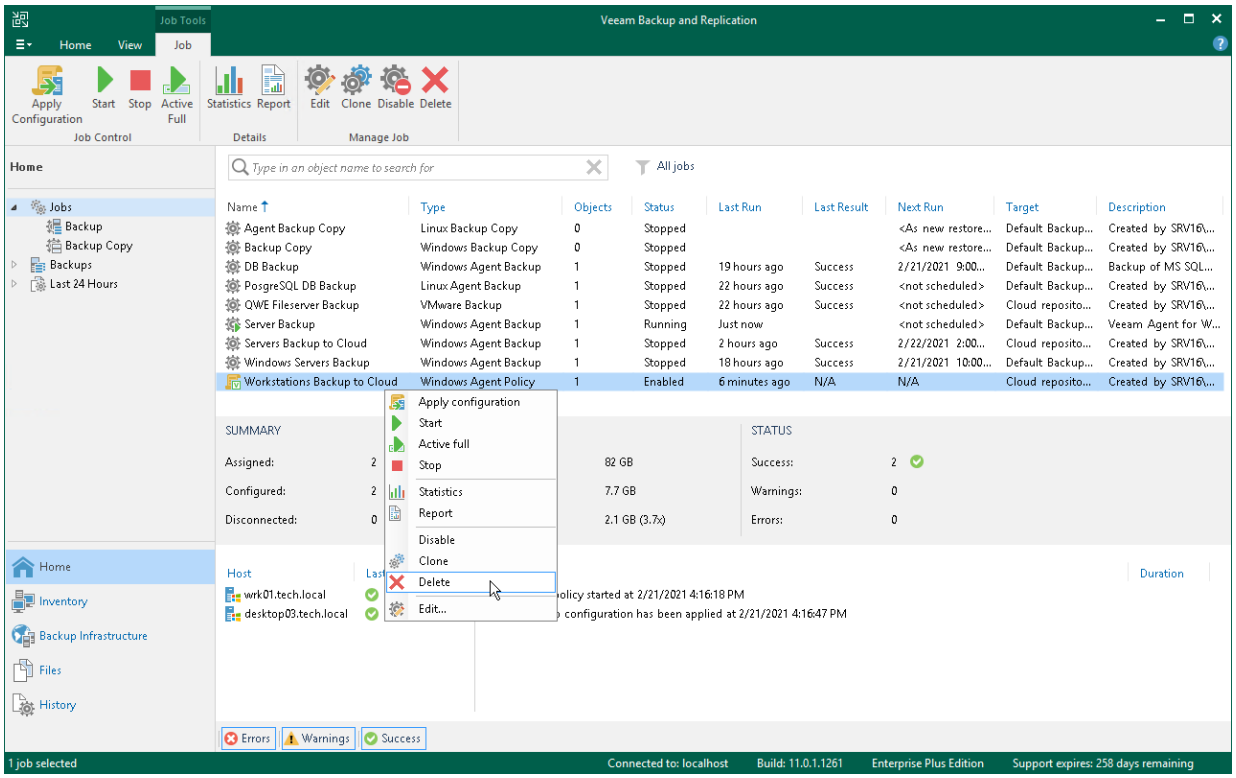


Removing Backup Policy

You can permanently remove a Veeam Agent backup policy from Veeam Backup & Replication. When you remove a backup policy, Veeam Backup & Replication also removes child backup jobs configured on Veeam Agent computers. Backups created by these jobs remain on the target location.

To remove a Veeam Agent backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup policy and click **Delete** on the ribbon or right-click the policy and select **Delete**.



Managing Protected Computers

> **IMPORTANT**
>
> A protection group for pre-installed Veeam Agents offers a limited set of operations to manage protected computers. To learn more, see Managing Protected Computers with Pre-Installed Veeam Agents.

You can perform the following operations with computers added to the inventory in Veeam Backup & Replication:

- Move an unmanaged computer to a protection group.
- Add a protected computer to a Veeam Agent backup job.
- Perform quick backup for a protected computer.
- View properties of a protected computer.
- Rescan a protected computer.
- Manage Veeam Agent installed on a protected computer:
  - Create Veeam Recovery Media for a protected computer.
  - Install Veeam Agent on a protected computer.
  - Upgrade Veeam Agent on a protected computer.
  - Install Veeam CBT driver on a protected computer.
  - Reboot a protected computer.
  - Uninstall Veeam Agent on a protected computer.

Managing Protected Computers with Pre-Installed Veeam Agents

A protection group for pre-installed Veeam Agents offers a limited set of operations to manage protected computers. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

For Veeam Agent computers added to the protection group for pre-installed Veeam Agents, you can perform the following operations:

- Move an unmanaged computer to a protection group.
- Add a protected computer to a Veeam Agent backup job.
- View properties of a protected computer.

Moving Unmanaged Computer to Protection Group

You can quickly move an unmanaged Veeam Agent computer to a protection group in the Veeam Backup & Replication inventory. This allows you to start using Veeam Backup & Replication to manage Veeam Agent that is already set up to create backups in the Veeam backup repository.

Keep in mind, that you can move an unmanaged Veeam Agent computer only to a protection group that includes individual computers and a protection group for pre-installed Veeam Agents:

- In case of the protection group that includes individual computers, you can move unmanaged computer using the Veeam Backup & Replication console.
- In case of the protection group for pre-installed Veeam Agents, you can move unmanaged computer only from the Veeam Agent side. This operation is similar to the initial Veeam Agent configuration. To learn more, see one of the following sections depending on the Veeam Agent that is installed on the computer you plan to move:
  - Veeam Agent for Microsoft Windows Configuration
  - Veeam Agent for Linux Configuration
  - Veeam Agent for Unix Configuration
  - Veeam Agent for Mac Configuration

You can move a computer from the *Unmanaged* protection group to a new protection group or protection group that you have already created.

- When you move an unmanaged computer to a new protection group, Veeam Backup & Replication creates the protection group and adds the computer to this group. In the protection group settings, you can define discovery and deployment options according to which Veeam Backup & Replication will process the added computer.
- When you move an unmanaged computer to an already existing protection group, Veeam Backup & Replication adds this computer to the protection group and starts processing the computer according to discovery and deployment settings defined in the properties of the protection group. Veeam Backup & Replication discovers the added computer, checks whether Veeam Agent running on the computer needs upgrade and upgrades Veeam Agent if needed.

NOTE

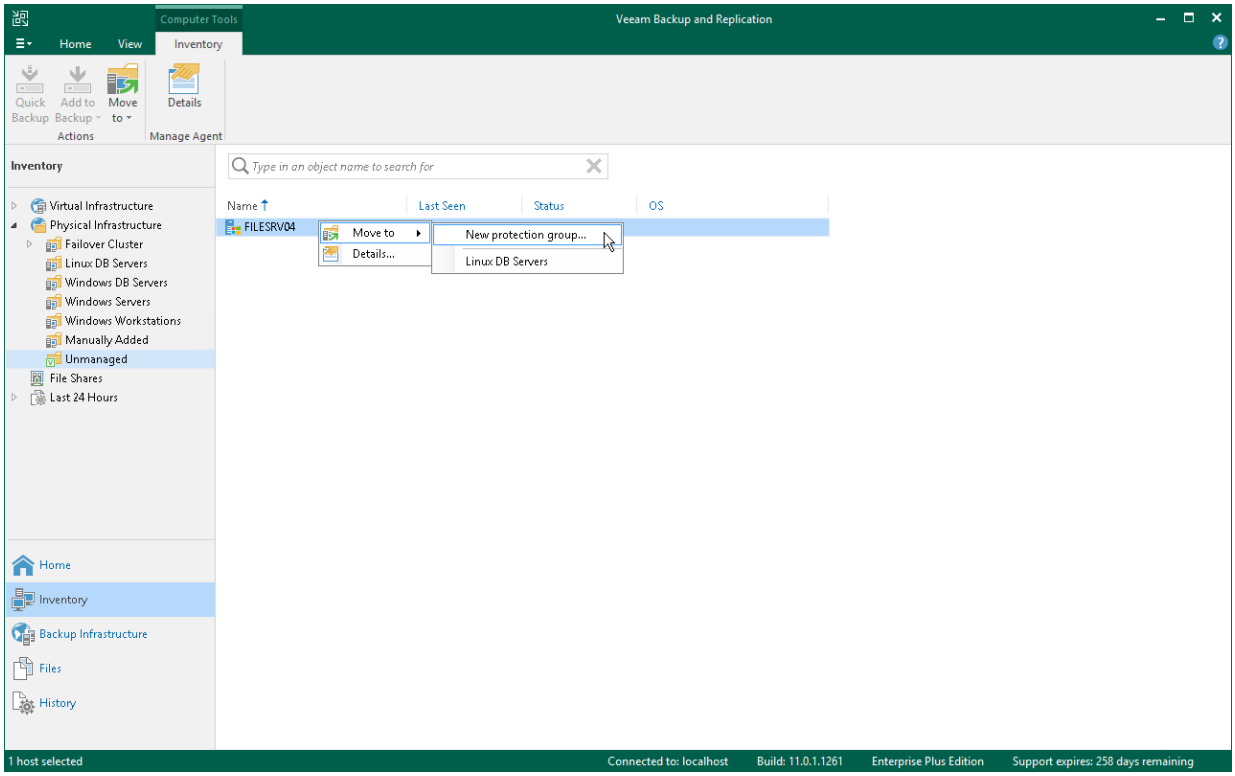
- After you move a computer to a protection group, data backup for this computer will be performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer will start a new backup chain on a target location specified in the backup job settings. The original backup job configured on the Veeam Agent computer will be removed in Veeam Agent, and you will not be able to continue the backup chain created with this job.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created on a backup repository by Veeam Agent operating in the standalone mode.

To move an unmanaged computer to a new protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the **Unmanaged** node.
3. In the working area, select the necessary computer and click **Move to** > **New protection group** on the ribbon or right click the computer and select **Move to** > **New protection group**.

To move an unmanaged computer to a protection group that is already created in the inventory:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the **Unmanaged** node.
3. In the working area, select the necessary computer and click **Move to** > **name of the protection group** on the ribbon or right click the computer and select **Move to** > **name of the protection group**.



Adding Computer to Backup Job

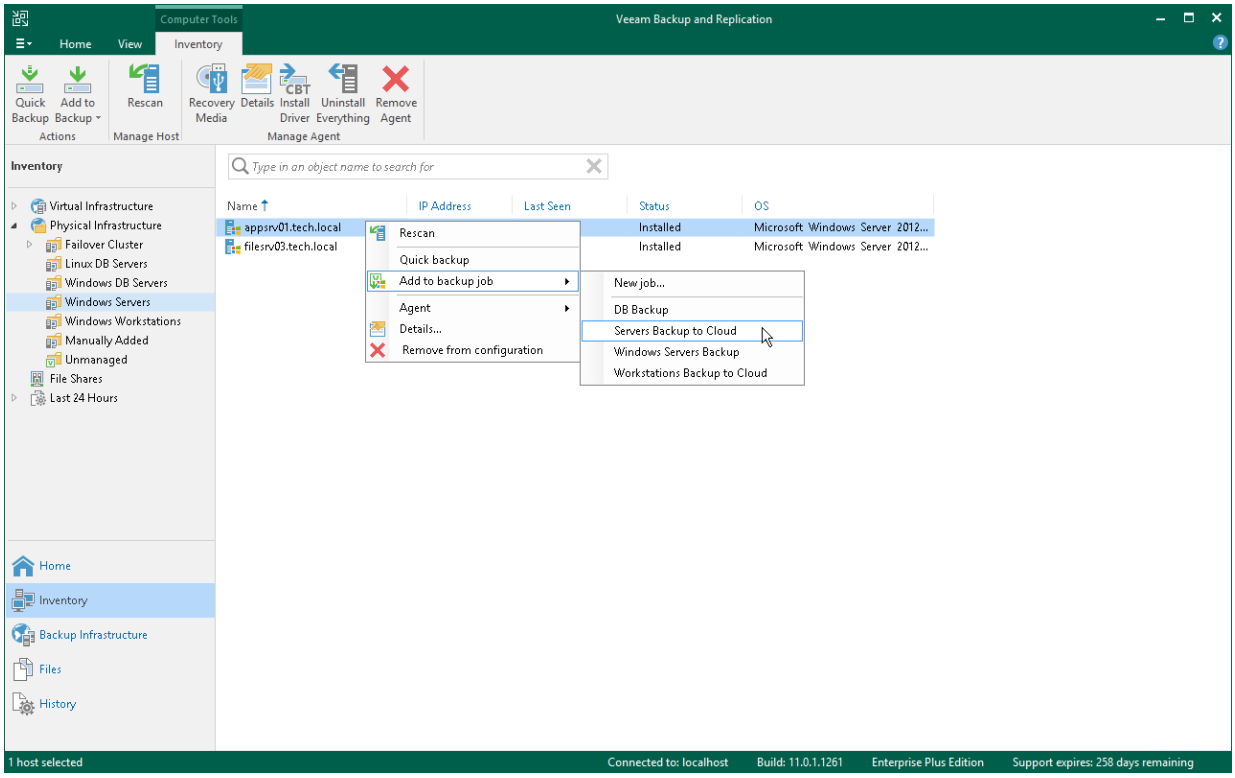
You can quickly add a specific protected computer to a Veeam Agent backup job that you have configured in Veeam Backup & Replication. To do this, do the following:

1. Open the **Inventory** view.
2. In the inventory pane, in the **Physical Infrastructure** node, select a protection group whose computers you want to add to a Veeam Agent backup job and do one of the following:
   - In the working area, select the computer that you want to add to the job and click **Add to Backup** > *name of the job* on the ribbon.
   - In the working area, right-click the computer that you want to add to the job and select **Add to backup job** > *name of the job*.

NOTE

Consider the following:

- You can add a computer to a Veeam Agent backup job configured for computers of the same platform. For example, you can add a Linux computer only to a Veeam Agent backup job for Linux computers.
- You can also add a specific protected computer to a new backup job. To learn more, see Creating Veeam Agent Backup Jobs.



Performing Quick Backup

You can create an ad-hoc incremental backup for one or more protected computers — quick backup, and add it to the backup chain on the backup repository. Quick backup can be helpful if you want to produce an additional restore point for one or more computers in the Veeam Agent backup job and do not want to configure a new job or modify the existing one.

Quick backup can be performed for computers that meet the following requirements:

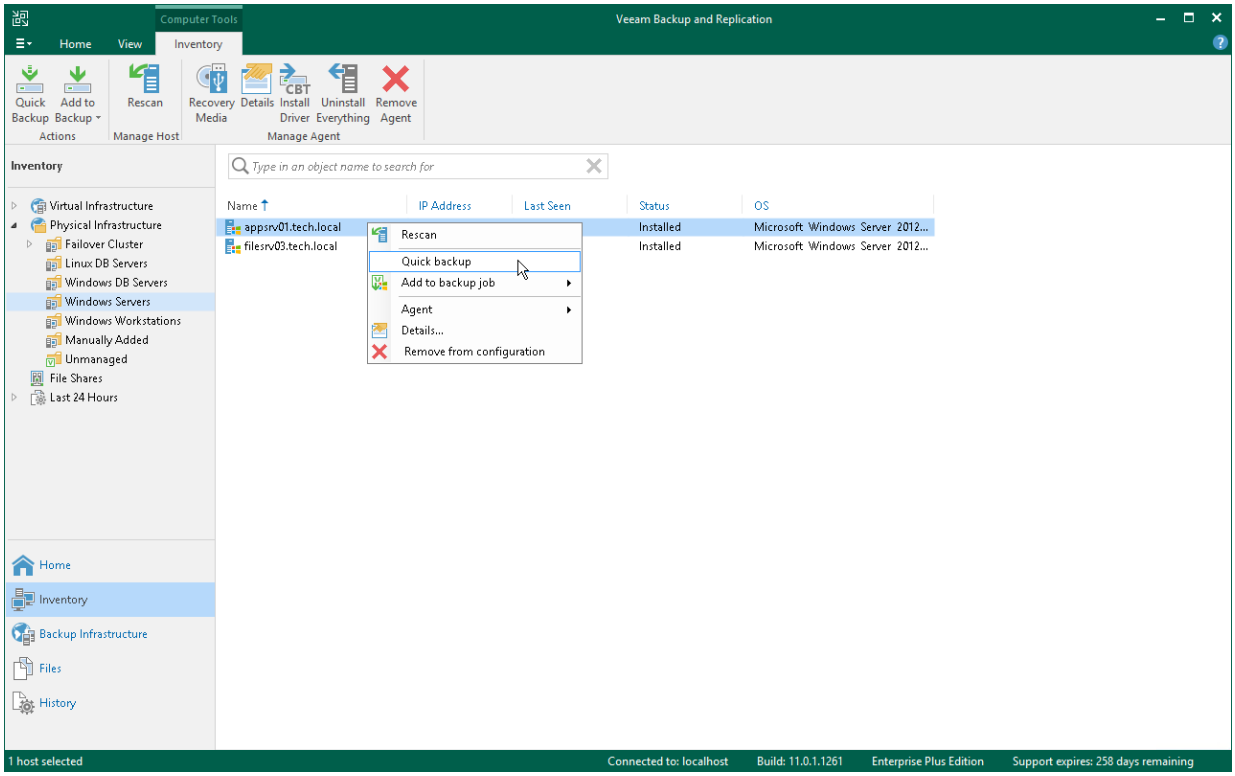
- A protected computer is added to a Veeam Agent backup job managed by the backup server.
- A full backup file for the protected computer exists on the backup repository configured in the backup infrastructure.

To perform quick backup:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the protected computer that you want to back up.
3. In the working area, select one or more computers and click **Quick Backup** on the ribbon or right-click the computers and select **Quick backup**.

Veeam Backup & Replication will trigger a Veeam Agent backup job to create a new incremental restore point for selected computers. Details of a running quick backup task are displayed in the job session window.

> **NOTE**
>
> If a computer for which you want to perform quick backup is added to more than one Veeam Agent backup job, Veeam Backup & Replication will trigger only the job that created the latest restore point for this computer.



Viewing Properties

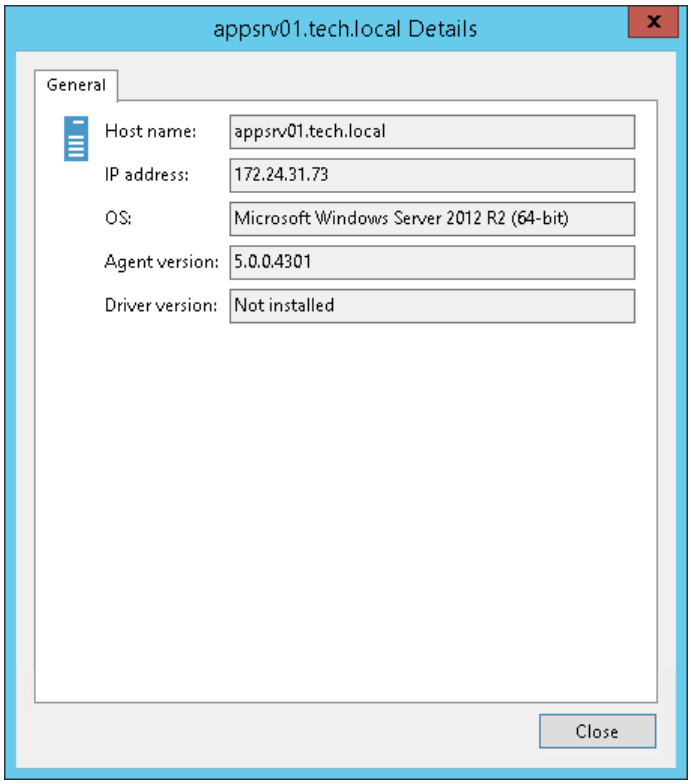
You can view detailed information about protected computers. The detailed information provides the following data:

- Host name
- IP address

  Keep in mind that IP address is not available for members of a protection group for pre-installed Veeam Agents.
- Fingerprint (for computers running a Linux OS)
- Key algorithm (for computers running a Linux OS)
- Operating system
- Veeam Agent version
- CBT driver version (for computers running a Microsoft Windows Server OS)

To view detailed information about a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the working area, select the computer and click **Details** on the ribbon or right-click the computer and select **Details**.



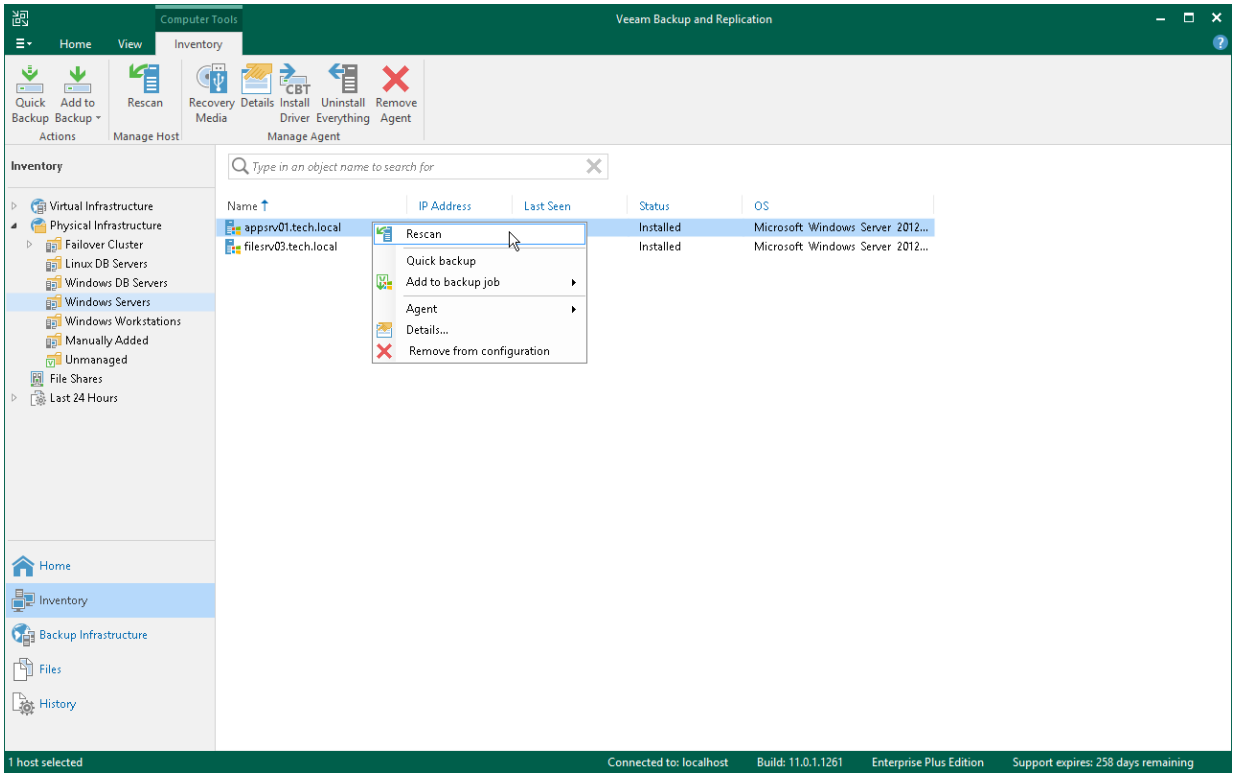
Rescanning Protected Computer

You can rescan protected computers added to the inventory. The rescan operation may be required, for example, if you want to refresh information about the protected computer in the Veeam Backup & Replication database. During the rescan operation, Veeam Backup & Replication communicates to Veeam Installer Service running on the protected computer, retrieves information about the computer and stores this information to the configuration database.

Keep in mind that rescan is not available for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in such protection groups connect to Veeam Backup & Replication every 6 hours and provide information about the Veeam Agent computer.

To rescan a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the computer and click **Rescan** on the ribbon or right-click the computer and select **Rescan**.



Creating Veeam Recovery Media

You can use the backup console to create a Veeam Recovery Media for a Veeam Agent computer that you manage in Veeam Backup & Replication. The process of creating a Veeam Recovery Media in Veeam Backup & Replication practically does not differ from the same procedure performed on a Veeam Agent computer. To learn more about the Veeam Recovery Media, see the Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.

Keep in mind that you can create Veeam Recovery Media in Veeam Backup & Replication only for computers that are protected with Veeam Agent for Microsoft Windows.

Before You Begin

You can create a Veeam Recovery Media for a protected computer in Veeam Backup & Replication if the following conditions are met:

- A protected computer runs a Microsoft Windows OS.
- A full backup file of one of the following backup types was created for the protected computer on the target location by a Veeam Agent backup job:
  - Entire computer backup
  - Volume-level backup of the computer OS data (created with the *Operating system* option selected in the backup job settings) or computer system volume
  - File-level backup of the computer OS data created with the *Operating system* option selected in the backup job settings

NOTE

- You can create a Veeam Recovery Media for a protected computer using a copy of a full backup file that meets all the conditions. The copy must be created by a backup copy job. To learn more, see the Backup Copy section in the Veeam Backup & Replication User Guide.
- By default, you cannot create a Veeam Recovery Media for a failover cluster with Cluster Shared Volumes (CSV). You can enable creation of a Veeam Recovery Media for such clusters with a registry value. For more information, contact Veeam Customer Support.

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

- The removable storage device must be inserted into a corresponding slot on the computer or connected to the computer.
- The removable storage device must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- During the recovery image creation, Veeam Agent for Microsoft Windows formats the removable storage device. If you have important information on the device, create a copy of this data in some other location.

CD/DVD/BD Scenario

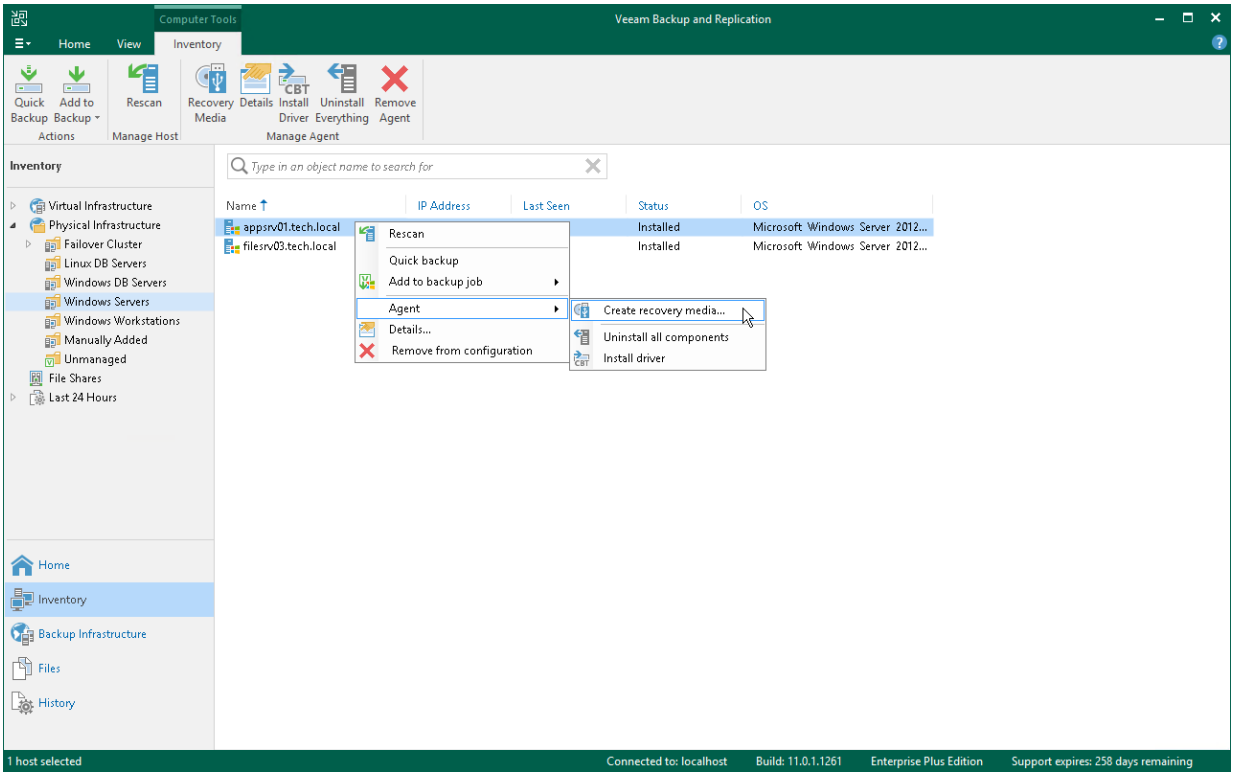
- An empty or re-writable CD/DVD/BD must be inserted into a CD/DVD/BD drive on the computer.
- The CD/DVD/BD must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- [For RW CD/DVD/BD] During the recovery image creation, Veeam Agent for Microsoft Windows erases information on the CD/DVD/BD. If you have important information on the CD/DVD/BD, create a copy of this data in some other location.

Step 1. Launch Create Recovery Media Wizard

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

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the necessary protected computer.
3. In the working area, select the computer and click **Recovery Media** on the ribbon or right-click the computer and select **Agent** > **Create recovery media**.

> **TIP**
>
> You can also launch the **Create Recovery Media** wizard from the **Backups** node in the **Home** view of the Veeam backup console. To learn more, see Creating Recovery Media from Backup.



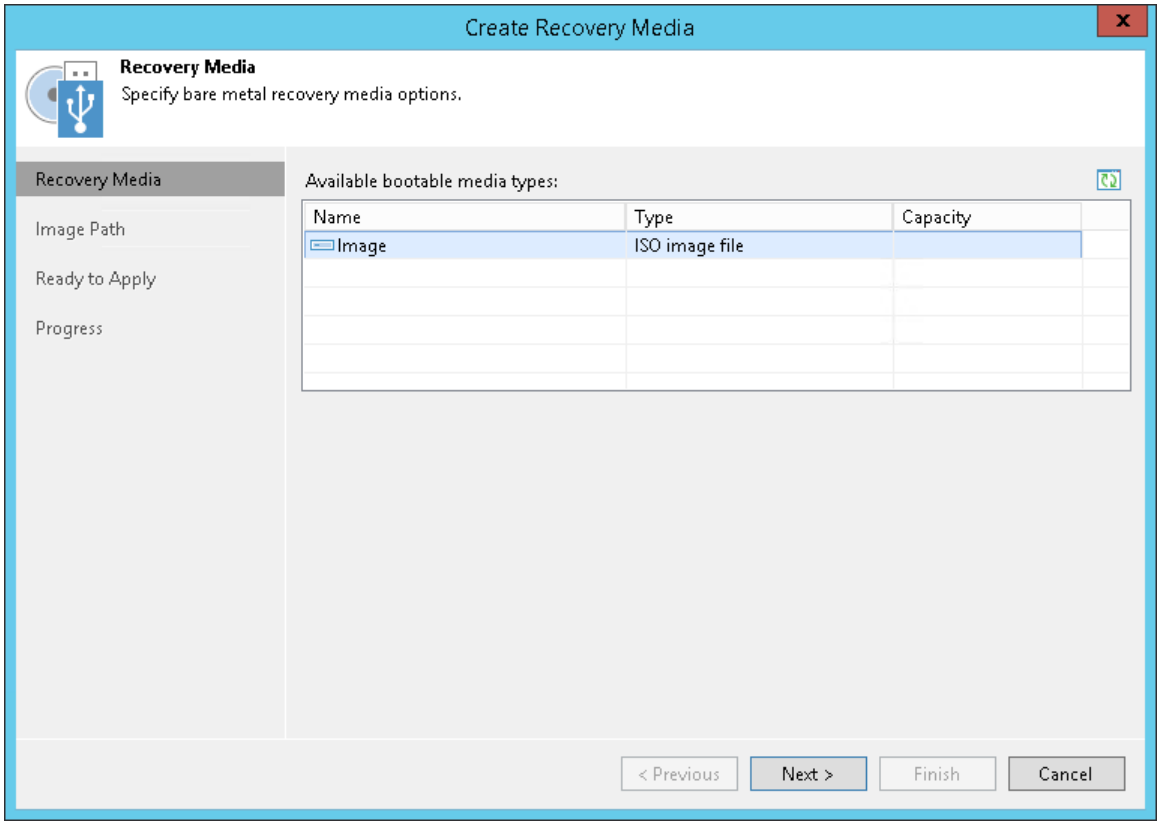
Step 2. Specify Recovery Media Options

At the **Recovery Media** step of the wizard, in the **Available bootable media types** list, specify on which type of media you want to create a 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 Backup & Replication displays all removable storage devices currently attached to the backup server. 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 Backup & Replication displays all CD, DVD and BD drives available on the backup server. 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 the backup server.

NOTE

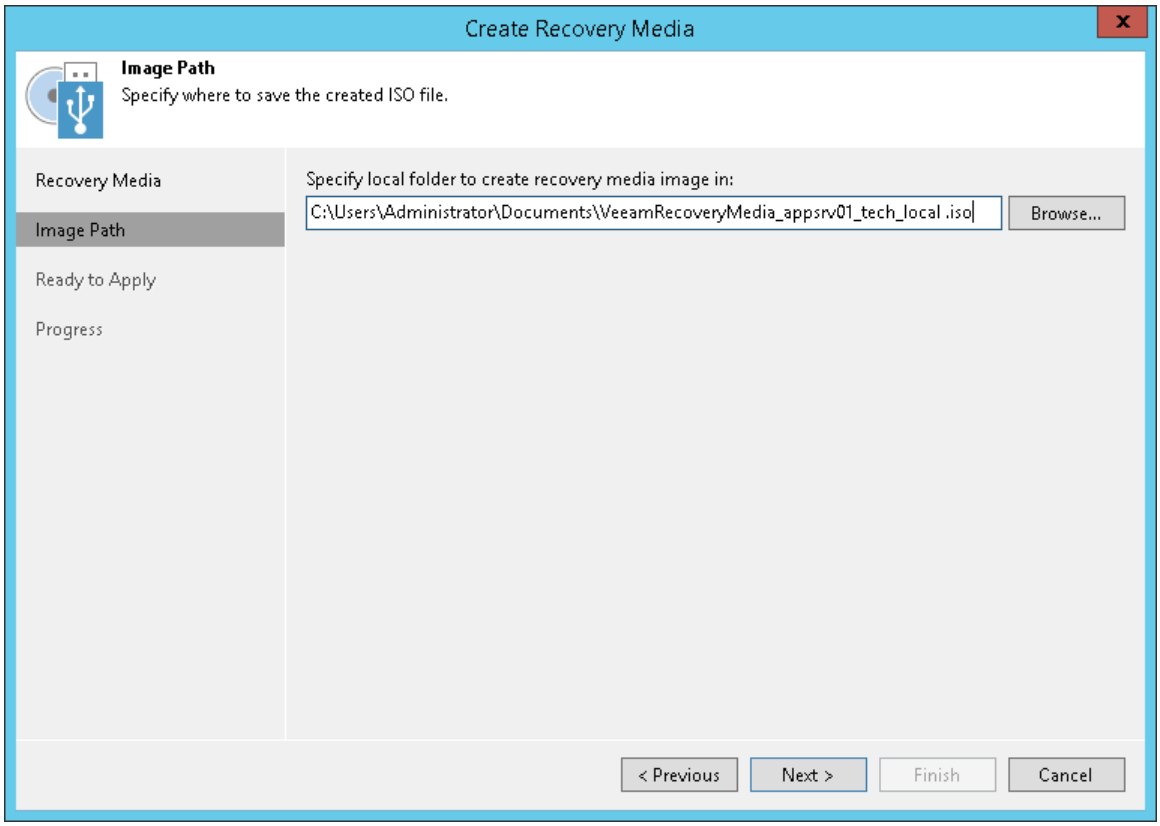
When you create a recovery image from the Veeam backup console, you cannot specify additional recovery media options in the same way as when you create a recovery image on the Veeam Agent computer. In this scenario, the recovery image is created with default settings: Veeam Backup & Replication includes network connection settings and hardware drivers installed on the Veeam Agent computer in the recovery image.



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.

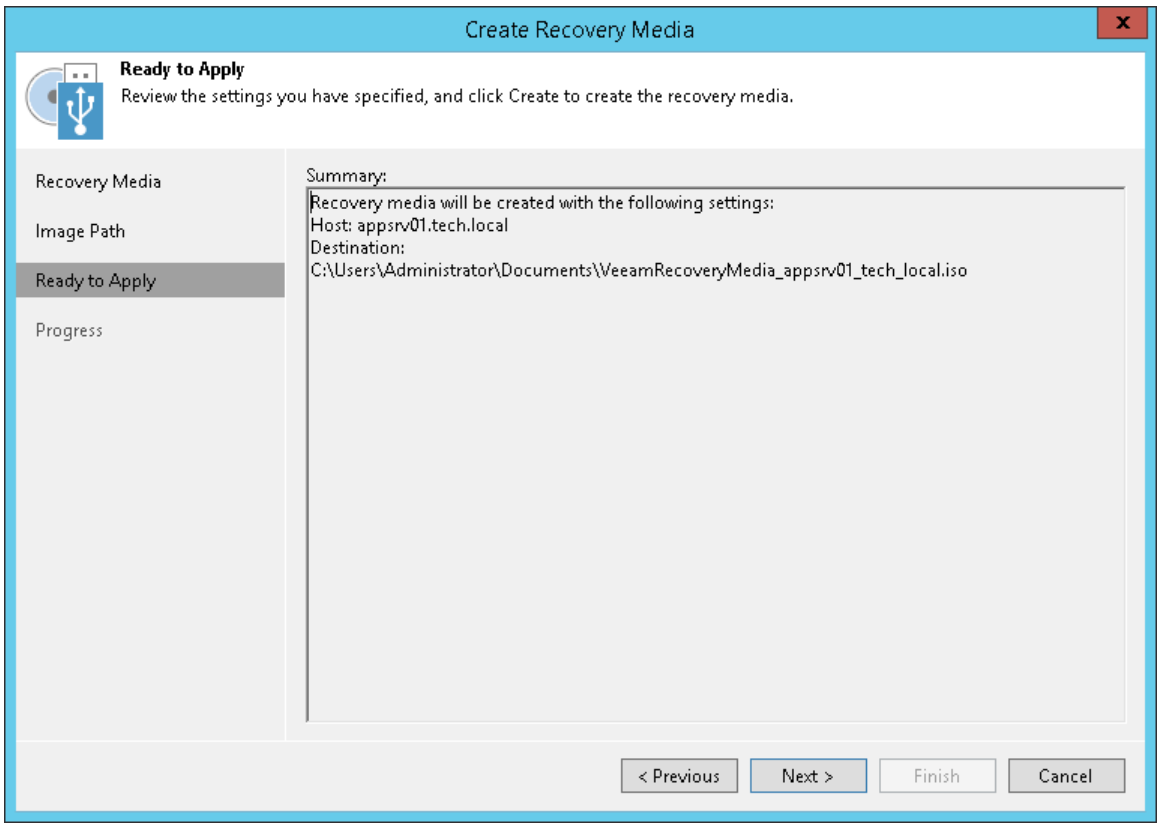
In the **Specify folder to create recovery media image in** field, specify a real path to the folder where you want to save the created recovery image, and the ISO file name. When you create Veeam Recovery Media using the Veeam Backup & Replication console, you can save the ISO file on the local drive of the Veeam backup server only. Thus, the recovery image will always be available should Veeam Agent computer volumes get corrupted or the computer fail to start.



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**.

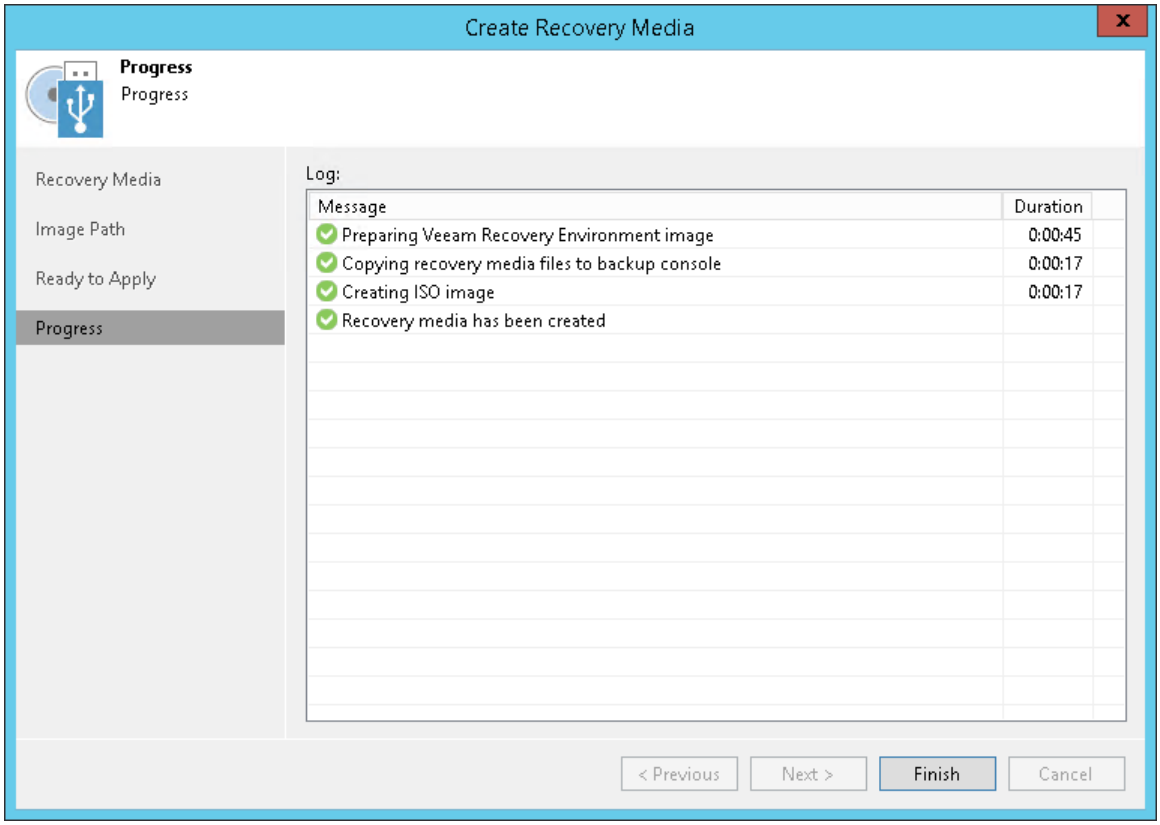
Veeam Backup & Replication will collect data necessary for recovery image creation and write the resulting recovery image to the specified target.



Step 5. Finish Working with Wizard

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

Installing Veeam Agent

You can install Veeam Agent on a specific protected computer in the inventory. This operation may be required, for example, if you want to test the installation process before allowing Veeam Backup & Replication to deploy Veeam Agent to all computers included in the protection group.

Keep in mind that Veeam Agents for computers that you plan to add to a protection group for pre-installed Veeam Agents require a different installation approach. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

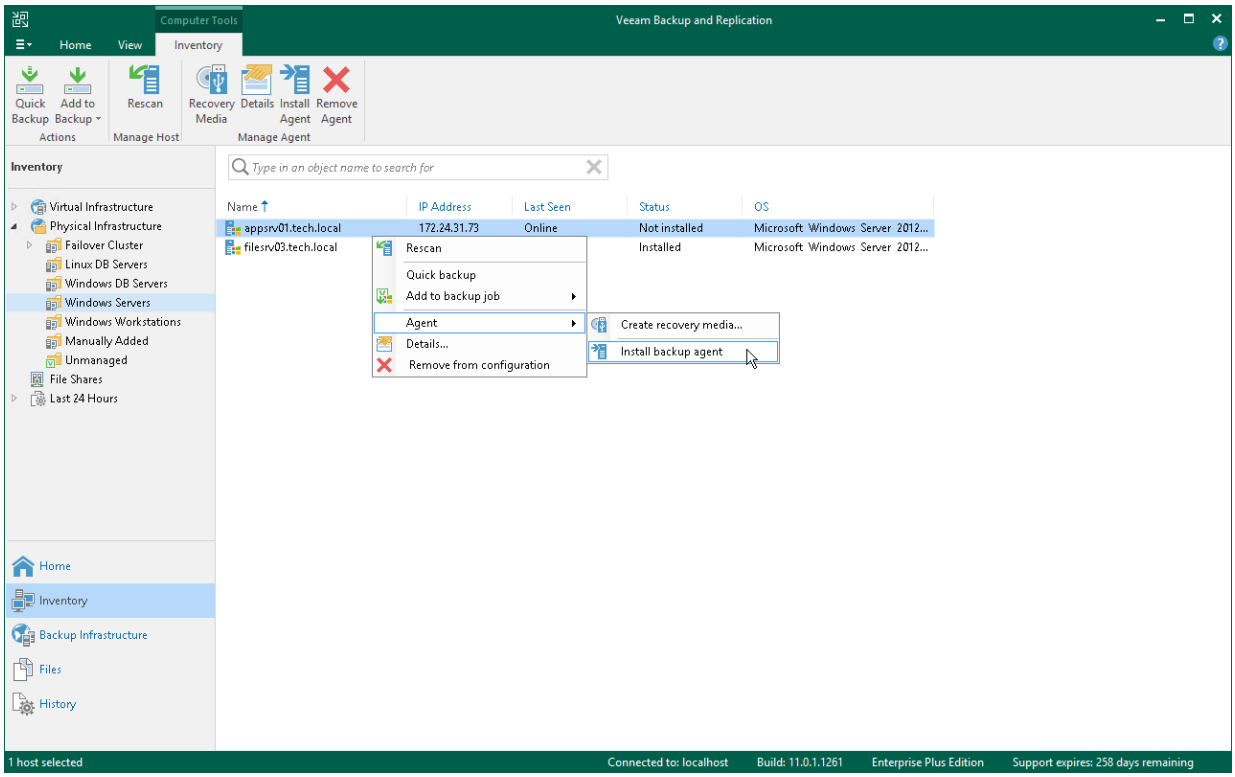
Before you install Veeam Agent, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Agent must be available on the distribution server.

To install Veeam Agent on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Install Agent** on the ribbon or right-click the computer and select **Agent** > **Install backup agent**.

> **NOTE**
>
> In some cases, installation of Veeam Agent for Microsoft Windows may require computer reboot. This can happen, for example, if you have an earlier version of Microsoft .NET Framework installed on the computer and during the installation process the framework is used by third-party software.



Upgrading Veeam Agent

You can upgrade Veeam Agent running on a specific protected computer. This operation may be required, for example, if you did not allow Veeam Backup & Replication to automatically upgrade Veeam Agent on computers included in the protection group and want to test the upgrade process on a selected computer first.

Keep in mind that you can upgrade Veeam Agent on a computer added to a protection group for pre-installed Veeam Agents only from the Veeam Agent computer side. To learn more, see Upgrading from Veeam Agent Side.

Before you upgrade Veeam Agent, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Agent must be available on the distribution server.
- There are no running jobs.

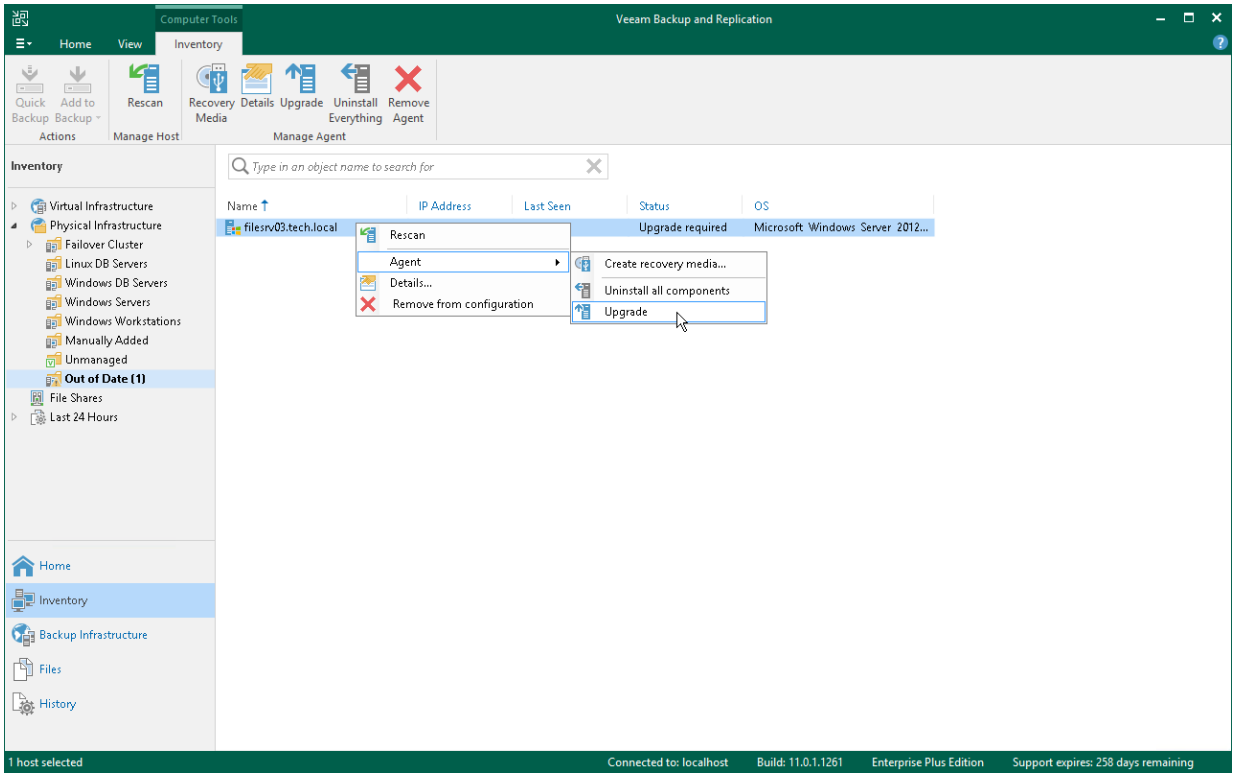
  We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If the protected computer runs VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived logs) is enabled in the backup job for the computer, disable this backup job too.

> **TIP**
>
> During the protected computers discovery process, Veeam Backup & Replication checks the version of Veeam Agent running on a protected computer and the version of Veeam Agent available on the distribution server. If a newer version of Veeam Agent becomes available on the distribution server, and automatic upgrade of Veeam Agent is disabled for a protection group, Veeam Backup & Replication puts a computer to the *Upgrade required* state.
>
> In addition, Veeam Backup & Replication includes computers that require upgrade of Veeam Agent in the *Out of Date* protection group. You can upgrade Veeam Agent on all computers that require upgrade at once. To learn more, see Upgrading Veeam Agent on Multiple Computers.

To upgrade Veeam Agent on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Upgrade** on the ribbon or right-click the computer and select **Agent** > **Upgrade**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Agent for Microsoft Windows may require computer reboot.

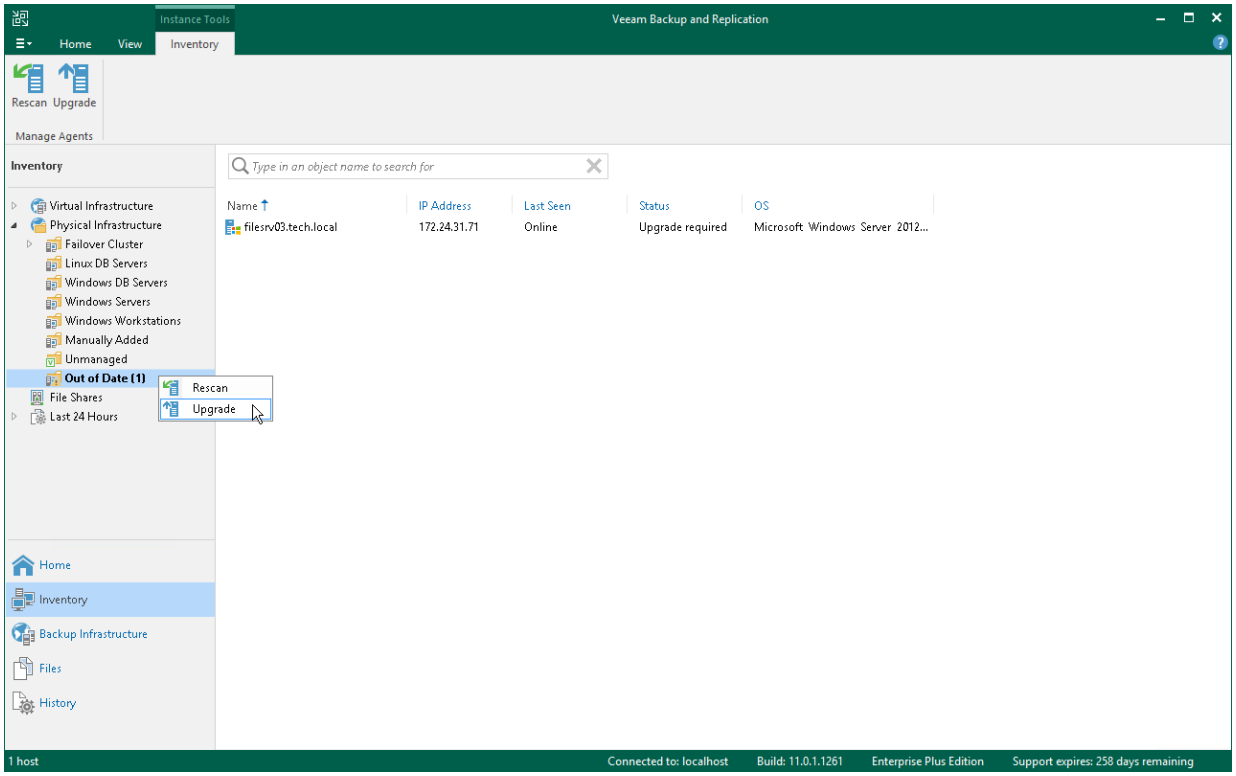


Upgrading Veeam Agent on Multiple Computers

You can upgrade Veeam Agent on all computers that require upgrade at once. To upgrade Veeam Agent on protected computers:

1. Open the **Inventory** view.
2. In the inventory pane, in the **Physical Infrastructure** node, select the **Out of Date** protection group and click **Upgrade** on the ribbon or right-click the **Out of Date** protection group and select **Upgrade**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Agent for Microsoft Windows may require computer reboot.



Upgrading from Veeam Agent Side

You can also upgrade Veeam Agent from the Veeam Agent computer side. This approach is required, for example, for Veeam Agent computers that are added to a protection group for pre-installed Veeam Agents. The process of upgrading differs depending on the Veeam Agent computer OS:

- For Windows-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Microsoft Windows User Guide.
- For Linux-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Linux User Guide.
- For Unix-based Veeam Agent computers running the IBM AIX operating system, see the Upgrading Product section in the Veeam Agent for IBM AIX User Guide.
- For Unix-based Veeam Agent computers running the Oracle Solaris operating system, see the Upgrading Product section in the Veeam Agent for Oracle Solaris User Guide.
- For macOS-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Mac User Guide.

Installing Veeam CBT Driver

You can use the Veeam Backup & Replication console to quickly install the Veeam changed block tracking (CBT) driver on a protected computer. This operation may be required, for example, if you want to evaluate driver performance on a selected computer rather than deploy driver to all computers in the protection group at once.

If you work with computer included in a protection group for pre-installed Veeam Agents, you can install and uninstall Veeam CBT driver only from the Veeam Agent computer side. To learn more, see the InstallCBTDriver and UninstallCBTDriver sections in the Veeam Agent Configurator Reference.

Before you install the Veeam CBT driver, check the following prerequisites:

- The protected computer on which you want to install the driver must run a Microsoft Windows Server OS.
- The protected computer on which you want to install the driver must be powered on and able to be connected over the network.

IMPORTANT

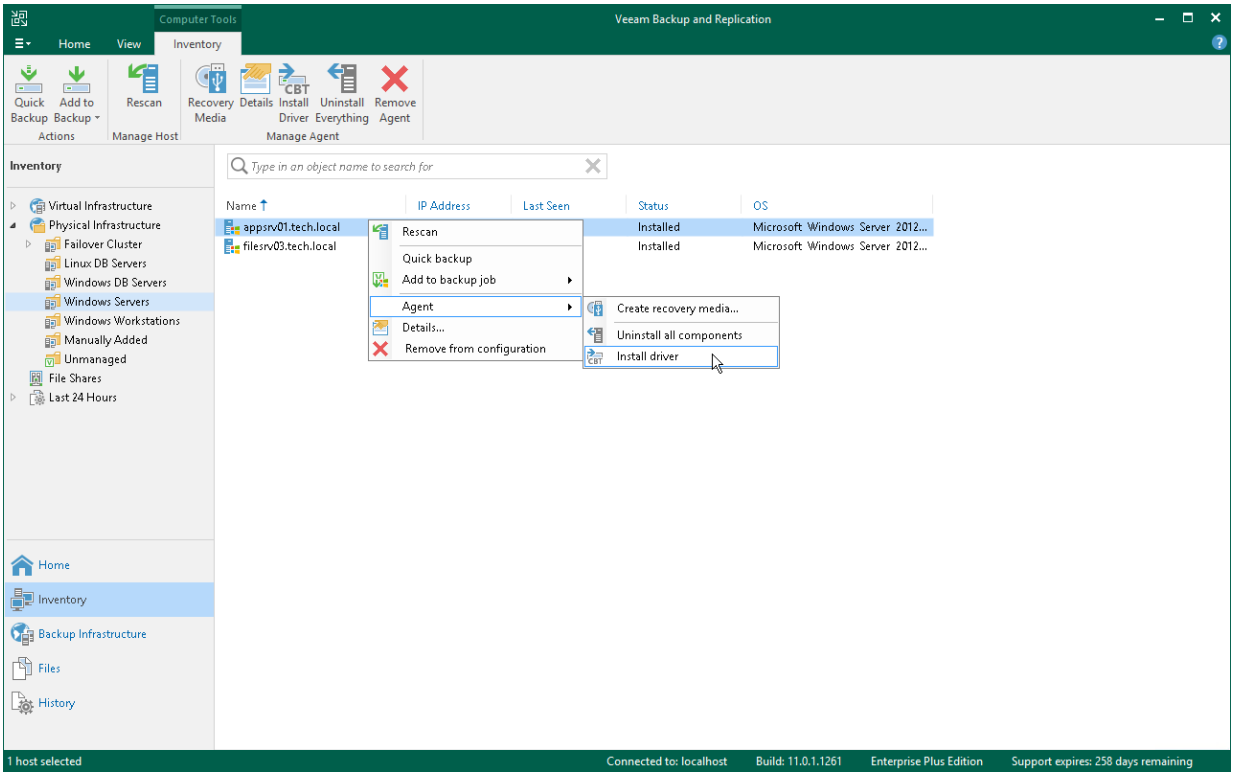
- Prior to installing the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, make sure that update KB3033929 is installed in the OS.

  The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver. To learn more, see this Microsoft KB article.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, 2012 or 2012 R2 if one or more volumes on this computer are encrypted with Microsoft BitLocker (or other encryption tool), or if you plan to use Microsoft BitLocker to encrypt volumes on this computer. Concurrent operation of Microsoft BitLocker and Veeam CBT driver may result in driver failures and may prevent the OS from starting.

To install the Veeam CBT driver on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer on which you want to install the driver.
3. In the working area, select the necessary computer and click **Install Driver** on the ribbon or right-click the computer and select **Agent** > **Install driver**.

> **NOTE**
>
> To enable the CBT driver after installation, you need to reboot the computer. To learn more, see Rebooting Protected Computer.

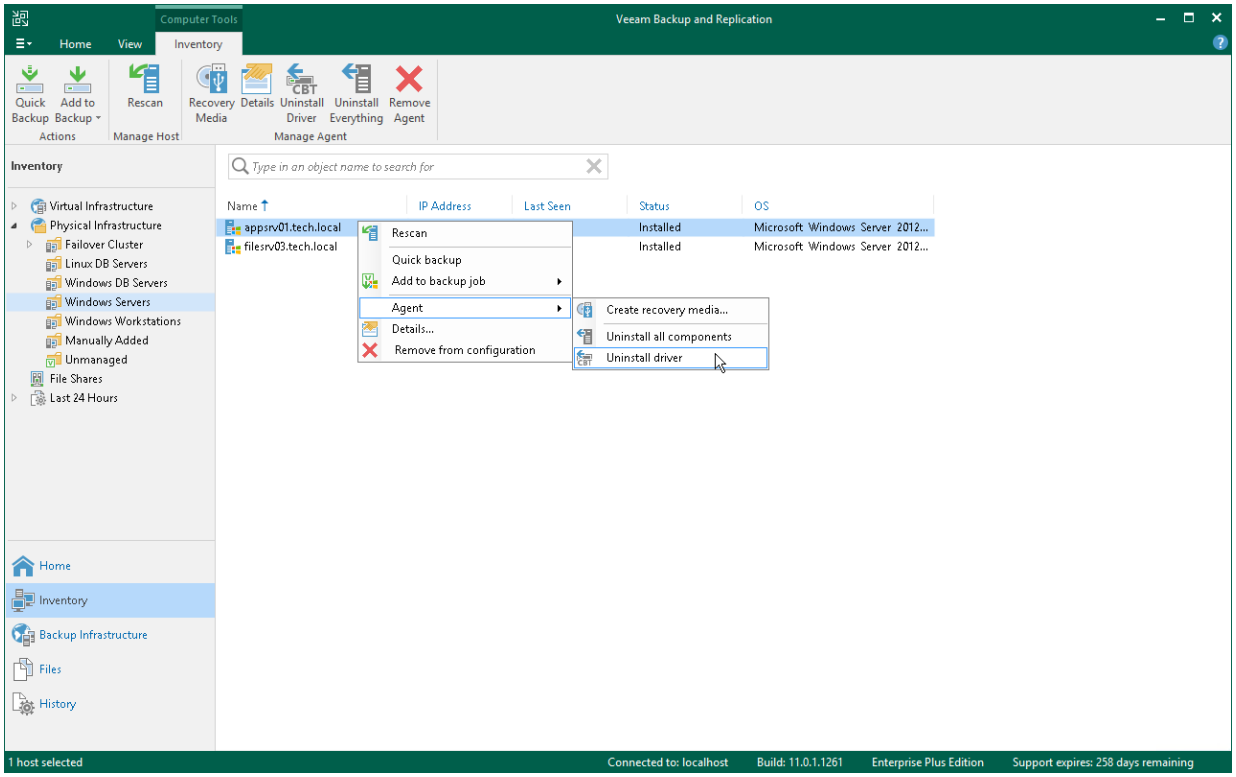


Uninstalling Veeam CBT Driver

You can uninstall the Veeam CBT driver at any time you need. To uninstall the driver:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer on which you want to uninstall the driver.
3. In the working area, select the necessary computer and click **Uninstall Driver** on the ribbon or right-click the computer and select **Agent** > **Uninstall driver**.

> **NOTE**
>
> To complete the driver uninstallation process, you need to reboot the computer. To learn more, see Rebooting Protected Computer.



Rebooting Protected Computer

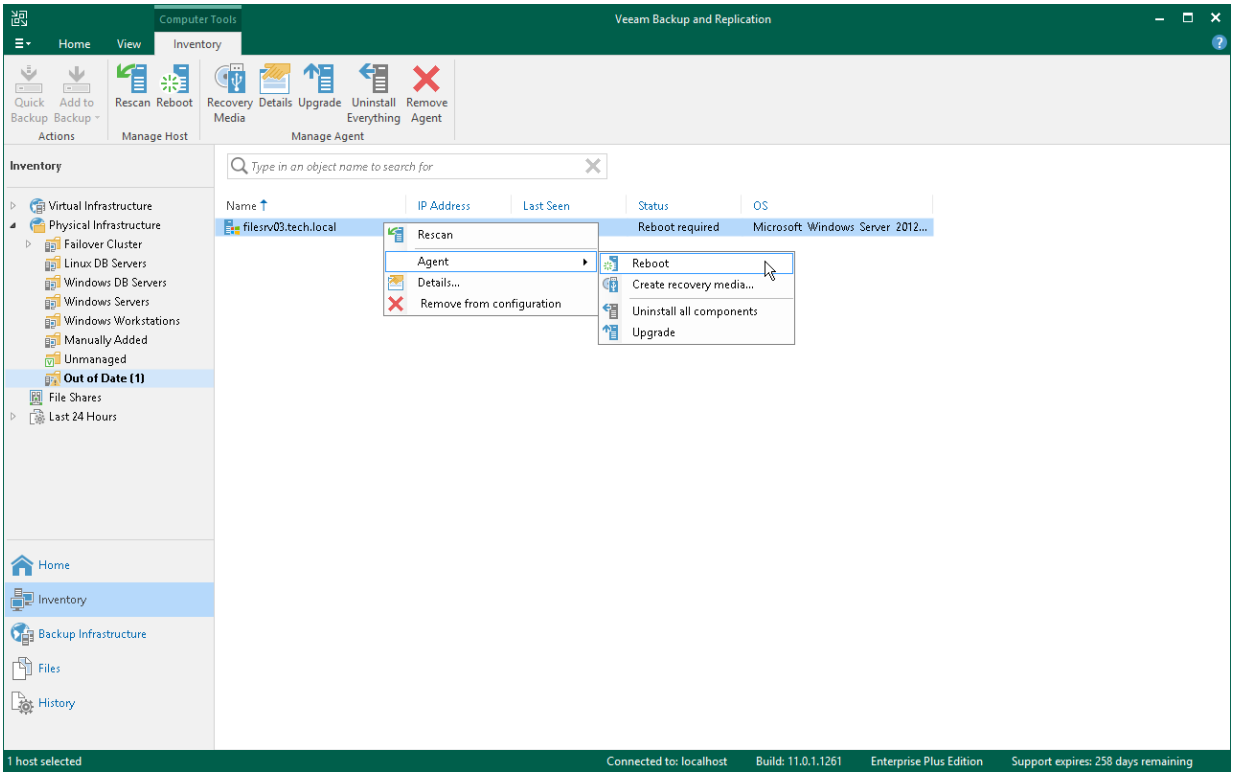
You can use the Veeam Backup & Replication console to reboot a protected computer. This operation may be required, for example, if you have installed the CBT driver on a selected computer and need to reboot this computer to finish the installation process and enable the driver.

Keep in mind that you cannot reboot a protected computer that is added to a protection group for pre-installed Veeam Agents. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

To reboot a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer that requires reboot. The computer that requires reboot is displayed in the *Reboot required* status in the Veeam Backup & Replication console.
3. In the working area, select the necessary computer and click **Reboot** on the ribbon or right-click the computer and select **Agent** > **Reboot**.
4. In the displayed window, click **Yes**.

> **TIP**
>
> You can also reboot a computer with a different status than the *Reboot required* status. To do this, press and hold the **[CTRL]** key, right-click the necessary computer and select **Agent** > **Reboot**.



Uninstalling Veeam Agent

You can remove Veeam Agent from a specific protected computer, for example, if you want to reinstall Veeam Agent running on the protected computer. When you remove Veeam Agent from a protected computer, Veeam Backup & Replication also removes the Veeam Installer Service from this computer.

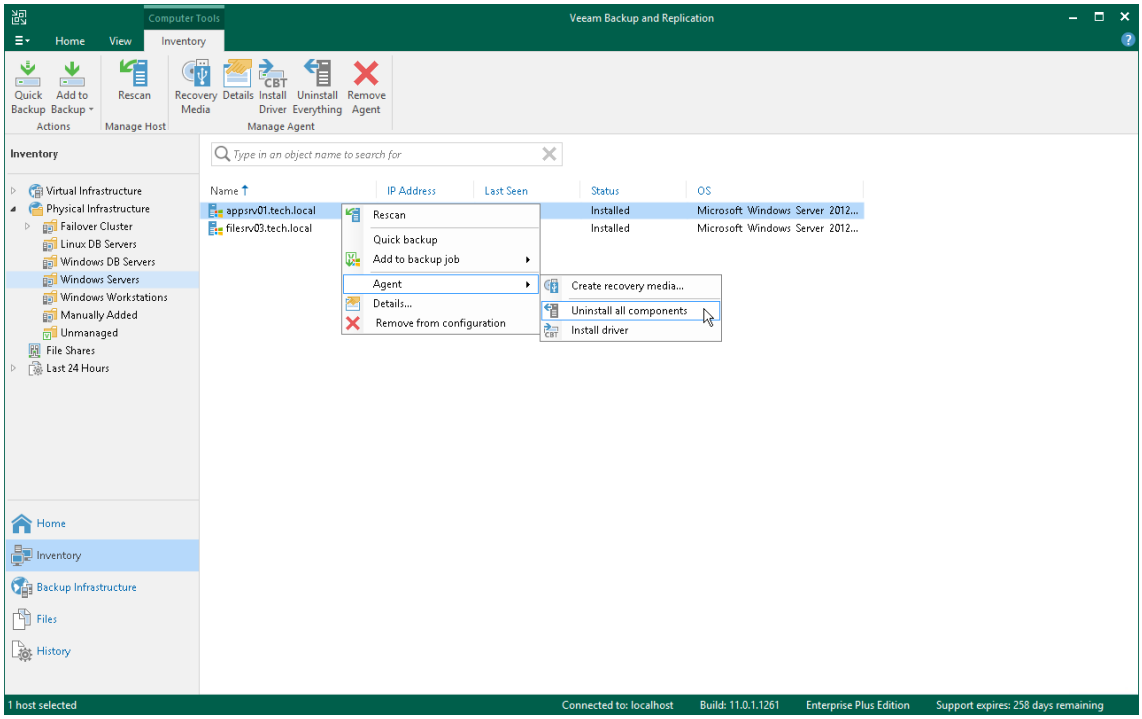
To uninstall Veeam Agent:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Uninstall Everything** on the ribbon or right-click the computer and select **Agent** > **Uninstall all components**.
4. In the displayed notification window, click **Yes**.

NOTE

Mind the following:

- If automatic installation of Veeam Agent is enabled in the protection group settings, after you remove Veeam Agent from a selected computer, Veeam Backup & Replication will install Veeam Agent on this computer during the next rescan job session started by schedule.
- Prerequisite components installed and used by Veeam Agent are not removed during the uninstall process. To remove the remaining components, use the Microsoft Windows Control Panel on the computer from which you uninstalled Veeam Agent.
- If you uninstall Veeam Agent for Microsoft Windows added to the protection group for pre-installed Veeam Agents and then re-install on the same computer, Veeam Agent will not connect to Veeam backup server automatically. To connect Veeam Agent, you must repeat the configuration step of the Veeam Agent deployment scenario. To learn more, see Deploying Veeam Agents Using Generated Setup Files.



Removing Computer from Protection Group

You can remove one or more computers from a protection group, for example, if you do not want to protect these computers with Veeam Agent any longer but want to back up data of other computers in the protection group.

When you remove a computer from a protection group, Veeam Backup & Replication removes records about the computer from the Veeam backup console and configuration database but does not uninstall Veeam Agent from the computer. You can remove Veeam Agent from the computer in advance, before you remove the computer from the protection group. To learn more, see Uninstalling Veeam Agent.

Alternatively, you can remove a computer from a protection group, and then uninstall Veeam Agent from this computer. Keep in mind that in this case you will have to uninstall Veeam Agent using the Microsoft Windows control panel directly on the Veeam Agent computer.

> **TIP**
>
> You can also remove entire protection groups from the Veeam Backup & Replication inventory. When you remove a protection group, you can instruct Veeam Backup & Replication to uninstall Veeam Agents from all protected computers included in this protection group. To learn more, see Removing Protection Group.

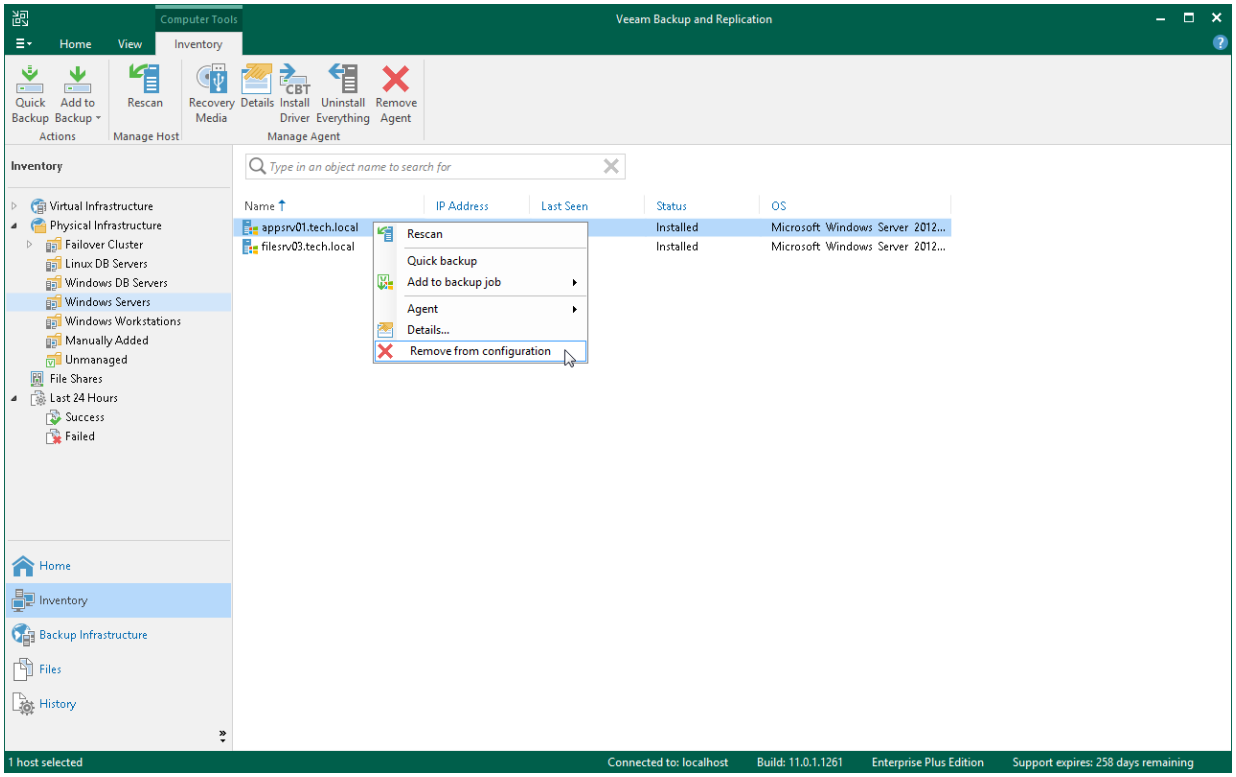
To remove a computer from a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click Remove Agent on the ribbon or right-click the computer and select **Remove from configuration**.

Backups created for computers that were removed from a protection group remain intact in the backup location. You can delete this backup data manually later if needed.

NOTE

You cannot remove a computer from the protection group if this computer is a failover cluster node.



Alternative Ways to Remove Computer from Protection Group

There are alternative ways to remove computer from protection group that may be suitable for specific situations. For example, you want to remove a Mac computer from a protection group from the Veeam Agent computer side.

Alternative ways of removing computer from protection group differ depending on the type of the protection group that contains the computer you want to remove.

- For a protection group that contains individual computers, edit the protection group and remove the necessary computer at the **Computers** step of the **Edit Protection Group** wizard. To learn more, see Editing Protection Group Settings.

  You can also use this option to remove a computer from the *Manually Added* protection group. This protection group contains computers that you add directly to a Veeam Agent backup job. To learn more, see Removing Computer from "Manually Added" Protection Group.

- For a protection group that contains Active Directory objects, edit the protection group and remove the necessary computer account at the **Active Directory** step of the **Edit Protection Group** wizard.

  Alternatively, if the protection group contains a container, organization unit, group or entire domain, you can exclude the computer at the **Exclusions** step of the wizard. To learn more, see Exclude Objects from Protection Group.

- For a protection group that contains computers listed in a CSV file, remove the record about the necessary computer from the CSV file. During subsequent rescan of the protection group, Veeam Backup & Replication will remove the computer from the protection group.

- For a protection group for pre-installed Veeam Agents, you can remove the computer from the Veeam Agent computer side. The process of removing a computer from a protection group for pre-installed Veeam Agents differs depending on the Veeam Agent computer OS:

  - For Windows-based Veeam Agent computers, see the RemoveOwner section in the Veeam Agent Configurator Reference.
  - For Linux-based Veeam Agent computers, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Linux User Guide.
  - For Unix-based Veeam Agent computers running the IBM AIX operating system, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Mac User Guide.
  - For Unix-based Veeam Agent computers running the Oracle Solaris operating system, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Mac User Guide.
  - For macOS-based Veeam Agent computers, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Mac User Guide.

Removing Computer from "Manually Added" Protection Group

Individual computers that you add directly to a Veeam Agent backup job are included in the *Manually Added* protection group. When you remove such a computer from the backup job, Veeam Backup & Replication does not remove the computer from the *Manually Added* protection group as well. The computer remains in the *Manually Added* protection group until you remove the computer from this protection group.

To remove a computer from the *Manually Added* protection group, you must edit this protection group and remove the computer at the **Computers** step of the **Edit Protection Group** wizard. To learn more, see Editing Protection Group Settings.

> **NOTE**
>
> You cannot remove a computer from the *Manually Added* protection group if this computer is added to a Veeam Agent backup job.

Restoring Data from Veeam Agent Backups

You can recover data from backups created by Veeam Agent backup jobs configured in Veeam Backup & Replication. For data restore with the Veeam backup console, you can use Veeam Agent backups created on a Veeam backup repository or cloud repository. If you specified a local drive or network shared folder as a target for Veeam Agent backups, you need to restore data from such backups using Veeam Agent UI on a protected computer.

You can perform the following data restore tasks with Veeam Agent backups in Veeam Backup & Replication:

- Restore a Veeam Agent backup to a vSphere VM.
- Restore a Veeam Agent backup to a Hyper-V VM.
- Restore a Veeam Agent backup to a Nutanix AHV VM.
- Restore data from a Veeam Agent backup to Microsoft Azure.
- Restore data from a Veeam Agent backup to Amazon EC2.
- Restore data from a Veeam Agent backup to Google Cloud Platform.
- Restore computer volumes from a Veeam Agent backup.
- Restore individual files and folders from a Veeam Agent backup.
- Restore application items from a Veeam Agent backup with Veeam Explorers.
- Export computer disks as VMDK, VHD or VHDX disks.
- Export a specific restore point in a Veeam Agent backup to a full backup (VBK) file.

Restoring Data with Veeam Recovery Media

In addition to data restore tasks available in the Veeam backup console, you can also recover data on a Veeam Agent computer using the Veeam Recovery Media. To do this, you must have a backup of the computer whose data you want to restore and the Veeam Recovery media created for this computer.

- For a Microsoft Windows computer, you can create the Veeam Recovery Media with the Veeam backup console. To learn more, see Creating Veeam Recovery Media.
- For a Linux computer, you can download the Veeam Recovery Media from the Veeam website or create a custom Veeam Recovery Media. To learn more, see the Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

The process of data restore with the Veeam Recovery Media in the Veeam Agent management scenario does not differ from the same process on a computer that runs Veeam Agent operating in the standalone mode.

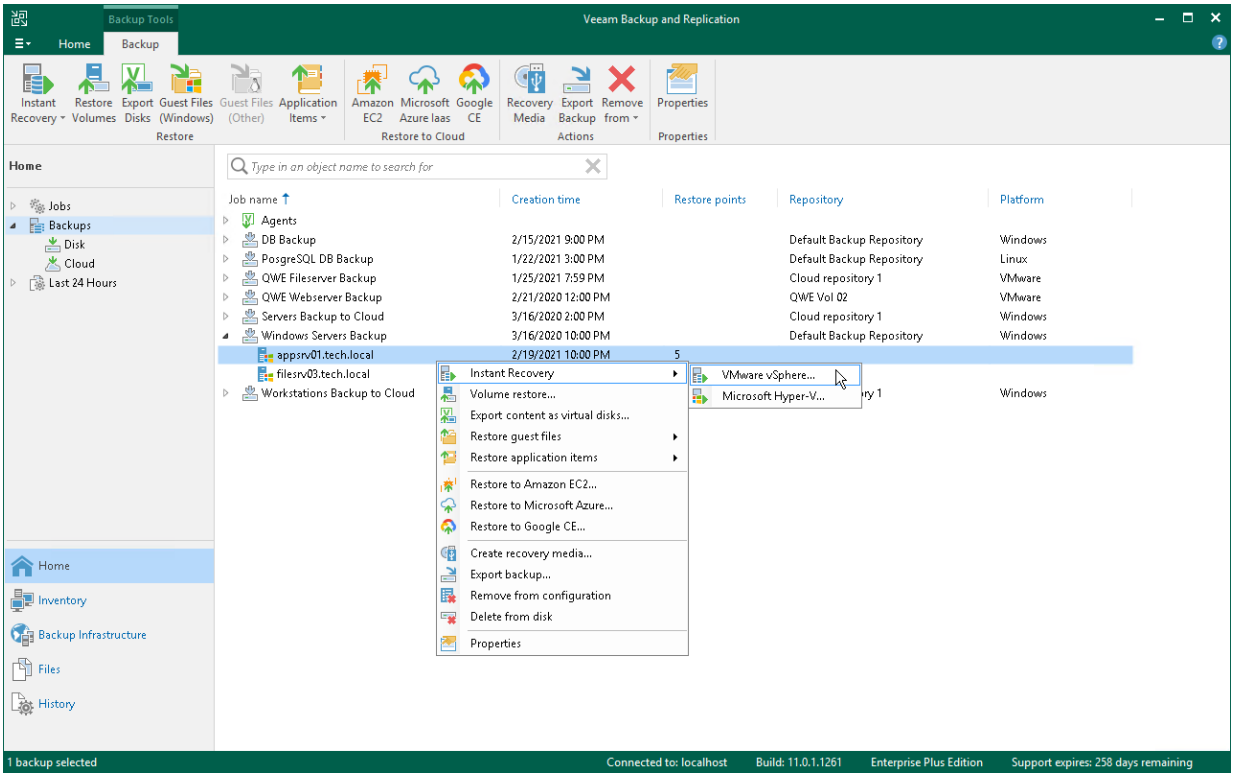
- For information on data restore with the Veeam Recovery Media on a Microsoft Windows computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.
- For information on data restore with the Veeam Recovery Media on a Linux computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

Restoring Veeam Agent Backup to vSphere VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment. For Instant Recovery to a vSphere VM, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more, see the Instant Recovery section in the Veeam Backup & Replication User Guide.



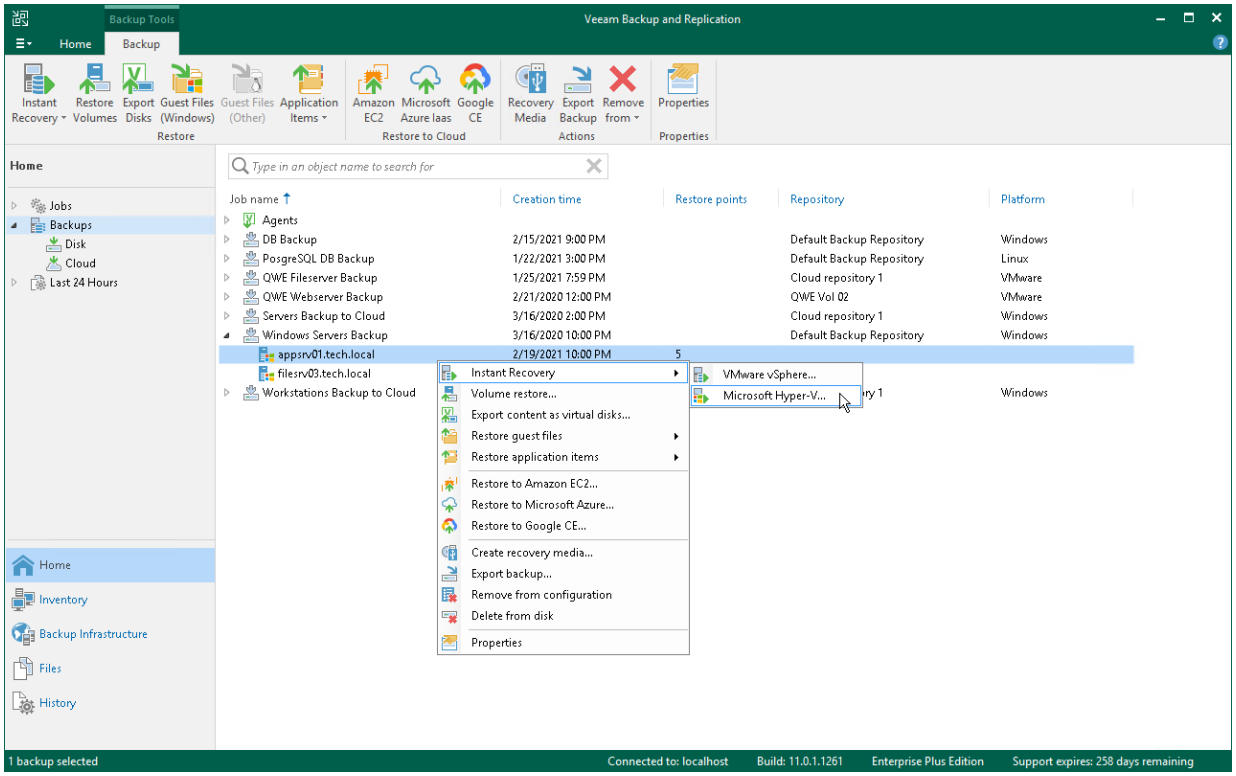
Restoring Veeam Agent Backup to Hyper-V VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For Instant Recovery to a Hyper-V VM, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot use backups created on the Veeam Cloud Connect repository for this operation.

Mind that to restore to a Hyper-V VM using a backup of a Linux computer, you must consider the Hyper-V limitations. To learn more, see this Microsoft article.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Instant Recovery section in the Veeam Backup & Replication User Guide.



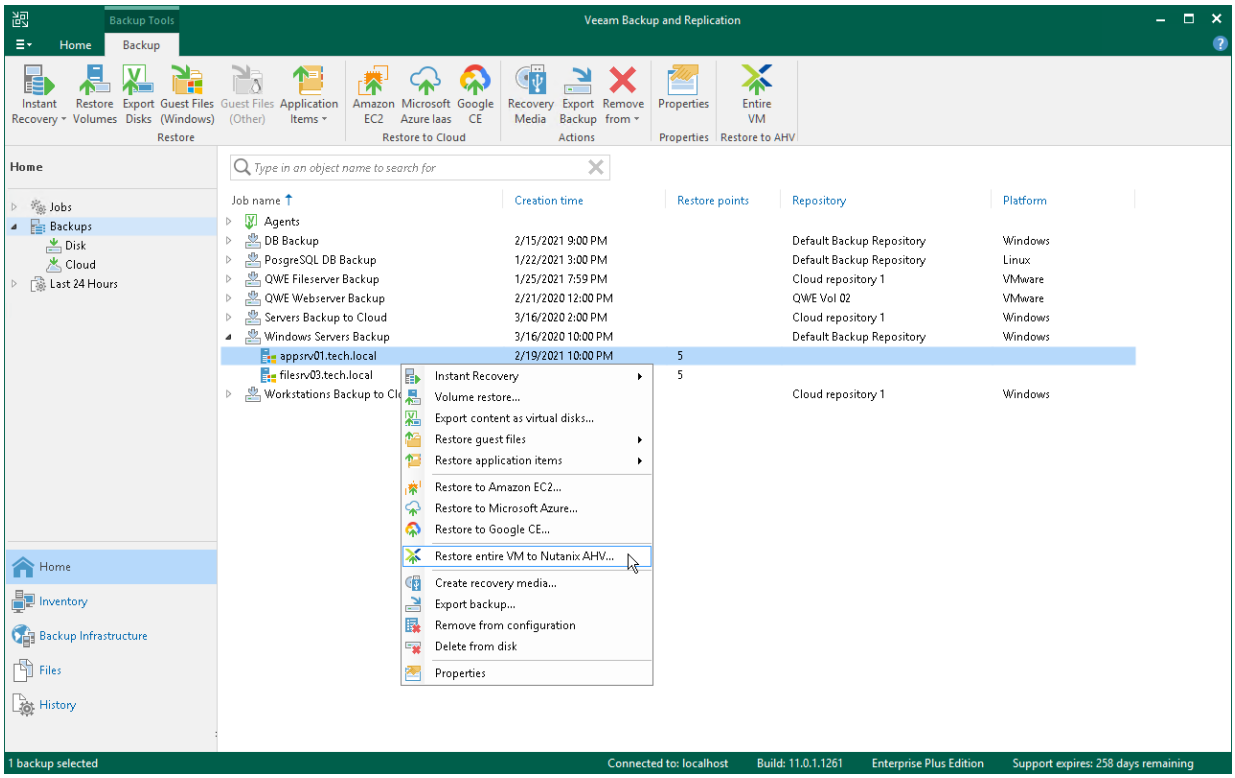
Restoring Veeam Agent Backup to Nutanix AHV VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Nutanix AHV VM in your virtualization environment. For restore to Nutanix AHV, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

Mind that to restore to Nutanix AHV, you must install Nutanix AHV Plug-in on the Veeam Backup & Replication server. To learn more, see the Installation section in the Veeam Backup for Nutanix AHV User Guide.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Nutanix AHV for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Nutanix AHV, see the Restoring VMs Using Veeam Backup & Replication Console section in the Veeam Backup for Nutanix AHV User Guide.

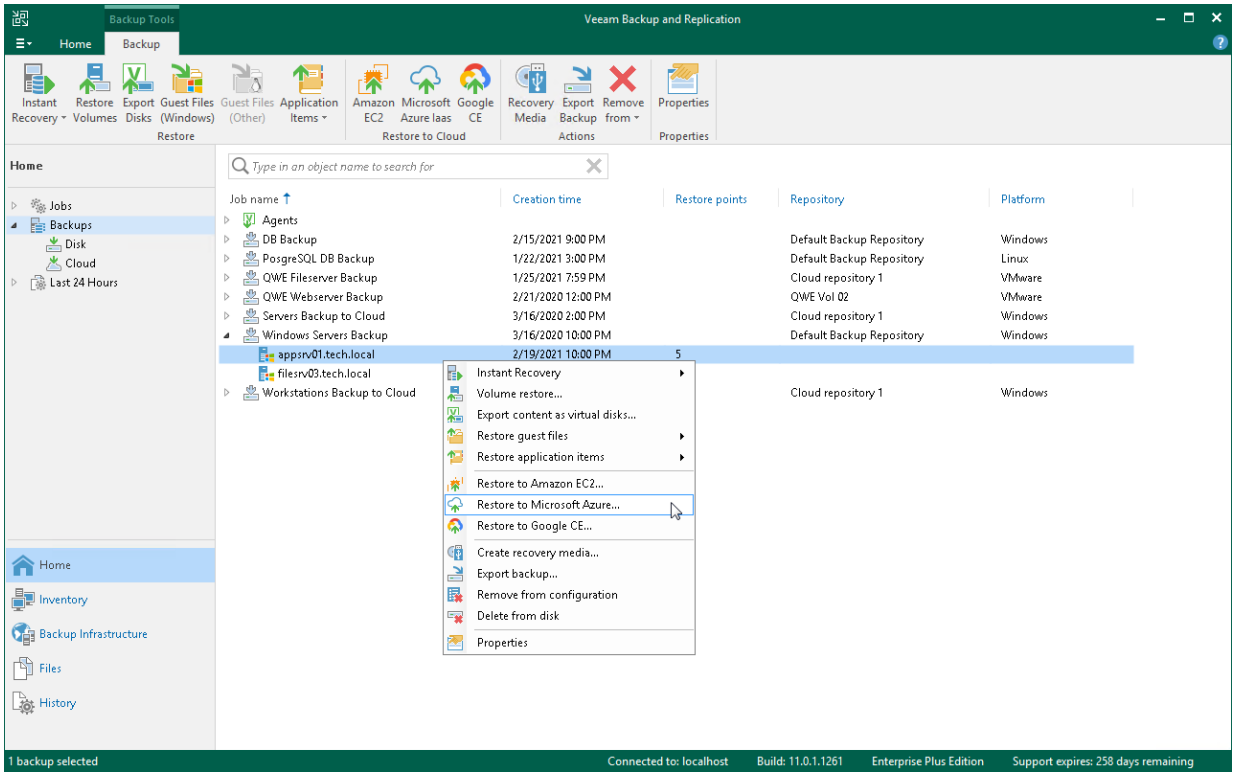


Restoring to Microsoft Azure

You can restore computers from Veeam Agent backups to Microsoft Azure. For restore to Microsoft Azure, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Microsoft Azure from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Microsoft Azure, see the Restore to Microsoft Azure section in the Veeam Backup & Replication User Guide.

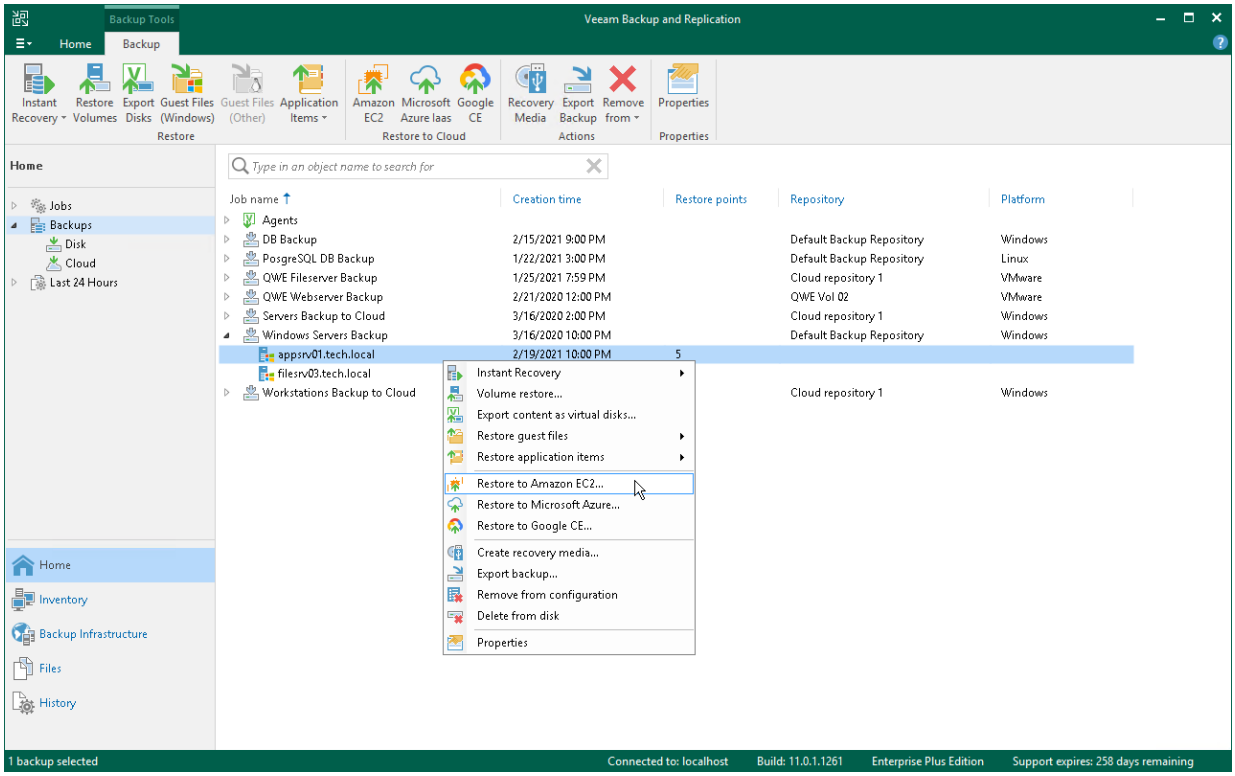


Restoring to Amazon EC2

You can restore computers from Veeam Agent backups to Amazon EC2. For restore to Amazon EC2, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Amazon EC2 from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Amazon EC2, see the Restore to Amazon EC2 section in the Veeam Backup & Replication User Guide.

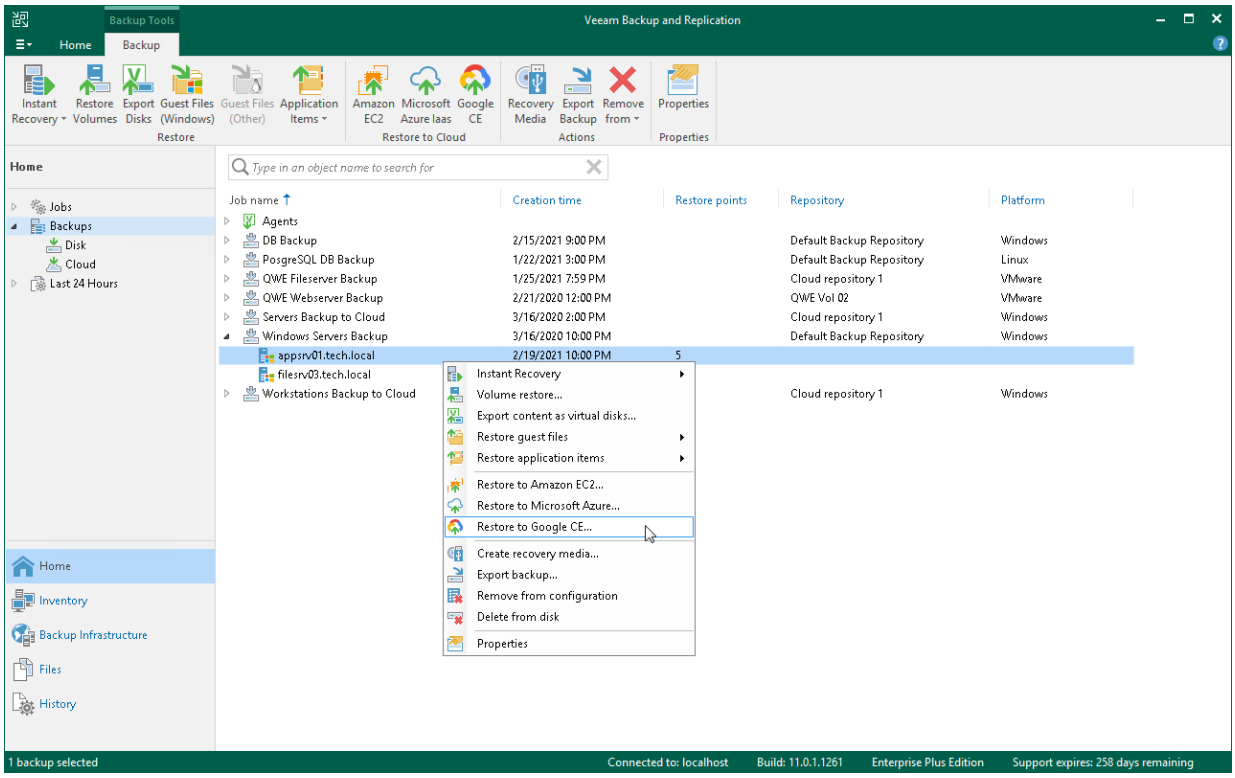


Restoring to Google Cloud Platform

You can restore computers from Veeam Agent backups to Google Cloud Platform. For restore to Google Cloud Platform, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire computer level or volume level.

> **IMPORTANT**
>
> [For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Google Cloud Platform from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Google Cloud, see the Restore to Google Cloud Platform section in the Veeam Backup & Replication User Guide.



Restoring Volumes

You can use Veeam Backup & Replication to restore a specific computer volume or all volumes from a volume-level backup created with Veeam Agent for Microsoft Windows.

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

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

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 a new location. If you restore the volume to its original location, Veeam Backup & Replication overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Backup & Replication overwrites data in the target location with data retrieved from the backup.

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

Before You Begin

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

- The volume-level backup from which you plan to restore data must be successfully created at least once.
- A computer on which you want to restore a volume must be added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows operating in the managed mode.

Volume-level restore has the following limitations:

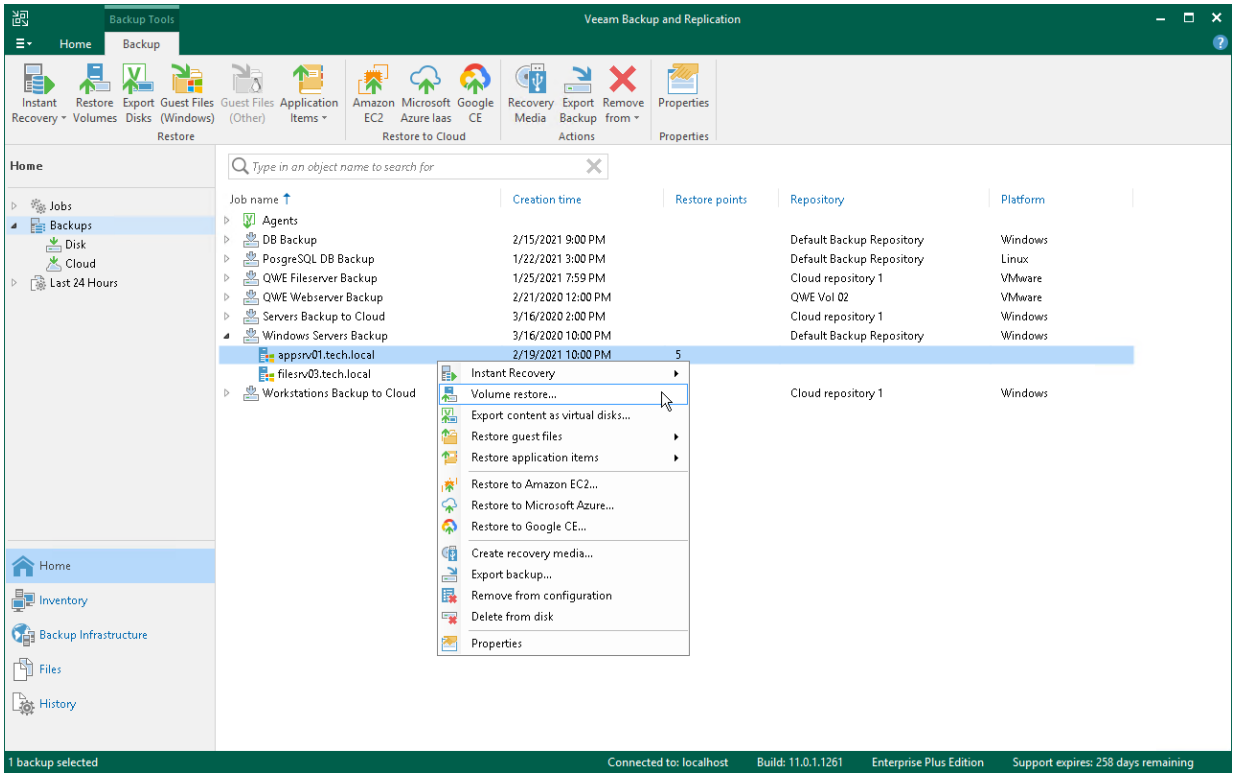
- You can restore volumes only from backups created with Veeam Agent for Microsoft Windows.
- You cannot restore a system volume to a system volume of the original Veeam Agent computer or another computer with the running OS. To perform such restore, you need to boot the OS from the recovery image. For details, see Restoring Data with Veeam Recovery Media. You can also restore a system volume to a non-system volume that has enough free space.
- You cannot restore a volume to a volume on which the Microsoft Windows swap file is hosted.

Step 1. Launch Volume Level Restore Wizard

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

- Open the **Home** tab and click **Restore** > **Agent** > **Volume restore** > **Volume restore**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the Backup step of the wizard.
- Open the **Home** view. In the inventory pane, click the **Backups** node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click **Restore Volumes** on the ribbon or right-click the computer and select **Volume restore**.

  In this case, you will proceed immediately to the Restore Point step of the wizard.

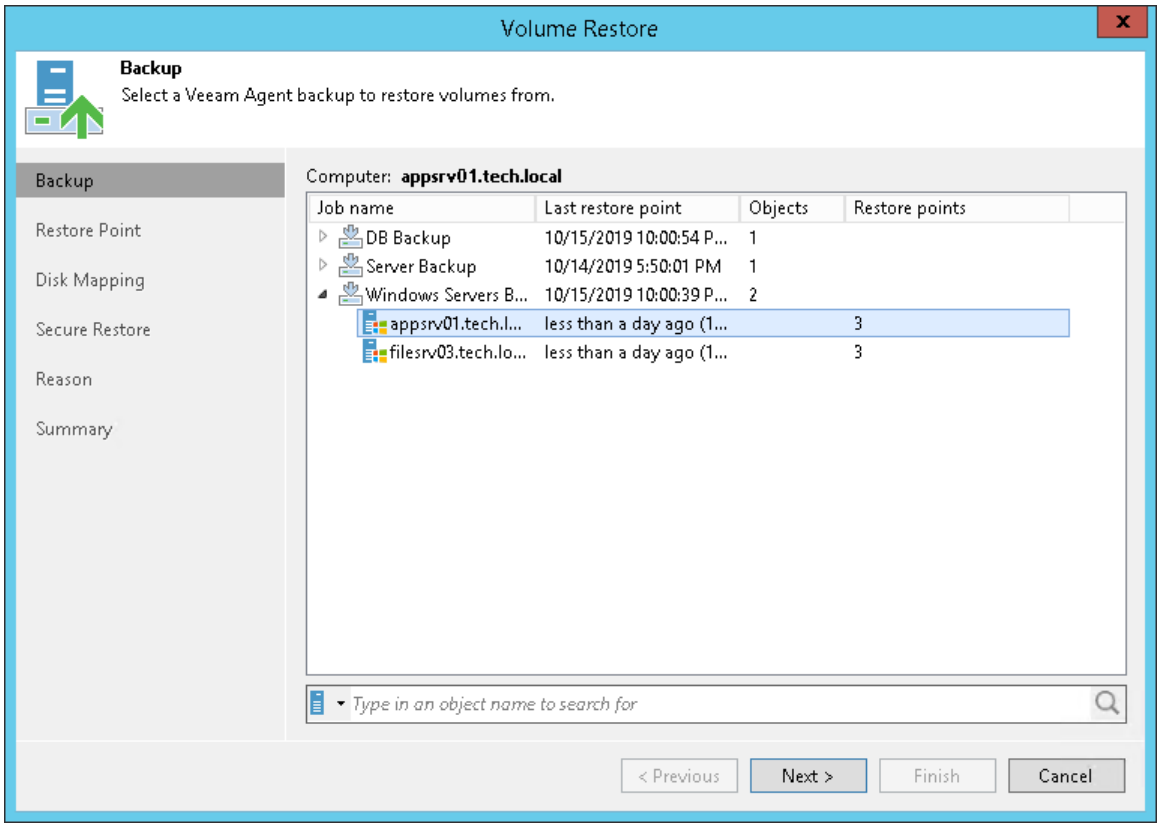


Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to recover data.

To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

In the list of backups, Veeam Backup & Replication displays only volume-level backups created with Veeam Agent for Microsoft Windows. File-level backups and backup created with Veeam Agent for Linux are not displayed.

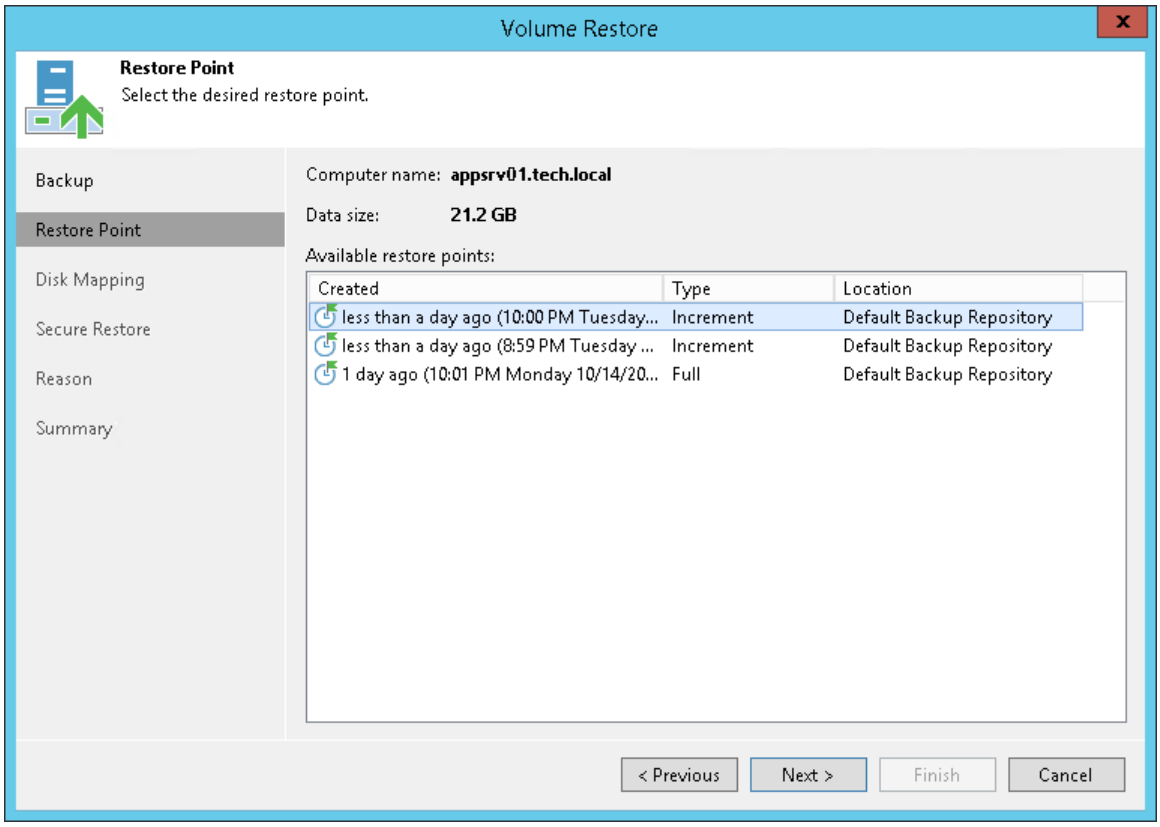


Step 3. Select Restore Point

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

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

Veeam Backup & Replication displays restore points for volume-level backups only. For example, if you have run 3 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Backup & Replication will display only 3 restore points in the list.



Step 4. Map Restored Disks

At the **Disk Mapping** step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on the target computer.

> **IMPORTANT**
>
> It is strongly recommended that you change disk mapping settings only if you have experience in working with Microsoft Windows disks and partitions. If you make a mistake, your computer data may get corrupted.

To select volumes for restore:

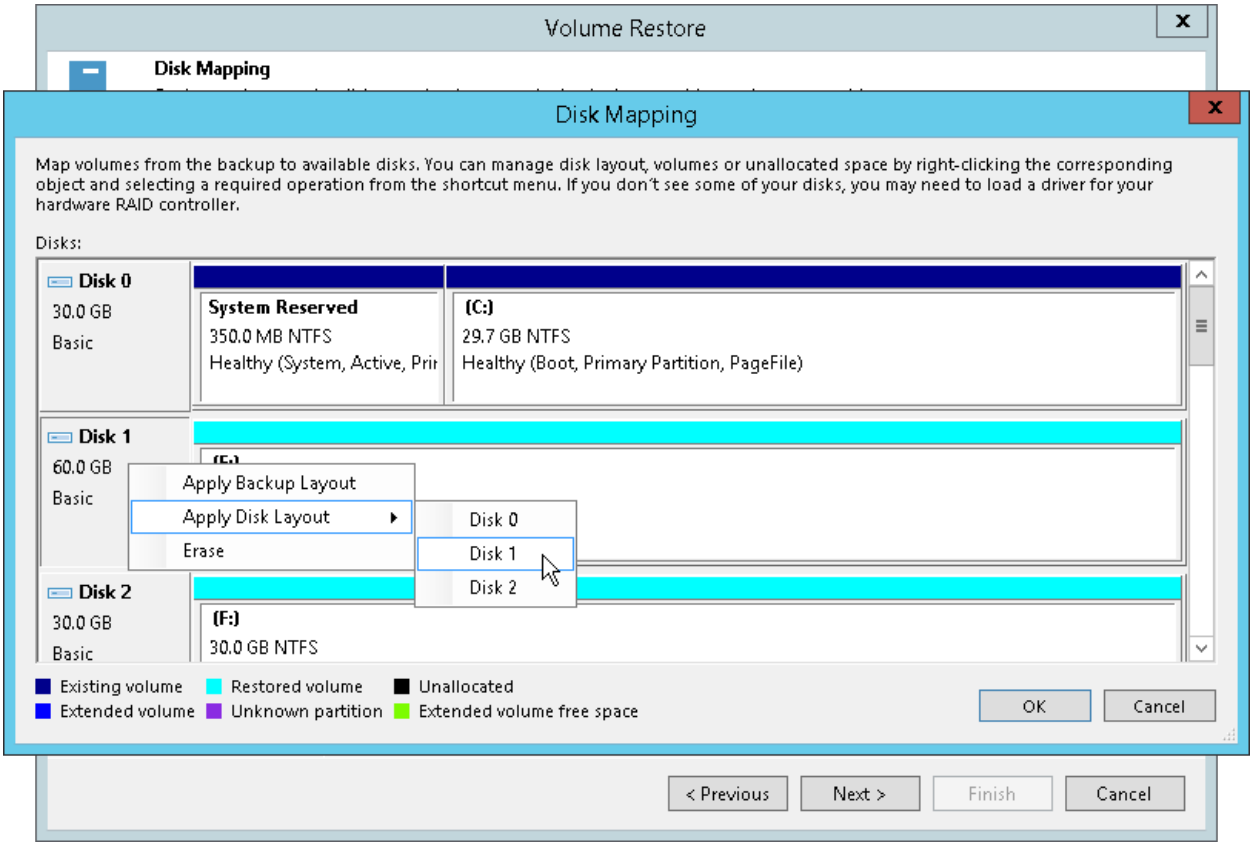
1. In the **Destination hosts** field, specify the target computer where you want to restore volumes. By default, Veeam Backup & Replication restores volumes to their original location. If you want to restore volumes from the backup to another computer, click **Choose** and select the necessary computer. You can restore volumes only to computers that are added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows.

   If you select a computer included in a protection group for pre-installed Veeam Agents, you must provide credentials of the account that has administrator permissions on the target computer. Keep in mind that Veeam Backup & Replication will keep these credentials only during the restore process and delete them after the restore process completion. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

2. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. If you want to map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**.

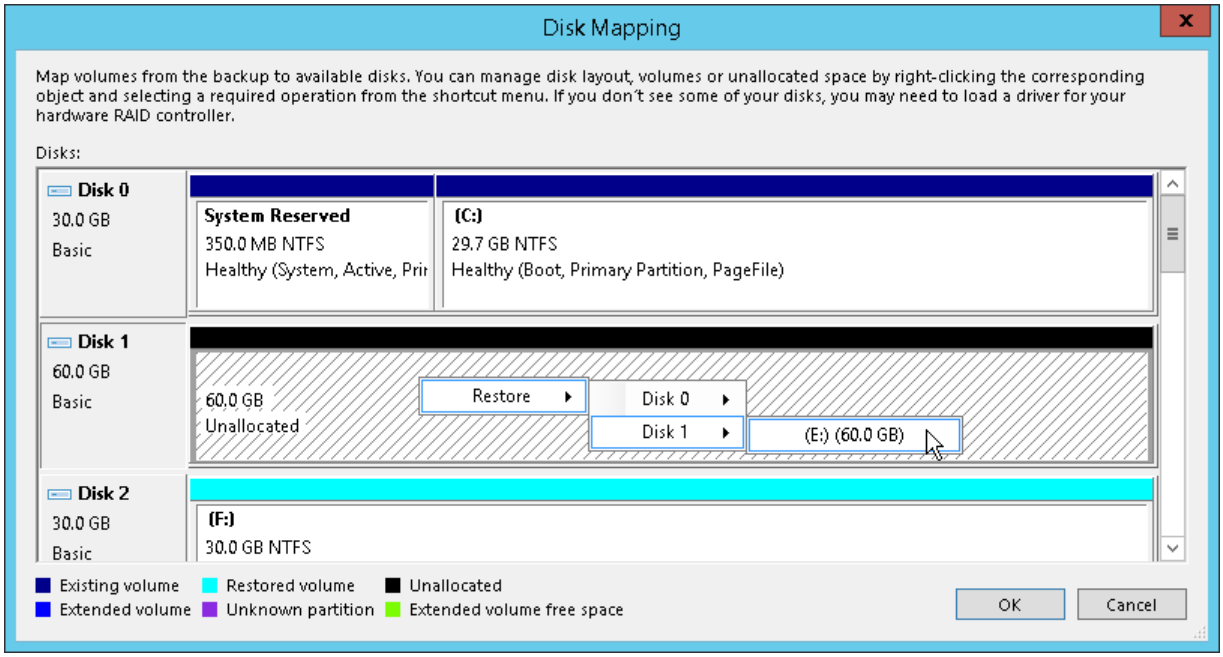
   > **NOTE**
   >
   > If Veeam Backup & Replication cannot map a volume automatically, Veeam Backup & Replication will prompt you to perform disk mapping manually. To proceed to the **Disk Mapping** window, click **Yes**.

3. At the **Disk Mapping** window, specify how volumes must be restored:
   - Right-click the target disk on the left and select the necessary disk layout:
     - **Apply Backup Layout** – select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.
     - **Apply Disk Layout** – select this option if you want to apply to the current disk settings of another disk.
     - **Erase** – select this option if you want to discard the current disk settings.



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

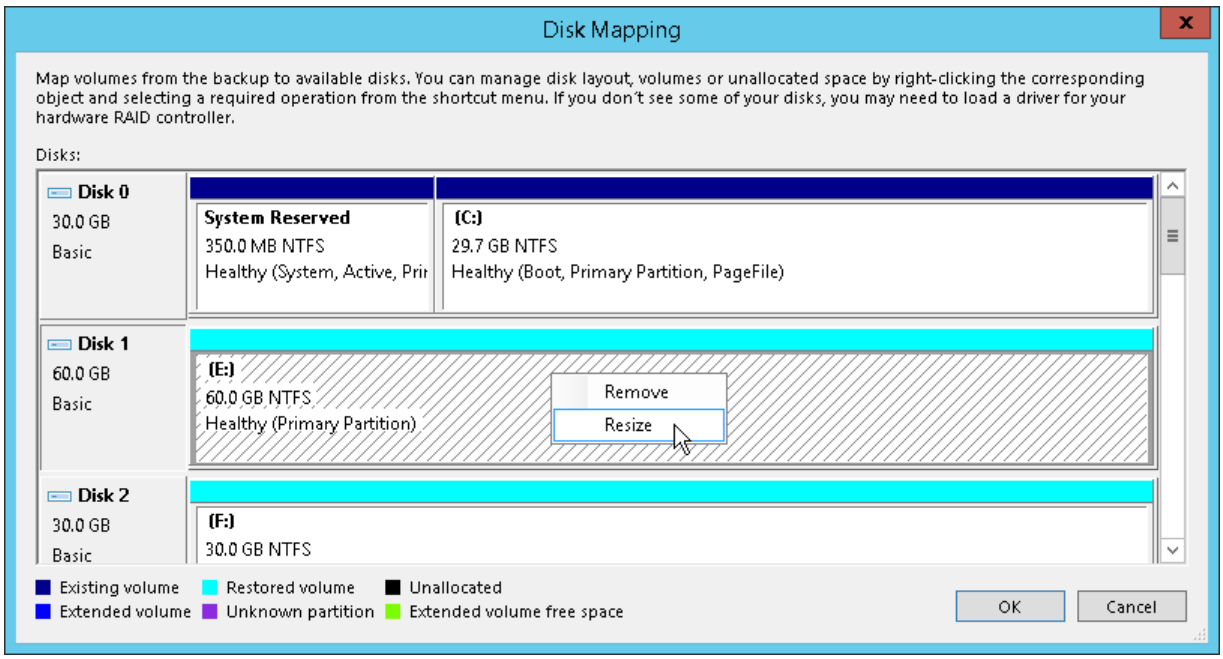
  If you want to change disk layout configured by Veeam Backup & Replication, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.



4. [For restore with volume resize] You can resize a volume mapped by Veeam Backup & Replication to a target computer disk. To resize a volume, right-click it in the **Disk Mapping** window and select **Resize**. With this option selected, you will pass to the Volume Resize window.

NOTE

If you map a backup volume that is larger than the amount of available space on the target disk, Veeam Backup & Replication will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Backup & Replication will prepare to shrink the volume to the size of available disk space.



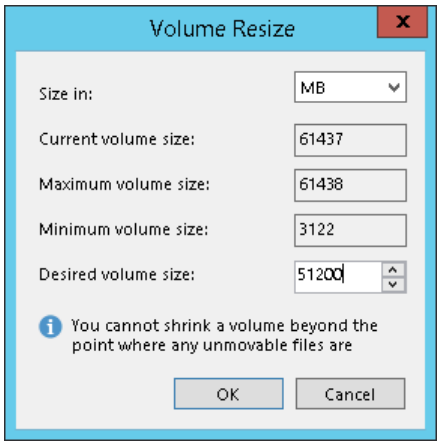
Step 5. Resize Restored Volumes

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

> **NOTE**
>
> By default, Veeam Agent for Microsoft Windows displays volume size in megabytes (MB). This allows you to specify the desired size for the volume precisely. You can also choose to display volume size in gigabytes (GB). This may be helpful when you need to resize volumes on larger computer disks and want to simplify disk size calculations.
>
> When you use GB as a volume size unit, you can specify volume size with integral numbers, for example, 1 GB, 60 GB or 200 GB, but not 0,8 GB, 60,5 GB or 200,7 GB. However, if the maximum volume size is in fact greater than the displayed value for less than 1 GB, Veeam Agent for Microsoft Windows will automatically add the exceeding amount of disk space to the extended volume. For example, if the maximum volume size is 60,2 GB, Veeam Agent for Microsoft Windows will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Agent for Microsoft Windows will extend the volume to 60,2 GB.

To resize a volume:

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

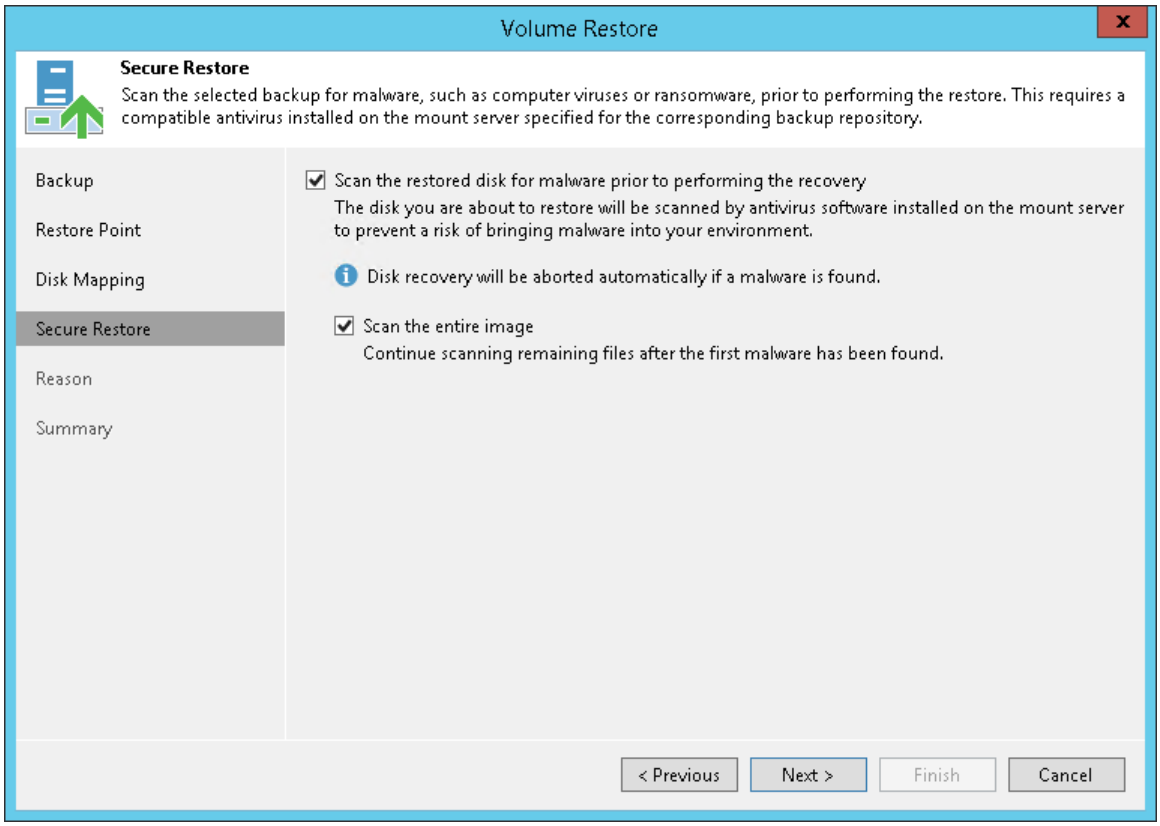


Step 6. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan restored volume data with antivirus software before restoring the volume. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

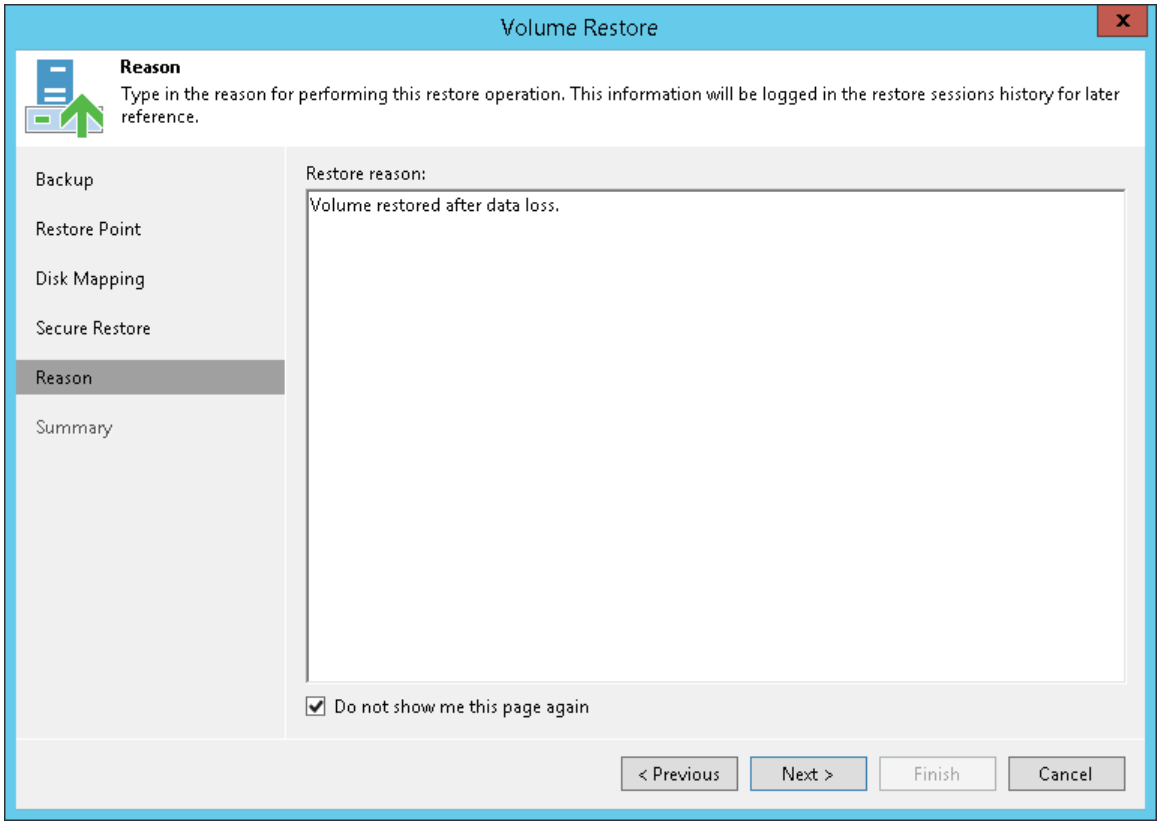
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. Select the **Scan the entire image** check box if you want the antivirus software to continue volume scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Antivirus Scan Results section in the Veeam Backup & Replication User Guide.



Step 7. Specify Restore Reason

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

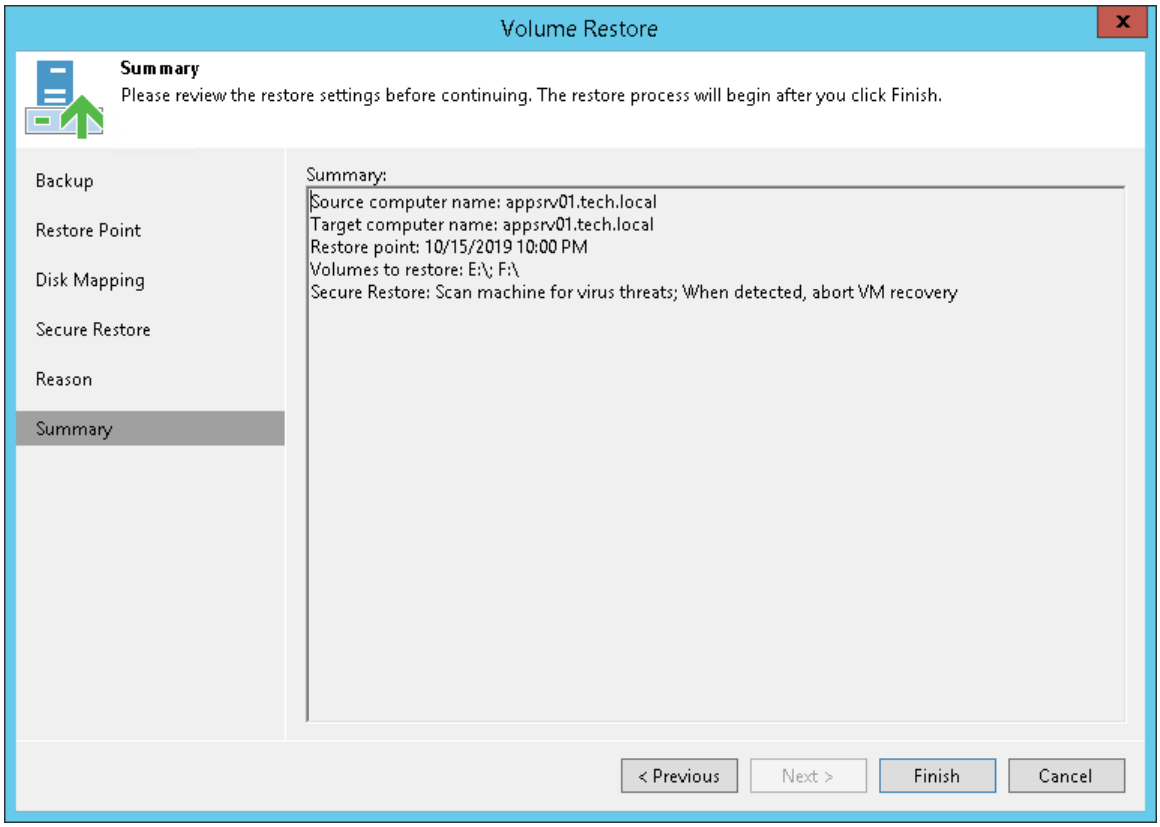
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of volume-level restore.

1. Review settings of the restore process.
2. Click **Finish** to start the recovery process. Veeam Backup & Replication will perform partition re-allocation operations if necessary, restore the necessary volume data from the backup and overwrite volume data on the target computer with the restored data.



Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups. The procedure of file-level restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the **File Level Restore** wizard. To learn more, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.

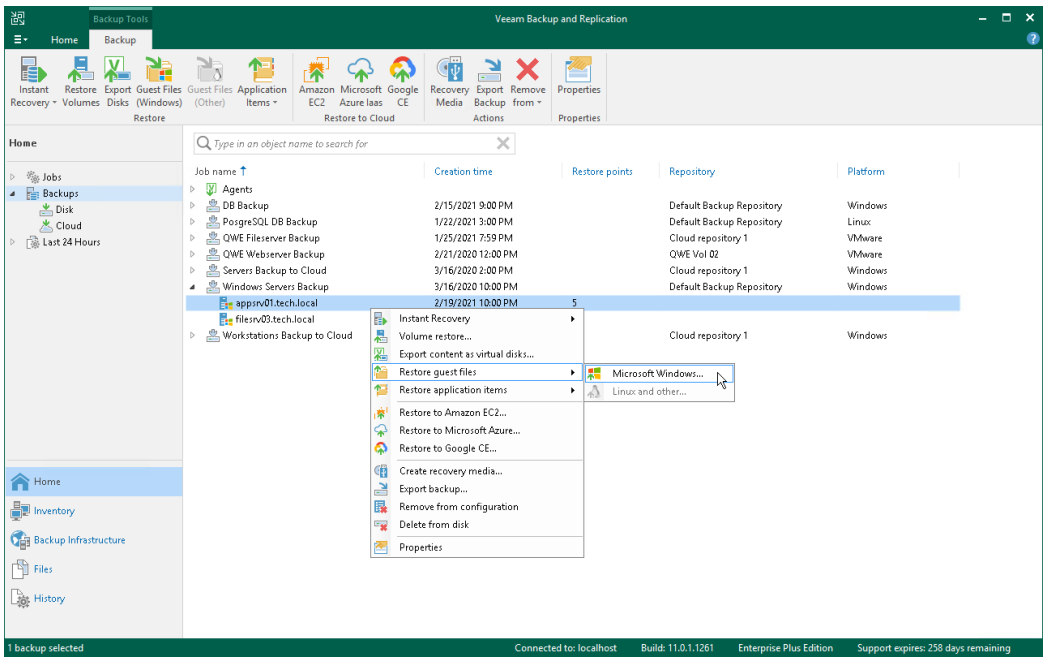
Consider the following:

- When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux computer from the backup or replica:
  - Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host.
  - Mounting disks to a helper appliance — a helper VM required to mount Linux computer disks from the backup.

    If you have selected to mount disks to a helper appliance, it is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as *orphaned*.

  To learn more about these options, see the Restore from Linux, Unix and Other File Systems section in the Veeam Backup & Replication User Guide.
- Before you start file-level restore from a backup of a failover cluster, make sure that the cluster is added to a protection group in the Veeam Backup & Replication inventory. The failover cluster may be not present in the inventory, for example, in the following cases:
  - The original protection group that contained the cluster was removed from Veeam Backup & Replication.
  - You want to restore cluster data from a backup created on another backup server and imported in the Veeam backup console.

  In this case, add the failover cluster whose data you want to restore to a protection group.



Restoring Application Items

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

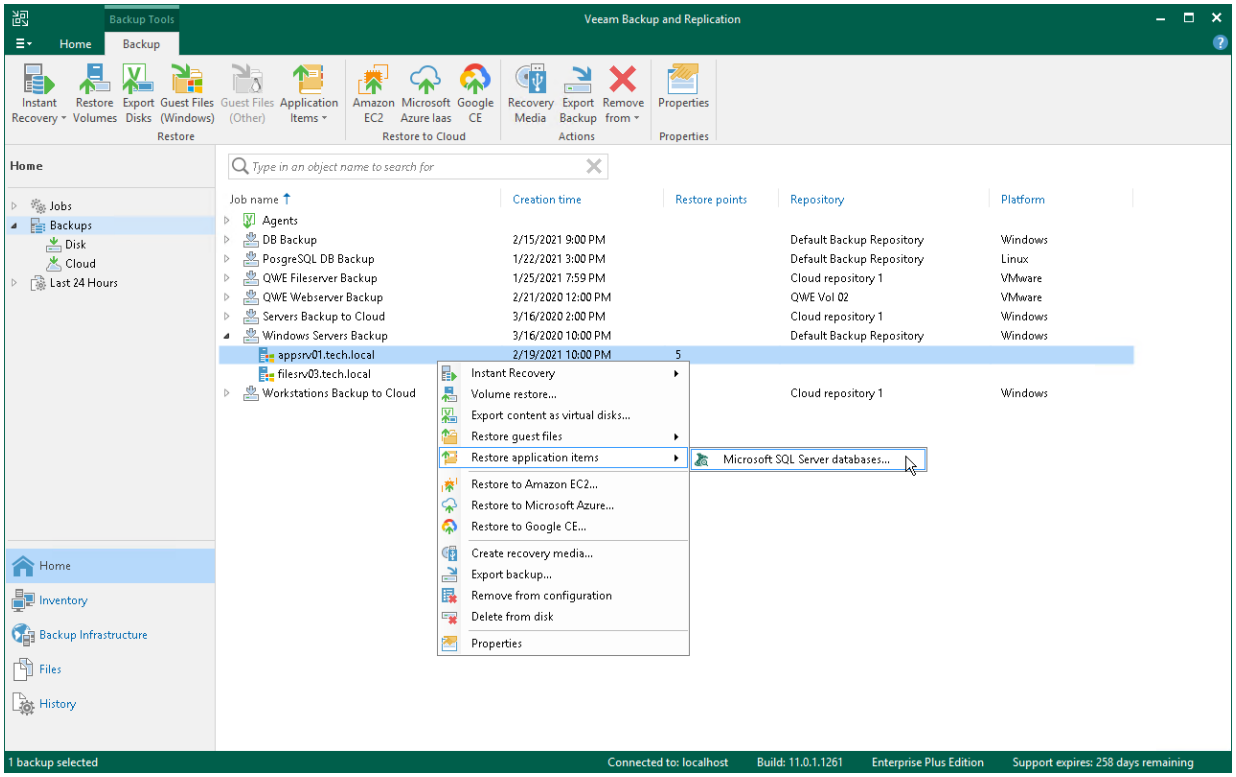
From backups created with Veeam Agent for Microsoft Windows

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

From backups created with Veeam Agent for Linux

- Oracle

The procedure of application-item restore from a Veeam Agent backup does not differ from the same procedure for a VM backup. To learn more, see the Restoring Application Items section in the Veeam Backup & Replication User Guide.



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 Backup & Replication creates standard virtual disks that can be used by VMware vSphere and Microsoft Hyper-V VMs.

- When you restore a disk in the VMDK format, Veeam Backup & Replication creates a pair of files that make up the VM virtual disk: a descriptor file and file with the virtual disk content.
- When you restore a disk in the VHD/VHDX format, Veeam Backup & Replication creates a file of the VHD or VHDX format.

You can save converted disks locally on any server added to the backup infrastructure or place disks on a datastore connected to an ESXi host (for VMDK disk format only). VMDK disks can be restored as thin provision and thick disks:

- Disks restored to a datastore are saved in the thin provisioned format.
- Disks restored to a server are saved in the thick format.

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

> **IMPORTANT**
>
> If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

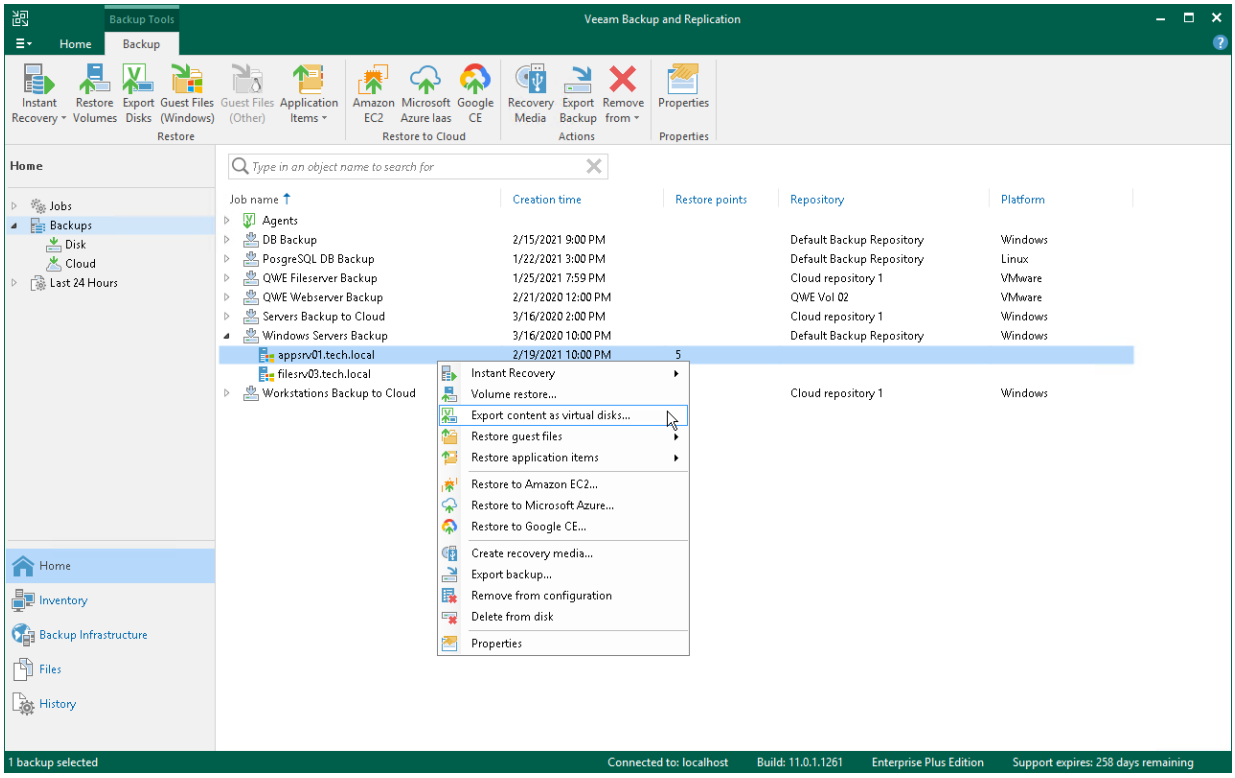
To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

- Open the **Home** tab and click **Restore** > **Agent** > **Disk restore** > **Export disk**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the Backup step of the wizard.
- Open the **Home** view. In the inventory pane, click the **Backups** node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click **Export Disks** on the ribbon or right-click a computer in the backup and select **Export disk content as virtual disks**.

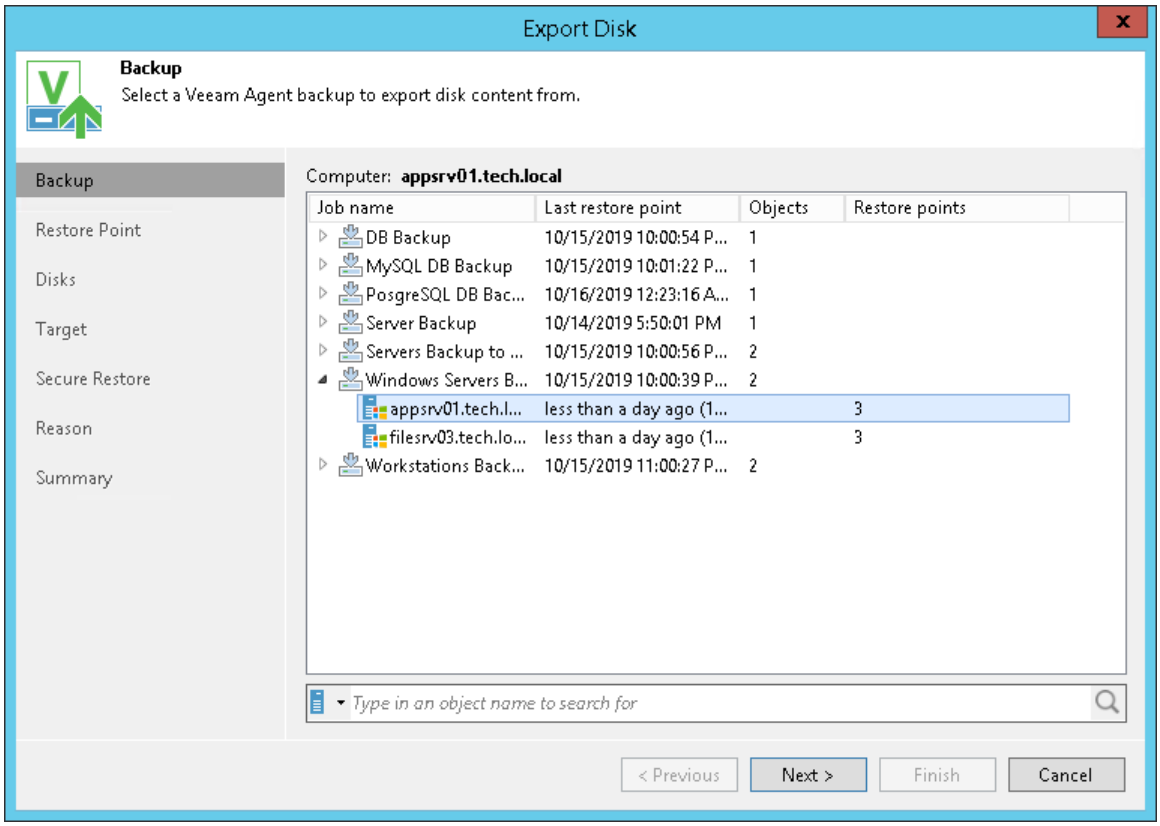
  In this case, you will pass immediately to the Restore Point step of the wizard.



Step 2. Select Backup

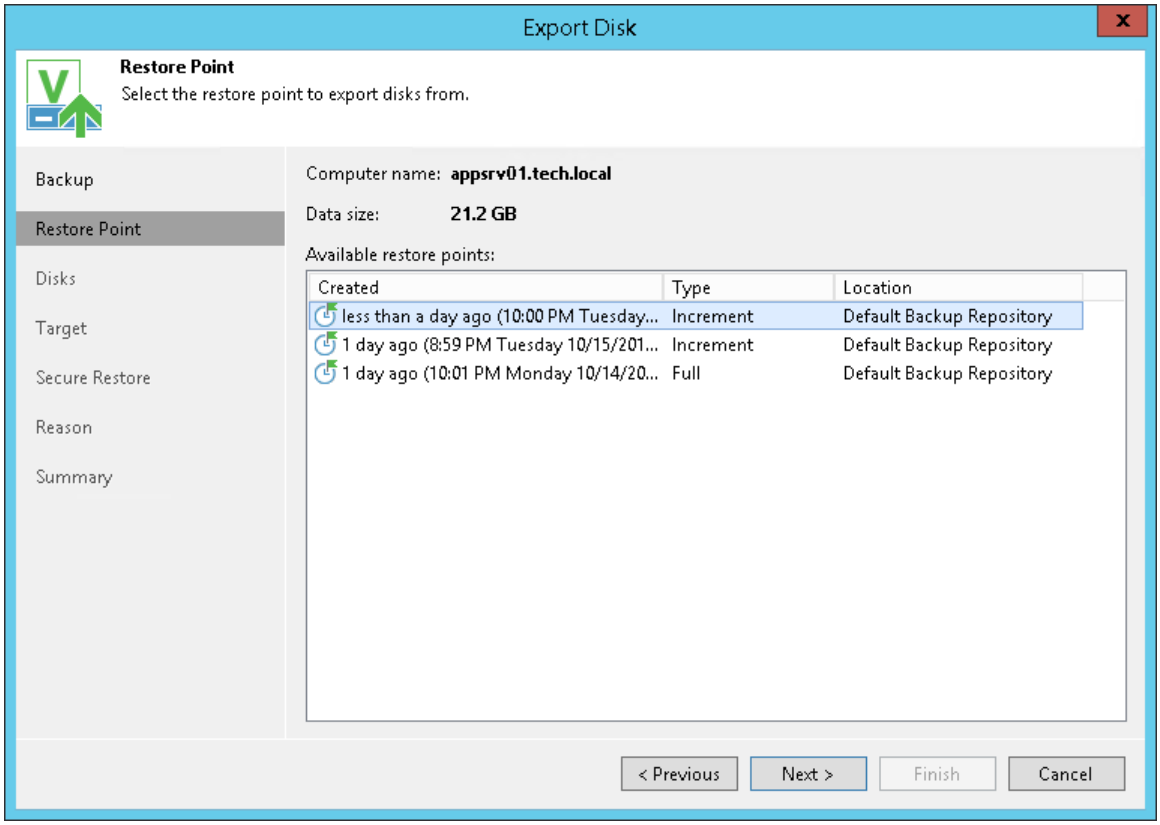
At the **Backup** step of the wizard, select a backup from which you want to restore disks. In the list of backups, Veeam Backup & Replication displays all backups that are currently hosted on the Veeam backup repository.

Make sure that you select a volume-level backup in the list.



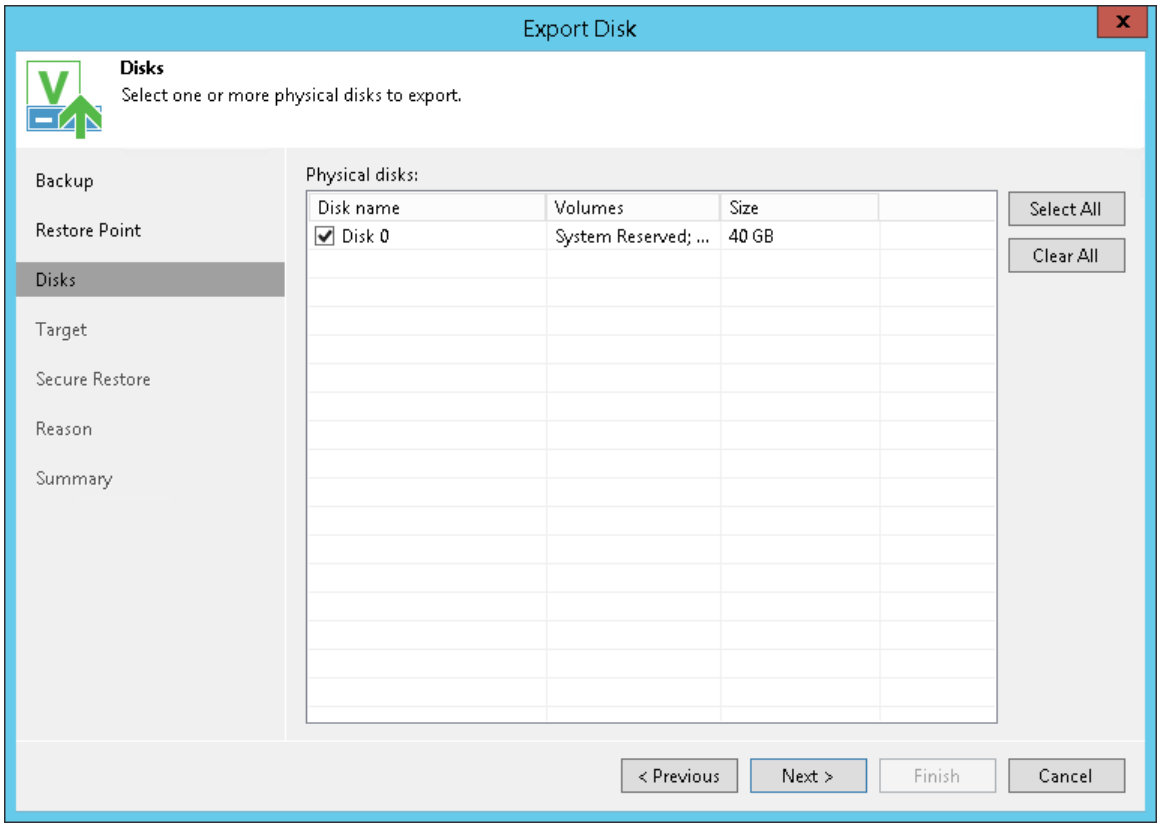
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disks. In the list of points, Veeam Backup & Replication displays all restore points that have been created. Make sure that you select a restore point that relates to a volume-level backup.



Step 4. Select Disks

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



Step 5. Select Destination and Disk Format

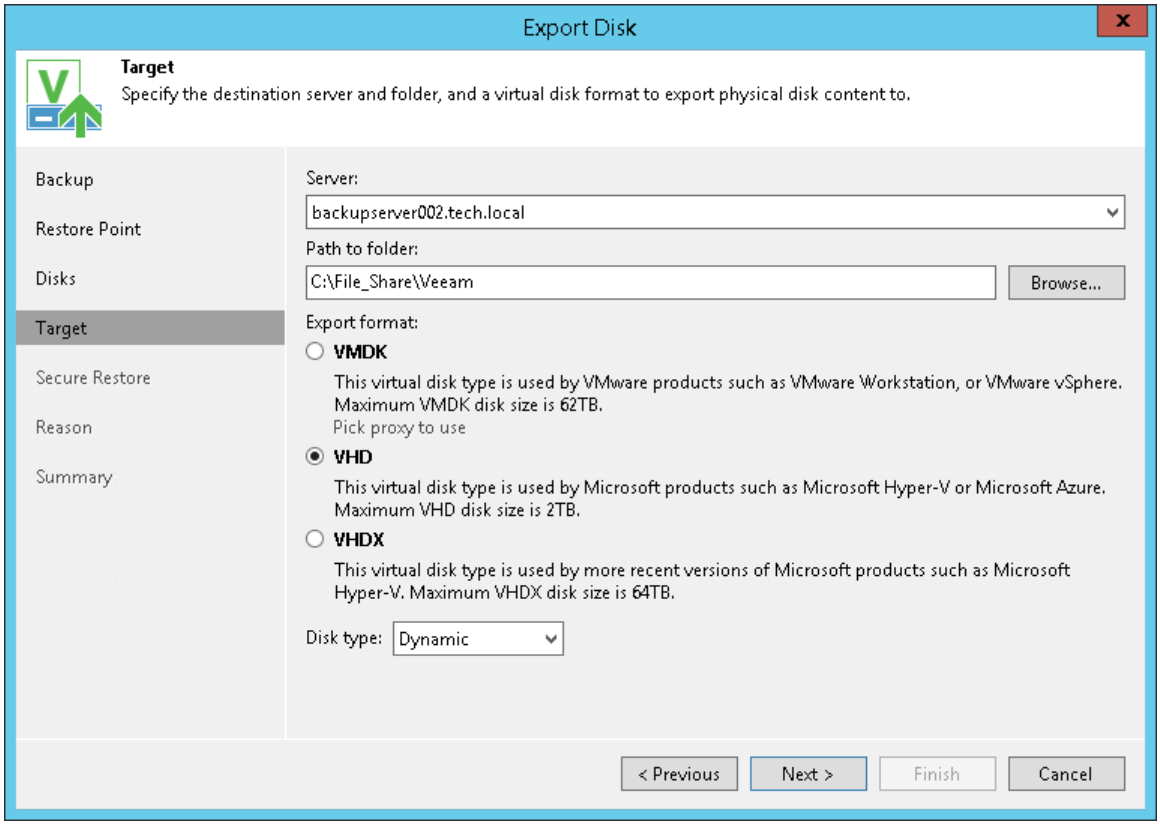
At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

1. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.
2. In the **Path** to folder field, specify a folder on the server or datastore where the virtual disks must be placed.
3. Select the export format for disks:
   - **VMDK** — select this option if you want to save the resulting virtual disk in the VMware VMDK format.
   - **VHD** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHD format.
   - **VHDX** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).
4. Click **Disk type** to specify how the resulting disk must be saved:
   - [For VMDK disk format] in the thin provisioned, lazy zeroed thick provisioned, or eagerly zeroed thick provisioned format
   - [For VHD and VMDX disk formats] in the dynamic or fixed format
5. [For export of a VMDK disk to an ESXi host] Click the **Pick proxy to use** link to select backup proxies over which backup data must be transported to the target datastore.

NOTE

Consider the following:

- If you have selected to store the resulting virtual disk to a datastore, you will be able to save the virtual disk in the VMDK format only. Other options will be disabled.
- If you have selected to store the resulting virtual disk on the server running Microsoft Windows Server OS and in the VMDK format, you will be able to save the virtual disk in the lazy zeroed thick provisioned format only.



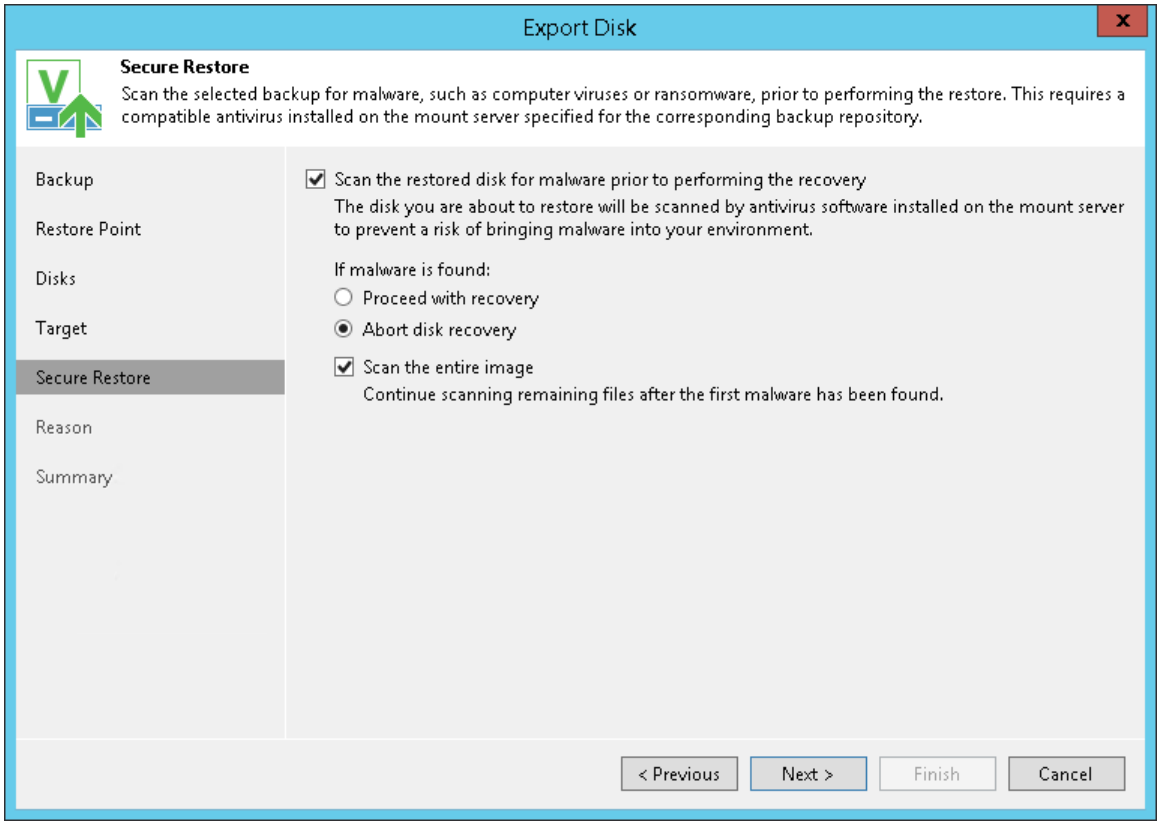
Step 6. Specify Secure Restore Settings

The **Secure Restore** step of the wizard is available if you export disks from a Veeam Agent backup of a Microsoft Windows computer.

At this step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan restored disk data with antivirus software before restoring the disk. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

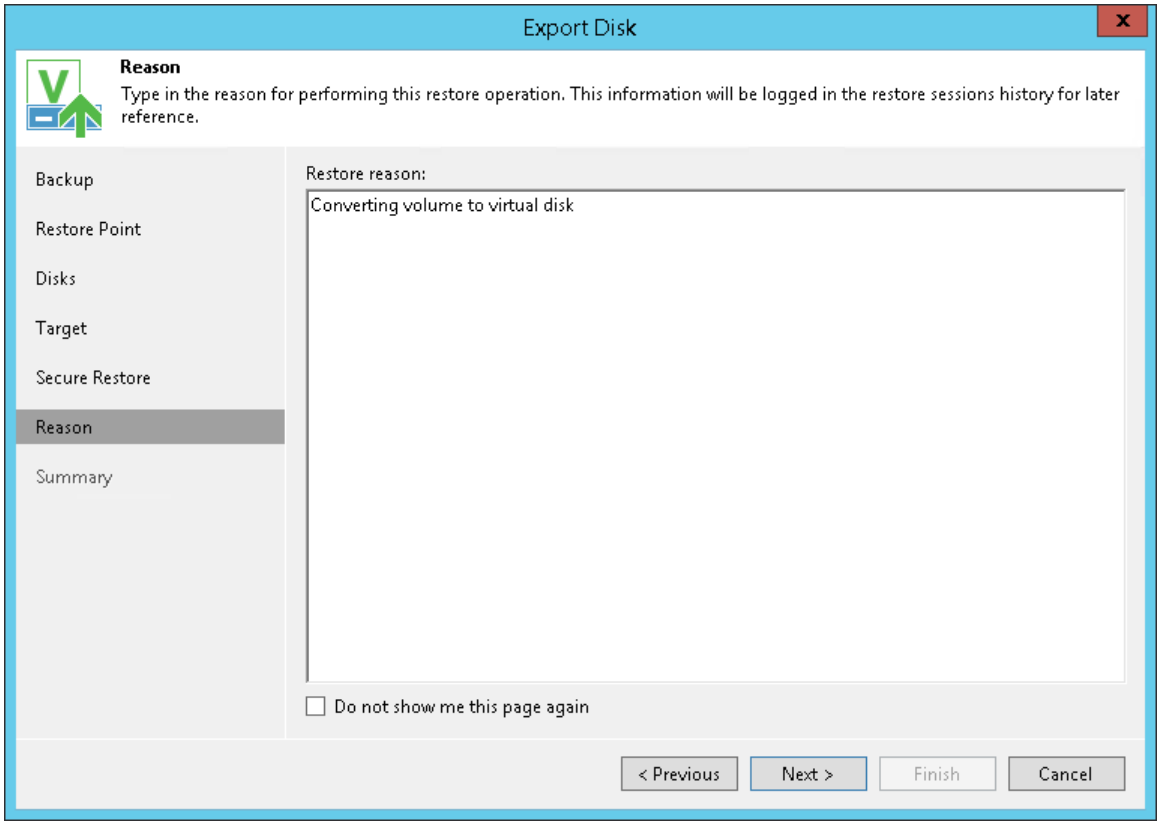
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. Specify how the antivirus software must behave after the first malware thread is found: continue or abort disk scan.
3. Select the **Scan the entire image** check box if you want the antivirus software to continue disk scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Antivirus Scan Results section in the Veeam Backup & Replication User Guide.



Step 7. Specify Restore Reason

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

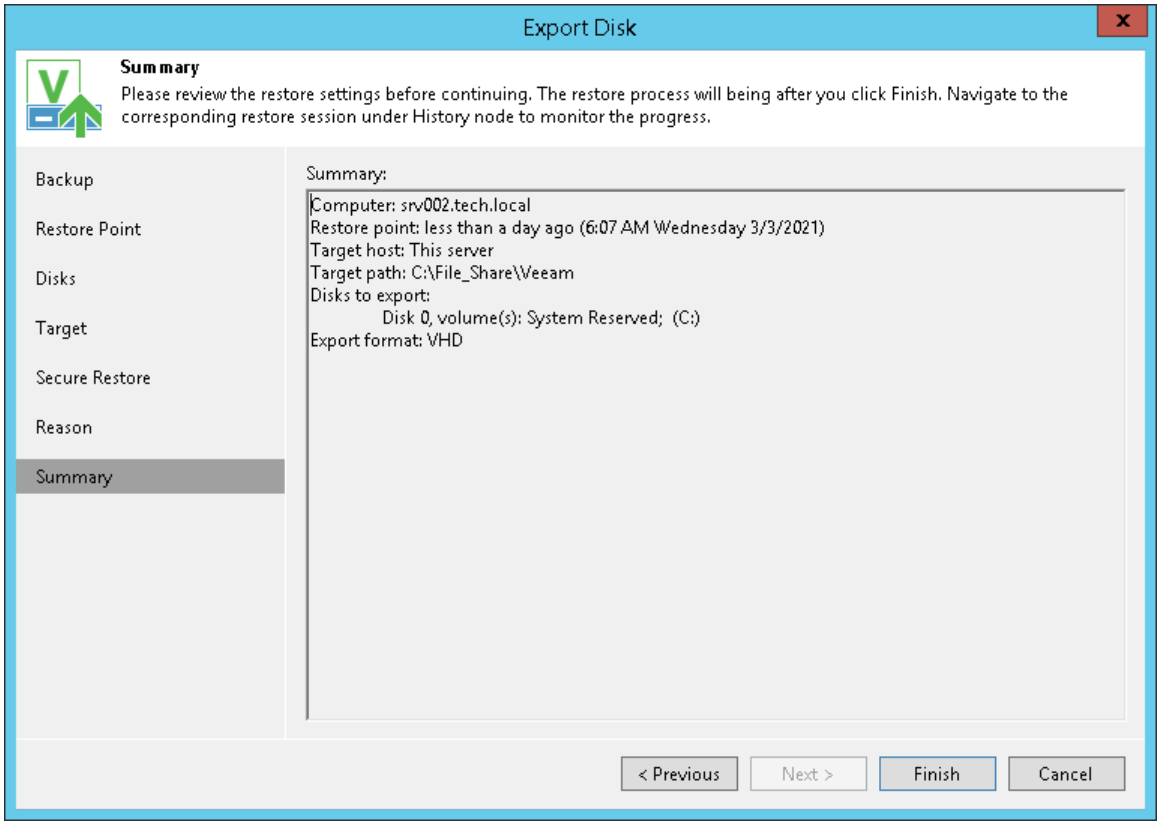
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. Complete Restore Process

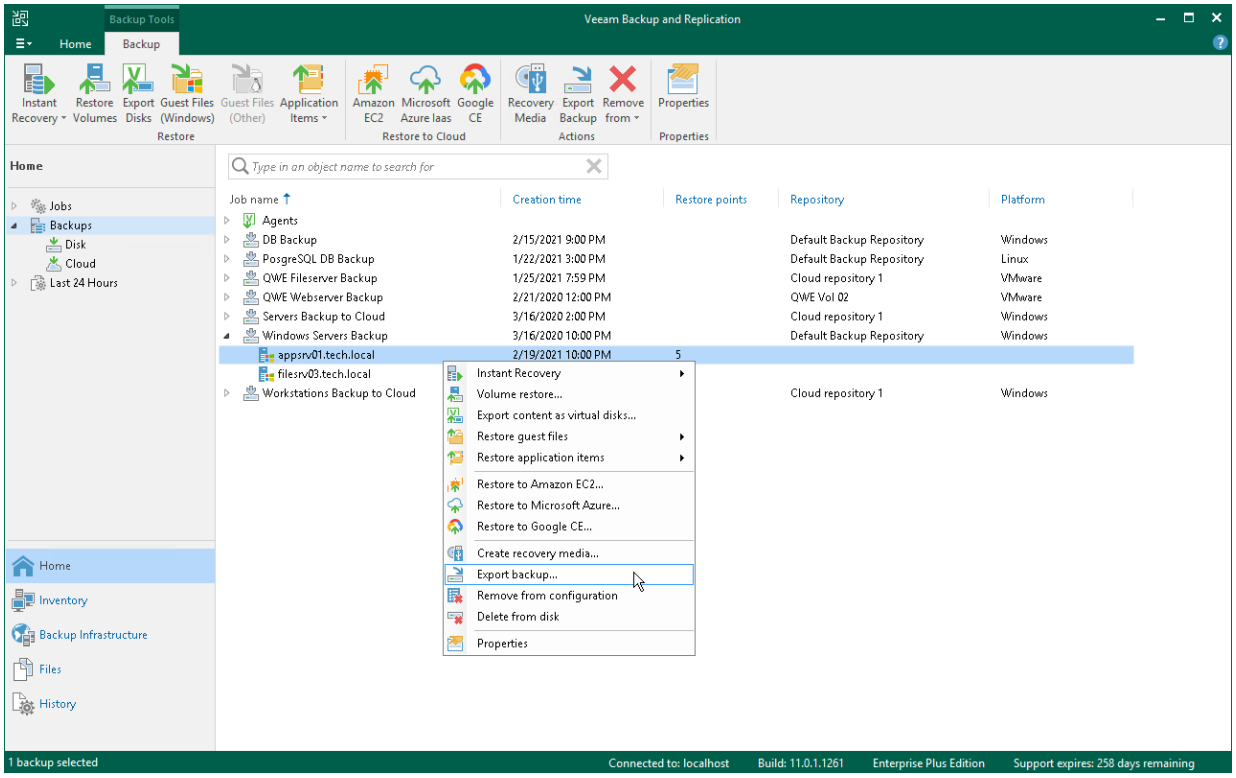
At the **Summary** step of the wizard, complete the disk restore procedure.

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



Exporting Restore Point to Full Backup File

You can restore data from a specific restore point in a Veeam Agent backup and export this data to a standalone full backup file. The procedure of Veeam Agent backup export does not differ from the same procedure for a VM. To learn more, see the Exporting Backups section in the Veeam Backup & Replication User Guide.



Managing Veeam Agent Backups

You can perform administration tasks with backups created on a Veeam backup repository by Veeam Agent backup jobs configured in Veeam Backup & Replication. For such Veeam Agent backups, Veeam Backup & Replication allows you to perform the same set of operations as for backups created with Veeam Agent backup jobs configured directly on a Veeam Agent computer. You can perform the following tasks:

- Create the Veeam Recovery Media for a computer in backup.
- Remove a Veeam Agent backup from configuration.
- Delete a Veeam Agent backup from disk.
- View properties of a Veeam Agent backup.

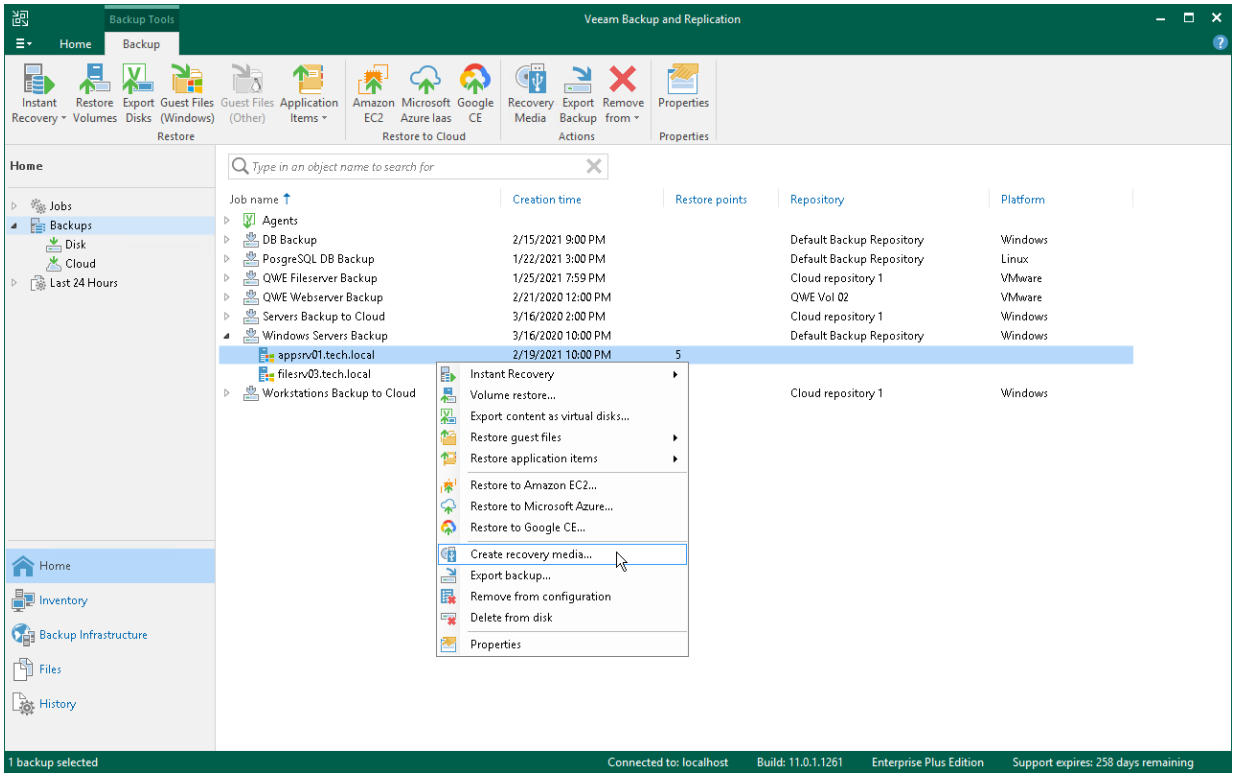
Creating Veeam Recovery Media from Backup

You can create the Veeam Recovery Media for a computer whose Veeam Agent backup resides on a Veeam backup repository. For this operation, you can use a backup created by any type of a Veeam Agent backup job: a backup job managed by the backup server or backup job managed by Veeam Agent (backup policy).

Creating the Veeam Recovery Media for a computer in a backup does not differ from creating the Veeam Recovery Media for a protected computer in the Veeam Backup & Replication inventory. To learn more, see Creating Veeam Recovery Media.

To create Veeam Recovery Media:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, expand the Veeam Agent backup, select the necessary computer in the backup and click **Recovery Media** on the ribbon or right-click the computer and select **Create recovery media**.
4. Complete the steps of the **Create Recovery Media** wizard.



Removing Backup from Configuration

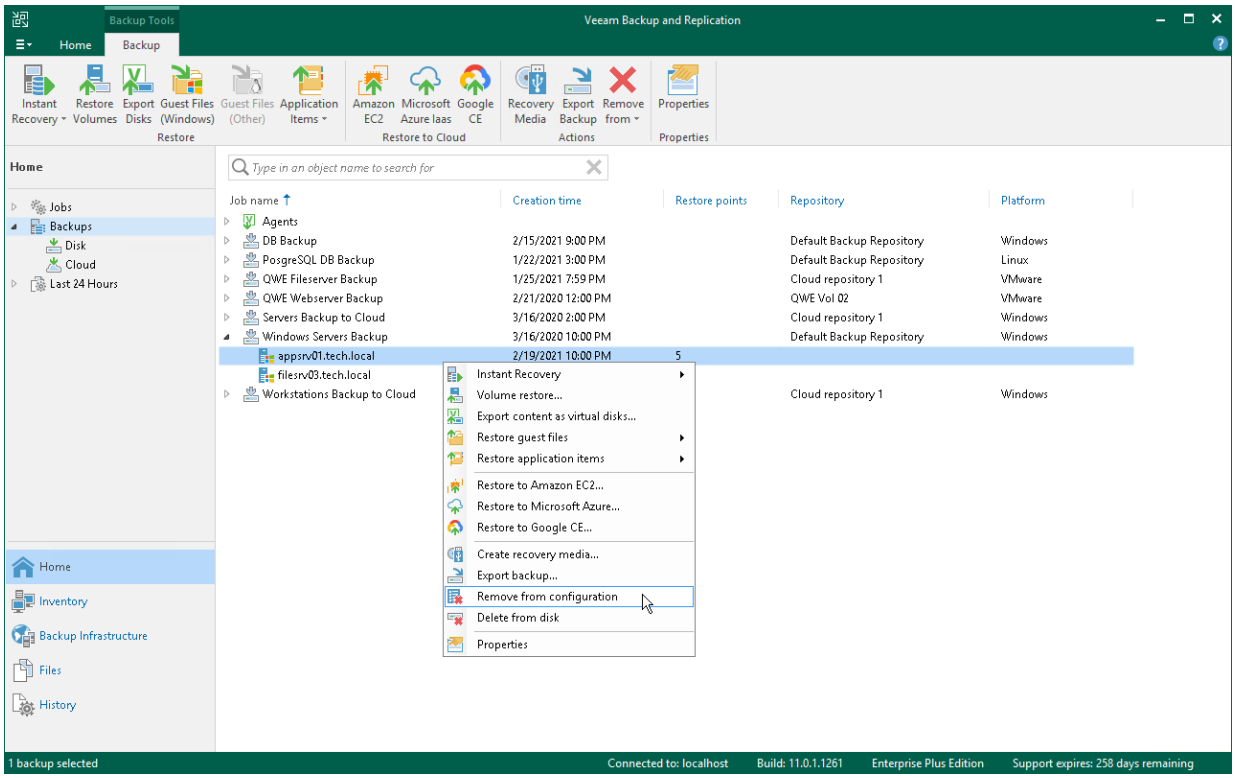
If you want to remove records about Veeam Agent backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation. When you remove a Veeam Agent backup from configuration, the actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it.

> **NOTE**
>
> Mind the following:
>
> - You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam backup console.
> - The **Remove from configuration** operation is not available for backups created on the Veeam Cloud Connect repository.
> - If you remove from configuration a backup of a failover cluster node, all backups of this failover cluster will be removed.

You can remove an entire backup related to a Veeam Agent backup job or remove specific child backups — backups related to individual computers in the backup.

To remove a Veeam Agent backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
   - To remove the entire backup related to the Veeam Agent backup job or policy, select the backup and click **Remove from** > **Configuration** on the ribbon or right-click the backup and select **Remove from configuration**.
   - To remove a backup of a specific computer in the Veeam Agent backup job or policy, expand the parent backup, select the necessary computer and click **Remove from** > **Configuration** on the ribbon or right-click the computer and select **Remove from configuration**.



Deleting Backup from Disk

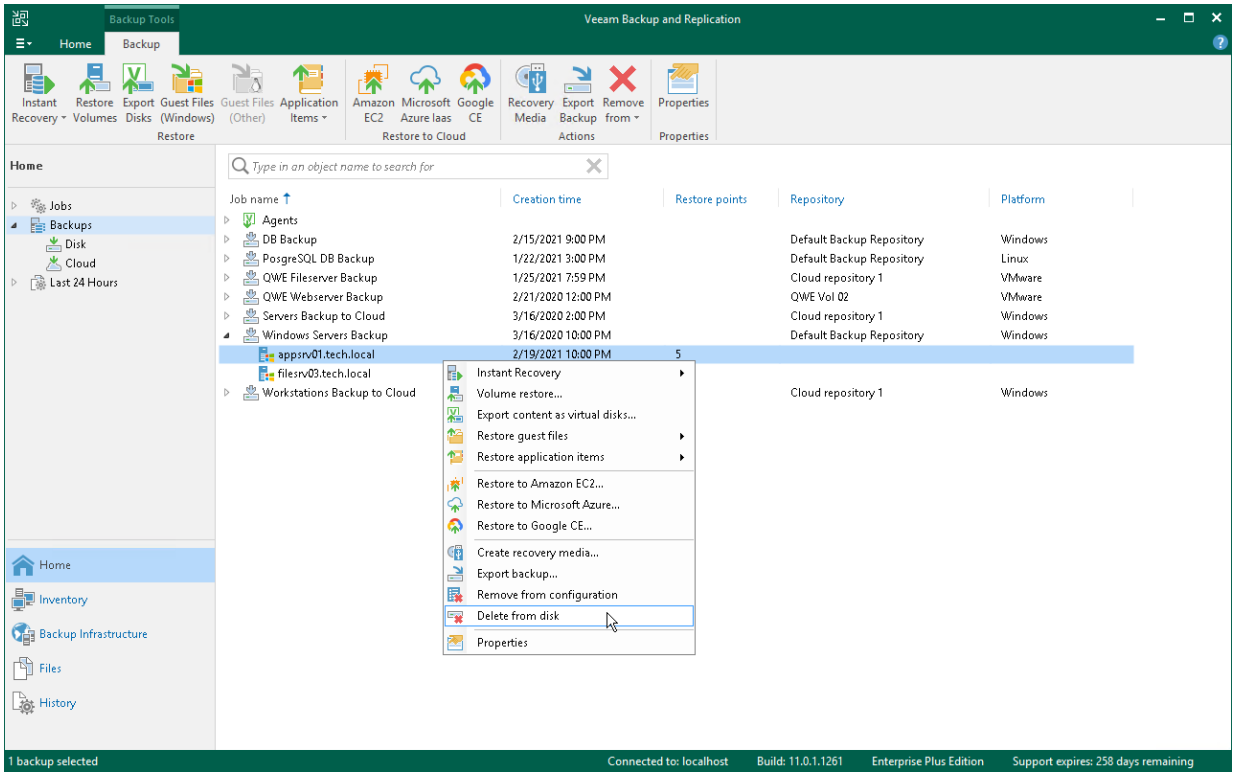
If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation.

> **NOTE**
>
> You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam Backup & Replication console.

You can remove an entire backup related to a Veeam Agent backup job or remove specific child backups — backups related to individual computers in the backup.

To remove a Veeam Agent backup from the backup repository:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
   - To remove the entire backup related to the Veeam Agent backup job or policy, select the backup and click **Remove from** > **Disk** on the ribbon or right-click the backup and select **Delete from disk**.
   - To remove a backup of a specific computer in the Veeam Agent backup job or policy, expand the parent backup, select the necessary computer and click **Remove from** > **Disk** on the ribbon or right-click the computer and select **Delete from disk**.



Viewing Backup Properties

You can view summary information about backups created by Veeam Agent backup jobs on the backup repository. The summary information provides the following data:

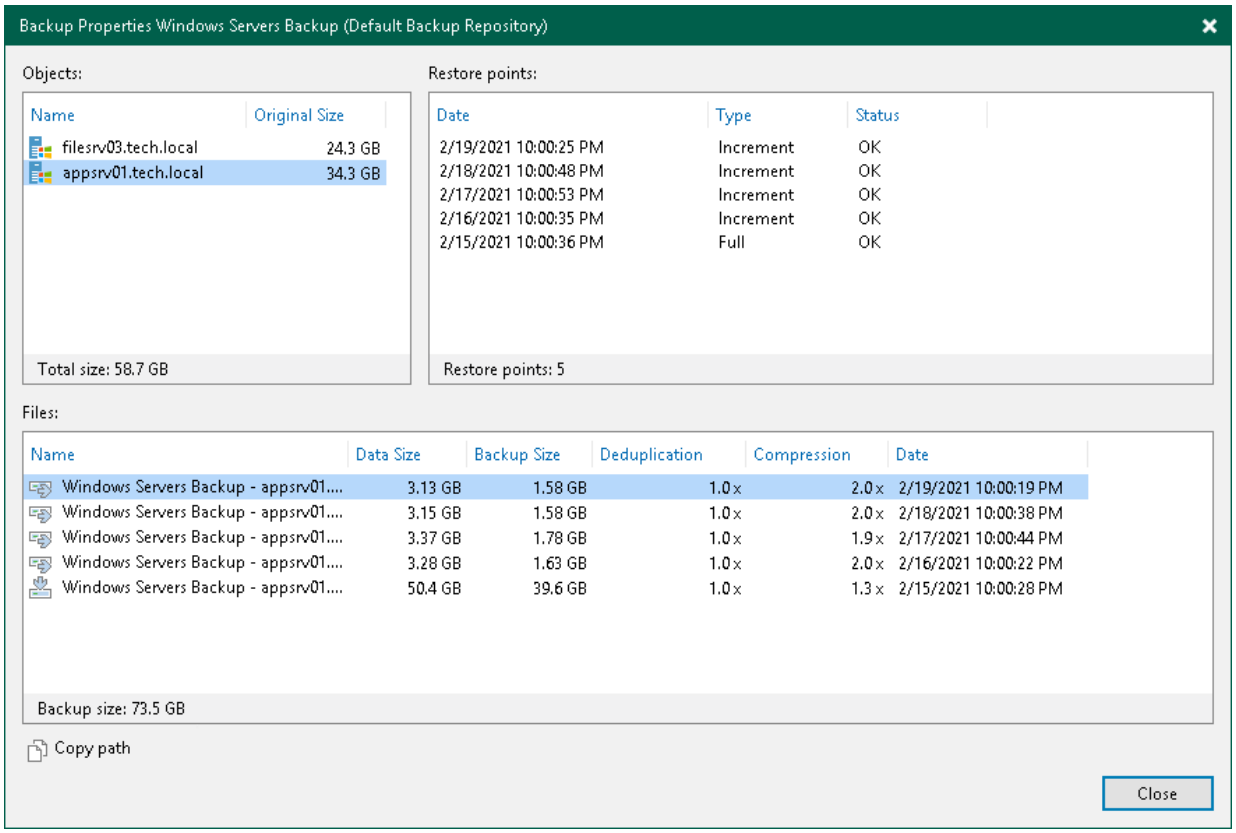
- Backup location
- Available restore points
- Date of restore points creation
- Compression and deduplication ratios
- Data size and backup size

You can view summary information for the following types of Veeam Agent backups:

- Entire backup related to a Veeam Agent backup job (parent backup)
- Backup of a separate protected computer in the Veeam Agent backup job (child backup)

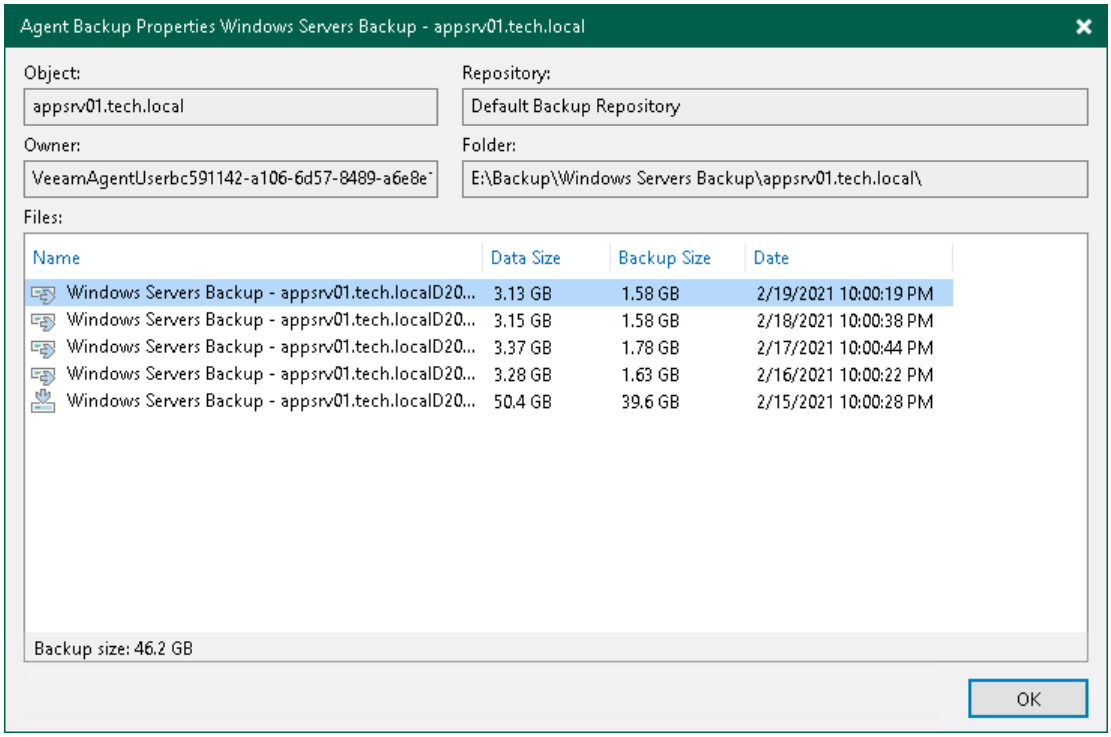
To view summary information for a parent backup:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.



To view summary information for a child backup (backup of a specific Veeam Agent computer):

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, expand the parent backup, select the necessary child backup and click **Properties** on the ribbon or right-click the child backup and select **Properties**.



Reporting

You can view real-time statistics for rescan jobs, as well as Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication. You can also generate reports with statistics data for performed rescan job or backup job sessions. You can generate reports manually in the Veeam Backup & Replication console or set up Veeam Backup & Replication to send reports automatically by email.

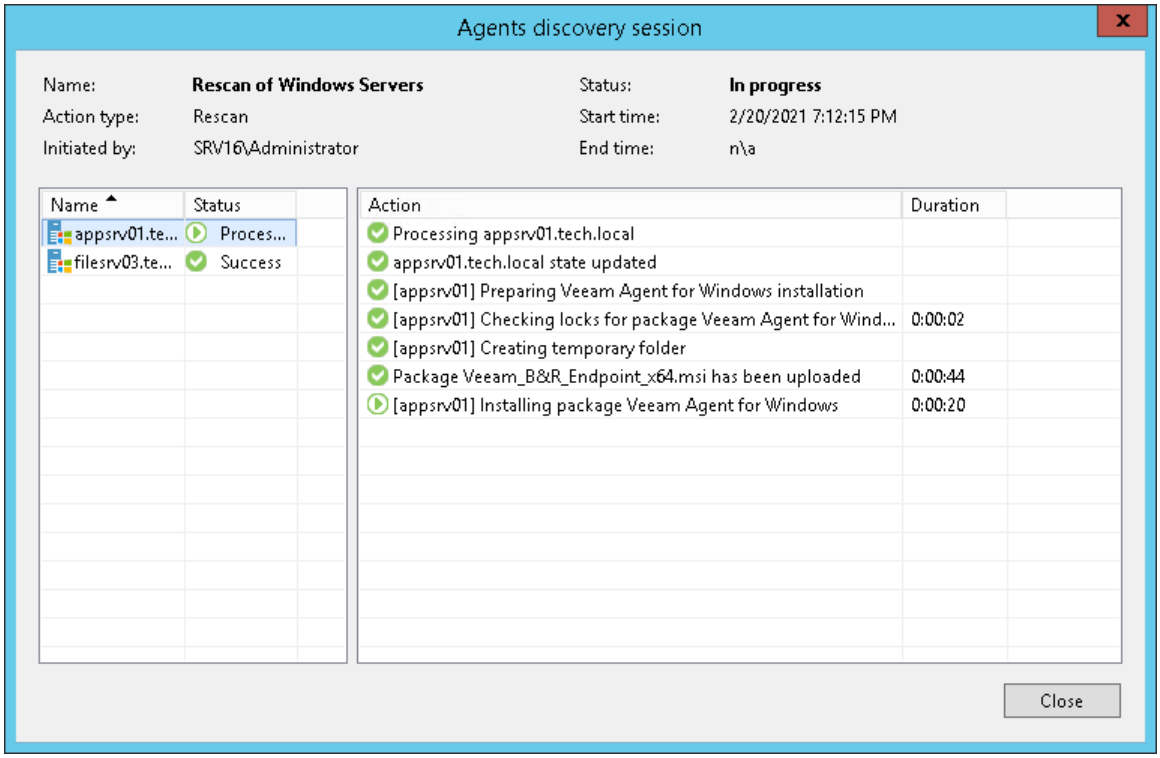
Viewing Rescan Job Statistics

You can view statistics about performed rescan job sessions. When you create a protection group or manually start the discovery process for a protection group or individual protected computer, Veeam Backup & Replication displays statistics for the currently running rescan job session. In the statistics window, Veeam Backup & Replication displays session duration details and a list of operations performed during the job.

In addition to overall rescan job statistics, the statistics window provides information on each protected computer processed within the rescan job session. To view the processing progress for a specific computer, select it in the list on the left.

You can also view statistics for any performed rescan job session. To view rescan job statistics, do one of the following:

- Open the **Inventory** view. In the inventory pane, select the necessary protection group and click **Statistics** on the ribbon or right-click the protection group and select **Statistics**.
- Open the **History** view. In the inventory pane, select the **System** node. In the working area, select the necessary rescan job session and click **Statistics** on the ribbon or right-click the rescan job session and select **Statistics**.



Viewing Rescan Job Report

You can generate reports with details about rescan job sessions performed for a specific protection group. The report contains data on the latest rescan job session initiated for the job upon schedule. To generate a report:

1. Open the **Inventory** view.
2. In the inventory pane, select the necessary protection group and click **Report** on the ribbon or right-click the protection group and select **Report**.

The report contains the following data:

- Cumulative session statistics: details of the session performance, including the number of protected computers in the protection group and the number of newly discovered computers.
- Detailed statistics for every protected computer processed within the session: DNS name, IP address and operating system of the protected computer, list of warnings and errors (if any).

> **TIP**
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.

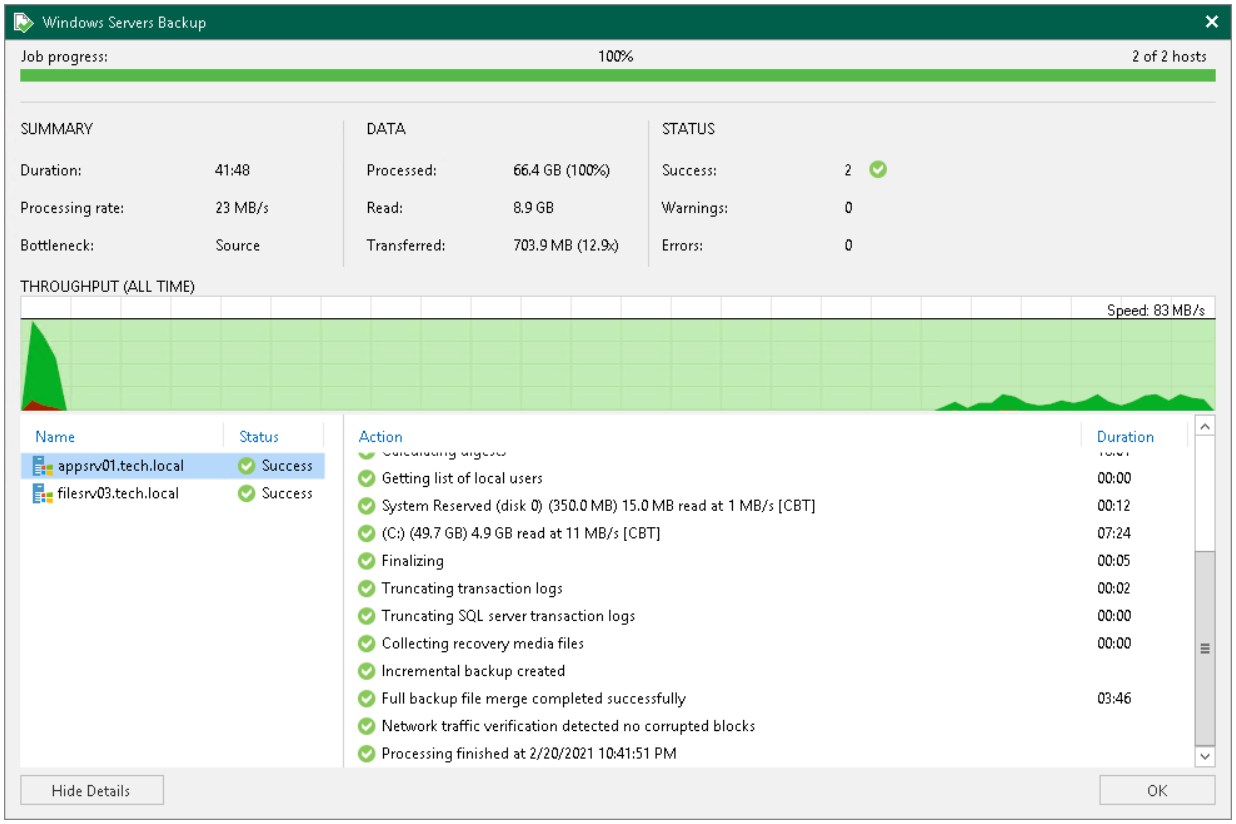
Windows Servers				Success
Assigned	2	**Success**	2	
Seen	2	**Warnings**	0	
Updated	2	**Errors**	0	
Name	**IP address**	**Status**	**Operating System**	**Details**
appsrv01.tech.local	172.24.30.120	Success	Microsoft Windows Server 2012 R2 (64-bit)	Backup agent has been installed.
filesrv03.tech.local	172.24.30.121	Success	Microsoft Windows Server 2012 R2 (64-bit)	Backup agent has been installed.

Viewing Veeam Agent Backup Job Statistics

You can view statistics about Veeam Agent backup jobs configured in Veeam Backup & Replication. For Veeam Agent backup jobs managed by the backup server, Veeam Backup & Replication displays statistics in the similar way as for backup jobs for VM data backup. To learn more, see the Reporting section in the Veeam Backup & Replication User Guide.

To view Veeam Agent backup job statistics:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, double-click the necessary Veeam Agent backup job. Alternatively, you can select the necessary Veeam Agent backup job and click **Statistics** on the ribbon or right-click the job and select **Statistics**.



Viewing Veeam Agent Backup Job Report

You can generate a report with details about Veeam Agent backup job session performance. The report contains data on the latest backup job session initiated for the job. To generate a report:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary job and click **Report** on the ribbon or right-click the job and select **Report**.

The report contains data on the latest job session:

- Cumulative 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 every protected computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

> **TIP**
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.

Agent Backup job: Windows Servers Backup — **Success** — 2 of 2 hosts processed

Saturday, February 20, 2021 10:00:08 PM

Success	2	**Start time**	10:00:08 PM	**Total size**	90.2 GB	**Backup size**	703.9 MB	
Warning	0	**End time**	10:41:57 PM	**Data read**	8.9 GB	**Dedupe**	1.0x	
Error	0	**Duration**	0:41:48	**Transferred**	703.9 MB	**Compression**	2.7x	

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
filesrv03.tech.local	Success	10:00:28 PM	10:11:51 PM	40.2 GB	4 GB	420.2 MB	0:11:23	
appsrv01.tech.local	Success	10:00:33 PM	10:41:51 PM	50 GB	4.9 GB	283.7 MB	0:41:18	

Viewing Backup Policy Statistics

You can view statistics about Veeam Agent backup jobs configured in Veeam Backup & Replication. For Veeam Agent backup jobs managed by Veeam Agent, or backup policies, Veeam Backup & Replication displays statistics in the following way:

- After you create a backup policy, Veeam Backup & Replication applies the backup policy to protected computers. In the policy statistics window, Veeam Backup & Replication displays information about policy application process and results. This information remains in the policy statistics window until the first Veeam Agent backup job session is performed on computers included in the backup policy.
- After the Veeam Agent backup job session statistics becomes available in Veeam Backup & Replication, this statistics appears in the policy statistics window. The job session statistics becomes available in Veeam Backup & Replication at a different time depending on what target for backup files is selected in the backup policy settings:
    - If a Veeam Agent backup job whose settings are defined by the backup policy creates backup files on a Veeam backup repository, backup job session statistics is available in Veeam Backup & Replication on real-time basis.
    - If a Veeam Agent backup job creates backup files on a local drive of a Veeam Agent computer, in a network shared folder or in a Veeam Cloud Connect repository, backup job session results are not passed to Veeam Backup & Replication in real time. Statistics for such backup sessions becomes available in Veeam Backup & Replication later, after rescan of a protection group that contains computers added to the backup policy. This process happens regularly upon the discovery schedule defined in the protection group settings.
- Veeam Backup & Replication regularly applies the backup policy to protected computers. This operation is performed during automatic rescan of a protection group that contains computers added to the backup policy. If the application process completes with a warning or an error, Veeam Backup & Replication displays information about the application process results in the policy statistics window. Information about successful application of the backup policy is not displayed in the statistics window between two backup sessions.

Veeam Backup & Replication displays statistics for backup policies in a different way than for Veeam Agent backup jobs managed by the backup server. The main differences are the following:

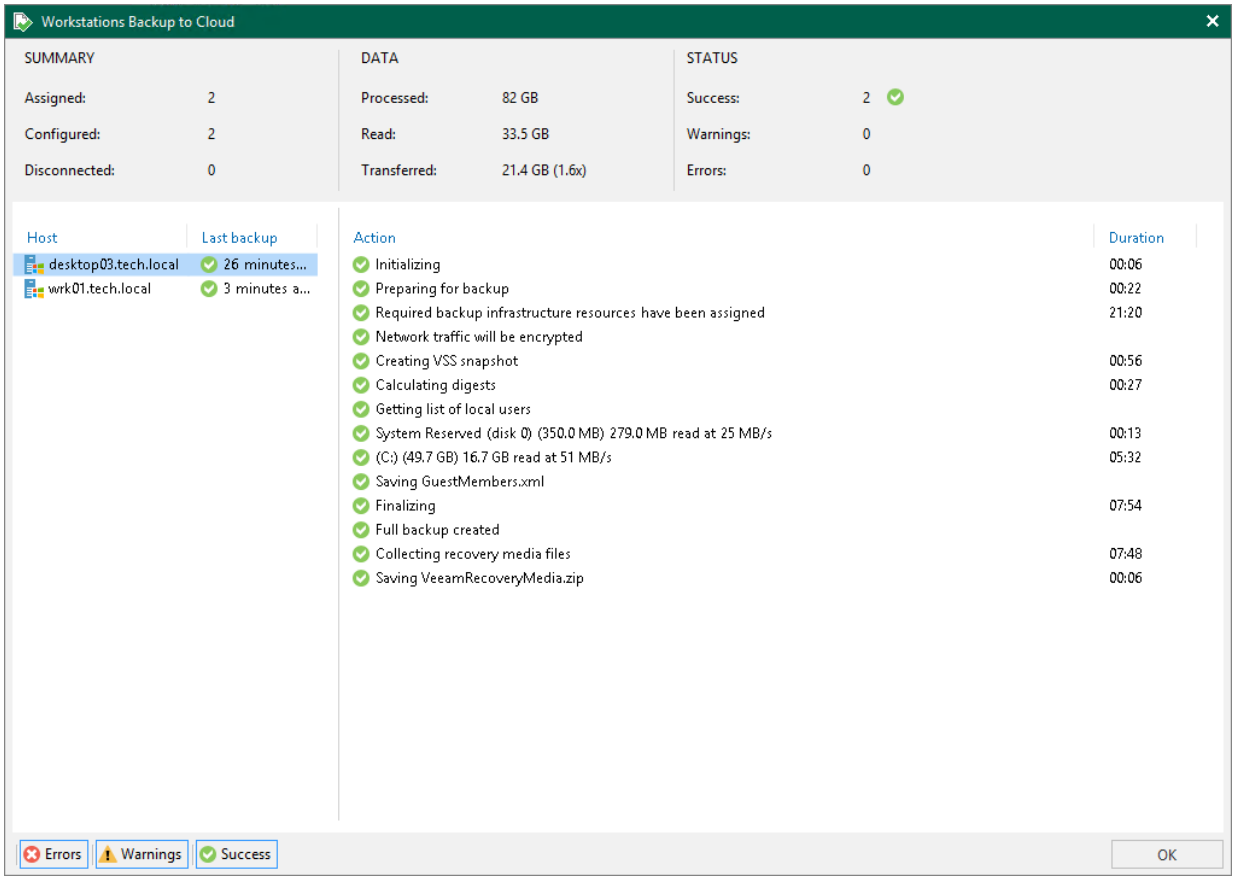
- For backup policies, Veeam Backup & Replication does not display the job progress bar. You can monitor backup progress only for individual computers in the backup policy.
- Detailed statistics include the number of Veeam Agent computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of computes that have no connection to the backup server at the time when the Veeam Agent backup job is performed.
- You can use the **Errors**, **Warnings** and/or **Success** buttons at the bottom of the job statistics window to view details on operations that failed, completed with a warning or completed successfully during a Veeam Agent job session performance.

> **TIP**
>
> In addition to backup policy statistics, Veeam Backup & Replication displays individual backup session statistics for each computer in the backup policy. You can view these statistics in the **Last 24 Hours** node of the **Home** view and in the **History** view of the Veeam backup console.

To view Veeam Agent backup policy statistics:

1. Open the **Home** view.

2. In the inventory pane, click the **Jobs** node.
3. In the working area, double-click the necessary Veeam Agent backup policy. Alternatively, you can select the necessary Veeam Agent backup policy and click **Statistics** on the ribbon or right-click the backup policy and select **Statistics**.



Viewing Backup Policy Report

You can generate a report with details about Veeam Agent backup job sessions performed on protected computers added to a backup policy. The report contains data on the latest backup job session initiated for the backup policy. To generate a report:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary backup policy and click **Report** on the ribbon or right-click the backup policy and select **Report**.

The report contains data on the latest job session:

- Cumulative session statistics: details on the number of protected computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of disconnected computes, details of the session performance, amount of read, processed and transferred data.
- Detailed statistics for every protected computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

> **TIP**
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.

Workstations Backup to Cloud — **Success** — 2 of 2 hosts processed

Assigned	2	**Processed**	82 GB	**Success**	2
Configured	2	**Read**	5.5 GB	**Warnings**	0
Disconnected	0	**Transferred**	2 GB	**Errors**	0

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
desktop03.tech.local	Success	10/15/2020 11:00:00 PM	10/15/2020 11:05:23 PM	50 GB	3.5 GB	1.2 GB	00:05:23	
wrk01.tech.local	Success	10/15/2020 11:00:00 PM	10/15/2020 11:09:21 PM	32 GB	2 GB	754 MB	00:09:21	

Enabling Email Reporting

You can set up Veeam Backup & Replication to send reports automatically by email. To do this, you must enable and configure global email notification settings in Veeam Backup & Replication. To learn more, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

In addition, you can enable and configure custom notification settings for a specific protection group, Veeam Agent backup job or backup policy. This may be useful if you want to change subject, notification rules or list of recipients for some reports.

Rescan Job Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends rescan job reports at 10:00 PM daily. Veeam Backup & Replication sends a separate report for every protection group that you configured. The report contains cumulative statistics for rescan job sessions performed within the last 24-hour period.

You can specify custom notification settings for a specific protection group. To learn more, see Notification Settings.

Veeam Agent Backup Job Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends an email notification after every backup job session completes.

You can specify custom notification settings for a specific Veeam Agent backup job. To learn more, see the following sections:

- Notification Settings for Veeam Agent Backup Job (for Microsoft Windows computers)
- Notification Settings for Veeam Agent Backup Job (for Linux computers)

Backup Policy Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends backup policy reports at 10:00 AM daily. Veeam Backup & Replication sends a separate report for every backup policy that you configured. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

You can specify custom notification settings for a specific backup policy. To learn more, see the following sections:

- Notification Settings for Backup Policy (for Microsoft Windows computers)
- Notification Settings for Backup Policy (for Linux computers)
- Notification Settings for Backup Policy (for Unix computers)
- Notification Settings for Backup Policy (for macOS computers)

Appendix A. Deploying Hotfix on Protected Computers

This scenario describes how to deploy a hotfix on protected computers with installed Veeam Agent for Microsoft Windows or Veeam Agent for Linux:

- A Veeam Agent for Microsoft Windows hotfix is an updated Veeam Agent setup archive that addresses a certain issue in the product.
- A Veeam Agent for Linux hotfix is a set of updated Veeam Agent packages that addresses a certain issue in the product.

Veeam Software issues a hotfix in one of the following cases:

- To mitigate an existing issue in the product. In this case, a hotfix is provided by Veeam Customer Support.
- [For Veeam Agent for Linux hotfix] To add support of a new Linux distribution version to the product. In this case, a hotfix is available in the Veeam software repository.

If you have several Microsoft Windows and Linux computers with Veeam Agent installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed agents. Keep in mind that this scenario is not available for Veeam Agent computers add

Prerequisites

Before you deploy a Veeam Agent hotfix on protected computers:

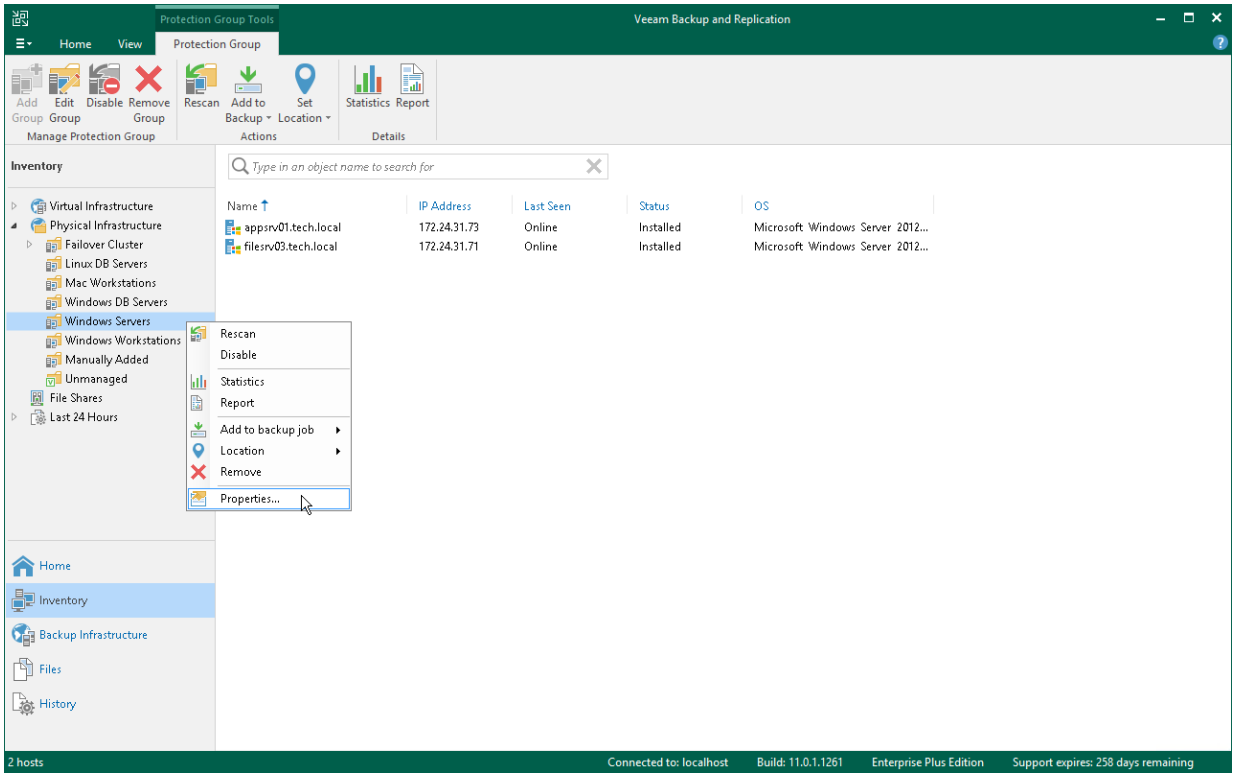
1. Check that protected computers are powered on and can be connected over the network.
2. Check that there are no running jobs.

   We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If protected computers run VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived logs) is enabled in the backup job for these computers, disable this backup job too.
3. Check that automatic Veeam Agent deployment options are enabled in the protection group settings:

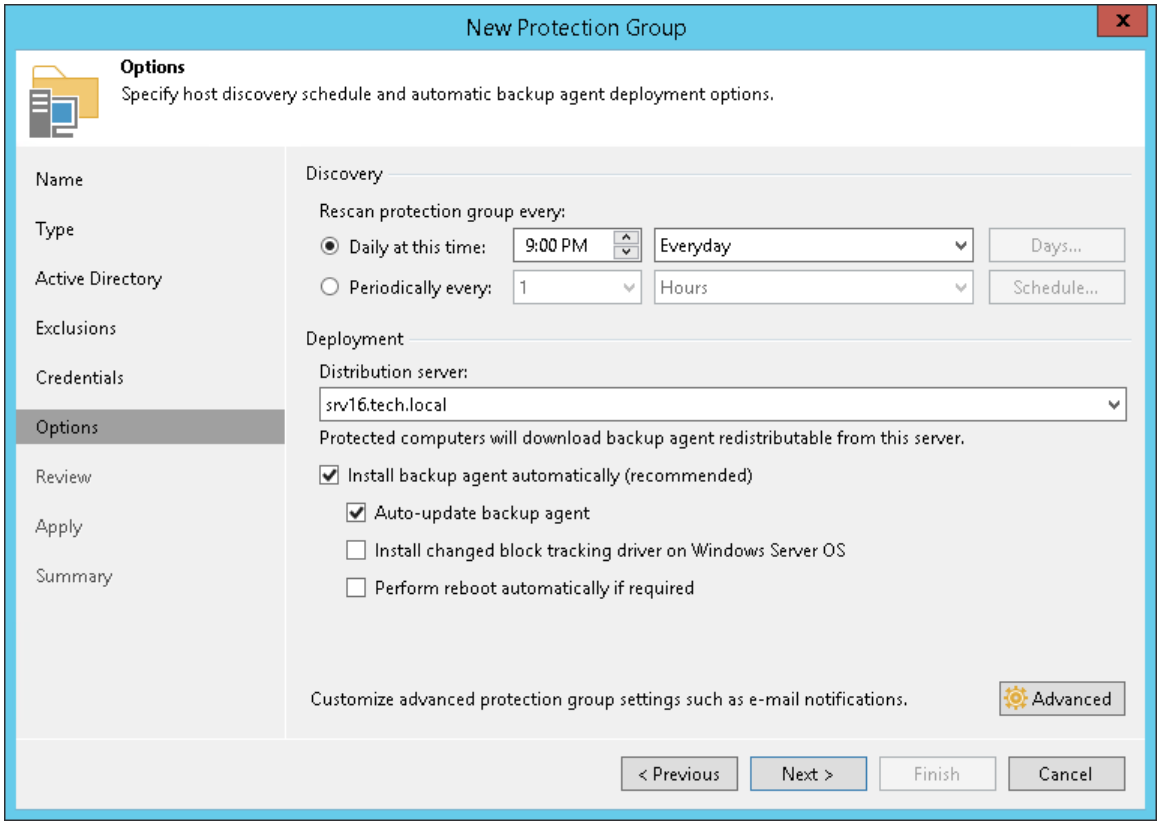
   a. Open the **Inventory** view.

   b. In the inventory pane, expand the **Physical Infrastructure** node.

   c. In the inventory pane, select the protection group that contains computers with an outdated Veeam Agent installed and click **Edit Group** on the ribbon or right-click the protection group that you want to edit and select **Properties**.



d. At the **Options** step of the wizard, in the **Deployment** section, make sure that the **Install backup agent automatically** and **Auto-update backup agent** check boxes are selected.



4. Determine a location for the hotfix distribution:

   a. If you plan to deploy a Veeam Agent for Microsoft Windows hotfix, you will need to place the hotfix to a folder on the backup server.

   b. If you plan to deploy a Veeam Agent for Linux hotfix, you will need to place the hotfix to a folder on the distribution server specified for the protection group.

      Each protection group can have a different distribution server, so you need to place the hotfix on the distribution server of each protection group that contains Veeam Agent computers on which you need to deploy a hotfix.

Deployment Procedure for Protected Computers

The hotfix deployment procedure differs depending on the OS running on the protected computers:

- Deployment procedure for Microsoft Windows computers
- Deployment procedure for Linux computers

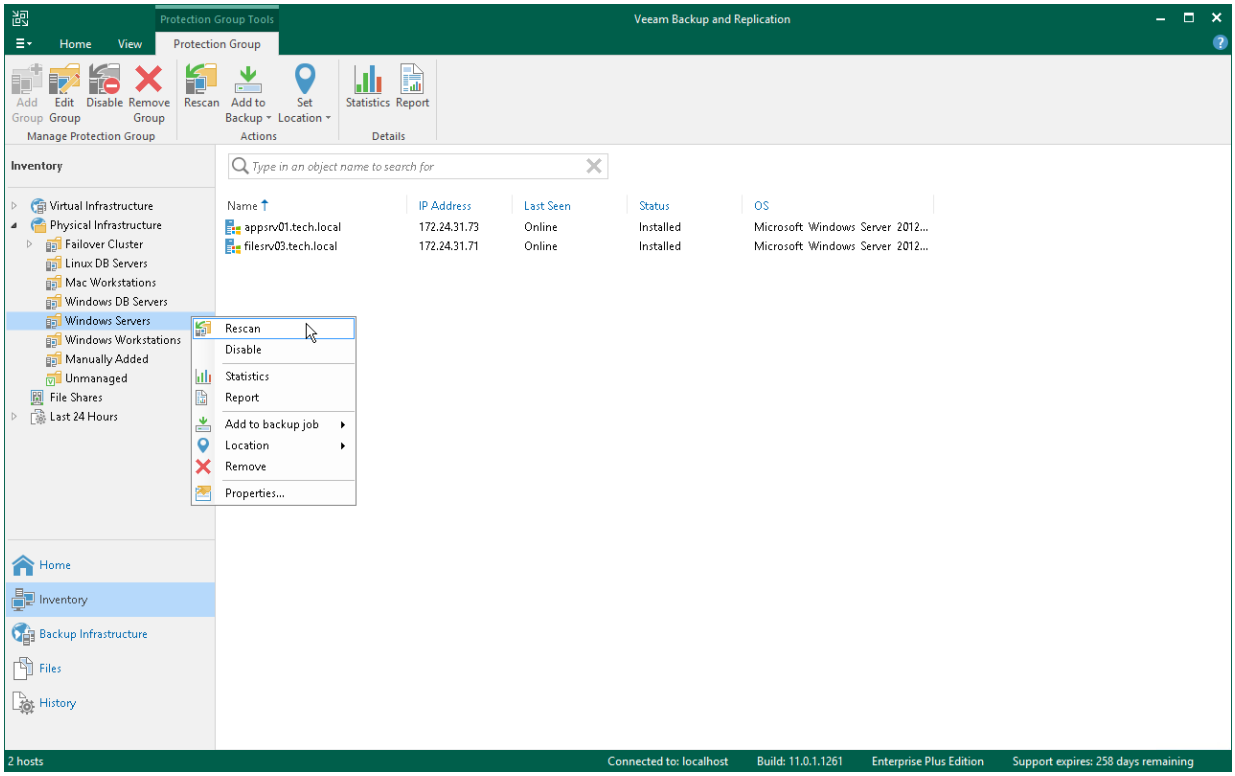
Deployment Procedure for Windows Computers

To deploy a hotfix on Microsoft Windows computers included in the protection group, perform the following steps:

1. Obtain a hotfix from Veeam Customer Support or download it from the Veeam software repository.
2. Save the Veeam Agent for Microsoft Windows setup archive to the following folder on the backup server:

   ```
   C:\Program Files\Veeam\Veeam Distribution Service\Fixes\vaw
   ```

3. Rescan the protection group:
   a. Open the **Inventory** view.
   b. In the inventory pane, expand the **Physical Infrastructure** node.
   c. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.



Deployment Procedure for Linux Computers

To deploy a hotfix on Linux computers included in the protection group, perform the following steps:

1. Obtain a hotfix from Veeam Customer Support or download it from the Veeam software repository.
2. Save Veeam Agent for Linux packages to the following folder on the distribution server specified in the protection group settings:

   For 32-bit CentOS / RHEL / Oracle Linux / Fedora / openSUSE / SLES

   ```
   C:\ProgramData\Veeam\Agents\val\x86\rpm
   ```

   For 64-bit CentOS / RHEL / Oracle Linux / Fedora / openSUSE / SLES

   ```
   C:\ProgramData\Veeam\Agents\val\x64\rpm
   ```

   For 32-bit Debian / Ubuntu

   ```
   C:\ProgramData\Veeam\Agents\val\x86\deb
   ```

   For 64-bit Debian / Ubuntu

   ```
   C:\ProgramData\Veeam\Agents\val\x64\deb
   ```

3. Replace names of Veeam Agent for Linux package in the index file.

   a. Open the `ValPackageIndex.xml` file that is located in the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val
   ```

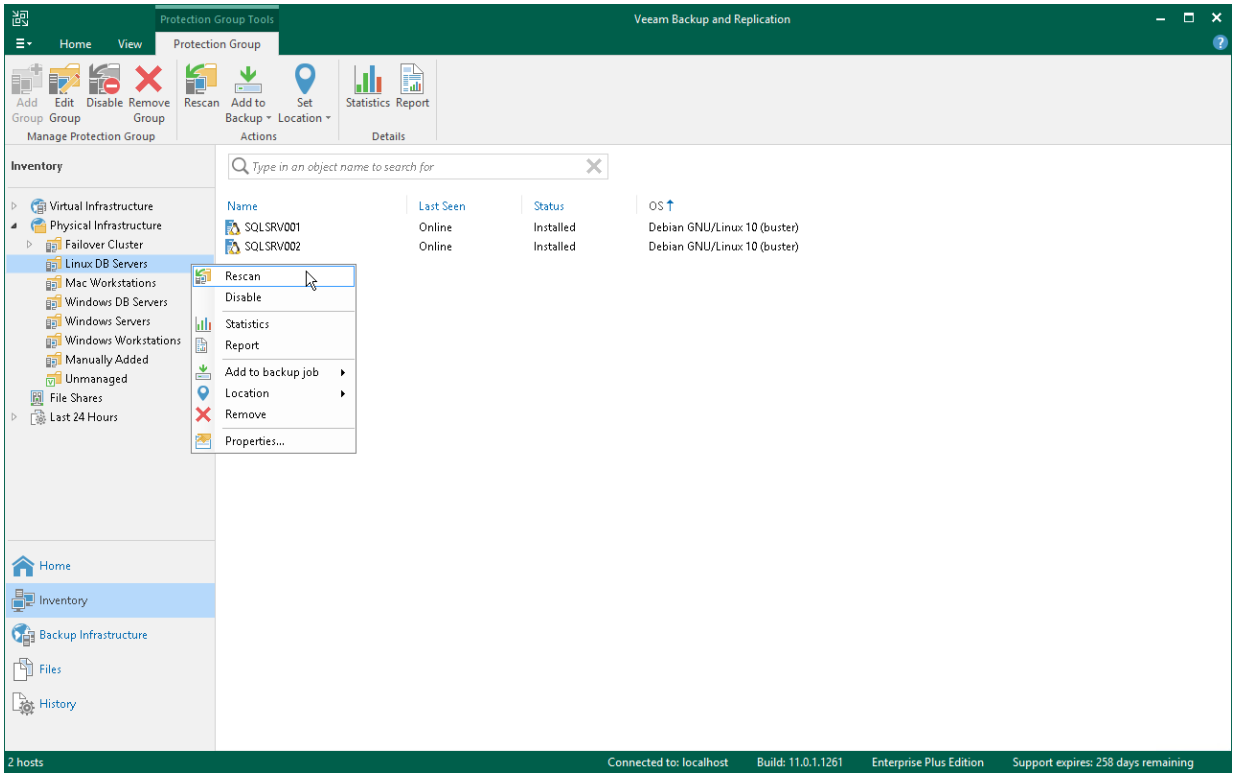
   b. In the `ValPackageIndex.xml` file, locate packages that you want to update. Replace their names with names of Veeam Agent for Linux packages you saved in step 2. After that, save changes and close the index file. For more detailed explanation, see Example.

4. Rescan the protection group:

    a. Open the **Inventory** view.

    b. In the inventory pane, expand the **Physical Infrastructure** node.

    c. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.



Example

For example, Veeam Software issued a hotfix for Veeam Agent for Linux 5.0.2 for 64-bit RHEL 8 and you want to deploy it on your Veeam Agent computers.

In this scenario, the hotfix consists of the following Veeam Agent packages:

- `veeamsnap-5.0.2.XXXX-1.noarch.rpm`
- `veeam-5.0.2.XXXX-1.el8.x86_64.rpm`
- `kmod-veeamsnap-5.0.2.XXXX-1.el8.x86_64.rpm`

To deploy the hotfix, you need to do the following:

1. Obtain all three updated Veeam Agent for Linux packages from Veeam Customer Support or download them from the Veeam software repository.
2. Save the packages to the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val\x64\rpm
   ```

   You do not need to delete obsolete Veeam Agent for Linux packages you want to update.
3. Edit the index file located in the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val
   ```

   a. Open the `ValPackageIndex.xml` file.

   b. Locate the packages that you want to update and replace their version and names with version and names of the packages you saved is step 2.

   Usually, the packages that are available as a hotfix have a build version that is different from the obsolete packages. In this scenario, obsolete packages have the 5.0.2.4567 build version and the updated packages have the 5.0.2.XXXX build version.

In the example below, replaced package version and names are highlighted in green:

```
...
<Distribution id="RHEL" displayName="Red Hat">
  <Version majorVersions="6">
     <Packages version="5.0.2.4567" arch="x64">
        <driver_noarch value="veeamsnap-5.0.2.4567-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-5.0.2.4567-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-5.0.2.4567-
2.6.32_131.0.15.el6.x86_64.rpm"/>
        <veeam value="veeam-5.0.2.4567-1.el6.x86_64.rpm" />
     </Packages>
     <Packages version="5.0.2.4567" arch="x86">
        <driver_noarch value="veeamsnap-5.0.2.4567-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-5.0.2.4567-
2.6.32_131.0.15.el6.i386.rpm"/>
        <veeam value="veeam-5.0.2.4567-1.el6.i386.rpm"/>
     </Packages>
  </Version>
  <Version majorVersions="7">
     <Packages version="5.0.2.4567" arch="x64">
        <driver_noarch value="veeamsnap-5.0.2.4567-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-5.0.2.4567-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-5.0.2.4567-1.el7.x86_64.rpm"/>
        <veeam value="veeam-5.0.2.4567-1.el7.x86_64.rpm"/>
     </Packages>
  </Version>
  <Version majorVersions="8">
     <Packages version="5.0.2.XXXX" arch="x64">
        <driver_noarch value="veeamsnap-5.0.2.XXXX-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-5.0.2.4567-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-5.0.2.XXXX-1.el8.x86_64.rpm"/>
        <veeam value="veeam-5.0.2.XXXX-1.el8.x86_64.rpm"/>
     </Packages>
  </Version>
</Distribution>
....
```

c. Save changes and close the index file.

4. Rescan the protection group:

   a. Open the **Inventory** view.

   d. In the inventory pane, expand the **Physical Infrastructure** node.

   e. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.

During the rescan, Veeam Backup & Replication will use updated packages specified in the index file to install Veeam Agent for Linux version with the hotfix on protected computers.

Appendix B. Restoring Files from Backup without Administrator Privileges

If you have Veeam Agent for Microsoft Windows installed on your computer and you work on this computer under an account that does not have Administrator privileges, you can still restore files from the file-level backup.

This scenario describes how to restore a file from the backup under an account that does not have local administrator permissions to its original location.

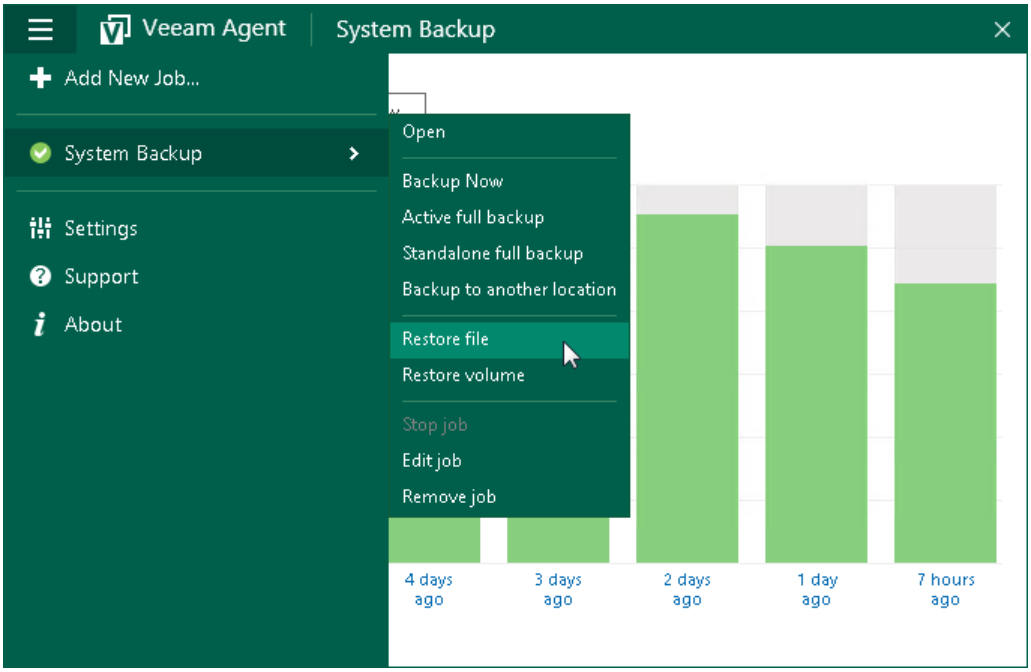
Before restoring, check the following prerequisites:

- Your Veeam Agent computer must be a member of a protection group for which file-level restore without Administrator privileges is allowed. To learn more, see Veeam Agent for Microsoft Windows Settings.
- You must restore from the backup created by a backup job managed by Veeam Agent. To learn more, see Selecting Job Mode.
- You must restore from the backup stored on Veeam backup repository or Veeam Cloud Connect repository.
- You must restore from the backup of the same Veeam Agent computer.
- You must open the restore wizard from the Veeam Agent for Microsoft Windows control panel.

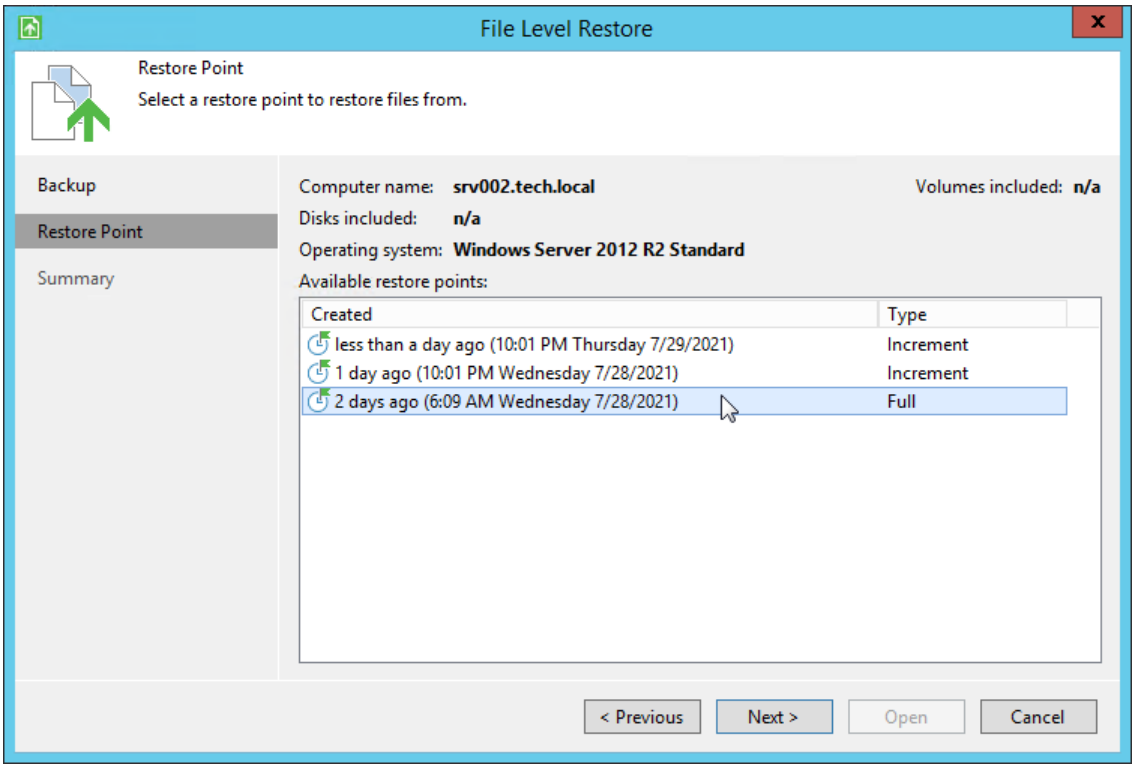
To restore files, perform the following operations.

1. On the Veeam Agent computer, double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the icon in the system tray and select **Control Panel**.
2. From the main menu in the upper left corner, hover over the name of the necessary job and select **Restore file** to open the **File Level Restore** wizard.

   Mind that when you work on the Veeam Agent computer under an account that does not have Administrator privileges, you can open the **File Level Restore** wizard only from the Veeam Agent for Microsoft Windows control panel. If you try to open the wizard from the system tray, Veeam Agent will ask you to enter Administrator credentials.



3. In the **File Level Restore** wizard, select a restore point from which you want to restore the file.

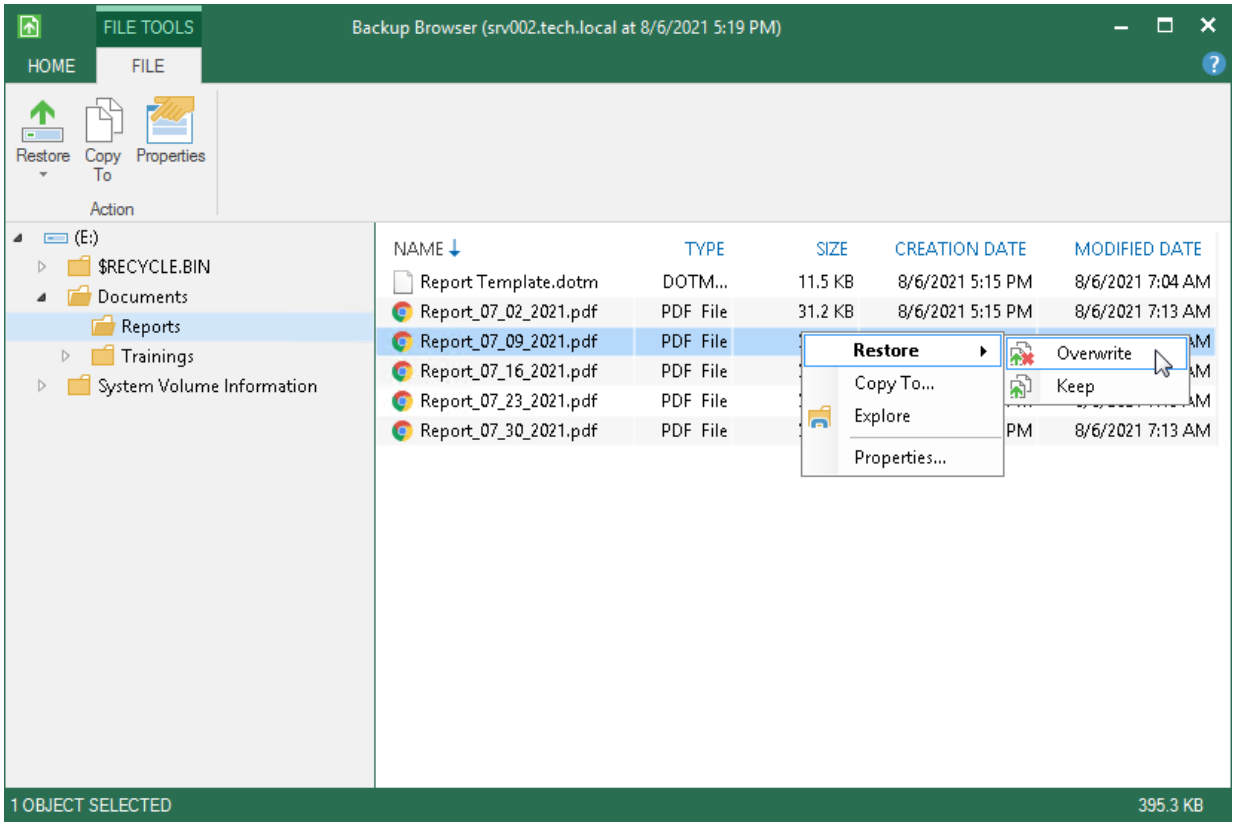


4. At the **Summary** step, click **Open**. Veeam Agent will display the backup file content in the Veeam Backup browser.

5. Locate the file you want to restore, right-click it and select **Restore** > **Overwrite**. The file will be restored to its original location.

   Mind that access rights to files and folders are managed by Veeam Agent computer OS. When you cannot access the folder in the original location, you cannot view the content of this folder in the Veeam Backup browser as well. If you select file to restore, but do not have enough access rights to restore it, Veeam Agent will not restore the file and will display an error message in the restore job session.

   To get the access rights you need, you can switch to another system user with the Veeam Backup browser. To learn more, see the Elevating Access Rights section in the Veeam Agent for Microsoft Windows User Guide.



Appendix C. Updating Pre-Installed Veeam Agents

This scenario describes how to update Veeam Agents on the computers added to protection groups for pre-installed Veeam Agents.

> **TIP**
>
> During each rescan job and synchronization session, Veeam Backup & Replication checks the version of Veeam Agents installed on the protected computers. If the Veeam Agent version does not coincide with the version of Veeam Backup & Replication, Veeam Agent computer will be moved to the *Out of Date* protection group.

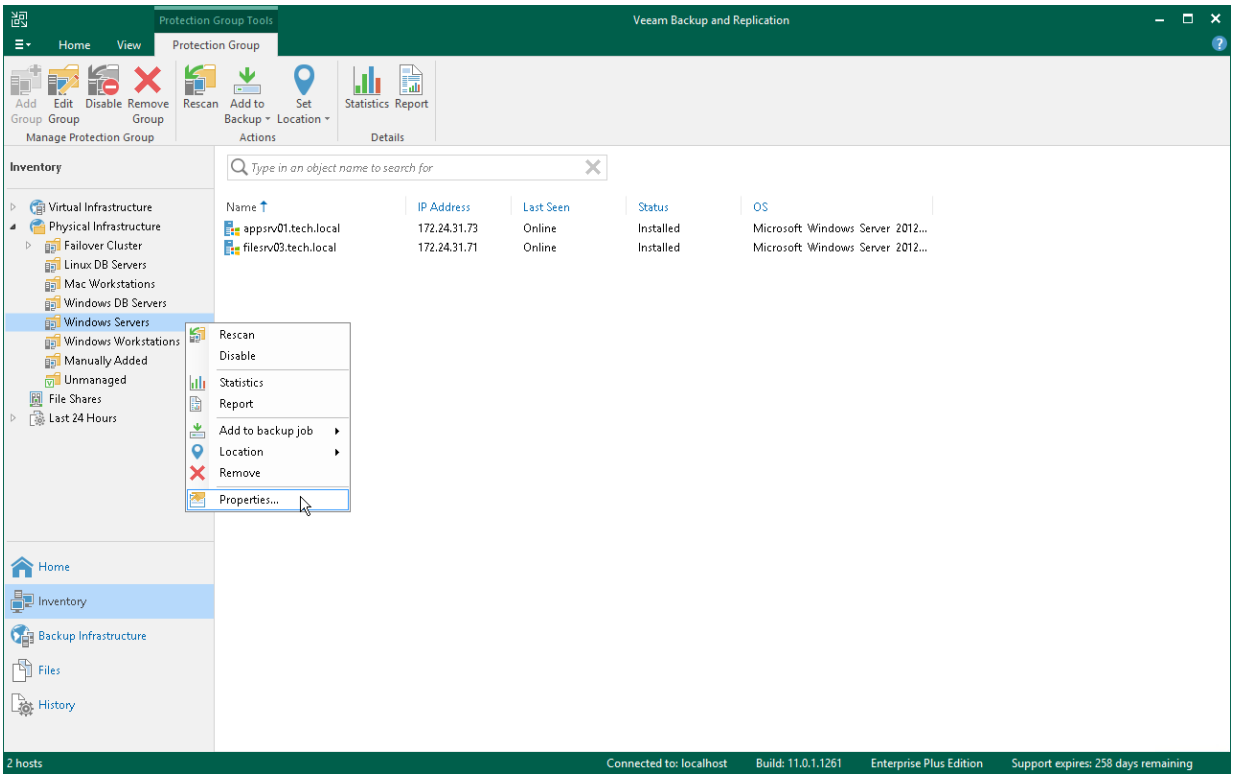
Before you update pre-installed Veeam Agents:

- Check that the latest update for Veeam Backup & Replication is installed on your backup server. For details, see Updating Veeam Backup & Replication 11 or 11a section in the Veeam Backup & Replication Guide.
- Make sure that Veeam Backup & Replication remote components, such as the distribution server, are updated.
- Make sure that a user account that you plan to use for installation on the Veeam Agent computer side has Local Administator privileges.

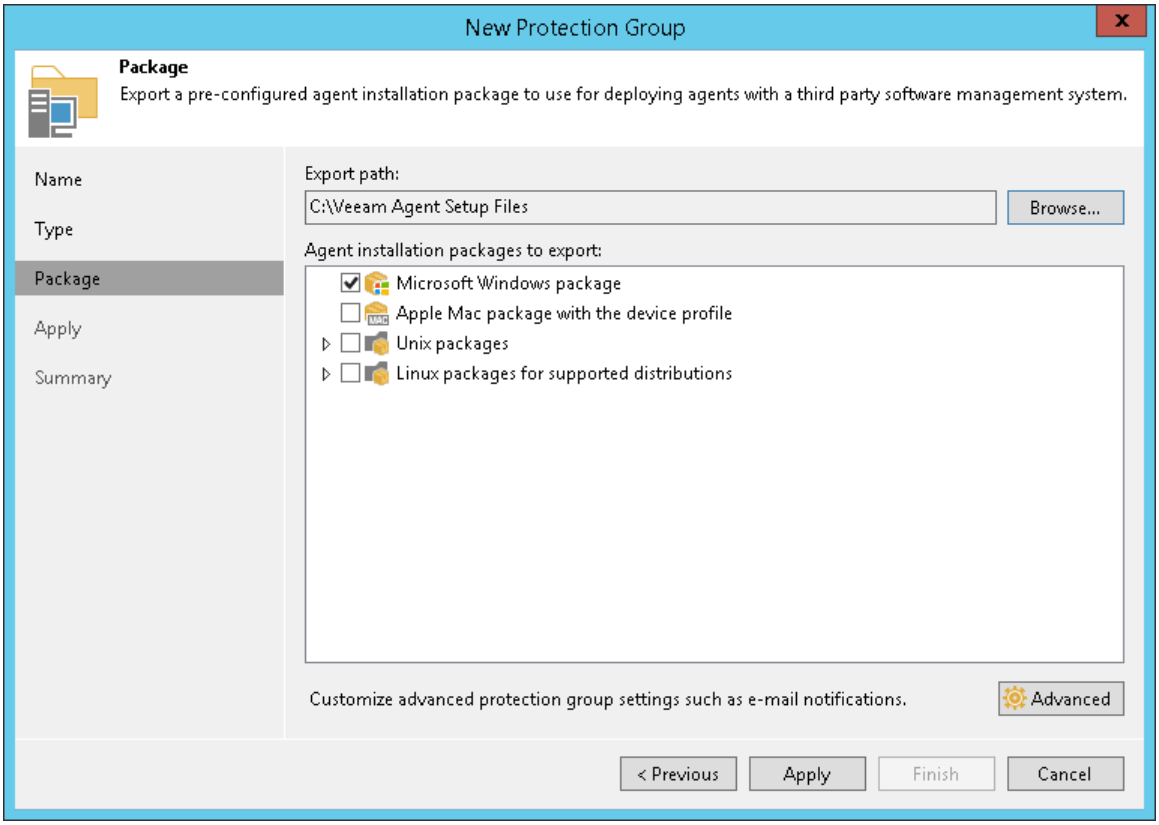
To update pre-installed Veeam Agents, you must generate new Veeam Agent setup files on the Veeam Backup & Replication side, To do so, edit protection group settings:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.

3. In the inventory pane, select the protection group for pre-installed Veeam Agents that you want to update and click **Edit Group** on the ribbon or right-click the protection group for pre-installed Veeam Agents that you want to update and select **Properties**.



4. At the **Package** step, check that the export path and setup files for OSes that runs on computers with Veeam Agents you want to update are specified correctly.



5. Click **Apply** to generate setup files. Then click **Finish** to close the wizard.

On the Veeam Agent computer side, the update procedure differs depending on the OS running on the protected computers:

- Update procedure for Microsoft Windows computers
- Update procedure for Linux computers
- Update procedure for Mac computers

Update Procedure for Windows Computers

To update pre-installed Veeam Agent on the Microsoft Windows computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Update the Veeam Installer Service. To do this:
   a. Uninstall obsolete version of the Veeam Installer Service. To do this, navigate to Control Panel > Programs > Programs and Features, find the Veeam Installer Service in the list of programs and uninstall it.
   b. Install the updated version of the Veeam Installer Service. Double-click the `VeeamInstallerSvc` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder.
3. Install updated version of Veeam Agent. Use one of the following files depending on the architecture of your computer OS:

   For 32-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x86.msi` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder

   For 64-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/5.0.2.4680/VAW` folder
4. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -syncnow
```

Update Procedure for Linux Computers

To update pre-installed Veeam Agent on the Linux computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the installation of the Veeam Agent for Linux in the offline mode. For details, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.

   Keep in mind that if you use the APT package manager and the installation command reports that some dependencies for package not installed, run the following command instead:

   ```
   apt-get install -f
   ```

   After that, repeat the Veeam Agent installation procedure.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Update Procedure for Mac Computers

To update pre-installed Veeam Agent on the Linux computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Mac. For details, see the Installing Veeam Agent section in the Veeam Agent for Mac User Guide.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Veeam Backup Enterprise Manager

Version 11

User Guide

October, 2021

© 2021 Veeam Software.

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

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

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE 8
ABOUT THIS DOCUMENT 9
ABOUT VEEAM BACKUP ENTERPRISE MANAGER 10
What's New in Version 11 11
What's New in Version 11a 13
How Veeam Backup Enterprise Manager Works 14
Enterprise Manager Components 15
Veeam Backup Catalog 17
Veeam Backup Search Capabilities 18
File-Level Restore Capabilities 20
How Indexing Works 21
Indexing Data 22
Indexing Data Retention 27
SAML Authentication Support 29
PLANNING AND PREPARATION 31
System Requirements 32
Required Permissions 35
Used Ports 37
LICENSING 43
Installing License 44
Viewing License Details 45
Updating License 47
Revoking License 49
Managing Monthly Usage Reports 50
Reviewing Monthly Usage Report 51
Adjusting Monthly Usage Report 52
Downloading Monthly Usage Report 53
Submitting Monthly Usage Report 54
DEPLOYMENT 56
Installing Veeam Backup Enterprise Manager 57
Before You Begin 58
Step 1. Start Setup Wizard 59
Step 2. Read and Accept License Agreement 60
Step 3. Provide License File 61
Step 4. Review Components and Select Installation Folder 62
Step 5. Install Missing Software 63

Step 6. Specify Installation Settings 64
Step 7. Specify Service Account Settings 66
Step 8. Select Microsoft SQL Server 67
Step 9. Specify Service Ports 68
Step 10. Specify File Locations 69
Step 11. Begin Installation 70
Maintaining Veeam Backup Enterprise Manager 71
Upgrading Veeam Backup Enterprise Manager 72
Uninstalling Veeam Backup Enterprise Manager 74
Migrating Veeam Backup Enterprise Manager 75
GETTING TO KNOW VEEAM BACKUP ENTERPRISE MANAGER 76
Accessing Enterprise Manager Website 77
Veeam Backup Enterprise Manager UI 79
Viewing Operation Statistics 82
CONFIGURING VEEAM BACKUP ENTERPRISE MANAGER 85
Initial Configuration 86
Managing Backup Servers 87
Collecting Data from Backup Servers 89
Reports on Backup Servers 91
Audit Reports 93
Viewing vCenter Servers 95
Configuring Retention Settings for Index and History 96
Configuring Security Settings 99
Configuring Accounts and Roles 100
Configuring Backup Server Roles 108
Configuring SAML Authentication Settings 109
Updating Security Certificate 113
Configuring Notification Settings 114
Email Server Settings 115
Notifications on Job Results 116
Notifications on Lab Requests 118
Notifications on Restore Operations 119
Notifications on Licensing 120
Notifications on Key Management 122
Viewing Information About Enterprise Manager 123
Managing Languages 124
Language Files Overview 125
Adding Languages 126
MANAGING JOBS 130

Viewing Jobs 131
Starting, Stopping and Retrying Jobs 132
Enabling and Disabling Jobs 133
Editing Jobs 134
Step 1. Launch Wizard 135
Step 2. Edit Job Name and Retention Settings 136
Step 3. Edit List of VMs 137
Step 4. Change VM Processing Order 139
Step 5. Configure Guest Processing Settings 140
Step 6. Edit Job Schedule 150
Creating Active Full Backups 153
Cloning Jobs 154
Deleting Jobs 155
MANAGING CDP POLICIES 156
Viewing Policies 157
Enabling and Disabling Policies 158
Editing Policies 159
Step 1. Launch Edit Policy Wizard 160
Step 2. Edit Policy Name and Description 161
Step 3. Edit List of VMs 162
Step 4. Edit Policy Schedule 165
Step 5. Configure Guest Processing Settings 167
Deleting Policies 174
SUPPORT FOR VEEAM AGENTS 175
Guest File Browsing and 1-Click Restore 176
Preparing for File Browsing and Restore 177
Browsing and Restore Procedures 179
Application Item Restore 180
WORKING WITH FILE SHARES 181
Viewing File Share Backups 182
Browsing File Share Backups 184
Performing File Restore 186
Restoring Files to Original Location 187
Downloading Files 189
Restoring Multiple Files 192
Deleting File Share Backups 194
WORKING WITH MACHINES 195
Viewing, Searching, Deleting Machines 196
Performing Quick Backup 198

Performing 1-Click Restore 199
Performing Failover 201
Performing Virtual Disk Restore 205
Running Failover Plans 209
RESTORING GUEST OS FILES 211
Preparing for File Browsing and Searching 212
Performing Catalog Replication and Indexing 213
Preparing for File Search and Restore (non-Windows machines) 214
Browsing Machine Backups for Guest OS Files 216
Searching Guest OS Files in Machine Backups 218
Performing 1-Click File Restore 220
Restoring Files to Original Location 221
Downloading Files to Local Machine 223
Restoring Multiple Files 225
Using Self-Service File Restore Portal to Restore Machine Guest Files 227
BACKUP AND RESTORE OF APPLICATION ITEMS 230
Backup and Restore of Microsoft Exchange Items 231
Preparing Application-Consistent Backup 232
Providing Access Rights 234
Restore Procedure 236
Backup and Restore of Microsoft SQL Server Databases 238
Preparing Application-Consistent Backup 239
Providing Access Rights 242
Restore Procedure 243
Backup and Restore of Oracle Databases 249
Preparing Application-Consistent Backup 250
Providing Access Rights 253
Restore Procedure 254
MANAGING ENCRYPTION KEYS 260
Generating Enterprise Manager Keyset 261
Activating Enterprise Manager Keyset 262
Specifying Retention Settings for Enterprise Manager Keyset 263
Exporting and Importing Enterprise Manager Keyset 264
Deleting Enterprise Manager Keyset 266
Handling Password Recovery Requests 267
WORKING WITH VIRTUAL LAB REQUESTS 269
Creating Virtual Lab Requests 270
Approving Virtual Lab Requests 273
WORKING WITH VMWARE VCLOUD DIRECTOR 274

Managing Configurations for vCD Organizations 276
Before You Begin 277
Viewing Organization Configurations 279
Adding Organization Configuration 280
Editing Organization Configuration 283
Removing Organization Configuration 284
Exporting Configuration Report 285
Veeam Self-Service Backup Portal 286
Required Permissions 287
Accessing Veeam Self-Service Backup Portal 288
Working with Veeam Self-Service Backup Portal 291
CONTROLLING BACKUP INFRASTRUCTURE WITH VSPHERE WEB CLIENT PLUG-IN 302
Getting Started 303
Configuring Plug-in Settings 306
Examining Backup Infrastructure 308
Creating Restore Points with VeeamZIP and Quick Backup 310
VSPHERE SELF-SERVICE BACKUP PORTAL 314
Configuring Delegation Mode 316
Managing Tenant Accounts 318
Adding Tenant Account 319
Editing Tenant Account 323
Exporting List of Tenant Accounts 326
Removing Tenant Account 327
Using vSphere Self-Service Backup Portal 328
Viewing Self-Service Backup Portal Statistics 330
Managing Backup Jobs 332
Managing VMs 334
Restoring Guest OS Files 337
Restoring Application Items 338
APPENDIX A. LICENSE UPDATE SESSION DATA 339
APPENDIX B. CONFIGURING AD FS FOR SAML AUTHENTICATION 340

Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

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

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

About This Document

This guide is intended for IT managers, virtual infrastructure administrators, and other personnel responsible for the product deployment and operation.

This document describes the features included in the Veeam Backup Enterprise Manager. It also provides usage examples and gives step-by-step instructions that will help you better understand how to install the Veeam Backup Enterprise Manager and monitor your Veeam Backup infrastructure, services and jobs.

Intended Audience

The document is intended for backup administrators and other IT professionals who plan to deploy and use Veeam Backup Enterprise Manager. This guide assumes that you have a good understanding of Veeam Backup & Replication and VMware vSphere.

About Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager (Enterprise Manager) is a management and reporting component that allows you to manage multiple Veeam Backup & Replication installations from a single web console. Veeam Backup Enterprise Manager helps you optimize performance in remote office/branch office (ROBO) and large-scale deployments and maintain a view of your entire virtual environment.

The distributed architecture of Veeam Backup & Replication allows you to create a custom backup infrastructure that meets your company needs. Veeam Backup Enterprise Manager manages backup and replication according to your administrative, business and security requirements and restrictions. With a number of Veeam Backup & Replication instances installed on different servers, Veeam Backup Enterprise Manager acts as a single management point. It allows you to control license distribution, manage backup jobs across the backup infrastructure, analyze operation statistics of Veeam backup servers, perform restore operations, and so on.

In particular, with Veeam Backup Enterprise Manager you can:

- Manage jobs across multiple Veeam backup servers.
- View on-going reporting data for all jobs running on these servers, set up email notifications to get information on the status of all jobs.
- Search for machines, file shares, and guest files in backups and replicas.
- Perform recovery operations for VMs and physical machines, including 1-Click restore, 1-click guest OS file restore and application items restore (for Microsoft Exchange mailboxes, Microsoft SQL Server databases and Oracle databases); perform 1-Click restore for file share backups.
- Centrally manage and update licenses to ensure compliance.
- Delegate permissions for restore operations to personnel in charge.
- Manage VMware vCloud Director organizations and support their administrators with the Veeam Self-Service Backup Portal.
- Manage vSphere user accounts and support them with the vSphere Self-Service Backup Portal.
- Install vSphere Web Client plug-in on vCenter servers.
- Implement data encryption and decryption processes for the Veeam solutions.
- Provide operation automation with Veeam Backup Enterprise Manager REST API.

What's New in Version 11

Veeam Backup Enterprise Manager 11 introduces the following new features and enhancements.

Continuous Data Protection (CDP)

Now Veeam Backup Enterprise Manager lets you manage CDP policies that have been created on backup servers added to the Enterprise Manager infrastructure. Depending on the account role, you can view, edit, enable and disable CDP policies. For replicated VMs, you can start failover. For more information, see Managing CDP Policies and Performing Failover.

VMware vCloud Director Replication

In Veeam Backup Enterprise Manager, you can manage vCD replication jobs as well as start failover for replicated vApps. For more information, see Managing Jobs and Performing Failover.

Multiple Repositories for vCD Organizations

Now you can add multiple repositories for each vCD organization. It allows tenants to select which backup repository to use for their backup jobs. For more information, see Managing Configurations for vCD Organizations.

Veeam Plug-in for VMware vCloud Director

Veeam Plug-in for VMware vCloud Director allows members of vCD organizations to manage their vCD jobs and restore VMs, files and application items in the native vCD interface. Users get access to the portal features by logging in to the vCloud Director Service Provider Tenant Portal under their vCD credentials.

Localization

Veeam Backup Enterprise Manager 11 is available in the following languages:

- Chinese (Simplified, PRC)
- English
- French
- German
- Italian
- Japanese
- Spanish

You can select a preferred language on the login page. If the language you need is not available, you can add it. Localization is based on the GNU gettext tools, and English strings are used as message IDs. For more information, see Managing Languages.

SAML Authentication for vSphere Self-Service Backup Portal

In version 11, you can configure SAML authentication for vSphere Self-Service Backup Portal. Both the External User and External Group are supported. In case of SAML authentication, you can configure the delegation mode based on vSphere tags only. For more information, see SAML Authentication Support.

What's New in Version 11a

Veeam Backup Enterprise Manager 11a (build 11.0.1.1261) introduces the following new features and enhancements.

Licensing

Now Veeam Backup Enterprise Manager can apply its license to backup servers that have Veeam Backup & Replication version 10 or later installed.

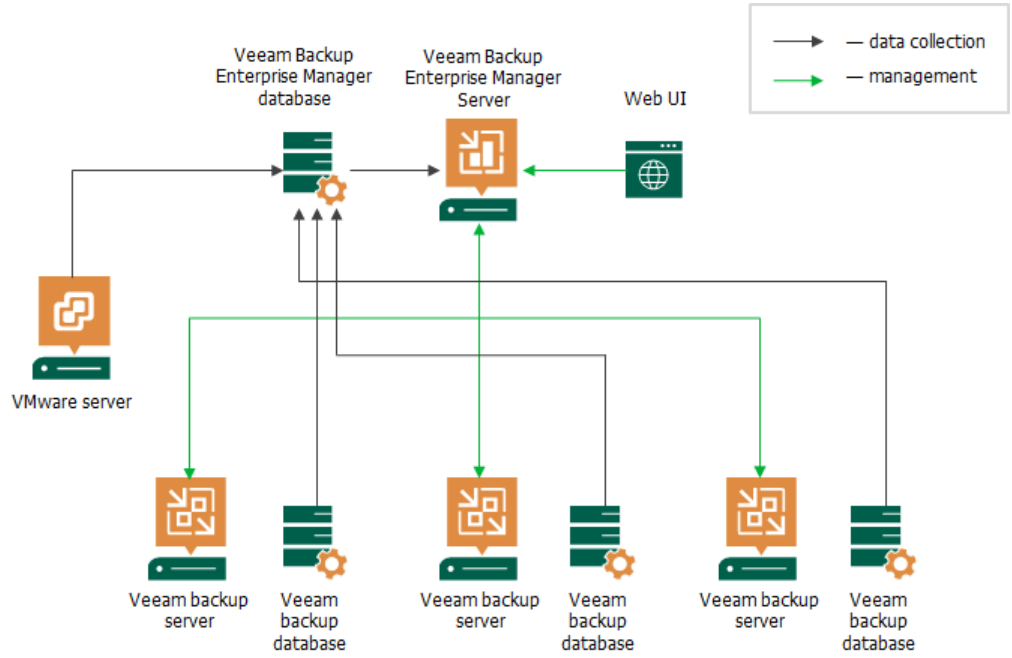
Veeam Self-Service Backup Portal

- Starting from Veeam Backup Enterprise Manager 11a, you can add vCD organization configurations for multiple vCD servers. All vCD servers must be added to the backup infrastructure of the same backup server. For more information, see Adding Organization Configuration.
- In version 11, you can select a display language for Veeam Self-Service Backup Portal when you access the portal by its URL. In version 11a, the portal is available in the selected language when you open it from the vCD environment as well. For more information, see Accessing Veeam Self-Service Backup Portal.

How Veeam Backup Enterprise Manager Works

Veeam Backup Enterprise Manager aggregates data from multiple Veeam backup servers, as well as from the underlying VMware vCenter servers.

1. Veeam Backup Enterprise Manager retrieves data from the managed Veeam backup servers using a data collection job. This job gets information about the backup and replication jobs, processed machines, and other data from the configuration databases used by Veeam backup servers.
2. Collected data is stored to the Veeam Backup Enterprise Manager database (hosted on SQL Server) and can be accessed by multiple users from the web interface. This web interface also allows for modifying job settings, license management, installing Veeam plug-in on vCenter server, and other tasks.
3. When a user modifies a backup job using Veeam Backup Enterprise Manager, these changes are communicated to the backup server that manages the job and stored in its configuration database.



If you have a Veeam Agent integrated with Veeam Backup & Replication, you can use Veeam Backup Enterprise Manager to browse and restore guest OS files and application items from a backup stored in a Veeam backup repository. These processes involve appropriate backup job setup, as well as mount and data transfer operations. For more information, see Support for Veeam Agents.

Enterprise Manager Components

Veeam Backup Enterprise Manager incorporates the following services and components:

- **Veeam Backup Enterprise Manager Service** coordinates all operations performed by Veeam Backup Enterprise Manager such as backup, replication, recovery verification and restore tasks. The Veeam Backup Enterprise Manager Service runs under the *Local System* account or an account that has the *Local Administrator* permissions on the backup server. This service is installed and started automatically on the local Windows server.
- **VeeamBackup** and **VeeamBackup site** (IIS extension) application pools are created and displayed in IIS Manager. These web applications are deployed on the local IIS web server.
- Web interfaces used to access Veeam Backup Enterprise Manager from different infrastructures:
  - **Main web interface** is used to browse and perform operations with jobs, backups and machines, to configure Enterprise Manager functionality and control infrastructure. For more information, see Getting to Know Veeam Backup Enterprise Manager.
  - **Veeam Self-Service File Restore Portal** that allows administrators to restore files or folders from the guest OS of a virtual or physical machine. For more information, see Using Self-Service Portal to Restore Machine Guest Files.
  - **Veeam Self-Service Backup Portal** and Veeam Plug-in for VMware vCloud Director that provide members of vCloud Director organizations with a UI for self-service operations on machine protection. For more information, see Veeam Self-Service Backup Portal.
  - **VMware vSphere Self-Service Backup Portal** that provides Service Providers with a UI for managing access permissions and vSphere quotas for their customers. For more information, see vSphere Self-Service Backup Portal.

> **NOTE**
>
> Veeam Self-Service File Restore Portal, Veeam Self-Service Backup Portal, Veeam Plug-in for VMware vCloud Director and VMware vSphere Self-Service Backup Portal features are available in the Enterprise Plus edition of Veeam Backup & Replication.

- **SQL Server database** is used to store configuration and performance data. For more information, see Deployment.
- **Veeam Backup Catalog** is used for guest OS file indexing, index data retention and its synchronization with the information on a Veeam backup server. It comprises a Windows service named *Veeam Guest Catalog* also installed on the Veeam Backup Enterprise Manager server. For more information, see Veeam Backup Catalog.
- **Veeam Backup Search** is an optional component used for guest OS file indexing of protected machines. This component is included in the installation package to provide backward compatibility with older existing deployments. For a new deployment, there is no need to install Veeam Backup Search, since all operations related to guest OS file indexing and search will be performed by Veeam's proprietary built-in indexing engine. For more information, see Veeam Backup Search Capabilities.
- **Veeam Cloud Connect Portal** is an optional component that comprises the Veeam Cloud Connect Portal website (IIS extension) and UI. It is intended for the tenants of Service Providers. For more information, see the Veeam Cloud Connect Guide.

- **Veeam Backup Enterprise Manager REST API** lets developers communicate with Veeam Backup Enterprise Manager to query information about Veeam Backup Enterprise Manager objects and perform basic operations with them using HTTP and HTTPS protocols and the principles of REST. For more information, see the Veeam Backup Enterprise Manager REST API Reference.
- **Veeam VMware vSphere Web Client plug-in** allows vSphere administrators to manage backup infrastructure of the virtual environment. For more information, see the Controlling Backup Infrastructure with vSphere Web Client Plug-in.

Veeam Backup Catalog

Veeam Backup Catalog is a feature that stands for VM guest OS file indexing. Veeam Backup Catalog comprises Veeam Guest Catalog services that run on the following servers in the backup infrastructure: Veeam backup server and Veeam Backup Enterprise Manager server.

- Veeam Guest Catalog service on the Veeam backup server works as a local catalog service. It collects index data for backup jobs on this specific Veeam backup server and stores this data locally in the Veeam Backup Catalog folder.
- Veeam Guest Catalog service on Veeam Backup Enterprise Manager works as a federal catalog service. It communicates with Veeam Guest Catalog services on Veeam backup servers connected to Veeam Backup Enterprise Manager and performs the following tasks:
    - Replicates index data from Veeam backup servers to create a federal catalog
    - Maintains index data retention
    - Lets you search for machine guest OS files in backup files

Veeam Backup Search Capabilities

Veeam Backup Enterprise Manager allows you to browse the guest OS file system in a machine backup, search for guest OS files and restore necessary files. These operations are also supported for the backups of physical machines created by Veeam Agents (Server edition is needed). For more information on Veeam Agents, see Support for Veeam Agents.

> **NOTE**
>
> While browsing and search possibilities are available to all Veeam Backup Enterprise Manager users, file restore operations can be performed by authorized users only.

Guest OS Files Indexing

By default, Veeam uses its proprietary file indexing mechanism to index machine guest OS files and facilitate search for files in backups with Veeam Backup Enterprise Manager. For more information on how to enable guest OS file system indexing in the backup job settings, see the Application-Aware Processing section of the Veeam Backup & Replication User Guide.

1. When a backup job with guest OS files indexing enabled is run, Veeam Backup & Replication creates a catalog (or index) of the machine guest OS files and stores index files on the Veeam backup server.
2. After that, the Veeam Guest Catalog Service performs index replication — it aggregates index data for all machine image backups from managed backup servers. This consolidated index is stored on the Veeam Backup Enterprise Manager server in the `C:\VBRCatalog\Index\` folder and is used for search queries.
3. Then you can browse or search through machine guest OS files using the search criteria you need. Once you find a necessary file, you can use the File-Level Restore feature to recover the file from the machine backup. For more information, see How Indexing Works.

Importing Indexed Guest OS Files

When you move machine backups to an external storage device or tape, indexing data for such machines remains in the catalog. It means that these machines still appear in search results. You can use the **Import** feature to import the backup to the Veeam Backup & Replication backup server, and then recover the file.

However, consider that by default, backup repository is the primary destination for the search. This means, in particular, that if a backup (with indexed guest) is stored in both locations — repository and tape — then Enterprise Manager search results will only include files from the backup stored on the repository. Files from tape-archived backup will appear in search results only if not found on the repository. For more information, see Configuring Retention Settings.

> **NOTE**
>
> This capability is supported in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Searching for Physical Server Guest OS Files

If your Veeam Backup & Replication server is integrated with Veeam Agent, you can set up the integrated Veeam Agent to create an index (catalog) of files and folders on the physical machine OS. This allows you to search for backed-up files and perform 1-Click restore of server files in Veeam Backup Enterprise Manager; all operations are similar to those performed for virtual machine backup.

For more information, see the following sections:

- Guest File Browsing and 1-Click Restore section of this guide

- Guest Processing section of the Veeam Agent for Windows User Guide
- File System Indexing section of the Veeam Agent for Linux User Guide
- File System Indexing section of the Veeam Agent for Oracle Solaris User Guide
- File System Indexing section of the Veeam Agent for IBM AIX User Guide

File-Level Restore Capabilities

When you restore files from the restore point created for a virtual or physical machine *with guest OS file indexing enabled*, Veeam uses the following workflow:

1. To provide for browsing and search, Veeam uses index data to represent the file system of the guest OS.
2. If you then select to download the necessary files, Veeam Backup & Replication will mount virtual or physical machine disks (from the restore point in repository) on the Veeam backup server and then copy these files from the backup server to the target location.
3. If you select to restore files to the original location, an additional mount point will be created on the mount server associated with the backup repository storing the backup file. During restore, machine data will flow from repository to target, keeping the machine traffic in one site and reducing load on the network.
4. After you download or restore the necessary files, and finish the restore session, the machine (or server) disks will be unmounted.

When you restore files from the restore point that was created *without guest OS file indexing*, Veeam Backup & Replication uses the following workflow:

1. To provide for browsing, disks of the virtual machine or physical server from the backup file are mounted to Veeam backup server.
2. If you then select to download the necessary files, Veeam will copy these files from the backup server to the destination location, using this mount point.
3. If you select to restore files from the backup to the original location on the production machine, an additional mount point will be created on the mount server associated with the backup repository storing the backup file.
4. If you restore machine files from a VM replica, a single mount point for all these operations (browsing, download, restore to original location) will be created on the Veeam backup server.
5. After you download or restore the necessary files, and finish the restore session, the machine (or server) disks will be unmounted.

How Indexing Works

When you run a backup job with the file indexing option enabled, Veeam Backup & Replication indexes the machine file system, collects indexing data and writes it to the *GuestIndexData.zip* file. The *GuestIndexData.zip* file is first stored in a temporary folder on the Veeam backup server.

As soon as the backup job completes, Veeam Backup & Replication notifies the local Veeam Backup Catalog service. The service saves indexing data in the Veeam Backup Catalog folder on the Veeam backup server. During the next catalog replication session started on Veeam Backup Enterprise Manager, indexing data from the Veeam backup server is replicated to the Veeam Backup Catalog on Veeam Backup Enterprise Manager server. By federating indexing data from all connected Veeam backup servers, the Veeam Backup Catalog service on Veeam Backup Enterprise Manager creates a global catalog for the whole backup infrastructure.

Veeam Backup & Replication supports file-level restore not only for machines included in guest catalog but also for the machines that are not indexed. Indexing may be disabled at the time of restore point creation, or indexing operation may fail. In this case, the restore point of a Windows machine is mounted to the backup server that manages the job, and the restore point of a non-Windows machine is mounted to the helper appliance.

Then a user will be able to locate the necessary files and folders and perform restore operation. To learn more about mount operation, refer to the Veeam Backup & Replication User Guide and to the Search and Restore of Machine Guest Files section of this guide.

Indexing Data

Veeam Backup & Replication stores indexing data in the Veeam Backup Catalog folder. By default, the Veeam Backup Catalog is located in the `C:\VBRCatalog` folder on the Veeam backup server and on Veeam Backup Enterprise Manager.

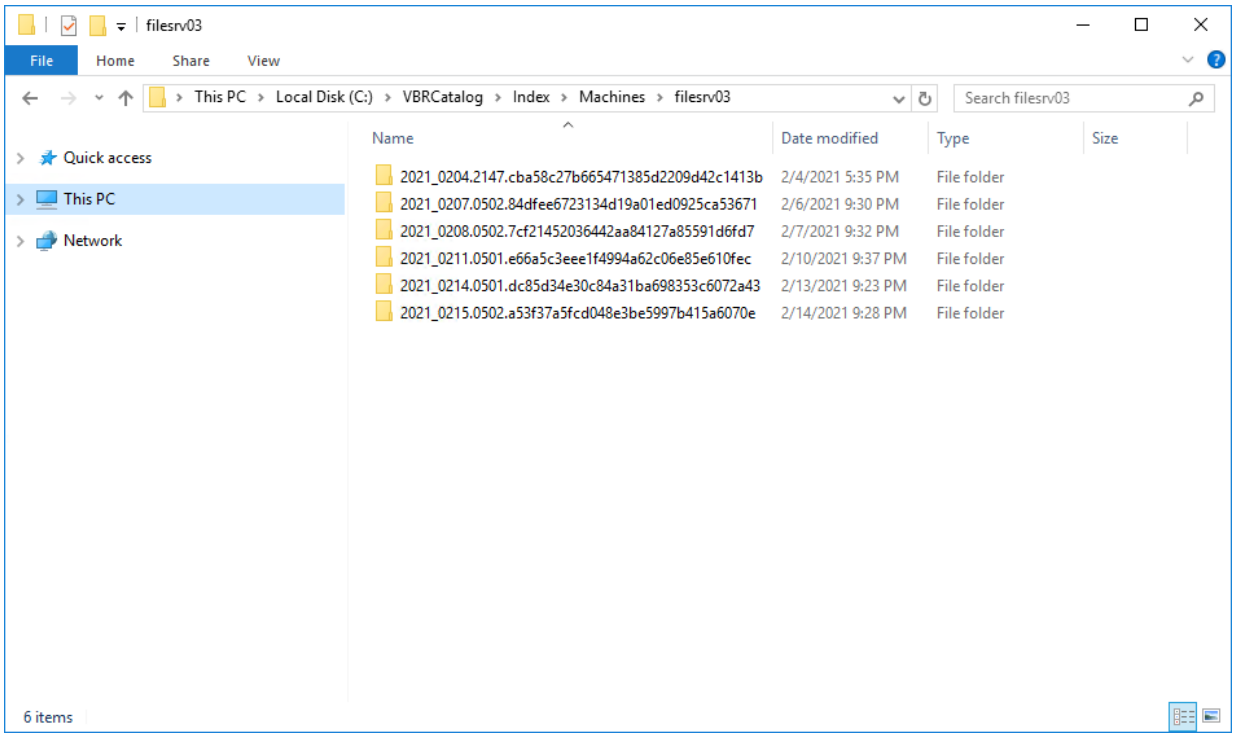
Veeam Backup Catalog comprises the following data:

- Machine index
- Session index

Machine Index

Machine index reproduces the structure of files and folders on the machine guest OS.
Veeam Backup & Replication uses the file index to search for guest OS files within machine backups.

For every machine whose file system has been indexed, there is a dedicated folder that contains indexing data for all restore points available for the machine.



Session Index

Veeam Backup Catalog keeps information for every backup job session. Session indexing data describes which machine restore points correspond with a specific backup job session and what sets of files are required to restore a machine to a specific point in time.

Session indexing files vary for incremental and reverse incremental backup chains:

- **For incremental backup chains**, a session indexing file contains information about only one restore point — the restore point that is created with this backup job session. Additionally, it contains information about a set of files that is required to restore a machine to this point in time. For example, if a backup chain contains 5 restore points, the 5th session indexing file will contain information about the 5th restore point and a group of 5 files that are required to restore the machine to this point in time.

```
BackupServer=BACKUP01
JobName=srv04
SessionDateUtc=05/13/2014 08:05:57.081
####################################################
#  OIBS
oib0.VmName=srv04
oib0.BackupTimeUtc=05/13/2014 08:02:04.988
oib0.OibUID=f81f790c-103e-4351-81a4-e4ec8a8c290c
oib0.Platform=EVmware
oib0.Group=grp0
####################################################
#  BACKUP FILE GROUPS
grp0.file0.Server=BACKUP01
grp0.file0.Path=c:\backup\srv04\srv042014-05-13T010101.vib
grp0.file0.ModifyDateUtc=05/13/2014 08:04:10.293
grp0.file1.Server=BACKUP01
grp0.file1.Path=c:\backup\srv04\srv042014-05-13T004536.vib
grp0.file1.ModifyDateUtc=05/13/2014 07:47:52.077
grp0.file2.Server=BACKUP01
grp0.file2.Path=c:\backup\srv04\srv042014-05-13T000053.vib
grp0.file2.ModifyDateUtc=05/13/2014 07:04:24.38
grp0.file3.Server=BACKUP01
grp0.file3.Path=c:\backup\srv04\srv042014-05-12T230102.vib
grp0.file3.ModifyDateUtc=05/13/2014 06:04:25.003
grp0.file4.Server=BACKUP01
grp0.file4.Path=c:\backup\srv04\srv042014-05-12T220051.vib
grp0.file4.ModifyDateUtc=05/13/2014 05:03:53.817
grp0.file5.Server=BACKUP01
grp0.file5.Path=c:\backup\srv04\srv042014-05-12T210105.vbk
grp0.file5.ModifyDateUtc=05/13/2014 04:07:55.047
```

- **For reverse incremental backup chains**, a session indexing file contains information about all restore points engaged in the backup job session. In a reverse incremental chain, the last restore point is always a full backup. To produce a full backup and calculate incremental changes, Veeam Backup & Replication needs to address all points in the job. For this reason, the session indexing file refers not only to the restore point created with the backup job session, but also to all restore points preceding it. Additionally, a session indexing file describes groups of files that are required to restore a machine to all possible restore points. For every restore point, there is a separate group of files.

  For example, if you have a reverse incremental chain of 3 restore points, the session indexing file for the last backup job session will contain information about 3 restore points and will describe three groups of files:

  - Group 0 will list restore points that are required to restore the machine to the 1st, the earliest restore point.
  - Group 1 will list restore points that are required to restore the machine to the 2nd restore point.

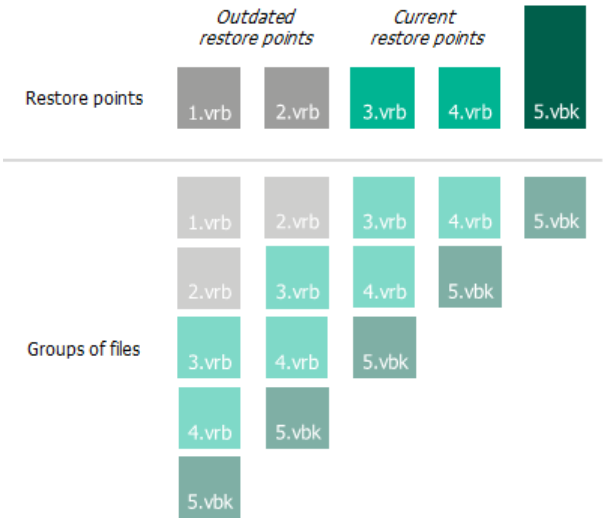
- Group 2 will list restore points that are required to restore the machine to the 3rd, the latest restore point.

```
BackupServer=SRV02
JobName=srv01_reversed
SessionDateUtc=05/14/2014 11:20:18.952
####################################################
#  OIBS
oib0.VmName=srv01
oib0.BackupTimeUtc=05/14/2014 10:56:55.993
oib0.OibUID=47c62e82-3066-478c-8272-1fb65a47d601
oib0.Platform=EVmware
oib0.Group=grp1
oib1.VmName=srv01
oib1.BackupTimeUtc=05/14/2014 11:02:20.15
oib1.OibUID=d39f4a3c-2b5b-415a-ae0d-e9acc49f63a0
oib1.Platform=EVmware
oib1.Group=grp2
oib2.VmName=srv01
oib2.BackupTimeUtc=05/14/2014 11:16:52.779
oib2.OibUID=1f3c31bf-9541-46ac-9826-62ecfd76a291
oib2.Platform=EVmware
oib2.Group=grp3
####################################################
#  BACKUP FILE GROUPS
grp0.file0.Server=BACKUP
grp0.file0.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T035606.vrb
grp0.file0.ModifyDateUtc=05/14/2014 10:56:55.993
grp0.file1.Server=BACKUP
grp0.file1.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T040137.vrb
grp0.file1.ModifyDateUtc=05/14/2014 11:18:14.43
grp0.file2.Server=BACKUP
grp0.file2.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T041612.vbk
grp0.file2.ModifyDateUtc=05/14/2014 11:18:45.973
grp1.file0.Server=BACKUP
grp1.file0.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T040137.vrb
grp1.file0.ModifyDateUtc=05/14/2014 11:18:14.43
grp1.file1.Server=BACKUP
grp1.file1.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T041612.vbk
grp1.file1.ModifyDateUtc=05/14/2014 11:18:45.973
grp2.file0.Server=BACKUP
grp2.file0.Path=c:\backup\srv01_reversed\srv01_reversed2014-05-14T041612.vbk
grp2.file0.ModifyDateUtc=05/14/2014 11:18:45.973
BSessionVersion=5
```

A full backup file "moves forward" with every new backup job run, and Veeam Backup & Replication updates groups of files. This helps maintain valid groups of files required to restore a machine to a necessary point in time.

The session indexing files maintain groups of files for all restore points that have ever existed in the backup chain. This behavior lets you search and restore machine guest OS files in archived backups.

When a backup is archived to tape or to a secondary backup repository, you can still browse the machine file system to this point in time using historical indexing data. Once you find a necessary file, Veeam Backup Enterprise Manager uses the session indexing file to inform you what group of files is required to restore the machine to the selected point in time.



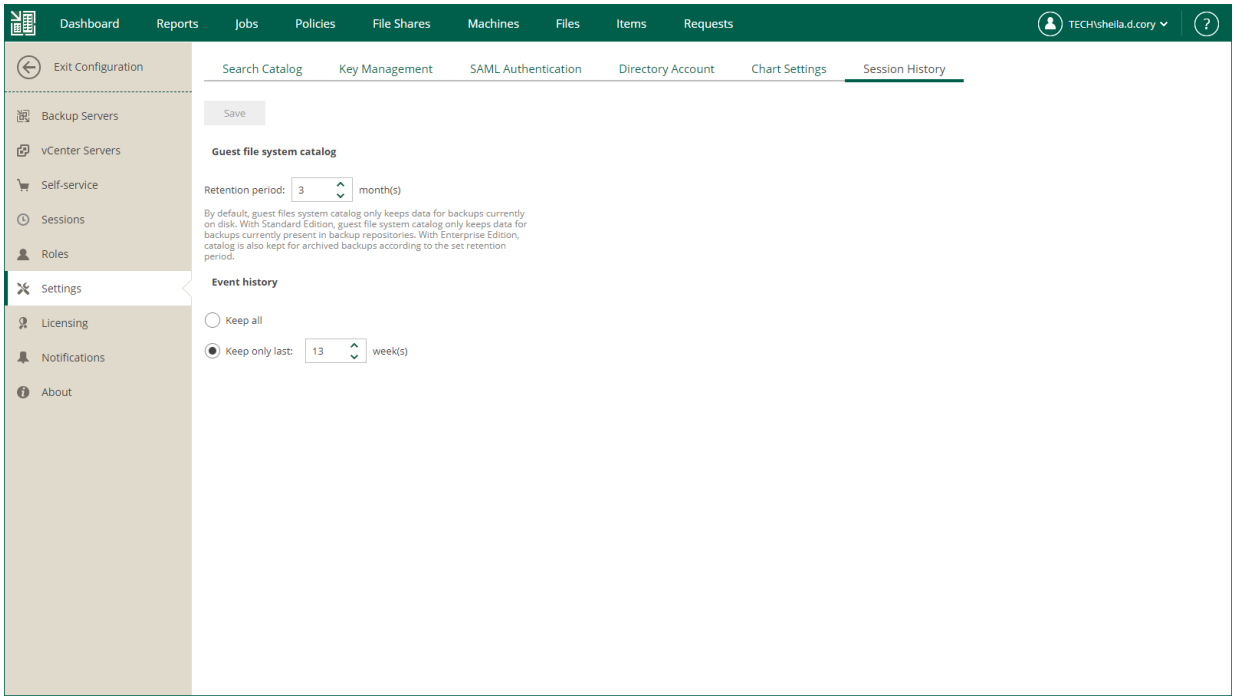
Current and Historical Indexing Data

Indexing data structures in Veeam Backup Catalog are divided into two groups:

- Current indexing data stores information for valid restore points that are currently available in the backup chain in the backup repository. For example, if the retention policy for a backup job is set to 14, Veeam Backup Catalog will contain indexing data for 14 restore points and 14 backup job sessions.
- Historical indexing data stores information for obsolete restore points: the points that were removed from the backup chain. When you run a backup job to create a new restore point, the earliest restore point is marked as obsolete and removed from the backup chain. Indexing data for this restore point in the Veeam Backup Catalog is not removed. Instead, it is marked as historical.

  Historical indexing data helps the user accomplish file search in backup files that were archived to tape or to a secondary backup repository.

By default, Veeam Backup Enterprise Manager keeps historical indexing data for 3 months. To change this value, navigate to the **Configuration** > **Settings** > **Session History** > **Guest file system catalog** section in Veeam Backup Enterprise Manager.



Indexing Data Retention

The retention policy for Veeam Backup Catalog helps you maintain the necessary amount of indexing data on the Veeam Backup Enterprise Manager server.

The retention policy for Veeam Backup Catalog is controlled by two values:

- Retention policy for a backup job on the Veeam backup server: the number of restore points in the backup chain
- Retention period for indexing data in Veeam Backup Enterprise Manager

The retention period is calculated differently for backup chains created with different backup methods:

- Retention for forward incremental backup chains
- Retention for reverse incremental backup chains

Retention for Forward Incremental Backups

The retention policy for the forward incremental backup chain is calculated by the following formula:

Retention period = MAX (Catalog Retention, X)

where:

- *Catalog Retention* is the retention period specified in Veeam Backup Enterprise Manager.
- *X* is the amount of time for which restore points are kept by a backup job.

For example, the retention policy settings are specified in the following manner:

- The retention policy for a backup job is set to 5 points. The backup job is run daily.
- The retention period in Veeam Backup Enterprise Manager is set to 1 month, or 30 days.

In this case, Veeam Backup Enterprise Manager will retain indexing data for 30 days, because this value is greater than the number of restore points in the job.

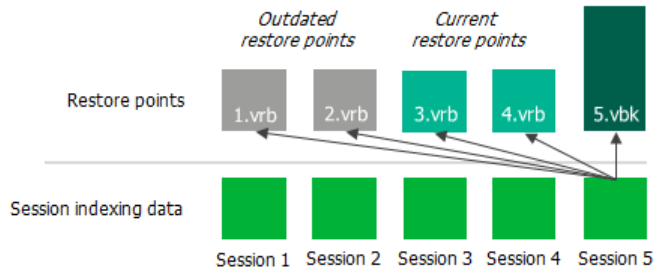
Retention for Reverse Incremental Backups

For reverse incremental backup chains, Veeam Backup Enterprise Manager keeps more indexing data in Veeam Backup Catalog than it may seem to be required according to the retention policy. This happens due to backward nature of reverse incremental backups.

When Veeam Backup Enterprise Manager deletes indexing data by retention, it removes the whole set of files: machine indexing data and session indexing data. Before removing indexing data for a specific machine restore point, Veeam Backup Enterprise Manager makes sure that this restore point is not referenced by any of backup job sessions:

- If no relations are detected, indexing data for this machine restore point is removed from Veeam Backup Catalog.
- If the machine restore point is referenced by any backup job session, indexing data for this machine restore point remains in Veeam Backup Catalog.

However, in reverse incremental chains, session indexing data references the machine restore point that was created in the backup job sessions, and restore points preceding it. To learn more, see Session Index.



For this reason, Veeam Backup Enterprise Manager retains more indexing data for reverse incremental chains. The retention period is calculated by the following formula:

Retention period = MAX (Catalog Retention, X) + X

where:

- *Catalog Retention* is the retention period specified in Veeam Backup Enterprise Manager.
- *X* is the amount of time for which restore points are kept by a backup job.

For example, the retention policy settings are specified in the following manner:

- The retention policy for the backup job is set to 3 points. The backup job is run daily.
- The retention period in Veeam Backup Enterprise Manager is set to 1 month, or 30 days.

In this case, Veeam Backup Enterprise Manager will retain in Veeam Backup Catalog indexing data for 30 days plus indexing data for 3 restore points in the backup chain.

> **IMPORTANT**
>
> The longer the backup chain, the more indexing data is stored in Veeam Backup Catalog.
>
> In case of long backup chains, indexing data may take a lot of space on the Veeam Backup Enterprise Manager server. To overcome this situation, you can adjust the retention policy scheme or provide enough space for indexing data in Veeam Backup Catalog on Veeam Backup Enterprise Manager.

SAML Authentication Support

Veeam Backup Enterprise Manager supports single sign-on authentication based on the SAML 2.0 protocol. Enterprise organizations who use a single sign-on (SSO) service in their IT infrastructure can extend single sign-on capabilities to Veeam Backup Enterprise Manager. Once a user of the organization is logged in to the single sign-on service, the user can access Veeam Backup Enterprise Manager without the need to provide their credentials.

You can enable SSO for the following Veeam Backup Enterprise Manager components:

- Veeam Backup Enterprise Manager website
- vSphere Self-Service Backup Portal

SAML authentication scenario in Veeam Backup Enterprise Manager comprises the following parties:

- User that logs in to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal.
- Service provider (SP) — an application accessed by the user. In the Veeam backup infrastructure, the service provider is the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal.
- Identity provider (IdP) — an external service (hosted on premises or in the public cloud) that facilitates SSO. The IdP keeps user identity data in a user store (or attribute store). Upon requests from the SP, the IdP issues SAML authentication assertions, that is, identifies the user and provides the SP with required information about the user.

  Veeam Backup Enterprise Manager supports identity providers that support the SAML 2.0 protocol, for example, Active Directory Federation Services (AD FS), Azure Active Directory (Azure AD), Okta, Auth0, Keycloak and so on.

The SP and IdP exchange information in the XML format in accordance with the SAML V2.0 Standard. The Enterprise Manager administrator can specify what information is required from the IdP to set up SAML authentication in Enterprise Manager and how SAML requests and responses are sent.

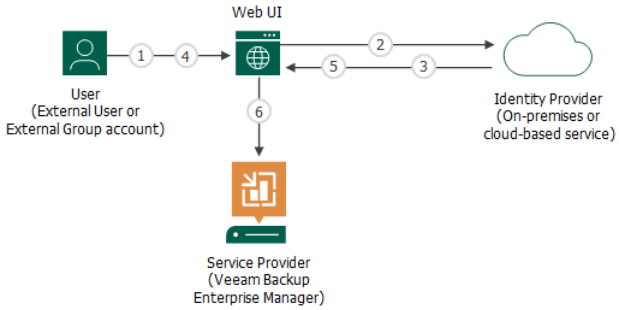
How It Works

In Veeam Backup Enterprise Manager, SAML authentication is performed in the following way:

1. The user accesses the website under an account of the *External* type. The account must be registered in advance in Enterprise Manager by the Enterprise Manager administrator.
2. Veeam Backup Enterprise Manager redirects a SAML authentication request to the IdP.
3. If the user has not previously logged in with the single sign-on service of the IdP, the IdP redirects the user to the URL of the single sign-on webpage.

   Alternatively, if the user is already logged in with the single sign-on service, the user proceeds directly to the step 6.
4. If the user has not previously logged in with the single sign-on service, the user specifies the password of their account on the single sign-on webpage.
5. The IdP issues a SAML assertion and redirects it to Veeam Backup Enterprise Manager in the SAML response. The SAML assertion must meet the following requirements:
   - Contain a User Principal Name (UPN) of the user in the *<NameID>* element of the SAML response.
   - Specify that the UPN type is *Persistent*.

6. The user gains access to the website and can perform operations according to the role and restore scope specified for the user account.



Getting Started

To set up SAML authentication, the Enterprise Manager administrator must complete the following tasks in Enterprise Manager:

1. Obtain SAML metadata from the IdP and import this metadata to Veeam Backup Enterprise Manager. The IdP metadata includes the IdP entity ID, login URL, SAML binding and public key certificate that will be used to validate authentication assertions sent by the IdP. For more information, see Specifying Identity Provider Settings.

2. [Optional] If you want to use a digital certificate to encrypt and sign SP SAML requests, specify certificate settings. For more information, see Selecting SP Certificate.

3. [Optional] Specify advanced settings for SAML authentication. These settings define how the SP and IdP will exchange SAML information. You may want to adjust the settings to strengthen SAML information exchange between the SP and IdP. For more information, see Specifying Advanced SAML Authentication Settings.

4. Export SP SAML metadata in Veeam Backup Enterprise Manager and pass this metadata to the IdP. The SP metadata includes the SP entity ID, assertion consumer URL and public key certificate that will be used to encrypt SAML responses sent by the IdP. For more information, see Obtaining Service Provider Settings.

5. Create user accounts. To provide users of a SSO service with access to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal, the administrator must create for these users accounts of the *External User* or *External Group* type. For more information, see Managing Accounts and Roles and Managing Tenant Accounts.

On the IdP side, the IdP must configure trust relationship with Veeam Backup Enterprise Manager and configure rules that define what information to provide to the SP. Depending on the IdP, these rules may be configured in the form of claims, attribute statements and so on. For an example of how to perform this task in AD FS, see Appendix B. Configuring AD FS for SAML Authentication.

Planning and Preparation

Before you install Veeam Backup Enterprise Manager, you must check that the virtual environment and machines that you plan to use as backup infrastructure components meet the product hardware recommendations and system requirements.

System Requirements

Make sure that servers that you plan to use as Veeam Backup Enterprise Manager infrastructure components meet system requirements listed below:

- Veeam Backup Enterprise Manager
- Veeam Cloud Connect Portal
- VMware vCloud Director

Veeam Backup Enterprise Manager

It is recommended to install the same product version on the Veeam Backup Enterprise Manager server and Veeam backup servers.

Specification	Requirement
Hardware	• CPU: x86-64 processor. • Memory: 4 GB RAM (minimum recommended). • Hard disk space: 2 GB on the system disk (required to extract all components from the setup package during the product installation). • Network: 1 Gbps or faster connection to Veeam Backup & Replication servers.
OS	64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2022[1] • Microsoft Windows Server Semi-Annual Channel (from version 1803 to version 20H2) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows 2008 R2 SP1 • Microsoft Windows 10, version 21H1[1] • Microsoft Windows 10 (from version 1803 to version 20H2) • Microsoft Windows 8.1 • Microsoft Windows 7 SP1 [1] This version is supported starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261).

Specification	Requirement
SQL Server	Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported): • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 (Microsoft SQL Server 2016 SP1 Express Edition is included in the setup)[1] • Microsoft SQL Server 2014 with Microsoft SQL Server 2014 Management Objects and Microsoft System CLR for SQL Server 2014 • Microsoft SQL Server 2012 (Microsoft SQL Server 2012 SP4 Express Edition is included in the setup)[2] • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 SQL Server 2008 databases and later with compatibility to SQL Server 2005 are not supported. Veeam Backup Enterprise Manager configuration database can be deployed in Microsoft SQL AlwaysOn Availability Groups. For more information, see this Veeam KB article. [1] For machines running Microsoft Windows Server 2012 or later. [2] For machines running Microsoft Windows 7 or Microsoft Windows Server 2008 R2.
Server Software	• Microsoft Internet Information Services 7.5 or later: support for extentionless URLs for IIS 7.5 or later, ASP.NET 4.5, .NET Extensibility 4.5 for IIS 8.0. For IIS 8.5, the URL rewrite module is required if you plan to use Veeam Self-Service Backup Portal or vSphere Self-Service Backup Portal. • Directory Browsing component, Default Document component, HTTPS Errors component, Static Content component, Windows Authentication component, WebSocket Protocol component. • Microsoft .NET Framework 4.7.2 (included in the setup). • Windows Installer 4.5 (included in the setup).
Client Software	• Browsers: Microsoft Internet Explorer 11.0 or later, Microsoft Edge, latest versions of Mozilla Firefox and Google Chrome are supported. The browser must have JavaScript and WebSocket protocol enabled. • Microsoft Excel 2007 or later (view reports exported to Microsoft Excel format).

IMPORTANT

To restore Microsoft Exchange items with Veeam Backup Enterprise Manager, Microsoft Exchange servers must be members of the same Microsoft Active Directory forest.

[Optional] Veeam Cloud Connect Portal

Specification	Requirement
Hardware and software	Refer to hardware system requirements and software system requirements for Veeam Backup Enterprise Manager.
Supported browsers	For PC: • Microsoft Internet Explorer 11.0 or later • Microsoft Edge • Latest versions of Mozilla Firefox and Google Chrome For portable devices (tablets): latest versions of Apple Safari for iOS or Google Chrome for Android.

[Optional] VMware vCloud Director

Specification	Requirement
VMware vCloud Director	VMware vCloud Director 9.5-10.2. For vCD replication: 9.7-10.2.
Other software	If your Enterprise Manager deployment uses IIS 8.5, then URL rewrite module is required to work with Veeam Self-Service Backup Portal for vCloud Director.

Required Permissions

This section provides information on the account permissions required for installing/upgrading and using Veeam Backup Enterprise Manager and its components.

Veeam Backup Enterprise Manager

Account	Required Permission
Account used to run the setup	The account used for product installation must have the *local Administrator* permissions on the target machine.
	To create a new Veeam Backup Enterprise Manager database during the setup process, the account must have the CREATE ANY DATABASE permission on the SQL Server level. After the database is created, this account automatically gets a *db_owner* role and can perform all operations with the database. Note: If a database is created in advance (by a database administrator or SQL Server administrator), the setup account must have the *db_owner* role for the database.
	To upgrade an existing Enterprise Manager database, the account must have the *db_owner* role.
Veeam Backup Enterprise Manager service account	It is recommended to use the *Local System* account as the Veeam Backup Enterprise Manager Service account. If you set another account to run this service, this account must have the following permissions: • *Local Administrator* permissions on the Veeam Backup Enterprise Manager server. • *Log on as service* right (granted automatically to the Veeam Backup Enterprise Manager Service account). • *Db_datareader* and *db_datawriter* roles, as well as permissions to *execute stored procedures* for the Enterprise Manager database on the Microsoft SQL Server. Alternatively, you can assign this account the *db_owner* role for the Enterprise Manager database. • *Full Control* NTFS permissions for the *VBRCatalog* or another folder where index files are stored. To add Active Directory user or group accounts to the Veeam Backup Enterprise Manager roles, the Veeam Backup Enterprise Manager service must be started under the Active Directory service account that has permissions to enumerate Active Directory domains. Active Directory users have enough permissions to enumerate Active Directory domains by default. If you use the local machine account instead, you will get the "*Cannot find user account DOMAIN\username*" error.

Account	Required Permission
Enterprise Manager user	To be able to work with the Veeam Backup Enterprise Manager web UI, users must be assigned the Portal Administrator, Portal User or Restore Operator role. For more information, see Configuring Accounts and Roles.
vSphere Web Client Plug-in for Veeam Backup & Replication (optional)	The account used to install the plug-in and the vCenter server account must belong to the same Active Directory domain in case of cross-domain access. The account used to install the plug-in must be assigned the following vCenter Server permissions: • To install the plug-in: **Extension** > **Register extension** • To uninstall the plug-in: **Extension** > **Unregister extension**
vSphere Self-Service Backup Portal user	The account used to work with vSphere Self-Service Backup Portal must have interactive logon permissions on the Enterprise Manager server.

Used Ports

This section covers typical connection settings for Veeam Backup Enterprise Manager, including:

- Enterprise Manager Operation Ports
- Ports for Restore Operations

> **NOTE**
>
> For more information on ports specific for Veeam Backup & Replication infrastructure components, see the Used Ports section of the Veeam Backup & Replication User Guide.

Veeam Backup Enterprise Manager Connections

The following ports must be opened to ensure proper operation of Veeam Backup Enterprise Manager and communication between components.

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager	Veeam backup server	TCP	9392	Default port used by Veeam Backup Enterprise Manager for collecting data from Veeam backup servers. Can be customized during Veeam Backup & Replication installation. For more information, see Specify Service Ports.
			9393	Default port used by the Veeam Guest Catalog service for catalog replication. Can be customized during Veeam Backup & Replication installation.
			2500 to 2600	Ports used by the Veeam Guest Catalog service for replicating catalog data.
			135	Default RPC port.
			49152 to 65535 (for Microsoft Windows 2008 and later)	Dynamic RPC port range. For more information, see this Microsoft KB article.

From	To	Protocol	Port	Notes
	SQL Server hosting the Enterprise Manager configuration database	TCP	1433	Default port used for communication with Microsoft SQL Server hosting a Veeam Backup Enterprise Manager database. For more information, see Specify Installation Settings. Additional ports may be needed depending on your configuration. For more information, see the Microsoft SQL Docs Configure the Windows Firewall to Allow SQL Server Access article.
	vCenter Server	TCP	443	Default port used for connection to a vCenter Server and deploying the Veeam Plug-in for vSphere web client. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.
	Active Directory Domain Controller	TCP, UDP	389	Port used by Enterprise Manager service to communicate with Active Directory over the LDAP protocol.
		TCP	636	Port used by Enterprise Manager service to communicate with Active Directory over the LDAPS (LDAP over TLS/SSL) protocol.
		TCP	3268	Port used by Enterprise Manager service to communicate with LDAP Global Catalog.
		TCP	3269	Port used by Enterprise Manager service to communicate with LDAP Global Catalog over TLS/SSL.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and later)	Ports used by Enterprise Manager service to communicate with Active Directory. These ports are also used during restore through Veeam Self-Service File Restore Portal. This is a default dynamic port range. For more information, see Microsoft Support KB 832017.

From	To	Protocol	Port	Notes
	Veeam License Update Server (vbr.butler.veeam.com, autolk.veeam.com)	TCP	443	Default port used for license auto-update.
Veeam Backup Enterprise Manager website (IIS extension)	Veeam Backup Enterprise Manager service	TCP	9394	Default port used by IIS extension to communicate with Veeam Backup Enterprise Manager. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.
Veeam Cloud Connect Portal website (IIS extension)	Veeam Backup Enterprise Manager service	TCP	9397	Default port used by IIS extension to communicate with Veeam Backup Enterprise Manager. This port value is built-in and cannot be customized during installation.
Browser	Veeam Backup Enterprise Manager website (IIS extension)	HTTP	9080	Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports. When you work with Veeam Self-Service Backup Portal (accessed by the portal URL or from the vCD environment) and vSphere Self-Service Backup Portal, your browser also communicates with the Veeam Backup Enterprise Manager website over this port.
		HTTPS	9443	
	Veeam Cloud Connect Portal website (IIS extension)	HTTPS	6443	Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.
		HTTP	9399	

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager REST API client and VMware vSphere web client plug-in	Veeam Backup Enterprise Manager REST API	HTTPS	9398	Default ports used to communicate with Veeam Backup Enterprise Manager REST API. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.
Veeam ONE Server (optional)	Veeam Backup Enterprise Manager	TCP	Dynamically assigned ports	If you use Veeam Availability Suite and add a Veeam Backup Enterprise Manager server to Veeam ONE monitoring scope, you must open ports required to gather data through WMI. For more information on enabling and disabling WMI traffic, see the Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection articles of the Microsoft Windows Dev Center.

NOTE

Consider the following:

- During installation, Veeam Backup & Replication automatically creates firewall rules for default ports to allow communication for the application components.
- For more information on Enterprise Manager network connectivity, refer to the Enterprise Manager article of the Veeam Backup and Replication Best Practices documentation.

Ports for Restore Operations

Guest OS File Restore (Windows)

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager	Mount server associated with backup repository	TCP	2500 to 6000	Ports used for file download.

Guest OS File Restore (non-Windows)

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager	Helper appliance	TCP	2500 to 6000	Ports used for file download. For more information on the helper appliance, see Preparing for File Search and Restore (non-Windows machines).

NOTE

Consider the following:

- For more information on the list of ports used by the mount server associated with the backup repository during file-level restore, see the Mount Server Connections section of the Veeam Backup & Replication User Guide.
- For more information on the list of ports used by the components involved in 1-Click Restore to Original Location, see the Used Ports section of the Veeam Backup & Replication User Guide.

SQL Server Database Restore

From	To	Protocol	Port	Notes
Target remote SQL Server	Mount server associated with backup repository	TCP	3260 to 3270	Ports used for transfer of iSCSI traffic during database restore to the original Microsoft SQL Server. These ports are used during the restore process only.

Oracle Database Restore (1-Click)

From	To	Protocol	Port	Notes
Target remote machine to which application items are restored	Machine running mount service[1]	TCP	3260 to 3270	Range of ports used by Veeam Backup and Replication for iSCSI traffic. Ports are open only during the application item restore session.

[1] Mount server associated with the repository (if restoring from backup), or a backup server (if restoring from replica).

NOTE

For more information on 1-Click Database Restore to the original Oracle server machine (remote machine), see 1-Click Restore to Original Location.

Oracle Database Restore (Custom Settings)

From	To	Protocol	Port	Notes
Machine running mount service[1]	Oracle on Windows server	TCP	49152 to 65535	Recommended dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see Microsoft Support KB 832017.
		TCP	1025 to 1034	Default port range for the runtime component installed on the guest machine to support restore operations in most scenarios. These ports are opened only during application item restore.
	Oracle on Linux server	TCP	22	Default SSH port used as a control channel.
		TCP	2500 to 5000	Default port range for data transmission.

[1] Mount server associated with the repository (if restoring from backup), or a backup server (if restoring from replica).

NOTE

For more information on the process of database restore with custom settings, see Restore with Custom Settings.

Licensing

The Veeam Backup & Replication infrastructure requires license instances to process backup and replication jobs.

When you run a job, Veeam Backup & Replication uses a number of instances required for each type of protected workloads (for per-instance licenses) or applies a license to the protected hosts (for per-socket license).

Veeam Backup Enterprise Manager collects information about the type of license installed on Veeam backup servers connected to it and the number of instances in the license. When Veeam Enterprise Manager replicates databases from backup servers, it also synchronizes license data: checks if the license installed on the Veeam backup server coincides with the license installed on the Veeam Backup Enterprise Manager server. If the licenses do not coincide, the license on the Veeam backup server is automatically updated with that on the Veeam Backup Enterprise Manager server.

Keep in mind that you cannot use the same Veeam Backup Enterprise Manager server to manage backup servers that require different licenses, for example, a backup server of a Veeam Cloud Connect service provider and a regular backup server used to process Veeam Backup & Replication jobs.

For example, you add to Veeam Backup Enterprise Manager a backup server with the Veeam Cloud Connect service provider license installed. Veeam Backup Enterprise Manager will obtain information about the license and save it to its database. If you then add another backup server with a different type of license installed, Veeam Backup Enterprise Manager will install the Veeam Cloud Connect service provider license on this backup server. As a result, you will be able to use the second backup server to configure the Veeam Cloud Connect infrastructure, and will not be able to use this server to run backup and replication jobs.

Using Veeam Backup Enterprise Manager to work with Veeam Backup & Replication licenses reduces administration overhead. You can manage and activate licenses for the entire backup infrastructure from a single web console. You can view what workloads consume instances in the license, install a new license, or revoke the license from protected workloads.

For information on Veeam Backup & Replication license types, see the Licensing section of the Veeam Backup & Replication User Guide.

For information on Veeam Cloud Connect license types and license management tasks, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

For more information on Veeam licensing, see Veeam Licensing Policy.

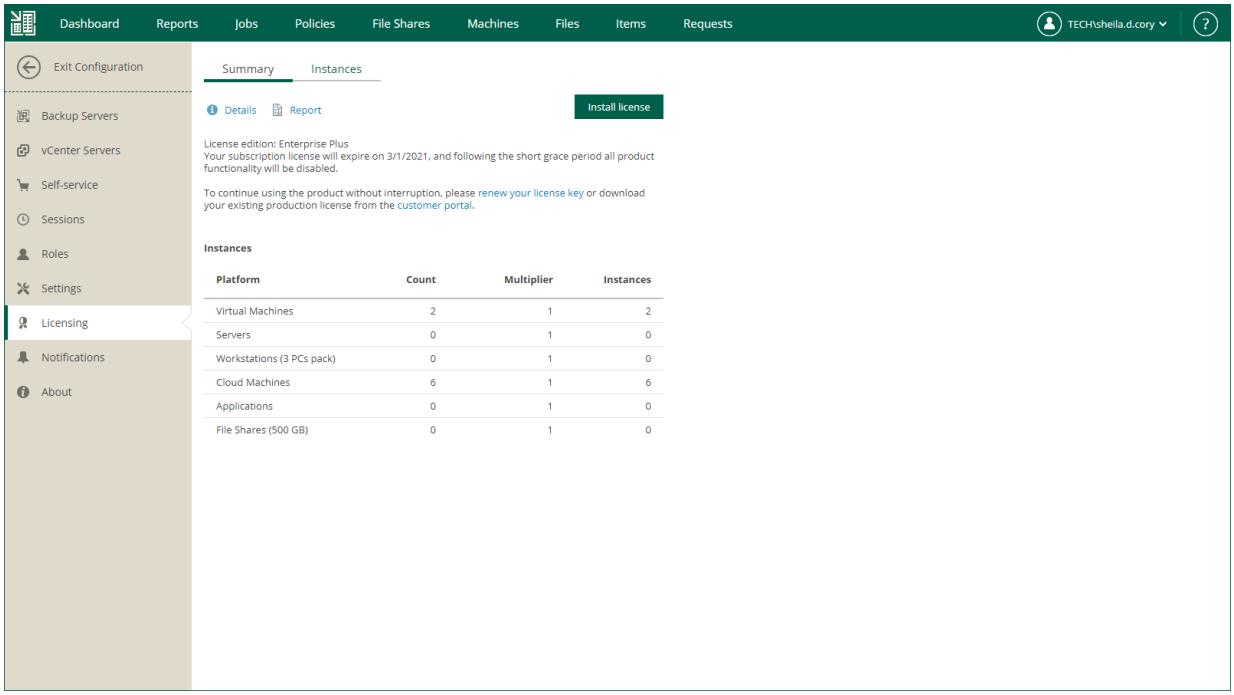
Installing License

You can install a new license on the Veeam Backup Enterprise Manager server. The new license is automatically applied to all backup servers connected to Enterprise Manager. This approach simplifies tracking license usage and license updates across multiple backup servers.

> **NOTE**
>
> Starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261), Veeam Backup Enterprise Manager applies its license to connected backup servers that have Veeam Backup & Replication version 10 or later installed.

To install a license:

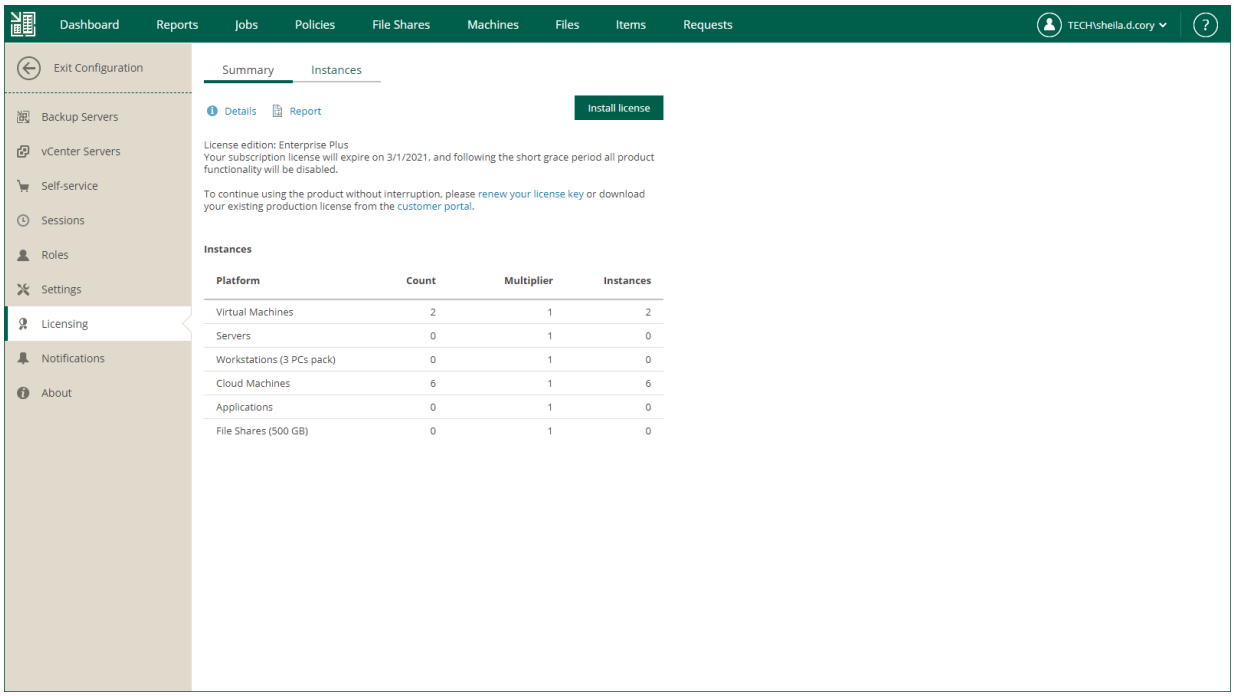
1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Install license**.
5. Select the necessary LIC file and click **Open**.



Viewing License Details

To view license details:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, open the **Licensing** section.



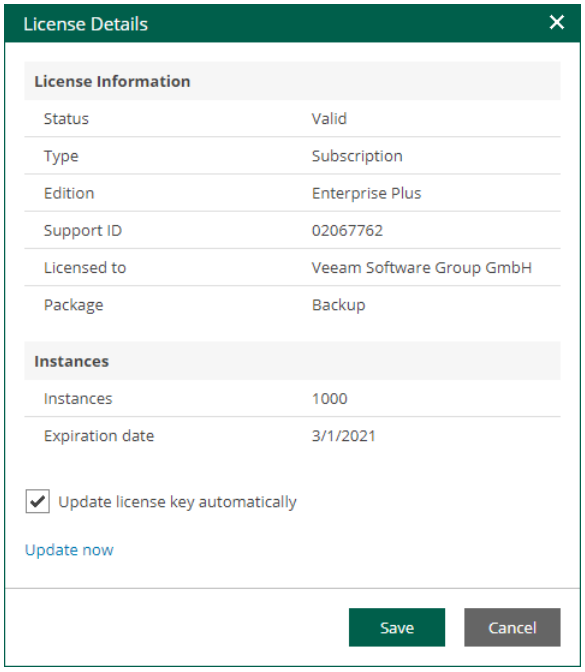
On the **Summary** tab of the **Licensing** section, you can find information about the license edition, license state and a spreadsheet of the available and used instances per each type of protected workloads: virtual machines, physical servers and workstations, cloud machines, applications and file shares.

Each type of workloads processed by Veeam Backup & Replication consumes a specific number of instances in the license. For more information on Veeam licensing, see Veeam Licensing Policy.

> **TIP**
>
> You can configure Veeam Backup Enterprise Manager to send notifications if your license expires. For more information on the Veeam Backup Enterprise Manager notification functionality, see the Configuring Notification Settings section of this guide.

> **NOTE**
>
> Veeam Backup Enterprise Manager does not display information about instances consumed in the Veeam Cloud Connect service provider license by tenant workloads. This information is available only in the Veeam backup console on the Veeam backup server of the service provider. For more information, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

To display detailed information about the current license, including license type, expiration date and the number of instances, click the **Details** link.



TIP

You can also view detailed information about current license usage. To do this, click the **Report** link.

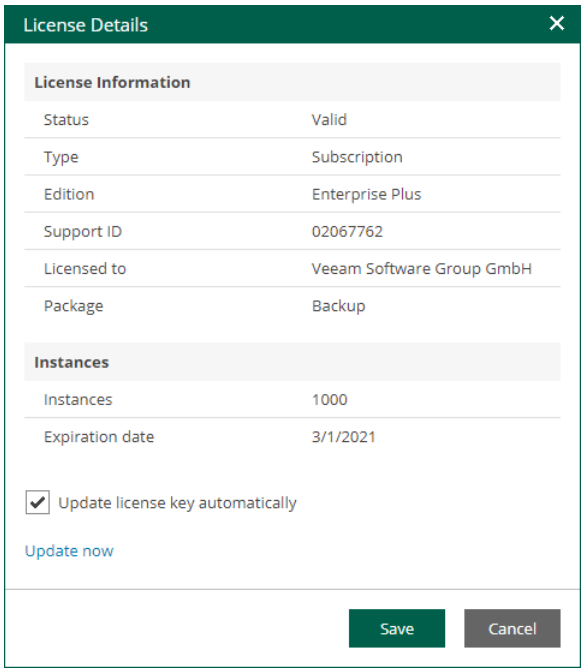
Updating License

Updating License Manually

You can update the license manually on demand. When you update the license manually, Veeam Backup Enterprise Manager connects to the Veeam License Update Server, downloads a new license from it (if the license is available) and installs it.

To update the license:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Details**.
5. Click the **Update now** link.



Updating License Automatically

You can instruct Veeam Backup Enterprise Manager to schedule automatic connection with Veeam License Update Server and periodically send requests for a new license. When the automatic update is enabled, Enterprise Manager requests a new license weekly, and 7 days before current license expiration date — daily.

To enable automatic update:

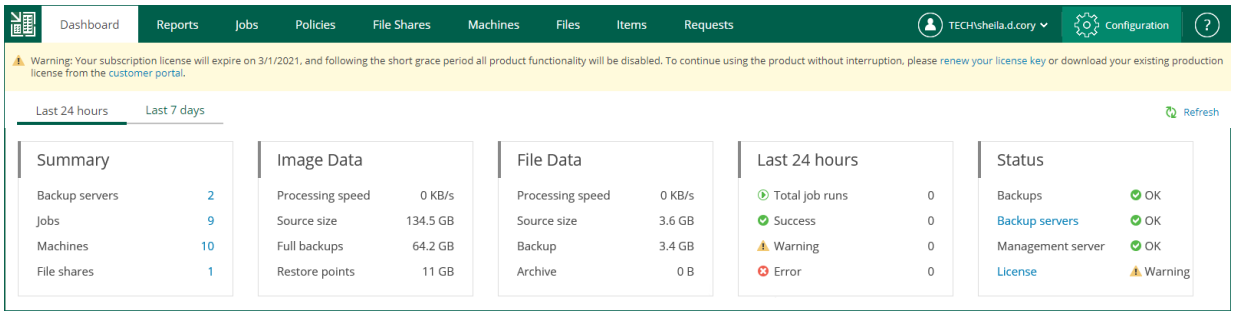
1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Details**.

5. In the **Details** window, select the **Update license key automatically** check box.

> **NOTE**
>
> If this option is enabled in Enterprise Manager (even if deactivated in the Veeam backup console), automatic update will be performed anyway: Enterprise Manager will obtain a new key from Veeam licensing server and propagate it to all managed Veeam backup servers.
>
> For information on license management in Veeam Backup and Replication, see the Licensing section of the Veeam Backup & Replication User Guide.
>
> For information on license management for Veeam Cloud Connect Server Providers, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

Grace Period

Veeam Backup Enterprise Manager supports a grace period after the license expiration date. For subscription license, it lasts for 30 days, for rental license — 2 months. During this period the product will be running, but a warning about license expiration (grace period) will appear in the main window and in the sessions information.



You must update your license before the end of the grace period.

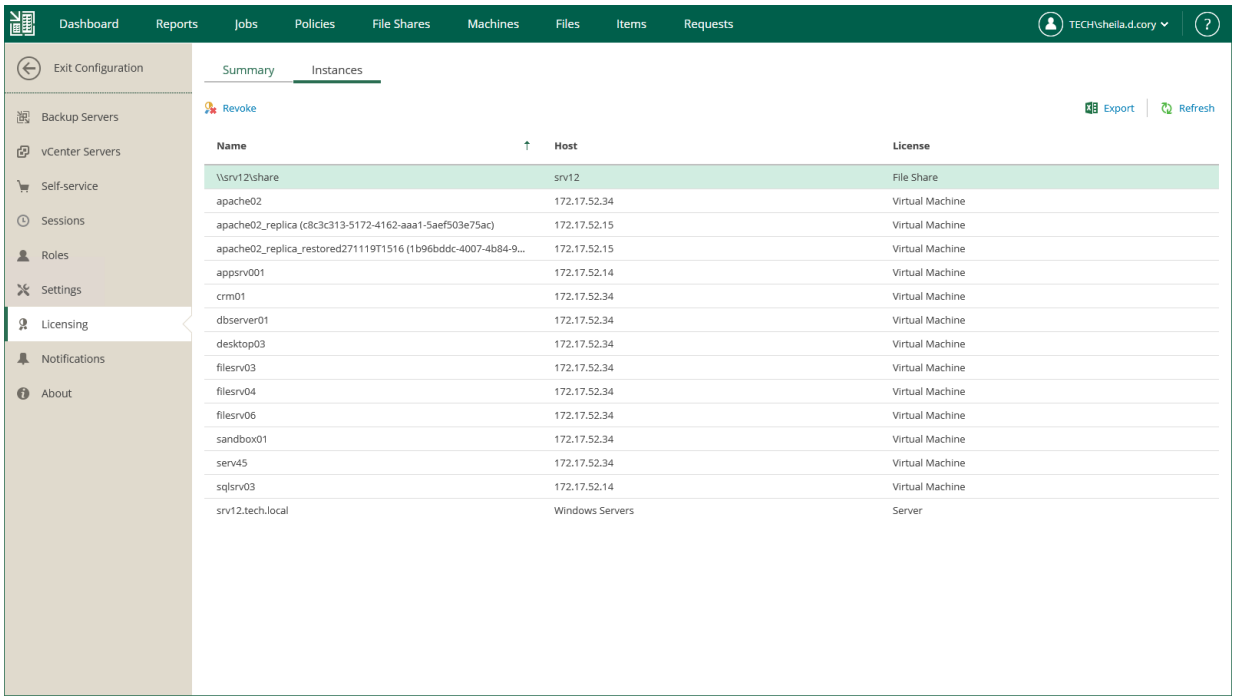
Messages that can appear in the automatic license update session log are listed in the Appendix A. Similar messages are received as pop-ups after you force the immediate update.

Revoking License

You can use Enterprise Manager to revoke instances from machines — that is, reclaim the instance used for a machine to apply it to another machine.

To revoke the license:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, open the **Licensing** section.
4. Select the **Instances** tab.
5. Select the required object in the list and click **Revoke**.



Managing Monthly Usage Reports

Veeam Cloud & Service Provides (VCSPs) who have a rental license installed in Veeam Backup Enterprise Manager must monthly submit a license usage report from Enterprise Manager.

Veeam offers two methods of usage reporting: automatic and manual. The automatic reporting is used if automatic license update is enabled. For more information about how license usage reporting works, see the License Usage Reporting section of the Veeam Cloud Connect Guide.

Veeam Backup Enterprise Manager generates a monthly usage report on the first day of the month. The report is based on the number of instances used for backup and replication in the previous month.

Reviewing Monthly Usage Report

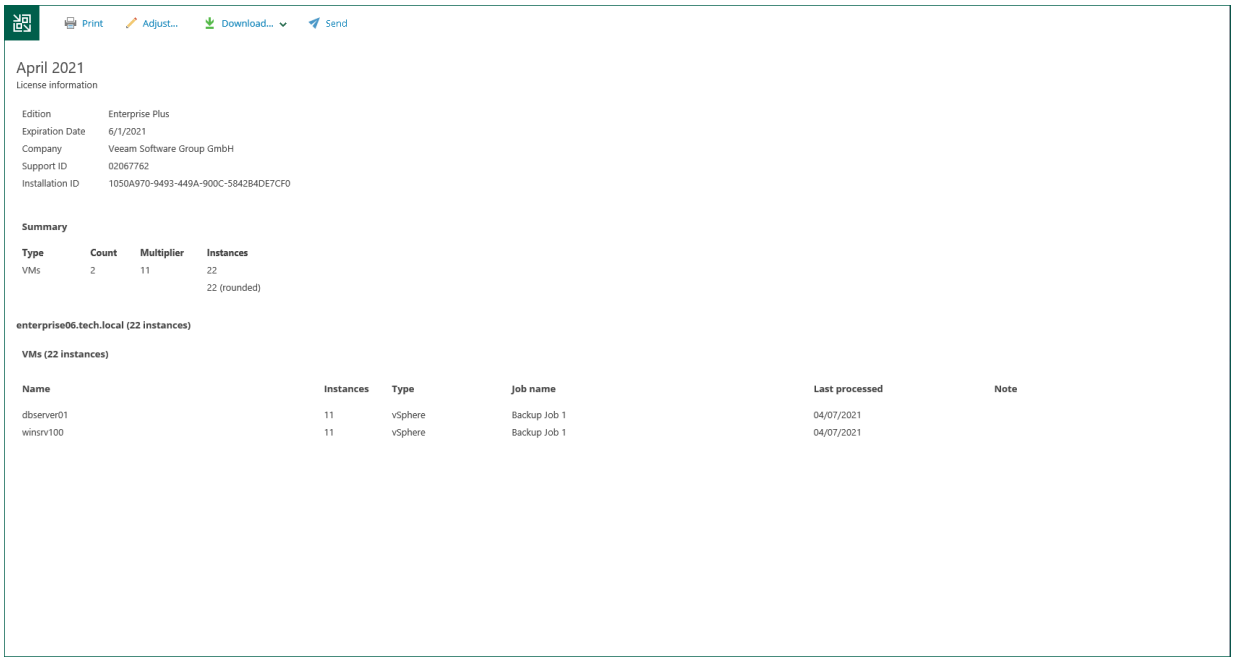
You can review a monthly usage report before sending it to Veeam.

To review a report:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, click **Review**.
3. In the monthly usage report, check the number of reported instances. The report contains the following data:
   - License information: Veeam Backup & Replication edition, license expiration date, name of the company to which the license was issued and support ID.
   - The number of instances used by each type of protected workloads (VMs, workstations, servers and file shares) and the total number of used instances.
   - For each type of protected workloads, the report displays information about processed workloads and jobs that process these workloads.
   - For each type of protected workloads, the report also displays the number of new objects that are not included in the report.

On the report page, you can perform the following actions:

- Print the report
- Adjust the number of processed VMs in the report
- Download the report
- [For automatic reporting] Submit the report



Adjusting Monthly Usage Report

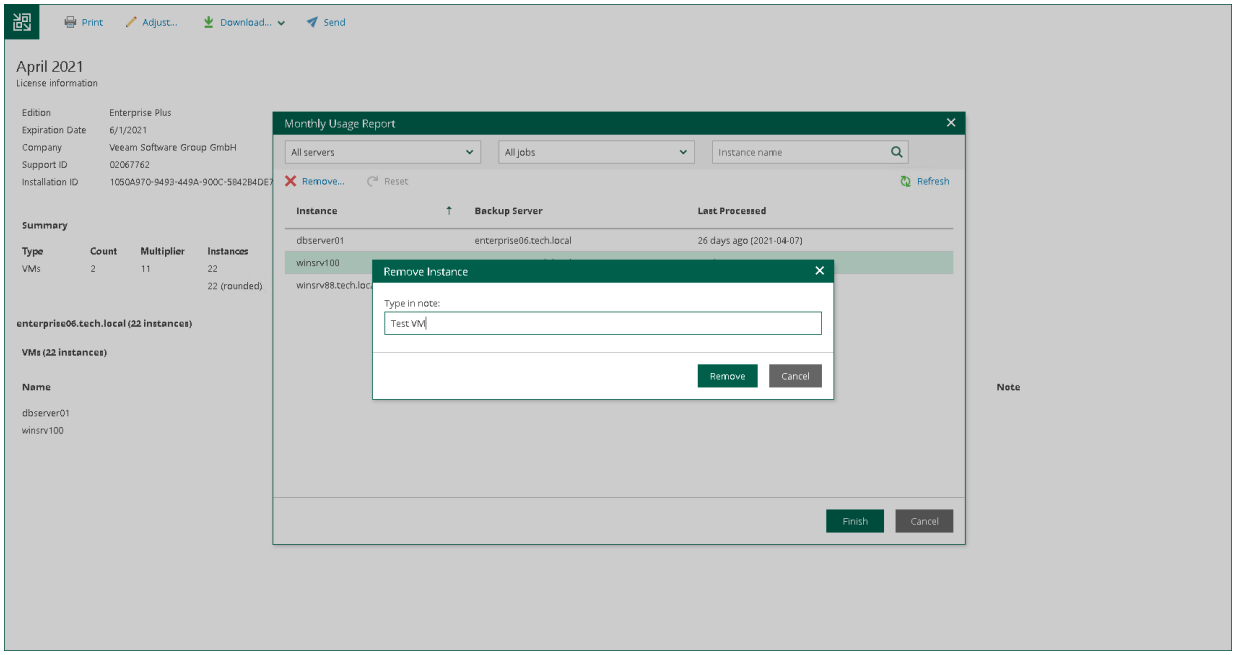
You can remove specific VMs from a monthly usage report. For every VM removal, you must specify a reason.

To adjust a report:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, click **Review**.
3. On the report page, click **Adjust**.
4. In the list of VMs, select the VM that you want to remove from the report and click **Remove**.

   By default, the list of VMs contains all managed VMs included in the report. To quickly find the necessary VM, you can use the search field at the top of the window. You can also select a backup server and job from the drop-down lists to view a list of VMs added to a specific job on a specific backup server.
5. In the **Remove Instance** window, in the **Type in note** field, provide a reason for removing the VM from the report.
6. Click **OK**, then click **Finish**. The change will be reflected in the report.

> **TIP**
>
> To reset changes introduced in the report, in the **Monthly Usage Report** window, click **Reset**.



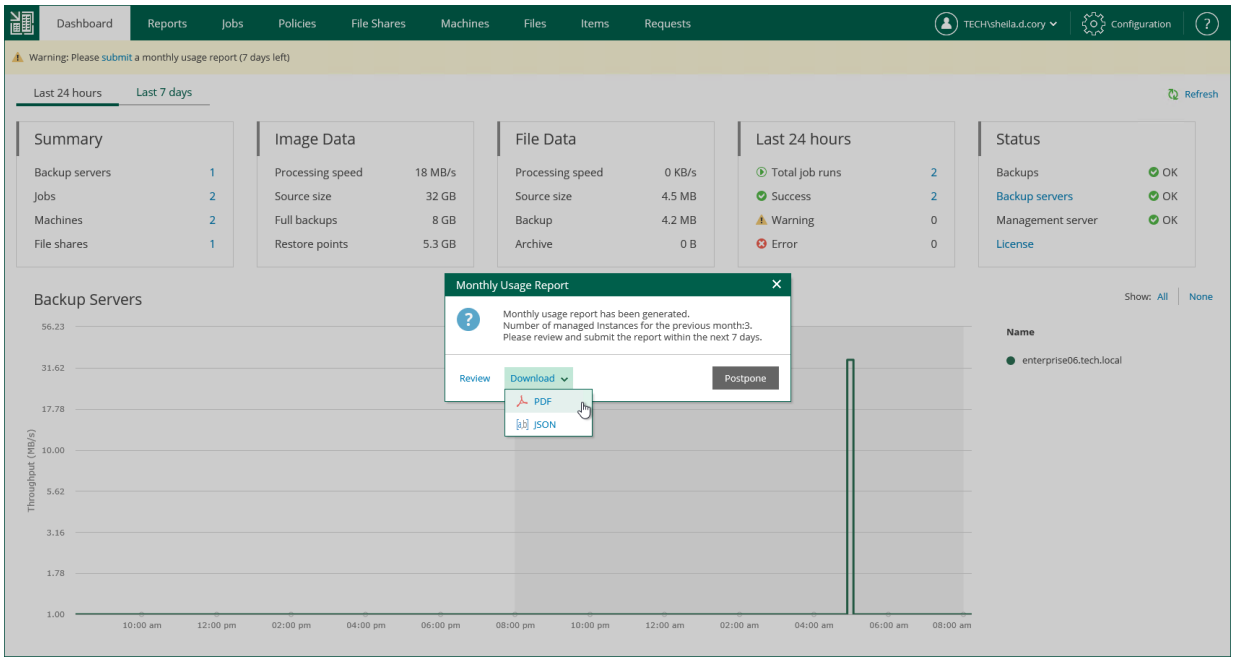
Downloading Monthly Usage Report

You can download a monthly usage report as a PDF or JSON file.

To download a monthly usage report:

1. In the monthly usage report notification, click the **submit** link.
2. Download the report. The procedure differs depending on the reporting method. For more information, see the License Usage Reporting section of the Veeam Cloud Connect Guide.
   - In case of automatic reporting, do the following:
     i. In the **Monthly Usage Report** window, click **Review**.
     ii. On the report page, click **Download** and select the report format: *PDF* or *JSON*.
   - In case of manual reporting, in the **Monthly Usage Report** window, click **Download** and select the report format: *PDF* or *JSON*.

     You can also download the report after review. To do this, take the same steps as in case of automatic reporting.



Submitting Monthly Usage Report

On the first day of the month, Veeam Backup Enterprise Manager shows a warning on the **Dashboard** tab. The warning prompts to submit a monthly usage report and informs on the number of days within which the report must be submitted.

You can submit a monthly usage report in one of the following ways:

- Automatically
- Manually

For more information about how license usage reporting works, see the License Usage Reporting section of the Veeam Cloud Connect Guide.

Submitting Report Automatically

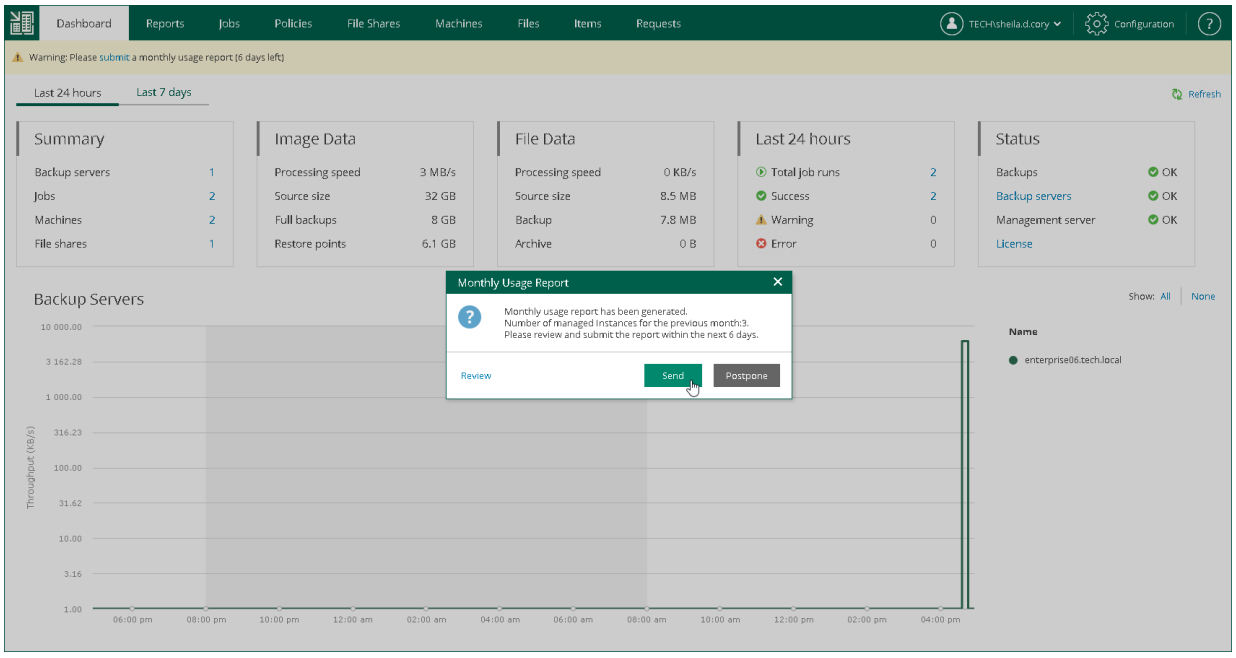
Automatic report submission allows you to send the report to Veeam directly from Veeam Backup Enterprise Manager. If you do not submit the report within 10 days, Veeam Backup Enterprise Manager sends the report on the eleventh day of the month.

To submit a monthly usage report automatically:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, to check or change the number of used instances, click **Review**.

   For more information, see Reviewing Monthly Usage Report and Adjusting Monthly Usage Report.
3. To submit the report, click **Send**.

   You can also postpone the report submission. To do this, click **Postpone**. In this case, Veeam Backup Enterprise Manager closes the **Monthly Usage Report** window. Until the report is sent to Veeam, on the **Dashboard** tab, Enterprise Manager keeps displaying a warning prompting to submit the report.



Submitting Report Manually

You must send the report before the day defined by the agreement with Veeam or your Aggregator (if any is involved). The default day is the tenth day of the month.

To submit a monthly usage report manually:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, to check or change the number of used instances, click **Review**. For more information, see Reviewing Monthly Usage Report and Adjusting Monthly Usage Report.
3. To download the report, click **Download**.

   You can also postpone the report submission. To do this, click **Postpone**. In this case, Veeam Backup Enterprise Manager closes the **Monthly Usage Report** window. Until the report is sent to Veeam, on the **Dashboard** tab, Enterprise Manager keeps displaying a warning prompting to submit the report.
4. Send the downloaded report to Veeam.

Deployment

To start working with Veeam Backup Enterprise Manager, you must install Veeam Backup Enterprise Manager components on a machine that meets the system requirements. To do this, you can use the setup wizard or install the product in the unattended mode.

You can install Veeam Backup Enterprise Manager either on a physical or virtual machine, co-install it with Veeam Backup & Replication or install it separately.

Installing Veeam Backup Enterprise Manager

Before you install Veeam Backup Enterprise Manager, check prerequisites. Then use the **Veeam Backup Enterprise Manager** setup wizard to install the product.

1. Start the setup wizard.
2. Read and accept the license agreement.
3. Provide a license file.
4. Review components and select an installation folder.
5. Install missing software.
6. Specify installation settings.
7. Specify service account settings.
8. Select Microsoft SQL Server.
9. Specify service ports.
10. Specify data locations.
11. Begin installation.

For more information on Veeam Backup Enterprise Manager installation in unattended mode, see the *Veeam Backup Enterprise Manager Server* subsection of the Installing Veeam Backup & Replication in Unattended Mode section of the Veeam Backup & Replication User Guide.

Before You Begin

Before you install Veeam Backup Enterprise Manager, check the following prerequisites:

- A machine on which you plan to install Veeam Backup Enterprise Manager must meet the system requirements. For more information, see System Requirements.
- A user account that you plan to use for installation must have sufficient permissions. For more information, see Required Permissions.
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see Used Ports.
- .NET 3.5.1 WCF HTTP Activation Windows component prevents Veeam Backup Enterprise Manager from functioning. Make sure there is no .NET 3.5.1 WCF HTTP Activation Windows component on the Veeam Backup Enterprise Manager server prior to the installation.
- Local antivirus or antimalware software can interfere with Veeam Backup Enterprise Manager installation and upgrade. If you receive the *"Failed to create website 0x80070020"* message, disable your local antivirus or antimalware software and run the installation process again. You can re-enable your antivirus software once the installation process completes. For more information, see this Veeam KB article.
- Check the *Known Issues* section of the Veeam Backup & Replication 11 Release Notes.

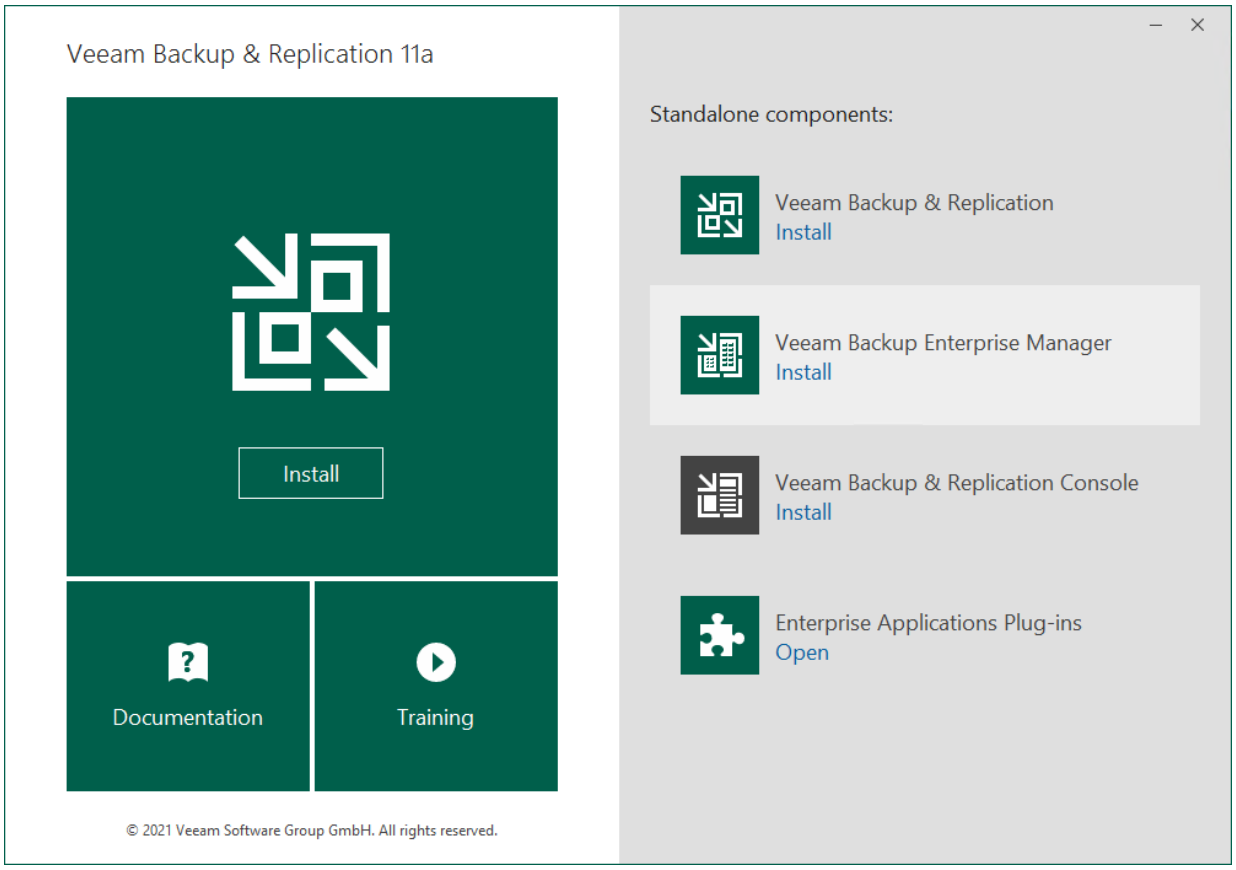
Step 1. Start Setup Wizard

To start the setup wizard:

1. Download the latest version of the Veeam Backup & Replication installation image from https://www.veeam.com/downloads.html.
2. Use disk image emulation software to mount the installation image to the machine where you plan to install Veeam Backup Enterprise Manager or burn the image file to a blank CD/DVD. If you plan to install Veeam Backup Enterprise Manager on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM. To extract the content of the ISO, you can also use the latest versions of utilities that can properly extract data from ISOs of large size and can properly work with long file paths.
3. After you mount the image or insert the disk, Autorun will open a splash screen with installation options. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. In the **Standalone components** section of the splash screen, click **Install** Veeam Backup Enterprise Manager.
5. Before installing the product, the setup will analyze the prerequisites and prompt to install .NET Framework if it is missing on the machine. Click **OK** to install this component. After you install the component, you will have to reboot your computer.

IMPORTANT

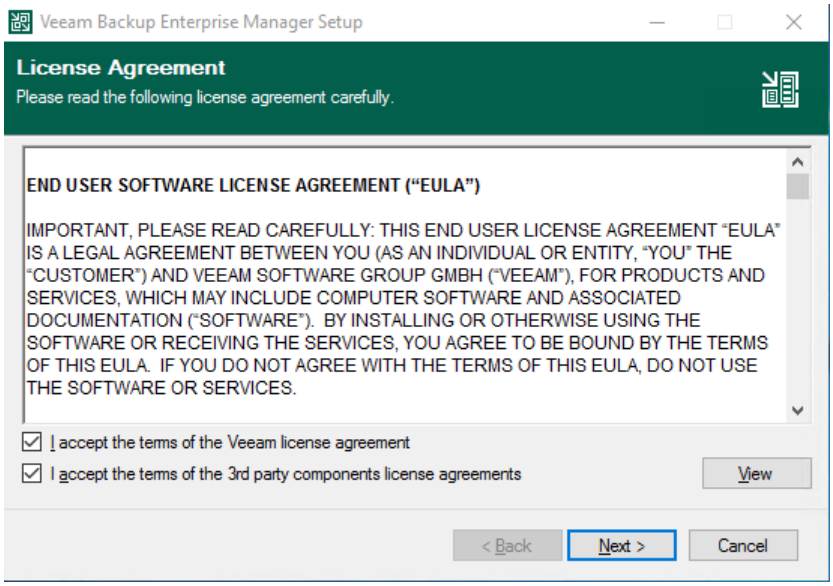
It is strongly recommended that you install Veeam Backup Enterprise Manager using Autorun or the `Setup.exe` file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup Enterprise Manager may not work as expected.



Step 2. Read and Accept License Agreement

At the **License Agreement** step of the wizard, you must accept the license agreement for Veeam and 3rd party components that Veeam incorporates. If you do not accept the license agreements, you will not be able to pass to next step of the setup wizard.

1. Read the license agreement. To view the license agreement for 3rd party components, click **View**.
2. Select the **I accept the terms of the Veeam license agreement** check box.
3. Select the **I accept the terms of the 3rd party components license agreements** check box.



Step 3. Provide License File

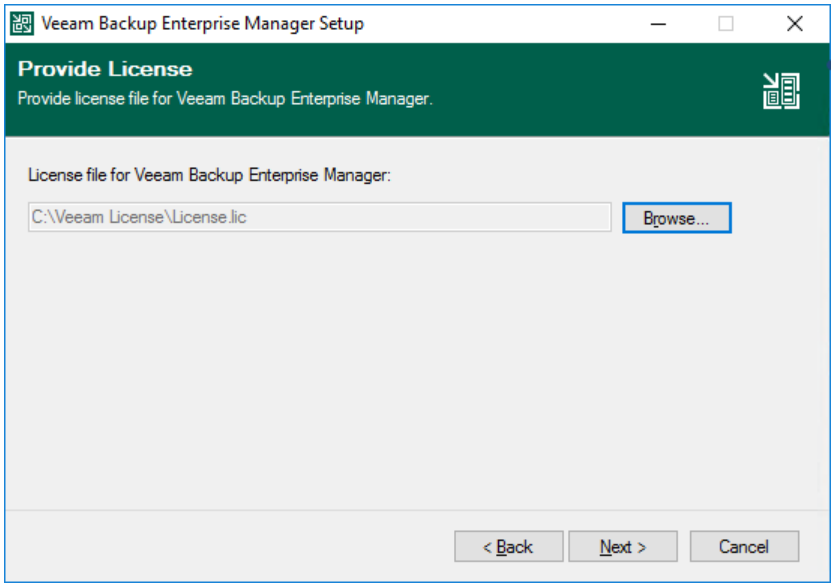
At the **Provide License** step of the wizard, you must specify what license for Veeam Backup Enterprise Manager you want to install. You can install the following types of licenses:

- Trial license that was sent to you after you downloaded the product.
- Purchased full license.

If a valid license is already installed on the machine, the setup wizard will inform you about it. In this case, you can skip the **Provide License** step and move to the next step of the wizard.

To install a license:

1. Next to the **License file for Veeam Backup Enterprise Manager** field, click **Browse**.
2. Select a valid license file for Veeam Backup Enterprise Manager.



Step 4. Review Components and Select Installation Folder

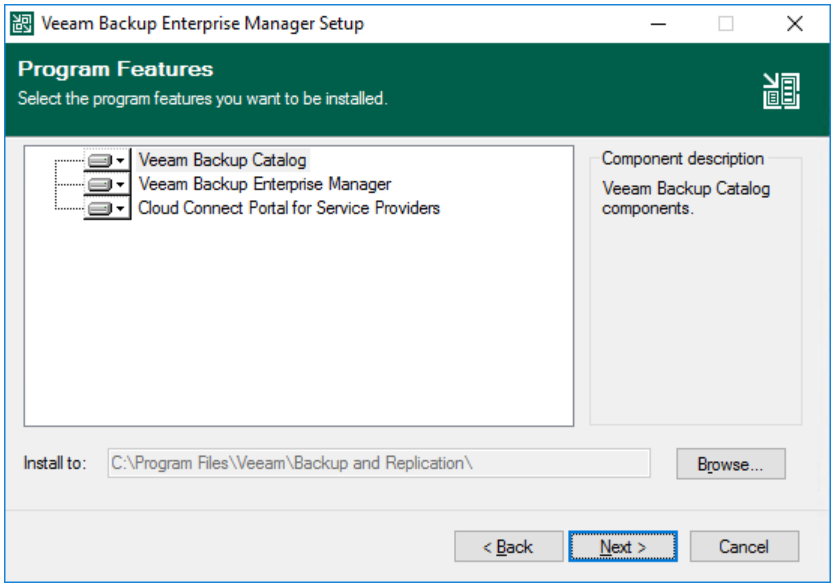
At the **Program features** step of the wizard, you can select what Enterprise Manager components to install on the machine and specify the installation folder.

Selecting Components

For on-site deployments, the setup wizard offers the following components:

- Veeam Backup Enterprise Manager
- Veeam Backup Catalog

Service providers can also install Veeam Cloud Connect Portal. For more information on Veeam Cloud Connect Portal, see the Veeam Cloud Connect Guide.



To choose components to install:

1. Click the hard drive icon next to a component.
2. Select the **This feature will be installed on local hard drive** option.

If the *Veeam Backup Catalog* or *Cloud Connect Portal for Service Providers* component is already installed, the setup will exclude it from the list of components to install.

The setup wizard also installs components in the background. For more information on the installed components, see Enterprise Manager Components.

Selecting Installation Folder

To choose the installation folder:

1. On the right of the **Install to** field, click **Browse**.
2. In the **Browse for Folder** window, select the installation folder for the product. The default installation folder is `%ProgramFiles%\Veeam\Backup and Replication`.

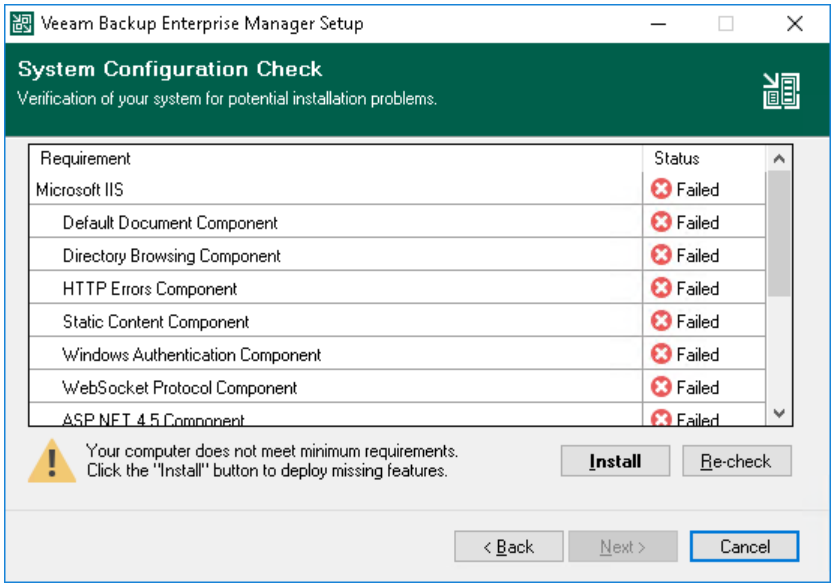
Step 5. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup wizard checks if all prerequisite software is installed on the machine. If required software components are missing, the setup wizard will offer you to install them.

You can install missing components automatically or manually.

- To install missing components automatically, click **Install**. The setup wizard will not interrupt the installation process and install the missing components during the current work session.
- To install missing components manually:
  a. Click **Cancel** and exit the setup wizard.
  b. Install and enable the necessary components manually on the machine.
  c. Start the setup wizard again, pass to the **System Configuration Check** step of the wizard and click **Re-run** to repeat the verification.

> **NOTE**
>
> If all required components are already installed on the machine, the **System Configuration Check** step will be skipped. For more information on the necessary software, see System Requirements.



Step 6. Specify Installation Settings

At the **Default Configuration** step of the wizard, you can select to install Veeam Backup Enterprise Manager with default installation settings or specify custom installation settings.

By default, the setup wizard installs Veeam Backup Enterprise Manager with the following settings:

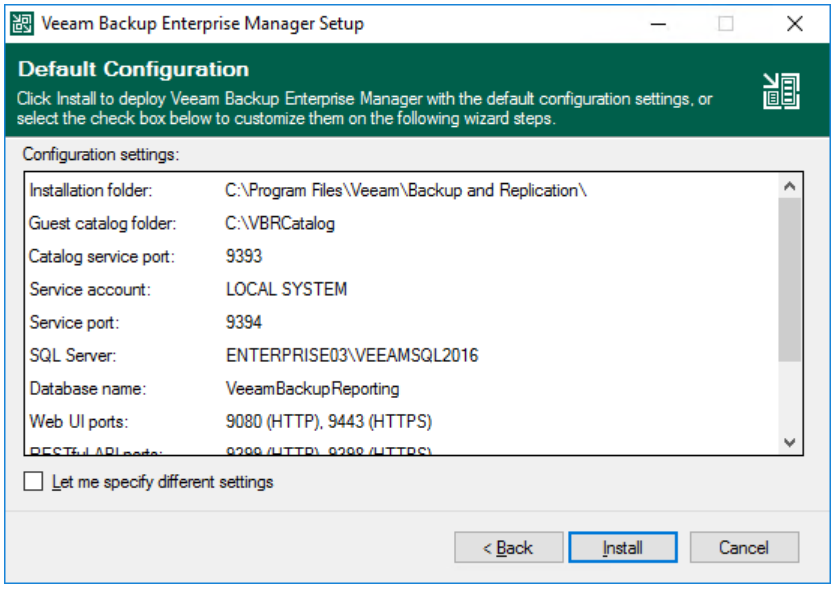
- **Installation folder**: `C:\Program Files\Veeam\Backup and Replication`.
- **Guest catalog folder**: the VBRCatalog folder on a volume with the maximum amount of free space, for example, `C:\VBRCatalog`.

  The guest catalog folder stores indexing data for VM guest OS files. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore.
- **Catalog service port**: *9393*. The catalog service port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager.
- **Service account**: *LOCAL SYSTEM*. The service account is the account under which the Veeam Backup Enterprise Manager runs.
- **Service port**: *9394*. The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers.
- **SQL Server**: *LOCALHOST\VEEAMSQL2012* or *LOCALHOST\VEEAMSQL2016*. During installation, the Veeam Backup Enterprise Manager setup installs a new instance of Microsoft SQL Server locally on the backup server:
  - For machines running Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup installs Microsoft SQL Server 2012 SP3 Express Edition.
  - For machines running Microsoft Windows Server 2012 and later, the setup installs Microsoft SQL Server 2016 SP2 Express Edition.
- **Database name**: *VeeamBackupReporting*. Veeam Backup Enterprise Manager deploys the Veeam Backup Enterprise Manager configuration database on the locally installed instance of Microsoft SQL Server.
- **Web UI ports**: *9080* (for HTTP protocol) and *9443* (for HTTPS protocol). These ports are used for accessing Veeam Backup Enterprise Manager web interface.
- **REST API ports**: *9399* (for HTTP protocol) and *9398* (for HTTPS protocol). These ports are used for accessing Veeam Backup Enterprise Manager REST API.
- **Cloud Connect Portal port**: *6443*. This port is used for accessing Veeam Cloud Connect Portal by tenants.

To use default installation settings:

1. Leave the **Let me specify different settings** check box not selected.
2. Click **Install**. The installation process will begin.

To use custom installation settings, select the **Let me specify different settings** check box. The setup wizard will include additional steps that will let you configure installation settings.



Step 7. Specify Service Account Settings

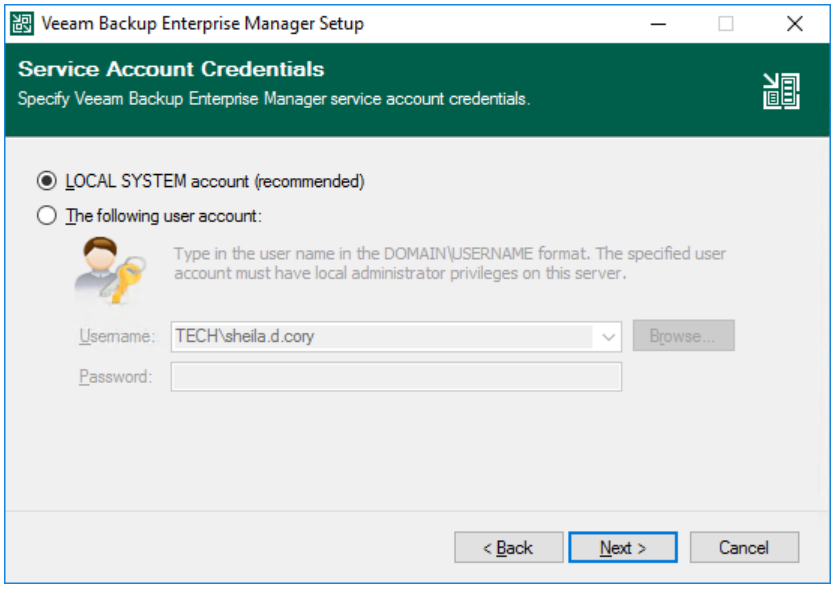
The **Service Account Credentials** step of the wizard is available if you have selected to configure installation settings manually.

You can select an account under which you want to run the Veeam Backup Enterprise Manager Service:

- LOCAL SYSTEM account (recommended, used by default)
- Another user account

The user name of the custom account must be specified in the *DOMAIN|USERNAME* format.

> **NOTE**
>
> The user account must have **Veeam Backup Enterprise Manager service account** permissions to run the Veeam Backup Enterprise Manager Service. For more information, see Required Permissions.



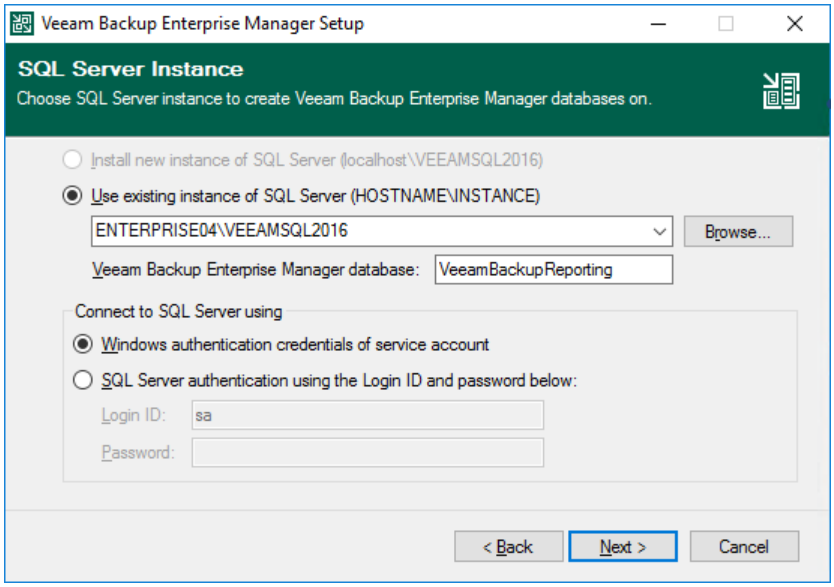
Step 8. Select Microsoft SQL Server

The **SQL Server Instance** step of the wizard is available if you have selected to configure installation settings manually.

You can select a Microsoft SQL Server on which you want to deploy the configuration database, and choose the authentication mode.

1. Select a Microsoft SQL Server:
   - If a Microsoft SQL Server is not installed locally or remotely, select the **Install new instance of SQL Server** option. The setup will install Microsoft SQL Server locally on the backup server:
     - For machines running Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup will install Microsoft SQL Server 2012 SP3 Express Edition.
     - For machines running Microsoft Windows Server 2012 and later, the setup will install Microsoft SQL Server 2016 SP2 Express Edition.
   - If a Microsoft SQL Server is already installed locally or remotely, select the **Use existing instance of SQL Server** option. Enter the instance name in the *HOSTNAME\INSTANCE* format. In the **Database** field, specify a name for the Veeam Backup Enterprise Manager configuration database.
2. Select an authentication mode to connect to the Microsoft SQL Server instance: Microsoft Windows authentication or Microsoft SQL Server authentication. If you select the SQL Server authentication, enter credentials for the Microsoft SQL Server account.

If the configuration database already exists on the Microsoft SQL Server (for example, it was created by a previous installation of Veeam Backup Enterprise Manager), the setup wizard will notify about it. To connect to the detected database, click **Yes**. If necessary, Veeam Backup Enterprise Manager will automatically upgrade the database to the latest version.



Step 9. Specify Service Ports

The **Additional Configuration** step of the wizard is available if you have selected to configure installation settings manually.

You can customize port number values that will be used for communication between backup infrastructure components.

> **NOTE**
>
> For more information about Veeam Backup Enterprise Manager used ports, see Used Ports.

Provide HTTP and HTTPS port numbers and select the certificate to be used by Veeam Backup Enterprise Manager. This certificate is needed to establish secure communication with the Enterprise Manager website using HTTPS (default port *9443*); Veeam plug-in for vSphere Web Client and RestAPI client also will use this certificate to receive data using HTTPS protocol.

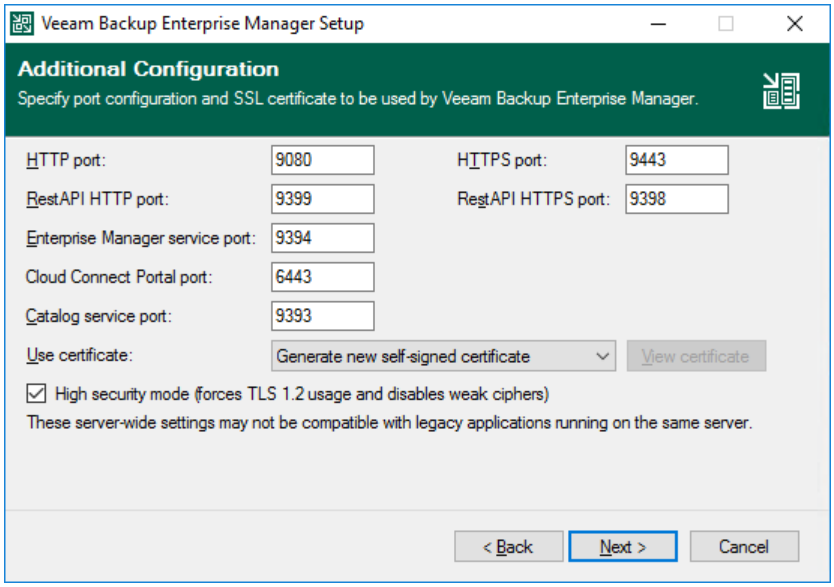
If the setup wizard does not find an appropriate certificate to be used, it generates a self-signed certificate.

Click **View certificate** to review the details of the selected certificate.

To enforce TLS 1.2 encryption protocol for network connections, select the **High security mode** check box.

> **NOTE**
>
> The **High security mode** option disables using weak ciphers for all communications with the machine on which Veeam Backup Enterprise Manager runs. This may interfere with the operation of 3rd party software installed on the same machine.

If you are installing Veeam Cloud Connect Portal, you can also provide port number that will be used by browser to access its website (default port is **6443**).

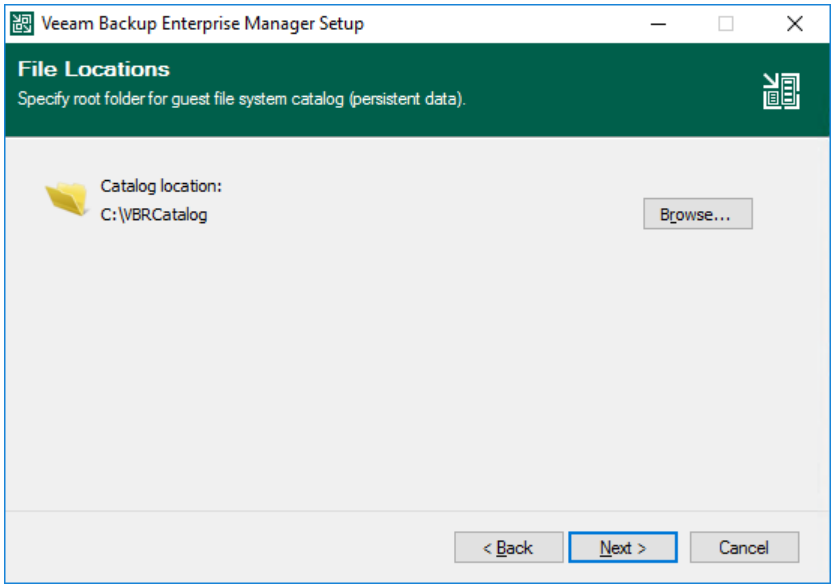


Step 10. Specify File Locations

The **File Locations** step is available if you have selected to install Veeam Backup Catalog at the Program features step of the wizard and to configure installation settings manually at the Default Configuration step of the wizard.

You can specify location for the guest file system catalog folder. Specify a path to the folder where index files must be stored.

By default, the setup wizard creates the *VBRCatalog* folder on a volume with the maximum amount of free space, for example: `C:\VBRCatalog`. To change the location, click **Browse**.

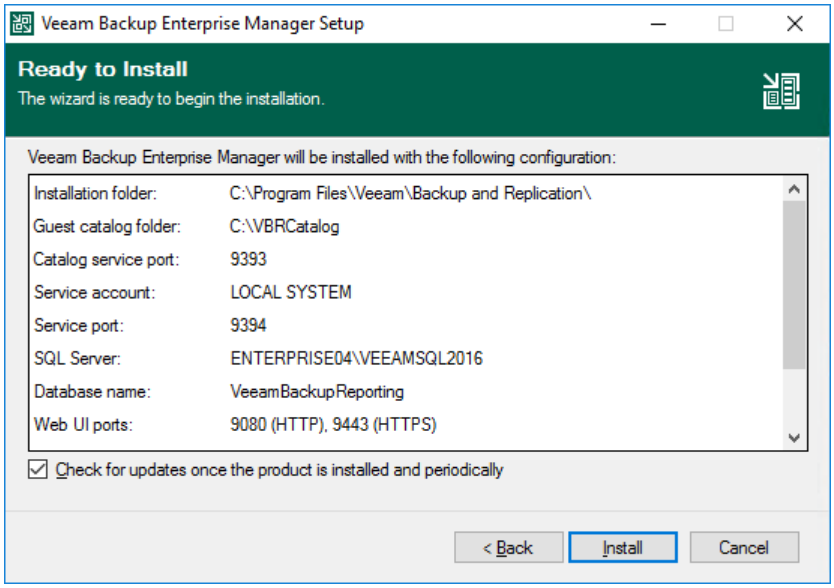


Step 11. Begin Installation

The **Ready to Install** step of the wizard is available if you have selected to configure installation settings manually.

You can review the Veeam Backup Enterprise Manager installation settings and start the installation process:

1. Click **Install** to begin the installation.
2. Wait for the installation process to complete and click **Finish** to exit the setup wizard.



Maintaining Veeam Backup Enterprise Manager

You can repair your installation of Veeam Backup Enterprise Manager. To do this:

1. Start the setup wizard on the Veeam Backup Enterprise Manager server. For more information, see Start Setup Wizard.
2. Read and accept the License Agreement. For more information, see Read and Accept License Agreement.
3. At the **Maintenance Mode** step of the setup wizard, select the **Repair** option and click **Next**.
4. Specify the service account credentials that will be used during the Veeam Backup Enterprise Manager repair. For more information, see Specify Service Account Settings.
5. At the **Ready to Install** step of the **Setup Wizard** check the installation prerequisites and click **Install**.

The setup wizard will re-install the Veeam Backup Enterprise Manager components. Wait for the installation process to complete and click **Finish** to exit the setup wizard.

Upgrading Veeam Backup Enterprise Manager

Before You Start Upgrade

Upgrade of Veeam Backup Enterprise Manager to version 11 is supported for version 9.5 Update 4b (build 9.5.4.2866) and later. To upgrade from earlier versions, contact Veeam Customer Support.

> **NOTE**
>
> Starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261), Veeam Backup Enterprise Manager applies its license to connected backup servers that have Veeam Backup & Replication version 10 or later installed.

Before starting the upgrade procedure, read and follow the recommendations below:

1. With Veeam Backup Enterprise Manager and connected Veeam backup servers, remember to begin the backup infrastructure upgrade process with Veeam Backup Enterprise Manager. Backup servers should be upgraded after that. If you have Veeam backup server installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server.
2. It is recommended to disable local antivirus and antimalware software to prevent it from interfering with Veeam Backup Enterprise Manager setup. You can enable it after the upgrade procedure is completed. For more information, see this Veeam KB article.
3. Ensure there is no active processes, such as running jobs and restore sessions. We recommend that you do not stop running jobs and let them complete successfully instead. Disable any periodic and backup copy jobs, so that they do not start during upgrade.
4. Perform backup of the SQL Server configuration databases used by Veeam backup servers and Veeam Backup Enterprise Manager server, so that you can easily go back to a previous version in case of issues with upgrade. Note that built-in configuration backup functionality does not protect Veeam Backup Enterprise Manager configuration.

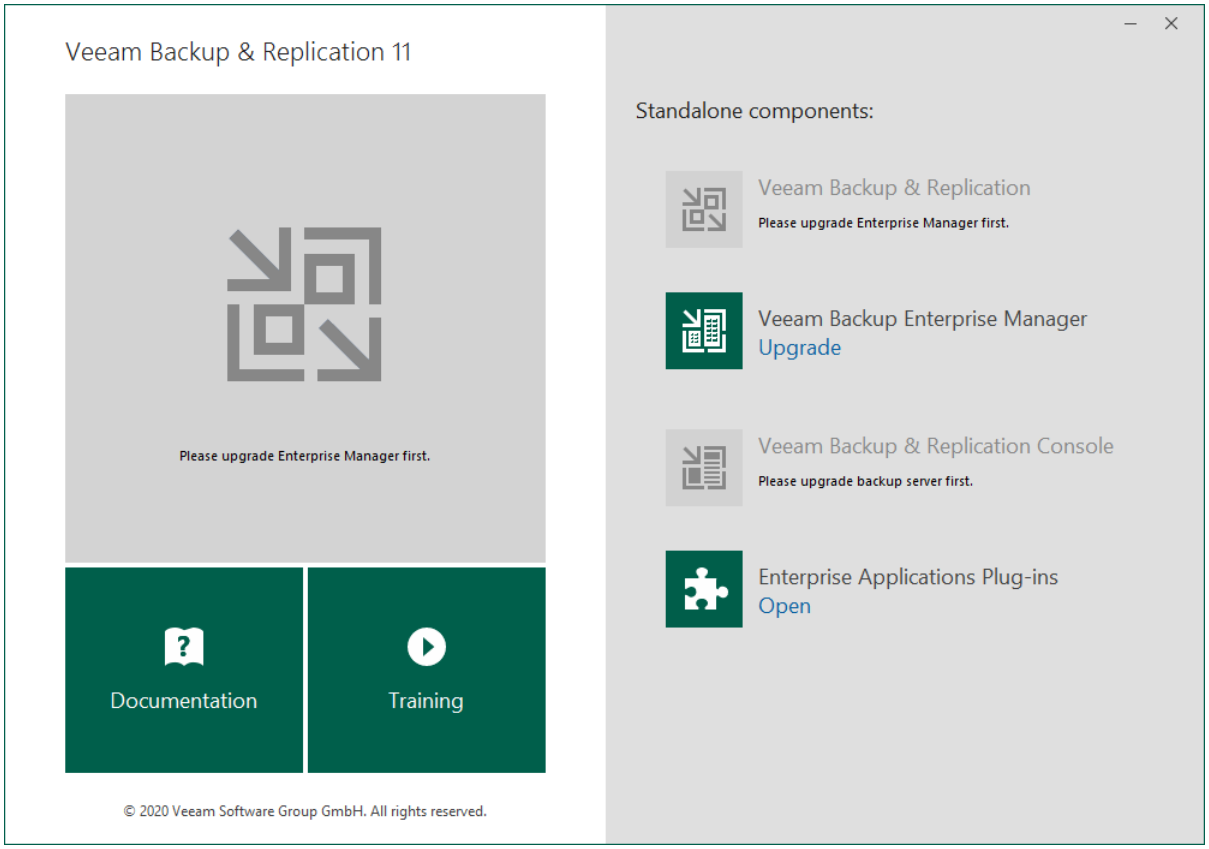
Upgrade Procedure

To upgrade Veeam Backup Enterprise Manager, take the following steps:

1. Download the latest version of Veeam Backup & Replication ISO from the Veeam website.
2. Mount the product ISO and use autorun, or run the `Setup.exe` file.
3. Click **Upgrade Veeam Backup Enterprise Manager**.
4. Follow the setup wizard steps. At the **SQL Server Instance** step, select the SQL server instance and database that were used by the previous version of Veeam Backup Enterprise Manager.
5. If you have Veeam Backup & Replication installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server, otherwise this local backup server will not be able to run jobs.
6. Proceed with upgrade of your Veeam backup servers.

> **IMPORTANT**
>
> After you upgrade Veeam Backup & Replication servers, Veeam Backup Enterprise Manager starts maintenance jobs to optimize the state of its database. The initial maintenance jobs session may take significant amount of time (up to an hour, depending on the database size). After the job finishes, the database will be brought to an optimal state, and subsequent maintenance job sessions will take much less time.

7. New features of Veeam Backup Enterprise Manager version 11 will be available after all managed Veeam backup servers are upgraded, and initial collection of data from these servers in Veeam Backup Enterprise Manager completes successfully.
8. Download and install the latest available update (if any) from https://www.veeam.com/updates.html.

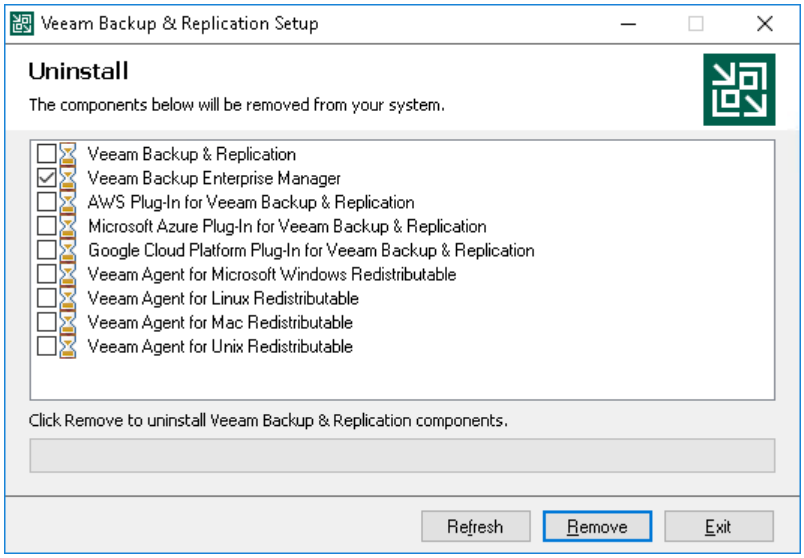


Uninstalling Veeam Backup Enterprise Manager

To uninstall Veeam Backup Enterprise Manager:

1. From the **Start** menu, select **Control Panel** > **Programs and Features**.
2. In the programs list, right-click **Veeam Backup & Replication** and select **Uninstall**.
3. In the **Uninstall** window, make sure the check box next to Veeam Backup Enterprise Manager is selected. If this component is co-installed with the Veeam Backup & Replication server, make sure the check box next to Veeam Backup & Replication is cleared. Click **Remove** and wait for the process to complete.

The Veeam Backup Enterprise Manager configuration database (default name is *VeeamBackupReporting*) is not removed during the uninstall process. All configuration data stored in the database remains as well.



Migrating Veeam Backup Enterprise Manager

You may need to migrate Veeam Backup Enterprise Manager or its configuration database, or both to another server.

Before you migrate Enterprise Manager, you must export Enterprise Manager keysets and prepare the credentials stored in the Enterprise Manager configuration database so you will be able to re-enter the credentials on a new server. If you migrate the Enterprise Manager configuration database only, the credentials and keysets will remain valid.

For more information on migration scenarios, see this Veeam KB article.

Getting to Know Veeam Backup Enterprise Manager

After you install Veeam Backup Enterprise Manager, you can learn how to access the main product UI and get familiar with it.

Accessing Enterprise Manager Website

When you access Veeam Backup Enterprise Manager for the first time, you must log in as a user with administrative rights. To do that, enter credentials of a user account with local administrative rights or a user account that was used to install Enterprise Manager. Later you can add other account in Enterprise Manager. For more information, see Managing Accounts and Roles.

To access the Veeam Backup Enterprise Manager website:

1. Double-click the **Veeam Backup Enterprise Manager** icon on the desktop or select **Programs** > **Veeam** > **Veeam Backup Enterprise Manager** from the **Start** menu.

   Alternatively, open your web browser and enter the following URL in the address bar:

   ```
   https://<hostname>:9443
   ```

   For example:

   ```
   https://vbr-em:9443
   ```

2. From the drop-down list, select a display language.

   For more information, see Managing Languages.

3. Log in using your credentials:

   - To log in with Enterprise Manager credentials:

     i. In the **Username** and **Password** fields, specify your Enterprise Manager credentials. Provide the user account name in the *DOMAIN|Username* format.

     ii. To save the entered credentials for future access, select the **Remain signed in** option.

     iii. Click **Sign in**.

   - To log in with single sign-on, click **Use Single Sign-On (SSO)**. Enterprise Manager will redirect you to the login webpage of the single sign-on service. Complete the sign-in procedure on the login page. If the account is already authenticated in the single sign-on service, you will immediately access the Enterprise Manager website.

     > **NOTE**
     >
     > The **Use Single Sign-On (SSO)** option is available if SAML authentication is configured for Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.

When you log in under a user account which is not assigned a role for Enterprise Manager, you are automatically redirected to the **Veeam Self-Service File Restore Portal**. On this portal, you can browse and restore only machines on which your user account has local administrative rights. For more information on configuring Enterprise Manager security roles, see Managing Accounts and Roles.

> **NOTE**
>
> Veeam Self-Service File Restore Portal is available in the Enterprise Plus edition of Veeam Backup & Replication.

If you cannot access web UI over HTTPS, this can be due to several reasons. For more information, see this Veeam Knowledge Base article.

> **TIP**
>
> If you use Internet Explorer, then to be able to access the Enterprise Manager website using an account currently logged in to the Microsoft Windows OS, you can add this website to Local intranet sites in the Internet Options. In case the current user cannot be authenticated using this method, the Enterprise Manager login window will be displayed. This method works only for Internet Explorer. If you use another web browser, you may be prompted for login.

After you finish working with the Enterprise Manager website, or if you need to switch the user account, click the user name in the top right corner of the main window and then click **Sign Out**.

Veeam Backup Enterprise Manager UI

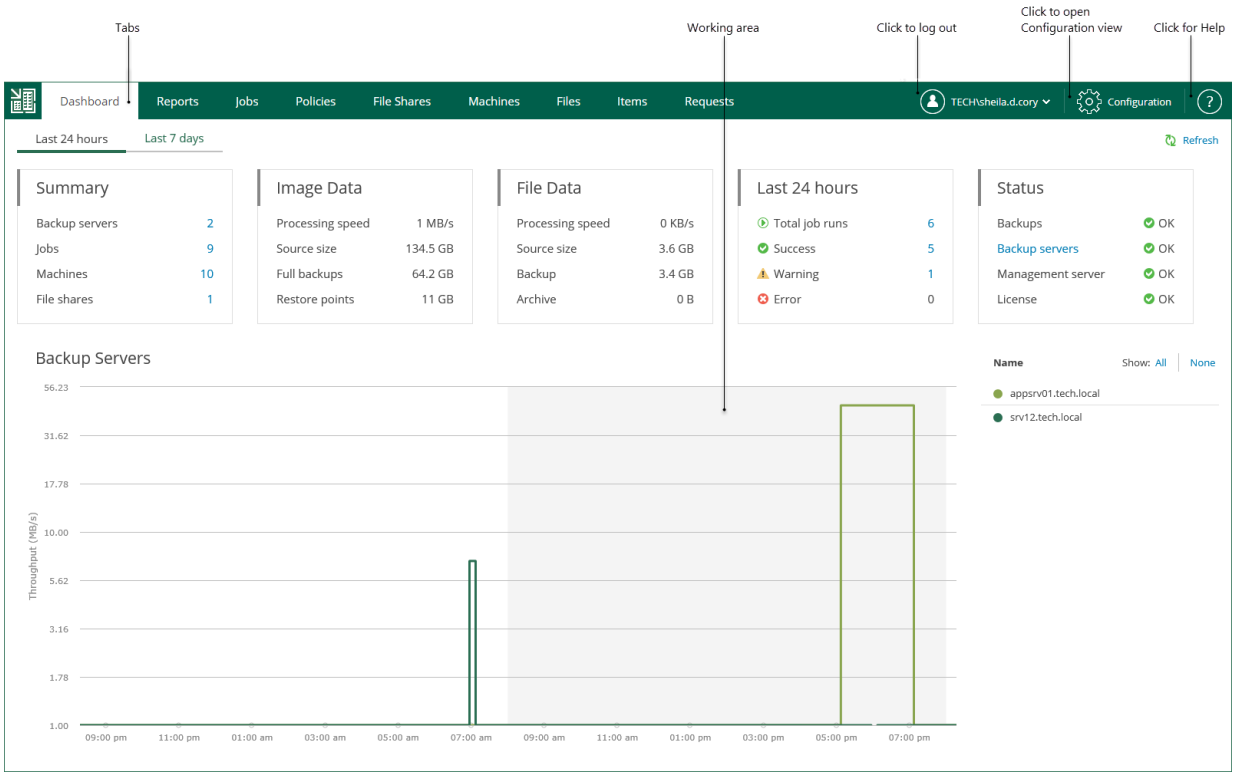
Home View

After you log in to Veeam Backup Enterprise Manager, the **Home** view opens. In the **Home** view, you can navigate through *tabs* to perform management and restore operations. A user can navigate only the tabs they are authorized to view in accordance with their security role. For more information on the Enterprise Manager roles and operations allowed to them, see Managing Accounts and Roles.

Below is the list of operations that you can perform in the **Home** view of the Veeam Backup Enterprise Manager UI:

- View on-going statistics for your backup infrastructure using the **Dashboard** tab. For more information, see Viewing Operation Statistics.
- View detailed information about Veeam backup servers managed by Enterprise Manager using the **Reports** tab. For more information, see Reports on Backup Servers.
- Manage jobs on all managed Veeam backup servers using the **Jobs** tab. For more information, see Managing Jobs.
- Browse for file share backups, search for file shares, delete file shares and perform tile-level restore from file share backups using the **File Shares** tab. For more information, see Working with File Shares.
- Browse for machine backups, search for machines, delete machines and perform failover and replication operations with managed virtual or physical machines using the **Machines** tab. For more information, see Working with Machines.
- Browse the guest OS file system in a machine backup, search for guest OS files and restore necessary files using the **Files** tab. For more information, see Restoring Guest OS Files.
- Perform item-level recovery from application-aware backups created by Veeam Backup & Replication using the **Items** tab. For more information, see Backup and Restore of Application Items.

- Approve submitted virtual lab requests, reject them or prolong the time for which a requested virtual lab should be up using the **Requests** tab. For more information, see Working with Virtual Lab Requests.



Configuration View

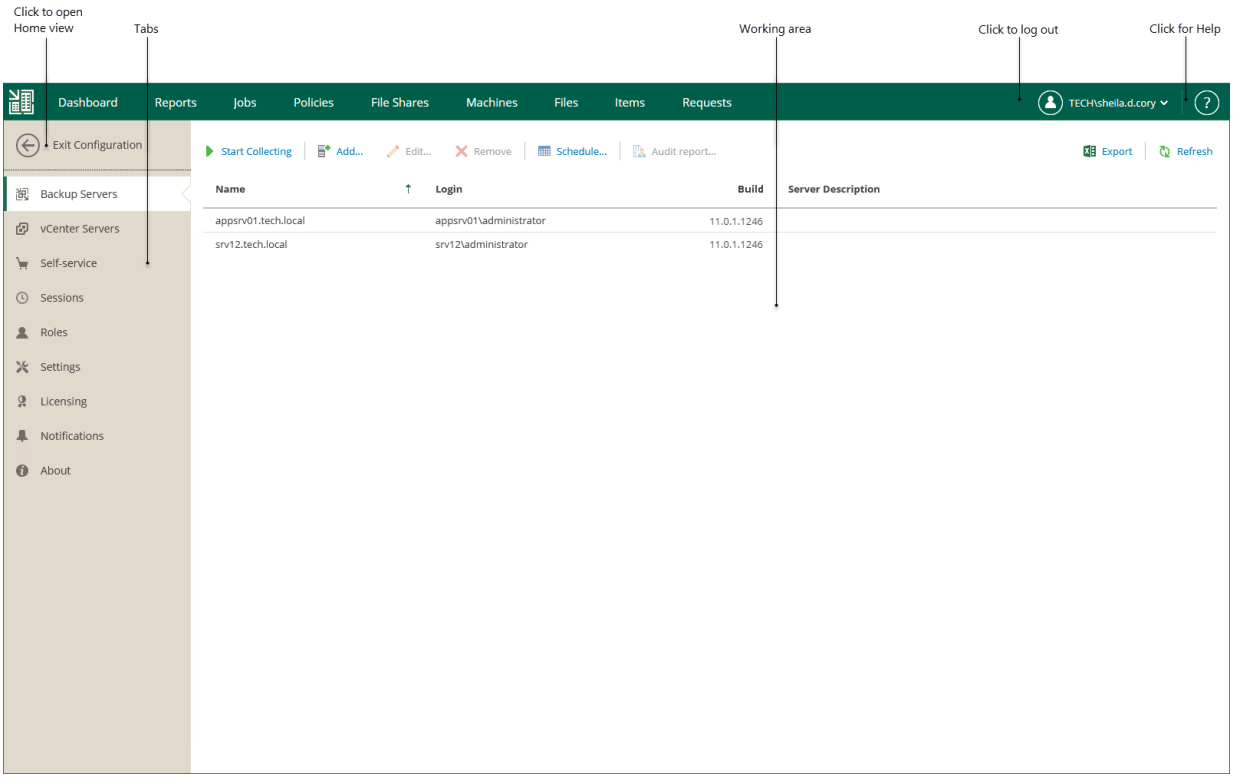
If you logged in with an administrative account, on the **Home** view you can click **Configuration** to open the **Configuration** view.

The tabbed pane, located on the left of the window, allows you to navigate to the configuration settings you need — for example, notifications, security roles, and others. The working area is located on the right; it allows you to view data, perform the necessary operations or manage the settings you need.

Below is the list of operations that you can perform in the **Configuration** view of the Veeam Backup Enterprise Manager UI:

- Add, edit or remove Veeam Backup servers using the **Backup Servers** tab. For more information, see Managing Backup Servers.
- Work with vCenter servers managed by Enterprise Manager using the **vCenter Servers** tab. For more information, see Viewing vCenter Servers.
- Manage vCloud Director organizations and vSphere tenant accounts using the **Self-Service** tab. For more information, see Working with VMware vCloud Director and vSphere Self-Service Backup Portal.
- View and manage data collection job sessions using the **Sessions** tab. For more information, see Collecting Data from Backup Servers.
- Configure Enterprise Manager security roles using the **Roles** tab. For more information, see Managing Accounts and Roles.
- Configure Enterprise Manager settings using the **Settings** tab. For more information, see Managing Encryption Keys, Configuring SAML Authentication Settings, Customizing Chart Appearance and Configuring Retention Settings for Index and History.

- Manage licenses and view detailed reports on license consumption using the **Licensing** tab. For more information, see Licensing.
- Set email notifications using the **Notifications** tab. For more information, see Configuring Notification Settings.
- View product versions, URLs and log paths using the **About** tab. For more information, see Viewing Information About Enterprise Manager.



Viewing Operation Statistics

On the **Dashboard** tab of the home page, Veeam Backup Enterprise Manager displays on-going statistics on backup servers, their jobs, processed machines and file shares as well as data size, processing speed and so on.

Statistics are divided into the following blocks:

- The **Summary** block shows the total number of managed backup servers, performed jobs, processed machines and file shares.
- The **Image Data** block shows the average processing speed, total size of processed machines, full backups and incremental backups.
- The **File Data** block shows the average processing speed, total size of processed file shares, backed-up and archived files.

  This block is displayed only if one or more file shares are added on a backup server connected to Veeam Backup Enterprise Manager.
- The **Last 24 hours / Last 7 days** block shows the total number of job runs, successful jobs, jobs with warnings and failed jobs.

  To switch between the time ranges, select a necessary tab in the top left corner.
- The **Status** block shows the status of backup files, managed backup servers, Veeam Backup Enterprise Manager management server, and licenses.

  License status is displayed as follows:

  - *OK* — current license is valid
  - *Warning* — working in grace period, or failed to update the license
  - *Error* — license is expired, and grace period is over

You can use the links in these blocks to drill down into detailed reports on specific aspects of the backup infrastructure.

Backup Servers Chart

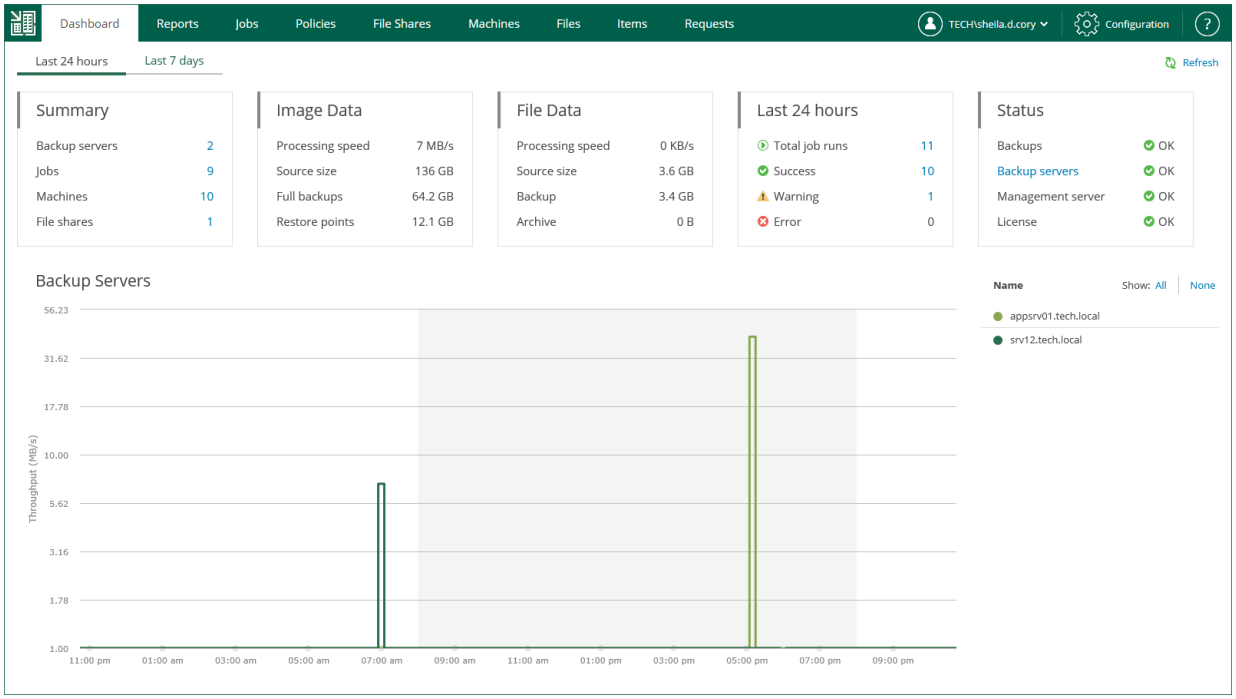
The **Backup Servers** chart shows date and time when backup jobs were performed, and the network throughput rate during the backup jobs. Jobs related to each backup server have their own color on the chart. The legend on the right interprets the color scheme used for all managed backup servers.

You can view the chart for one of the time ranges:

- Last 24 hours
- Last 7 days

To switch between the ranges, select a necessary tab in the top left corner.

In the **Last 24 hours** view, the highlighted part of the chart represents the configured backup window. You can configure the backup window in the chart settings. For more information, see Customizing Chart Appearance.

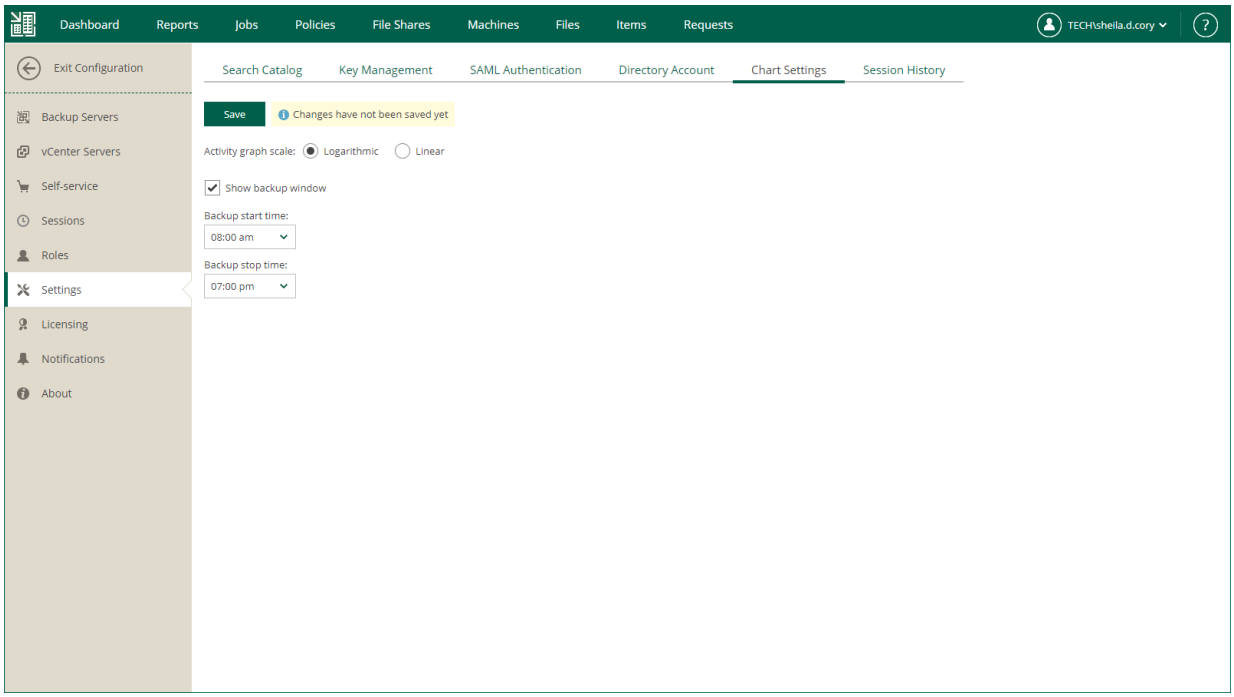


Customizing Chart Appearance

To customize the appearance of the chart:

1. Open the **Configuration** view.
2. Click the **Settings** section on the left of the **Configuration** view.
3. Use the **Activity graph scale** options on the **Chart Settings** tab to switch between graph types: **Linear** and **Logarithmic**.
4. By default, the time interval specified under the selected **Show backup window** check box is highlighted on the activity graph. Default interval is from 8:00 PM to 8:00 AM. You can change the highlighted interval to correlate with your planned backup window by editing the start and stop time. If you do not want to highlight the backup window on the graph, clear the **Show backup window** check box.

5. Save the changes.



Configuring Veeam Backup Enterprise Manager

As part of the Veeam Backup Enterprise Manager configuration process, you can perform the following tasks:

- Manage backup servers
- Collect data from backup servers
- View vCenter servers and install Veeam plug-in for vSphere Web Client on necessary servers
- Configure retention settings for index and history
- Configure security settings
- Configure notification settings
- Manage display languages

To start working with Veeam Backup Enterprise Manager, you must perform initial configuration. For more information, see Initial Configuration.

Initial Configuration

To start working with Veeam Backup Enterprise Manager, perform the following steps:

1. Log in to the Veeam Backup Enterprise Manager website. For more information, see Accessing Enterprise Manager Website.
2. Add backup servers you want to manage. For more information, see Adding Backup Servers.
3. Retrieve data from added backup servers. For more information, see Collecting Data from Backup Servers.
4. Assign the Portal Administrator, Restore Operator or Portal User roles to users who will work with Veeam Backup Enterprise Manager. For more information, see Configuring Accounts and Roles.
5. Provide email notification settings to be able to receive emails with summary on performed backup and replication jobs, lab request status changes and file restore operations. For more information, see Configuring Notification Settings.

Once you have performed initial configuration, you can start working with managed backup servers. You can change the necessary settings in the **Configuration** view at any time.

> **NOTE**
>
> The initial configuration tasks can be performed either by the user who installed Veeam Backup Enterprise Manager or any of the users listed in the local Administrators group (these accounts are automatically included in the Portal Administrators group).

Managing Backup Servers

With Veeam Backup Enterprise Manager, you can perform the following actions with backup servers:

- Add backup servers
- Edit backup servers
- Remove backup servers
- View reports on backup servers
- View audit reports
- Collect data from backup servers

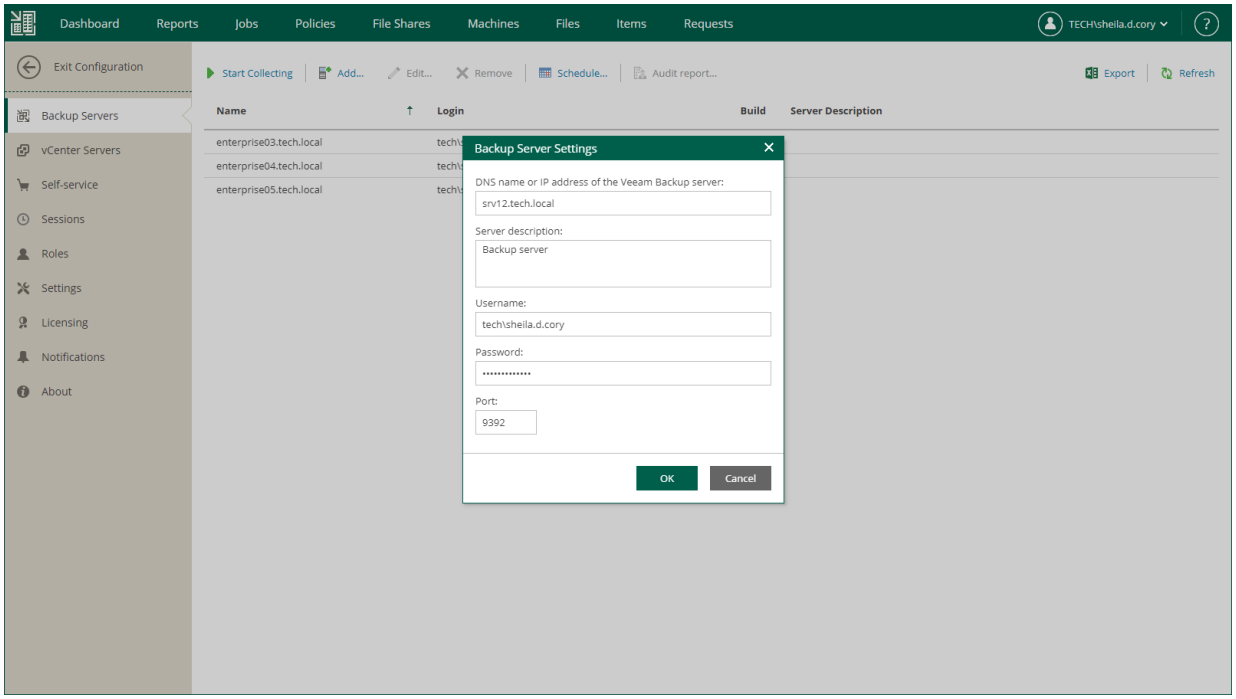
Adding Backup Servers

Veeam Backup Enterprise Manager allows users to manage jobs across several Veeam Backup & Replication servers and perform restore operations with backups using the information from these backup servers.

To add a backup server to the Enterprise Manager infrastructure:

- Log in to Enterprise Manager using an administrative account.
- To open the **Configuration** view, click **Configuration** in the top right corner.
- Go to the **Backup Servers** section on the left.
- Click **Add** at the top of the **Backup Servers** section.
- In the **Backup Server Settings** window, enter a full DNS name or IP address of the server you want to add, and provide a server description.
- Provide a name and password of the user with administrative rights on the added server. The Veeam Backup Enterprise Manager user must be assigned the Veeam Backup Administrator role on the backup server. For more information see Configuring Backup Server Roles.
- Specify the port used by Veeam Backup Service. By default, port **9392** is used.

- Click **OK** to add the server.



Limitations for Adding Backup Servers

Consider these limitations when you add backup servers to the Veeam Backup Enterprise Manager infrastructure:

- You must not add a backup server to multiple instances of Veeam Backup Enterprise Manager.
- You must not add a backup server cloned from an added backup server.
- You must not add a backup server that holds the same configuration database as an added backup server, even after you remove the original backup server from Enterprise Manager. You may have two backup servers with the same configuration database when, for example, you restore the configuration database from one backup server to another. In case you want to manage such a backup server with Enterprise Manager, contact Veeam Customer Support.
- You must not add more than one backup server that has a vCloud Director server in its infrastructure.
- Install the same product version on the Veeam Backup Enterprise Manager server and Veeam backup servers. If you use different versions of Veeam Backup Enterprise Manager and Veeam Backup & Replication, you may not be able to leverage all features in Veeam Backup Enterprise Manager.

  Veeam Backup Enterprise Manager supports adding backup servers with Veeam Backup & Replication 9.5 Update 4 and later.

Editing Backup Servers

To edit settings of a server after it was added, select the sever in the **Backup Servers** list and click **Edit** on the toolbar.

Removing Backup Servers

To delete an added Veeam backup server, select it in the **Backup Servers** list and click **Remove** on the toolbar.

Collecting Data from Backup Servers

Veeam Backup Enterprise Manager retrieves data from added backup servers using the data collection job. The data collection job collects information about backup and replication jobs from Veeam Backup & Replication databases on the managed backup servers. The collected data is stored to the Veeam Backup Enterprise Manager configuration database and can be accessed by multiple users on the Veeam Backup Enterprise Manager website.

There are two options for running the data collection job:

- Periodic data collection (default)
- Manual data collection

Every run of the data collection job initiates a new data collection job session. For more information, see Data Collection Job Sessions.

NOTE

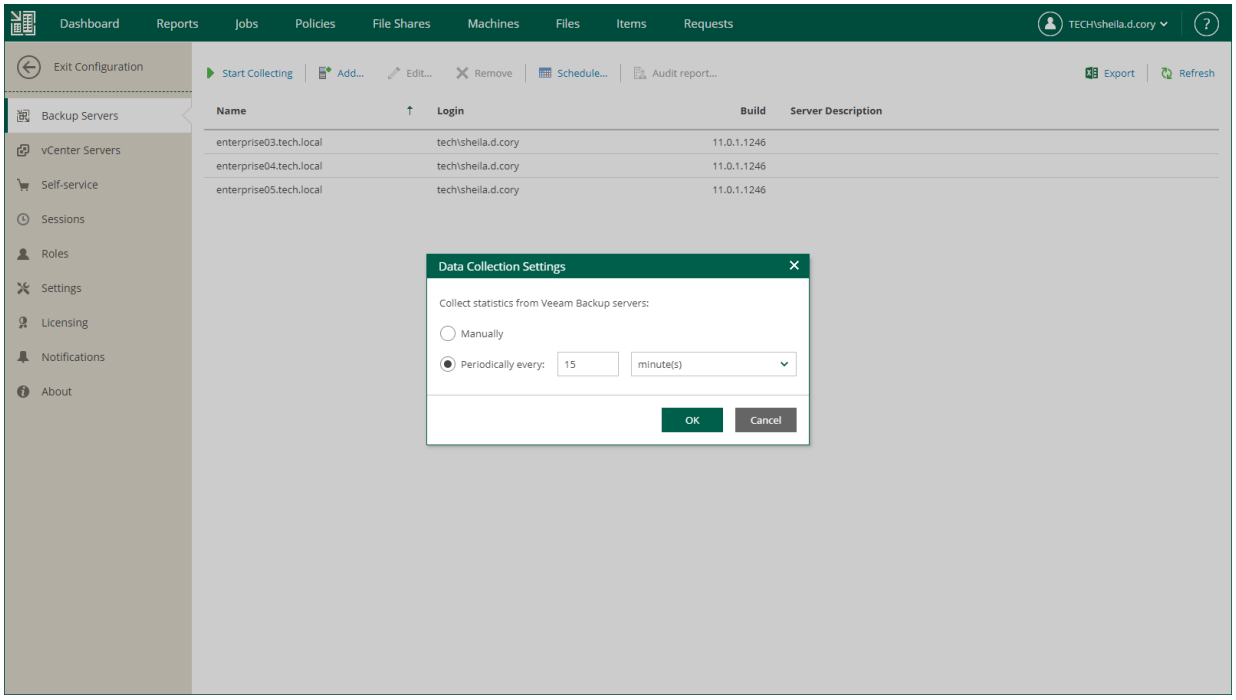
- Data collection job collects data from all added backup servers at once.
- To ensure periodic update of the information available to Veeam Backup Enterprise Manager users, use periodic data collection.

Periodic Data Collection

By default, Veeam Backup Enterprise Manager collects data from added backup servers every 15 minutes.

To change the data collection interval:

1. Select **Backup Servers** on the left of the **Configuration** view and click **Schedule** on the toolbar.
2. In the **Data Collection Settings** window, specify the desired interval in the **Periodically every** option.
3. Click **OK**.



You can also disable periodic data collection. In this case, you can only start the data collection job manually.

To disable periodic data collection:

1. Select **Backup Servers** on the left of the **Configuration** view and click **Schedule** on the toolbar.
2. In the **Data Collection Settings** window, select the **Manually** option.
3. Click **OK**.

Manual Data Collection

You can start the data collection job manually at any time.

To start the data collection job manually:

1. Select **Backup Servers** on the left of the **Configuration** view.
2. Click **Start Collecting** on the toolbar.

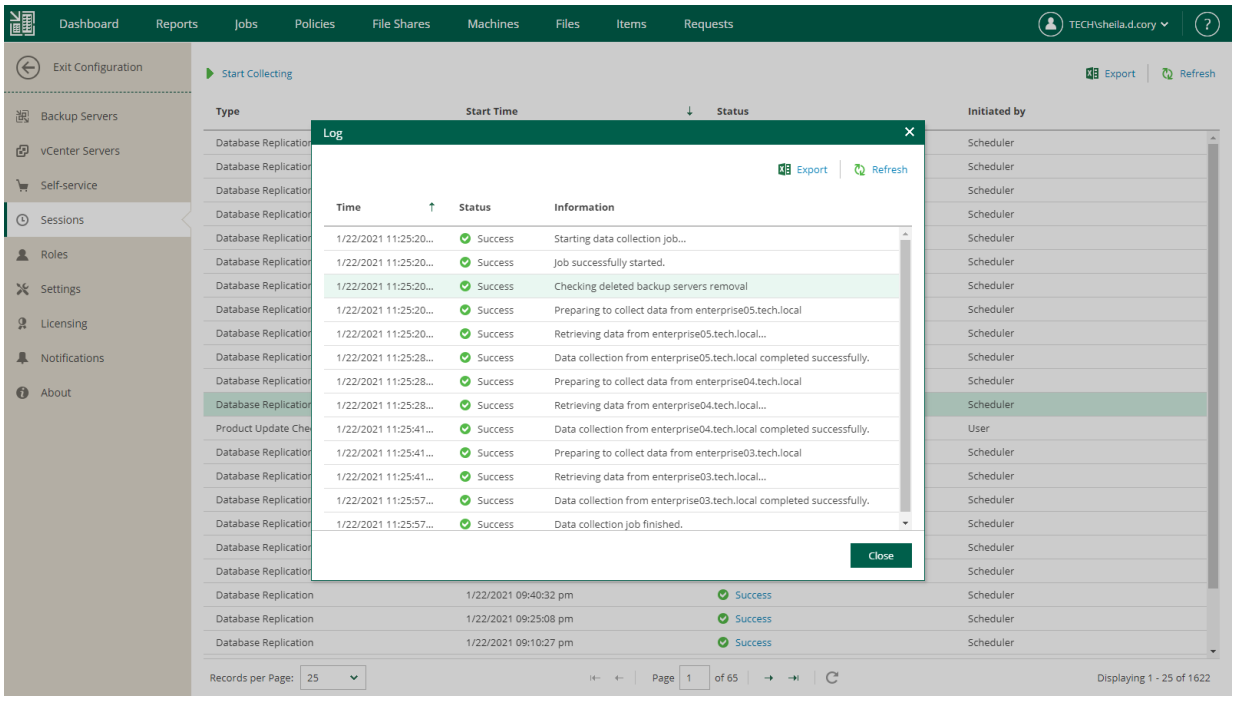
You can view the details on the started job session in the **Sessions** section of the **Configuration** view. For more information, see Data Collection Job Sessions.

Data Collection Job Sessions

Every run of the data collection job initiates a new data collection job session.

To view details on job sessions:

1. Select **Sessions** on the left of the **Configuration** view.
2. In the list of sessions, select the necessary session and click the link in the **Status** column.
3. In the displayed window, Veeam Backup Enterprise Manager shows the list of the job session events. For each job session event, Enterprise Manager shows the time of the event, its current status and information about the event.



Reports on Backup Servers

On the **Reports** tab, you can view statistical information about backup servers added to the Enterprise Manager infrastructure.

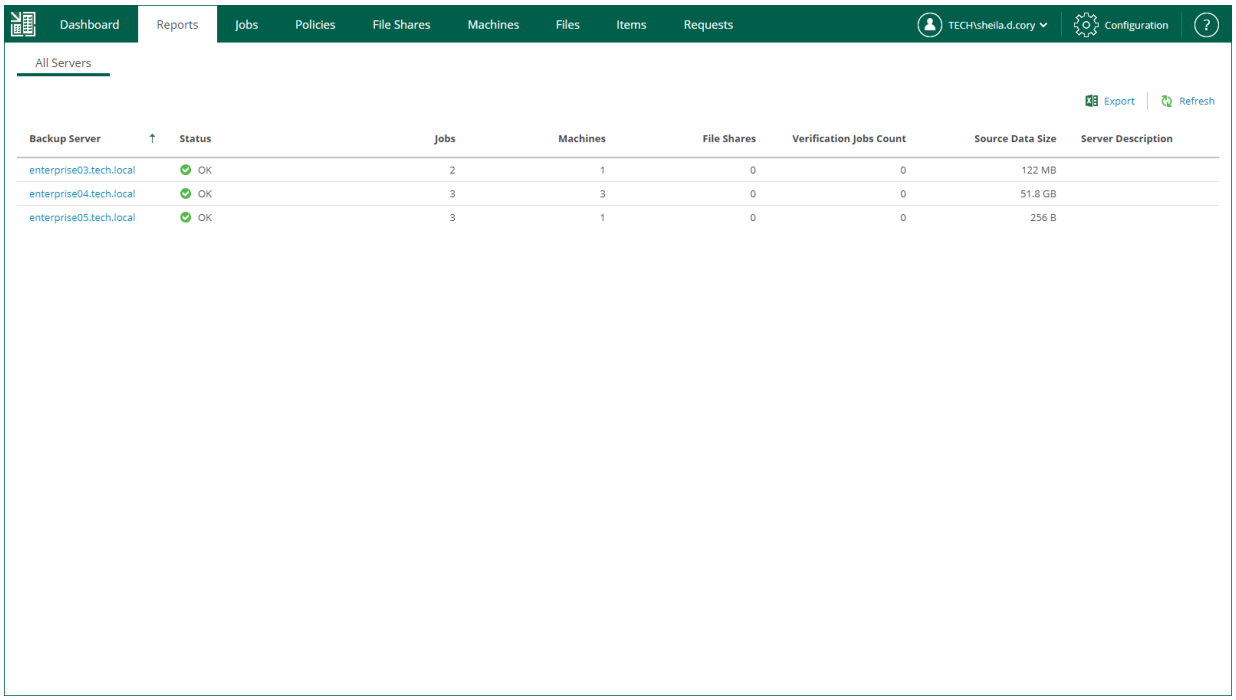
For each backup server, the report contains the following data.

Parameter	Description
Backup Server	Name of the backup server.
Status	Status of the last data collection job session for the backup server. For more information on data collection, see Collecting Data from Backup Servers. Possible values: • *Never processed* — data collection has never been started for the backup server • *Processing* — data collection is in progress • *OK* — data was collected successfully • *Warning* — data collection completed with a warning • *Error* — data collection failed
Jobs	Number of jobs on the backup server.
Machines	Number of machines processed by the backup server, including the machines from imported or orphaned backups.
File Shares	Number of file shares processed by the backup server, including the file shares from imported or orphaned backups.
Verification Jobs Count	Number of SureBackup jobs on the backup server.
Source Data Size	Size of source data processed by the backup server.
Server Description	Backup server description that was specified when adding the server to the Enterprise Manager infrastructure.

You can drill down into this data by clicking a link in the **Backup Server** column to move through the levels in the following succession: *Backup servers > Jobs > Job sessions > Session details*. Each level contains a list of entries with details for that particular level.

NOTE

You can export displayed information to a file using the **Export** link on the toolbar. To open the file on your machine, use the associated application.



Audit Reports

Audit reports contain records of user activity performed on the selected backup server for the specified period. Users with the Portal Administrator role can generate audit reports for backup servers added to the Veeam Backup Enterprise Manager infrastructure. For more information, see Generating Audit Report.

Audit reports include the following details about user activity:

- Date and time when a user performed an operation
- User name
- User security identifier (SID)
- Name of the operation performed by the user
- Operation result
- Details on the performed operation

	A	B	C	D	E	F
1	Time	User	SID	Operation	Result	Details
2	28.09.2020 19:35:23Z	ENTERPRISE03\Administrator	S-1-5-21-3589086896-2179654325-2245872042-500	Login	Success	
3	29.09.2020 14:24:40Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	Login	Failed	errorMsg='Access denied.'
4	29.09.2020 14:29:46Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	Login	Success	
5	29.09.2020 18:58:35Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='2c4ee74003764f1aaffd08c47e471fc0';vmName='virt03-vm01'
6	30.09.2020 09:29:30Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='593f11877c31422a973619491531f0e4';vmName='virt03-vm01'
7	02.10.2020 10:51:51Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	Login	Success	
8	02.10.2020 21:28:33Z	TECH\sheila.d.cory		JobDisable	Success	jobName='Backup Job 2';jobUid='152756dd-65bd-42dd-a3b5-09e53193b5f2'
9	02.10.2020 21:28:36Z	TECH\sheila.d.cory		JobEnable	Success	jobName='Backup Job 2';jobUid='152756dd-65bd-42dd-a3b5-09e53193b5f2'
10	05.10.2020 11:37:11Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	Login	Success	
11	08.10.2020 08:50:36Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='ce6199e4cc1e47abb0b1e947a4d2fc1c';vmName='virt03-vm01'
12	08.10.2020 10:46:22Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='6e95a8f34555412b899334986de9f27e';vmName='virt03-vm01'
13	08.10.2020 14:38:08Z	tech\hue.spenser		JobEdit	Success	jobName='Backup Job 1';jobUid='23443dc9-466e-4b30-9eb5-5f633a72c38c'
14	08.10.2020 15:51:32Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='d0b1640995a24130860779239 56f7f88';vmName='virt03-vm01'
15	13.10.2020 15:11:39Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionUid='fb47bdd80c01493cab2521d1359ef27e';vmName='virt03-vm01'

Generating Audit Report

When you generate an audit report, it is downloaded in the CSV format to the local machine.

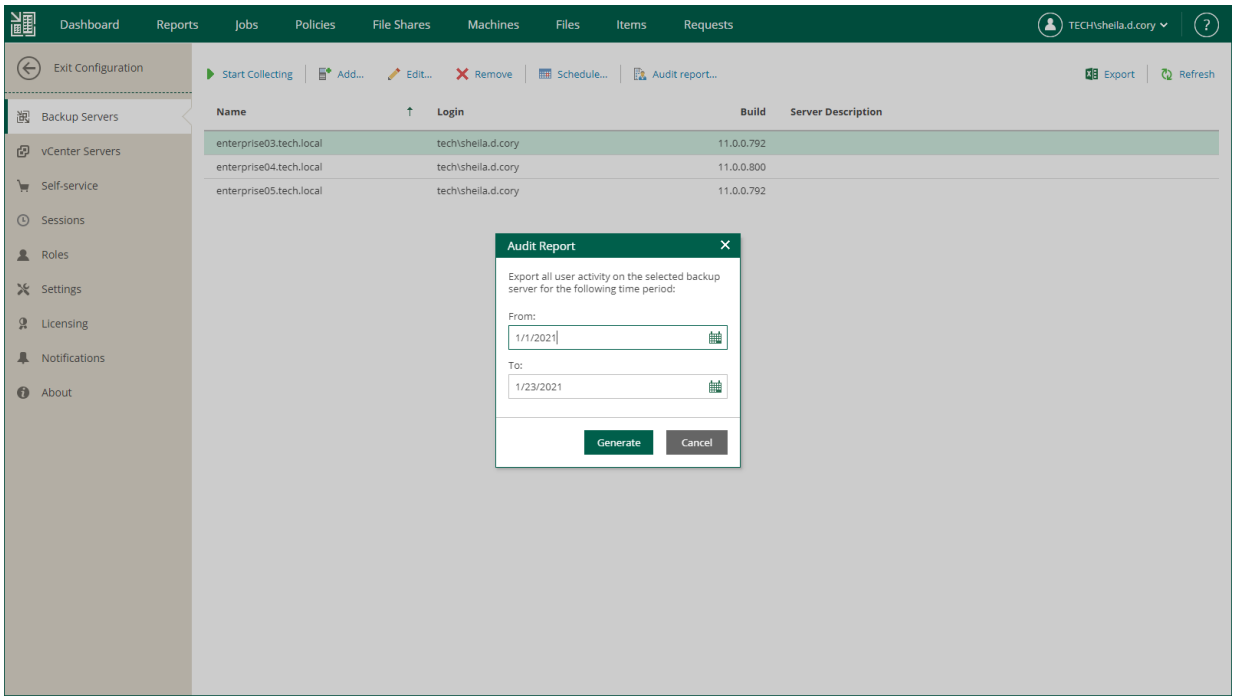
The generated file is also saved on the Enterprise Manager machine. Enterprise Manager does not clean up these files. You can find all reports in the following folder: `%ProgramData%\Veeam\Backup\WebRestore`.

To generate an audit report:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Backup Servers** section, select a backup server whose report you want to export.
4. Click **Audit report**.

5. In the **Audit Report** window, specify a time period covered by the report and click **Generate**.

   The report contains only the audit records whose retention period is not expired. The retention period is defined by the **Event history** setting of Enterprise Manager. For more information on retention settings, see Configuring Retention Settings for Index and History.



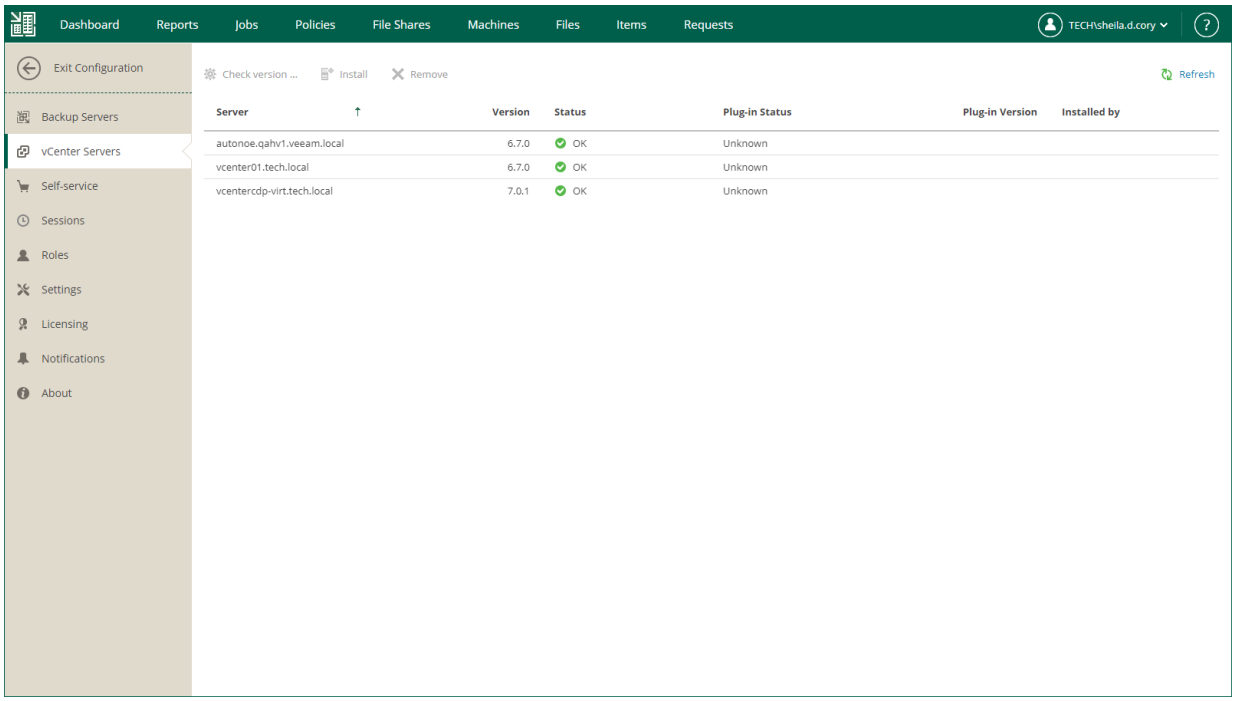
Viewing vCenter Servers

On the **vCenter Servers** tab of the **Configuration** view, you can view information on vCenter servers added to your Veeam backup infrastructure.

You can perform the following operations with vCenter servers:

- **Check version** – use this command to request vCenter server version and operation status. If Veeam plug-in for vSphere Web Client is deployed, its version, status and installation account will be also displayed.
- **Install** – use this command to install Veeam plug-in for vSphere Web Client on the selected server. For details, see Controlling Backup Infrastructure with vSphere Web Client.
- **Remove** – use this command to uninstall Veeam plug-in for vSphere Web Client from selected server.

> **IMPORTANT**
>
> To perform these operations, you should supply a user account with sufficient permissions to access vCenter Server. User account information is not imported from the Veeam Backup & Replication configuration database to the Enterprise Manager database for security reasons.



Configuring Retention Settings for Index and History

Veeam Backup Enterprise Manager allows you to configure retention settings for the index files, as well as for the event history.

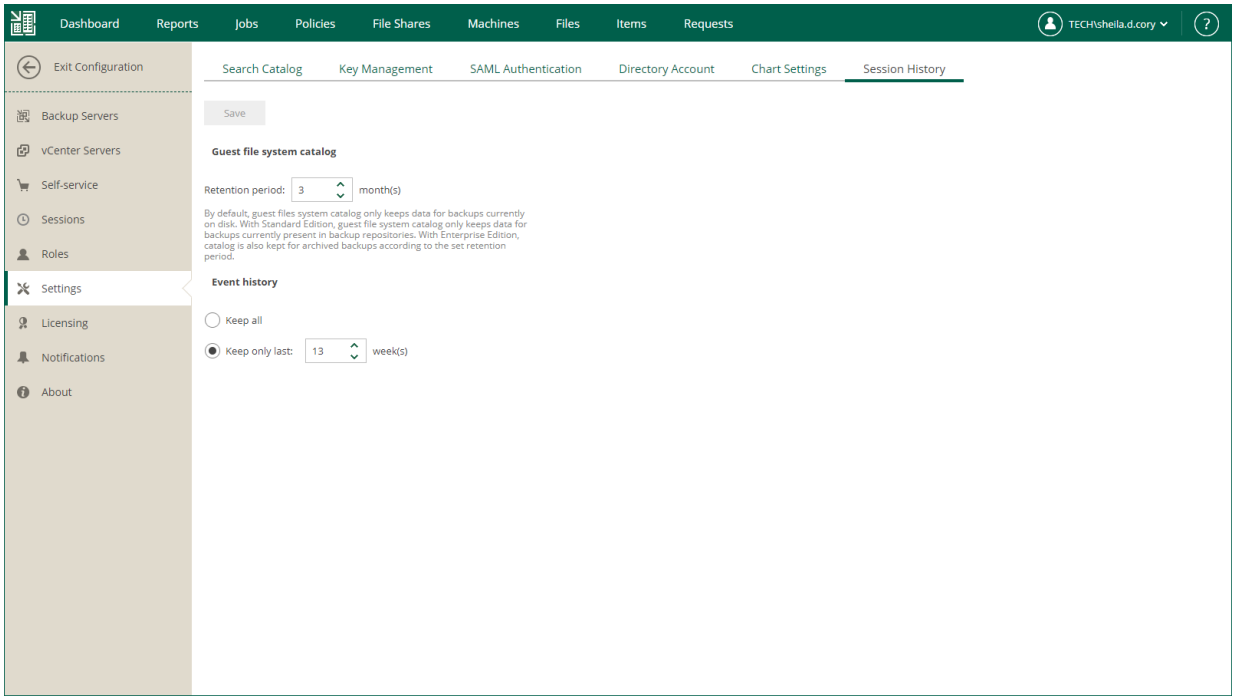
- If you are using the Standard edition of Veeam Backup & Replication in your virtual environment, Veeam Backup Enterprise Manager will keep index files only for those backups that are currently stored on disk (that is, the backups are available on backup repositories).
- If you are using the Enterprise or Enterprise Plus edition, Veeam Backup Enterprise Manager will keep index files for backups that are currently stored on disk and for archived backups (for example, backups that were recorded to tape). Thus, you will be able to browse and search through backup contents even if the backup in repository is no longer available or it was removed by **Remove from Backups** or **Remove from Disk** command in Veeam Backup console. For more information, see Managing Backups and Managing Replicas sections of the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> Consider that, by default, backup repository is the primary destination for the search. This means, in particular, that if a backup (with indexed guest) is stored in both locations — repository and tape — then Enterprise Manager search results will only include files from backup stored in the repository. Files from tape-archived backup will appear in search results only if not found in the repository.

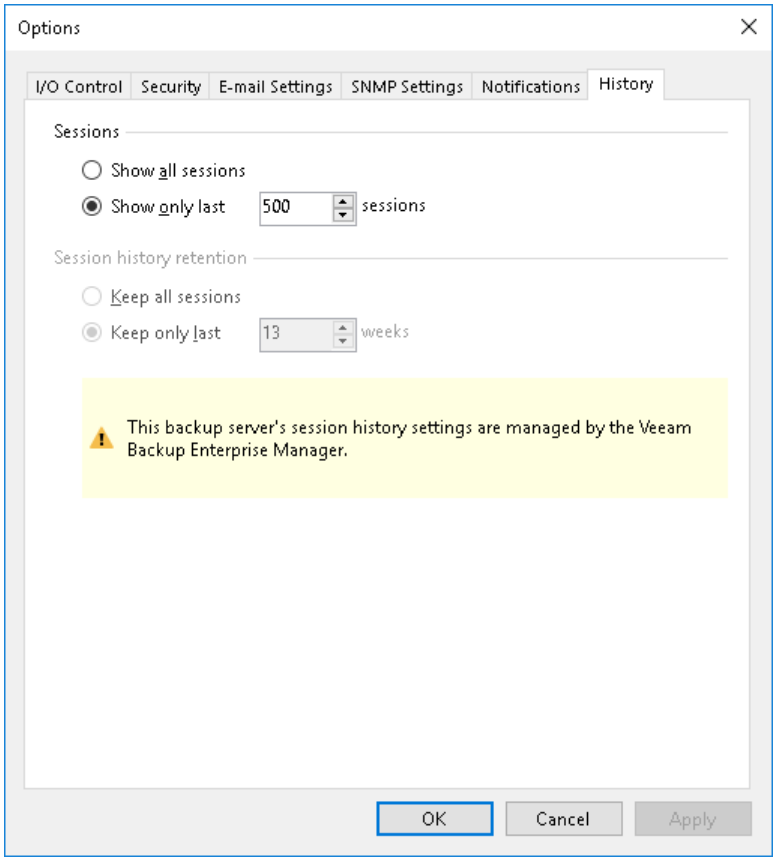
To configure retention settings:

1. To open the **Configuration** view, click **Configuration** in the top right corner.
2. Open the **Settings** section on the left of the **Configuration** view.
3. On the **Session History** tab, in the **Guest file system catalog** section, specify how long index files must be stored on the Veeam Backup Enterprise Manager server:
   a. Enter the desired number of months in the **Retention period, months** field. The default value is **3 months**, the minimum allowed value is **1 month**, and the maximum allowed value is **99 months**.
   b. When finished, click the **Save** button under the **Event history** section. New retention settings will be saved in the Enterprise Manager database, and pop-up message notifying you on the update will be displayed at the top of the window.
4. In the **Event history** section, specify the period for which Veeam Backup Enterprise Manager should keep historical data available in the main working area of the Veeam Backup Enterprise Manager website.
   a. Enter the desired number of weeks or select **Keep all**. By default, the retention period for session data is set to **Keep only last 13 weeks**. The minimum allowed value is **1 week**, and the maximum allowed value is **53 weeks**.

b. When finished, click the **Save** button below the section. New retention settings will be saved in the Enterprise Manager database, and pop-up message notifying you on the update will be displayed at the top of the window.



Note that the retention settings you specify in Veeam Backup Enterprise Manager are propagated to all Veeam backup servers connected to it. These settings override the **Session history retention** values specified at the level of the Veeam backup server.



For example, if the retention options of the Veeam backup server are configured to keep the session history for **50** weeks, and in Veeam Backup Enterprise Manager you select to **Keep only last 53 weeks**, the latter value will be propagated to the Veeam backup server; so the history will be kept for **53** weeks.

Configuring Security Settings

To establish secure connection with Veeam Backup Enterprise Manager, make sure you configure the following security settings:

- Configure accounts and roles of Veeam Backup Enterprise Manager
- Configure users and roles on added backup servers
- [Optional] Configure SAML authentication settings
- Update an expired security certificate

Configuring Accounts and Roles

Veeam Backup Enterprise Manager implements security based on user roles by limiting access to features and data. This empowers the administrator to delegate permissions in a granular way, on an as-needed basis. For example, the administrator can grant permissions to another user to recover files without being able to see the content of the files.

Administrators grant users and groups access to Enterprise Manager by adding accounts. When adding an account, administrators assign a role to the account to provide it with permissions.

Enterprise Manager offers the following roles:

- Portal Administrator
- Portal User
- Restore Operator

For the Portal User and Restore Operator roles, administrators can also configure restore scope and restrictions for delegated restore.

> **NOTE**
>
> This section describes management of user accounts and roles required to work with the main Enterprise Manager UI. If you plan to provide a user with access to vSphere Self-Service Backup Portal (and not to the main Enterprise Manager UI), you do not need to configure an account for this user in the **Roles** tab of the **Configuration** view. Such accounts are configured in the **Self-service** tab of the **Configuration** view. For more information, see Managing Tenant Accounts.

Accounts and Roles Overview

Accounts

Administrators can add accounts to Veeam Backup Enterprise Manager to grant users access to the website. Enterprise Manager offers the following account types: User, Group, External User and External Group.

Type	Description	How to Sign In	Name Format
User	Local or AD user	By specifying a user name and password	*DOMAIN|Username* Domain is optional
Group	Local or AD group	By specifying a user name and password	*DOMAIN|Groupname* Domain is optional
External User	IdP user	By using single sign-on*	*Username@Suffix*
External Group	IdP group	By using single sign-on*	Free-form string

* For more information on the single sign-on capability, see SAML Authentication Support.

Roles

To provide an account with permissions, administrators assign one of the following roles to the account: Portal Administrator, Portal User or Restore Operator.

Role	How Is Assigned	Access to Configuration	Permissions
Portal Administrator	• Initially by default to the users listed in the local Administrators group and the user who installed Enterprise Manager • By Portal Administrator in **Configuration** > **Roles**	Yes	Full access to all available operations on all tabs of the web UI
Portal User	By Portal Administrator in **Configuration** > **Roles**	No	• Access objects from the restore scope on the **Machines** and **Files** tabs • Run Quick Backup for machines from the restore scope on the **Machines** tab • Perform restore operations as permitted by the delegation settings • View information about all backup servers and jobs on the **Dashboard**, **Reports**, **Jobs** and **Policies** tabs
Restore Operator	By Portal Administrator in **Configuration** > **Roles**	No	• Access objects from the restore scope on the **Machines** and **Files** tabs • Perform restore operations as permitted by the delegation settings

Users with the Portal User or Restore Operator role can access their *restore scope* — a list of objects that can be recovered by appropriate personnel. For example, the restore scope of database administrators is database servers (SQL, Oracle or other), the restore scope of Exchange administrators is Exchange server machines, and so on. For more information on configuring restore scope, see Configuring Restore Scope.

IMPORTANT

You can customize the restore scope if you have the Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all objects and cannot be customized. However, you can delegate recovery of entire machines, guest files, or selected file types. For more information, see Configuring Restrictions for Delegated Restore.

Managing Accounts

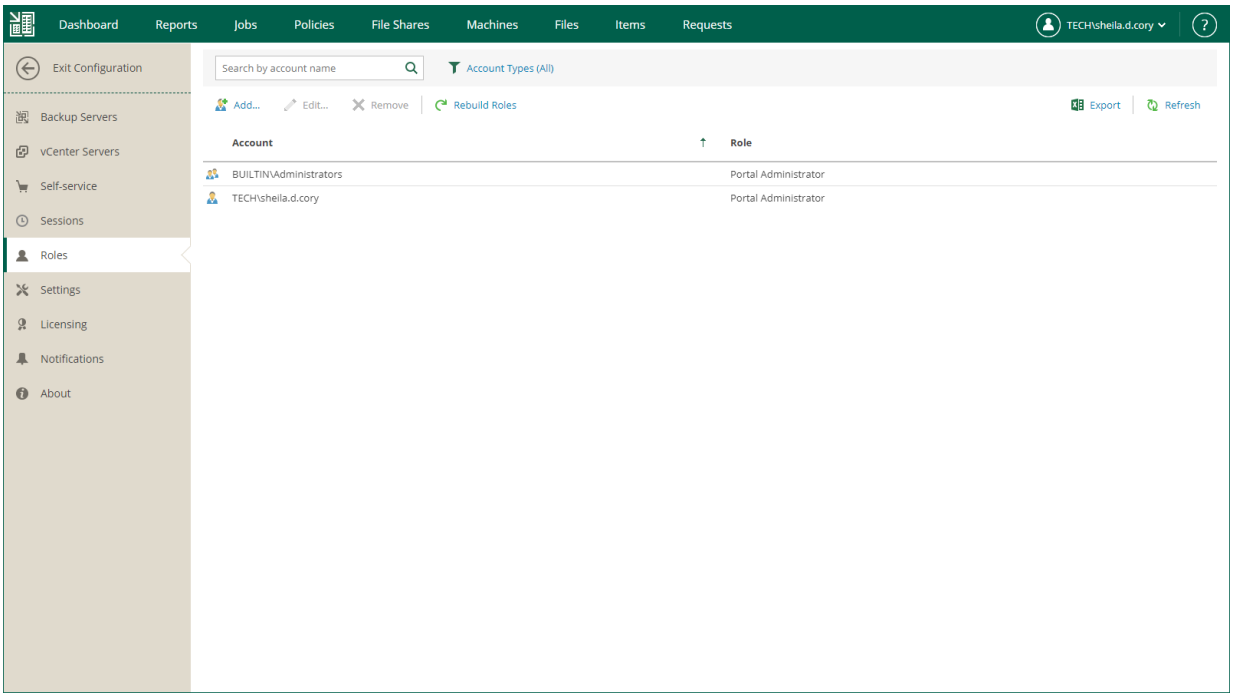
Administrators can perform the following actions with accounts:

- Add account
- Edit account
- Remove account

Adding Account

To add an account:

1. Select the **Roles** section of the **Configuration** view.

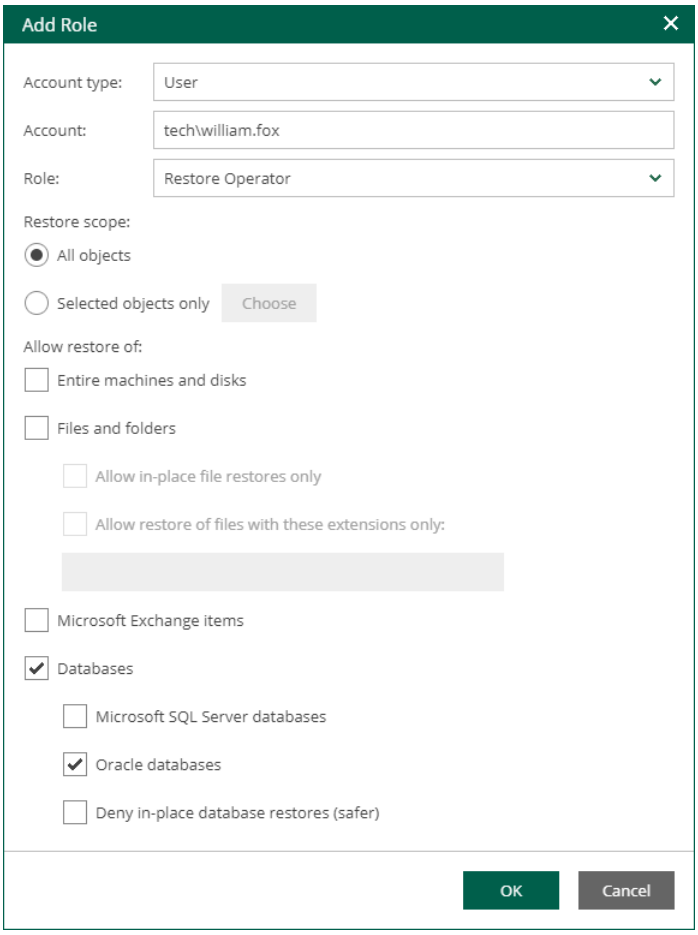


2. Click **Add** on the toolbar.
3. From the **Account type** list, select a type of the account: *User*, *Group*, *External User* or *External Group*. For more information, see Accounts.
4. In the **Account** field, specify an account name in the *DOMAIN|Username* or *Username@Suffix* format depending on the account type. For more information, see Accounts.
5. From the **Role** list, select a role you want to assign to the account: *Portal Administrator*, *Portal User* or *Restore Operator*. For more information, see Roles.

> **NOTE**
>
> To be able to assign any of portal roles to Active Directory domain users or groups, make sure that Veeam Backup Enterprise Manager service account has sufficient rights to enumerate Active Directory domains (by default, Active Directory users have enough rights to enumerate Active Directory domains).

6. [For Portal User or Restore Operator] In the **Restore scope** section, you can allow a user to restore all objects (machines and file shares) processed by managed backup servers or the selected objects only. For more information, see Configuring Restore Scope.

   In the **Allow restore of** section, you can configure additional restrictions for the restore scope. For more information, see Configuring Restrictions for Delegated Restore.



Editing Account

To edit settings of an added user or group, select it in the list of roles and click **Edit** on the toolbar. Then edit user or group settings as required.

Removing Account

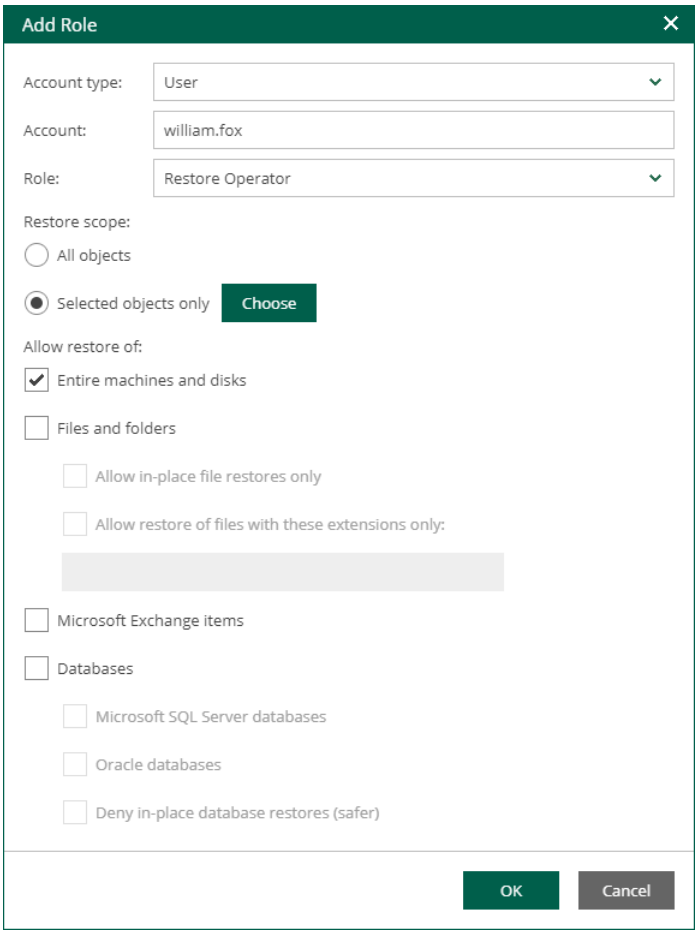
To remove an added user or group, select it in the list and click **Remove** on the toolbar.

Configuring Restore Scope

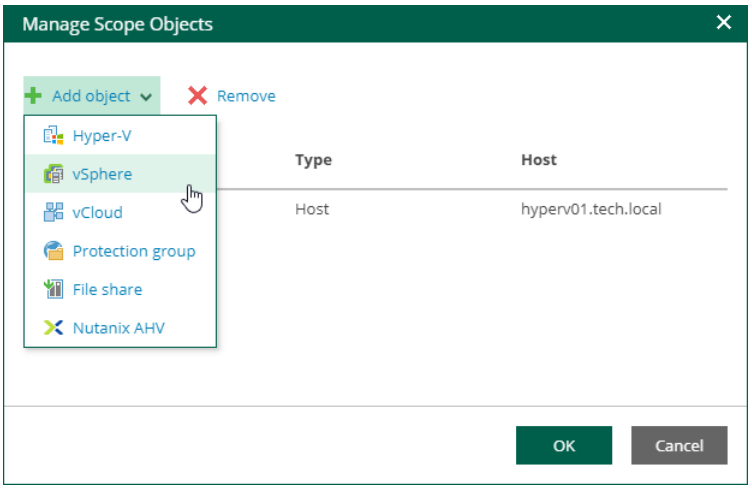
Default restore scope for users with a non-administrative role includes **All objects** from available backups. If you have the Enterprise Plus edition of Veeam Backup & Replication deployed in your environment, you can customize restore scope for non-administrative users.

To narrow the restore scope, perform the following steps when adding or editing a Portal User or Restore Operator account:

1. Open the **Roles** section of the **Configuration** view.
2. Click **Add** to add an account, or select an existing account and click **Edit**.
3. In the **Restore scope** section, select the **Selected objects only** option and click **Choose**.



4. In the **Manage Scope Objects** window, click **Add object** and select what type of objects to display. You can select from the following types: *Hyper-V*, *vSphere*, *vCloud*, *Protection Group*, *File share* or *Nutanix AHV object*.

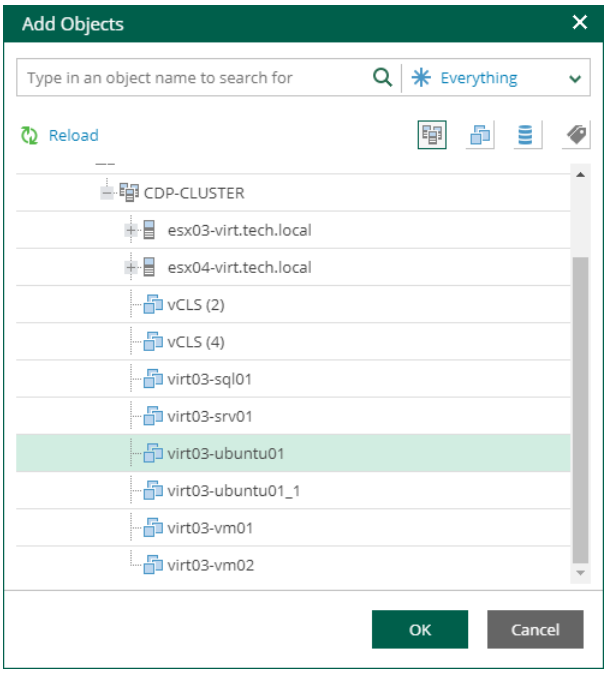


5. In the **Add Objects** window, select the objects you allow the user to restore.

   To search for an object, type a name or its part in the search field. Specify the type of the object from the drop-down list next to the search field.

   You can also switch between virtual infrastructure views using the buttons in the top right corner:

   - For VMware objects, you can switch between the **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** and **Tags and VMs** views.
   - For Hyper-V objects, you can switch between the **Hosts and VMs**, **Hosts and Volumes**, and **Hosts and VM Groups** views.



> **NOTE**
>
> For setting up self-service recovery restore scope, consider that reverse DNS lookup on Veeam Backup Enterprise Manager server must be functional. Otherwise, the **Add Objects** window will display incomplete infrastructure.

4. Click **OK** to save the settings.

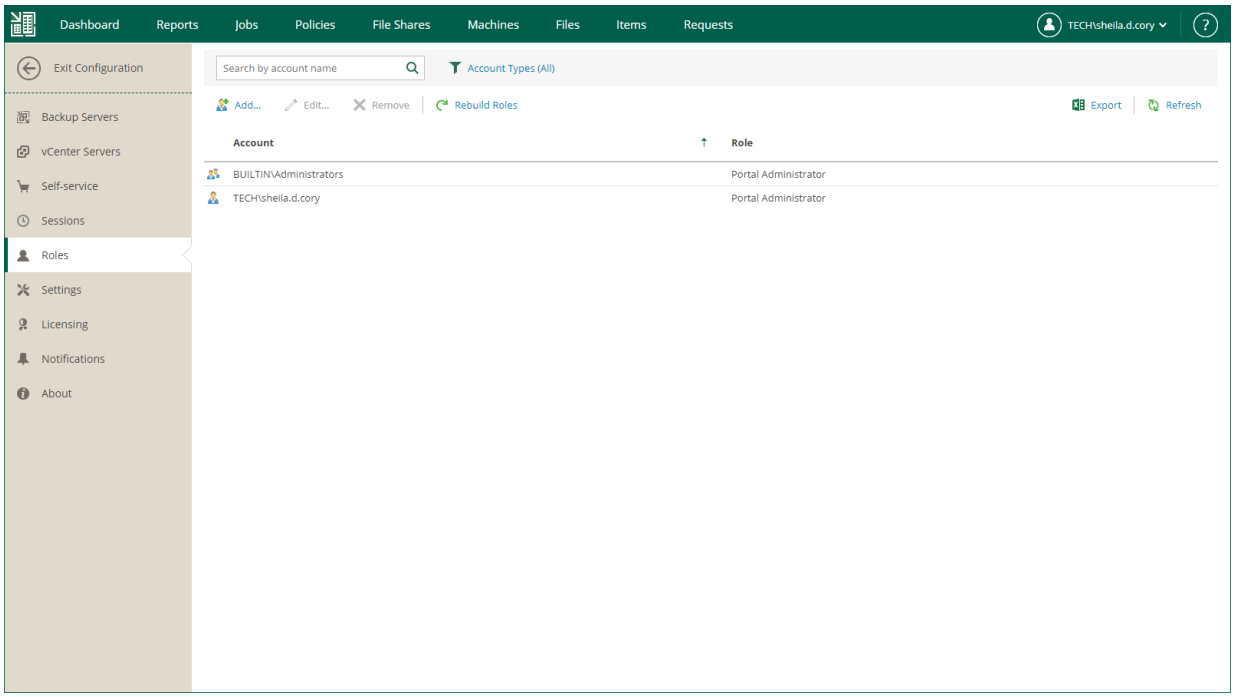
After a user logs in to Enterprise Manager, they will be able to view objects and files included in their restore scope.

> **NOTE**
>
> The **Machines** and **File Shares** tabs display only machines and file shares that have been backed up. The **Files** tab displays guest OS files only for machines that have been backed up with guest file indexing enabled. For more information on indexing, see Preparing for File Browsing and Searching.

Restore scope is automatically refreshed daily on built-in schedule and after any role modification. It may happen that some newly created machines, file shares and backups are not yet presented to users in the **Machines**, **File Shares** or **Files** tabs right after the login to Enterprise Manager. If you cannot find an object after making a search query, click the link **I don't see my VM** to refresh the view. This link, however, will not be visible until you have made an unsuccessful search.

Administrative user can click **Rebuild Roles** in the **Roles** section of **Configuration** page to refresh all scopes of all accounts manually. Consider that this operation will affect all configured roles.

Portal Administrators can watch the progress of security scope rebuild process on the **Sessions** page.



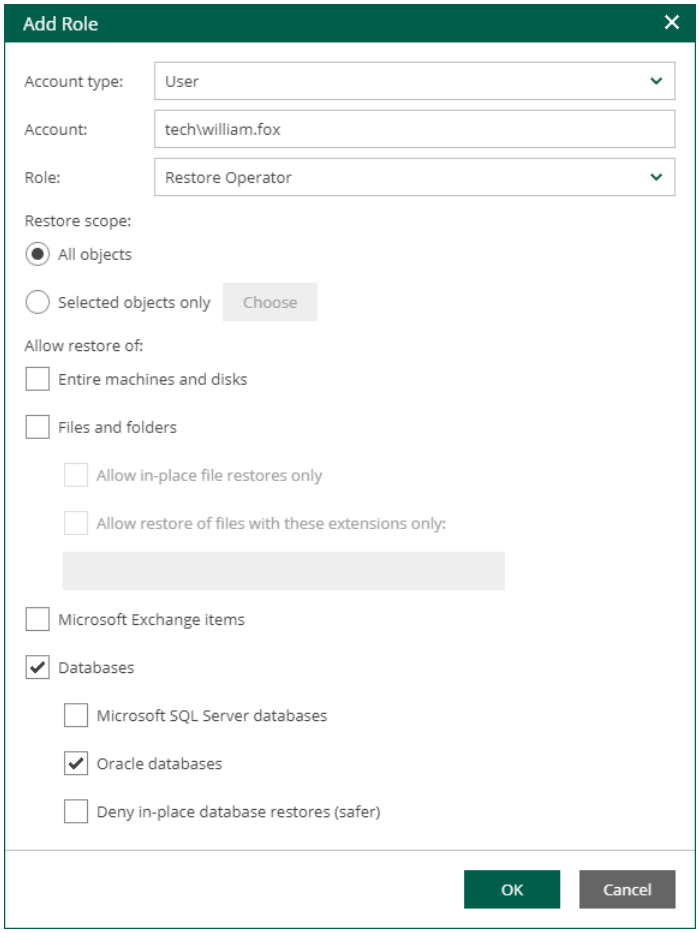
Configuring Restrictions for Delegated Restore

By default, users can restore all types of files from available backups. Files can be restored either to the local machine or the original location. For security purposes, you can configure additional restrictions for the restore scope. For example, you can specify the list of file types available to the operator or prohibit downloading of restored files at all.

To restrict the restore operator actions, perform the following steps when adding or editing the account:

1. Open the **Roles** section of the **Configuration** view.
2. Click **Add** to add an account, or select an existing account and click **Edit**.

3. In the **Allow restore of** section, to allow restore of entire machines and VM disks of machines included in the restore scope, select the **Entire machines and disks** check box.
4. To allow restore of guest OS files, select the **Files and folders** check box. If you select this check box, you can also select the following options:
   - **Allow in-place file restores only** – select this option to allow file-level restore to the original location only. Consider that the restored files will be available only to accounts that have access to the original machine.
   - **Allow restore of files with these extensions only** – select this option to define which file types are allowed for restore. In the text box, enter a list of extensions for allowed file types, separated by commas.
5. To allow restore of Microsoft Exchange items (mail, calendars, tasks), select the **Microsoft Exchange items** check box.
6. To allow restore of databases, select the **Databases** check box. If you select this check box, you can also select the following options:
   - **Microsoft SQL Server databases** – select this option to allow restore of Microsoft SQL databases on machines included in the user's restore scope.
   - **Oracle databases** – select this option to allow restore of Oracle databases on machines included in the user's restore scope.
   - **Deny in-place database restores** – select this option to restrict the restore operator from overwriting the original databases during the database restore process.
7. Click **OK**.



Configuring Backup Server Roles

Veeam Backup Enterprise Manager communicates with backup servers under accounts that you specified when adding the backup servers. For more information, see Adding Backup Servers.

All operations on the backup server side are performed by Veeam Backup Service. The service verifies beforehand if the account used by Enterprise Manager has rights to accomplish the necessary actions. For that, the account must have the Veeam Backup Administrator role assigned in Veeam Backup & Replication.

By default, when you install Veeam Backup & Replication on a backup server, the Veeam Backup Administrator role is assigned to the Windows Server Administrators group, so you can choose a user from the Administrators group as an account that will be used to communicate with the backup server. As soon as the group settings can be changed, it is recommended to explicitly assign the Veeam Backup Administrator role to the user account. For more information on assigning roles, see the Roles and Users section of the Veeam Backup & Replication User Guide.

Configuring SAML Authentication Settings

Organizations who use single sign-on (SSO) in their IT infrastructure can allow users to access the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal with their SSO credentials. To do this, the Enterprise Manager administrator must configure SAML authentication settings.

> **NOTE**
>
> If SAML authentication is enabled, users can log in to vSphere Self-Service Backup Portal under SSO accounts only.

To configure SAML authentication settings:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. Open the **Settings** section of the **Configuration** view.
4. Click the **SAML Authentication** tab.
5. Select the **Enable SAML 2.0** option.
6. In the **Identity Provider Configuration** section, specify identity provider settings. For more information, see Specifying Identity Provider Settings.
7. [Optional] If you want to use a certificate to encrypt and sign service provider SAML requests, specify certificate settings. For more information, see Selecting Service Provider Certificate.
8. [Optional] Click the **Advanced Settings** link and specify advanced SAML authentication settings. For more information, see Specifying Advanced SAML Authentication Settings.
9. In the **Enterprise Manager Configuration** section, export or manually copy metadata of the service provider (the Veeam Backup Enterprise Manager website, vSphere Self-Service Backup Portal, or both) for which you configure SSO. Use the metadata to register the service provider on the identity provider side. For more information, see Obtaining Service Provider Settings.
10. Click **Save**.

After you configure SAML authentication settings, you can register user accounts that will be able to log in to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal using SSO. For more information, see Managing Accounts and Roles and Managing Tenant Accounts.

Specifying Identity Provider Settings

To set up SAML authentication, you must obtain SAML authentication settings from the identity provider and specify them in Enterprise Manager. You can specify identity provider settings in one of the following ways:

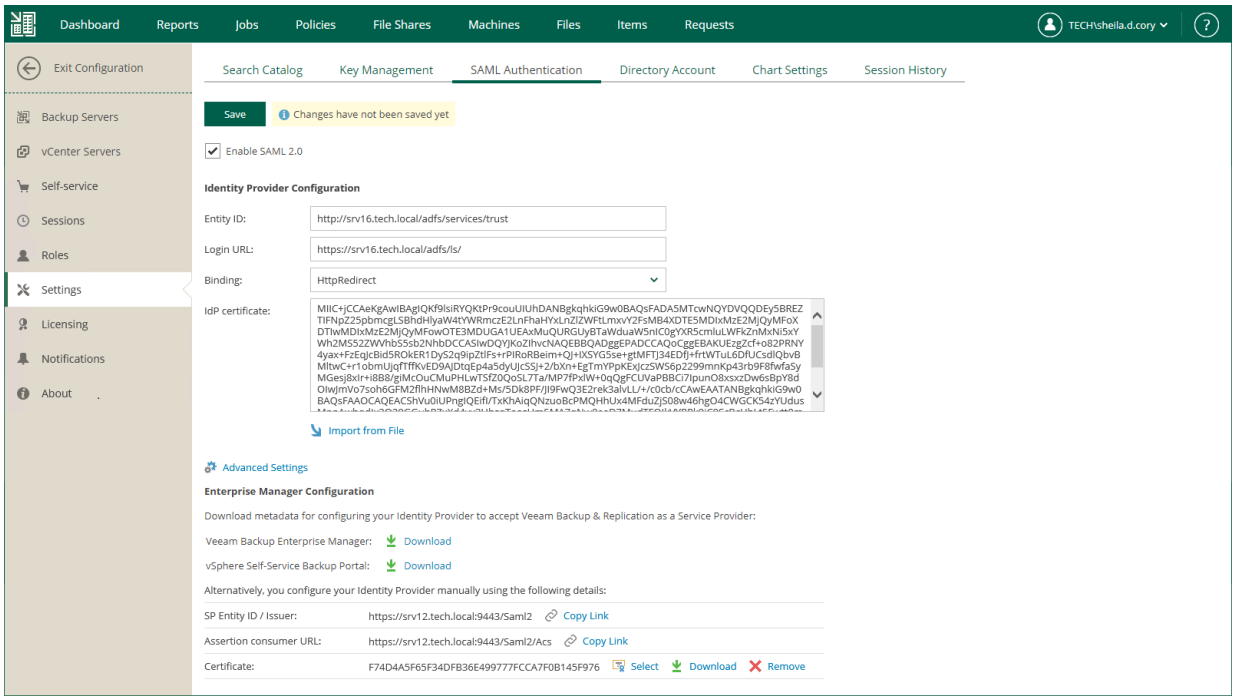
- Import identity provider settings from a SAML metadata file obtained from the identity provider.
- Specify identity provider settings manually.

To import identity provider settings from the SAML metadata file, in the **Identity Provider Configuration** section of the **SAML Authentication** view, click the **Import from File** link and browse to the metadata file. The metadata file structure must conform to the SAML 2.0 Metadata Schema.

Alternatively, you can specify identity provider settings manually:

1. In the **Identity Provider Configuration** section, in the **Entity ID** field, specify a unique ID of the identity provider.
2. In the **Login URL** field, specify the URL of the single sign-on login page provided by the identity provider.
3. From the **Binding** list, select a SAML binding used by the identity provider to send SAML responses: *HttpRedirect* or *HttpPost*.
4. In the **IdP certificate** field, specify a certificate that will be used to validate the signature of the signed authentication assertions and decrypt assertions sent by the identity provider.

> **NOTE**
>
> Veeam Backup Enterprise Manager does not support identity provider certificate rollover.



Selecting Service Provider Certificate

If you want to sign and encrypt authentication requests sent from Veeam Backup Enterprise Manager to the identity provider, you must select a certificate with a private key that will be used for encryption and signing. To select a certificate:

1. In the **Enterprise Manager Configuration** section of the **SAML Authentication** view, click the **Select** link next to the **Certificate** field.
2. In the **Select Service Provider Certificate** window, Veeam Backup Enterprise Manager will display certificates located in the certificate store on the Enterprise Manager server. Choose the necessary certificate from the list and click **Select**.

If you use a certificate to sign end encrypt SAML authentication requests, you must pass the public key certificate to the identity provider. The identity provider will use this certificate to encrypt requests and validate the request signature. For more information, see Obtaining Service Provider Settings.

TIP

Consider the following:

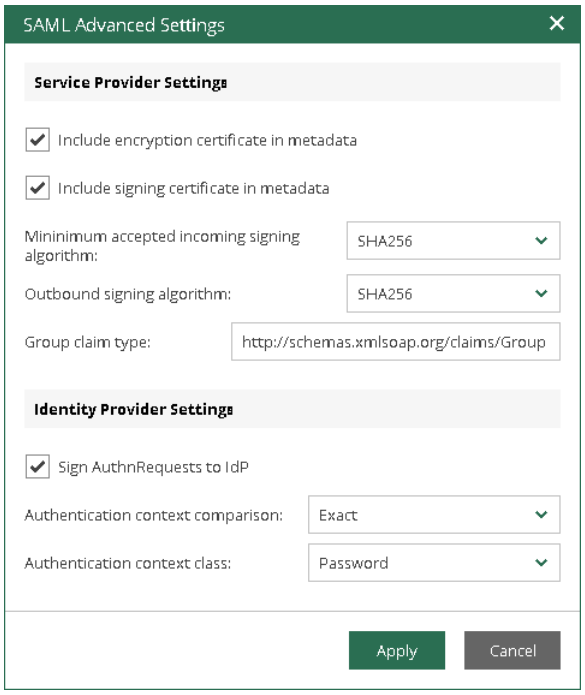
- To change the service provider certificate, click the **Remove** link next to the **Certificate** field. Then select another certificate from the certificate store.
- You can choose whether to include the certificate in the service provider metadata. For more information, see Specifying Advanced SAML Authentication Settings.

Specifying Advanced SAML Authentication Settings

In the **SAML Advanced Settings** window you can specify advanced settings for SAML authentication.

1. To include in the service provider SAML metadata a security certificate required to decrypt service provider authentication requests, select the **Include encryption certificate in metadata** check box.
2. To validate the signature of the signed requests, select the **Include signing certificate in metadata** check box.
3. From the **Minimum accepted incoming signing algorithm** and **Outbound sign algorithm** lists, select what type of signed requests and responses Enterprise Manager will be able to send and receive. By default, the *SHA256* option is selected. With this option selected, Enterprise Manager will send and receive requests and responses signed using the SHA256 or stronger algorithm.
4. By default, to provide for single sign-on authentication for groups of users, Veeam Backup Enterprise Manager accepts information about groups from the identity provider in statements of the *Group* type. If it is required to use for this purpose statements of a different type, in the **Group claim type** field, specify the necessary type.
5. If you want to sign authentication requests sent from Enterprise Manager to the identity provider with a digital certificate, in the **Identity Provider Settings** section, select the **Sign AuthnRequests to IdP** check box.
6. From the **Authentication context comparison** list, select a comparison method for authentication context: *Exact*, *Minimum*, *Maximum* or *Better*.
7. From the **Authentication context class** list, select one of the classes to specify an authentication method used by the Identity Provider. For example, for VMware Platform Services Controller, select *PasswordProtectedTransport*. By default, the *Password* option is selected.

8. Click **Apply**.



Obtaining Service Provider Settings

To set up SAML authentication for the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal, you need to register each of them individually as a service provider on the identity provider side. To do this, you need to obtain service provider settings and pass them to the identity provider.

You can obtain service provider settings in one of the following ways:

- Export service provider settings to an XML file
- Copy service provider settings

Exporting Service Provider Settings

You can export settings of each service provider to a SAML metadata file — an XML file that conforms to the SAML 2.0 Metadata Schema. If you plan to use a certificate to sign end encrypt SAML authentication requests, and need to pass the public key certificate to the identity provider, you must include the certificate in the metadata file. For more information, see Specifying Advanced SAML Authentication Settings.

- To export service provider settings of the Veeam Backup Enterprise Manager website, click the **Download** link next to the **Veeam Backup Enterprise Manager** field.
- To export service provider settings of vSphere Self-Service Backup Portal, click the **Download** link next to the **vSphere Self-Service Backup Portal** field.

Copying Service Provider Settings

To copy service provider settings:

1. Copy the links next to the **SP Entity ID / Issuer** and **Assertion consumer URL** fields.
2. If you have selected a certificate that will be used to sign end encrypt SAML authentication requests, you must also pass the public key certificate to the identity provider. To copy the certificate, click the **Download** link next to the **Certificate** field.

Updating Security Certificate

Security certificate ensures secure connection with the Veeam Backup Enterprise Manager website using HTTPS. You can specify path to existing certificate or generate a new self-signed certificate during Enterprise Manager installation. In case of installing on the same machine with Enterprise Manager, this certificate will be also used by Veeam plug-in for vSphere Web Client and REST API client to receive data using HTTPS protocol.

- To update the Enterprise Manager certificate, you can use Internet Information Services (IIS) Manager. For more information, see this Microsoft Docs article.
- To update the Enterprise Manager REST API certificate, use the `netsh` command. For more information, see the TLS Certificate section of the Veeam Backup Enterprise Manager REST API Reference.

Configuring Notification Settings

You can configure Veeam Backup Enterprise Manager to send email notifications.

To receive email notifications, configure SMTP server settings. For more information, see Email Server Settings.

After that, you can switch on or off the necessary notifications. You can configure the following notifications:

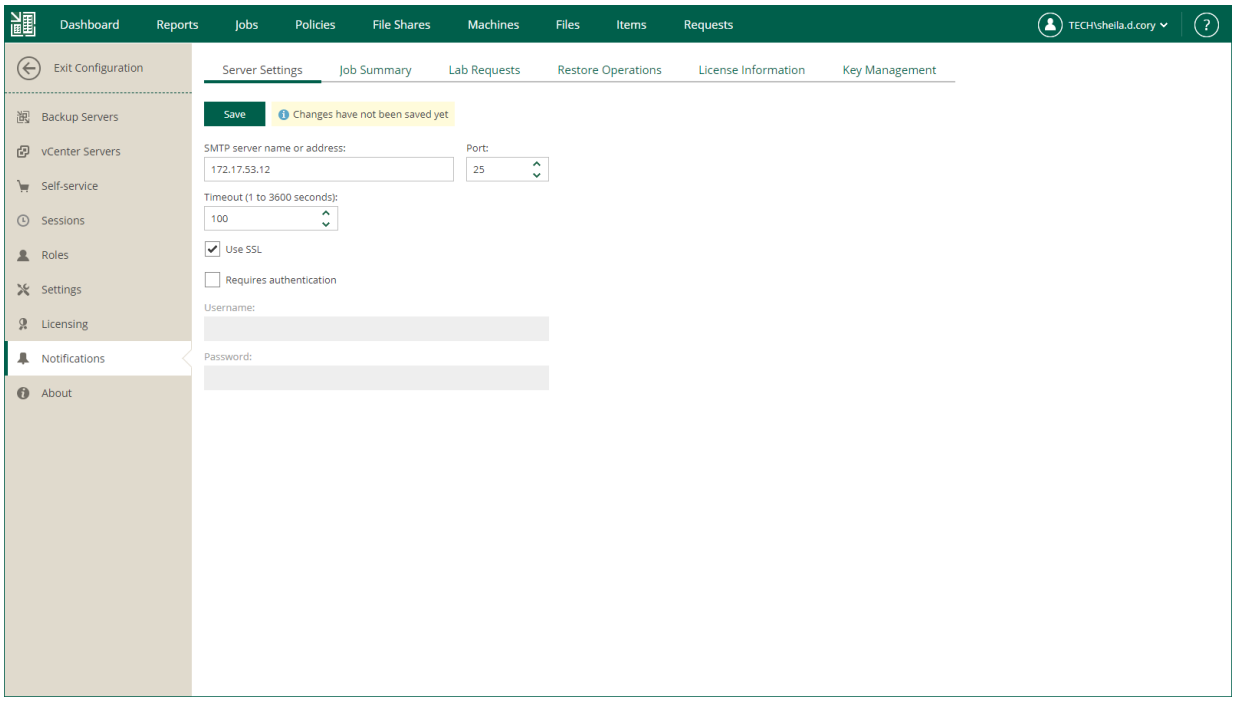
- Job Summary
- Lab Requests
- Restore Operations
- License Information
- Key Management

Email Server Settings

SMTP server is a server that is used for sending emails to the specified email address.

To configure email server settings:

1. Open the **Notifications** section of the **Configuration** view.
2. On the **Server Settings** tab, specify a full DNS name or IP address of the SMTP server. If necessary, change the port number that will be used to communicate with the mail server. The default port number is **25**.
3. In the **Timeout** field, specify a timeout for email server — this should be a value from 1 to 3600 seconds. Default is **100** seconds.
4. If the SMTP server requires SSL connection, select the **Use SSL** check box.
5. If the SMTP server requires authentication, select the **Requires authentication** check box and specify authentication credentials.
6. Click **Save**.



Notifications on Job Results

You can configure Veeam Backup Enterprise Manager to send daily notification emails with the results of finished jobs. The notification email contains a report about the number of jobs performed with the *Error*, *Warning* and *Success* statuses, and provides a link to the Veeam Backup Enterprise Manager web UI so that you can see jobs statistics in detail.

To receive daily email notifications about job results, do the following:

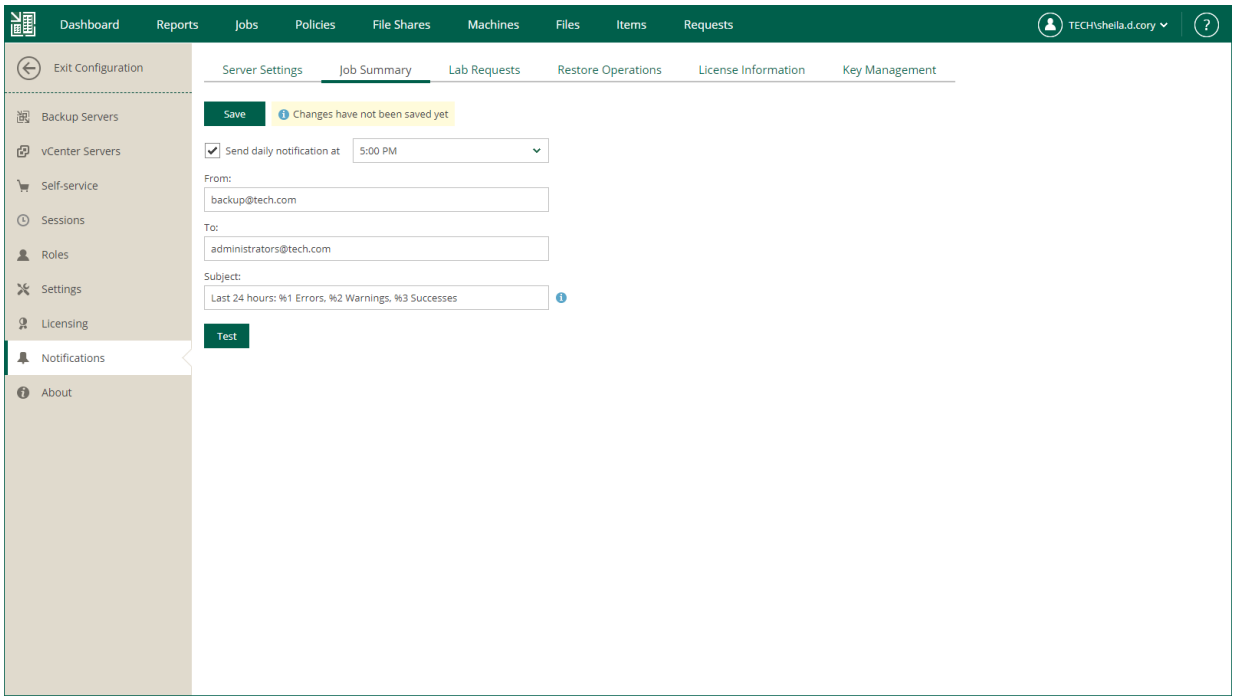
1. Open the **Notifications** section of the **Configuration** view.
2. Open the **Job Summary** tab.
3. Select the **Send daily notification at** check box and specify the time when you want a notification email to be sent.
4. In the **From** field, enter an email address of the notification sender.
5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. In the **Subject** field, enter a subject of email notifications. You can use the following variables in the subject:
   - %1 — number of jobs that ended with errors for the last 24 hours
   - %2 — number of jobs that ended with warnings for the last 24 hours
   - %3 — number of jobs that ended successfully for the last 24 hours

     Job retries performed in the last 24 hours are also included in the report.
   - %4 — number of jobs whose last session ended with an error.
   - %5 — number of jobs whose last session ended with a warning.
   - %6 — number of jobs whose last session ended successfully.

     Jobs which were in *Disabled* state during the last session are also included in the report.
7. Click **Save**.

TIP

To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.



Notifications on Lab Requests

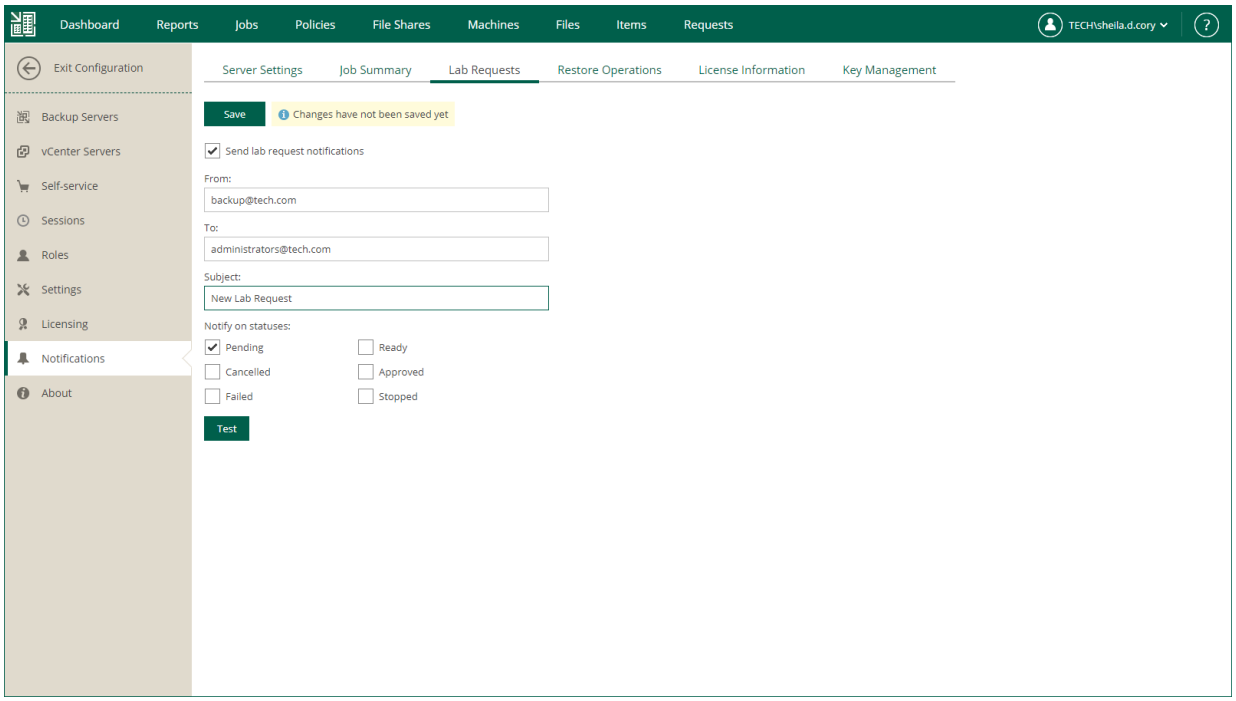
You can configure Veeam Backup Enterprise Manager to send notification emails about virtual lab requests created by users who need to perform universal application item-level restore.

To receive notifications about lab requests, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **Lab Requests** tab.
3. Select the **Send lab request notifications** check box.
4. In the **From** field, enter an email address of the notification sender.
5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Specify the subject of the email message.
7. Select request statuses for a report. The notification email will be sent if the request is **Pending**, **Ready**, **Canceled**, **Approved**, **Failed** or **Stopped**.
8. Click **Save**.

> **TIP**
>
> To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.

For more information about the universal application item-level restore, see Veeam Universal Application Item Recovery Guide.



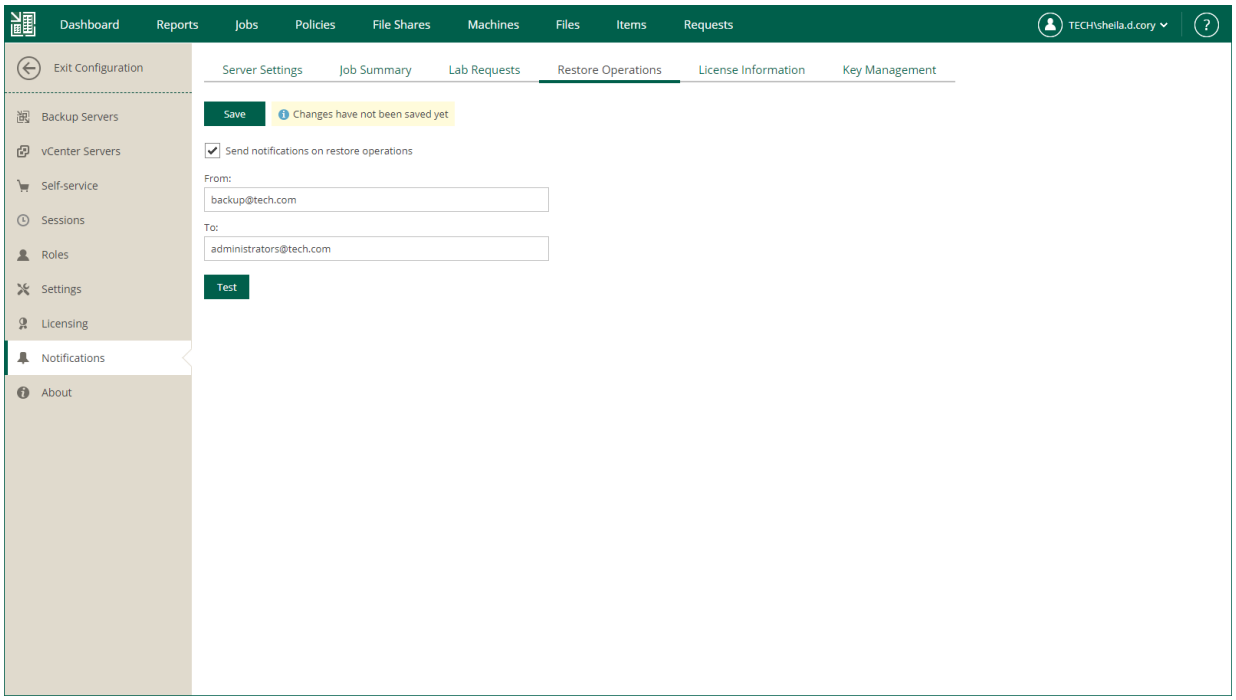
Notifications on Restore Operations

You can configure Veeam Backup Enterprise Manager to send notification emails about performed file restore operations.

To receive notifications about performed file restore operations, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **Restore Operations** tab.
3. Select **Send notifications on restore operations**.
4. In the **From** field, enter an email address of the notification sender.
5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Click **Save**.

> **TIP**
>
> To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.



Notifications on Licensing

You can configure Veeam Backup Enterprise Manager to send the following email notifications:

- Notifications on product updates
- [For perpetual licenses] Notifications on support contract expiration
- [For rental licenses] Notifications on license usage

Notifications on Product Updates

By default, Veeam Backup Enterprise Manager checks periodically and notifies you about new product versions and patches available on the Veeam website. Leave the update notifications enabled so you do not miss critical updates and patches.

To disable notifications on product updates:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **License Information** tab.
3. Select the **Check for product and hypervisor updates periodically** check box.

Notifications on Support Contract Expiration

If you have a perpetual license installed and your support contract is expired, Veeam Backup Enterprise Manager adds the *SUPPORT EXPIRED* prefix to the subject of all its email messages. You can configure Enterprise Manager to remove the prefix.

To remove the *SUPPORT EXPIRED* prefix from the message subject:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **License Information** tab.
3. Select the **Disable support contract expiration notifications** check box.

Notifications on License Usage

If you have a rental license installed, you can configure Veeam Backup Enterprise Manager to send email notifications on license usage. Every notification contains a monthly usage report about instances used for backup and replication in the previous month. For more information on the reports, see Managing Monthly Usage Reports.

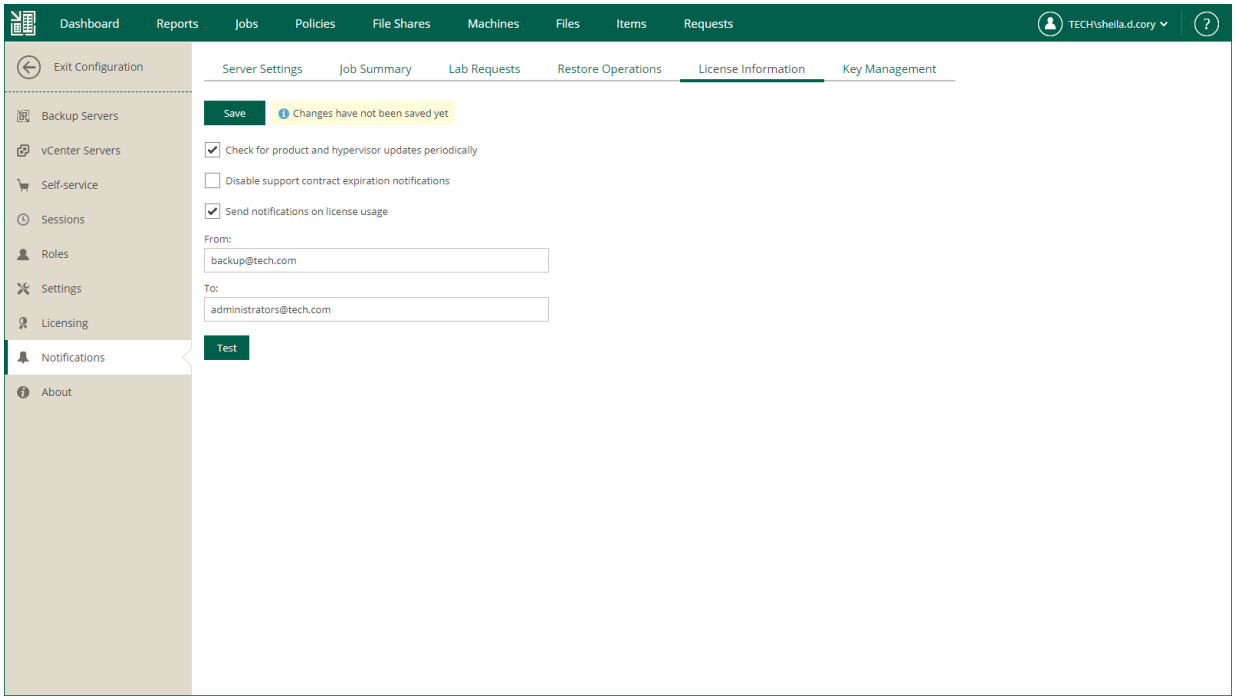
Enterprise Manager sends notifications on license usage on the first day of the month. If Veeam Backup & Replication does not perform any backup and replication jobs for the whole month, Enterprise Manager does not send the notifications.

To enable email notifications on license usage:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **License Information** tab.
3. Select the **Send notifications on license usage** check box.
4. In the **From** field, enter an email address of the notification sender.

5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Click **Save**.

> **TIP**
>
> To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email message to all specified email addresses.



Notifications on Key Management

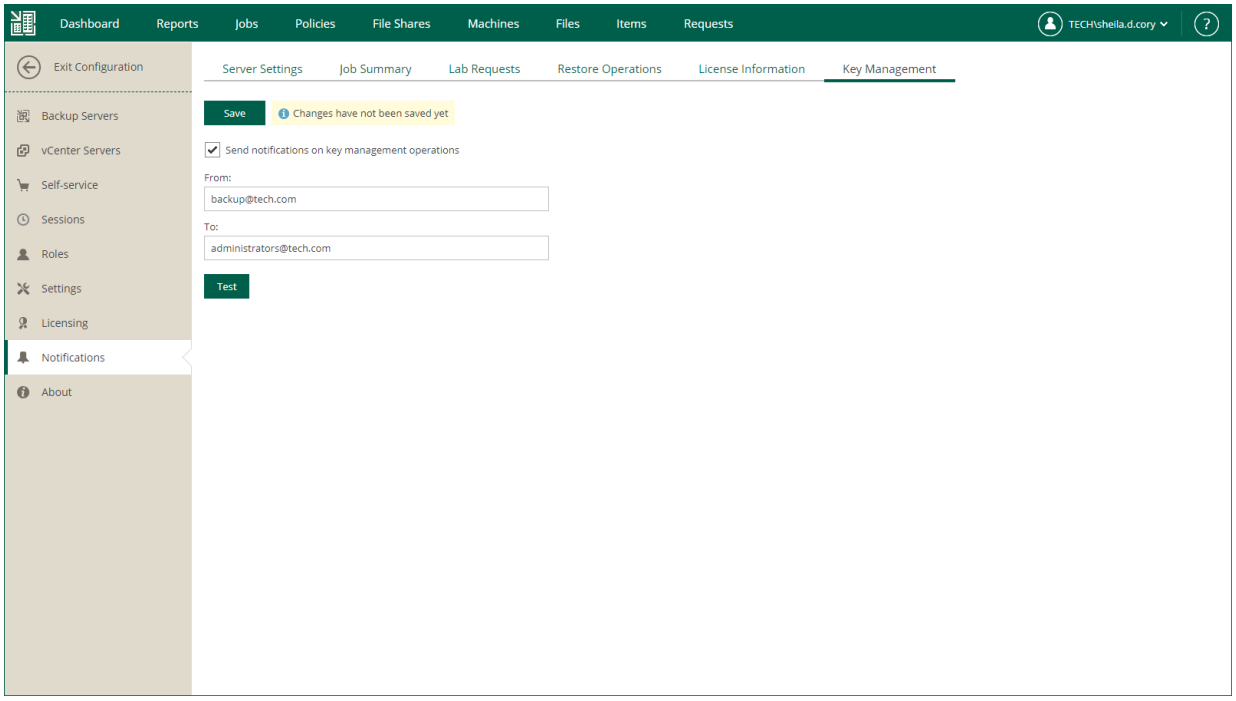
Veeam Backup Enterprise Manager allows you to perform operations with encryption keys. For more information, see Managing Encryption Keys.

You can configure Enterprise Manager to send notifications about the following key management operations: key expiration, key deletion, key modification.

To receive key management notifications, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **Key Management** tab.
3. Select the **Send notifications on key management operations** check box.
4. In the **From** field, enter an email address of the notification sender.
5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Click **Save**.

> **TIP**
>
> To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.



Viewing Information About Enterprise Manager

You can view detailed information about Enterprise Manager and its components, URLs of REST API and Veeam Self-Service File Restore Portal, as well as the paths to the Enterprise Manager logs.

To view information about Enterprise Manager:

1. Log in to Enterprise Manager using an administrative account.
2. Open the **About** section of the **Configuration** view.

The Enterprise Manager log files are available at the following paths:

- Veeam Backup Enterprise Manager Service logs

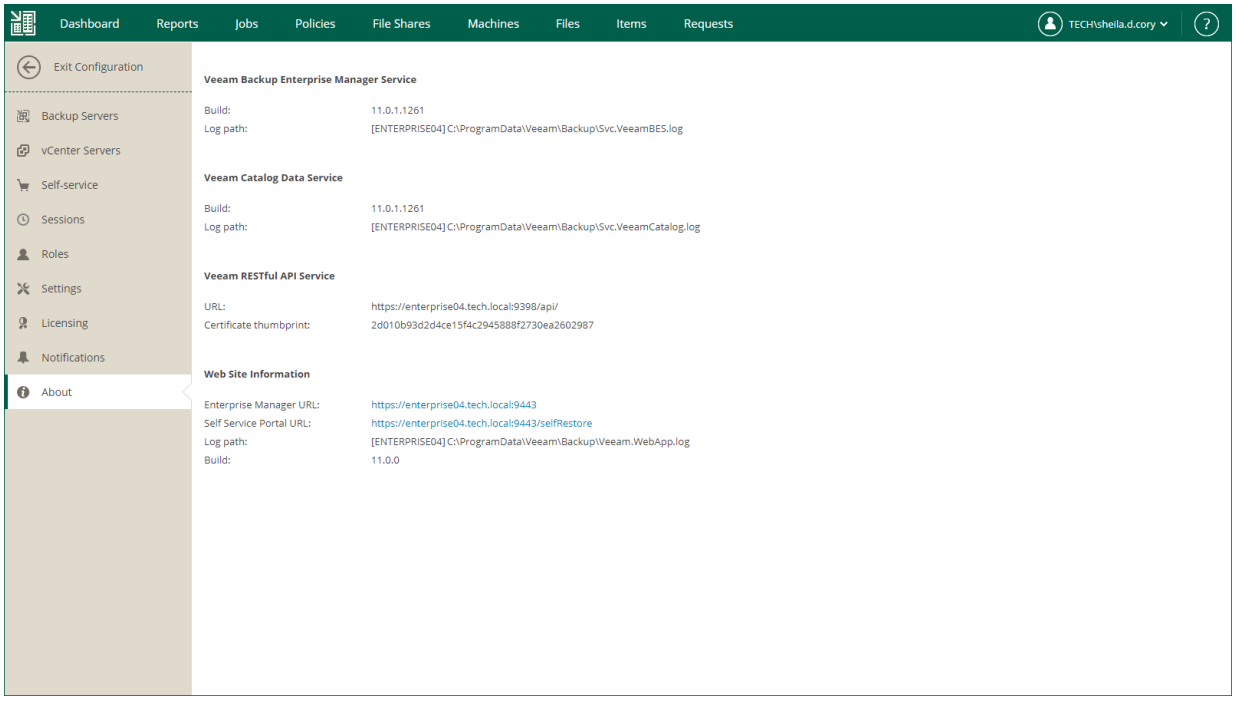
```
C:\ProgramData\Veeam\Backup\Svc.VeeamBES.log
```

- Veeam Guest Catalog Service logs

```
C:\ProgramData\Veeam\Backup\Svc.VeeamCatalog.log
```

- Enterprise Manager website logs

```
C:\ProgramData\Veeam\Backup\Veeam.WebApp.log
```



Managing Languages

Veeam Backup Enterprise Manager interface is available in several languages. You can select a language for the following Veeam Backup Enterprise Manager components:

- Veeam Backup Enterprise Manager website
- Veeam Self-Service Backup Portal
- vSphere Self-Service Backup Portal

Available Languages

Veeam Backup Enterprise Manager is available in the following languages:

- Chinese (Simplified, PRC)
- English
- French
- German
- Italian
- Japanese
- Spanish

Selecting Language

The first time you visit one of the Veeam Backup Enterprise Manager components, the content is displayed in the language of your browser. If the website does not support the browser language, the interface is displayed in English.

You can select a preferred language from the drop-down list on the login page. If the language you need is not available, you can add it. For more information, see Adding Languages.

Language Files Overview

To support multiple languages, Veeam Backup Enterprise Manager uses the GNU gettext tools. Veeam Backup Enterprise Manager languages are stored in POT, JSON and PO files. The files are located in the `lang` folder on the Enterprise Manager server. By default, the path to the folder is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

All files names must follow the naming conventions. For more information, see File Names.

File Formats

Enterprise Manager languages are stored in text files of the following formats:

- POT files that contain UI texts in the source language. The source language of Enterprise Manager is English.
- [Optional] PO files that contain UI texts as pairs of strings: source string and its translation. Each language is stored in a separate file. You can create PO files from the POT files and use them in the translation process. After you finish the translation, you must convert PO files to the JSON format.
- JSON files that contain UI texts as pairs of strings: source string and its translation. Enterprise Manager uses these files to display the interface in a language other than English.

File Names

In order for Veeam Backup Enterprise Manager to recognize files within the `lang` folder as language files, their names must follow the naming conventions.

POT files must have the following names:

- `messages.pot` — file used for the Veeam Backup Enterprise Manager website
- `vcloud_messages.pot` — file used for Veeam Self-Service Backup Portal
- `vsphere_messages.pot` — file used for vSphere Self-Service Backup Portal

JSON files must have the following names:

- `messages.<code>.json` — file used for the Veeam Backup Enterprise Manager website
- `vcloud_messages.<code>.json` — file used for Veeam Self-Service Backup Portal
- `vsphere_messages.<code>.json` — file used for vSphere Self-Service Backup Portal

where `<code>` is an ISO 639-1 code that represents the language. The code consists of a two-letter lowercase culture code and optional two-letter uppercase region code. For example: `en`, `fr-CA`, `fr-FR`, `pt-BR` or `pt-PT`.

Adding Languages

Veeam Backup Enterprise Manager is available in several languages. If the language you need is not available, you can add it. Before you start adding new languages, check whether the languages are supported by the server where Veeam Backup Enterprise Manager is deployed.

To check whether a language is supported, run the following command:

```
New-Object -TypeName 'System.Globalization.CultureInfo' -ArgumentList "<code>"
```

where `<code>` is an ISO 639-1 code that represents the language. The code consists of a two-letter lowercase culture code and optional two-letter uppercase region code. For example: `en`, `fr-CA`, `fr-FR`, `pt-BR` or `pt-PT`.

To add new languages:

1. Translate source UI texts to the new languages.

   For more information, see Translating Source Texts.

2. Convert the translation files.

   For more information, see Converting PO to JSON.

3. Save the translation files to the `lang` folder. The default path is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

   > **IMPORTANT**
   >
   > Make sure the JSON translation files are named as follows: `messages.xx.json`, `vcloud_messages.xx.json`, `vsphere_messages.xx.json`. For more information on file naming, see File Names.

4. In IIS Manager, restart the VeeamBackup website and recycle the VeeamBackup application pool. For more information, see the Site <site> and Recycling Settings for an Application Pool <recycling> sections of Microsoft Docs.

Translating Source Texts

Source texts are stored in POT files. The files are located in the `lang` folder on the Enterprise Manager server. By default, the path to the folder is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

To translate source texts:

1. Get the source files from the `lang` folder:

   - `messages.pot`
   - `vcloud_messages.pot`
   - `vsphere_messages.pot`

   For more information on file names and formats, see Language Files Overview.

2. For each language, create PO files using the POT files as templates.

   For more information, see this GNU gettext article.

3. Name the PO files as follows:

   - `messages.<code>.po`
   - `vcloud_messages.<code>.po`
   - `vsphere_messages.<code>.po`

   For more information, see File Names.

4. Translate PO files in a text editor or a CAT tool.

   For more information on PO files, see PO File Structure.

   > **TIP**
   >
   > Although PO files are not used by Veeam Backup Enterprise Manager, you can save them in the `lang` folder to keep them together with other language files.

PO File Structure

Each PO file contains the following elements:

- Header
- Translation entries

Header

Header contains meta data of the PO file: language code in the ISO 639-1 format, content type and encoding, and plural form information.

Parameter	Description
Language	ISO 639-1 code of the translation language.
MIME-Version	MIME version. Set it to *1.0*.
Content-Type	Content type and character encoding used for the translation language. Set the type value to *text/plain*.You can use the UTF-8 encoding for any language.
Content-Transfer-Encoding:	Content transfer encoding. Set the value to *8bit*.
Plural-Forms	Number of plural forms and the plural form formula of the translation language.

For example:

```
"Project-Id-Version: \n"
"POT-Creation-Date: \n"
"PO-Revision-Date: \n"
"Language-Team: \n"
"Language: de\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=UTF-8\n"
"Content-Transfer-Encoding: 8bit\n"
"Plural-Forms: nplurals=2; plural=(n != 1);\n"
"X-Generator: \n"
```

For more information on the PO header, see this GNU gettext article.

Translation entries

In a PO file, translation entries are separated with a blank string. Each entry consists of the following elements:

- `msgid` — string in the source language
- [Optional] `msgid_plural` — plural form of the `msgid` string
- `msgstr` — string in the translation language

Before you begin translating, consider the following:

- Do not modify `msgid` strings. They are references to the source code. Veeam Backup Enterprise Manager uses them to find their translation.
- If an `msgid` string contains variables, do not translate them.

  Variables are placed inside braces. For example, the following entry contains the `restoreItemsCount` variable:

  ```
  msgid "Pending restore ({restoreItemsCount} items)"
  msgstr "Ausstehende Wiederherstellung ({restoreItemsCount} Elemente)"
  ```

- If an `msgid` string is followed by its plural form `msgid_plural`, provide translation for each form.

  For example:

  ```
  msgid "${ pointsCount } point"
  msgid_plural "${ pointsCount } points"
  msgstr[0] "${ pointsCount } Punkt"
  msgstr[1] "${ pointsCount } Punkte"
  ```

  For more information on translating plural forms, see this GNU gettext article.

Converting PO to JSON

Veeam Backup Enterprise Manager loads translated strings from JSON files. After you finish translating PO files, convert them to the JSON format.

To convert a file from the PO format to the JSON format, use the `Veeam.Backup.Localization.PoConverter.exe` utility.

1. To locate the utility, use the `cd` command. By default, the utility is located in the Enterprise Manager folder.

   ```
   cd '<path>'
   ```

   where `<path>` is a path to the utility file.

   For example:

   ```
   cd 'C:\Program Files\Veeam\Backup and Replication\Enterprise Manager'
   ```

2. Run the utility with the following command:

   ```
   .\Veeam.Backup.Localization.PoConverter.exe '<po_file>'
   ```

   where `<po_file>` is a path to the PO file.

   For example:

   ```
   .\Veeam.Backup.Localization.PoConverter.exe 'C:\Program Files\Veeam\Backup
   and Replication\Enterprise Manager\WebApp\scripts\build\production\resourc
   es\lang\messages.zh_CN.po'
   ```

The JSON file will be created in the folder of the PO file.

> **TIP**
>
> To view help for the Veeam.Backup.Localization.PoConverter.exe utility, run the utility with the `/help` parameter.

Managing Jobs

Veeam Backup Enterprise Manager acts as a single point for managing jobs from all added backup servers. Users with the Portal Administrator role can centrally manage jobs that have been previously configured on added backup servers: start, stop, retry, clone, delete jobs and edit selective job settings.

Consider the following limitations:

- For Nutanix AHV VMs, Enterprise Manager displays only backup copy jobs.
- For physical machines, Enterprise Manager displays the following job types:
  - Backup copy jobs.
  - Veeam Agent backup jobs managed by the backup server. For more information, see Support for Veeam Agents.

Viewing Jobs

From Veeam Backup Enterprise Manager, you can view information about jobs configured on all backup servers added to Enterprise Manager. To view the jobs, open the **Jobs** tab. Every job in the list is described with the following data: job name, type, platform of the objects it processes, backup server on which the job was created, current job status, date of the latest run, date of the next run (if the job is scheduled) and job description.

To quickly find a job, you can use filters and the search field.

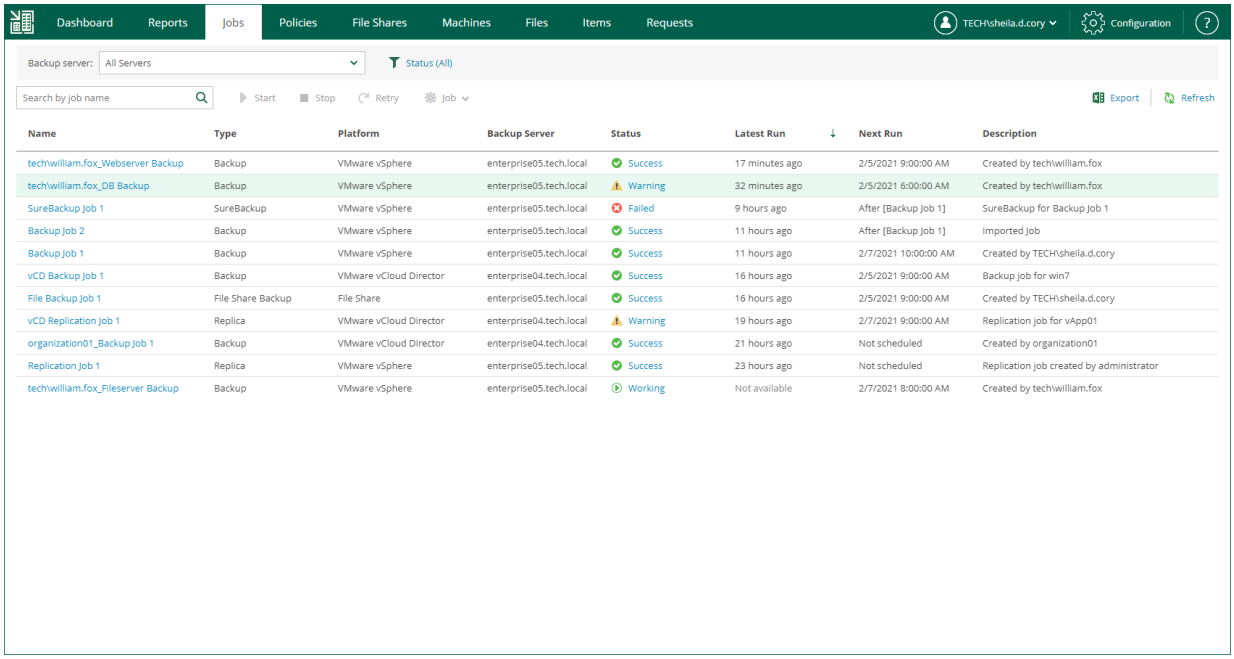
- To filter the list of jobs:
  - Use the **Backup server** drop-down list to view the jobs of the selected backup server only.
  - Use the **Status** filter to view the jobs with the selected job statuses.

    Once you have selected necessary statuses, click the **Apply** button to apply the filter.
- To find a job by its name, use the search field.

Besides the information presented in the list of jobs, the **Jobs** tab allows you to view advanced job data:

- To see a list of job sessions, click the job name link in the **Name** column.
- To see detailed statistics on the last job run, click the state link in the **Status** column.

> **NOTE**
>
> You can export displayed information to a file using the **Export** link on the toolbar. This file then can be opened on the client machine using the associated application.



Starting, Stopping and Retrying Jobs

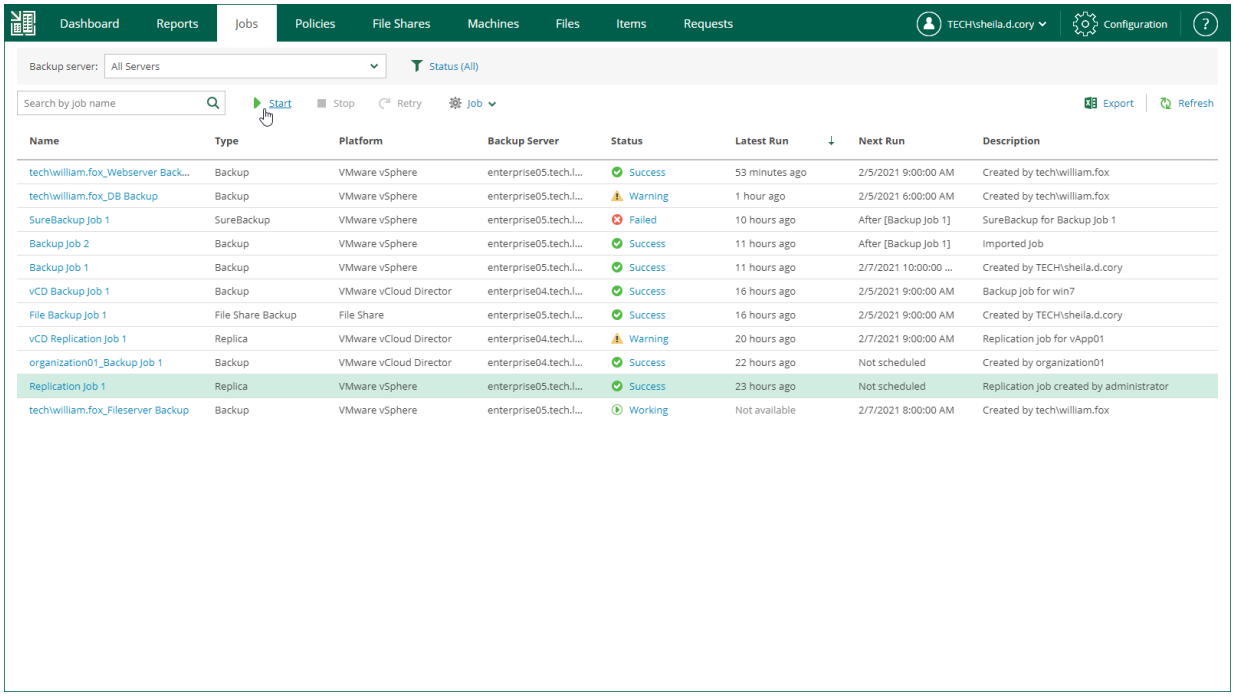
Users with the Portal Administrator role can control backup and replication jobs without the need to access the Veeam Backup & Replication console on the backup server.

On the **Jobs** tab, you can start, stop or retry a job.

- To start a job, select the job from the list and click **Start**.
- To stop a job, select the job from the list and click **Stop**.
- To retry a failed job, select the job from the list and click **Retry**.

NOTE

- For more information on starting a backup copy job, see the Starting Backup Copy Jobs Manually section of the Veeam Backup & Replication User Guide.
- For more information on starting and stopping an Oracle or SQL server backup job with transaction log processing enabled, see the Starting and Stopping Transaction Log Backup Jobs section of the Veeam Backup & Replication User Guide.



Enabling and Disabling Jobs

Veeam Backup Enterprise Manager allows you to enable and disable jobs of the following types:

- Scheduled backup jobs

  Disabled backup jobs do not start by the specified schedule. When you disable a job that backs up Microsoft SQL Server or Oracle VMs, transaction log processing (if enabled for that job) will be also disabled.

- Scheduled replication jobs

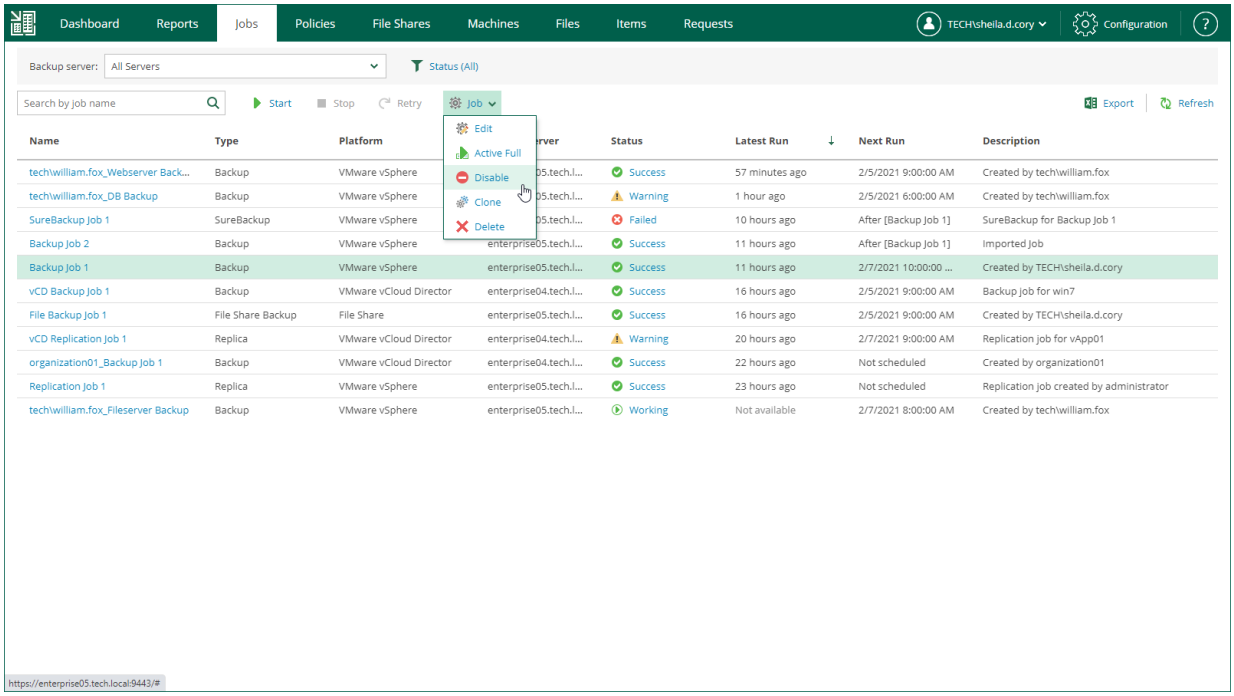
  Disabled replication jobs are not started by the specified schedule.

- Backup copy jobs

  Disabled backup copy jobs do not monitor source backup repositories and do not copy restore points to the target backup repository.

To enable or disable a job:

1. On the **Jobs** tab, select a job from the list.
2. On the toolbar, click **Job**.
3. Select **Enable** or **Disable** from the list of commands.



Editing Jobs

Users with the Portal Administrator role can modify settings of VMware and Hyper-V backup and replication jobs that have been previously configured on backup servers connected to Veeam Backup Enterprise Manager. In Enterprise Manager, you can change only a subset of the job settings. To edit other job settings, use the Veeam Backup & Replication console.

IMPORTANT

- You can edit jobs if you have an Enterprise or Enterprise Plus license installed.
- From Veeam Backup Enterprise Manager, you cannot edit jobs that are managed by backup servers of earlier versions as well as Veeam Agent backup jobs, file share backup jobs, and backup copy jobs. To edit settings of such jobs, use the Veeam Backup & Replication console.

In Veeam Backup Enterprise Manager, you can change the following job settings:

- Change a job name, description and retention settings for the restore points.
- Manage a list of machines that the job should process (add and remove machines or containers, exclude individual machines from containers, change the order in which the job will process machines).
- Configure guest processing settings.
- Change a job schedule.

The changes take effect with the next job run.

NOTE

If the *Location* properties of the source object and target object do not match, you will receive a warning message after you finish editing. For example, you may have a backup job targeted at repository located in Sydney, and source machines located in London.

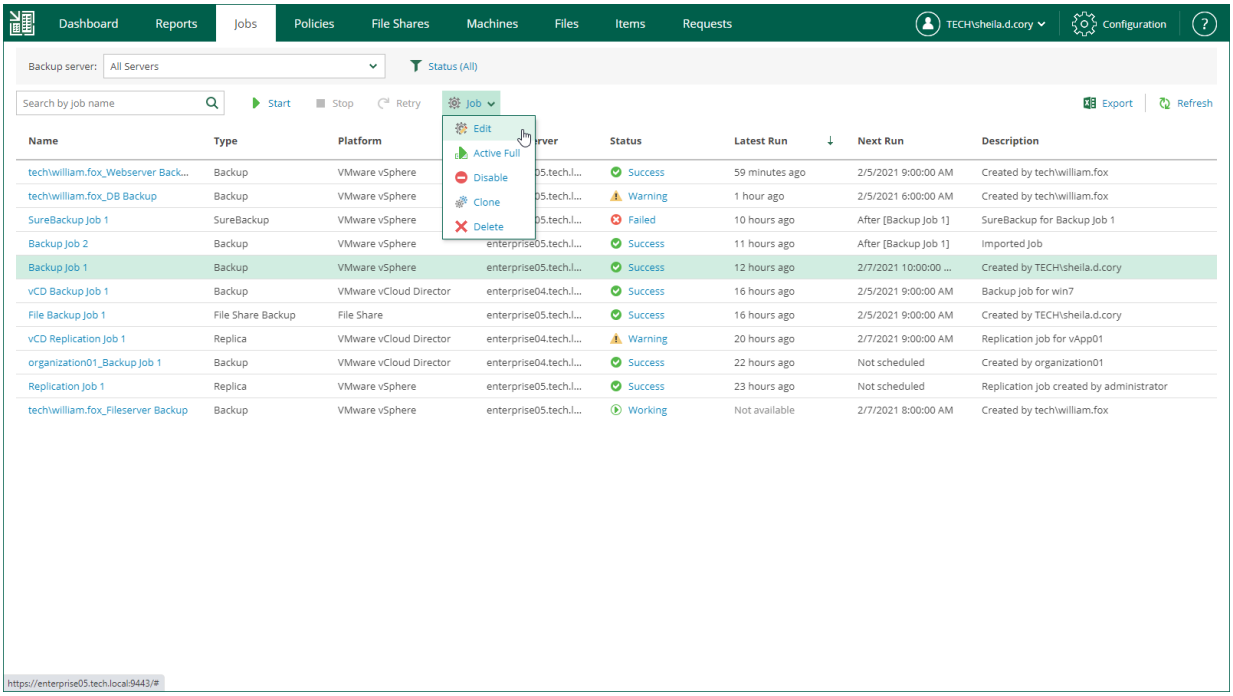
To edit a job, use the **Edit Backup Job** (or **Edit Replication Job**) wizard.

1. Launch the wizard for job editing
2. Edit job name and retention settings
3. Edit the list of VMs
4. Change the VM processing order
5. Configure guest processing settings
6. Edit job scheduling settings

Step 1. Launch Wizard

To launch the wizard for job editing:

1. Open the **Jobs** tab and select the necessary job in the list.
2. On the toolbar, click **Job** to expand the list of available actions.
3. Select **Edit**.

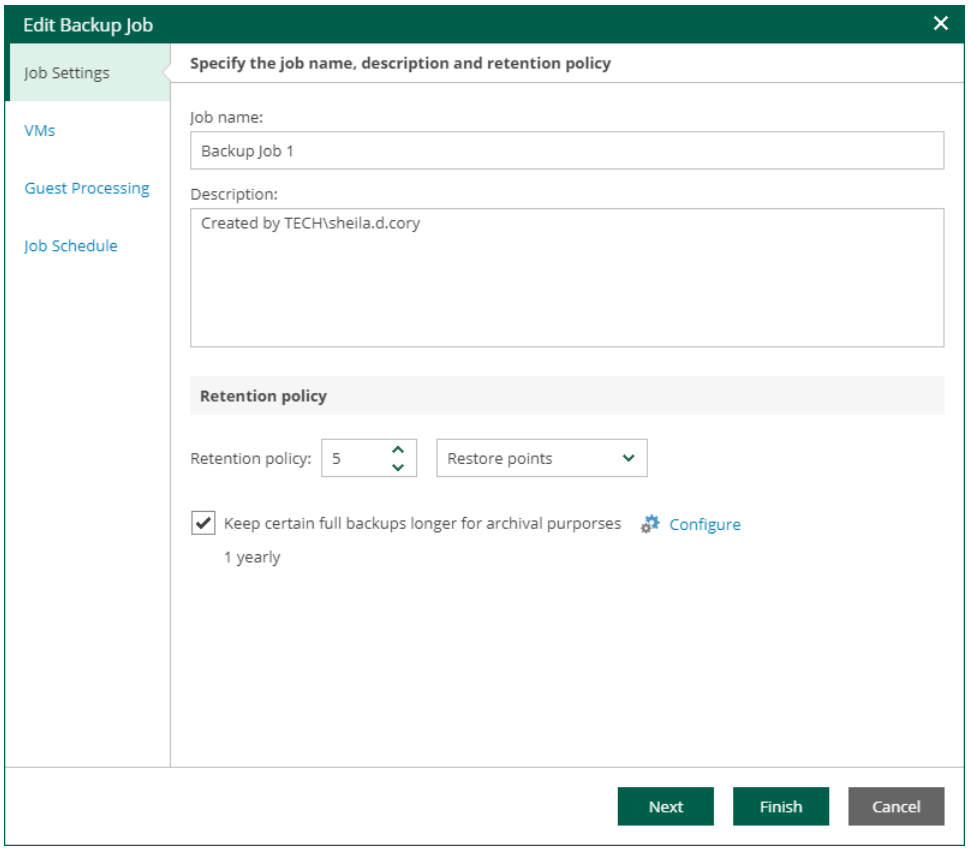


Step 2. Edit Job Name and Retention Settings

At the **Job Settings** step of the wizard, you can modify name and description for the selected job, as well as its retention policy.

1. In the **Job name** field, enter a name for the job.
2. In the **Description** field, provide an optional description for future reference. The default description contains information about the user who created the job, date and time when the job was created.
3. Specify backup retention policy settings:
   - From the **Retention policy** list, select *Restore points* and specify the number of restore points that you want to store in the backup repository. When this number is exceeded, the earliest restore point will be removed from the backup chain.
   - From the **Retention policy** list, select *Days* and specify the number of days for which you want to store restore points in the backup repository. After this period is over, a restore point will be removed from the backup chain.

   For more information on retention, see the Short-Term Retention Policy section of the Veeam Backup & Replication User Guide. Also, see this Veeam KB article.
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how often full backups are retained. For more information, see the Long-Term Retention Policy (GFS) section of the Veeam Backup & Replication User Guide.



Step 3. Edit List of VMs

At the **Virtual Machines** step of the wizard, you can add or remove individual VMs or VM containers, for example, entire hosts or clusters. Jobs with VM containers are dynamic in their nature: if a new machine is added to the container after the job is created, the job is automatically updated to include the added machine.

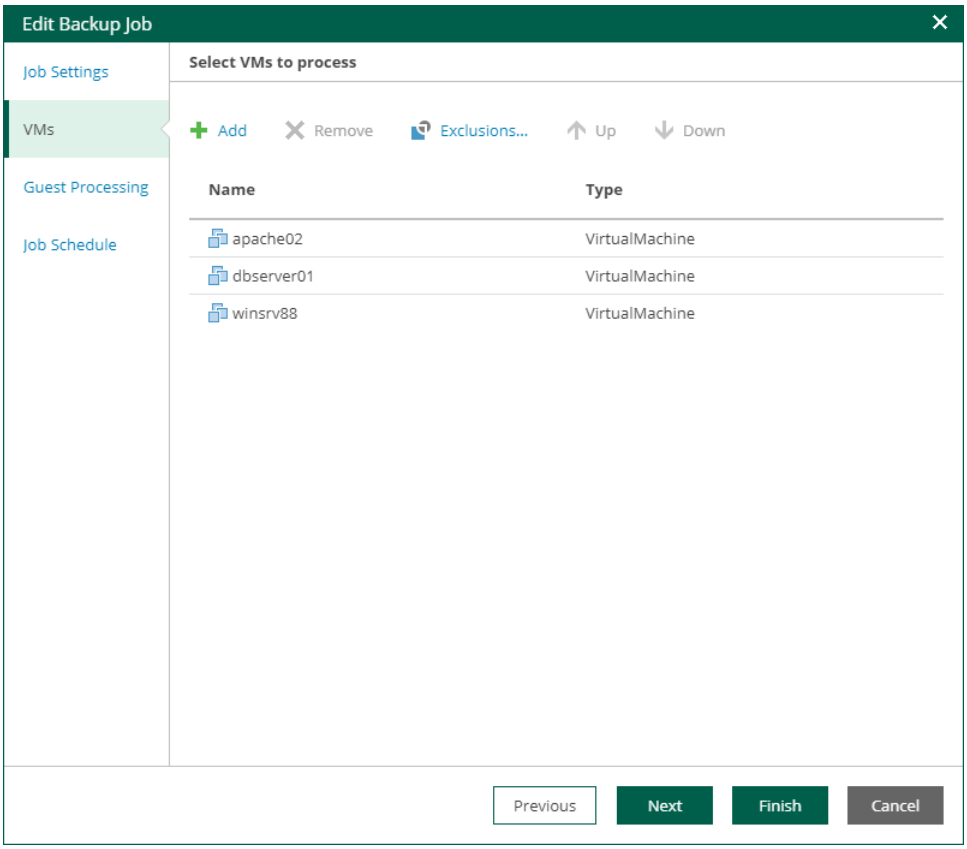
NOTE

- For vCD backup jobs, you can add and remove the following vCD objects: VMs, vApps, organization vDCs, organizations and the vCD instance. The scope depends on your vCD access rights.
- For vCD replication jobs, you cannot add or remove single VMs. You can manage only vApps and other vCD containers.

Adding VMs and VM containers

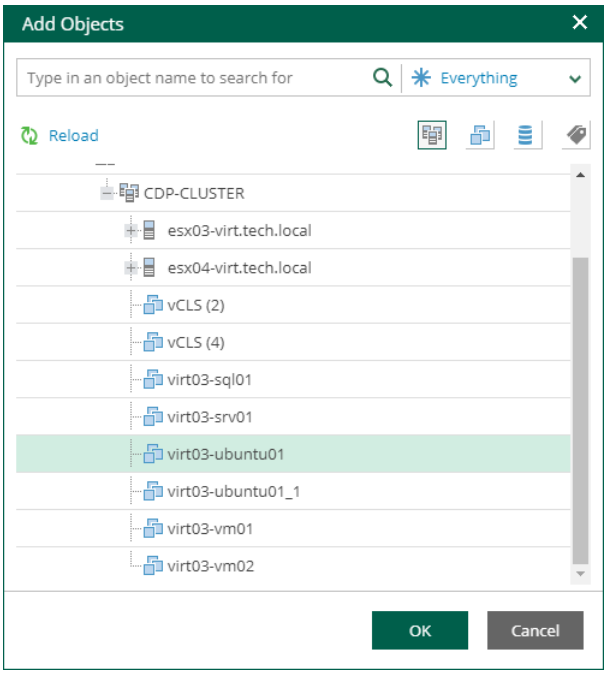
To add a VM or a VM container:

1. Click the **Add**.



2. In the virtual infrastructure tree, select the necessary VMs or VM containers.

   If you select a VM container and later add a new VM to the container, Veeam Backup & Replication will update job settings automatically to include the VM.



> **TIP**
>
> To quickly find the necessary objects, you can do the following:
>
> - Search for objects: type a name or part of a name in the search field. Specify the type of the object from a scroll list next to the search field.
> - Switch between virtual infrastructure views using the buttons in the top right corner:
>   - For VMware objects, you can switch between the **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** and **Tags and VMs** views.
>   - For Hyper-V objects, you can switch between the **Hosts and VMs**, **Hosts and Volumes**, and **Hosts and VM Groups** views.

3. Click **OK** to save the changes.

Removing VMs and VM containers

To remove a VM or VM container, select it in the list and click **Remove**.

Excluding VMs

You can also exclude individual VMs from VM containers (for example, if you need to back up the whole VMware or Hyper-V server except several machines running on this server).

To exclude VMs from a VM container:

1. Select a VM container in the list and click **Exclusions**.
2. In the **Exclusions** window, click **Add** and select machines that you want to exclude.

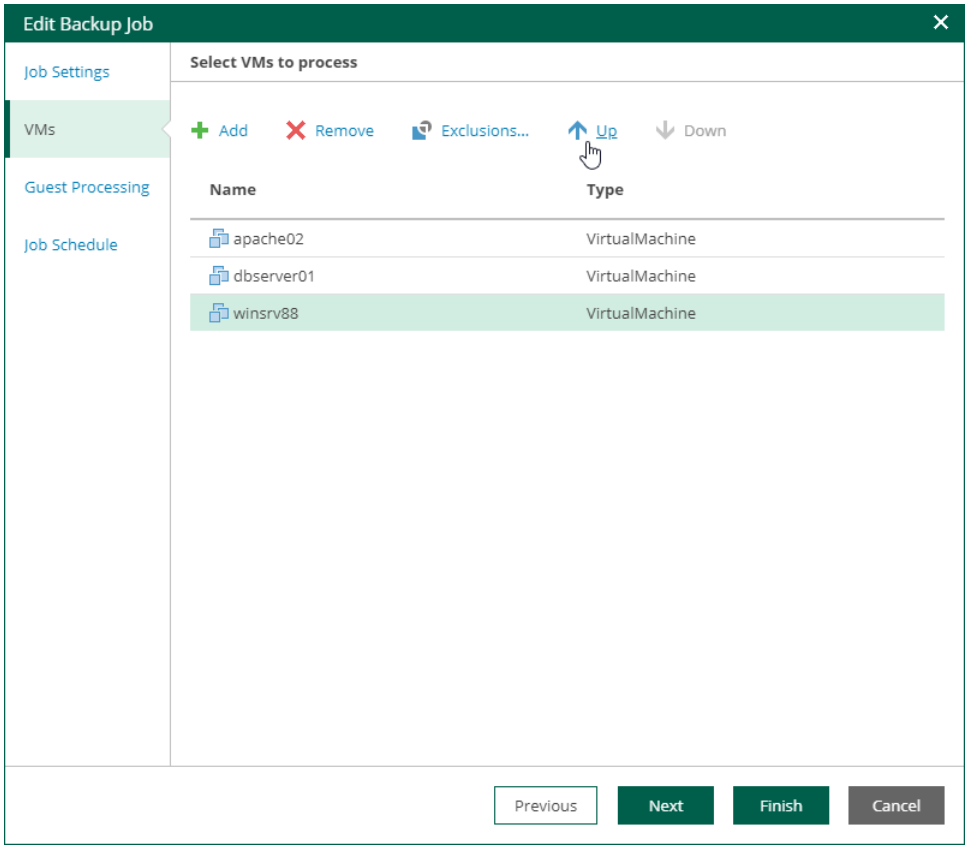
Step 4. Change VM Processing Order

At the **Virtual Machines** step of the wizard, you can change the VM processing order. It can be helpful if specific VMs must be processed first, if you want to ensure that processing of a MV does not overlap with other scheduled activities, or that VM processing is completed before the certain time.

To change the VM processing order, select the necessary machines and move them up or down the list using the **Up** and **Down** buttons on the right. In the same manner, you can set the backup order for containers in the backup list.

NOTE

- VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, add them as standalone VMs, not as a part of containers.
- The processing order may differ from the order that you have defined. For example, if resources of a VM that is higher in the priority are not available, and resources of a VM that is lower in the priority are available, the VM with the lower priority will be processed first.
- For vCD backup jobs you can change the order of the following vCD objects: VMs, vApps, organization vDCs, organizations and the vCD instance. The scope depends on your vCD access rights.
- For vCD replication jobs, you cannot change the VM processing order. You can manage only vApps and other vCD containers.



Step 5. Configure Guest Processing Settings

At the **Guest Processing** step of the wizard, you can select to create a transactionally consistent backup, configure transaction log handling settings, and enable guest file system indexing.

Application-Aware Processing

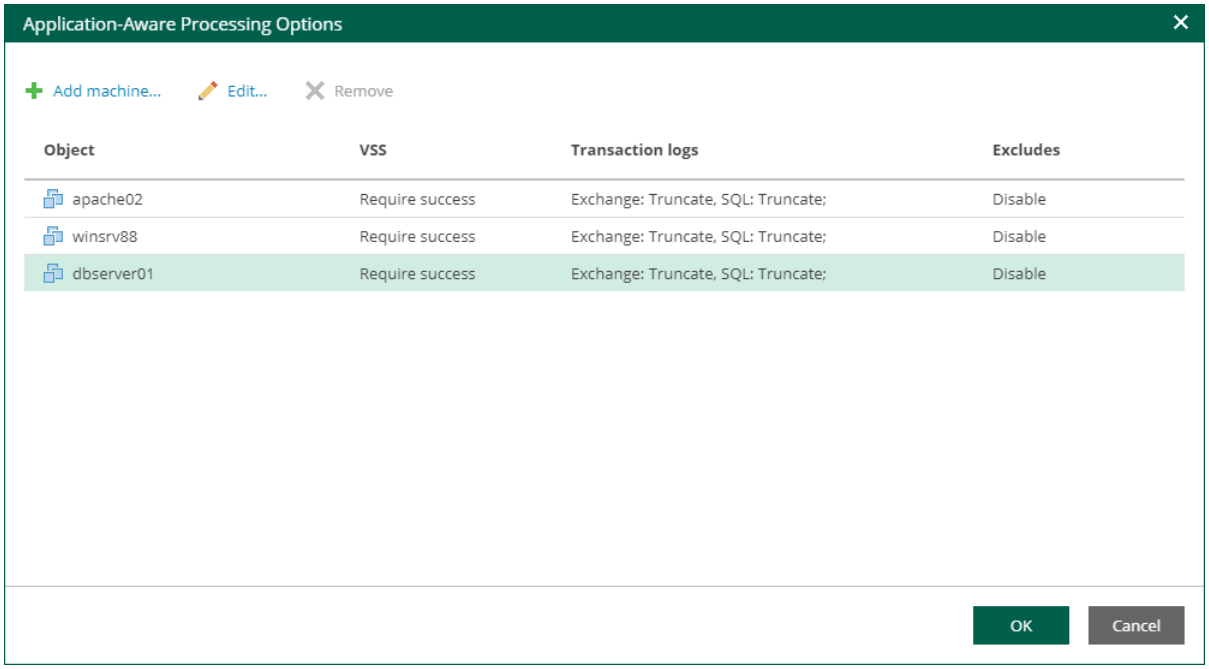
If VMs run Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle, you can enable application-aware processing to create transactionally consistent backups or replicas. The transactionally consistent replicas guarantee proper recovery of applications without data loss.

To configure application-aware processing:

1. Select the **Enable application-aware processing** check box.
2. Click the **Customize Application** link.
3. To define custom settings for a machine in the list, select it and click **Edit**.

   Consider the following:

   - To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
   - To discard custom settings of a machine, select the machine in the list and click **Remove**.
4. Configure the necessary settings for the selected application server:
   - General Settings
   - SQL Server Processing Settings
   - Oracle Server Processing Settings
   - File Exclusions



General Settings

Applications Section

In this section, select the option that corresponds to a transactionally-consistent backup creation scenario of your choice:

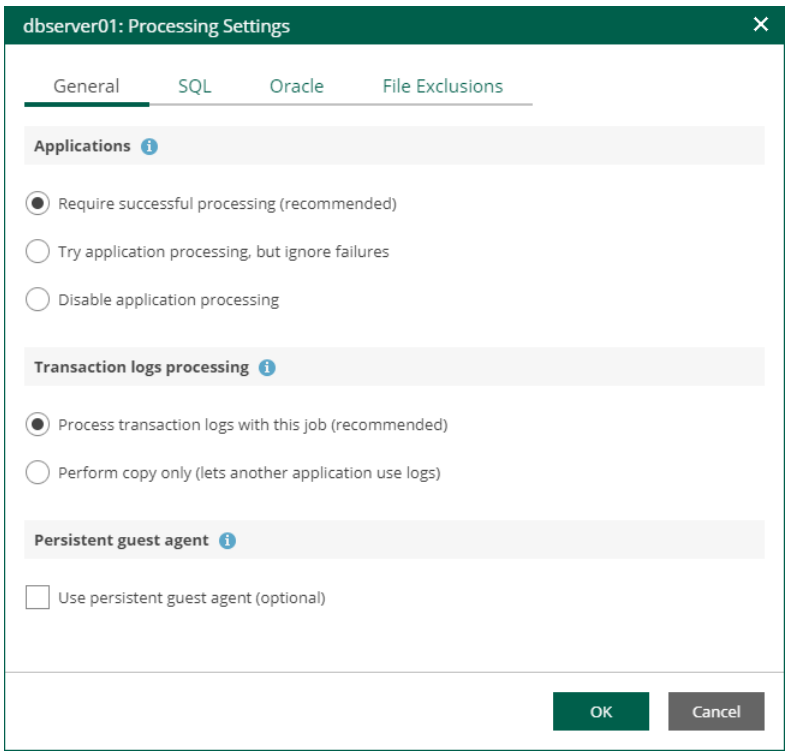
- Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the backup job if an error occurs.
- Select **Try application processing, but ignore failures** if you want to continue the backup process even if an error occurs. This option guarantees completion of the job. The created backup image will not be transactionally consistent, but rather crash-consistent.
- Select **Disable application processing** if you do not want to enable application-aware processing for the VM. This option makes the **Transaction Logs Processing** section unavailable.

Transaction Logs Processing Section

In this section, specify whether this job should process transaction logs upon a successful backup:

- Select **Process transaction logs with this job** if you want Veeam Backup & Replication to handle transaction logs. With this option enabled (default setting), Veeam will support log pruning for Microsoft Exchange and Microsoft SQL Servers, as well as for Oracle databases archived logs:
  - Truncation of transaction logs for Microsoft Exchange Server machines will be performed after the job completes successfully: the Veeam runtime process will wait for the machine backup to complete and then trigger truncation of transaction logs. If truncation of transaction logs is not possible for some reason, the logs will remain untouched in the machine guest OS until the next start of the Veeam runtime process.
  - Settings for SQL Server transaction log handling can be configured separately on the **SQL** tab — it becomes available to you with this option selected.
  - Similarly, you can configure settings for Oracle database archived logs processing on the **Oracle** tab.
- Select **Perform copy only** if you want to use native application means or a third-party tool to process transaction logs. Veeam Backup & Replication will create a copy-only backup for the selected machine. The copy-only backup preserves a chain of full/differential backup files and transaction logs, so Veeam Backup & Replication will not trigger transaction log truncation. This option is recommended if you are using another backup tool to perform the machine guest-level backup, and this tool maintains consistency of the database state. To learn more, see the Guest Processing section of the Veeam Backup & Replication User Guide.

> **NOTE**
>
> With this option selected, the **SQL** and **Oracle** tabs are not available.



SQL Server Processing Settings

For more information on configuring **Microsoft SQL Server** processing settings, see Backup and Restore of Microsoft SQL Server Databases.

Oracle Server Processing Settings

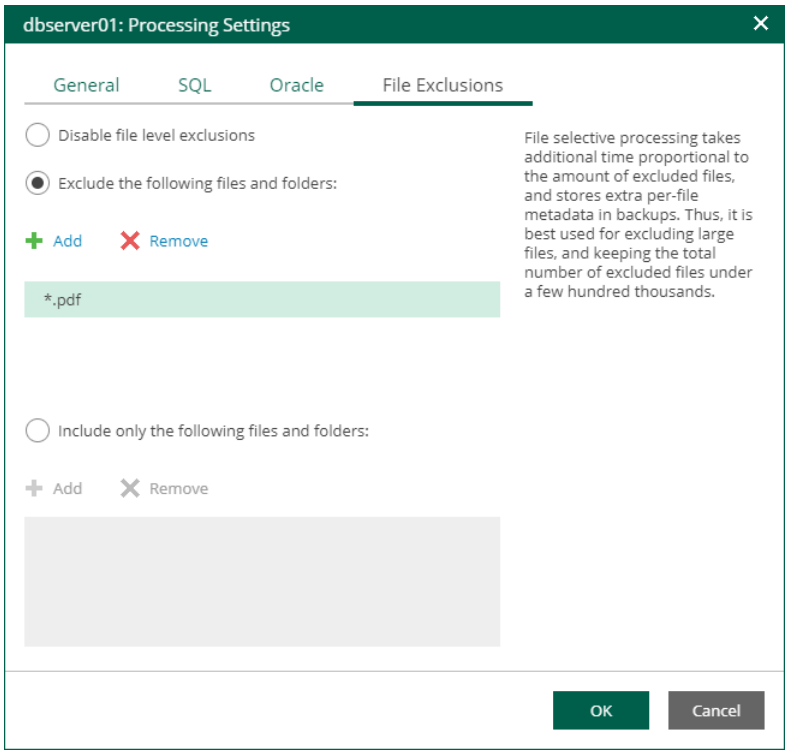
For more information on configuring **Oracle** processing settings, see Backup and Restore of Oracle Databases.

File Exclusions

On the **File Exclusions** tab, specify whether to exclude or include specific files in the backup. Exclusions can help decrease the backup file size. However, selective processing takes additional time that depends on the number of excluded files; also, it requires obtaining per-file metadata (stored in backups). Thus, it is recommended to use this option for excluding large files. By default, exclusions are disabled.

- **Exclude the following files and folders** – with this option selected, you can specify what files and folders must be excluded from the backup.
- **Include only the following files and folders** – with this option selected, you can specify exactly what files and folders must be only included in the backup.

Click **Add** and specify what files and folders you want to include or exclude.



To form the list of exclusions or inclusions, you can use full paths to files and folders, environmental variables, and file masks with the asterisk (*) and question mark (?) characters. For more information, see the VM Guest OS Files section of the Veeam Backup & Replication User Guide.

Guest OS File Indexing

To quickly find the necessary guest OS files in backups, select the **Enable guest file system indexing** check box. This setting provides, in particular, advanced search capabilities when viewing guest OS files and performing 1-Click file restore using Enterprise Manager web UI. If indexing is disabled, you can only use quick search within the selected restore point.

> **NOTE**
>
> For proper file indexing of Linux machines, Veeam Backup & Replication requires several utilities to be installed on the machines: `mlocate`, `gzip`, and `tar`. If these utilities are not found, you are prompted to deploy them to support index creation.

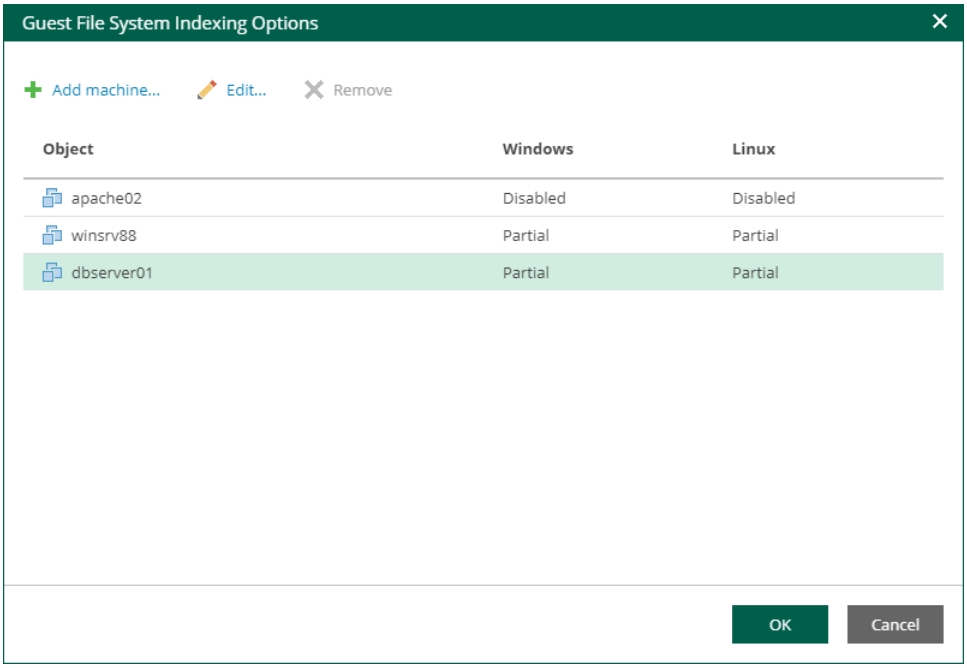
To provide granular indexing options for individual machines:

1. Click the **Customize Indexing** link.
2. In the **Guest File System Indexing Options** window, select a machine from the list and click **Edit**.

   Consider the following:

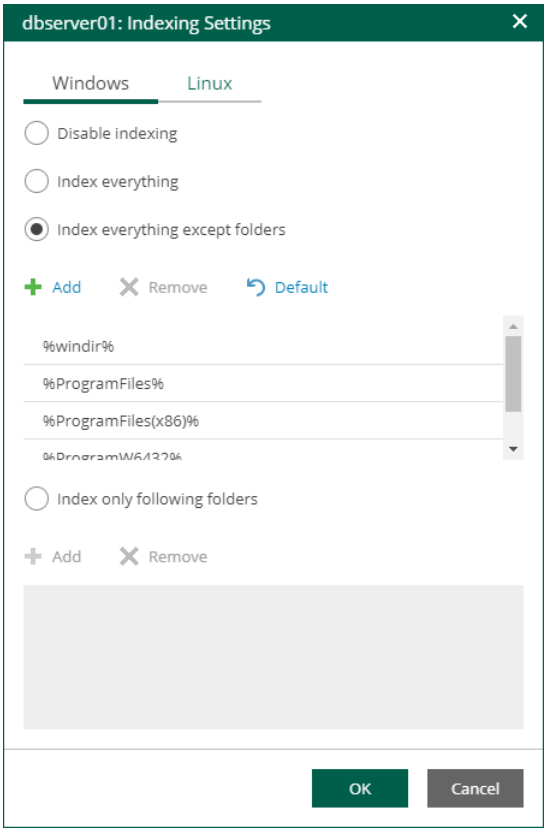
   - To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add Machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.

- To discard custom settings of a machine, select it from the list and click **Remove**.



3. In the **Indexing Settings** window displayed for the selected machine, go to the **Windows** or **Linux** tab and specify what files should be indexed:
   - Select **Disable indexing** if you do not want to index guest OS files of the machine.
   - Select **Index everything** if you want to index all guest OS files inside the machine.
   - Select **Index everything except folders** if you want to index all guest OS files except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders to exclude using the **Add** and **Remove** buttons.

- Select **Index only following folders** to select specific folders that you want to index. To form the list of folders, use the **Add** and **Remove** buttons.

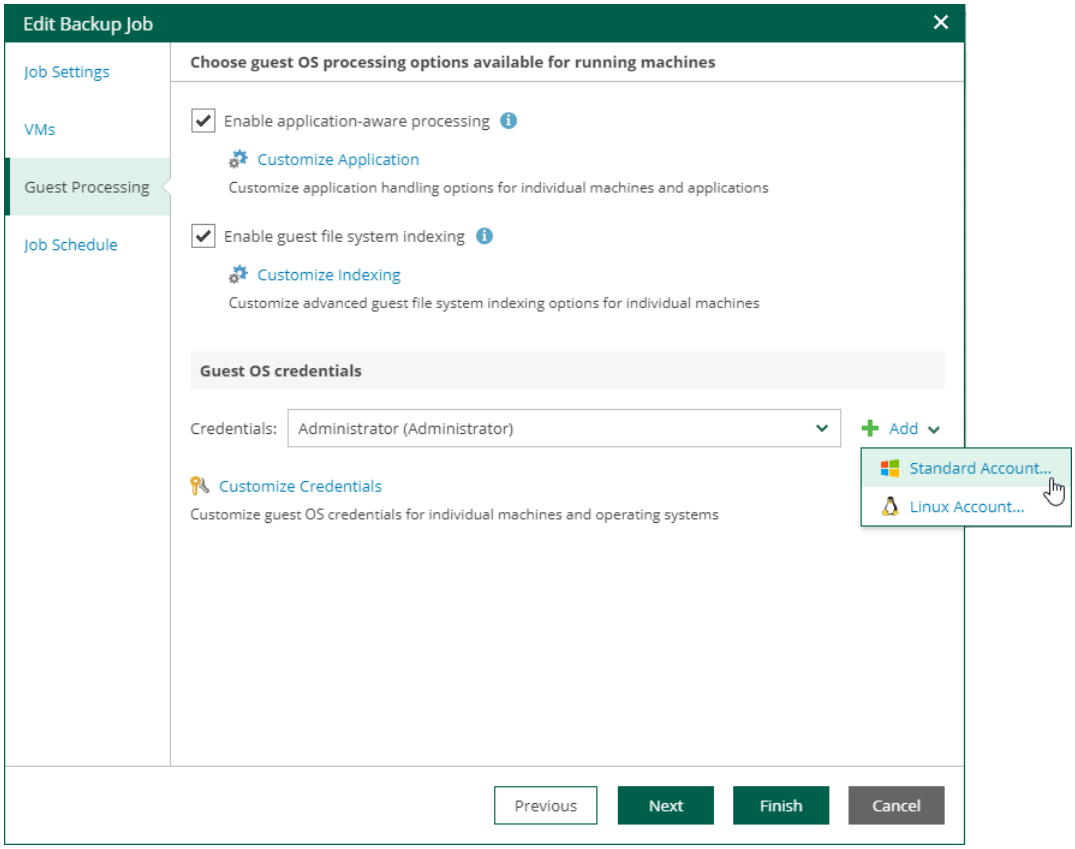


4. Click **OK** to save the settings and close the window.

Guest OS Credentials

To coordinate guest processing activities, Veeam Backup & Replication deploys a runtime process on the VM guest OS. The process runs only during guest processing and is stopped immediately after the processing is finished.

You must specify credentials that will be used to connect to the VM guest OS (Windows or Linux) and to deploy the runtime process.



In the **Guest OS credentials** section, you can select credentials from the list, or click the **Add** button to add new credentials.

- For Windows guest OS, specify a user account (name and password) with local administrative rights on target machine, and optional description. Credentials must be specified in the following format:
  - For Active Directory accounts: *DOMAIN|Username*
  - For local accounts: *Username* or *HOST|Username*
- For Linux guest OS, specify a user name, password, and SSH port (by default, port 22 is used).

  If you specify data for a non-root account that does not have root permissions on a Linux server, you can use the **Non-root account** section to grant sudo rights to this account.

  a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

  b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

  If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

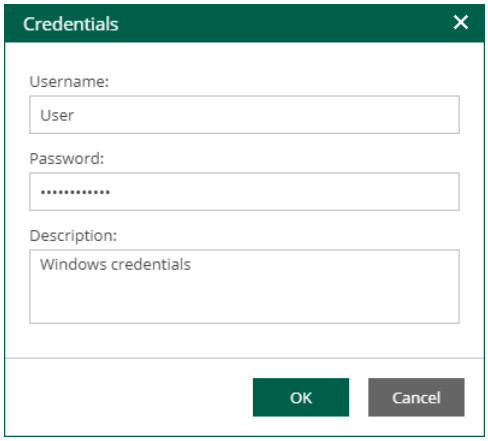
  c. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password for the root account.

  Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

IMPORTANT

For machine guest OS indexing of Linux-based machines, a user account with root privileges on the machine is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based machine, grant root privileges to this account and specify settings of this account in the **Guest OS credentials** section.

It is also recommended to avoid additional commands output for the specified user (like messages echoed from within `~/.bashrc` or command traces before execution), because they may affect Linux machine processing.



Linux Private Key

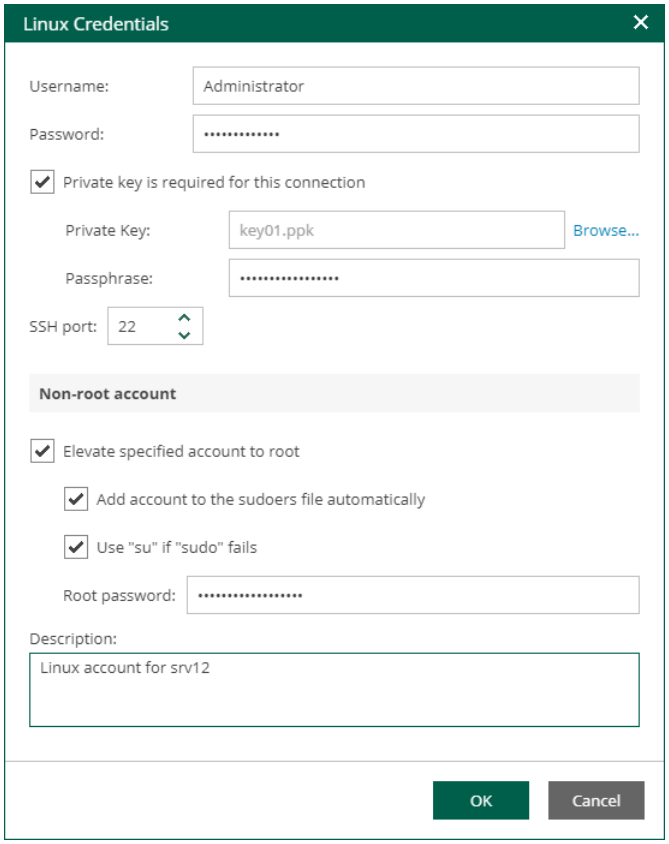
Another option is to use Linux private key. This method eliminates the need to supply password at each login, helps to protect against malicious applications like keyloggers, thus strengthening security, and simplifies launch of automated tasks, decreasing administrative load in Linux environments. For this method, a user must create a pair of keys:

- *Private key* is stored on the client (user's) machine — that is, on the machine where Veeam Backup & Replication runs. The key is usually stored in the encrypted form. To decrypt a private key, you need to supply a passphrase specified at key creation.
- *Public key* is stored on the server (Linux machine) in a special `authorized_keys` file that contains a list of public keys.

If you plan to use Linux private key for authentication, make sure you have created private and public keys and stored them appropriately: private key on the client side (Veeam backup server) and public key on the server side (Linux machine). You should also have the passphrase for the private key if it is encrypted. If you select to use Linux private key credentials, you should specify the following:

- User name
- Passphrase for private key
- Private key stored on the client side (Veeam backup server)
- SSH port (default is 22)

- Non-root account elevation options

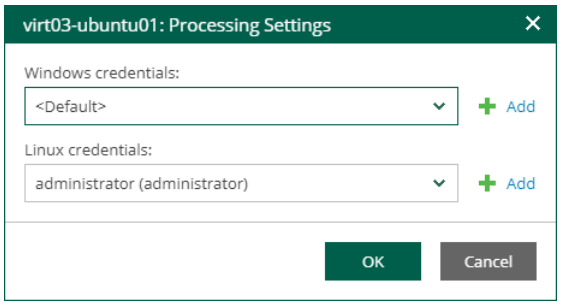


Special Credentials for Machine

By default, for all machines in the list, Veeam Backup & Replication uses common credentials you provided in the **Guest OS credentials** section. To use a different account for deploying the agent inside a specific machine, you can customize credentials for the machine.

To customize credentials:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Set User**.
3. Specify custom guest OS credentials and click **OK**.



To remove custom credentials for a machine:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Remove**.

NOTE

To customize settings of a machine added as part of a container, the machine should be included in the list as a standalone instance. For that, click **Add machine** and choose a machine whose settings you want to customize.

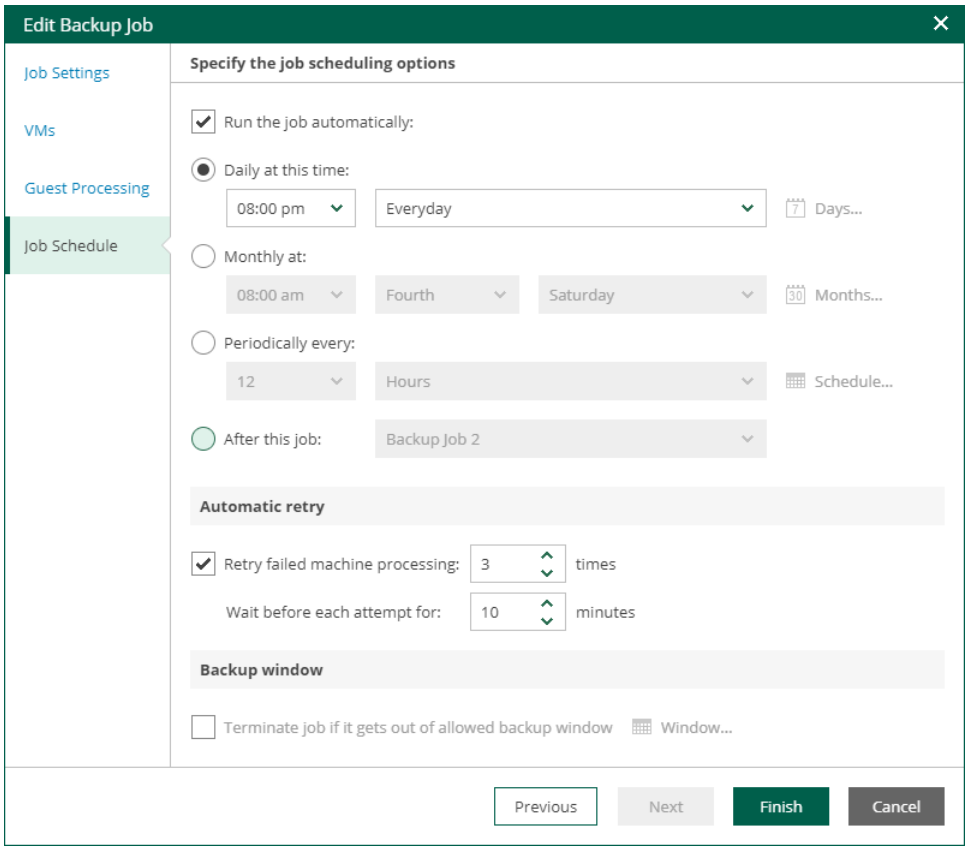
Step 6. Edit Job Schedule

At the **Job Schedule** step of the wizard, you can select to run the job manually or schedule the job to run on a regular basis.

To edit the job schedule:

1. Select the **Run the job automatically** check box. If the check box is not selected, you will need to start the job manually.
2. Edit the scheduling settings. You can select to run the job daily, monthly, periodically with a specific time interval, continuously or after a specific job.

   For more information, see Editing Scheduling Settings.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication must attempt to run the backup job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed machines only. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job runs.
4. In the **Backup window** section, edit the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not provide unwanted overhead on the production environment. To set up a backup window for the job:
   a. Select the **Terminate job if it gets out of allowed backup window** check box and click **Window**.
   b. Define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.



> **NOTE**
>
> If the *Location* property of the source object and target object do not match, you will receive a warning message after you click **Finish**. For example, you may have a backup job targeted at repository located in Sydney, and source machines located in London.

Editing Schedule Settings

If you have selected to run the job automatically, you can select one of the following options:

- To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
- To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

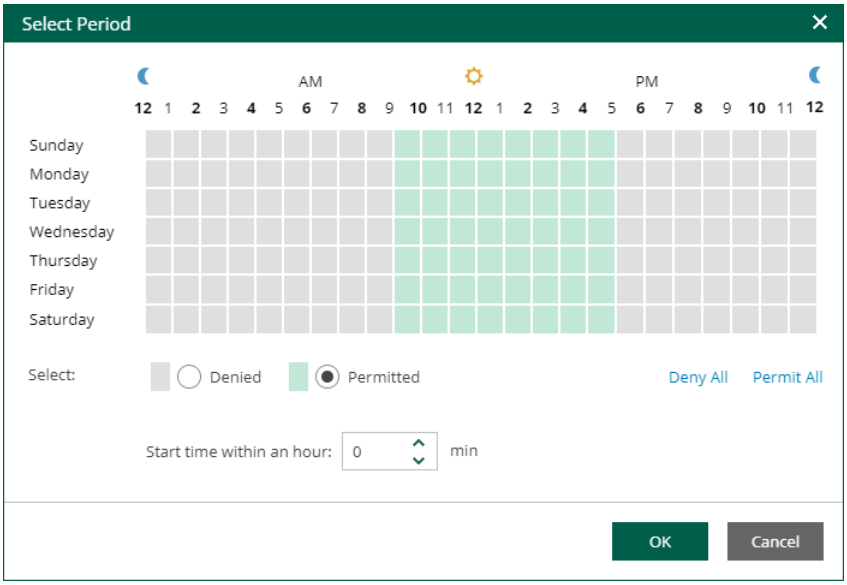
  > **NOTE**
  >
  > When you configure the job schedule, keep in mind possible date and time changes (for example, related to daylight saving time transition).

- To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

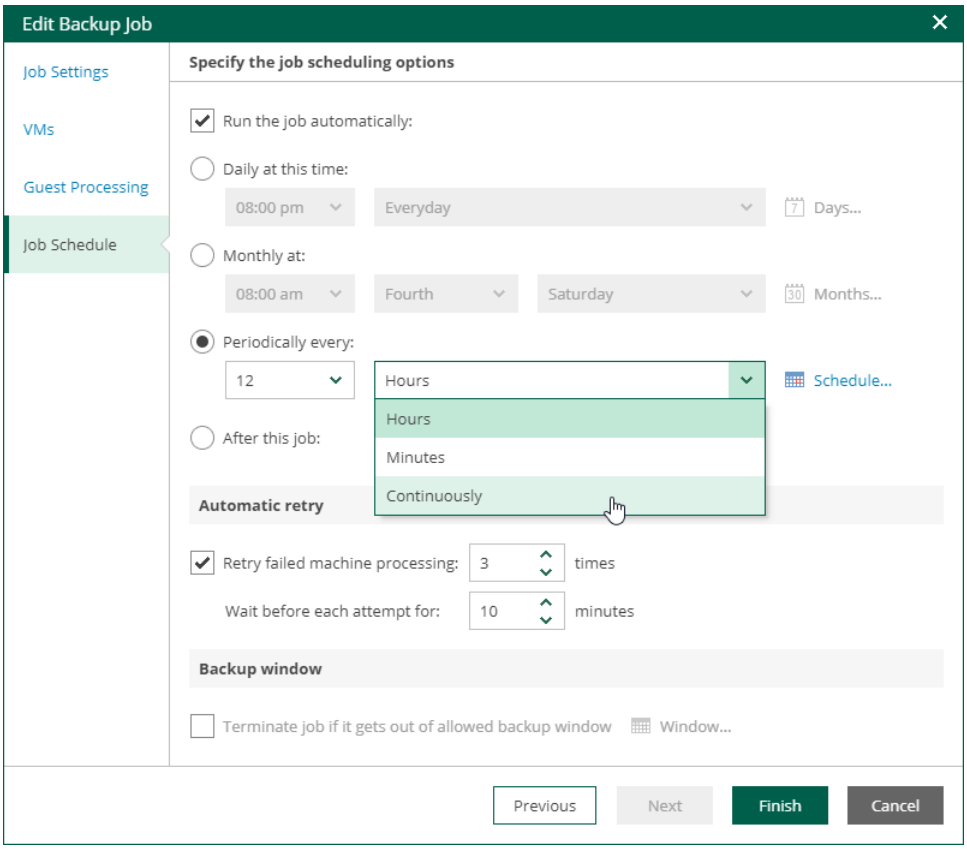
  A repeatedly run job is started by the following rules:

  - Veeam Backup & Replication always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
  - If you define permitted hours for the job, after the denied interval is over, Veeam Backup & Replication will immediately start the job and then run the job by the defined schedule.

  For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.



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



- To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list. If you start the first job manually, Veeam Backup Enterprise Manager will display a notification. You will be able to choose whether to start the chained job as well.

> **NOTE**
>
> You can chain jobs that are processed on the same backup server only.

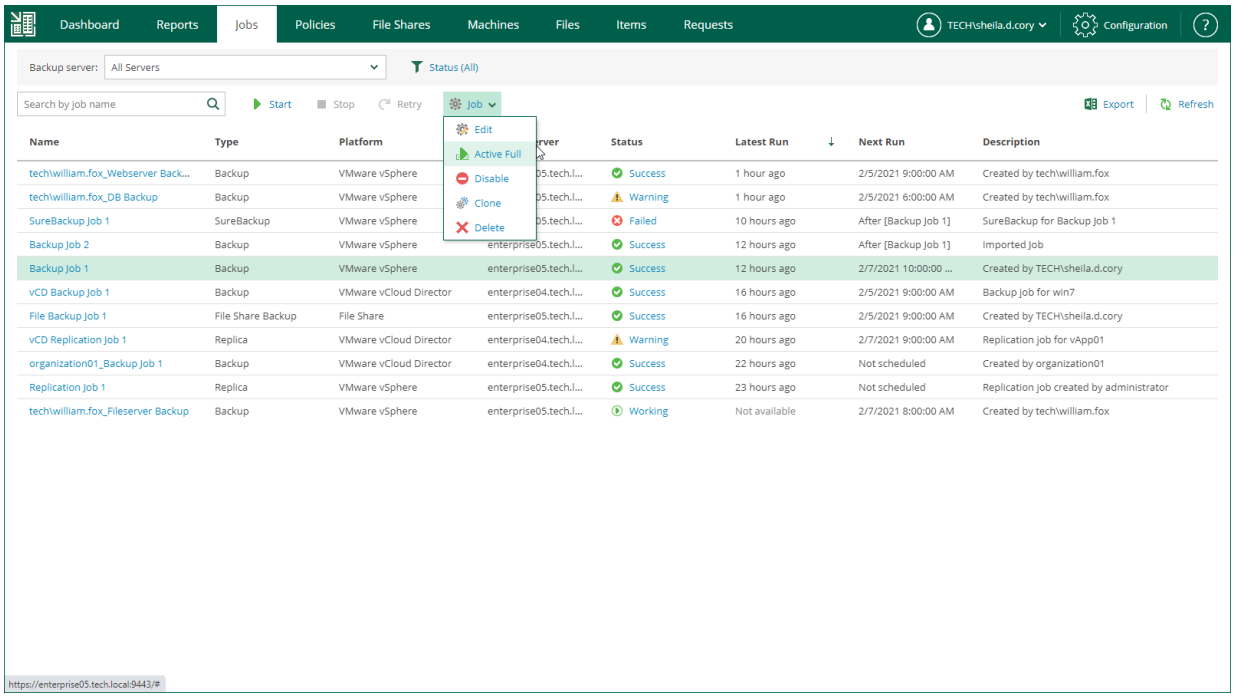
Creating Active Full Backups

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

> **NOTE**
>
> Creating active full backups is unavailable for backup copy jobs and file share backup jobs.

To perform an active full backup:

1. Select the required job in the list on the **Jobs** tab.
2. Expand the menu commands by clicking **Job**, then select **Active Full**.



Cloning Jobs

In addition to performing job editing tasks, you can add new jobs by means of job cloning. Job cloning allows you to create an exact copy of any backup or replication job available in the job list. The recommended practice is to configure a set of 'job templates' in advance, using the Veeam Backup & Replication console on every managed Veeam backup server. These job templates can be used by Enterprise Manager *Portal Administrators* for cloning and further editing.

> **NOTE**
>
> Consider the following:
>
> - The job cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
> - The job cloning functionality is not available for file share backup jobs.

To clone an existing job:

1. Open the **Jobs** tab.
2. Select the necessary job in the list.
3. Expand the menu commands by clicking **Job**, then select **Clone**.

Job clone name is created automatically, with the original job name and suffix of the following format: *_clone<n>* where *<n>* is the sequential number of the clone.

Once a job is cloned, you can edit its settings. For details, see Editing Jobs. Note, however, that not all of the job settings can be changed with the Enterprise Manager web UI. For example, you cannot change the backup repository and backup proxies used for the job or define advanced job settings.

Configuration details of a created job clone are written to the same SQL database that stores configuration details of the original job — thus, the job copy is available and can be managed both with the Veeam Backup Enterprise Manager web UI and the Veeam Backup & Replication console on the backup server that coordinates the job. The backup file produced by the clone will be located on the same repository as the backup file of the original job.

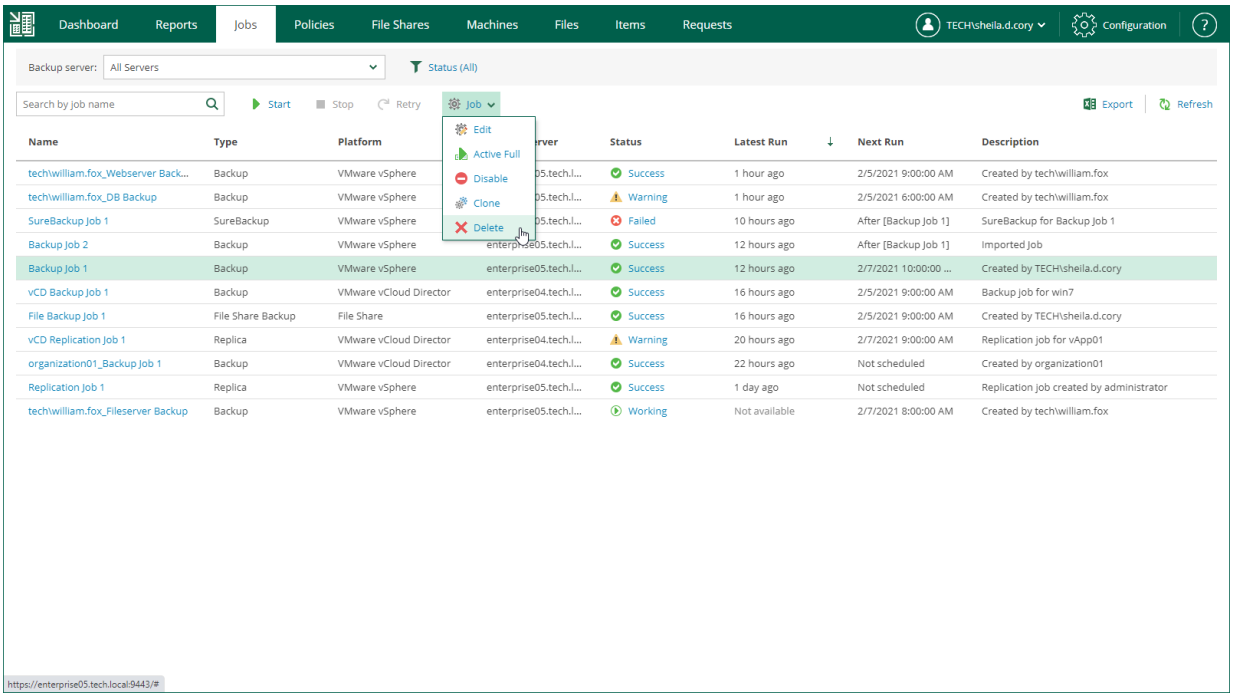
Deleting Jobs

Users with the Portal Administrator role can delete a job and also instruct Veeam Backup Enterprise Manager to delete backup files created by this job in the backup repository. Deleted jobs will no longer appear in the UI. They will be removed from the Enterprise Manager database and from the Veeam Backup configuration database on the backup server. If you select to delete backup files, they will be removed from backup repository.

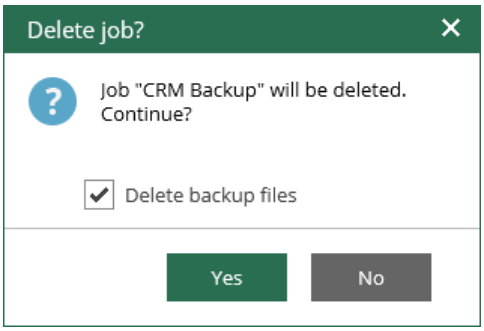
If you have Veeam backup servers of earlier versions added to Enterprise Manager, jobs managed by these servers cannot be deleted using Enterprise Manager.

To delete a job:

1. On the **Jobs** tab, select the required job in the list.
2. Expand the menu commands by clicking **Job**, then select **Delete**.



3. You will be prompted to delete backup files. To delete backup files, select the **Delete backup files** check box and click **Yes** to confirm the operation.



Managing CDP Policies

Veeam Backup Enterprise Manager allows you to manage CDP policies that were previously created on added backup servers. Users with the Portal User role can view CDP policies, and users with the Portal Administrator role can view, disable and enable, edit and delete CDP policies. For more information on CDP, see the Continuous Data Protection (CDP) section of the Veeam Backup & Replication User Guide.

Viewing Policies

From Veeam Backup Enterprise Manager, you can view information about all CDP policies from all backup servers added to Enterprise Manager. To view the CDP policies, open the **Policies** tab. Every policy in the list is described with the following data: policy name, current policy status, policy SLA, recovery point objective (RPO), maximum delay, target host and policy description.

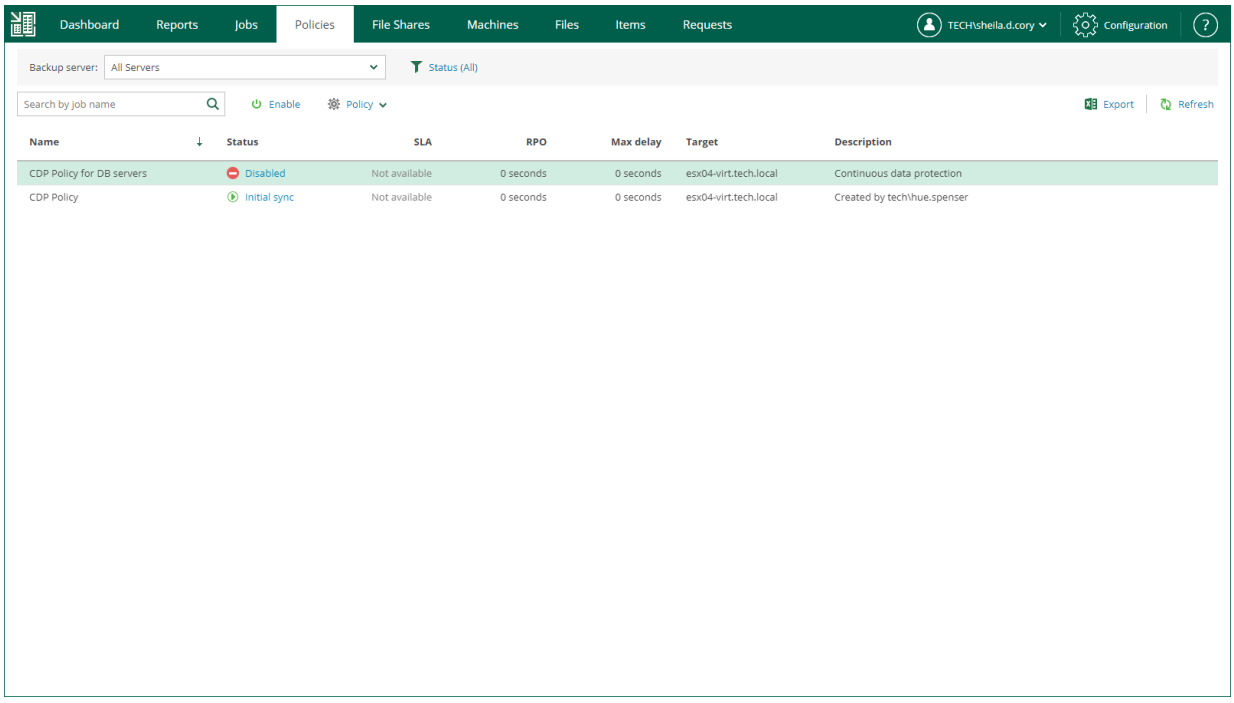
To quickly find a CDP policy, you can use filters and the search field.

- To filter the list of policies:
  - Use the **Backup server** list to view the policies of the selected backup server only.
  - Use the **Status** filter to view the policies with the selected statuses only.

    Once you have selected necessary statuses, click the **Apply** button to apply the filter.
- To find a policy by its name, use the search field.

In addition to the information presented in the list of policies, the **Policies** tab allows you to view advanced policy data. To see detailed policy statistics, click the state link in the **Status** column.

> **NOTE**
>
> You can export displayed information to a file using the **Export** link on the toolbar. This file then can be opened on the client machine using the associated application.

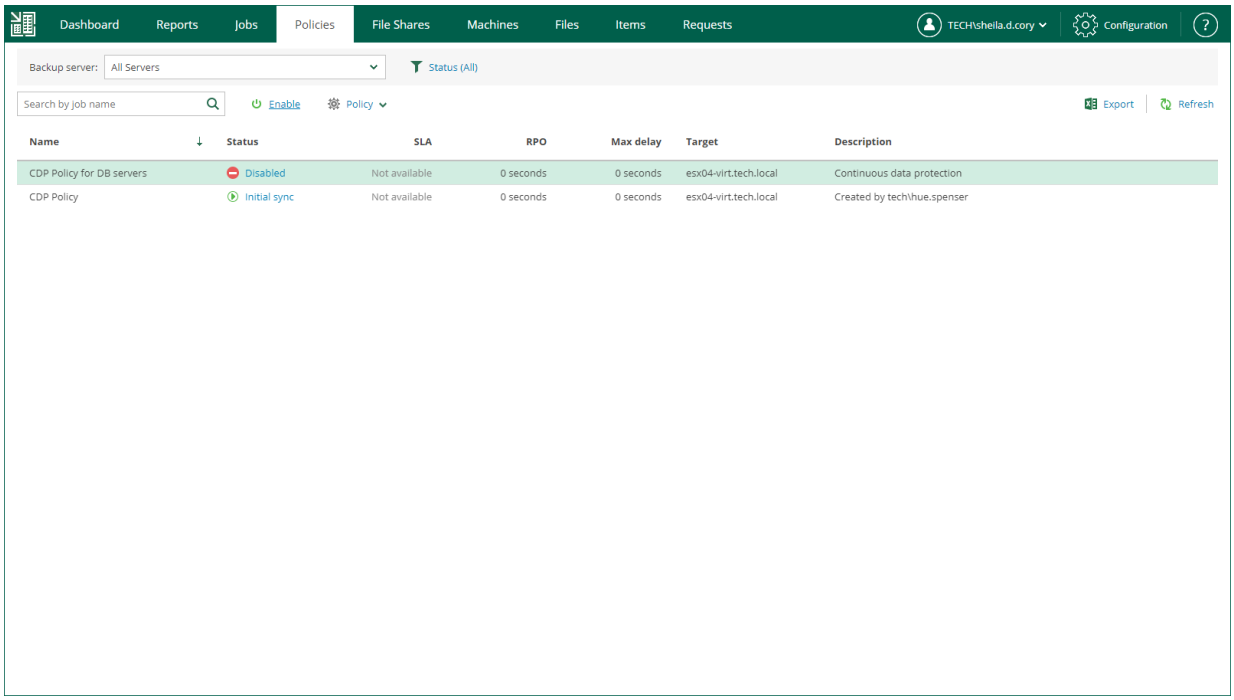


Enabling and Disabling Policies

Users with the Portal Administrator role can enable and disable CDP policies. Disabled CDP policies are temporary paused.

To enable or disable a policy:

1. On the **Policies** tab, select a policy from the list.
2. On the toolbar, click **Enable** or **Disable**.



Editing Policies

If Veeam Backup Enterprise Manager has an Enterprise or Enterprise Plus license installed, users with the Portal Administrator role can modify settings of CDP policies that have been previously configured on managed backup servers. In Veeam Backup Enterprise Manager, you can change only a subset of the CDP policy settings. You can configure other policy settings with the Veeam Backup & Replication console only.

You can edit the following CDP Policy settings:

- Policy name and description
- List of VMs that the policy processes
- Policy schedule
- Guest processing settings

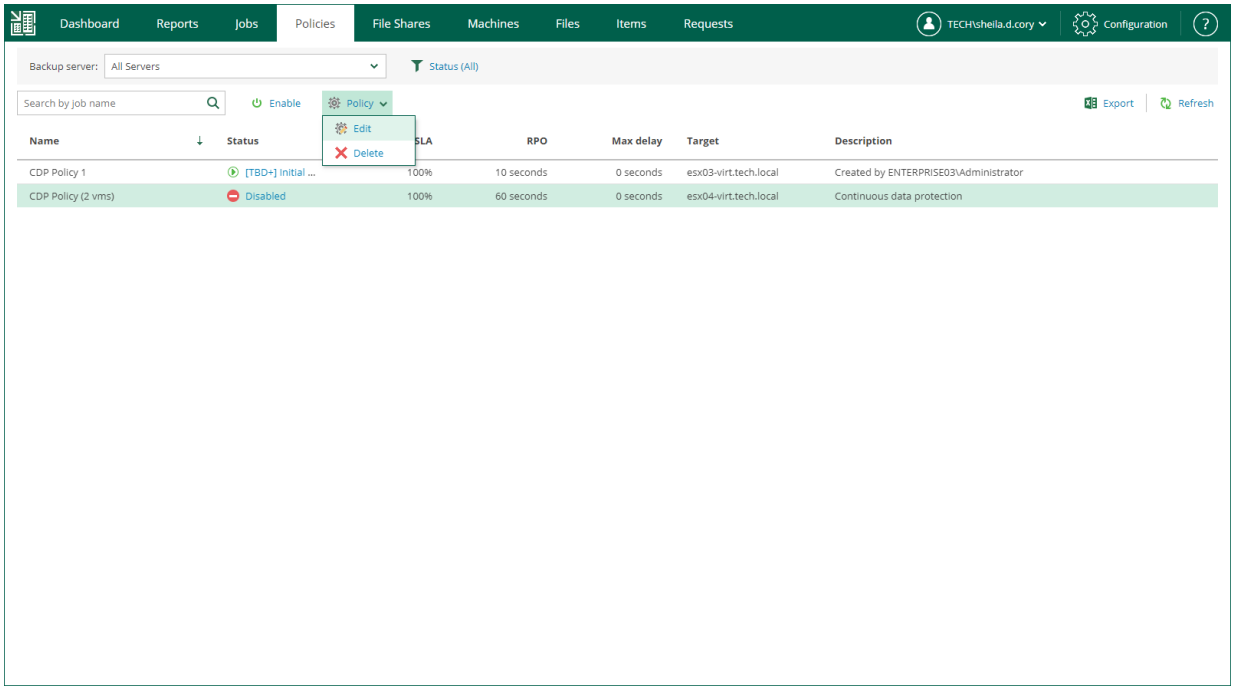
To edit a CDP policy, use the **Edit Policy** wizard.

1. Launch the Edit Policy wizard
2. Edit the policy name and description
3. Edit the list of VMs
4. Configure RPO and retention settings
5. Configure guest processing settings

Step 1. Launch Edit Policy Wizard

To launch the **Edit Policy** wizard:

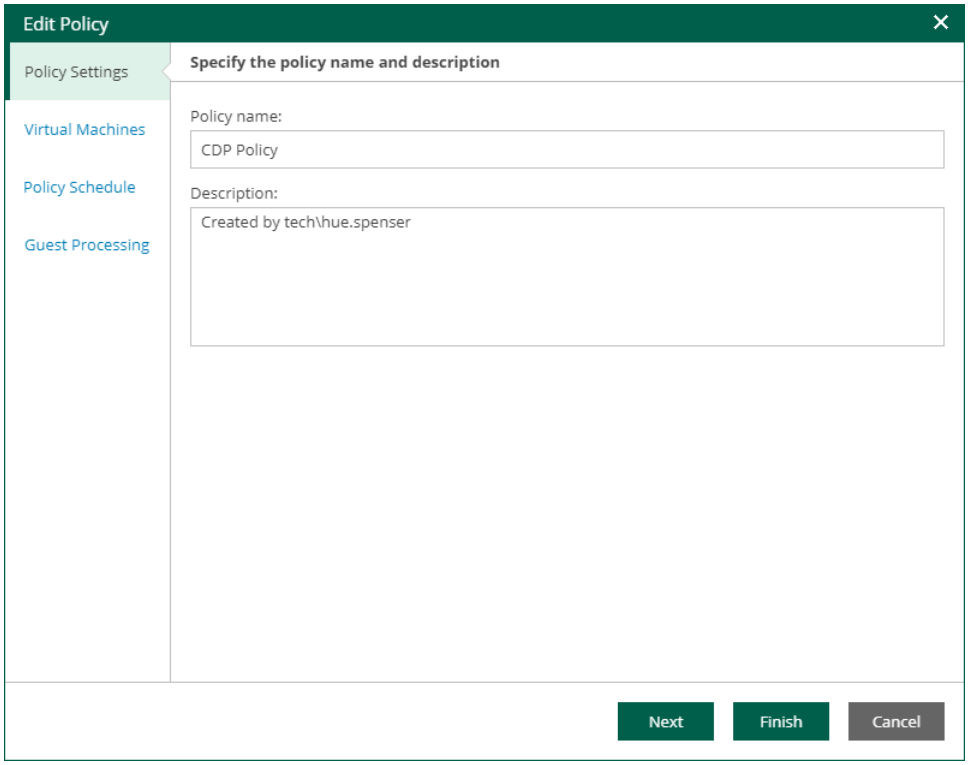
1. Open the **Policies** tab and select the necessary policy from the list.
2. On the toolbar, click **Policy** and select **Edit**.



Step 2. Edit Policy Name and Description

At the **Policy Settings** step of the wizard, you can modify the name and description of the selected CDP policy:

1. In the **Policy name** field, specify a name for the policy.
2. In the **Description** field, provide an optional description for future reference.



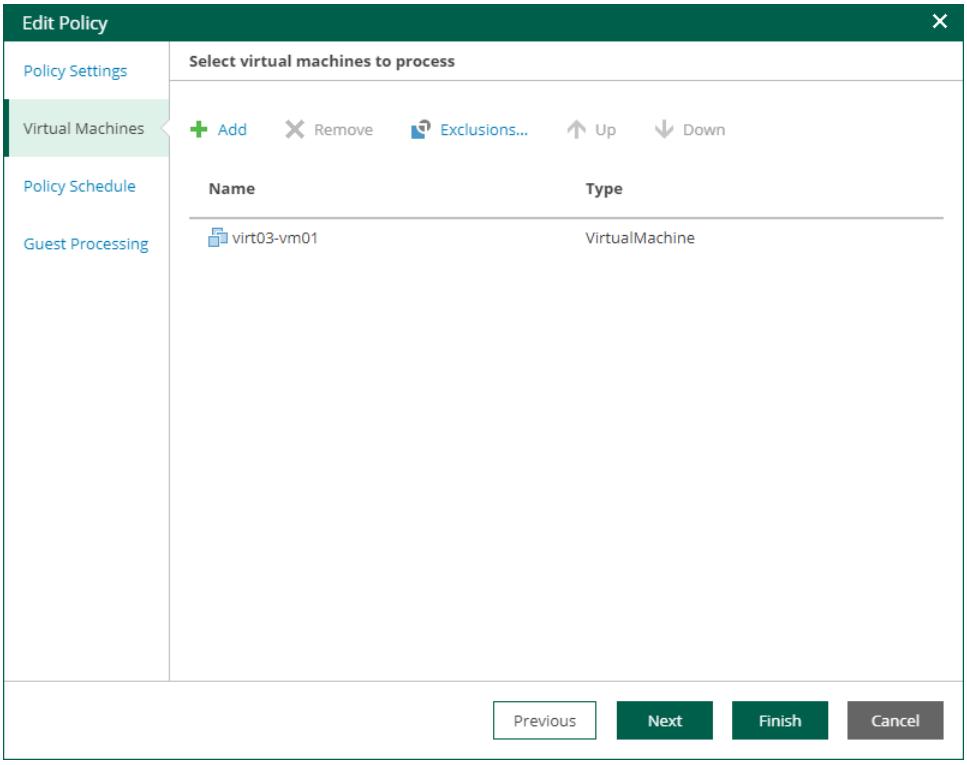
Step 3. Edit List of VMs

At the **Virtual Machines** step of the wizard, you can add or remove individual VMs or VM containers (for example, hosts or folders). You can also exclude individual VMs from VM containers, for example, if you need to replicate an entire VMware vSphere server except some machines running on this server.

Adding VMs and VM containers

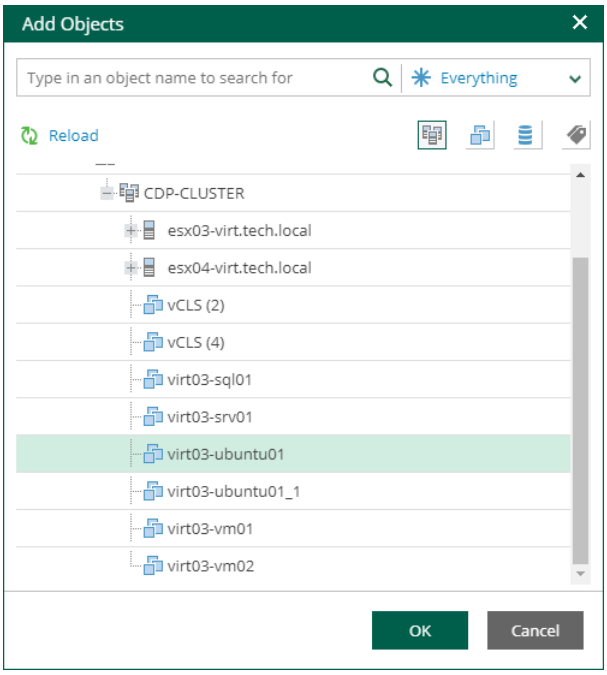
To add a VM or VM container:

1. Click **Add**.



2. In the virtual infrastructure tree, select the necessary VMs or VM containers.

   If you select a VM container and later add a new VM to the container, Veeam Backup & Replication will update policy settings automatically to include the VM.



> **TIP**
>
> To quickly find the necessary objects, you can do the following:
>
> - Search for objects: type a name or part of a name in the search field. Specify the type of the object from a scroll list next to the search field.
> - Switch between virtual infrastructure views using the buttons in the top right corner: **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** and **Tags and VMs**.

3. Click **OK** to save the changes.

Removing VMs and VM containers

To remove a VM or VM container, select it in the list and click **Remove**.

Excluding VMs from VM containers

To exclude VMs from a VM container:

1. Select a VM container in the list and click **Exclusions**.
2. In the **Exclusions** window, click **Add** and select machines that you want to exclude.

Changing Object Processing Order

If specific objects must be processed first, you can change the object processing order. The object processing order can be helpful if you want to ensure that processing of an object does not overlap with other scheduled activities, or that it is completed before the certain time.

To change the processing order, select the necessary objects and move them up or down the list using the **Up** and **Down** buttons on the right.

NOTE

- VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, add them as standalone VMs, not as a part of containers.
- The processing order may differ from the order that you have defined. For example, if resources of a VM that is higher in the priority are not available, and resources of a VM that is lower in the priority are available, the VM with the lower priority will be processed first.

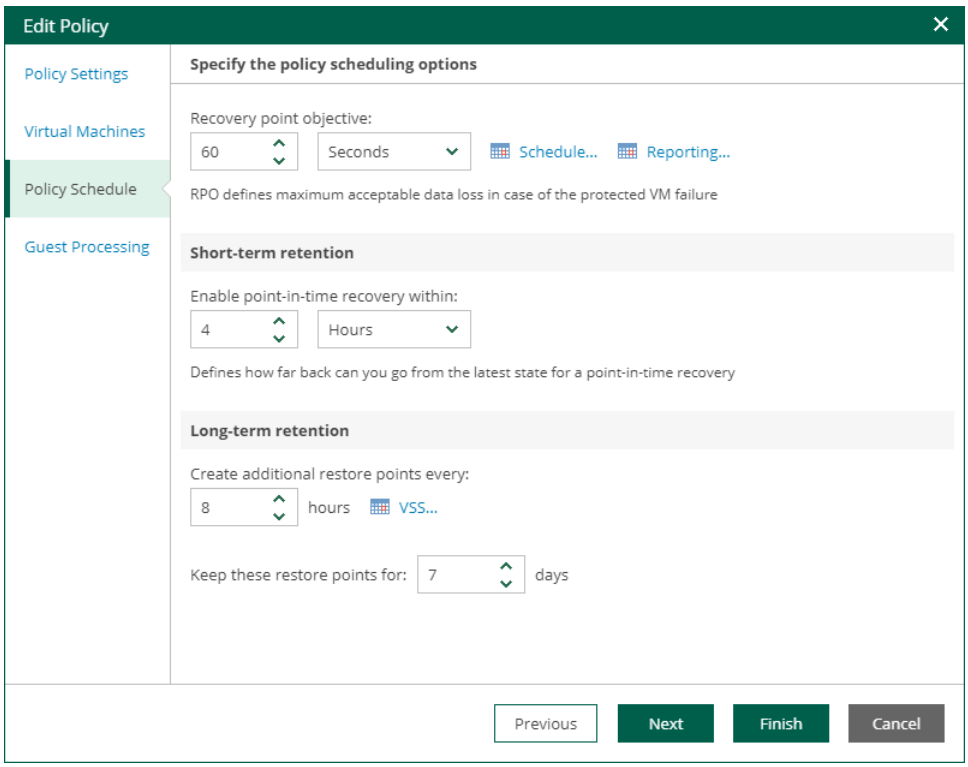
Step 4. Edit Policy Schedule

At the **Policy Schedule** step of the wizard, you can edit schedule and retention settings:

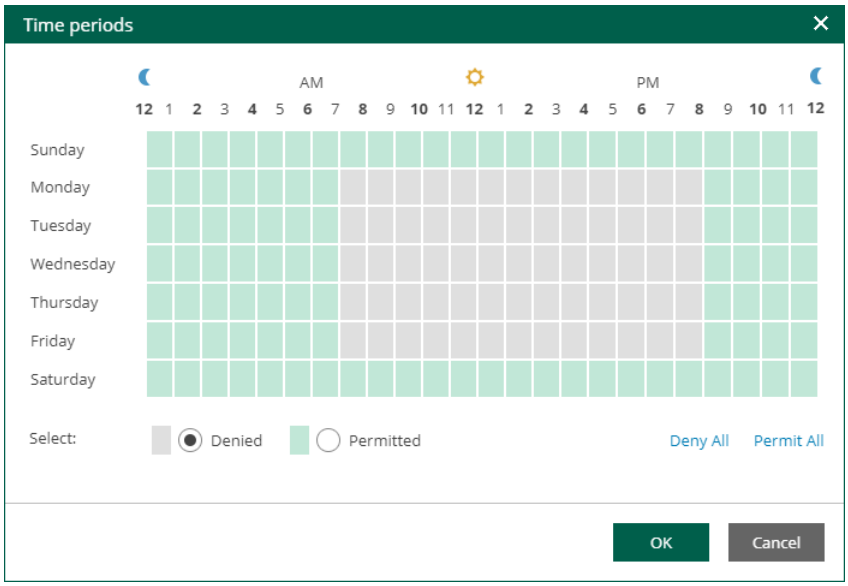
1. Configure scheduling settings:

   a. In the **Recovery point objective** section, specify an RPO in seconds or minutes. You can select the period from 2 seconds to 60 minutes.

   During every specified period, Veeam Backup & Replication will create short-term restore points for VM replicas and send these restore points to the target destination. Note that short-term restore points are crash-consistent.



   b. To specify permitted and denied hours for the policy run, click **Schedule** on the right and use the timetable.



2. To instruct the CDP policy to display a warning or error if a newly created replicated states are not transferred to the target within the set RPO, click **Reporting**. Then specify when the policy must display errors and warnings.

   If you have configured email notification settings, Veeam Backup & Replication will mark the policy with the *Warning* or *Error* status and will also send email notifications.

3. In the **Short-term retention** section, specify for how long to store short-term restore points.

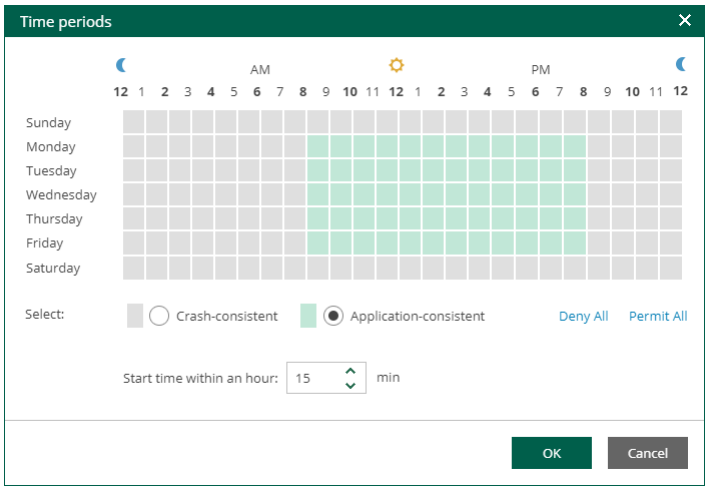
4. In the **Long-term retention** section, configure when to create long-term restore points and for how long to store them:

   a. In the **Create additional restore points every** field, specify how often you want to create long-term restore points.

   b. In the **Keep restore points for** field, specify for how long to store these long-term restore points.

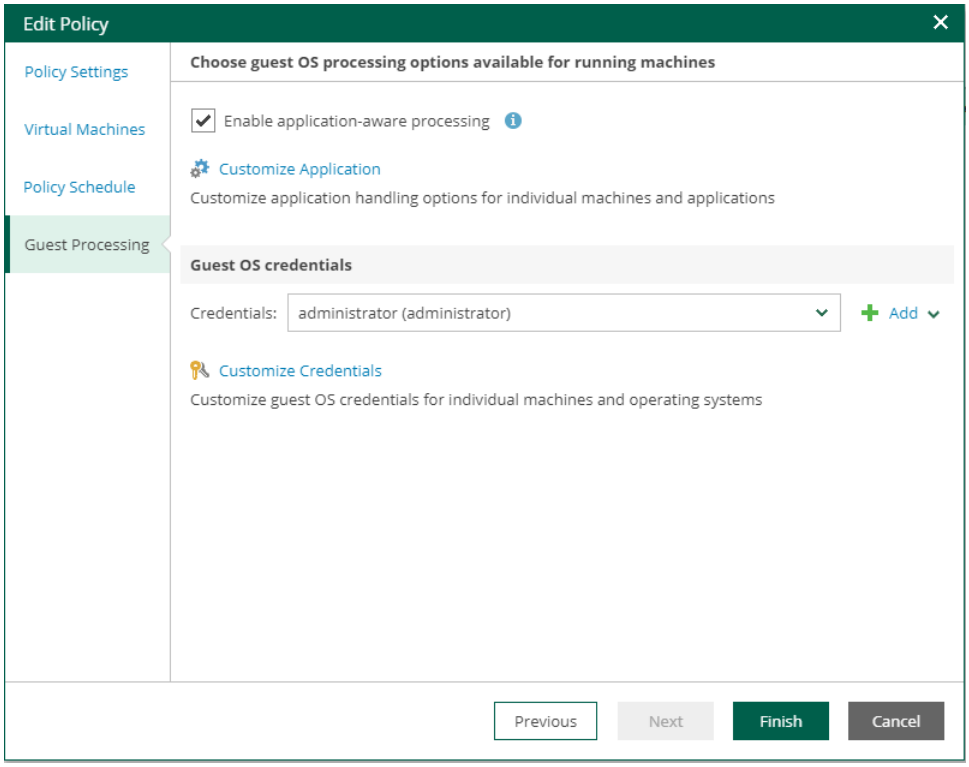
   c. To specify time periods when Veeam Backup & Replication must create application-consistent and crash-consistent long-term restore points, click **VSS**. In the **Time periods** window, select the necessary time area and click **Crash-consistent** or **Application-consistent**. By default, Veeam Backup & Replication creates application-consistent backups if you enable application-aware processing. If you do not enable application-aware processing, Veeam Backup & Replication will create crash-consistent long-term restore points.

      To shift the schedule, specify the offset in the **Start time within an hour** field. For example, you schedule creation of crash-consistent restore points from 00:00 to 01:00, and set the offset value to 25. The schedule will be shifted forward, and the crash-consistent restore points will be created from 0:25 and to 01:25.



Step 5. Configure Guest Processing Settings

At the **Guest Processing** step of the wizard, you can select to create a transactionally consistent replicas, configure transaction log handling settings, and enable guest file system indexing.



Application-Aware Processing

If VMs run Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle, you can enable application-aware processing to create transactionally consistent replicas. The transactionally consistent replicas guarantee proper recovery of applications without data loss.

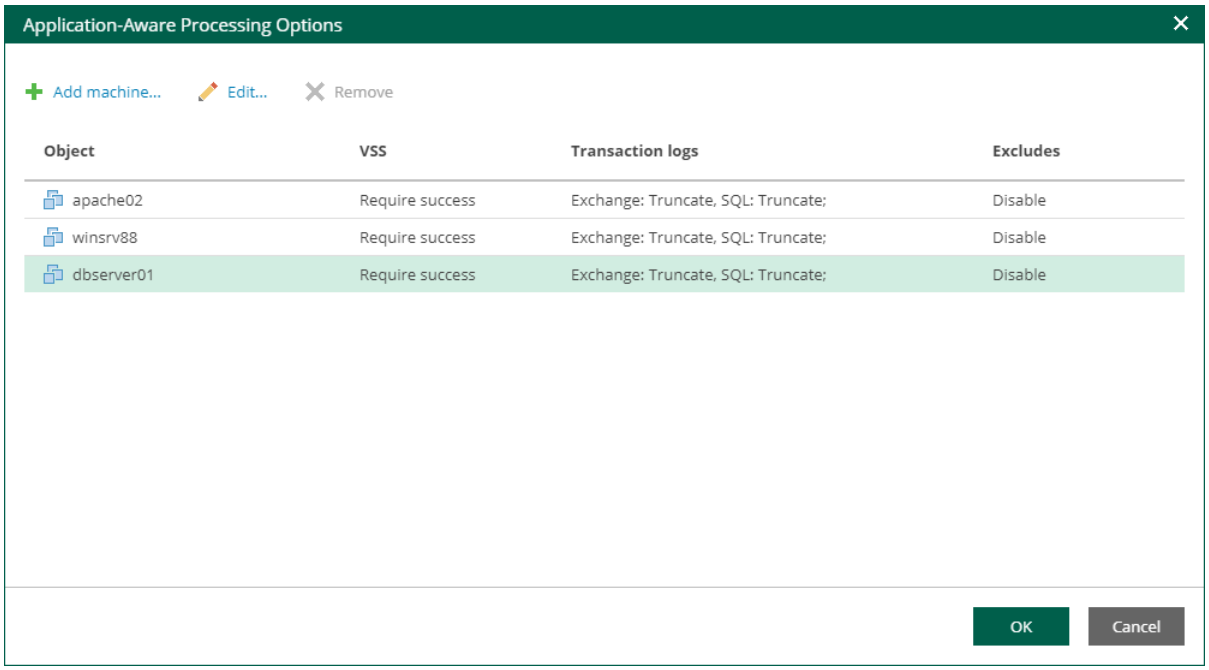
To configure application-aware processing:

1. Select the **Enable application-aware processing** check box.
2. Click the **Customize Application** link.
3. To define custom settings for a machine in the list, select it and click **Edit**.

   Consider the following:

   - To customize settings of a machine added as part of a container, add the machine as a standalone instance. For that, click **Add machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
   - To discard custom settings of a machine, select the machine in the list and click **Remove**.
4. Configure the necessary settings for the selected application server:
   - General Settings
   - SQL Server Processing Settings

- Oracle Server Processing Settings



General Settings

Applications Section

In this section, select the behavior scenario for application-aware processing:

- Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the CDP replication if an error occurs during application-aware processing.
- Select **Try application processing, but ignore failures** if you want to continue the CDP replication process even if an error occurs. This option guarantees the CDP policy will continue working. The created replica will not be transactionally consistent, but rather crash-consistent.
- Select **Disable application processing** if you do not want to enable application-aware processing for the VM. This option makes the **Transaction logs processing** section unavailable.

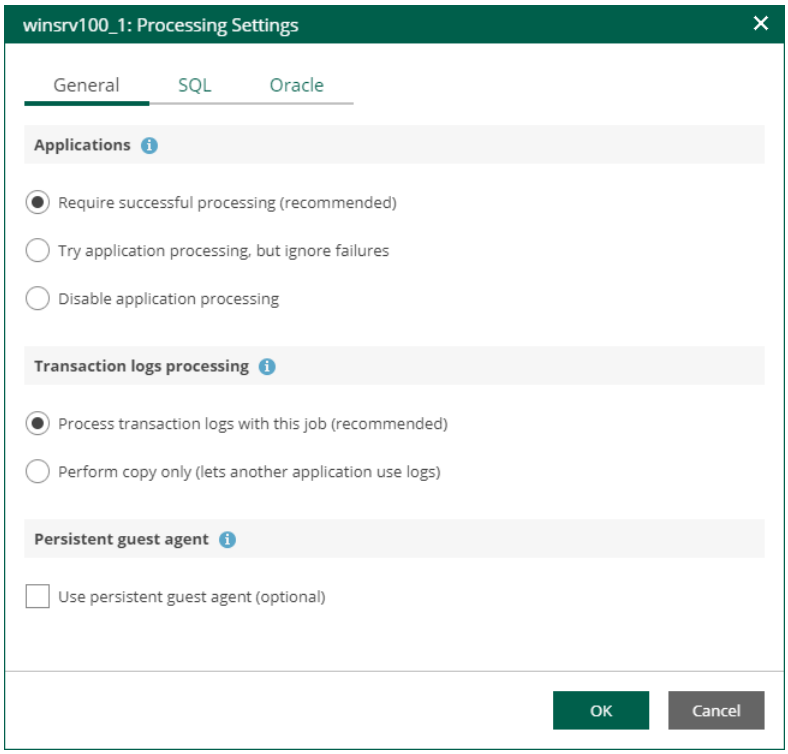
Transaction Logs Processing Section

In this section, specify whether the CDP policy should process transaction logs or create copy-only replicas:

- Select **Process transaction logs with this job** if you want Veeam Backup & Replication to handle transaction logs. With this option enabled (default setting), Veeam will support log pruning for Microsoft Exchange and Microsoft SQL Servers, as well as for Oracle databases archived logs:
  - Truncation of transaction logs for Microsoft Exchange Server VMs will be performed after the CDP policy completes successfully. If the CDP policy fails, the logs will remain untouched until the next start of the runtime process.
  - Settings for SQL Server transaction log handling can be configured separately on the **SQL** tab — it becomes available to you with this option selected.
  - Similarly, you can configure settings for Oracle database archived logs processing on the **Oracle** tab.

- Select **Perform copy only** if you use another replication tool to perform guest level replication, and this tool maintains consistency of the database state. Veeam Backup & Replication will create a copy-only replica for the selected VM. The copy-only replica preserves the chain of full and differential backup files and transaction logs on the VM. For more information, see Microsoft Docs.

  > **NOTE**
  >
  > With this option selected, the **SQL** and **Oracle** tabs are not available.



SQL Server Processing Settings

For more information on configuring Microsoft SQL Server processing settings, see Backup and Restore of Microsoft SQL Server Databases.

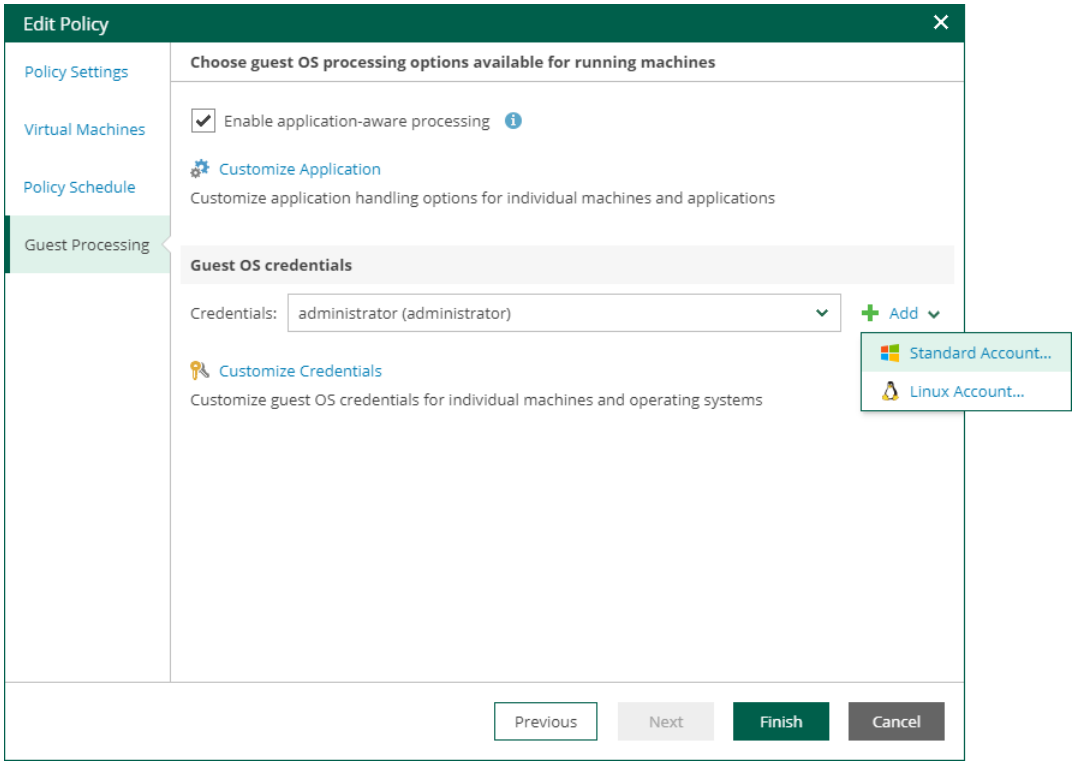
Oracle Server Processing Settings

For more information on configuring Oracle processing settings, see Backup and Restore of Oracle Databases.

Guest OS Credentials

To coordinate guest processing activities, Veeam Backup & Replication deploys a runtime process on the VM guest OS. The process runs only during guest processing and is stopped immediately after the processing is finished.

You must specify credentials that will be used to connect to the VM guest OS (Windows or Linux) and to deploy the runtime process.



In the **Guest OS credentials** section, you can select credentials from the list, or click the **Add** button to add new credentials.

- For Windows guest OS, specify a user account (name and password) with local administrative rights on target machine, and optional description. Credentials must be specified in the following format:
  - For Active Directory accounts: *DOMAIN|Username*
  - For local accounts: *Username* or *HOST|Username*
- For Linux guest OS, specify a user name, password, and SSH port (by default, port 22 is used).

  If you specify data for a non-root account that does not have root permissions on a Linux server, you can use the **Non-root account** section to grant sudo rights to this account.

  a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

  b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

  If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

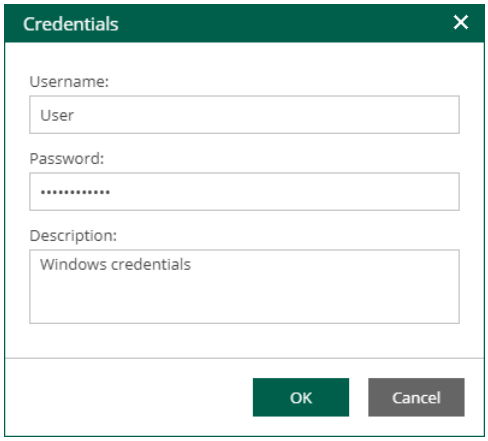
  c. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password for the root account.

  Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

IMPORTANT

For machine guest OS indexing of Linux-based machines, a user account with root privileges on the machine is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based machine, grant root privileges to this account and specify settings of this account in the **Guest OS credentials** section.

It is also recommended to avoid additional commands output for the specified user (like messages echoed from within `~/.bashrc` or command traces before execution), because they may affect Linux machine processing.



Linux Private Key

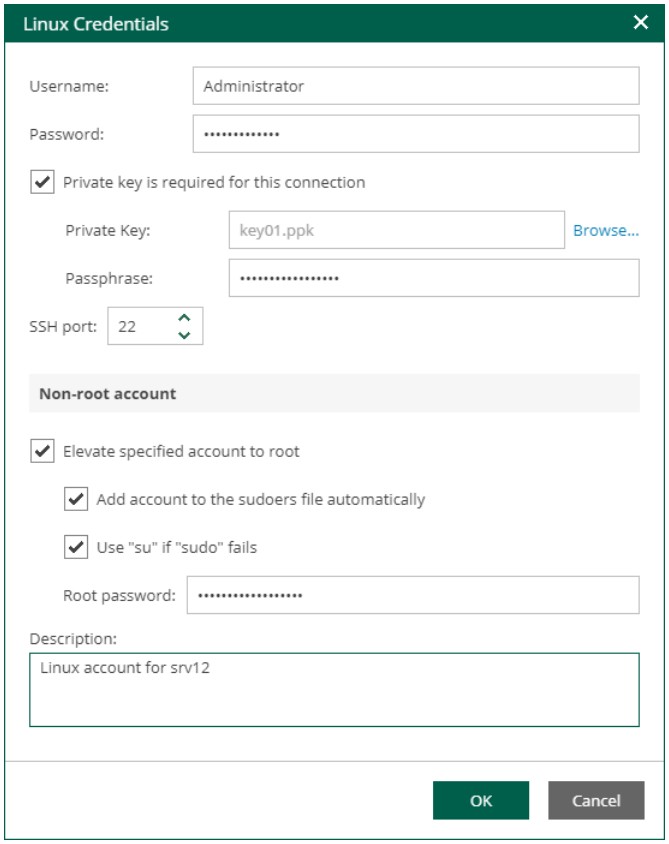
Another option is to use Linux private key. This method eliminates the need to supply password at each login, helps to protect against malicious applications like keyloggers, thus strengthening security, and simplifies launch of automated tasks, decreasing administrative load in Linux environments. For this method, a user must create a pair of keys:

- *Private key* is stored on the client (user's) machine — that is, on the machine where Veeam Backup & Replication runs. The key is usually stored in the encrypted form. To decrypt a private key, you need to supply a passphrase specified at key creation.
- *Public key* is stored on the server (Linux machine) in a special `authorized_keys` file that contains a list of public keys.

If you plan to use Linux private key for authentication, make sure you have created private and public keys and stored them appropriately: private key on the client side (Veeam backup server) and public key on the server side (Linux machine). You should also have the passphrase for the private key if it is encrypted. If you select to use Linux private key credentials, you should specify the following:

- User name
- Passphrase for private key
- Private key stored on the client side (Veeam backup server)
- SSH port (default is 22)

- Non-root account elevation options

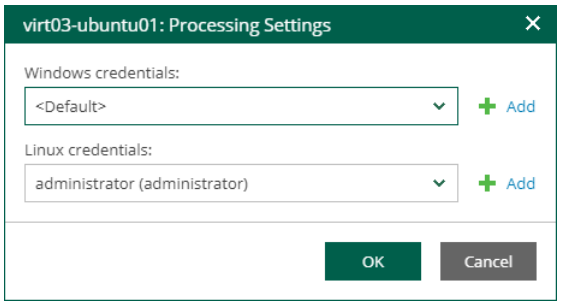


Special Credentials for Machine

By default, for all machines in the list, Veeam Backup & Replication uses common credentials you provided in the **Guest OS credentials** section. To use a different account for deploying the agent inside a specific machine, you can customize credentials for the machine.

To customize credentials:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Set User**.
3. Specify custom guest OS credentials and click **OK**.



To remove custom credentials for a machine:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Remove**.

NOTE

To customize settings of a machine added as part of a container, the machine should be included in the list as a standalone instance. For that, click **Add machine** and choose a machine whose settings you want to customize.

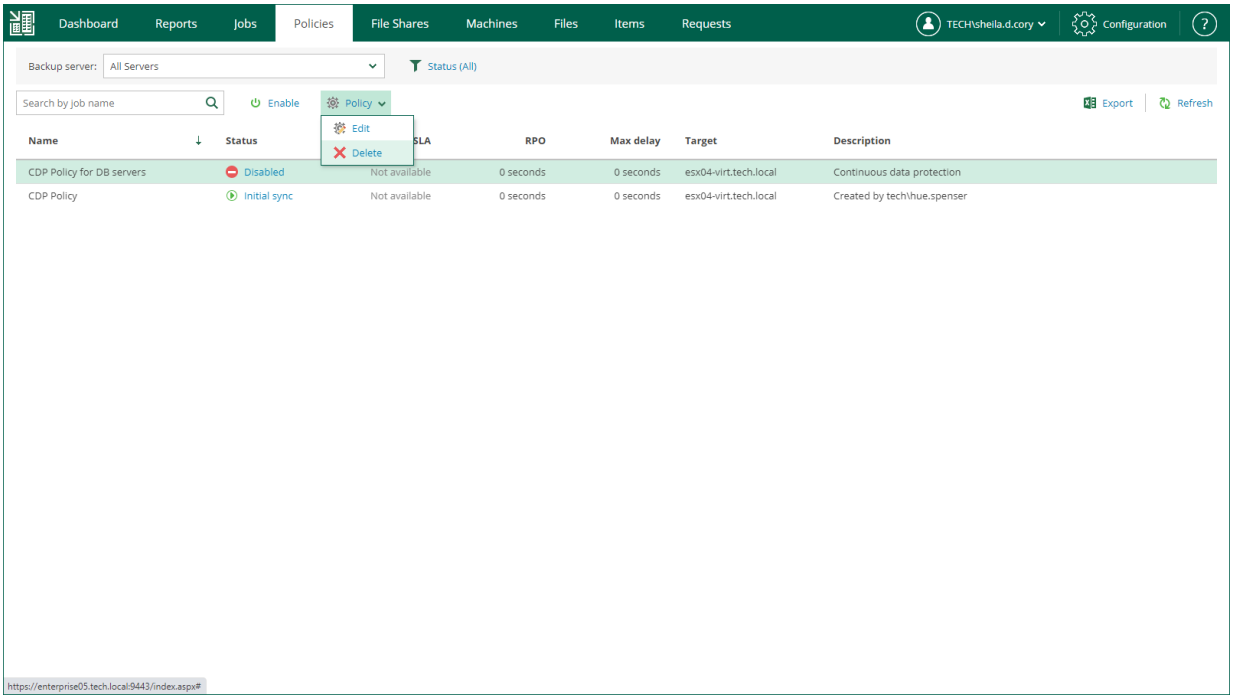
Deleting Policies

Users with the Portal Administrator role can permanently delete CDP policies. The deleted policies will no longer appear in the UI. They are removed from the Enterprise Manager database and from the Veeam Backup configuration database on the backup server.

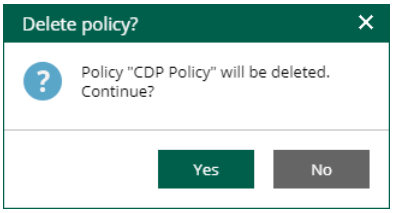
Before you delete a CDP policy, you must disable it.

To delete a policy:

1. On the **Policies** tab, select the required policy in the list.
2. On the toolbar, click **Policy** and select **Delete**.



3. In the displayed window, click **Yes** to confirm the operation.



Support for Veeam Agents

Veeam Backup Enterprise Manager allows you to browse and restore guest OS files and application items from backups created with the following Veeam Agents:

- Veeam Agents for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Mac
- Veeam Agent for Oracle Solaris
- Veeam Agent for IBM AIX

> **NOTE**
>
> File restore from backups of Veeam Agent for Mac, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX to the original location is not available.

Before you start browsing or restore, check the following prerequisites:

1. You have the Enterprise or Enterprise Plus edition of Veeam Backup & Replication.
2. For 1-Click restore of guest OS files and for restore of application items, you must have the Server edition of Veeam Agents. For more information, see Veeam Availability Suite: Product Comparison.
3. Veeam Agent should be integrated with Veeam Backup & Replication. For more information, see the *Integration with Veeam Backup & Replication* section of the following user guides:
   - Veeam Agent for Windows User Guide
   - Veeam Agent for Linux User Guide
   - Veeam Agent for Mac User Guide
   - Veeam Agent for Oracle Solaris User Guide
   - Veeam Agent for IBM AIX User Guide

> **NOTE**
>
> Veeam Agent backup policies, that is, Veeam Agent backup jobs managed by Veeam Agent, are not displayed in the Enterprise Manager web UI. Enterprise Manager displays only Veeam Agent backup jobs managed by the backup server. For more information on Veeam Agent backup jobs and policies, see the Working with Veeam Agent Backup Jobs and Policies section of the Veeam Agent Management Guide.

Guest File Browsing and 1-Click Restore

If you have Veeam Backup & Replication and Veeam Agent that both meet the prerequisites, you can browse, search and restore guest OS files from the backups created by Veeam Agent.

Preparing for File Browsing and Restore

You can browse and restore files from a backup of a physical server created by Veeam Agent with or without enabling guest OS file indexing. Take some preparatory steps for the server processed by Veeam Agent:

- Preparing for restore from a Windows Server backup
- Preparing for restore from a Non-Windows Server backup

Windows Server

Preparing Backup

You can restore files from a backup of a physical Windows server created with or without indexing.

To prepare a backup with guest file indexing:

1. Enable guest file system indexing on the Guest Processing step of the backup job wizard. For details, see the File Indexing section of the Veeam Agent for Microsoft Windows User Guide.
2. Run the backup job with guest file system indexing enabled.
3. Make sure the indexing data is imported to the Veeam backup database, and catalog replication is completed successfully. For details, see the Performing Catalog Replication and Indexing section.

If you restore files from an indexed guest OS, you do not need to mount the restore point for browsing purposes — file hierarchy is presented using the index. The restore point will be only mounted once (during 1-Click file restore process itself) — to the mount server associated with backup repository where Veeam Agent backups are stored.

Alternatively, you can process the backups created without guest file system indexing — for example, if indexing was disabled at restore point creation time, or if indexing operation failed. For such a server, its selected restore point first will be mounted (for the browsing and search purposes) to the Veeam backup server integrated with Veeam Agent. After you locate the necessary file and initiates 1-Click file restore, the restore point will be mounted to the mount server associated with the repository.

Other Prerequisites

During guest file restore to the original location, you are prompted for the credentials to access the target Windows server. Enter a user name and password; make sure that the account has sufficient access rights.

Non-Windows Server

Preparing Backup

You can restore files from a backup of a physical server created with or without indexing.

> **NOTE**
>
> Veeam Agent for Mac does not support file system indexing.

To prepare a backup with guest file indexing:

1. Check for the following utilities to be installed on the server: `mlocate`, `gzip`, and `tar`. These utilities are required for file indexing. When you enable file indexing, Veeam Agent will prompt you to deploy them in case they are not found.
2. Enable guest file system indexing in the backup job settings.

   For more information, see the File System Indexing section of the following guides:

   - Veeam Agent for Linux User Guide
   - Veeam Agent for Oracle Solaris User Guide
   - Veeam Agent for IBM AIX User Guide
3. Run the backup job with guest file system indexing enabled.
4. Make sure the indexing data is imported to Veeam backup database, and catalog data replication is completed successfully. For more information, see Performing Catalog Replication and Indexing.

Whether you restore from a backup with or without guest file indexing, prepare a machine to operate as an FLR helper appliance.

Preparing FLR Helper Appliance

To perform guest file restore, configure an FLR helper appliance on the Veeam backup server with which Veeam Agent is integrated. FLR helper configuration is similar to that described in the Restoring VM Guest OS Files (Multi-OS) section of the Veeam Backup & Replication User Guide. The only difference is that for restore of a physical machine, you can configure a helper appliance to work on a machine running on the platform of your choice (VMware or Hyper-V). Helper appliance settings are saved in Veeam Backup & Replication database on per-user basis. The settings are applied each time the user starts file-level restore.

When guest file-level restore is started from Veeam Backup Enterprise Manager, FLR helper configuration settings are obtained from the database of the Veeam backup server. If no FLR helper configuration is found for the current user account, Veeam Backup & Replication uses the default settings (set during the latest FLR appliance configuration process in Veeam backup console). Thus, before you start file-level restore from Enterprise Manager, make sure that FLR helper settings are configured on Veeam backup server.

> **NOTE**
>
> If you plan to deploy multiple FLR helper appliances to restore machines backed up by Veeam Agents integrated with different Veeam backup servers, their initial configuration should be performed on the backup servers. Centralized configuration from Veeam Backup Enterprise Manager is not supported.

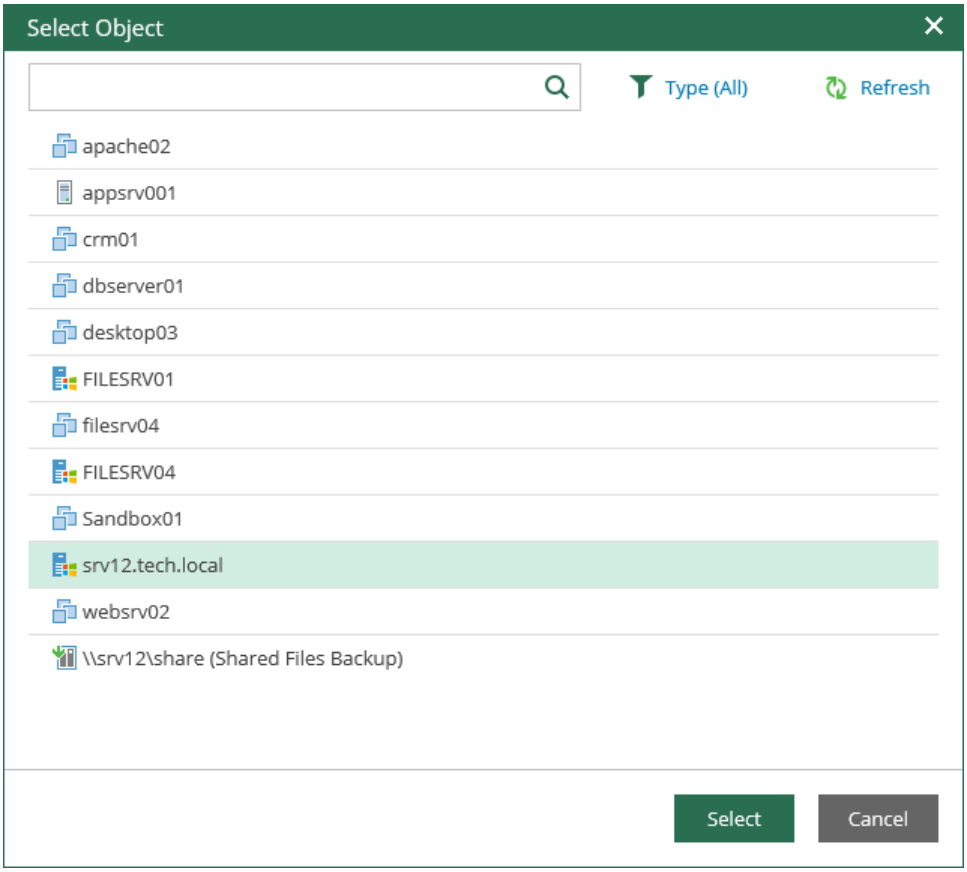
Other Prerequisites

1. Make sure that the DNS name of the target (original) server where you plan to restore the files is resolved properly.
2. During guest file restore to the original location, you are prompted for the credentials to access the target server. Specify a user name and password or private key for the account with sufficient access rights.

Browsing and Restore Procedures

To browse guest OS files in a physical server backup:

1. In the Enterprise Manager main window, click the **Files** tab.
2. Select a necessary server. You can type in a server name or pick it from the list. Note that server icons indicate server OSes.



3. If the server is backed up without guest indexing, click **Mount Backup** and wait for the process to complete.
4. In the **Restore point** field in the top left corner of the **Files** tab, select a necessary date of backup and a restore point. Note that the dates when backup of the selected server was performed are highlighted in the calendar.
5. To search for a file, take the steps similar to the Searching Guest OS Files in Machine Backups procedure.
6. To restore a file, take the steps similar to the Performing 1-Click File Restore procedure.

NOTE

File restore from backups of Veeam Agent for Mac, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX to the original location is not available.

IMPORTANT

When restoring files to the original location, you are prompted for user credentials to the target machine. Make sure the account you provide has sufficient access rights.

Application Item Restore

If your Veeam Backup & Replication is integrated with the Server edition of Veeam Agent, and other prerequisites are met, you can use the backups of the physical application servers (Microsoft SQL Server and Microsoft Exchange Server) to restore the necessary application items.

To restore application items, follow the procedures described in the following sections:

- Restore procedure for Microsoft Exchange mailbox items
- Restore procedure for Microsoft SQL Server database items

Working with File Shares

With Veeam Backup Enterprise Manager, authorized users can perform management operations with file shares processed by Veeam Backup & Replication: search and view file share backups, restore files from these backups and delete backups.

> **IMPORTANT**
>
> Restore scope (list of objects a user can recover) can be customized if you have the Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all objects and cannot be customized. However, you can delegate recovery of entire file shares or selected file types. Possible delegation options are described in the Configuring Restrictions for Delegated Restore section.

Viewing File Share Backups

From Veeam Backup Enterprise Manager, you can view information about file shares processed by backup jobs configured on Veeam backup servers. To view the file shares, open the **File Shares** tab. Each entry in the list contains the following data: file share name, path to backup file, number of restore points, backup server to which the job relates, job name and status of the last job run.

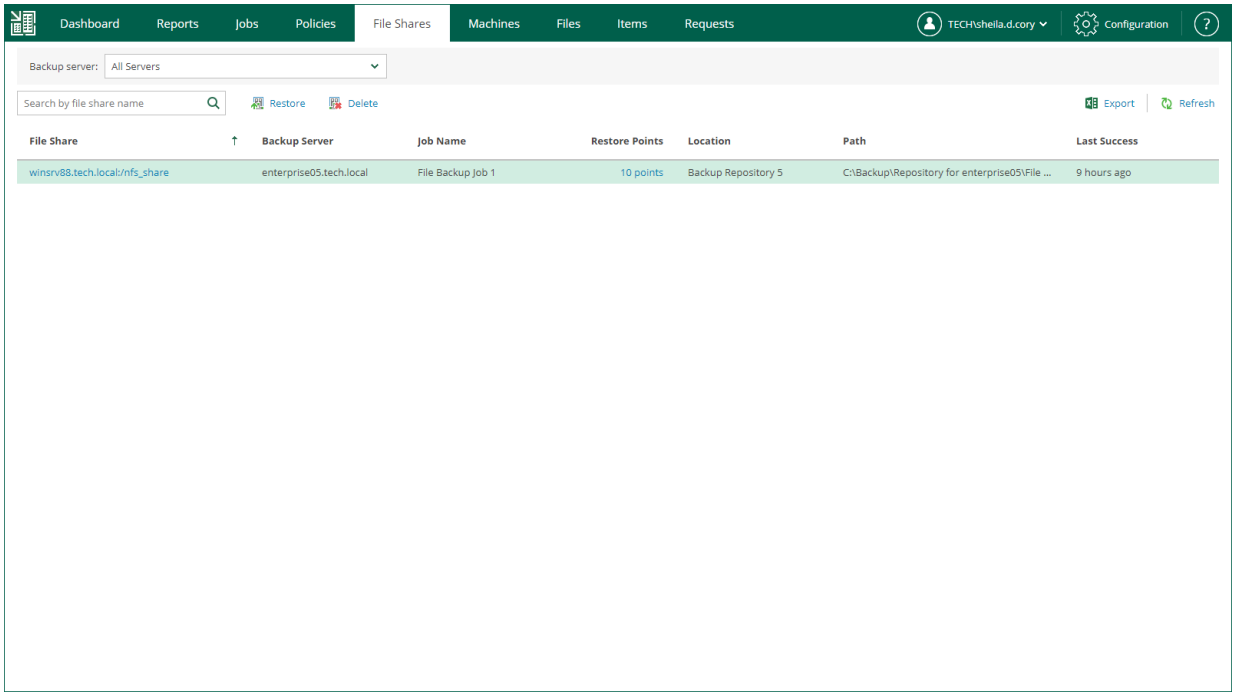
Veeam Backup Enterprise Manager allows you to search for the necessary file share in the list of file shares. This may be useful in case you manage large backup infrastructure with multiple backup servers that process multiple file shares.

You can search for file shares in one of the following ways:

- Filter file shares by the backup server. To do this, from the **Backup server** list, select the necessary backup server. Veeam Backup Enterprise Manager will display backups of only those file shares that are processed by the selected backup server.

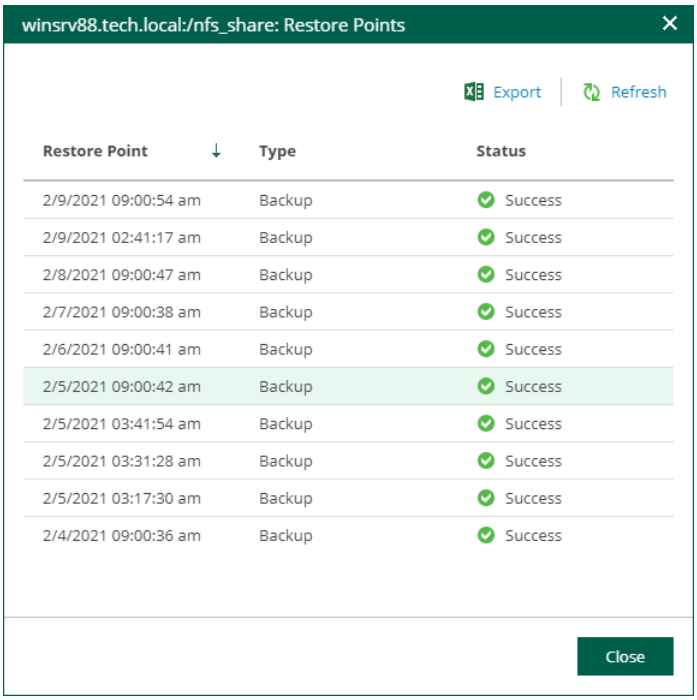
  > **NOTE**
  >
  > The **Backup server** filter is only available for users with the Portal Administrator or Portal User role.

- Search file shares by the file share name. To do this, enter the name or a part of the name in the search field. Veeam Backup Enterprise Manager will display backups of only those file shares whose names match the text that you entered.



Besides the information presented in the list of file shares, the **File Shares** tab allows you to view advanced data about each file share:

- To see detailed information about a file share, click its name in the **File Share** column.
- To see detailed information about file restore points, click a link in the **Restore Points** column.



NOTE

You can export displayed information to a file using the **Export** link on the toolbar. This file then can be opened on the client machine using the associated application.

Browsing File Share Backups

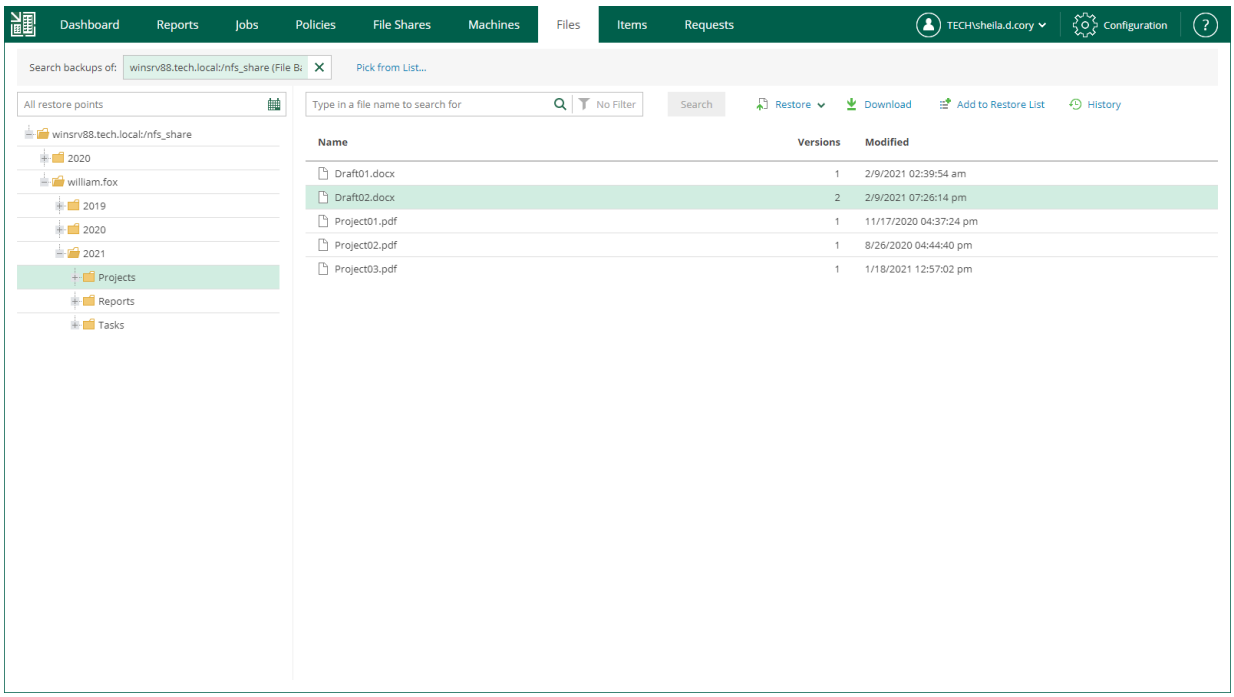
You can browse file share backups for backed-up files. Note that with the file browsing functionality, you can browse for files in the selected file share backup only.

If you use the Enterprise or Enterprise Plus edition of Veeam Backup & Replication in your virtual environment, consider that Enterprise Manager keeps index files for backups that are currently stored on disk and for archived backups (for example, backups that were recorded to tape). Thus, you will be able to browse and search through backup contents even if the backup in the repository is no longer available.

To browse files in a file share backup:

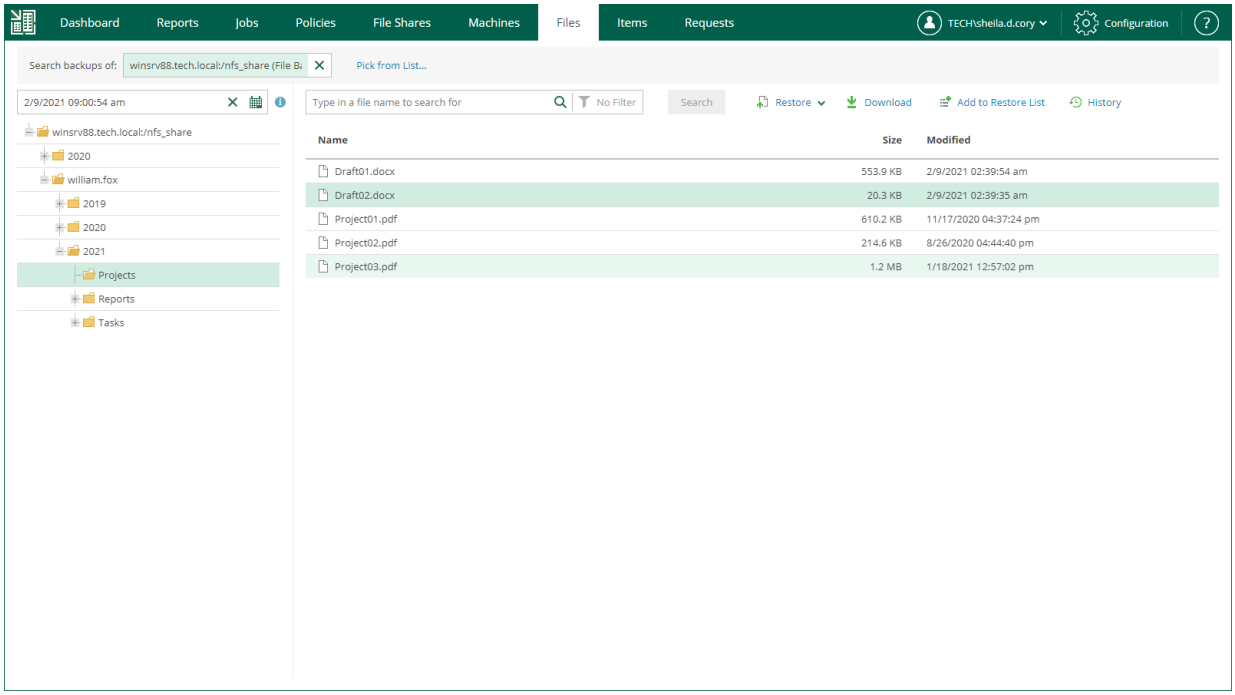
1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a file share whose files you want to browse or click the **Pick from List** link and select the necessary file share in the **Select Object** window.
3. Click **Mount**.
4. Wait while Veeam Backup & Replication mounts the file share from the backup to the backup server. When the process is completed, Veeam Backup Enterprise Manager displays the content of the backed-up file share.
5. You can browse files contained in all restore points created by the file share backup job or in a specific restore point.
   - By default, the **All restore points** option is selected. With this option selected, you can browse files contained in all restore points created by the file share backup job.

     For each file in the backup, Enterprise Manager displays the number of file versions and the date when the latest file version is created. If a file has more than one version, you can select a necessary file version during the restore process. For more information, see Performing File Restore.



- To select a specific restore point, click the calendar icon in the restore point field and select the necessary backup date and a restore point created on that date. Note that you cannot select a date on which the backup was not performed.

  For each file in the backup, Enterprise Manager displays file size and the date when the file version is created. Enterprise Manager displays only the file version contained in the selected restore point. For more information on file restore, see Performing File Restore.



TIP

You can use the search field at the top of the working area to search for specific files and folders. Depending on the number of files in the file share, the search process may take some time.

Performing File Restore

After you locate the necessary file, you can use Veeam Backup Enterprise Manager to restore it from the backup. You can choose to restore a file to the original location or download it to the local machine.

Restore operations are only available to authorized users according to their security settings. Users with the Portal Administrator role can both restore files to the original location or download them to the local machine.

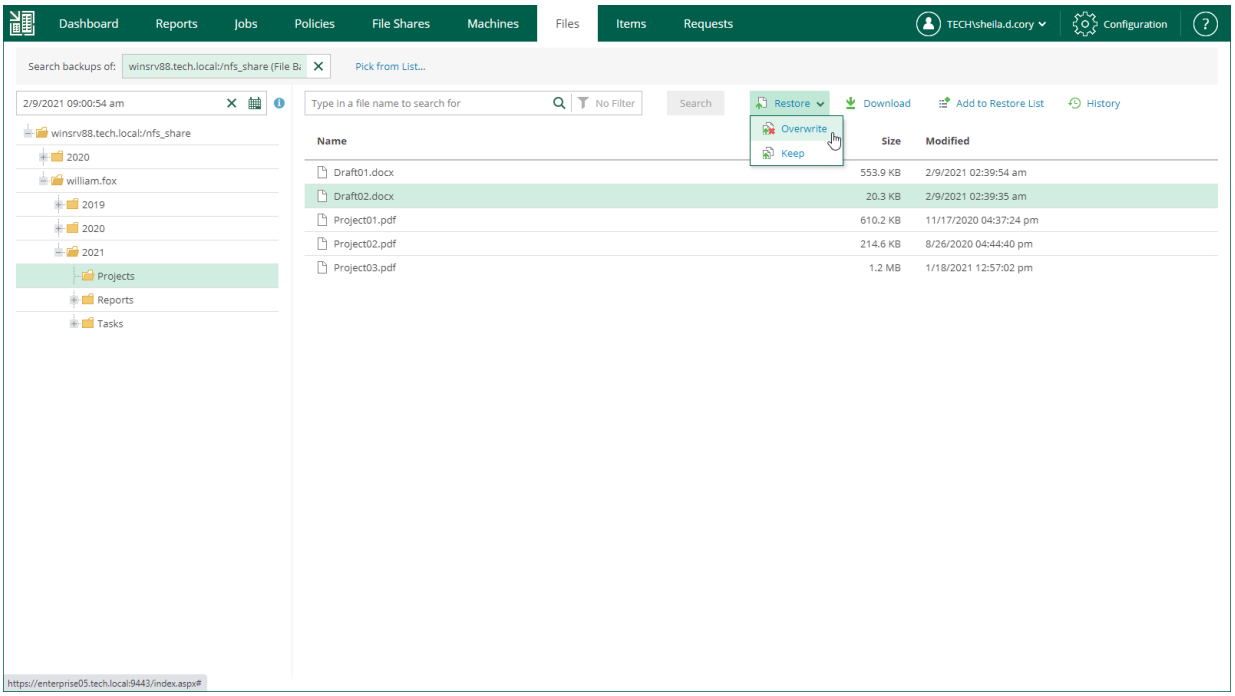
For users with the non-administrative roles, you can configure additional restriction settings. For example, you can prohibit restore operators to download files to the local machine so that they will be able to restore files to the original location only. Additionally, you can specify the types of files that can be restored by operators (this can be helpful if you want to limit operators' access to sensitive data). For details, see Configuring Accounts and Roles.

Restoring Files to Original Location

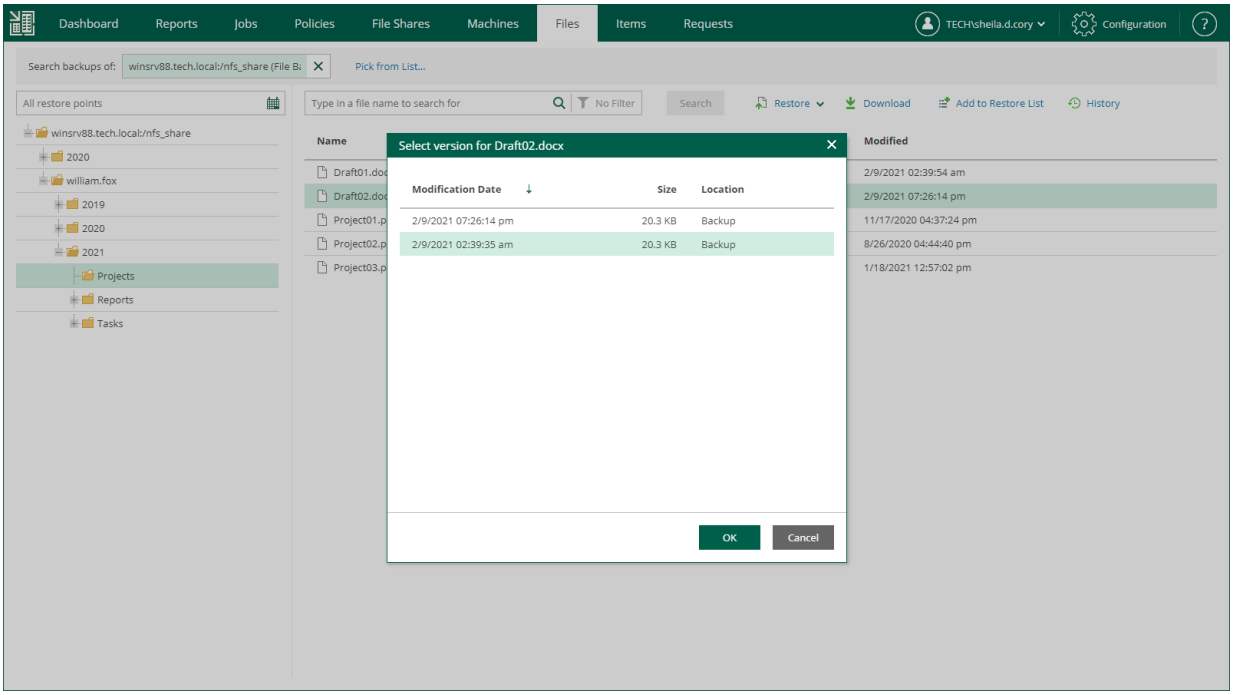
In this restore scenario, Veeam Backup Enterprise Manager will extract the file from the backup and restore it to the original location in the file share. Restoring files to the original location is the most secure file recovery method, as the user who initiates the file restore operation in the Enterprise Manager UI cannot access the file itself.

To restore a file to the original location:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. Multiple selection is also possible. For details, see Viewing File Share Backups and Browsing File Share Backups.
2. Click **Restore** and select how to restore selected files:
   - If you select **Overwrite**, the file from the backup will replace the original file in the file share.
   - If you select **Keep**, the file from the backup will be restored next to the original file in the file share. The restored file will have the *_RESTORED_<date>_<time>* suffix in the file name.



3. If you browse for files in all restore points created for the file share, and the restore points contain multiple versions of the file that you want to restore, Veeam Backup Enterprise Manager will prompt you to select the file version. In the **Select version** window, select the restore point that contains the necessary file version and click **OK**.



4. In the displayed window, click **Yes**.

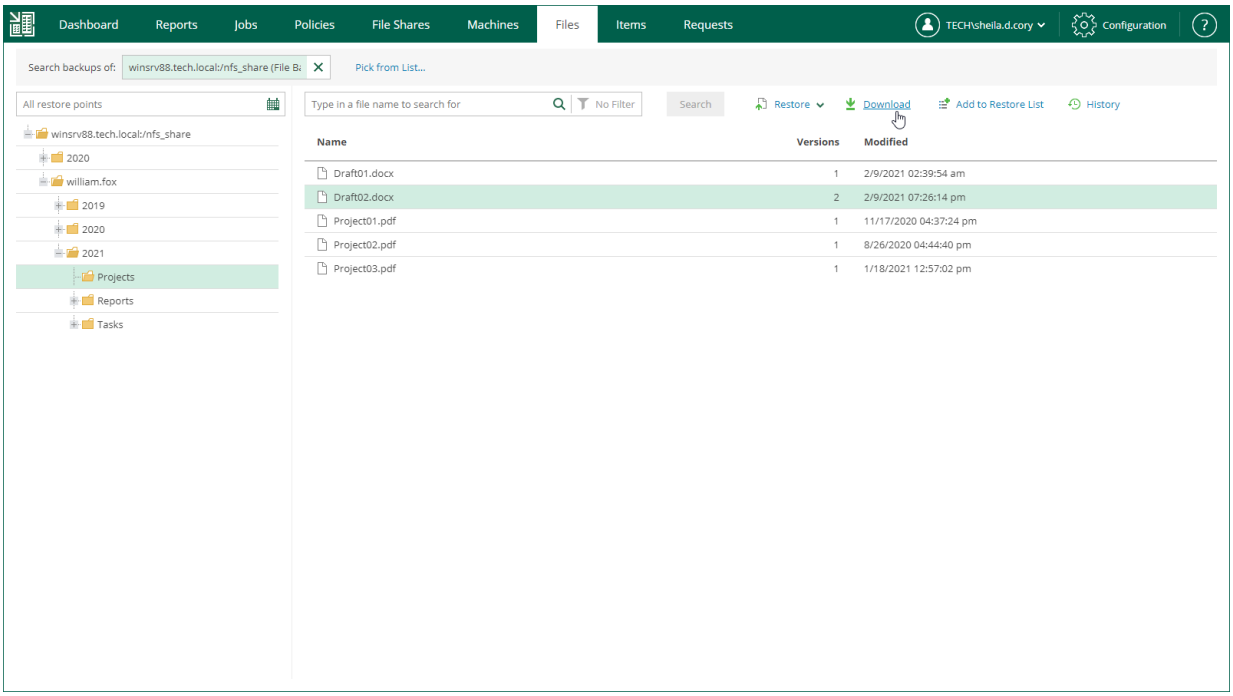
Veeam Backup Enterprise Manager will start the restore operation and display the progress and result of the operation in the **File Restore History** view.

Downloading Files

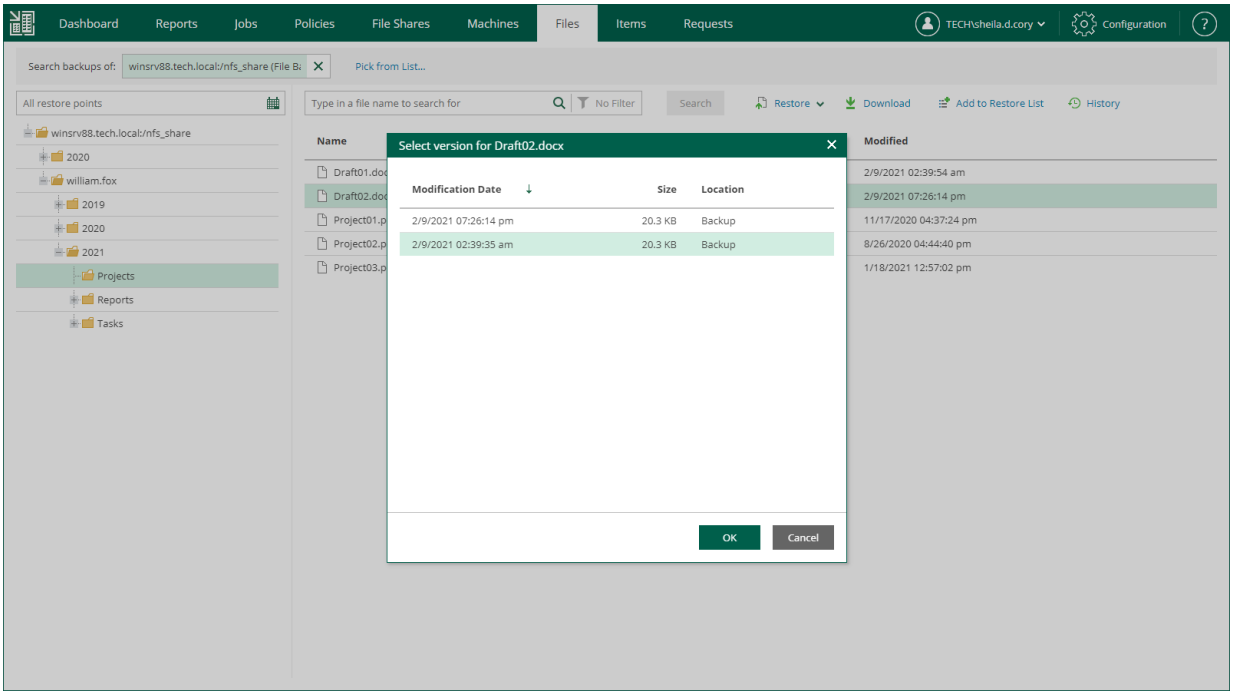
If you choose to download the restored file, Veeam Backup Enterprise Manager interacts with the Veeam backup server to extract the necessary file from the backup. The user who initiated file restore will be able to download the file to the local machine, that is, the Veeam Backup Enterprise Manager server.

To download a file:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For details, see Viewing File Share Backups and Browsing File Share Backups.
2. Click **Download**.



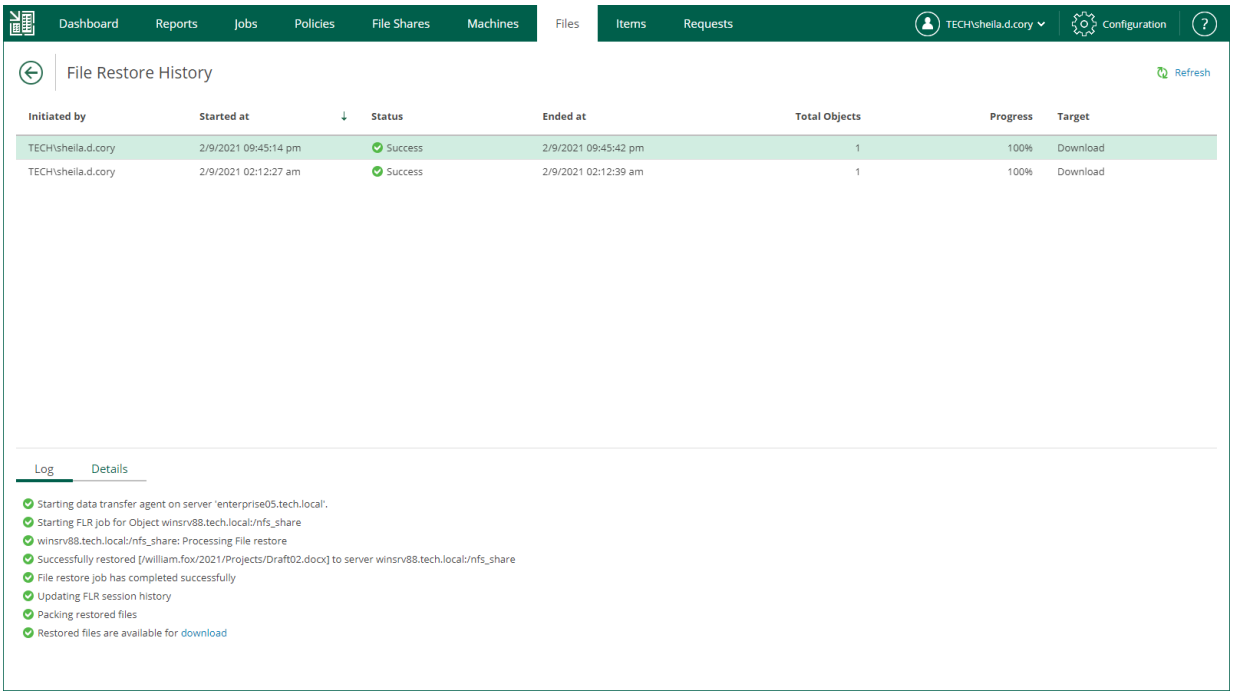
3. If you browsed for files in all restore points created for the file share, and the restore points contain multiple versions of the file that you want to restore, Veeam Backup Enterprise Manager will prompt you to select the file version. In the **Select version** window, select the restore point that contains the necessary file version and click **OK**.



4. In the displayed window, click **Yes**.
5. Wait for restore session to complete and the file to be retrieved from the backup.
6. Select the file from the list.
7. In the **Log** tab of the **File Restore History** view, click the **download** link in the *Restored files are available for download* record of the session log.

   The file is saved to the default download folder on your local machine.

If you download a single file, it is also saved in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Multiple files are packed in a ZIP file named `FLR_<date>_<time>.zip` and stored in the same folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.



Restoring Multiple Files

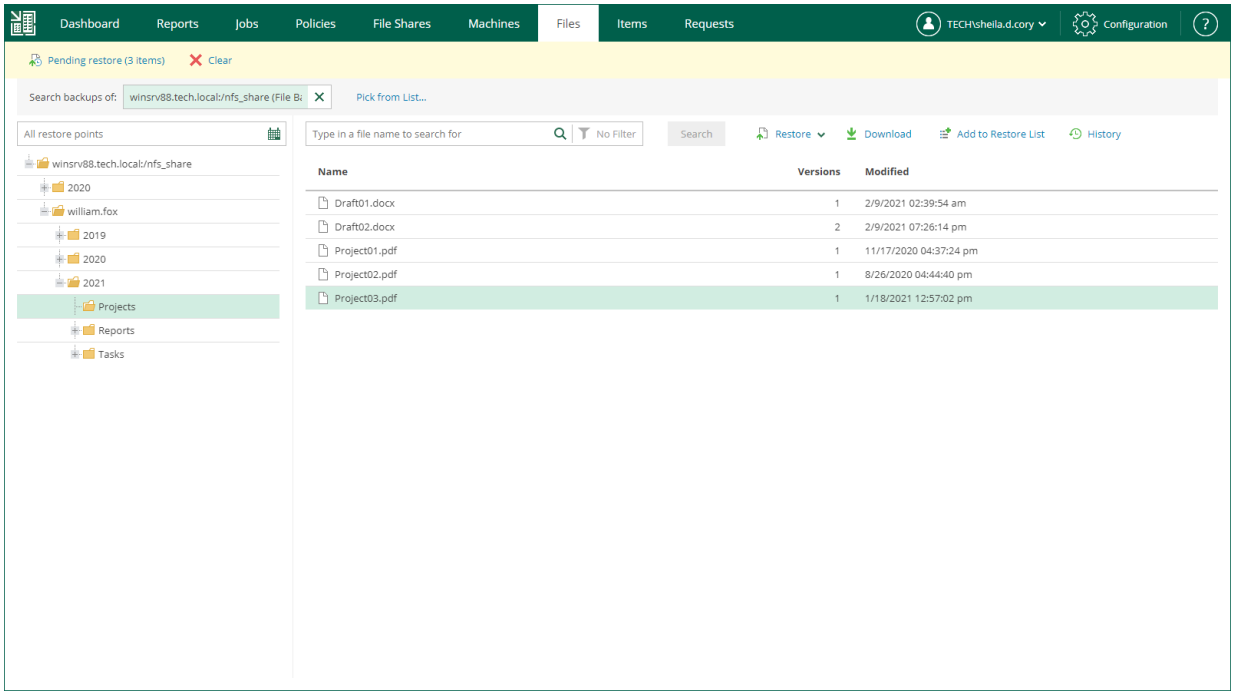
In addition to restoring single files from selected restore points, Veeam Backup Enterprise Manager supports bulk restore. If you need to restore multiple files at once, you can select more than one file in the preview pane when browsing, and then use the **Restore** command, or add the necessary files to the restore list and then restore all files at once. Unlike the **Restore** command, using the restore list helps you to prepare for restore files from different file shares and restore points.

To add a file to the restore list:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For more information, see Viewing File Share Backups and Browsing File Share Backups.
2. Click **Add to Restore List**.
3. If you browsed for files in all restore points created for the file share, and the restore points contain multiple versions of the file that you want to restore, Veeam Backup Enterprise Manager will prompt you to select the file version. In the **Select version** window, select the restore point that contains the necessary file version and click **OK**.

> **NOTE**
>
> You cannot add multiple versions of the same file to the restore list using the **Select version** window. If you want to restore multiple versions of a file, browse to this file in a specific restore point and add this file to the restore list.

When a file is added to the restore list, the **Pending restore** notification appears at the top of the Enterprise Manager UI window.



To restore files added to the restore list:

1. In the restore list notification, click **Pending restore**.

2. In the **Pending Restore** window, select check boxes next to the files that you want to restore. Use the check box next to the header of the **Name** column to select all files in the list at once.

   If you want to remove a file from the restore list, select the file and click **Delete**.

3. Click the **Restore** or **Download** link to perform the necessary restore operation for the selected files.

4. In the displayed window, click **Yes**.

5. [For the download operation] Wait for restore session to complete. In the **Log** tab of the **File Restore History** view, click the **download** link.

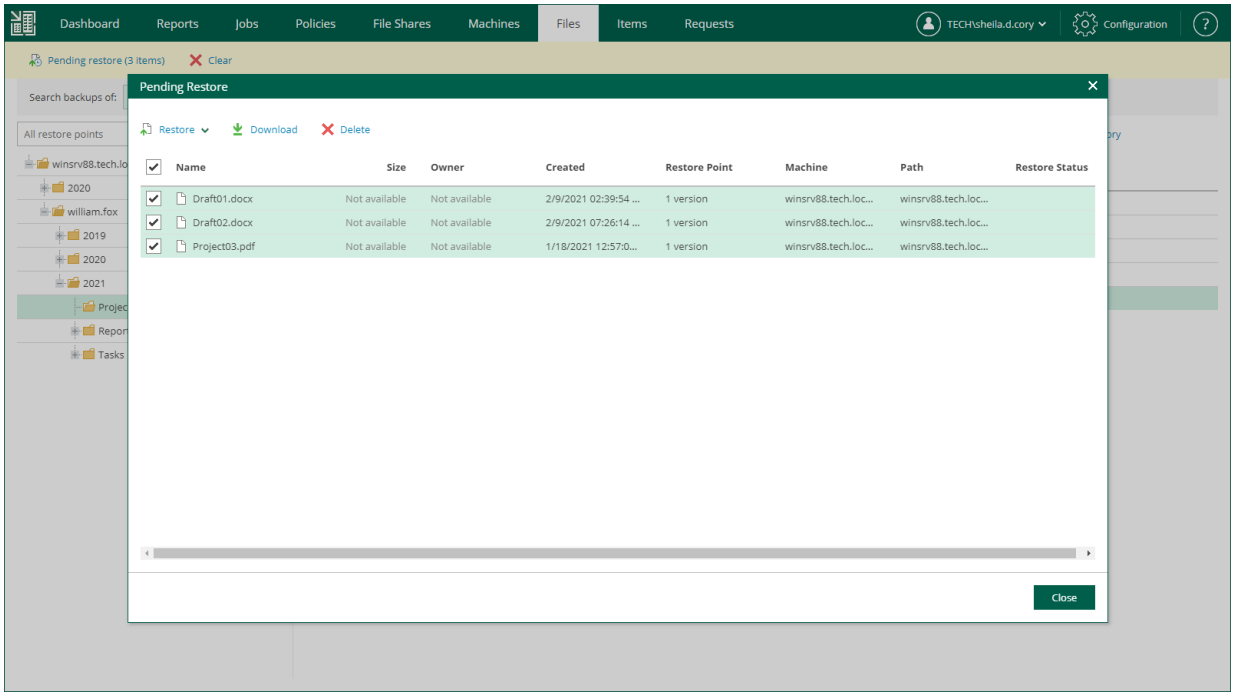
   The files are saved to the default download folder on your local machine.

   Multiple files are also saved in a ZIP file named `FLR_<date>_<time>.zip` in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.

TIP

Veeam Backup Enterprise Manager keeps links for downloaded files in the history for one day. To download a file that was previously restored:

1. In the **Files** tab, click **History**.
2. In the **File Restore History** view, select the necessary restore session.
3. In the **Log** tab, click the **download** link.



Deleting File Share Backups

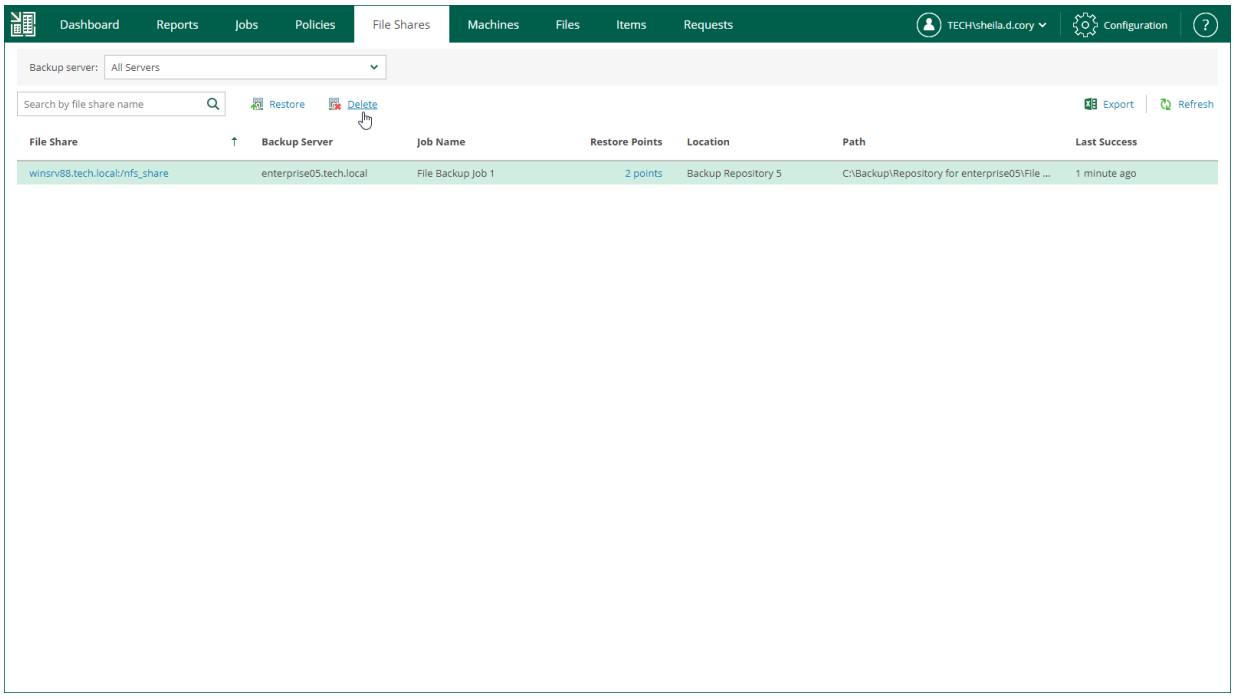
You can delete file share data from a backup created by a backup job in a backup repository. The deleted file share is not removed from the list of file shares immediately. The file share will be removed from the list after records about the file share are removed from the configuration database on the Veeam backup server. Once this operation completes, a notification will appear at the top of the Enterprise Manager UI window.

To delete a file share backup:

1. In Veeam Backup Enterprise Manager, open the **File Shares** tab.
2. In the list of file share backups, select the necessary backup and click **Delete**.

   To locate the necessary backup, you can filter file share backups by the backup server or search by the file share name.
3. In the displayed window, click **Yes**.

> **NOTE**
>
> If several file shares are processed by the same backup job, deletion of the selected file share backup will not affect other file shares in the job.



Working with Machines

With Veeam Backup Enterprise Manager, authorized users can perform the following operations with machines:

- View machines and delete them from backups
- Create on-demand incremental backups (quick backups) for machines
- Restore machines and VM disks from backups
- Failover to VM replicas and vCloud Director vApps
- Run failover plans for VMware vSphere and Microsoft Hyper-V VMs

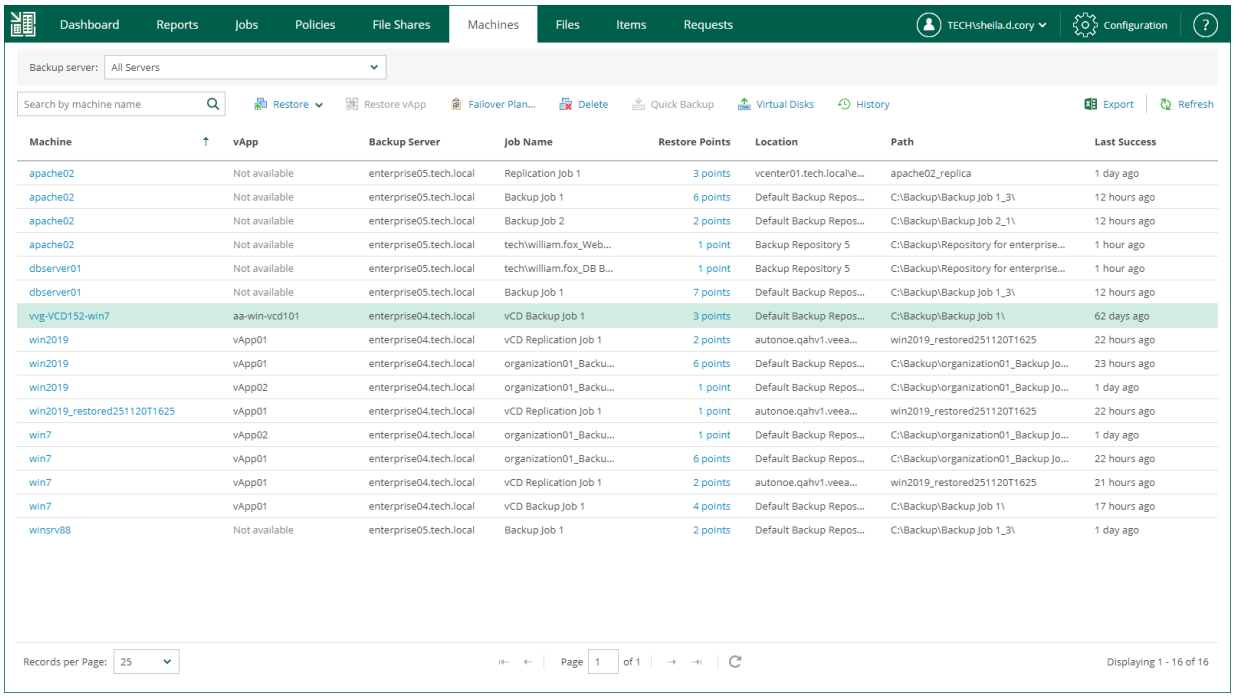
IMPORTANT

Restore scope (list of machines a user can recover) can be customized if you have the Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all machines and cannot be customized. However, you can delegate recovery of entire machines, guest files, or selected file types. Possible delegation options are described in the Configuring Restrictions for Delegated Restore section.

Viewing, Searching, Deleting Machines

From Veeam Backup Enterprise Manager, you can view information about all machines engaged in performed jobs configured on Veeam backup servers. To view the machines, open the **Machines** tab. Each entry in the list contains the following data: machine name, path to backup file, number of restore points, backup server to which the job relates, job name and status of the last job run.

You can filter machines in the list by a backup server or search for specific machines by a machine name. To search for a machine, enter its name or part of the name in the **Search** field.

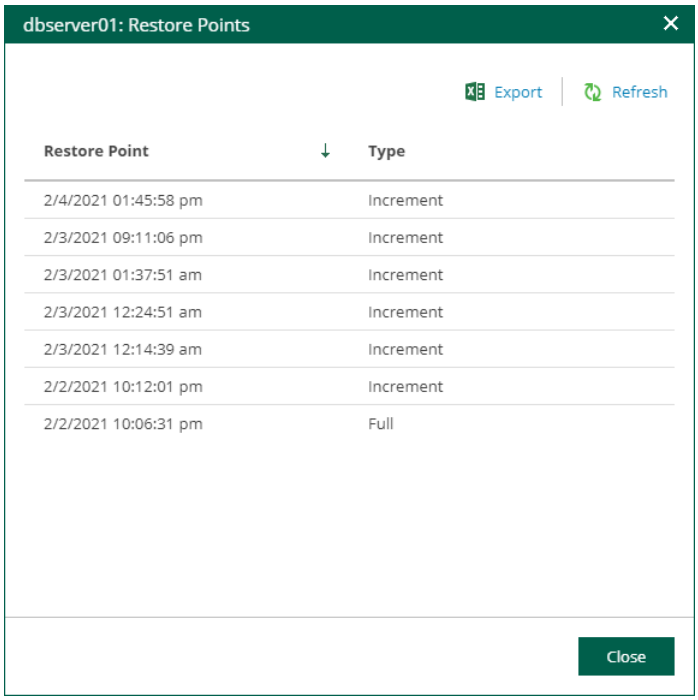


Besides the information presented in the list of machines, the **Machines** tab allows you to view advanced data about each machine:

- To see detailed information about a machine, click its name in the **Machine** column.
- To see detailed information about machine restore points, click a link in the **Restore Points** column.

NOTE

You can export displayed information to a file using the **Export** link on the toolbar. This file then can be opened on the client machine using the associated application.



Deleting Machine from Backups

To delete a machine from a backup:

1. On the **Machines** tab, select the necessary machine backup from the list of machines.

   To quickly find a machine, you can filter machines in the list by a backup server or search for specific machines by a machine name.

2. Click **Delete**.

3. To remove backups marked with weekly, monthly and yearly GFS flags, select the **Remove GFS full backups** check box.

   The check box is displayed if the machine has GFS backups.

4. Click **Yes** to confirm deletion.

The deleted machine is not removed from the list of machines immediately. The machine will be removed from the list after records about the machine are removed from the configuration database on the Veeam backup server. Once this operation completes, a notification appears at the top of the Enterprise Manager UI window.

NOTE

Consider the following:

- If several machines are processed by the same backup job, deletion of the selected machine will not affect other machines in the job.
- The delete operation is not available for replica machines, storage snapshots and machines backed up to tape.

Performing Quick Backup

You can create an ad-hoc incremental backup for one or more machines — quick backup. This backup will be added to the backup chain in the backup repository. Quick backup can be helpful if you want to produce an additional restore point for one or more machines in the backup job and do not want to configure a new job or modify the existing one.

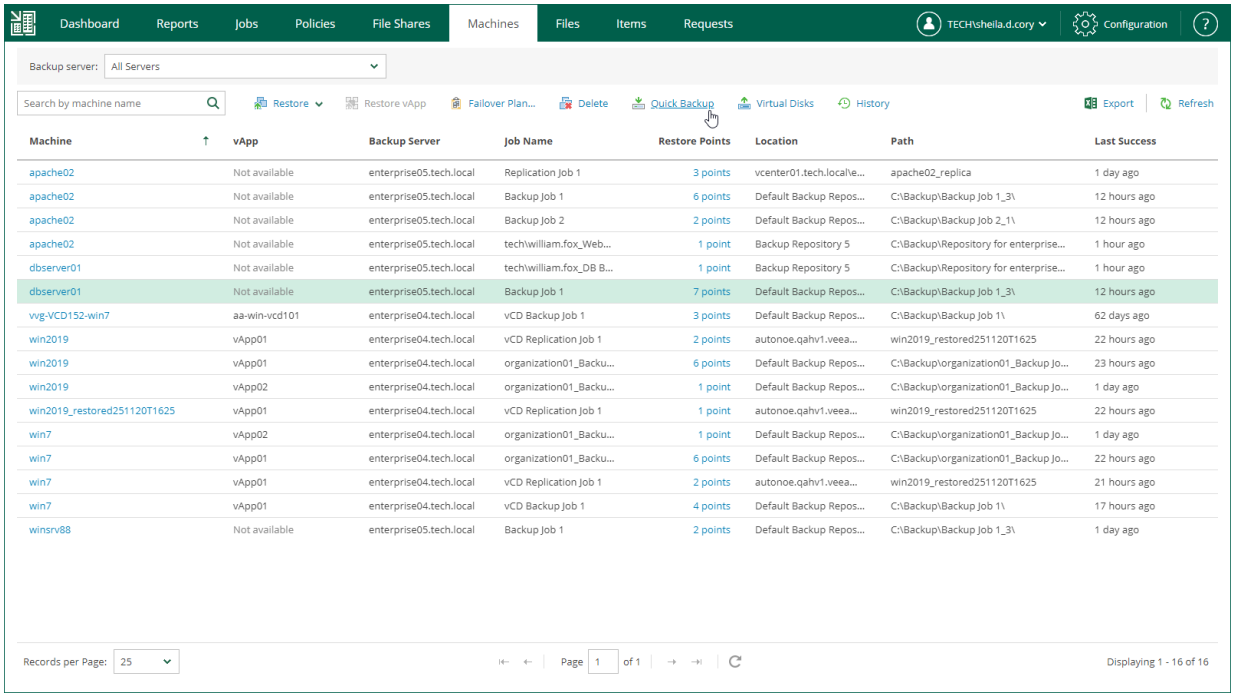
Quick backup can be performed for machines that meet the following requirements:

- A backup job processing the machine exists on the backup server.
- A full backup file for the machine exists in the backup repository.

> **NOTE**
>
> Quick backup is not available for vCloud Director VMs and Veeam Agent machines.

To perform quick backup, on the **Machines** tab, select the machine you need and click **Quick Backup**.

Veeam Backup & Replication will trigger a backup job to create a new incremental restore point for the selected machines. Details of the running quick backup operation are displayed in the job session window.



Performing 1-Click Restore

Authorized users can restore machines from backups to the original location included in their scope. Users with the Portal Administrator role have no scope limitations. For more information on restore scope, see Configuring Restore Scope.

IMPORTANT

- 1-Click Restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- 1-Click Restore from any storage snapshots, Veeam Agent backups and backups created with Veeam Plug-ins for Enterprise Applications are not supported by Veeam Backup Enterprise Manager.

To restore a machine from the backup:

1. On the **Machines** tab, select the necessary machine backup in the list of machines.

   To quickly find a machine, you can filter machines in the list by a backup server or search for specific machines by a machine name.

2. Click **Restore** and select one of the following restore options:

   - Select **Overwrite** if you want to replace the original machine in the production environment with the machine from the backup.
   - Select **Keep** if you want to restore the machine from the backup next to the original machine in the production environment.

   NOTE

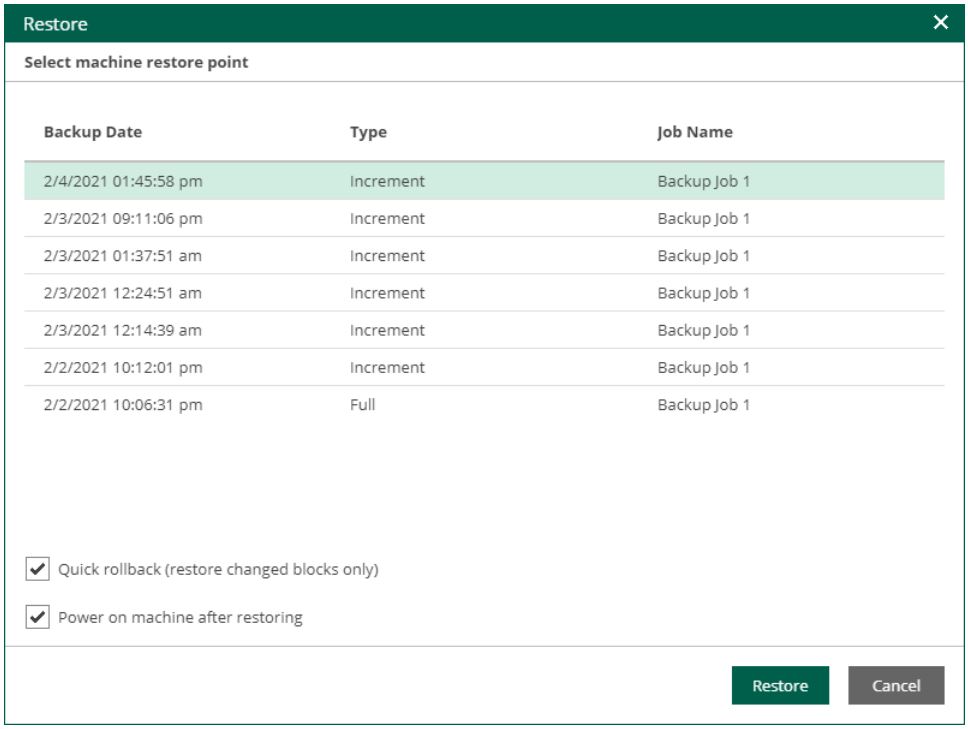
   Veeam Backup Enterprise Manager supports machine restore to the original location only. You cannot restore a VM to another location or with different settings (such as network settings, format of restored virtual disks and so on).

3. In the **Restore** window, select a restore point that will be used to restore the machine.
4. [Optional] Instead of restoring an entire machine from a backup file, you can instruct Enterprise Manager to recover only those data blocks that are necessary to revert the machine to the selected restore point. To do this, select the **Quick rollback** check box. Quick rollback significantly reduces the recovery time and has little impact on the production environment.

   For more information on quick rollback, see the Quick Rollback section of the Veeam Backup & Replication User Guide.

5. [Optional] To start a machine immediately after recovery, select the **Power on machine after restoring** check box.

6. Click **Restore**. Veeam Backup Enterprise Manager will display a message notifying you of the operation effect (machine from backup will replace the production machine if it is present in the original location). Click **Yes** in the message window to start the restore operation.



Performing Failover

Authorized users can perform the following failover operations:

- Failover of a VM processed by a regular replication job
- Failover of a VM processed by a CDP policy
- Failover of a vApp processed by a vCloud Director replication job

Users with the Portal User and Restore Operator roles can perform failover of machines included in the restore scope. Users with the Portal Administrator role have no restore scope limitations. For more information on restore scope, see Configuring Restore Scope.

> **IMPORTANT**
>
> Failover is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Performing Failover to VM Replica

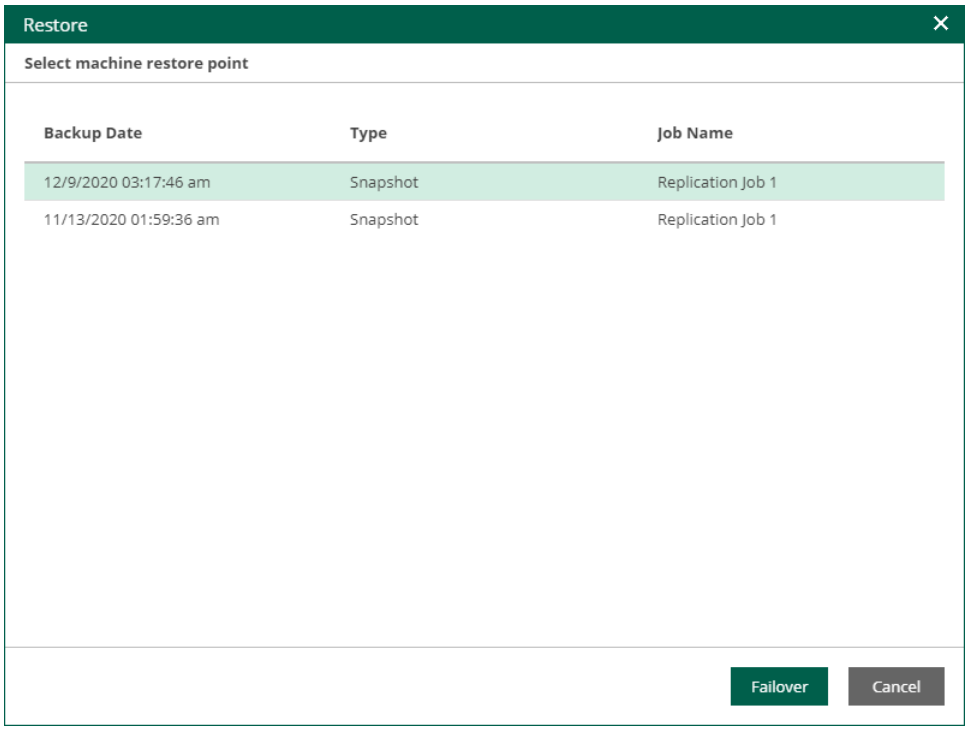
If a VM is processed by a regular replication job, you can fail over the VM to its replica. After the failover operation completes, the VM replica is powered on.

Failover is an intermediate step that needs to be finalized. To do that, you can undo failover, perform permanent failover or perform failback. You can take the final step in the Veeam Backup & Replication console. For more information, see the Replica Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover:

1. On the **Machines** tab, select a machine processed by a replication job.
2. Click **Restore**.
3. In the **Restore** window, select a restore point of the VM.
4. Click **Failover**.

5. To confirm failover, click **Yes**.



To view the failover progress, on the **Machines** tab, click **History**.

Performing Failover to CDP Replica

If a VM is processed by a CDP policy, you can fail over the VM to its replica. After the failover operation completes, the VM replica is powered on.

Failover is an intermediate step that needs to be finalized. To do that, you can undo failover, perform permanent failover or perform failback. The final step you can take in Veeam Backup & Replication console. For more information, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

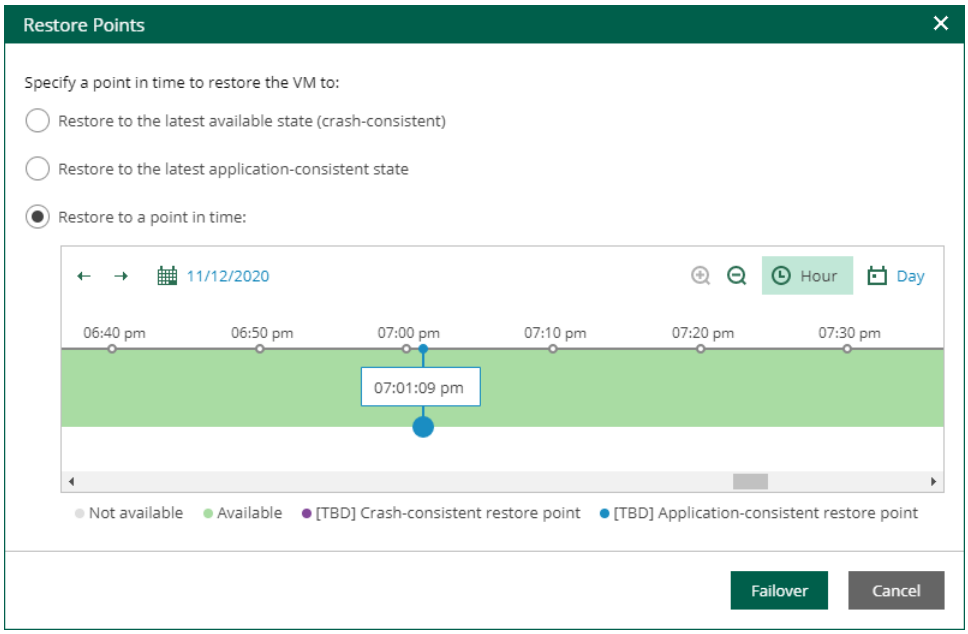
To perform failover:

1. On the **Machines** tab, select a machine processed by a CDP policy.
2. Click **Restore**.
3. In the **Restore** window, select the restore point you need. You can fail over to the latest available crash-consistent state, to the latest application-consistent state or to a specific point in time.

   TIP

   - To quickly find a long-term restore point, use the calendar.
   - To zoom in or zoom out the time line, use the **Plus** and **Minus** buttons or switch between the **Hour** and **Day** views.

4. Click **Failover**.



To view the failover progress, on the **Machines** tab, click **History**.

Performing Failover to vCD Replica

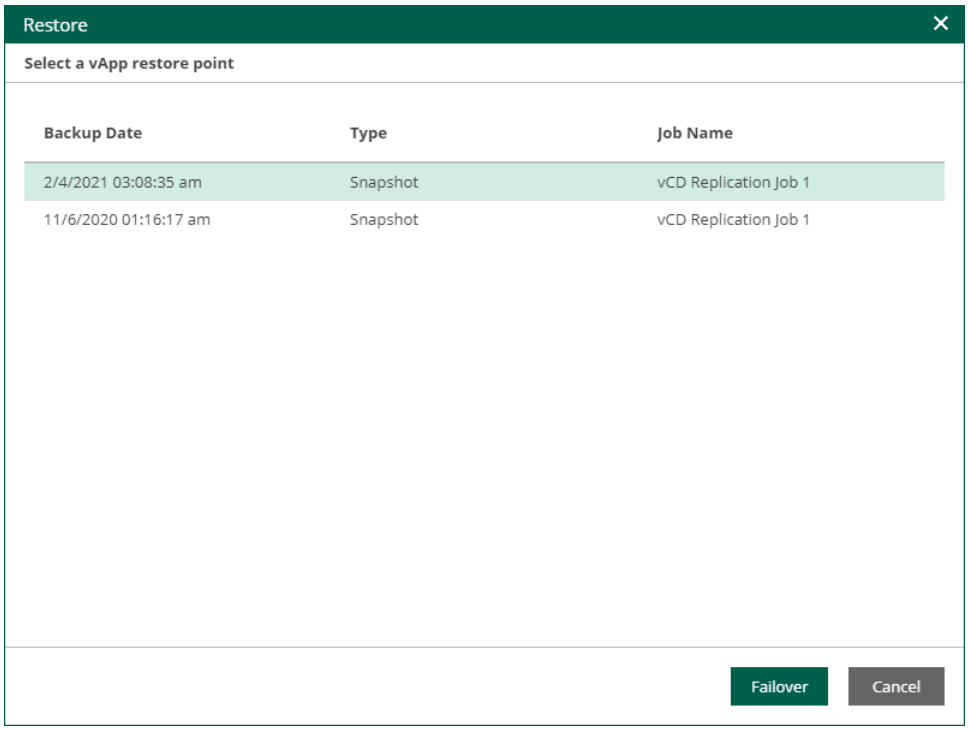
If a VM is processed by a vCD replication job, you can perform failover of the vApp that contains the VM.

Failover is an intermediate step that needs to be finalized. To do that, you can undo failover, perform permanent failover or perform failback. The final step you can take in Veeam Backup & Replication console. For more information, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover:

1. On the **Machines** tab, select a machine processed by a vCD replication job.
2. Click **Restore vApp**.
3. In the **Restore** window, select a restore point of the vApp.
4. Click **Failover**.

5. To confirm failover, click **Yes**.



To view the failover progress, on the **Machines** tab, click **History**.

Performing Virtual Disk Restore

Authorized users can restore virtual disks of machines included in their restore scope. This may be helpful if a VM disk becomes corrupted for some reason. The restored virtual disk can be attached to the original VM to replace a corrupted drive, or connected to any other VM.

For more information on virtual disk restore, see the Virtual Disks Restore section of the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> Consider the following:
>
> 1. This functionality is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
> 2. The disk restore operation is supported for backups of VMware vSphere VMs only.

Users with the Portal Administrator role have no scope limitations. They can restore VM disks to their original location. Restore scope for other users is defined as described in the Configuring Restore Scope section.

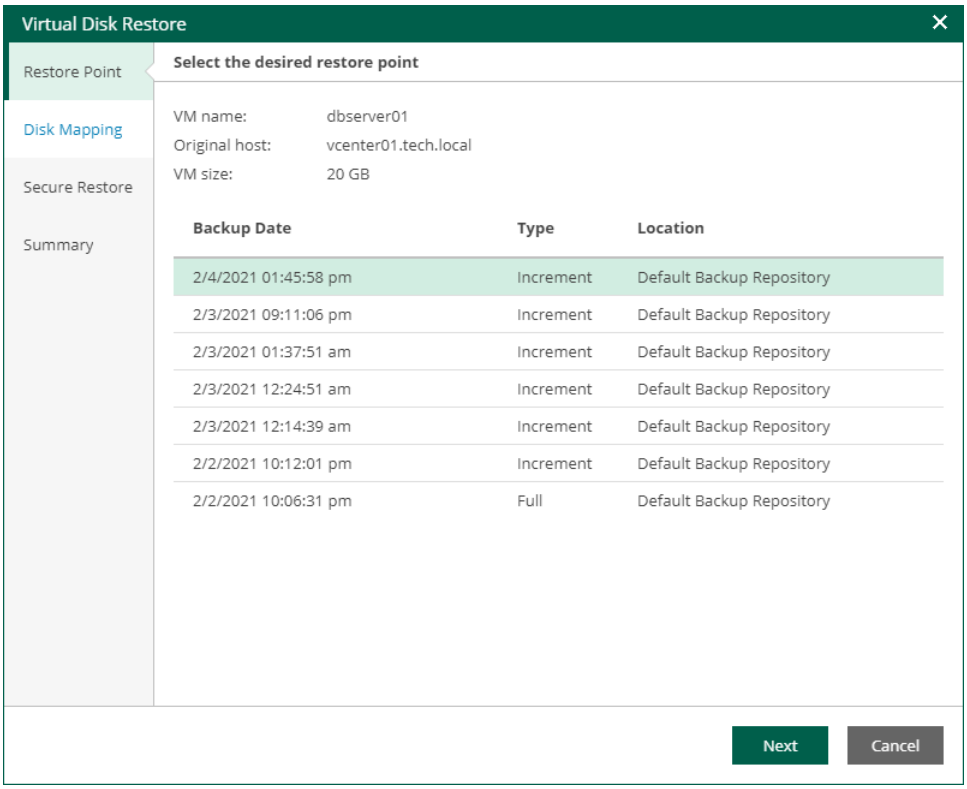
To restore a VM disk from backup:

1. On the **Machines** tab, select the necessary machine backup in the list of machines.

   To quickly find a machine, you can filter machines in the list by a backup server or search for specific machines by a machine name.

2. Click **Virtual Disks** to launch the **Virtual Disk Restore** wizard.

3. At the **Restore Point** step of the wizard, select the restore point that will be used to restore the VM disk.



4. At the **Disk Mapping** step of the wizard, specify VM disk restore settings:

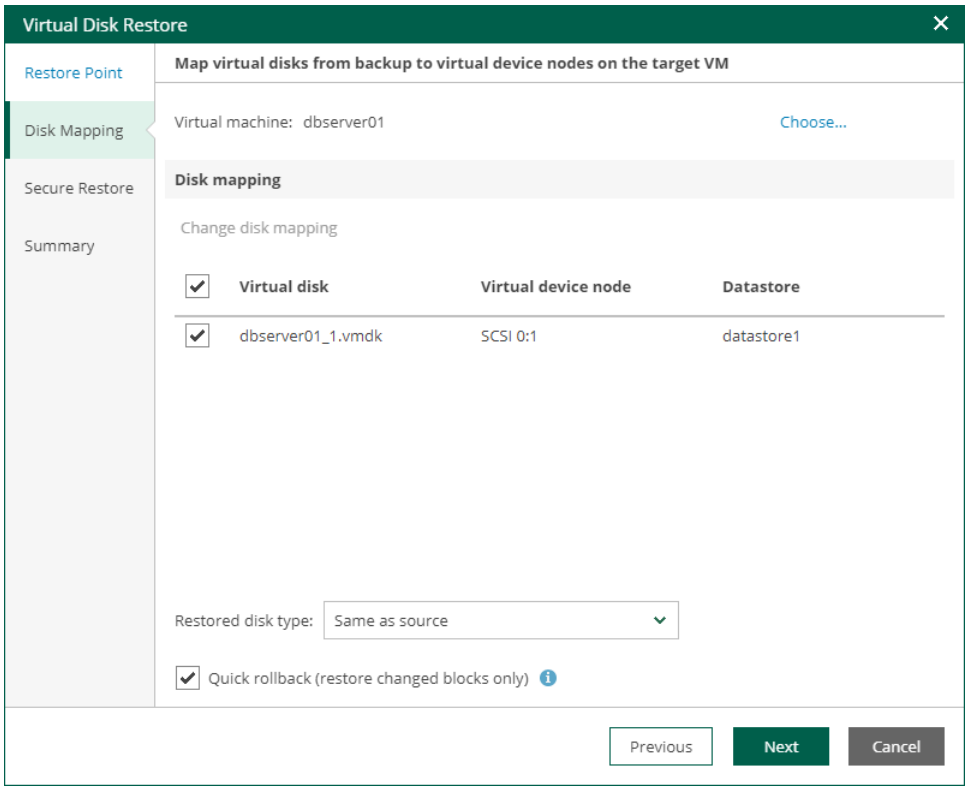
   a. By default, Veeam Backup Enterprise Manager offers you to restore virtual disks to the original VM. To select another VM, click **Choose** next to the **Virtual machine** field and select the necessary VM from the virtual environment.

   b. In the **Disk Mapping** section, select check boxes next to virtual disks that you want to restore.

   c. By default, virtual disks are restored in the original format. To change the disk format, select the necessary option from the **Restore disks** list: *Same as source*, *Thin*, *Thick (lazy zeroed)* or *Thick (eager zeroed)*. For more information about virtual disk types, see VMware Docs.

   > **NOTE**
   >
   > Disk format change is supported only for VMs with Virtual Hardware version 7 or later.

   d. [For disk restore to the original location and with original format] Instead of restoring an entire virtual disk from a backup file, you can instruct Enterprise Manager to recover only those data blocks that are necessary to revert the disk to the selected restore point. To do this, select the **Quick rollback** check box. Quick rollback significantly reduces the recovery time and has little impact on the production environment.



5. By default, virtual disks are restored to the target machine with the original properties. To change properties for the restored disks:

   a. In the **Disk Mapping** section, select the necessary virtual disk and click the **Change disk mapping** link.

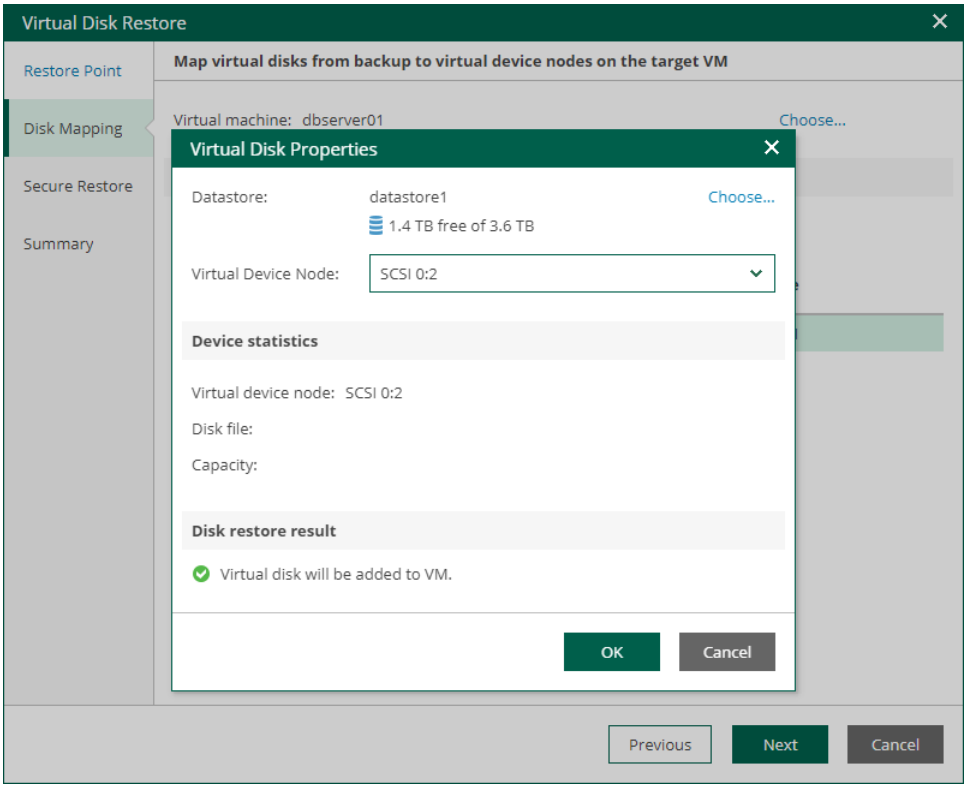
   b. In the **Virtual Disk Properties** window, click **Choose** next to the **Datastore** field and select a datastore where the virtual disk file will be placed.

   c. From the **Virtual Device Node** list, select a virtual device node for the restored disk on the target VM:

      - If you want to replace an existing virtual disk, select an occupied virtual device node.

- If you want to attach the restored disk to the VM as a new drive, select a node that is not occupied yet.

d. Repeat steps a-c for every virtual disk that you want to restore.



6. At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan virtual disk data with antivirus software before restoring the disk. For more information on secure restore, see the Secure Restore section of the Veeam Backup & Replication User Guide.

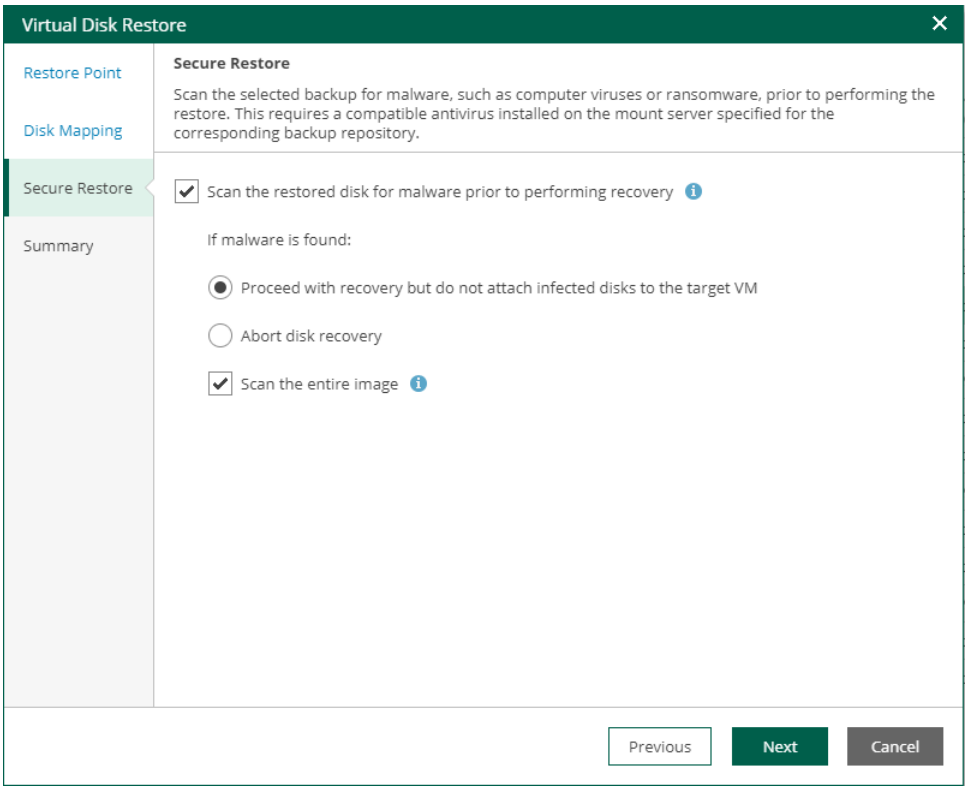
   To specify secure restore settings:

   a. Select the **Scan the restored disk for malware prior to performing recovery** check box.

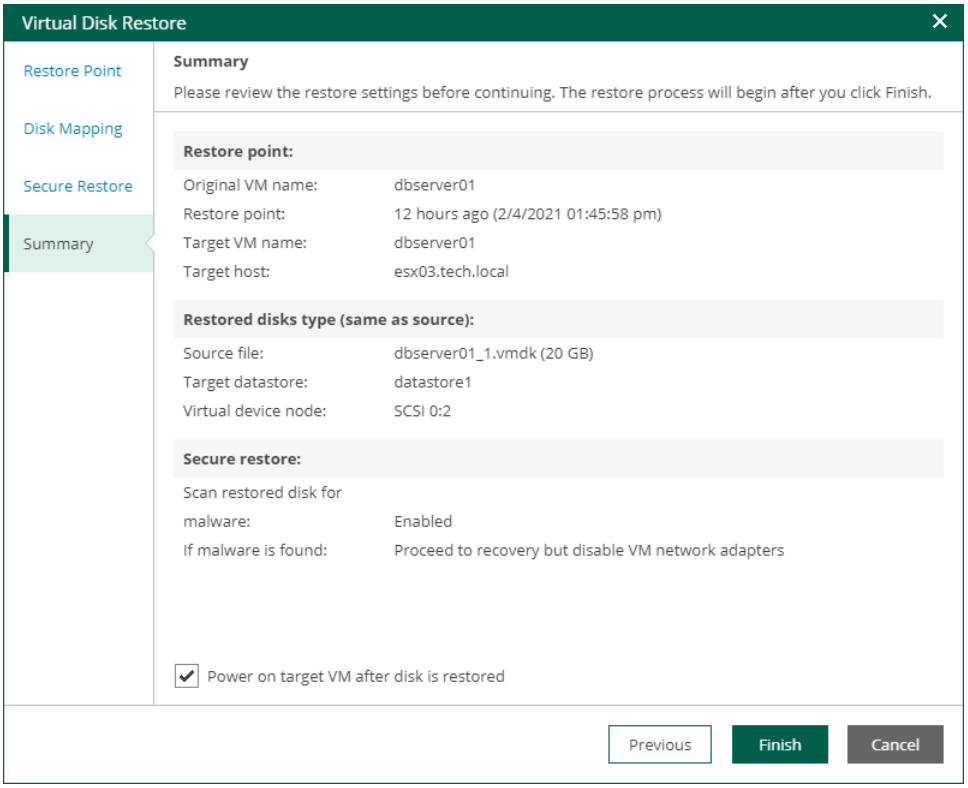
   b. Select the action that Veeam Backup & Replication will take if the antivirus finds a virus threat:

   - **Proceed with recovery but do not attach infected disks to the target VM**. Select this option if you want to continue the virtual disk restore. In this case, the restored disk will not be attached to the target VM.
   - **Abort disk recovery**. Select this option if you want to cancel the restore session.

c. Select the **Scan the entire image** check box if you want the antivirus to continue the machine data scan after the first malware is found.



7. At the **Summary** step of the wizard, complete the procedure of VM disk restore. To start a VM immediately after the restore process completes, select the **Power on target VM after disk is restored** check box. Then click **Finish**.



To view the progress of the virtual disk restore operation, on the **Machines** tab, click **History**.

Running Failover Plans

This feature is not available for physical machine backups. If your infrastructure comprises machines running interdependent applications (for example, Exchange Server and domain controller), it is reasonable to failover them one by one, as a group. To do this automatically, you can prepare a failover plan using Veeam Backup & Replication console.

In Veeam Backup Enterprise Manager, you can run failover plans created in Veeam Backup & Replication console for VMware vSphere and Microsoft Hyper-V VMs.

Failover plan sets the following:

- The order in which the machines should be processed: for example, AD domain services server first, Exchange server after it.
- The delay time needed to start each machine. The delay time helps to ensure that certain machines (AD domain services server in our example) are already running at the time the dependent machines start.

The failover process is performed in the following way (either ad-hoc or on schedule):

1. For each machine included in the plan, Veeam Backup & Replication detects its replica (the machines whose replicas are already in Failover or Failback state are skipped from processing).
2. The replica machines are started sequentially, in the order they appear in the failover plan, within the set time intervals.

Consider that failover is a temporary intermediate step that needs to be finalized. The finalizing options for a group failover are similar to a regular failover: undoing failover, permanent failover or failback. To learn more about failover planning and recommended course of action, refer to Veeam Backup & Replication User Guide.

Veeam Backup Enterprise Manager allows you to carry out a failover following the existing plan, and also to undo planned failover.

> **NOTE**
>
> For failover plan creation, as well as for permanent failover or failback, use the Veeam Backup & Replication console.

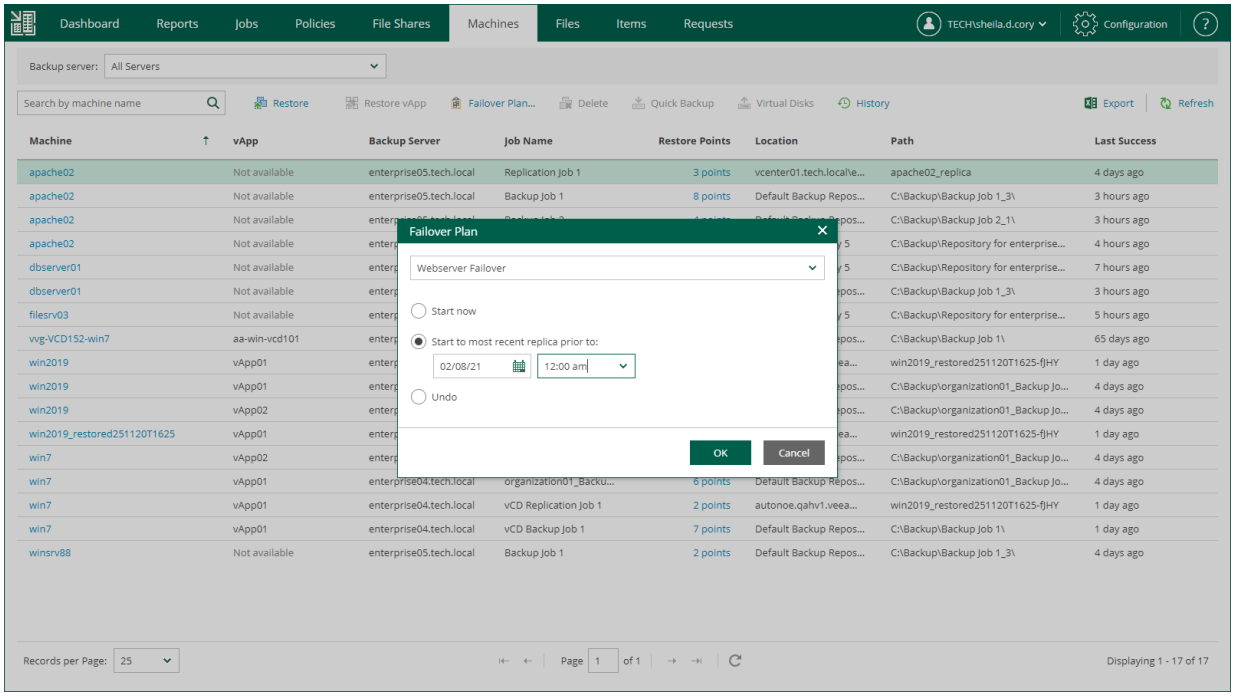
To run a failover plan:

1. Log in to Enterprise Manager using an administrative account or user account whose restore scope contains the machines from the failover plan.
2. Go to the **Machines** tab and click **Failover Plan**.
3. In the **Failover Plan** window, select the necessary plan from the list, then specify the starting option you need.

   The following options are available for a failover plan:

   - **Start now** – use this option if you need to fail over to the replicas' latest restore point.
   - **Start to most recent replica prior to** – use this option if you need to fail over to a certain restore point. For example, you may want your application server to failover to a state prior to the upgrade. In this case, for each machine participating in failover, Veeam will find the closest restore point (prior to the specified date and time) and fail over to it.
   - **Undo** – use this option to switch the workload back to source machines discarding the changes that were made to the replicas during failover.

4. Click **OK** and wait for the process to complete. You can examine session details in the **Machines > Restore sessions**.



Restoring Guest OS Files

Veeam Backup Enterprise Manager allows you to browse the guest OS file system in a machine backup, search for guest OS files and restore the necessary files. You can locate and restore files from the machine restore point created with or without guest OS file indexing.

NOTE

- Enterprise Manager does not support 1-Click restore, 1-Click guest OS file restore, or application item-level restore for Microsoft Exchange mailbox items or Microsoft SQL Server databases if it is performed from any storage snapshot.
- In Enterprise Manager, you can browse and restore guest OS files of Nutanix AHV VMs only from the backups created by backup copy jobs.

To browse and restore guest OS files and application items from a physical machine backup stored in a Veeam backup repository, you need a certain Veeam Agent deployed on the machine and integrated with Veeam Backup & Replication. For more information, see Support for Veeam Agents.

Browsing and restoring processes involve appropriate backup job setup, as well as mount and data transfer operations.

How File Restore Works

When you restore files from the restore point created with guest OS file indexing enabled, Veeam Backup & Replication uses the following workflow:

1. To provide for browsing and search, Veeam Backup & Replication uses index data to represent the file system of the machine guest OS.
2. If you then select to download the necessary files, Veeam Backup & Replication will mount machine disks (from the restore point) on the Veeam backup server and copy these files from the backup server to the destination location.
3. If you select to restore files to the original location, an additional mount point will be created on the mount server associated with the backup repository storing the backup file. During restore, machine data will flow from the repository to the target, keeping the machine traffic in one site and reducing load on the network.
4. After you download or restore the necessary files, and finish the restore session, the machine disks will be unmounted.

When you restore files from the restore point that was created without machine guest OS file indexing, Veeam Backup & Replication uses the following workflow:

1. To provide for browsing, disks of the machine from the backup file are mounted to the Veeam backup server. If you then select to download the necessary files, Veeam will copy these files from the backup server to the destination location, using this mount point.
2. If you select to restore files from the backup to the original location on the production machine, an additional mount point will be created on the mount server associated with the backup repository storing the backup file.
3. If you restore files from replica, a single mount point for all these operations (browsing, download, restore to original location) will be created on the Veeam backup server.
4. After you download and restore the necessary files and finish the restore session, machine disks will be unmounted.

Preparing for File Browsing and Searching

If you have Veeam Backup & Replication and Veeam Backup Enterprise Manager installed, you can use Veeam indexing capabilities to quickly find the files and folders.

To use guest file system indexing:

1. Enable guest file system indexing on the Guest Processing step of the backup job wizard. For more information, see Configure Guest Processing Settings.
2. Run the backup job with guest file system indexing enabled.
3. Perform catalog replication. For more information, see Performing Catalog Replication and Indexing.

Alternatively, you can process the machine without guest file system indexing. Veeam Backup & Replication supports file-level restore not only for machines included in guest catalog but also for the machines that are not indexed. Indexing may be disabled at the time of restore point creation, or indexing operation may fail. In this case, the restore point of a Windows machine is mounted to the backup server that manages the job, and the restore point of a non-Windows machine is mounted to the helper appliance.

Then a user will be able to locate necessary files and folders and perform restore operation. For more information, see Browsing Machine Backups for Guest OS Files.

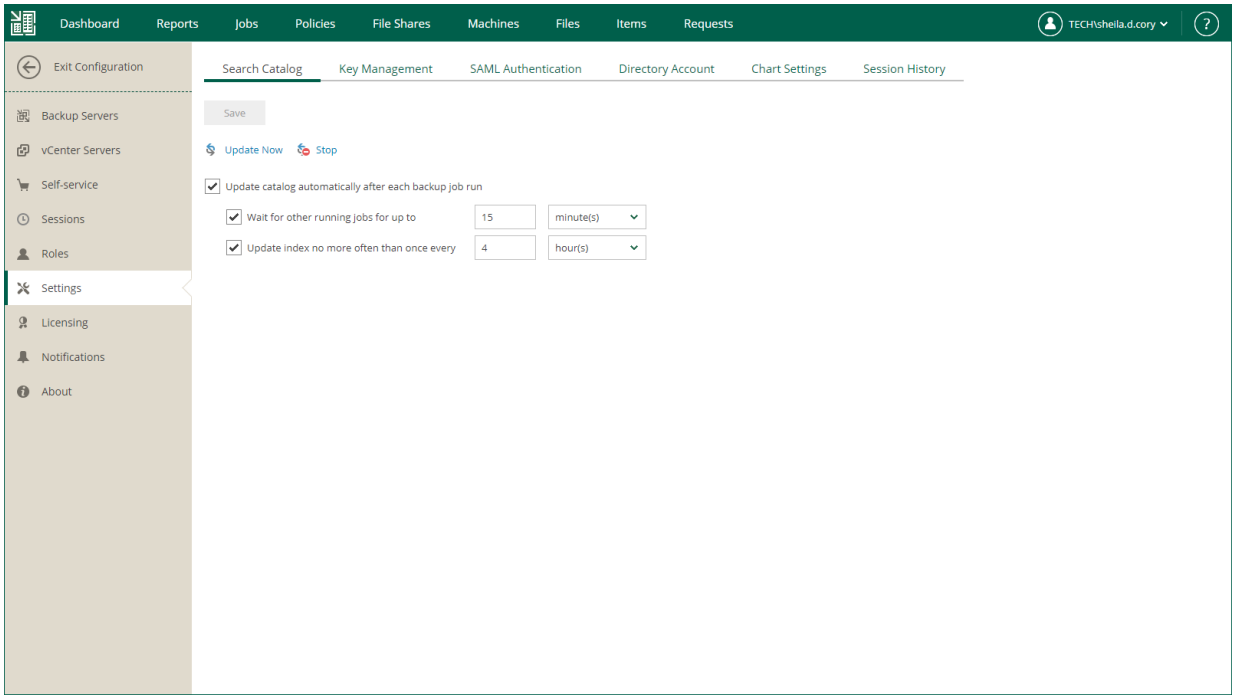
Performing Catalog Replication and Indexing

Once you have run backup jobs with guest OS file system indexing enabled, perform catalog replication to consolidate index files from multiple backup servers. During this operation, Veeam Backup Enterprise Manager aggregates index data from multiple backup servers and stores them on the Veeam Backup Enterprise Manager server to enable file browsing and search.

> **NOTE**
>
> Catalog replication is performed for the machines with indexed guest OS file systems on all managed backup servers.

Veeam Backup Enterprise Manager provides two options to perform catalog replication:

- To perform manual catalog replication, open the **Settings** tab of the **Configuration** view and click **Update Now** on the **Search Catalog** tab.
- To automatically run catalog replication after every backup job, open the **Settings** tab of the **Configuration** view. On the **Search Catalog** tab, select **Update catalog automatically after each backup job run** and specify other options as required.



Every run of a catalog replication job initiates a new job session which can be tracked on the **Sessions** tab of the **Configuration** view. To view detailed information for a specific session, select it in the list of sessions and click the link in the **Status** column.

Preparing for File Search and Restore (non-Windows machines)

To view, search and restore guest files of non-Windows machines, take the following preparatory steps:

1. To enable guest file indexing, use one of the options of the machine backup job: **Index everything**, **Index everything except**, or **Index only following folders** option. For more information, see the Guest OS File Indexing section of this guide and the VM Guest OS File Indexing section of the Veeam Backup & Replication User Guide.

   Keep in mind that indexing is optional. You can browse and restore machine guest files from the restore points created without guest indexing. For more information, see Browsing Machine Backups for Guest OS Files and Performing 1-Click File Restore.

   > **NOTE**
   >
   > If you want Veeam Backup Enterprise Manager to display symbolic links to folders when browsing through the machine file system at 1-click file restore, enable indexing in the backup job for that machine (running Linux or another non-Windows OS).

2. For proper file system indexing, Veeam Backup & Replication requires several utilities to be installed on the machine: `mlocate`, `gzip`, and `tar`. If these utilities are not found, you are prompted to deploy them to support index creation.

3. By default, guest file restore to the original location is performed using the account specified in the machine backup job. If it does not have sufficient access to target machine, you are prompted for the credentials. Specify user account with sufficient access rights.

   For more information, see the Guest OS Credentials section of this guide and the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Preparing FLR Helper Appliance

To perform guest file restore, configure an FLR helper appliance on the Veeam backup server that controls the backup job processing the machine. For details on FLR helper configuration, refer to the Restoring VM Guest OS Files (Multi-OS) section of the Veeam Backup & Replication User Guide. These settings are saved in Veeam Backup & Replication database on per-user basis. The settings are applied each time the user starts file-level restore.

When guest file-level restore is started from Veeam Backup Enterprise Manager, FLR helper configuration settings are obtained from the database of the backup server. If no FLR helper configuration is found for current user account, Veeam Backup & Replication uses the default settings (set during the latest FLR appliance configuration process in Veeam backup console). Thus, before starting file-level restore from Enterprise Manager, make sure that FLR helper settings are configured on Veeam backup server.

NOTE

- When you configure an FLR helper appliance for tenants that will perform self-service restore (from Veeam Self-Service Backup Portal or vSphere Self-Service Backup Portal), be aware that multiple tenants may run the restore procedure at the same time. In this case if you have configured a static IP address for helper appliances, a tenant will not be able to deploy a helper appliance until the IP address is in use by a helper appliance of another tenant. To let tenants start multiple helper appliances, use a DHCP server in your network and configure the helper appliance to obtain an IP address automatically.
- If you plan to deploy multiple FLR helper appliances to restore machines backed up by different Veeam backup servers, their initial configuration should be performed on the backup servers. Centralized configuration from Veeam Backup Enterprise Manager is not supported.

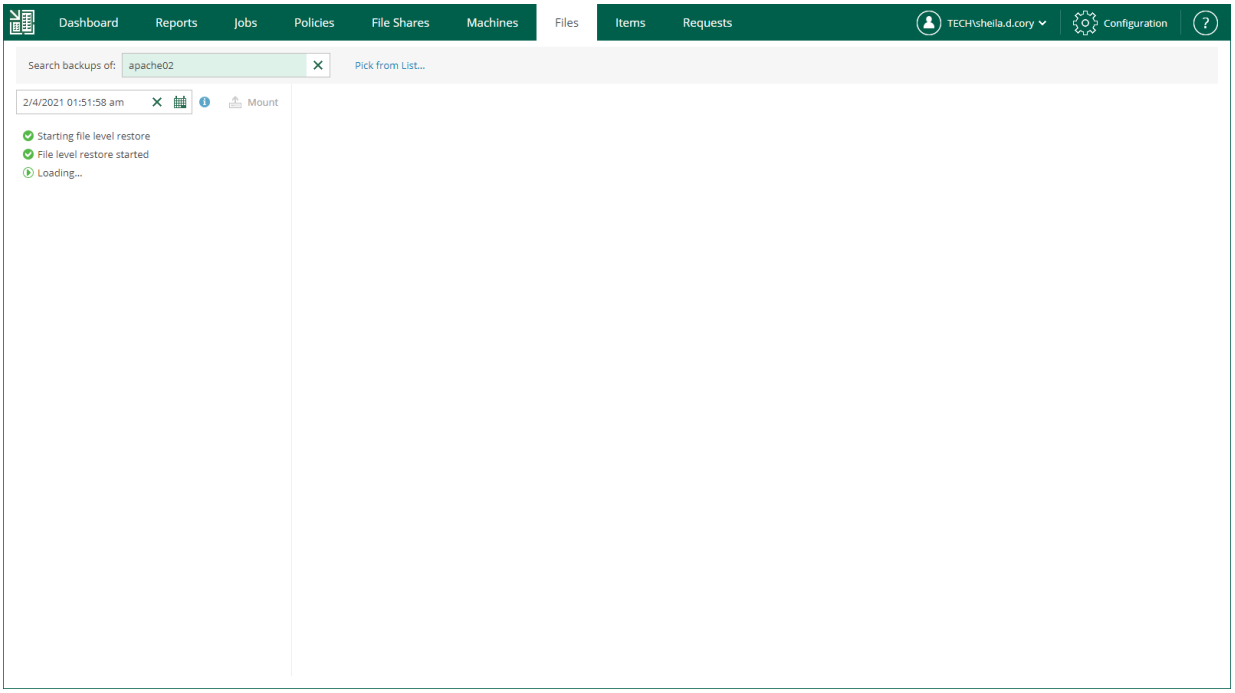
Browsing Machine Backups for Guest OS Files

After catalog replication, you can browse any machine backup for OS guest files. Note that with the file browsing functionality, you can browse and search for files in the selected machine backup at a specific restore point only.

If you are using the Enterprise or Enterprise Plus license edition in your virtual environment, consider that Veeam Backup Enterprise Manager keeps index files for backups that are currently stored on disk, and for archived backups (for example, backups that were recorded to tape). Thus, you will be able to browse and search through backup contents even if the backup in repository is no longer available.

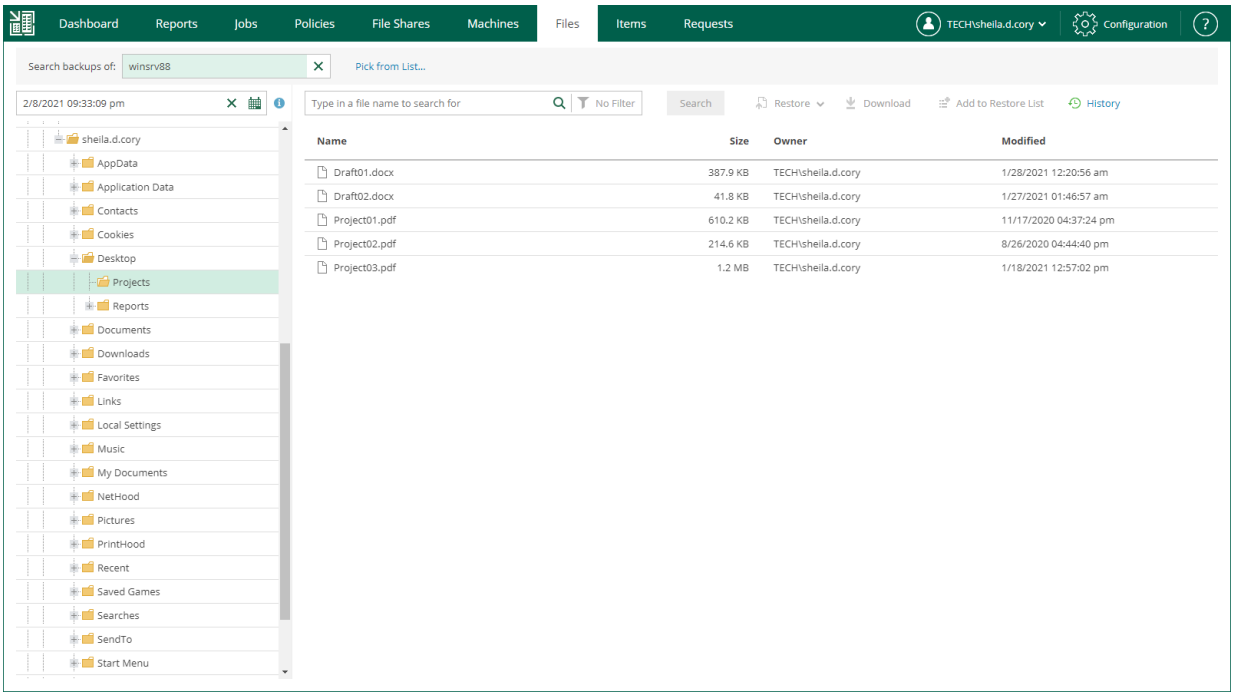
To browse guest OS files in a machine backup:

1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a machine whose files you want to restore or click the **Pick from List** link and select the necessary machine in the **Select Object** window.
3. To specify a restore point from which to restore guest OS files, click the calendar icon in the restore point field and select the necessary date when backup was performed and a restore point created on that date. Note that you cannot select dates when backup was not performed. By default, the latest restore point is selected in the restore point field.
4. If the machine has been backed up without guest indexing, click **Mount**. If the machine guest OS information has not been collected during the backup, you will be also prompted to specify the guest OS type. Machine disks from the backup will be mounted to Veeam backup server to present machine file system to you; wait for the process to complete.



If the machine has been backed up with guest indexing enabled, no additional operations are needed.

As a result, the file tree of the machine as of the selected backup and restore point date will be displayed. You can manually browse the file tree or use the search field to find a necessary file. Consider that depending on the number of files on the machine, the search process may take some time.



IMPORTANT

For machines processed without indexing, you can only use browsing or search to find the necessary files within the selected restore point. Advanced search capabilities (including search through multiple restore points) are available only for machines processed with guest indexing enabled.

Searching Guest OS Files in Machine Backups

Veeam Backup Enterprise Manager allows you to search for guest OS files in all machine backups created by managed backup servers with guest indexing enabled.

> **IMPORTANT**
>
> By default, backup repository is the primary destination for the search. This means, in particular, that if a backup (with indexed guest) is stored in both locations — repository and tape — then Enterprise Manager search results will only include files from backup stored in repository. Files from tape-archived backup will appear in search results only if not found in the repository. (This capability is supported in the Enterprise and Enterprise Plus editions.)

You can use one of two available search modes: simple or advanced.

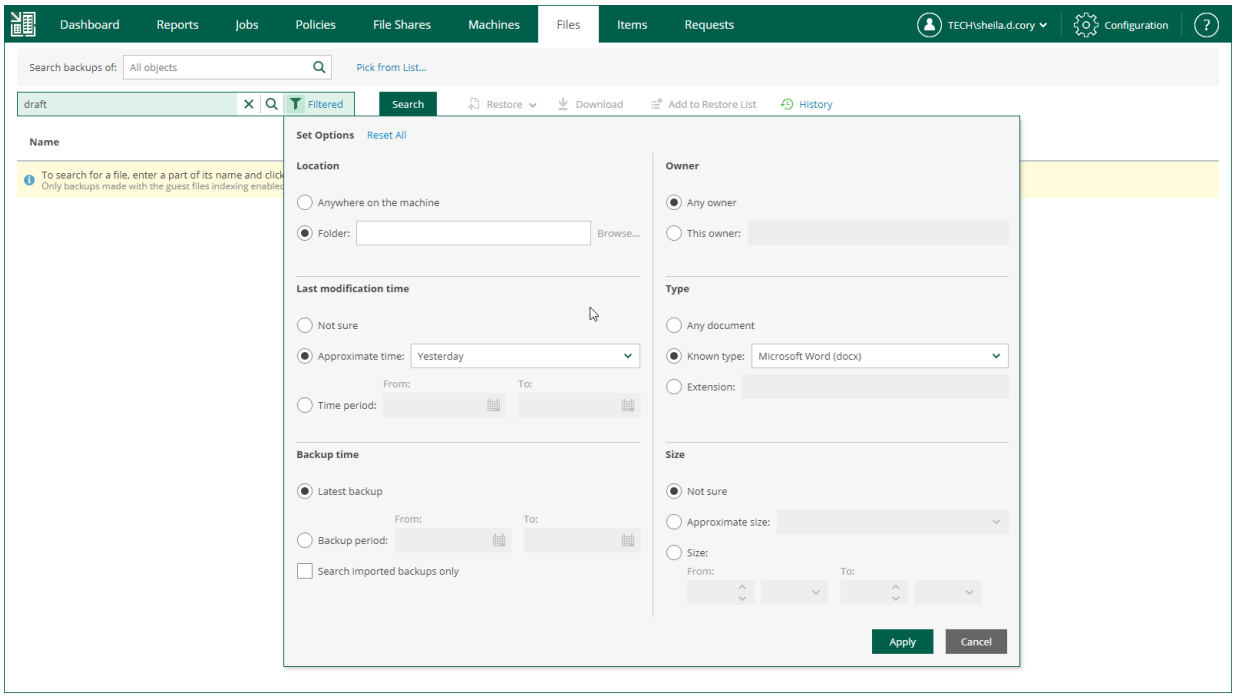
The simple search allows you to search for guest OS files in the latest restore point of the selected machine backup. To perform simple search:

1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a machine whose files you want to restore or click the **Pick from List** link and select the necessary machine in the **Select Object** window.
3. In the search field, enter the name of the necessary file or a part of it and click **Search**.

The advanced search allows you to search for guest OS files in all restore points of the selected machine backup and filter search results by certain criteria. To perform advanced search:

1. Open the **Files** tab and click **No Filter** next to the search field.
2. In the search field, enter the name of the necessary file or a part of it.
3. In the **Set Options** window, define the necessary search criteria:
   - **Location** — select a specific folder on the machine to search in.
   - **Last modification time** — specify approximate time when the file was last modified or set a time interval.
   - **Backup time** — choose to search through the latest backup of the specified machine or all backups of the machine created within a certain time interval.
   - **Owner** — select to search for files with a specific owner.
   - **Type** — select to search for files of specific type or with a certain extension.
   - **Size** — specify approximate size of file or set a size range.
4. To apply the filter, click **Apply**.

5. Click **Search** on the right of the search field.



Performing 1-Click File Restore

After you find the necessary file, you can use Veeam Backup Enterprise Manager to restore it from backup with one click. You can choose to restore it to the original location or download it to the local machine.

IMPORTANT

Consider the following:

- 1-Click file restore capability is available if you have the Enterprise or Enterprise Plus edition.
- 1-Click guest OS files restore from any storage snapshot is not supported by Veeam Backup Enterprise Manager.

Restore operations are only available to authorized users according to their security settings. Users with the Portal Administrator role can restore files both to the original location or download them to the local machine.

For users with the non-administrative roles, you can configure additional restriction settings. For example, you can prohibit restore operators to download files to the local machine so that they can restore files to the original location only. Additionally, you can specify the types of files that can be restored by operators (this can be helpful if you want to limit operators' access to sensitive data). For details, see Configuring Accounts and Roles.

NOTE

Consider the following:

- If you plan to restore a file from a machine backed up without guest indexing, consider that for restore operation this machine disk will be mounted directly from the backup in the repository to the mount server associated with that repository; if restoring from replica, it will be mounted to Veeam backup server. If restoring from an indexed machine, no interim mount operations are needed.
- If you want Veeam Backup Enterprise Manager to display symbolic links to folders when browsing through the machine file system at 1-click file restore, then you should enable indexing in the backup job for that machine (running Linux or another non-Windows OS).

Restoring Files to Original Location

In this restore scenario, Veeam Backup Enterprise Manager will extract the file from the backup and restore it to the original production machine. Restoring guest OS files to the original location is the most secure file recovery method, as the user who initiates the file restore operation in the Veeam Backup Enterprise Manager web UI cannot access the file itself.

> **IMPORTANT**
>
> This type of restore is only possible if the original machine is powered on and resides in the original location.

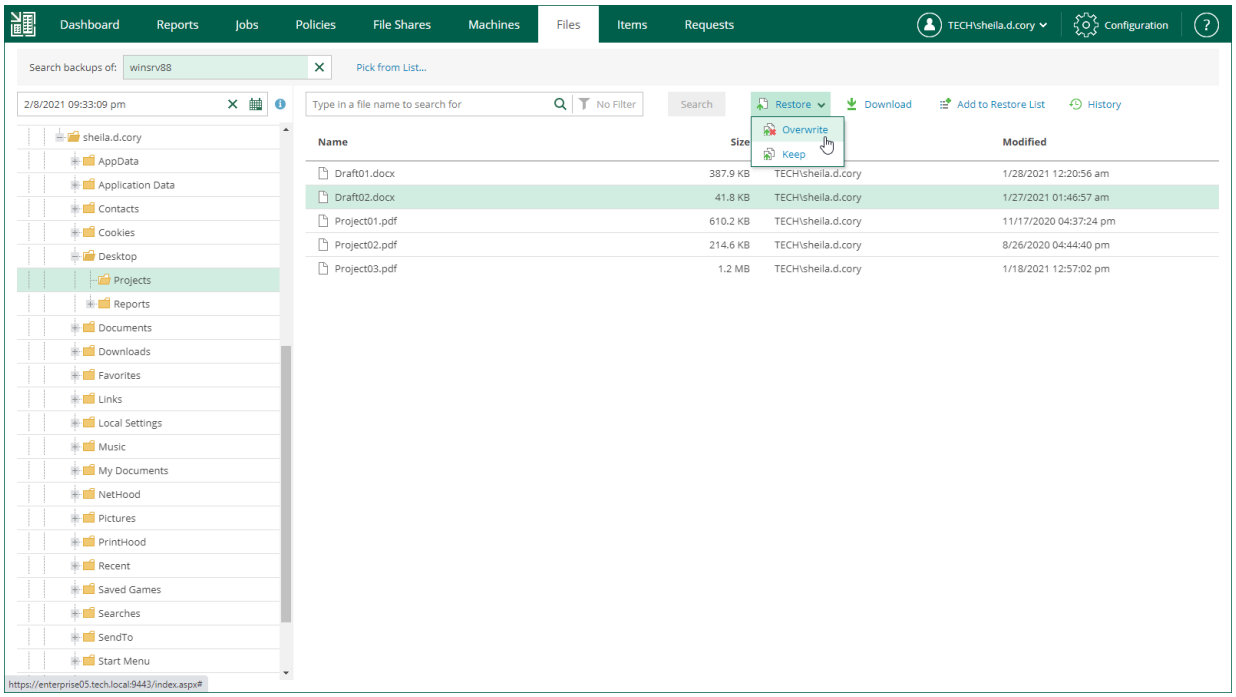
To restore a file to the original location:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. Multiple selection is also possible. For details, see Browsing Machine Backups for Guest OS Files or Searching Machine Backups for Guest OS Files.
2. Click **Restore** and select how to restore selected files:
   - If you select **Overwrite**, the file from the backup will replace the original file on the target machine.
   - If you select **Keep**, the file from the backup will be restored next to the original file on the target machine; the file from machine backup will have the *Restored* prefix in the file name.
3. In the displayed window, click **Yes**.

Veeam Backup Enterprise Manager will start the restore operation and display the progress and result of the operation in the **File Restore History** view.

IMPORTANT

By default, guest file restore to the original location is performed using the account specified in the backup job for guest OS access. If it does not have sufficient rights to access the target machine, you are prompted for the credentials. Specify user account and password, as required. For more information, see Guest OS Credentials.

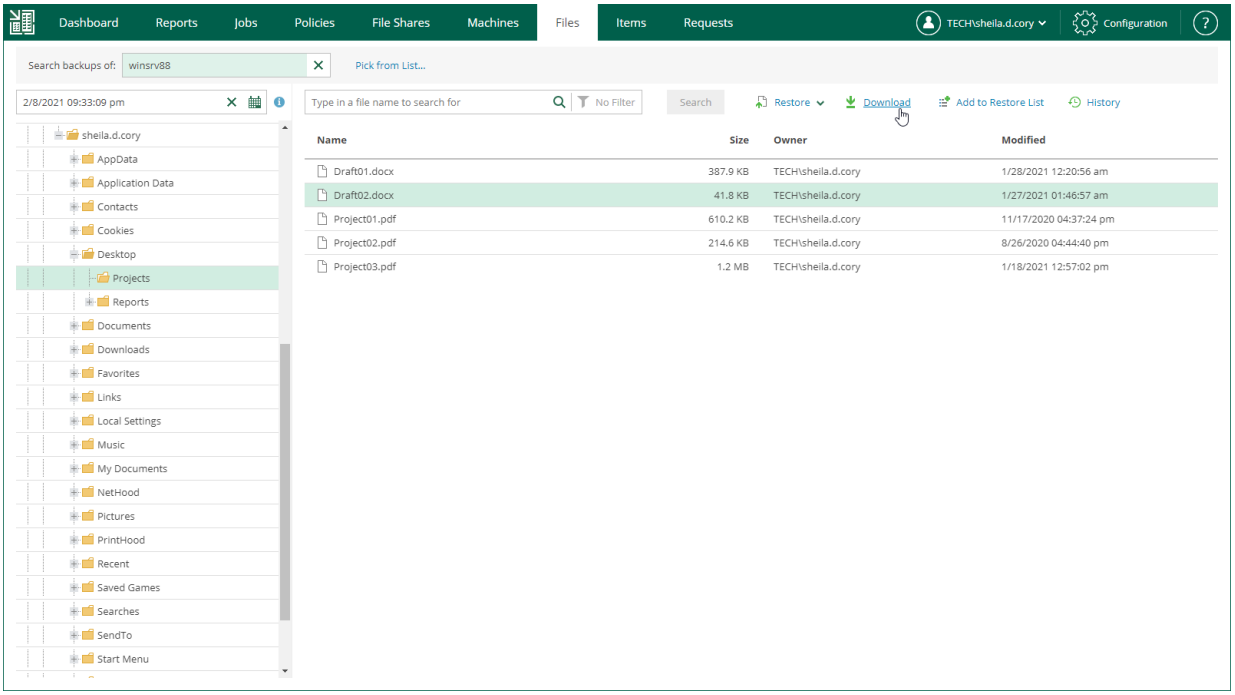


Downloading Files to Local Machine

If you choose to download the restored file, Veeam Backup Enterprise Manager interacts with the Veeam backup server to extract the necessary file from a backup. The user who initiated file restore will be able to download the file to the local machine.

To restore a file to the local machine:

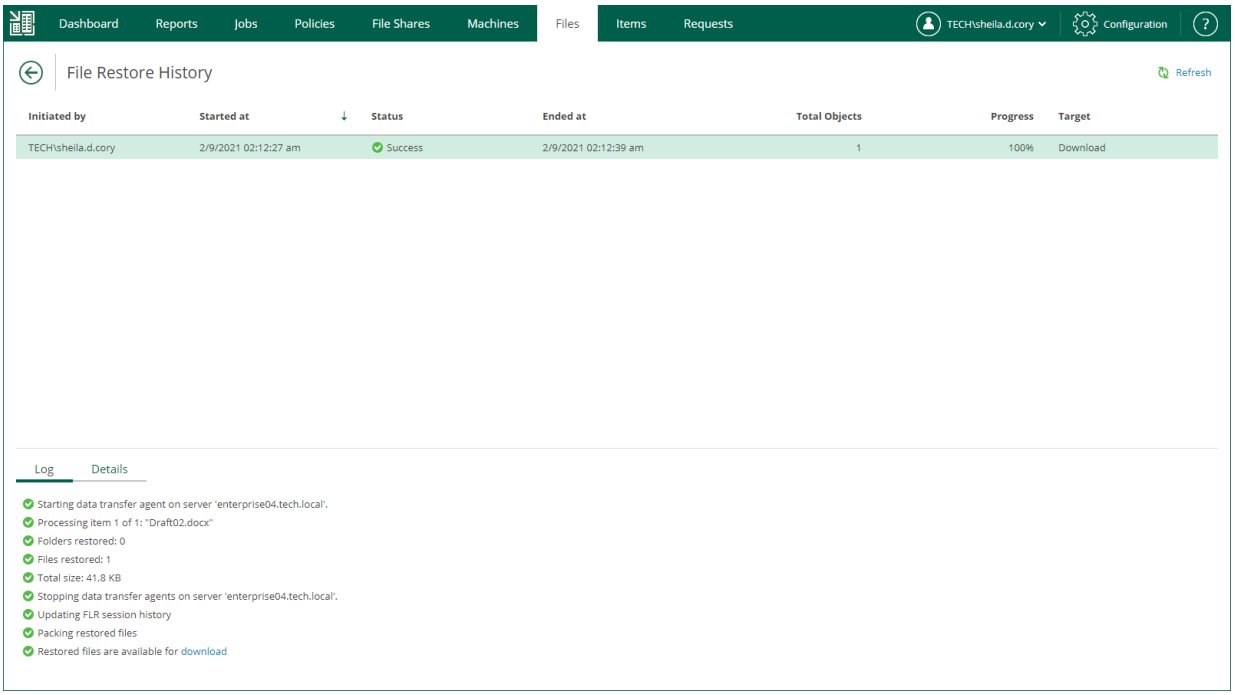
1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For details, see Browsing Machine Backups for Guest OS Files or Searching Machine Backups for Guest OS Files.
2. Click **Download**.



3. In the displayed window, click **Yes**.
4. Wait for restore session to complete and for the file to be retrieved from the backup.
5. Select the file from the list.
6. In the **Log** tab of the **File Restore History** view, click the **download** link in the *Restored files are available for download* record of the session log.

   The file is saved to the default download folder on your local machine.

If you download a single file, it is also saved in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Multiple files are packed in a ZIP file named `FLR_<date>_<time>.zip` and stored in the same folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.



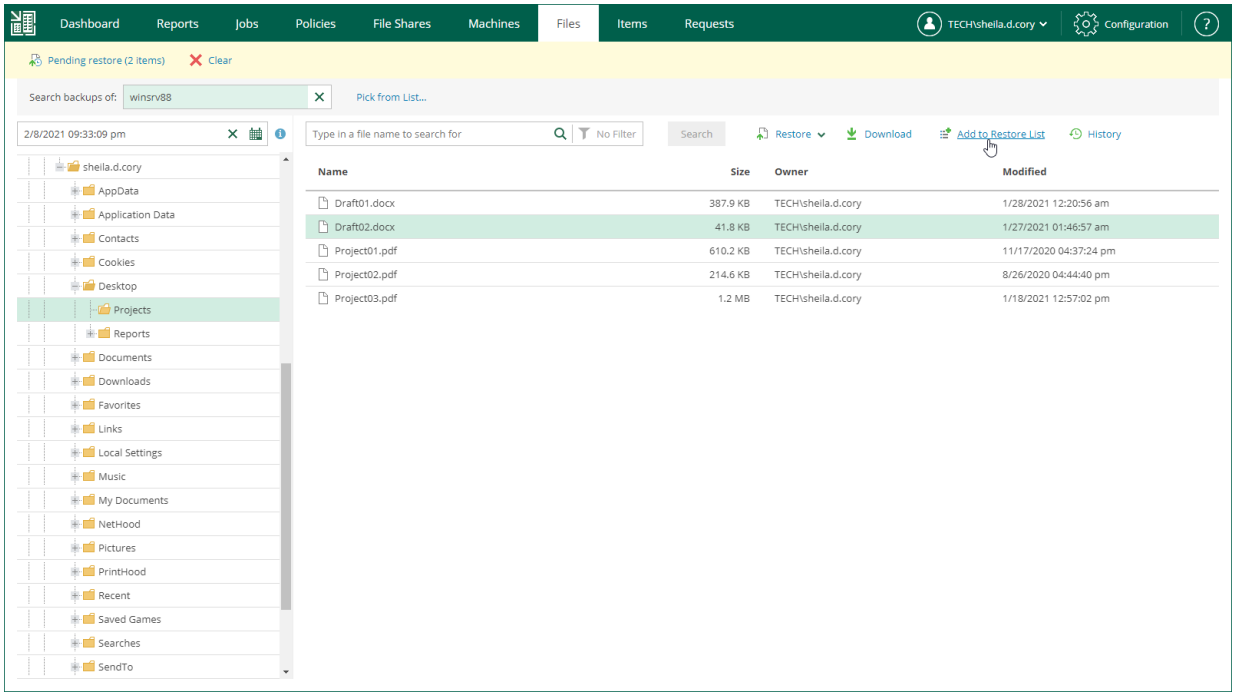
Restoring Multiple Files

In addition to restoring single files from selected restore points, Veeam Backup Enterprise Manager supports bulk restore. If you need to restore multiple files at once, you can select more than one file in the preview pane when browsing, and then use the **Restore** command, or add the necessary files to the restore list and then restore all files at once. Unlike the **Restore** command, using the restore list helps you to prepare for restore files from different machines, backups and restore points.

To add a file to the restore list:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For more information, see Browsing Machine Backups for Guest OS Files or Searching Machine Backups for Guest OS Files.
2. Click **Add to Restore List**.

When a file is added to the restore list, the **Pending restore** notification appears at the top of the Enterprise Manager window.



To restore files added to the restore list:

1. In the restore list notification, click **Pending restore**.
2. In the **Pending Restore** window, select check boxes next to files in the restore list that you want to restore. Use the check box next to the header of the **Name** column to select all files in the list at once.

   If you want to remove a file from the restore list, select the file and click **Delete**.
3. Click the **Restore** or **Download** link to perform the necessary restore operation for the selected files.
4. In the displayed window, click **Yes**.
5. [For the download operation] Wait for restore session to complete. In the **Log** tab of the **File Restore History** view, click the **download** link.

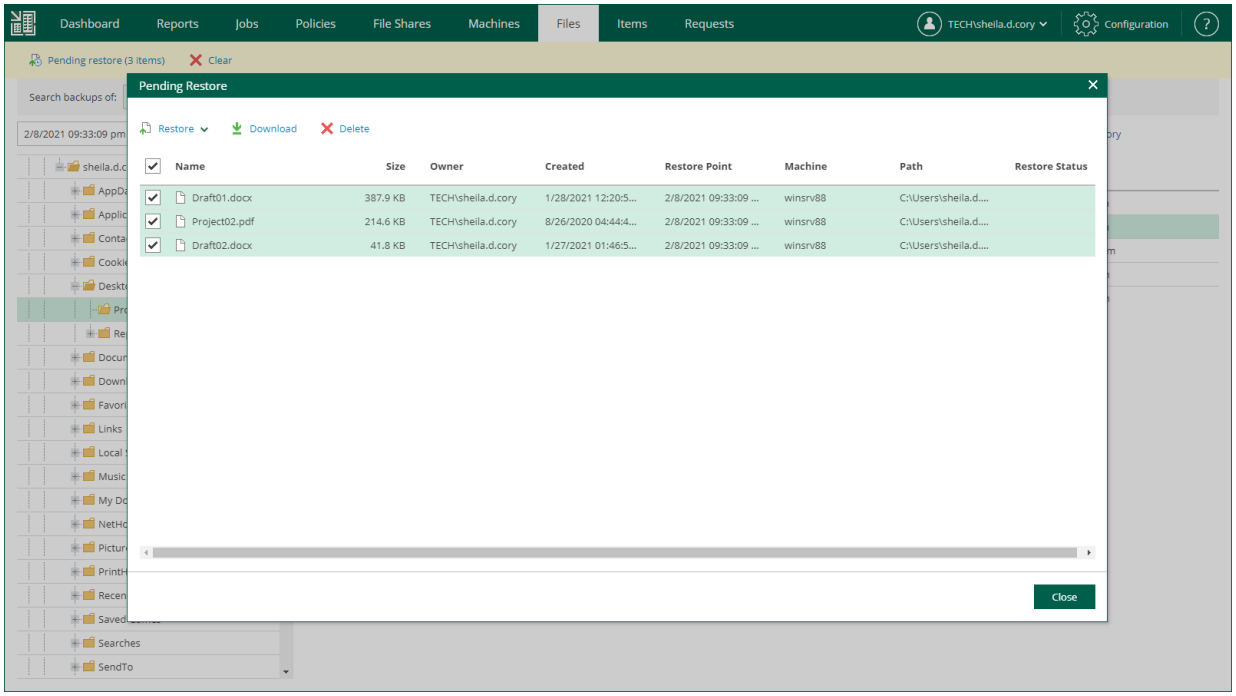
   The files are saved to the default download folder on your local machine.

Multiple files are also saved in a ZIP file named `FLR_<date>_<time>.zip` in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.

TIP

Veeam Backup Enterprise Manager keeps links for downloaded files in the history for one day. To download a file that was previously restored:

1. In the **Files** tab, click **History**.
2. In the **File Restore History** view, select the necessary restore session.
3. In the **Log** tab, click the **download** link.



Using Self-Service File Restore Portal to Restore Machine Guest Files

Veeam Backup Enterprise Manager streamlines delegation of restore capabilities: instead of multiple role assignments and restore scope fine-tuning, Enterprise Manager administrator can provide users that have *local administrator* rights on a Windows-based machine with a link to **Self-Service File Restore Portal** — a web UI that displays the controls for file-level restore of the protected machines.

This capability is supported by the Veeam runtime process which performs guest system indexing and also identifies local administrative accounts. Communication with the self-service webpage is performed over the HTTPS protocol. In particular, such delegation capabilities and self-service web portal can be used in enterprise deployments to elevate the first line support to perform in-place restores without administrative access.

Before You Begin

NOTE

- This functionality is supported only in the Enterprise Plus edition of Veeam Backup & Replication.
- Self-Service File Restore Portal is available only for users of Microsoft Windows machines. For Linux-based machines, guest OS file restore is performed in the Veeam Backup Enterprise Manager UI under a user account configured in Enterprise Manager. For more information, see Managing Accounts and Roles.
- Veeam Backup Enterprise Manager does not support guest OS files restore from storage snapshots. You can use the Veeam Backup & Replication console instead.

To provide a user account with the ability to access Self-Service File Restore Portal, make sure the following prerequisites are met:

- The account belongs to the trusted or same domain as the Enterprise Manager server (for the user account to be resolved to SID). Users from untrusted domains cannot utilize self-restore.
- The account has local administrative rights for the required machine guest OS, local user rights are not sufficient.

IMPORTANT

A Self-Service File Restore Portal user has access only to restore points created after the user is assigned with local administrator rights.

Machine restore points will stay available for self-restore to a user account whose local administrative rights were revoked after the restore point creation until the next restore point is created (then that user will not be able to access guest files any longer).

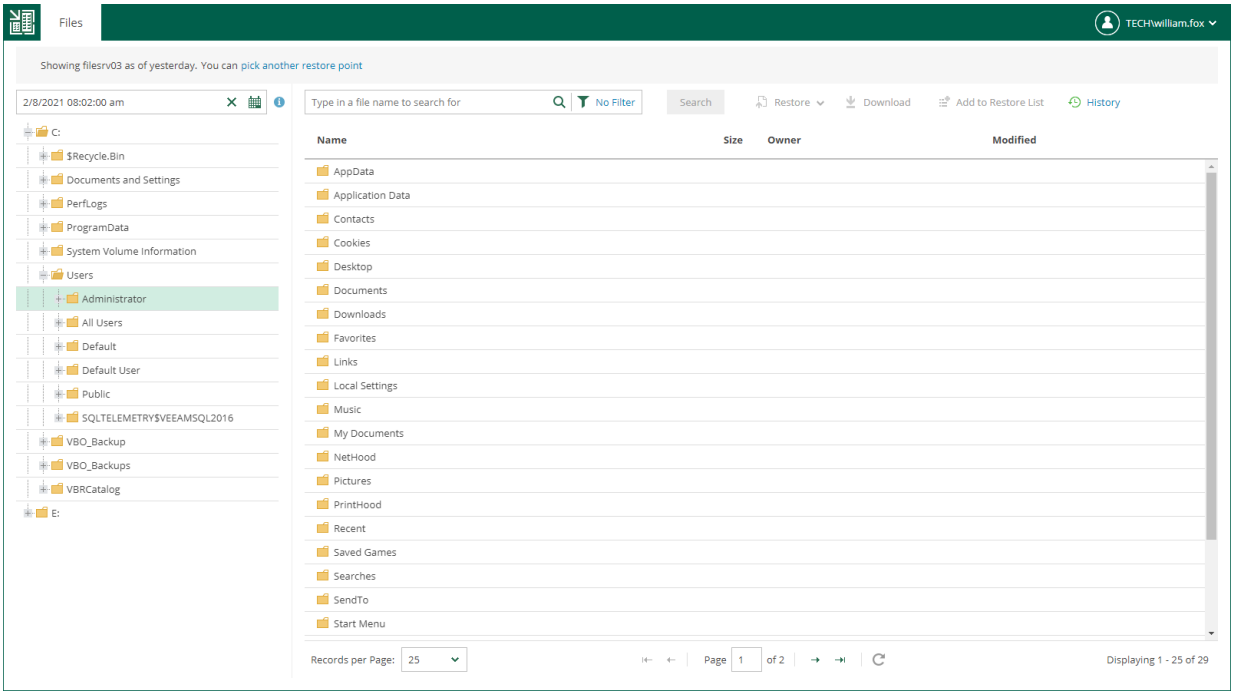
Browsing Guest OS Files Through Self-Service Portal

To access the guest files in a machine backup:

1. Start the Self-Service File Restore Portal by clicking its icon in the list of applications or on the desktop. Alternatively, in the web browser address bar, enter the portal URL, for example:

```
https://enterprise_manager_host:9443/selfrestore
```

2. Enter the account credentials to log in. Use the *DOMAIN|USERNAME* format to specify the user name. The **Files** tab will open. By default, it displays guest OS files as of the latest restore point of the machine to which you logged in with local administrative rights.



4. To view guest files as of earlier restore point, click the **calendar** icon and select the restore point. To view guest files of another machine (if available to you), use the **Search** field or the **Pick from List** link.

5. You can perform all operations supported for machine guest files by Veeam Backup Enterprise Manager. For more information on file browsing, search and restore, see Browsing Machine Backups for Guest OS Files, Searching Machine Backups for Guest OS Files, Performing 1-Click File Restore.

If no guest OS files are visible to the user, check the following reasons:

- The backup server that manages the job is not added to the Enterprise Manager infrastructure. For more information, see Adding Backup Servers.
- The recent backup job data has not been yet collected from the backup server (default time interval is 15 minutes). For more information on how to run data collection manually, see Collecting Data from Backup Servers.
- The **Enable guest file system indexing** option is turned off in the machine backup job. Edit the job setting and restart the job with indexing enabled.
- When the machine restore point was created, the user was not assigned local administrative rights. To access the guest OS files the user must be a part of the guest OS local administrator group.

If you cannot find your machine from the **Pick from List** window, you can select the **I don't see my machine** option to rebuild a security scope for your user account. Once complete, this action will reveal machines that were added to your security scope.

Disabling Self-Service File Restore Portal

You can prevent local administrators from accessing the self-service file restore functionality. You can do it by disabling Self-Service File Restore Portal. To disable the portal, change the Enterprise Manager registry key. For more information, contact Veeam Customer Support.

Backup and Restore of Application Items

Veeam Backup Enterprise Manager supports item-level recovery from application-aware backups created by Veeam Backup & Replication. This capability can be helpful, for example, to restore operators at Help Desk, as well as other authorized personnel.

Backup and Restore of Microsoft Exchange Items

Restore personnel can be delegated the ability to recover the necessary Microsoft Exchange items (emails, tasks, calendars) from the Microsoft Exchange server machine backups. This functionality is provided in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

> **IMPORTANT**
>
> To be able to restore Microsoft Exchange items from the Veeam Backup Enterprise Manager UI, make sure Veeam Backup Enterprise Manager is installed on the domain member server from the Microsoft Active Directory forest in which Microsoft Exchange mailboxes are located.

Restore Requirements and Limitations

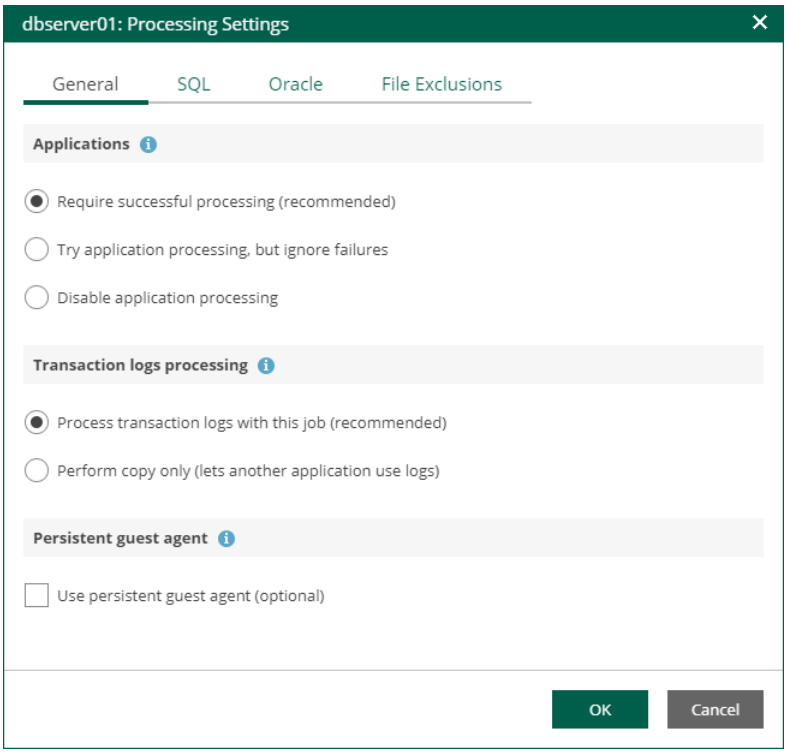
- Enterprise Manager supports restore from backups created with Veeam Backup & Replication versions 8.0 and later.
- Enterprise Manager supports restore over a network connection only. Restore with PowerShell Direct, VIX or Sphere API is not supported.
- Enterprise Manager does not support application item restore from storage snapshots.

Preparing Application-Consistent Backup

To provide for recoverability of Microsoft Exchange items, make sure you have an application-consistent backup (with VSS enabled) of your Microsoft Exchange server machine created successfully.

To check and configure job settings:

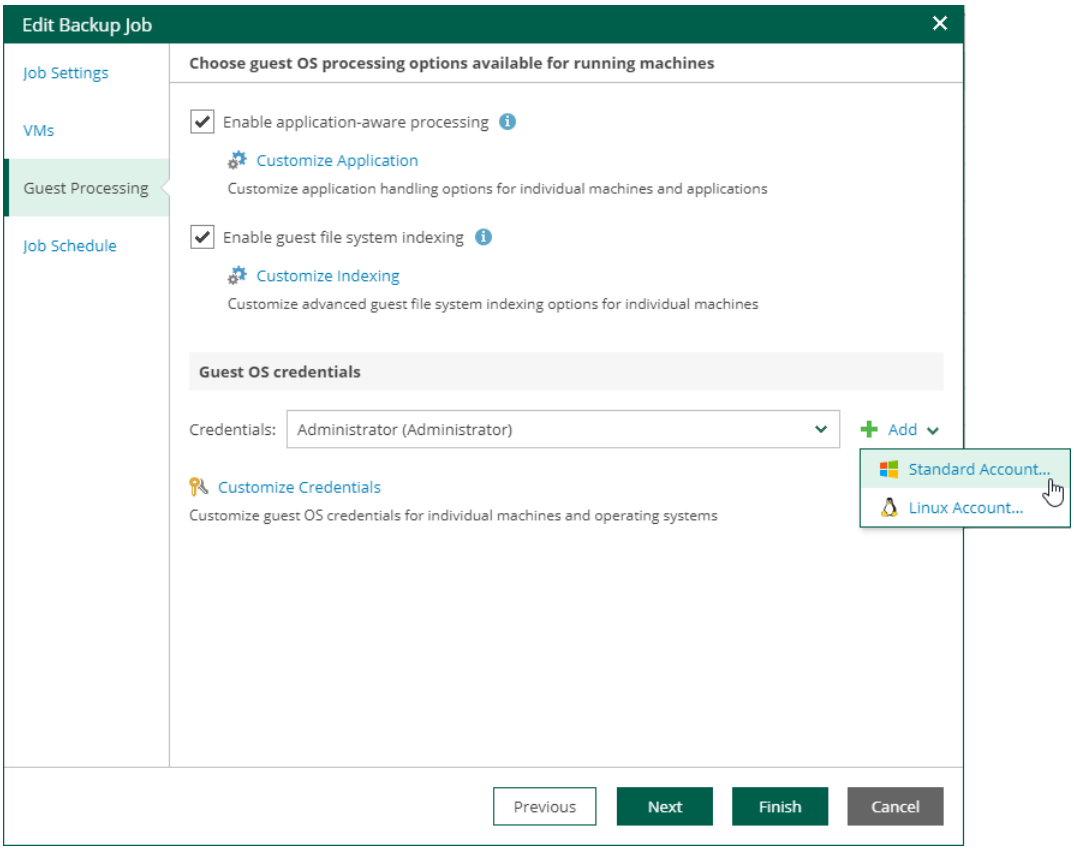
1. Go to the **Jobs** tab and select your Exchange server backup job.
2. Click **Job** on the toolbar and select **Edit** to start the job wizard.
3. Proceed to the **Guest Processing** step of the wizard and make sure the **Enable application-aware processing** check box is selected.
4. Click the **Customize Application** link. In the displayed window, select the Exchange server machine from the list and click **Edit**.
5. On the **General** tab, make sure that the **Require successful processing** option is selected in the **Applications** section.



6. In the **Transaction logs processing** section, the **Process transaction logs with this job** option is selected by default.
7. Click **OK** to save the settings and close the window.
8. In the **Guest OS credentials** section you can edit the account credentials under which guest OS will be accessed.
   - By default, for all machines in the job Veeam will use common credentials provided in the **Guest OS credentials** section — for that, you can select the account from the list, or click the '+' sign and select Windows (or Linux) OS. Then you will be prompted to enter a user name and password for guest OS access. Click **OK** to save the settings and return to the **Guest Processing** page.

- Alternatively, you can click the **Customize Credentials** link and then click **Set user**. Then you can specify custom guest OS credentials for the selected machine.

For more information on specifying guest OS access credentials, see Guest OS Credentials.



9. At the final step of the wizard, verify job schedule and click **Finish**.

Providing Access Rights

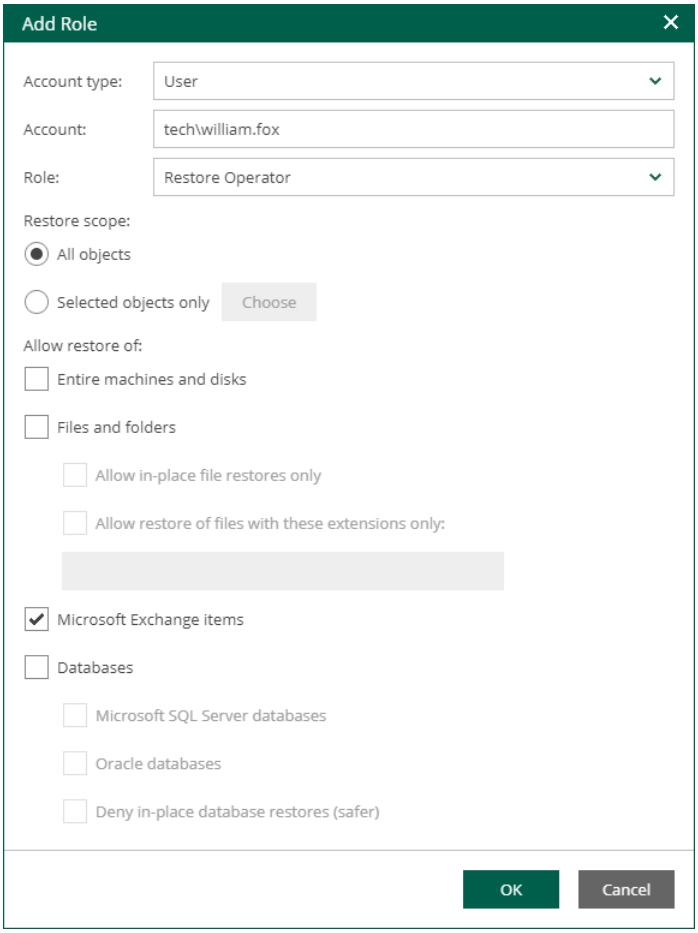
Users responsible for Exchange items restore must be assigned a security role in Enterprise Manager, and be allowed to access and restore Microsoft Exchange items.

To provide a user with access rights, do the following:

1. Assign a security role to the necessary user and allow them to restore Microsoft Exchange items:
   a. Open the **Roles** section of the **Configuration** view.
   b. Click **Add** to add an account, or select an existing account and click **Edit**.
   c. To allow restore of Microsoft Exchange items, select the **Microsoft Exchange items** check box.
   d. Click **OK** to save the changes.

   This makes the **Items** tab become available to these users after they log in to Enterprise Manager.

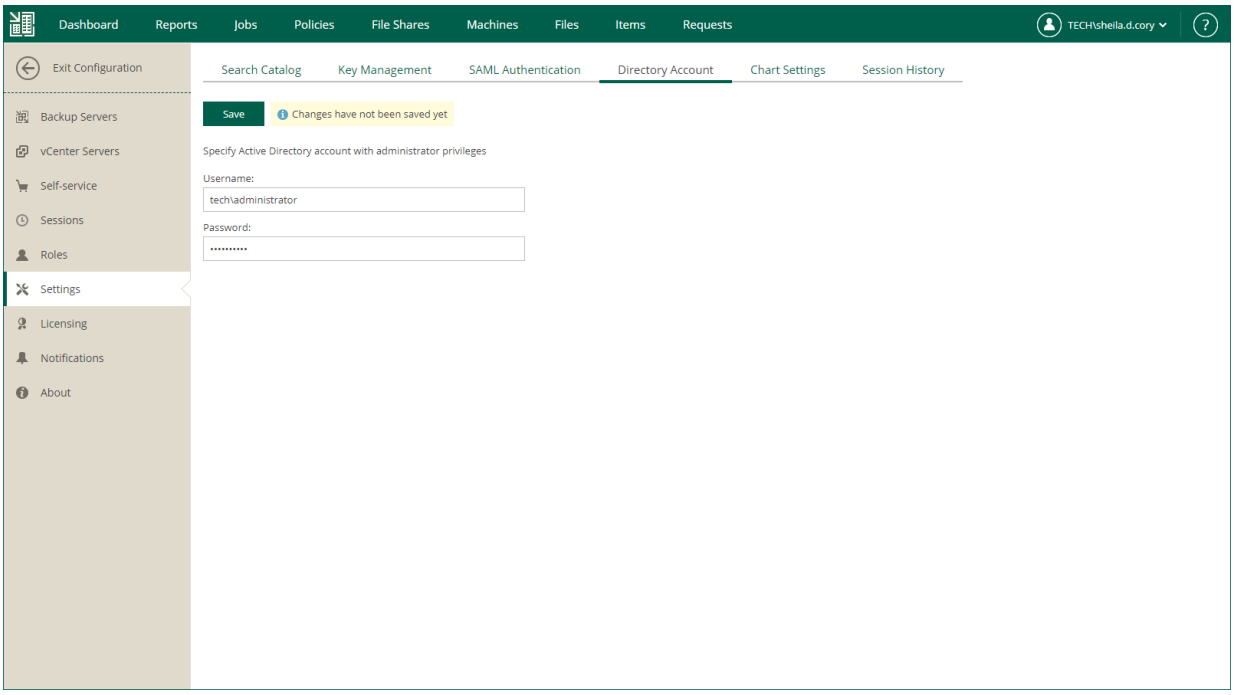
   For more information on Enterprise Manager accounts and roles, see Configuring Accounts and Roles.



2. Specify an Active Directory account that will be used to restore Exchange items:
   a. Open the **Settings** section of the **Configuration** view.
   b. On the **Directory Account** tab, specify a user name and password of the necessary account. Make sure the account meets the following requirements:
      - The account must be a member of the *Organization Management* or *Domain Administrators* group.

- The account must have sufficient rights to access mailboxes. To assign these rights, you can use Exchange Impersonation or grant the *Full Access* permission to the account. For more information on Exchange Impersonation, see Microsoft Docs.

c. Click **Save** to save the changes.



Restore Procedure

To restore a Microsoft Exchange item to the production Exchange Server:

1. Sign in to Veeam Backup Enterprise Manager using an account with the sufficient permissions. For more information, see Providing Access Rights.
2. Open the **Items** tab, then click **Mailbox Items**.
3. In the **Username** field, enter the account of Active Directory user whose mailbox will be restored. You can leave the **Username** field empty and click the search icon to display all mailboxes that currently exist in the production environment, or enter a search criteria. Enterprise Manager uses Global Catalog to examine Active Directory database and find the specified user mailbox, as well as the DNS name for the Exchange Server where the data should be restored. Then it looks for the VM backup or replica and its restore points.
4. In the **Restore point** field, select a restore point.

> **NOTE**
>
> Consider the following:
>
> - Restore points on tape are not supported (only those stored in repository can be used).
> - Restore to another domain is supported within the same forest only.

5. In the **Items** section, select the type of item you want to restore:
   - Mail
   - Calendar
   - Contacts

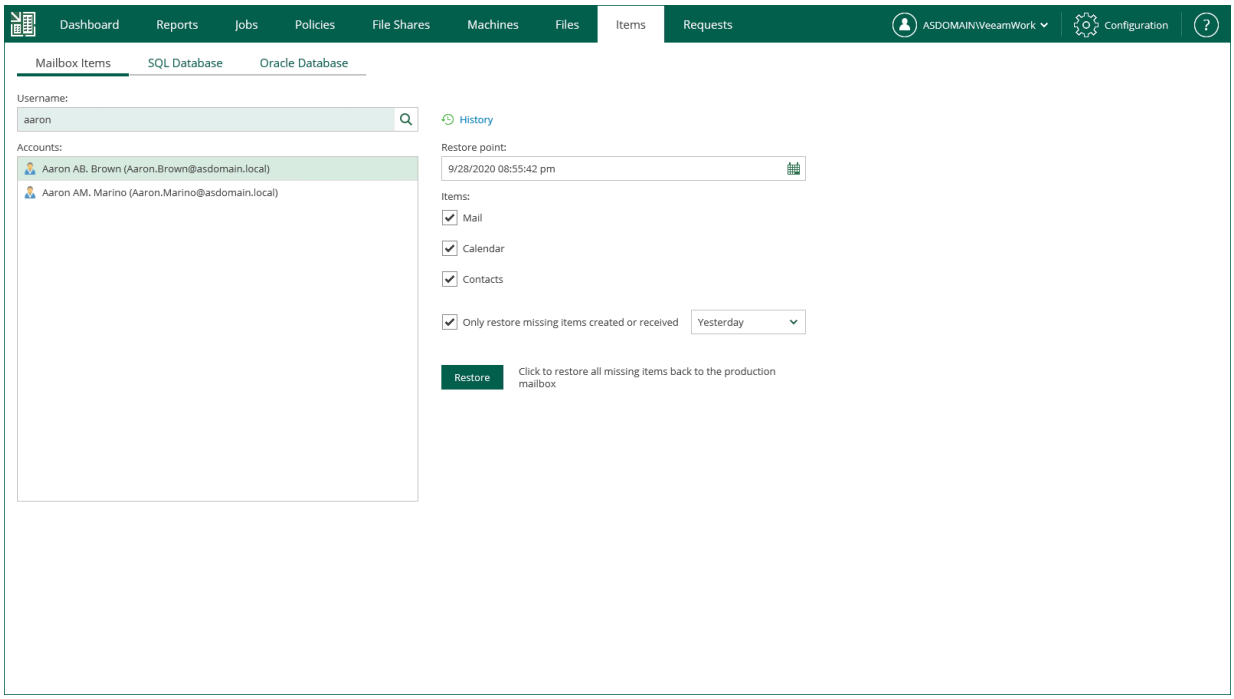
   You can select to **Only restore missing items created or received** during the certain time period. To specify the period, use the drop-down list.
6. Click the **Restore** button. Items that meet specified conditions will be restored to the production Exchange Server.

To view item restore session information, click **History**.

NOTE

Consider the following:

- You can use Veeam Backup Enterprise Manager to restore deleted items to the production mailbox only.
- If the specified mailbox does not exist in the machine restore point that you selected for restore, Veeam Backup Enterprise Manager will display an error message.



Backup and Restore of Microsoft SQL Server Databases

Authorized personnel can use Veeam Backup Enterprise Manager to restore the necessary SQL databases from Microsoft SQL Server machine backups.

> **NOTE**
>
> This functionality is provided in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Restore Requirements and Limitations

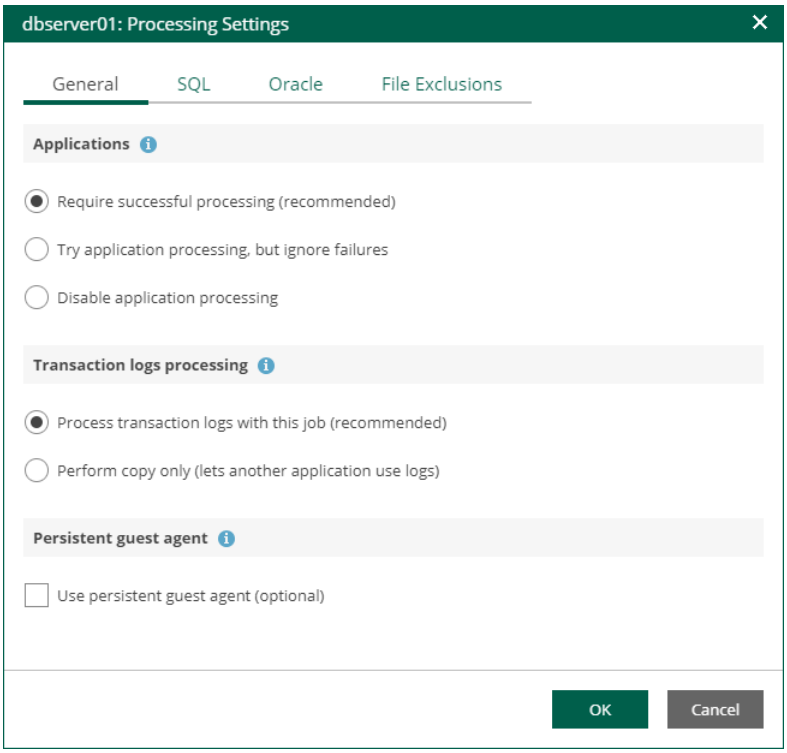
- Enterprise Manager supports restore from backups created with Veeam Backup & Replication versions 8.0 and later.
- Enterprise Manager supports restore over a network connection only. Restore using PowerShell Direct, VIX or Sphere API is not supported.
- Enterprise Manager does not support database restore from storage snapshots.

Preparing Application-Consistent Backup

To provide for recoverability of SQL database, make sure you have an application-consistent backup (with VSS enabled) of your SQL server machine created successfully. Also, if you plan to restore the database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then transaction log processing should be configured, as described below, as well as in the Veeam Backup & Replication User Guide.

To configure job settings:

1. Go to the **Jobs** tab and select your SQL server backup job.
2. Click **Job** on the toolbar and select **Edit** to start the job wizard.
3. Proceed to the **Guest Processing** step of the wizard and make sure the **Enable application-aware processing** check box is selected.
4. Click the **Customize Application** link. In the displayed window, select the SQL server machine from the list and click **Edit**.
5. On the **General** tab, make sure the **Require successful processing** option is selected in the **Applications** section.
6. To be able to specify transaction log handling options, make sure the **Process transaction logs with this job** option is selected. Otherwise, if you select the **Perform copy only** option, Veeam Backup & Replication will create a copy-only backup, and transaction logs will not be purged — that is why the **SQL** tab with log handling settings will be deactivated in this case. For more information, see the Microsoft SQL Server Transaction Log Settings section of the Veeam Backup & Replication User Guide.



7. Open the **SQL** tab and specify how SQL transaction logs will be handled:
   - Select **Truncate logs** if you want Veeam Backup & Replication to trigger truncation of transaction logs only after the job is finished successfully. If truncation of transaction logs is not possible for some reason, the logs will remain untouched in the machine guest OS until the next start of the Veeam runtime process responsible for application-aware processing.

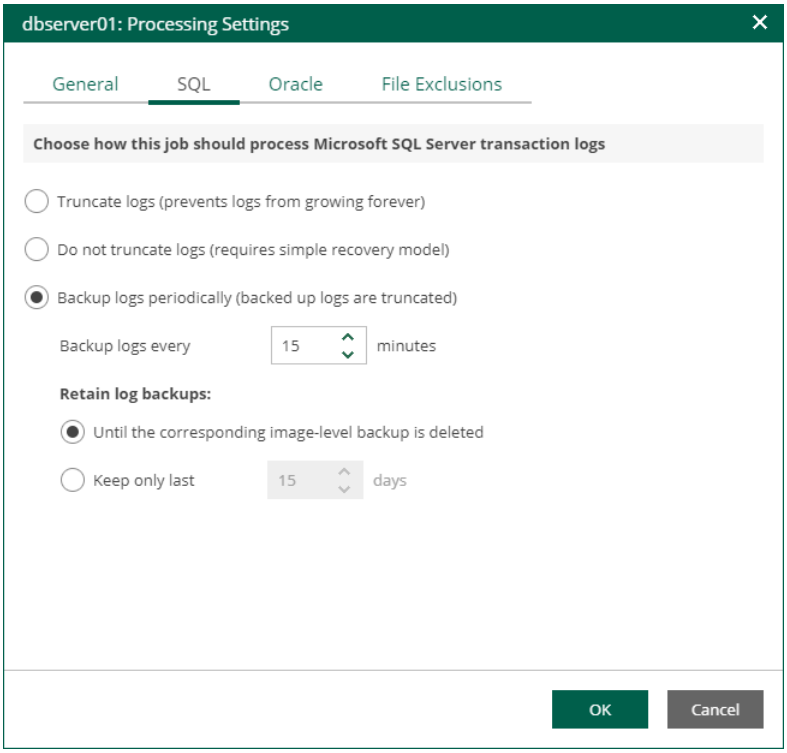
- Select **Do not truncate logs** if you do not want Veeam Backup & Replication to truncate logs at all.
- Select **Backup logs periodically** if you need to backup transaction logs of SQL server machine, storing them to backup repository next to server backup. After transaction logs are placed to repository, they will be truncated on guest. With this option selected, you should also specify how often Veeam will process these transaction logs, uploading them to repository. To set the processing frequency, enter the required value in the **Backup logs every <N> minutes** field (default is every 15 minutes).

  The last option allows you to restore the SQL database to a selected restore point or to a selected point in time, using Enterprise Manager. Restore to specific transaction can be performed using Veeam backup management console. For more information, see the Microsoft SQL Server Transaction Log Settings sections of the Veeam Backup & Replication User Guide.

IMPORTANT

Consider the following:

- If you select the **Do not truncate logs** option, make sure the recovery model for the necessary databases on the SQL server is set to simple (otherwise, logs may drastically increase in size).
- For the **Backup logs periodically** option to take effect, you should ensure that full or bulk-logged recovery model is turned on for the required databases on the SQL server machine. If recovery model is set to simple, no transaction logs will be backed up. If full model is enabled but neither **Backup logs periodically** nor **Truncate logs** option is selected, then logs will increase in size and occupy disk space.



8. If you selected to back up transaction logs, specify how long they should be kept using options in the **Retain log backups** section.

   Select the **Until the corresponding image-level backup is deleted** option, so that you do not have to manually check and ensure that your database and log backup retention policies are consistent, providing all the machine restore points and log backups required for database restore.

9. Click **OK** to save the settings and close the window.

10. At the **Job Schedule** step of the wizard, make sure the schedule is enabled for the job. Otherwise, log backup will not be activated.
11. Click **Finish**.

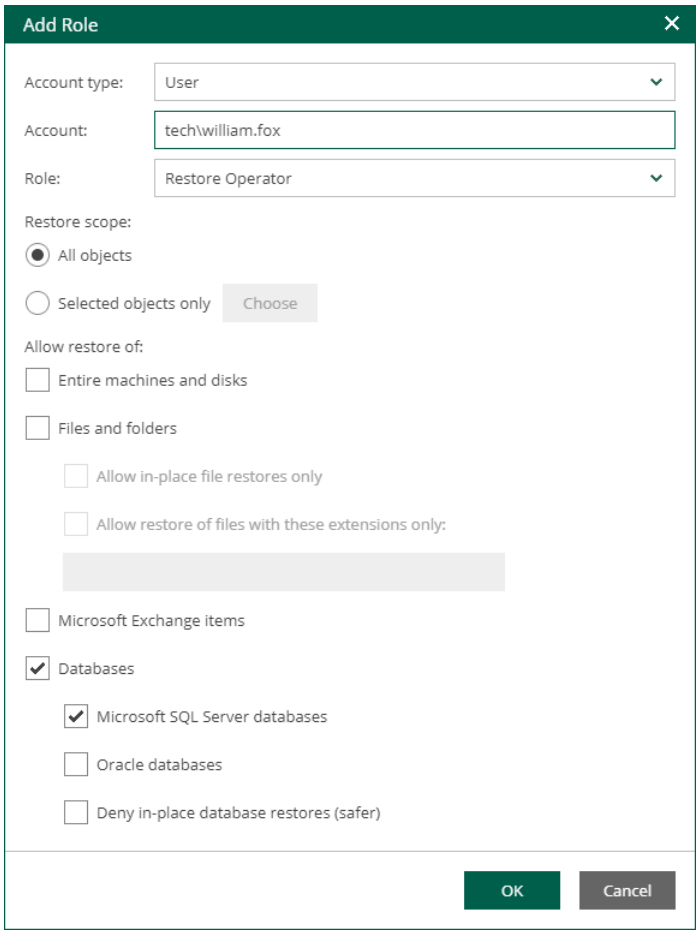
Providing Access Rights

Users responsible for SQL database restore should be assigned an Enterprise Manager role and be able to restore Microsoft SQL Server databases. To allow for database restore, select the **Microsoft SQL Server databases** check box in the **Add Role / Edit Role** window.

If necessary, select the **Deny in-place database restores** check box.

The **Items** tab will become available to these users after they log in to Enterprise Manager.

For more information on how to configure user access rights, see Configuring Accounts and Roles.



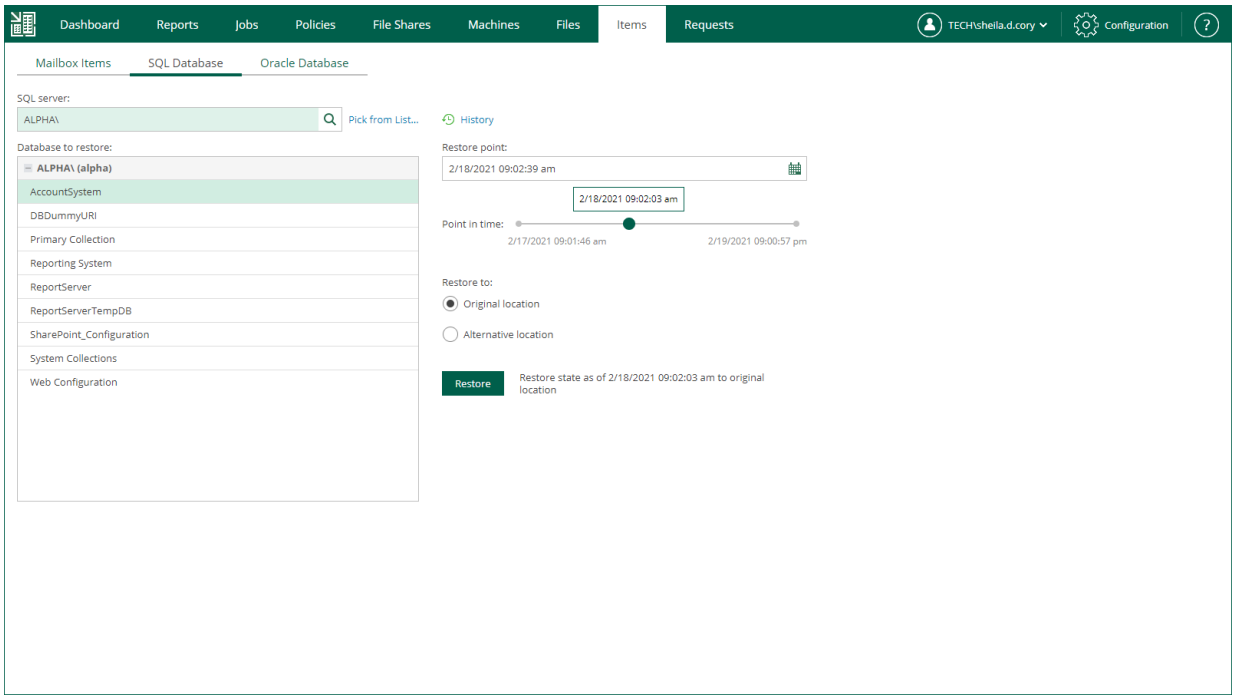
Restore Procedure

To restore a Microsoft SQL Server item:

1. Sign in to Veeam Backup Enterprise Manager using an account with the sufficient permissions. For more information, see Providing Access Rights.
2. Go to the **Items** tab and click **SQL Database**.
3. Enter a name of SQL Server hosting the database you need to restore; use the *server_name*|*instance_name* format. Alternatively, click the **Pick from List** link to select from the list of available SQL Server machine backups.
4. The list of available databases will be displayed. Select the database you need. Consider that user credentials for carrying out the restore procedure will be picked as follows:
   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the SQL Server machine.
   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), user will be prompted to provide the necessary credentials.

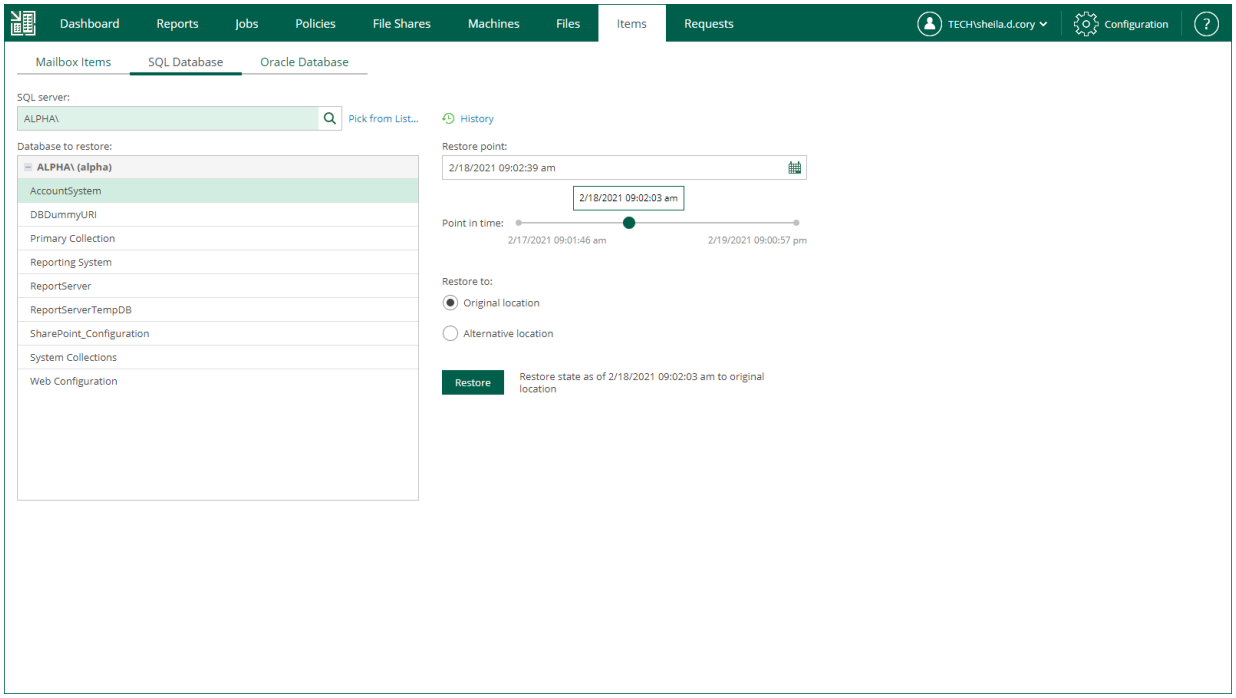
> **NOTE**
>
> For more information on the account roles in Veeam Backup Enterprise Manager that allow the user to restore SQL databases, see Providing Access Rights.

5. Perform restore following the required scenario. For information on the possible restore scenarios, see 1-Click Restore to Original Location and Restore with Custom Settings.



Scenario 1: 1-Click Restore to Original Location

This scenario allows you to restore the selected database to the latest available state back in the original location. For that, make sure the **Original location** option is selected in the **Restore to** section and click **Restore**.



When you restore database items to the original location, Enterprise Manager selects user credentials for the restore procedure according to the following rules:

1. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the SQL Server machine.
2. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), the Enterprise Manager user will be prompted to provide the necessary credentials.

> **NOTE**
>
> For more information on the account roles in Veeam Backup Enterprise Manager that allow a user to restore SQL databases, see Providing Access Rights.

When performing database restore to the original location, a temporary iSCSI connection is established between the target SQL server (it acts as an iSCSI initiator) and mount server associated with the backup repository (it acts as an iSCSI target). For that, Veeam opens a TCP port from the port range 3260-3270; it closes this port after restore session is over.

> **NOTE**
>
> If you restore a database that belongs to an AlwaysOn Availability Group, this database will be restored to the original server and added to the Availability Group.

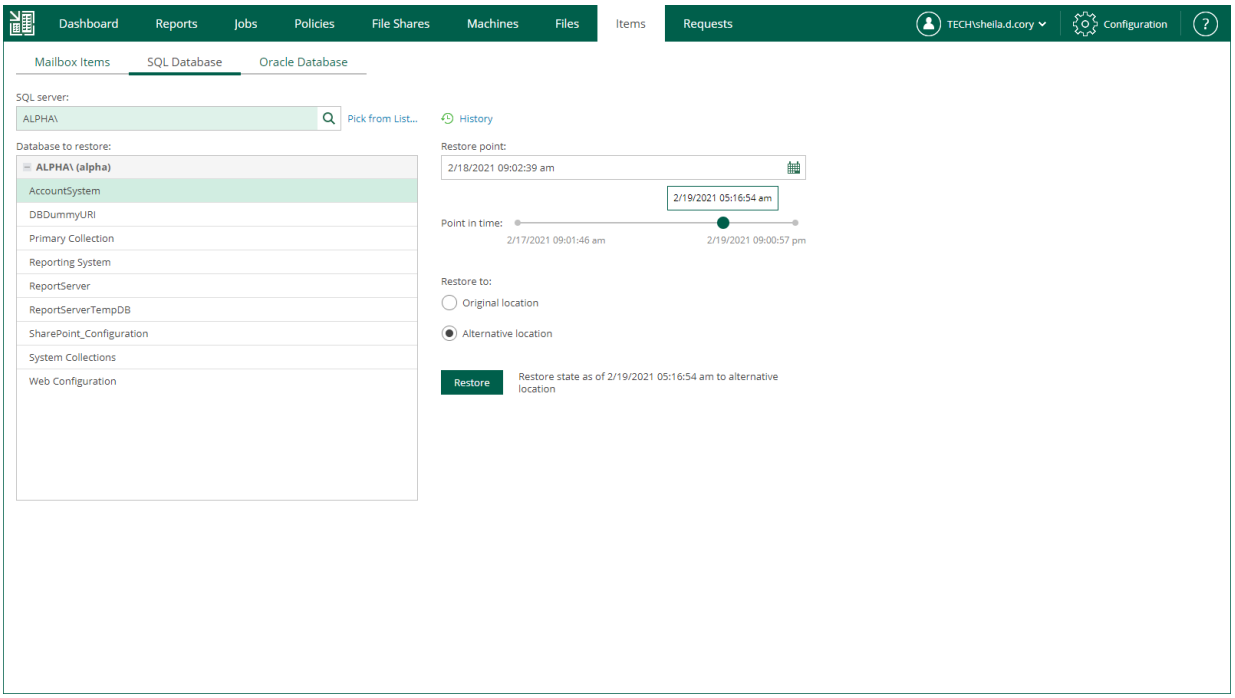
Scenario 2: Restore with Custom Settings

Alternatively, you can carry out the restore procedure with custom settings, specifying the restore point and destination location you need. Do the following:

1. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date.
2. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected SQL server restore point):
   - *Beginning* — refers to the previous restore point of the SQL Server machine that contains the selected database backup. If the previous restore point (server backup) was not found, or the database backup does not exist in it, then *Beginning* will refer to current restore point.
   - *End* — refers to the next restore point which contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then *End* will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then *End* will refer to the latest log backup time.

> **NOTE**
>
> For more information on the transaction log backup, see Microsoft SQL Server Logs Backup and Restore section of the Veeam Backup & Replication User Guide.

3. In the **Restore to** section, select the **Alternative location** option.
4. Click **Restore**.

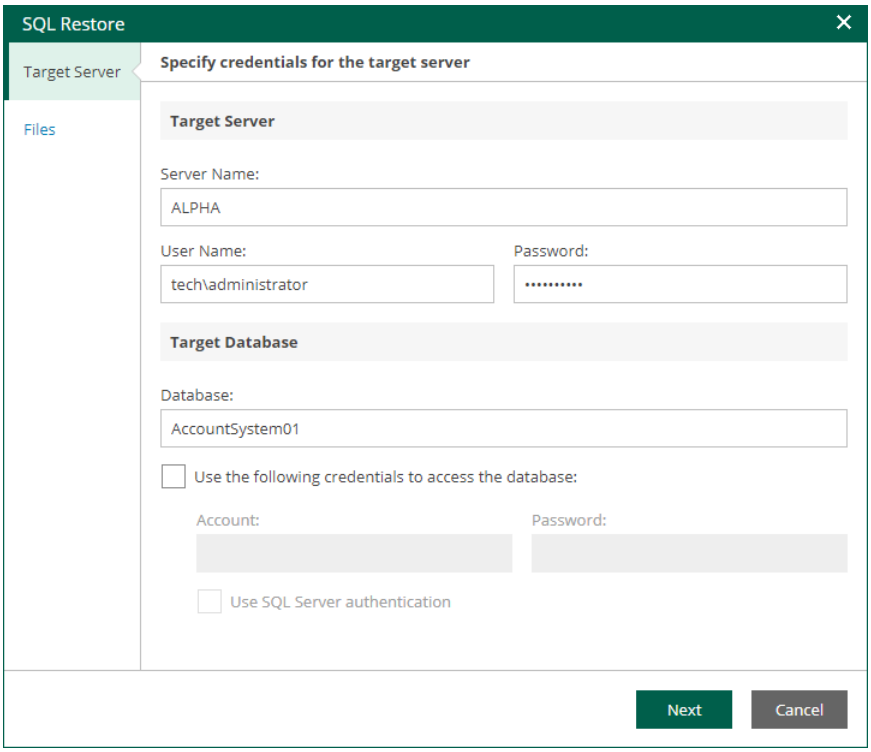


5. At the **Target Server** step of the wizard, specify settings to connect to the target server and database:
   a. In the **Target Server** section, enter the name of the SQL Server or SQL Server instance in the *SERVER\INSTANCE* format, and credentials of the account that will be used to connect to the target server.

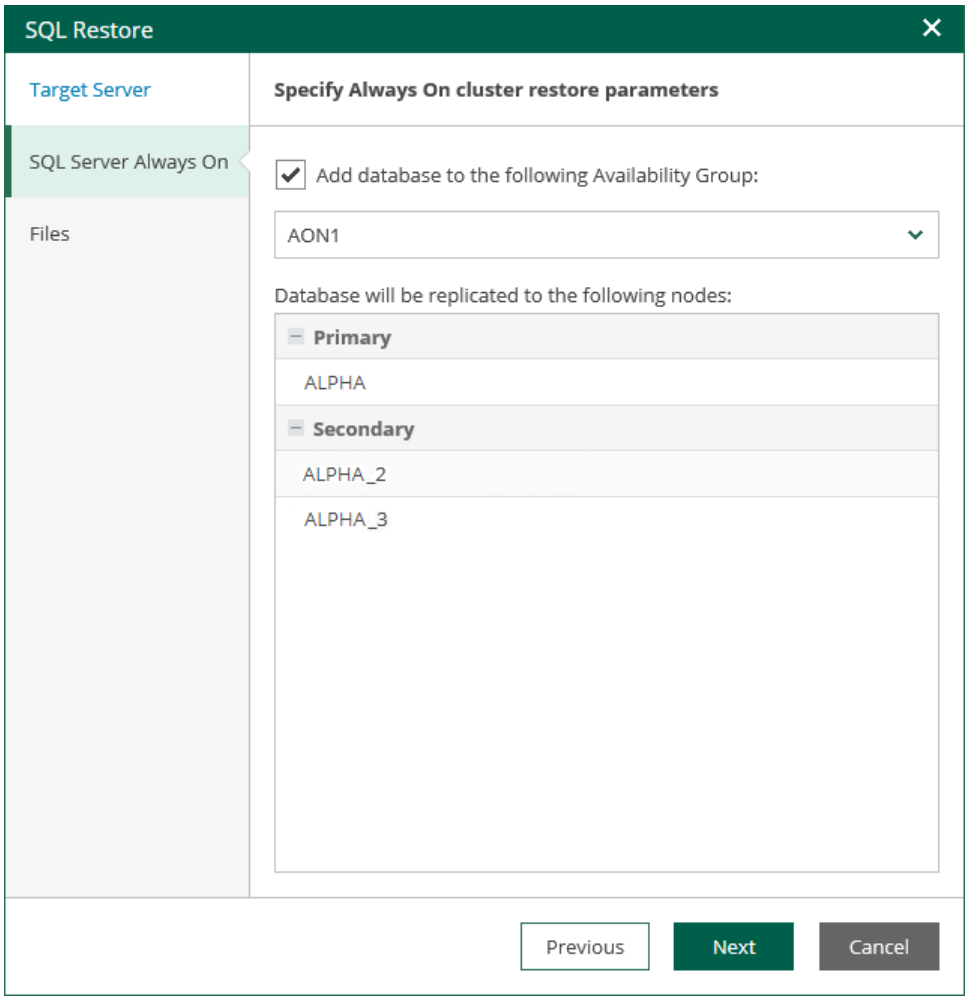
b. In the **Target Database** section, enter the name of the target database.

c. To use a separate account for connection to the target database, in the **Target Database** section, select the **Use the following credentials to access the database** check box and specify credentials of the necessary account.

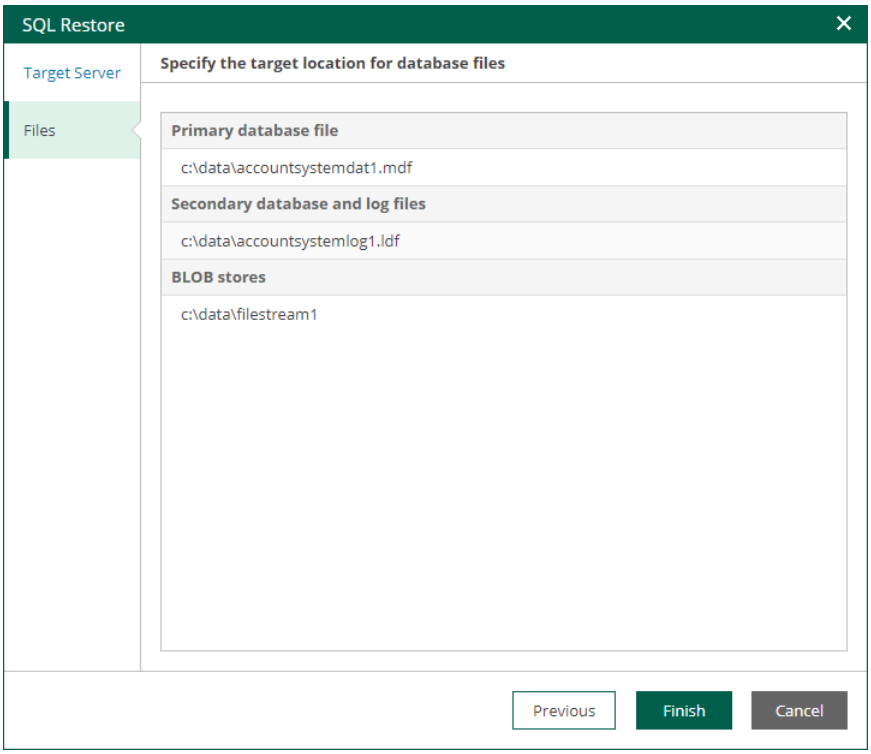
d. If you want to use SQL Server authentication when connecting to the database, select the **Use SQL Server authentication** check box.



6. If AlwaysOn Availability Groups are present on the target server, at the **SQL Server Always On** step of the wizard, you can add the restored database to an Availability Group.



7. At the **Files** step of the wizard, you can specify paths to database files on the target server. You can specify separate target locations for the primary database file and secondary database file with logs.



8. Click **Finish**. Veeam Backup Enterprise Manager will start the restore operation and display the status of the restore process on the **Items** tab.

Backup and Restore of Oracle Databases

Authorized personnel can use Veeam Backup Enterprise Manager to restore the necessary databases from Oracle Server machine backups.

> **NOTE**
>
> This functionality is provided in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Restore Requirements and Limitations

- Enterprise Manager supports restore from backups created with Veeam Backup & Replication versions 9.0 and later.
- Enterprise Manager supports restore over a network connection only. Restore using PowerShell Direct, VIX or Sphere API is not supported.
- Enterprise Manager does not support database restore from storage snapshots.

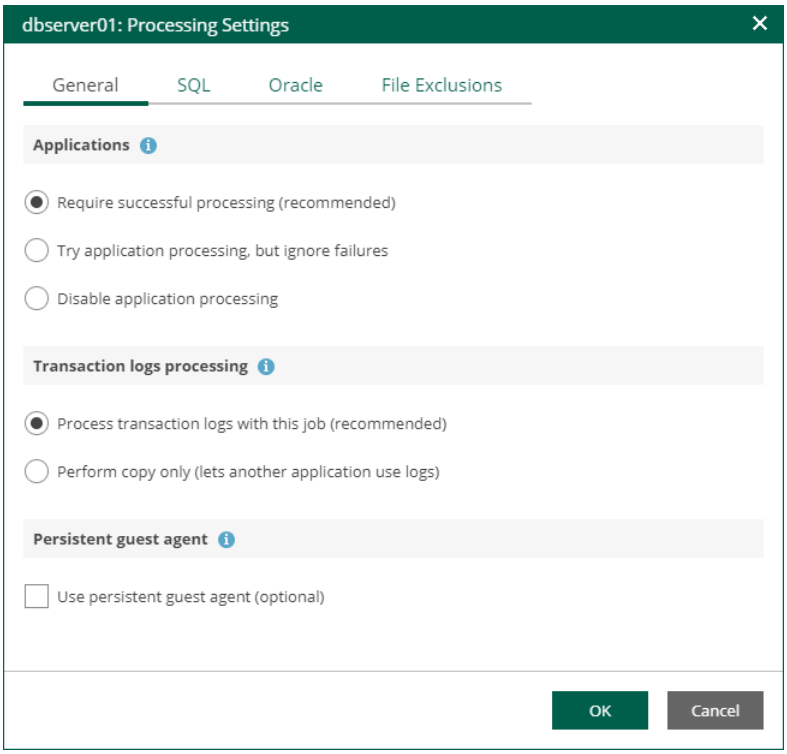
Preparing Application-Consistent Backup

To provide for recoverability of Oracle database, make sure you have an application-consistent backup of your Oracle server machine created successfully. For more information on an application-consistent backup, see Application-Aware Processing. Also, if you plan to restore the database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then log processing should be configured, as described below.

To configure job settings:

1. Go to the **Jobs** tab and select your Oracle server backup job.
2. Click **Job** on the toolbar and select **Edit** to start the job wizard.
3. Proceed to the **Guest Processing** step of the wizard and make sure the **Enable application-aware processing** check box is selected.
4. Click the **Customize Application** link. In the displayed window, select the Oracle server machine from the list and click **Edit**.
5. On the **General** tab, make sure the **Require successful processing** option is selected in the **Applications** section.
6. To be able to specify transaction log handling options, make sure the **Process transaction logs with this job** option is selected. Otherwise, if you select the **Perform copy only** option, Veeam Backup & Replication will create a copy-only backup, and Oracle archived logs will not be deleted — that is why the **Oracle** tab with log handling settings will be deactivated in this case. For more information, see the Oracle Archived Log Settings section of the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> If both Microsoft SQL Server and Oracle are installed on one machine, and this machine is processed by a job with log backup enabled for both applications, Veeam Backup & Replication will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.



7. Open the **Oracle** tab and specify how archived logs will be handled:

   a. Specify a user account that will connect to Oracle system and perform Oracle archived logs backup and\or deletion. You can select **Use guest credentials** – then Veeam will use the account specified for guest processing in the job configuration for both guest OS access and for connection to the Oracle system. You can also specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account. In any case, make sure the account you specify has sufficient rights. For details, see the Required Permissions section of the Veeam Explorer for Oracle guide.

   b. Specify whether archived logs should be deleted on the Oracle server machine, and whether Veeam should back them up them to repository. Veeam Backup & Replication supports the following options:

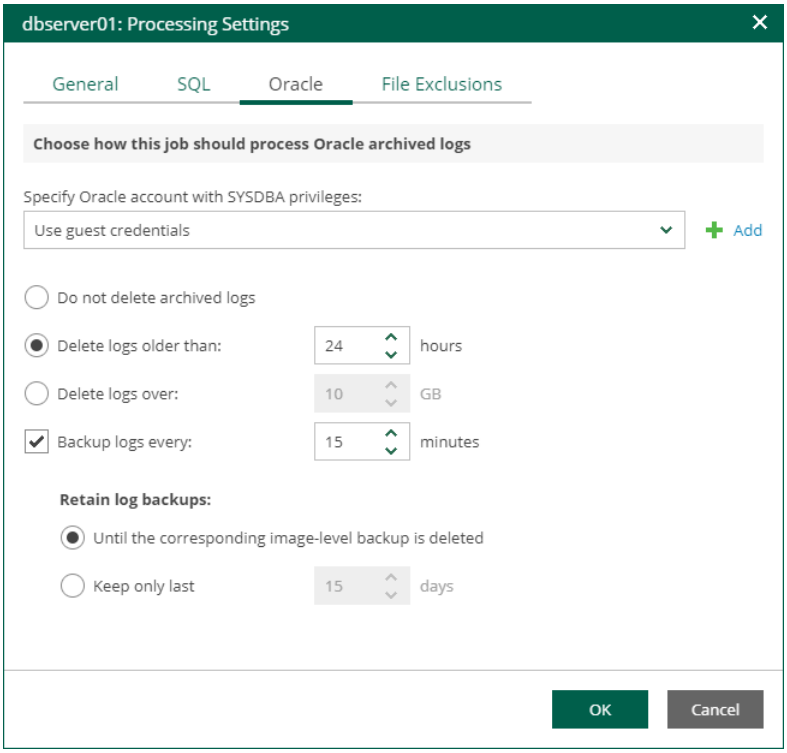
      - **Do not delete archived logs** – this option instructs Veeam to preserve archived redo logs (if any) on the original Oracle server. With this option selected, your database administrator will have to take care of database logs. Applicable restore scenario — database restore to the state as of the currently selected machine restore point, to the selected point in time and to the selected transaction.

      - **Delete logs older than <N> hours / Delete logs over <N> GB** – with this option selected, Veeam will wait for the image-level machine backup to complete, and then it will trigger archived log deletion from guest, using the specified condition (log age or size). If archived logs cannot be deleted for some reason, these logs will remain untouched in the guest machine until the next start of the Veeam runtime process.

      - With any of these options, you can also use the **Backup logs every <N> minutes** check box. If you select this check box, Veeam Backup & Replication will periodically ship archived logs to the backup repository and store them next to the Oracle server machine backup. Make sure that Oracle ARCHIVELOG mode is turned on (contact your database administrator, if necessary). This option will support any database restore scenario: to the state as of in currently selected machine restore point, to any point in time or to the state before particular transaction.

IMPORTANT

If you plan to use this option together with archived logs deletion from Oracle machine guest, make sure that these settings are consistent: logs should be deleted after they are backed up to repository, not vice versa. Thus, you need to set up backup schedule and log removal conditions appropriately. Default log backup interval is 15 minutes, maximum interval is 480 minutes.



8. If you selected to back up archived logs, specify how long they should be kept using the **Retain log backups** options.

   Select the **Until the corresponding image-level backup is deleted** option, so that you do not have to manually check and ensure that your database and log backup retention policies are consistent, providing all the machine restore points and log backups required for database restore.

9. Click **OK** to save the settings and close the window.

10. At the **Job Schedule** step of the wizard, make sure the schedule is enabled for the job. Otherwise, log backup will not be activated.

11. Click **Finish**.

Providing Access Rights

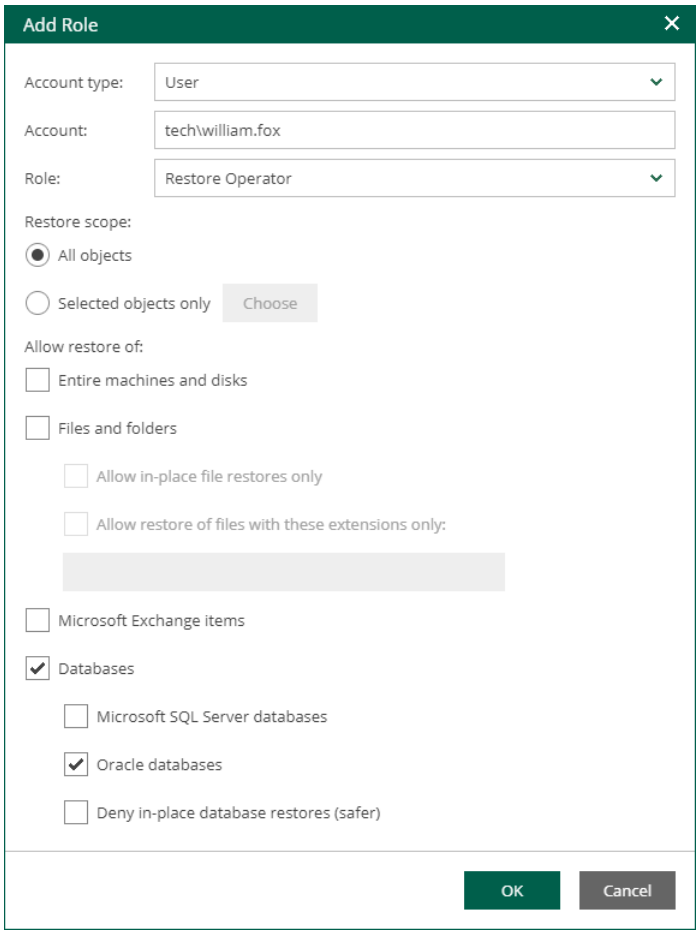
Users responsible for Oracle database restore must be assigned an Enterprise Manager role and be able to restore Oracle databases.

To allow users with the **Restore Operator** or **Portal User** role to restore Oracle databases:

1. In the **Add Role / Edit Role** window, select the **Databases** check box.
2. Select the **Oracle databases** check box.
3. [Optional] If necessary, select the **Deny in-place database restores** check box.
4. Click **OK**.

The **Items** tab will become available to these users after they log in to Enterprise Manager.

For more details on role assignment, see Configuring Accounts and Roles.



Restore Procedure

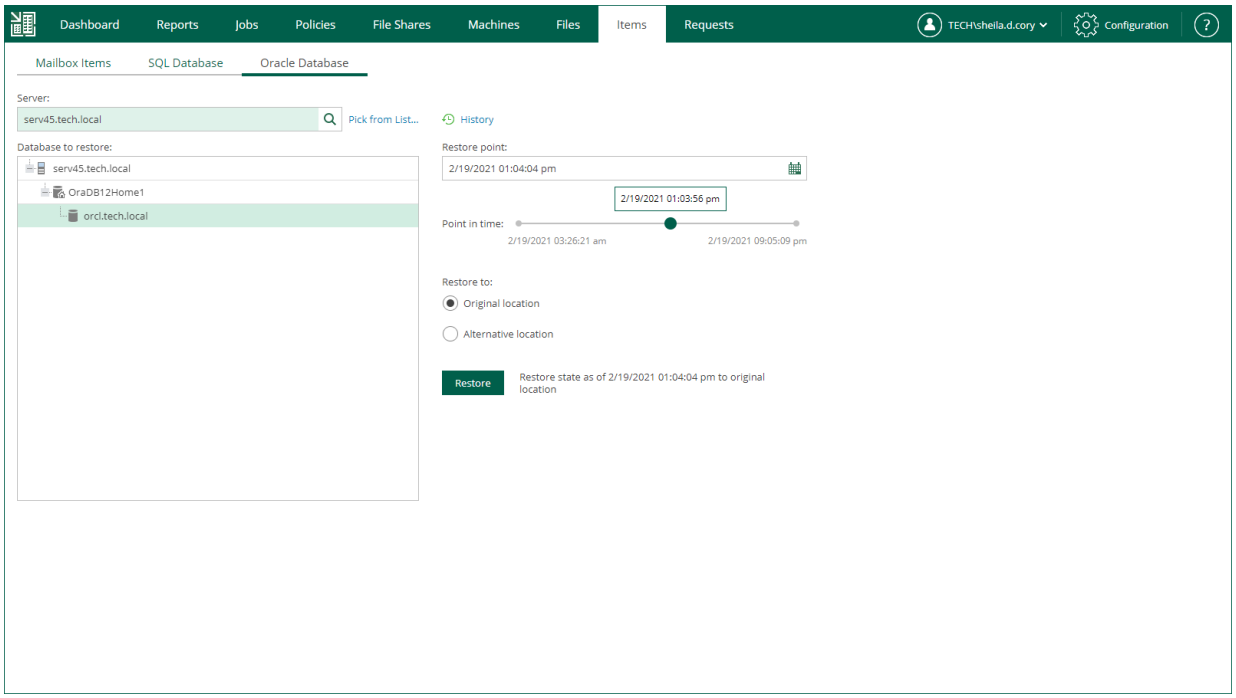
To restore a database item:

1. Sign in to Veeam Backup Enterprise Manager using an account with the sufficient permissions. For more information, see Providing Access Rights.
2. Go to the **Items** tab and click **Oracle Database**.
3. Enter the name of Oracle server hosting the database you need to restore. Alternatively, click the **Pick from List** link to select from the list of available Oracle server machine backups.
4. Select Oracle home and the database you need. Consider that user credentials for carrying out the restore procedure will be picked as follows:
   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Oracle server machine, or the account which is currently logged in.
   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on Windows server, then you may need to enter password for Oracle home.

> **NOTE**
>
> The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see Providing Access Rights.

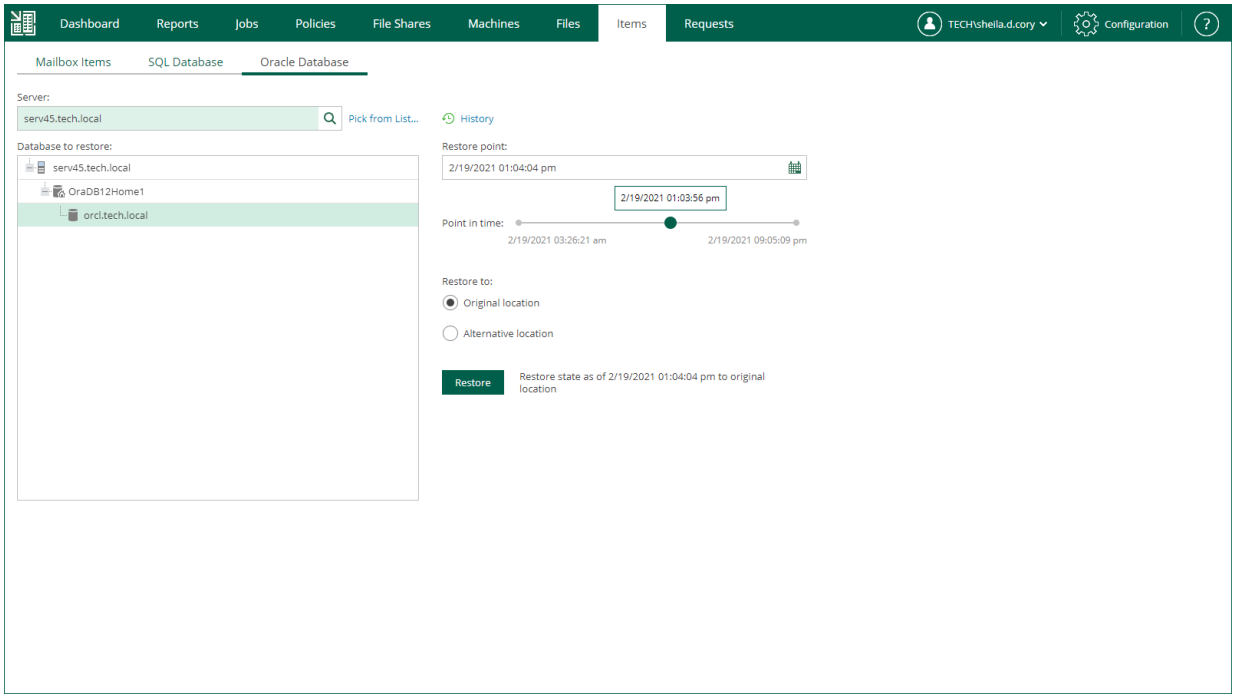
5. Perform restore following the required scenario. For information on the possible restore scenarios, see Scenario 1: 1-Click Restore to Original Location and Scenario 2: Restore with Custom Settings.

To view restore session log, click **History**.



Scenario 1: 1-Click Restore to Original Location

This scenario allows you to restore the selected database to the latest available state back in the original location. For that, make sure the **Original location** option is selected in the **Restore to** section and click **Restore**.

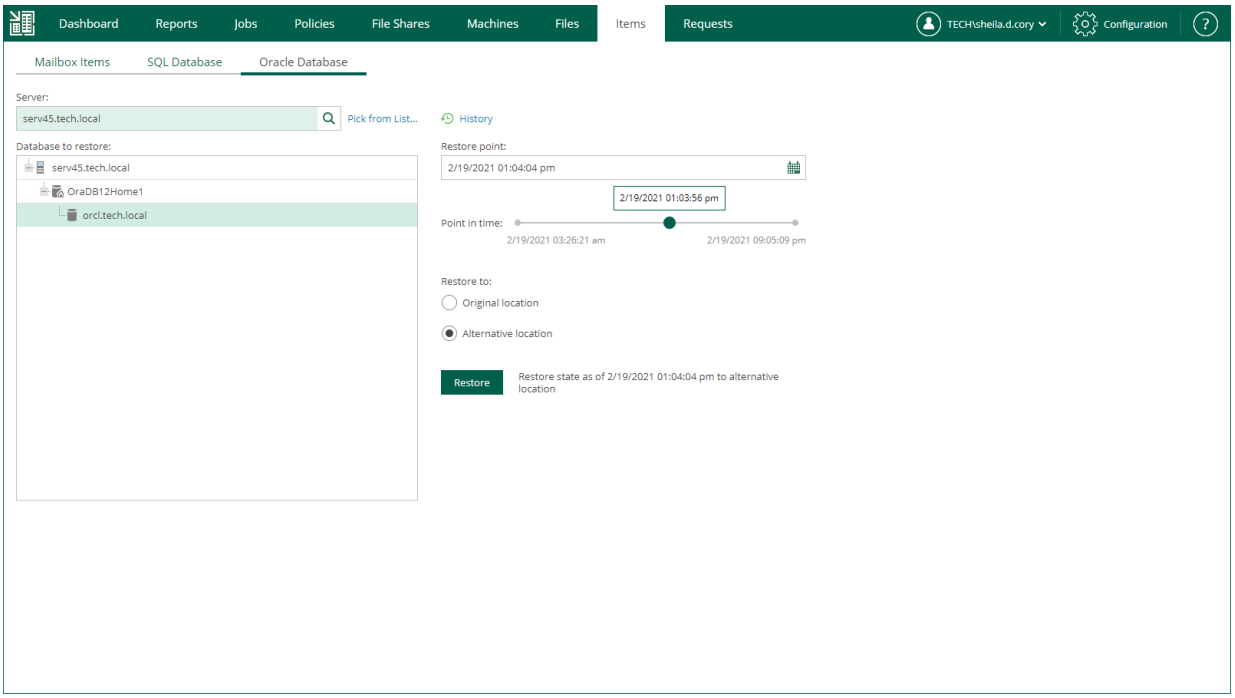


When performing database restore to the original location, a temporary iSCSI connection is established between the target Oracle server (it acts as an iSCSI initiator) and mount server associated with the backup repository (it acts as an iSCSI target). For that, Veeam opens a TCP port from the port range 3260-3270; it closes this port after restore session is over.

Scenario 2: Restore with Custom Settings

Alternatively, you can carry out the restore procedure with custom settings, specifying the restore point and destination location you need. Do the following:

1. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date.



2. If you have backed up archived redo logs for the database, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected Oracle database restore point):

   - *Beginning* — refers to the previous restore point of Oracle server machine that contains selected database backup. If the previous restore point (server backup) was not found, or the database backup does not exist in it, then *Beginning* will refer to current restore point.
   - *End* — refers to the next restore point that contains selected database backup. If the next restore point (server backup) and associated transaction log backup are not found, or if the database backup does not exist in the server backup, then *End* will refer to the current restore point. If the next restore point (server backup) is not found but transaction log backup exists for the preceding period, then *End* will refer to the latest log backup time.

> **NOTE**
>
> For more information on log backup, see Preparing and Application-Consistent Backup.

3. To specify a location where you want to restore the database items, select the necessary option in the **Restore to** section:

   - If you want to restore items to the original database, select **Original location**. If you select this option, consider that Enterprise Manager will select user credentials for the restore procedure according to the following rules:

     i. Veeam Backup Enterprise Manager will try to use the account specified in the backup job that contains the Oracle server machine or the account which is currently logged in.

ii. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on a Microsoft Windows server, you may need to enter password for the Oracle home.

> **NOTE**
>
> The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see Providing Access Rights.

- If you want to restore items to another database, select **Alternative location**. If you select this option, you will need to specify restore settings using the **Oracle Restore** wizard. For details, see Using Oracle Restore Wizard.

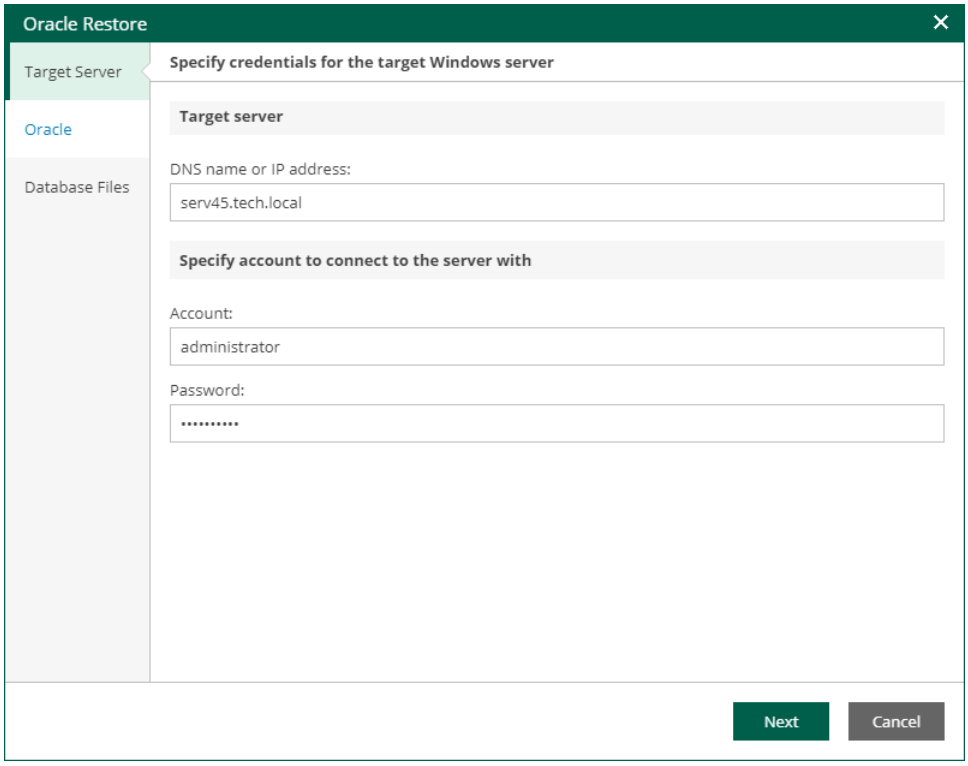
4. Click **Restore**.
   - In case of restore to the original location, the restore process will start immediately.
   - In case of restore to another location, Enterprise Manager will launch the **Oracle Restore** wizard. For more information, see Using Oracle Restore Wizard.

Using Oracle Restore Wizard

If you restore Oracle database items to another location, specify restore settings using the **Oracle Restore** wizard:

1. At the **Target Server** step of the wizard, specify settings to connect to the server where the database should be restored:
   - For database restore on a Microsoft Windows server, specify connection settings in the following way:
     i. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Microsoft Windows server.

ii. In the **Account** and **Password** fields, specify credentials of the account that will be used be used for connection with the target Windows-based Oracle server. Make sure the account has the *sysdba* rights on that server (Windows authentication will be used). To be able to copy archived logs from backup to the target server for further replay (in case of restore to certain point in time), the account should be also granted sufficient permissions to access the administrative share on that machine (for example, `\\myserver\C$`): *Read* and *Write* are minimum required, *Full Control* recommended.



- For database restore on a Linux server, specify connection settings in the following way:

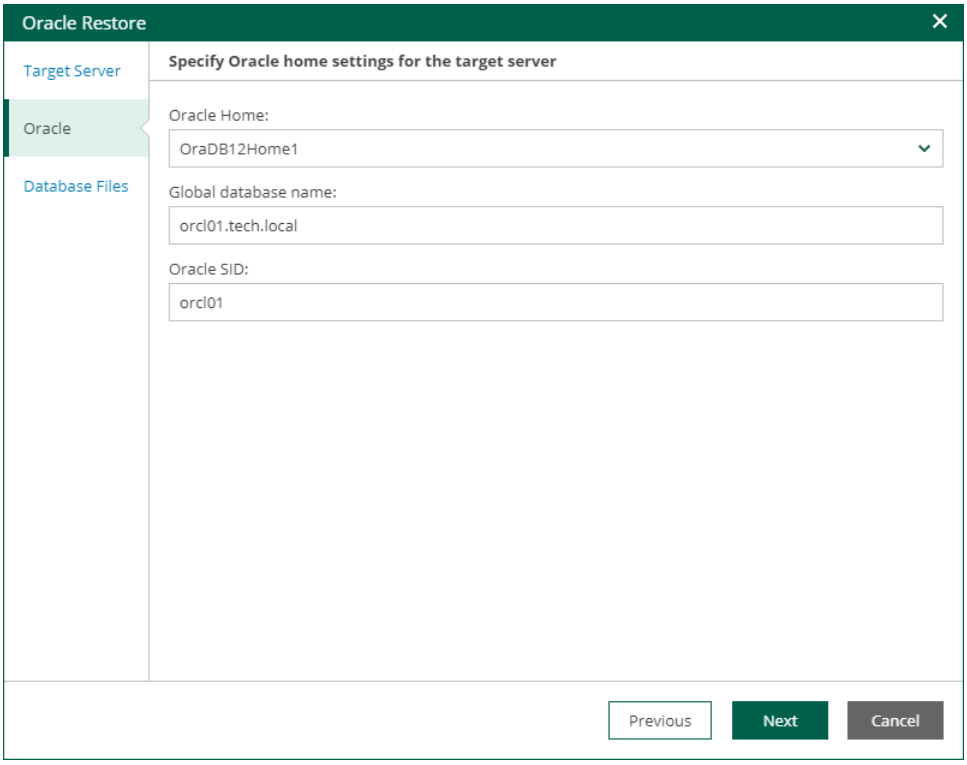
  i. Server name (or IP address) and SSH port — default port is **22**.

  ii. Account to be used to access the server. This should be a **root** account or account elevated to **root** and added to the `sudoers` file. To elevate the account and add it to the `sudoers` file, click **Settings** and select the corresponding options.

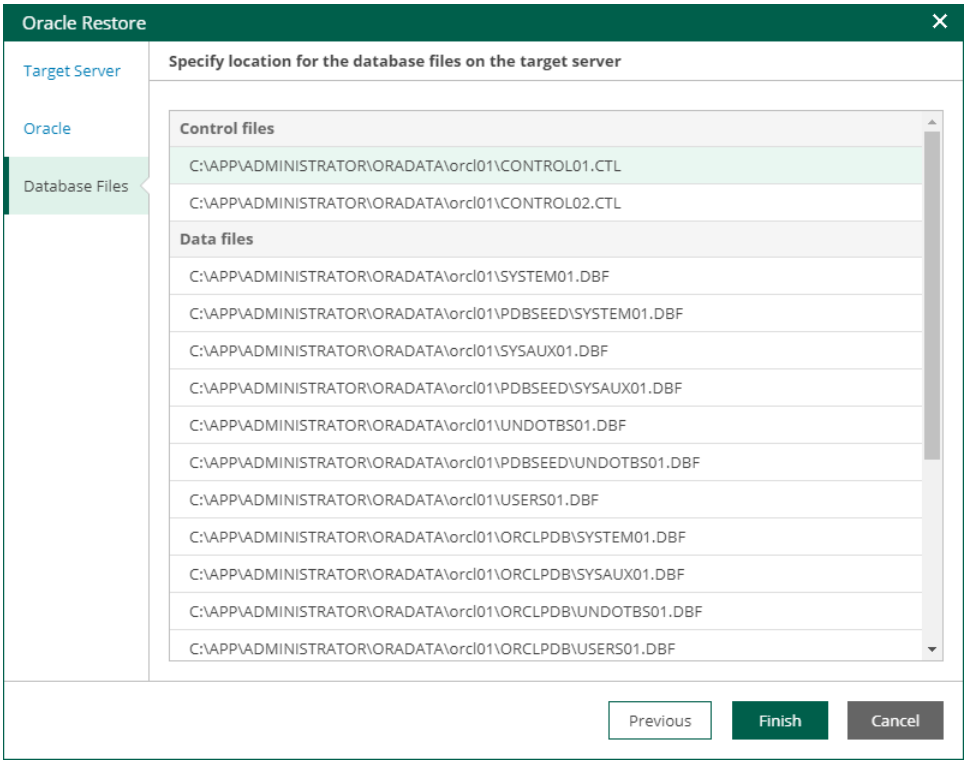
  You can use authentication by a user name and password or by a private key.

4. At the **Oracle** step of the wizard, select **Oracle Home** and specify **Global database name** and **Oracle SID** where to restore the database from backup.

   Consider that if database with the specified Oracle SID exists on the target Oracle home, the restore process by design will delete it and replace with the database from backup. Thus, before starting the restore process, a message will be displayed, asking you to confirm the operation.



5. At the **Database Files** step of the wizard, specify paths to database files on the target server.



6. Click **Finish**. Veeam Backup Enterprise Manager will start the restore operation and display the status of the restore process on the **Items** tab.

Managing Encryption Keys

Veeam Backup Enterprise Manager provides you with an alternative way for data encryption. It lets you decrypt the data in case you have lost or forgotten the password used for data encryption. For more information on the concept, terms and procedures of data encryption, see the Data Encryption section of the Veeam Backup & Replication User Guide.

For encryption, Veeam Backup Enterprise Manager uses an Enterprise Manager keyset — a pair of matching keys:

- Public Enterprise Manager key encrypts storage keys on backup servers connected to Veeam Backup Enterprise Manager.
- Private Enterprise Manager key decrypts storage keys in case a password for encrypted backup or tape is lost.

To let Veeam Backup & Replication encrypt and decrypt data with Enterprise Manager keys, make sure Enterprise Manager keys are enabled in Veeam Backup Enterprise Manager.

To enable Enterprise Manager keys, do the following:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, select the **Enable encryption password loss protection** check box.
3. To save the changes, click **Save**.

During Veeam Backup Enterprise Manager installation, the setup automatically generates an Enterprise Manager keyset. You can perform the following operations with Enterprise Manager keysets using Enterprise Manager:

- Generate a new Enterprise Manager keyset
- Activate an Enterprise Manager keyset
- Specify retention settings for an Enterprise Manager keyset
- Export and import an Enterprise Manager keyset
- Delete an Enterprise Manager keyset

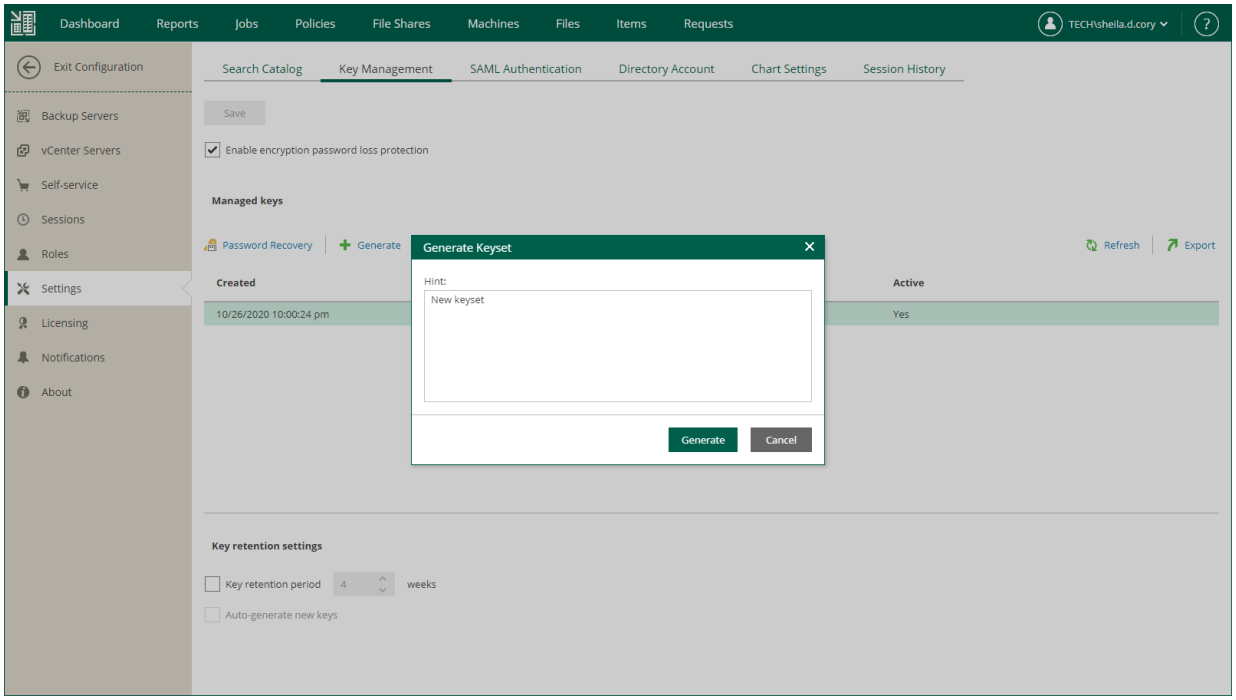
Generating Enterprise Manager Keyset

For safety's sake, periodically generate a new pair of Enterprise Manager keys. Regular change of encryption keys raises the encryption security level.

Enterprise Manager keys are created in the inactive state. To make the keys active and use them for encryption and decryption, you need to activate the keys.

To generate a new Enterprise Manager keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, click **Generate**.
3. In the **Hint** field, enter a description for the created keyset. The keyset description will help you to distinguish the created keyset in the list. Click the **Generate** button when ready.



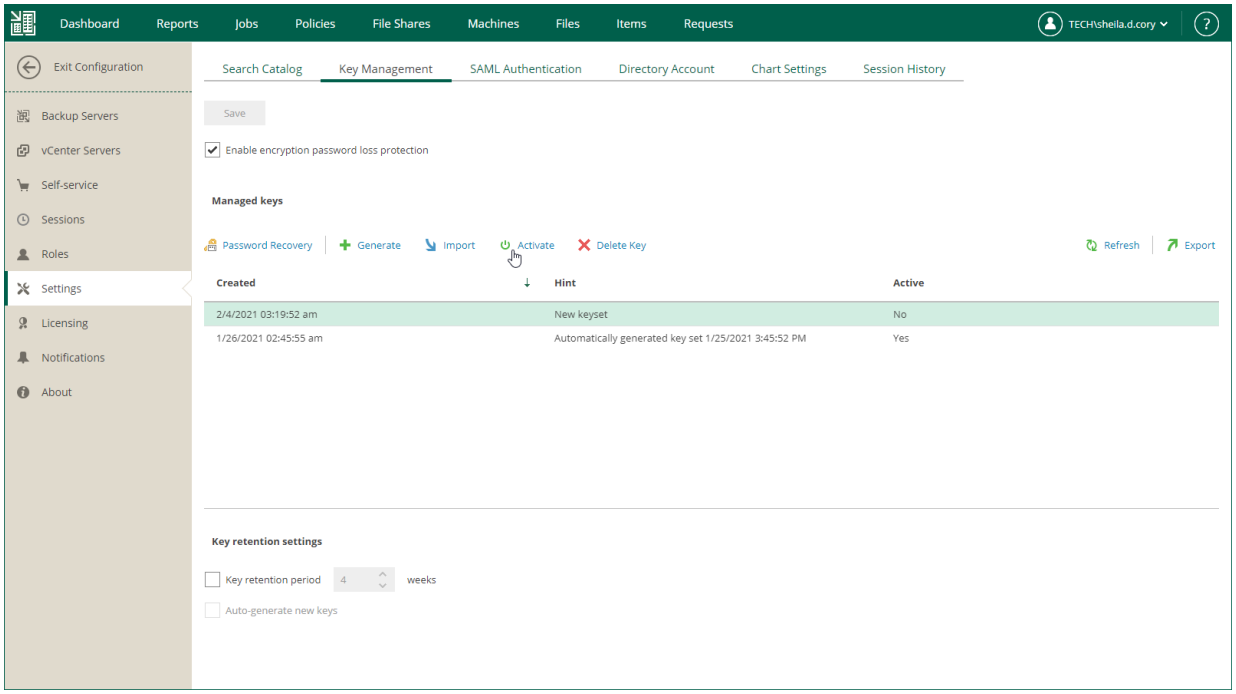
Activating Enterprise Manager Keyset

Active Enterprise Manager keys are the keys that are currently used in the encryption process. After you create a new keyset, you need to activate it. As a result of activation, Veeam Backup Enterprise Manager performs the following actions:

- Public Enterprise Manager key is propagated to all Veeam backup servers connected to Veeam Backup Enterprise Manager.
- Private Enterprise Manager key remains on Veeam Backup Enterprise Manager and marked as active.

You can activate a keyset manually. For that, do the following:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select an inactive keyset in the list and click **Activate**.



Note that manual activation can be performed for any keyset in the list (generated manually or automatically).

If you want your automatically generated keysets to be activated automatically upon creation, then you should configure the retention policy settings. For more information, see Specifying Retention Settings for Enterprise Manager Keyset.

> **NOTE**
>
> Consider that manually generated keysets will require manual activation.

Specifying Retention Settings for Enterprise Manager Keyset

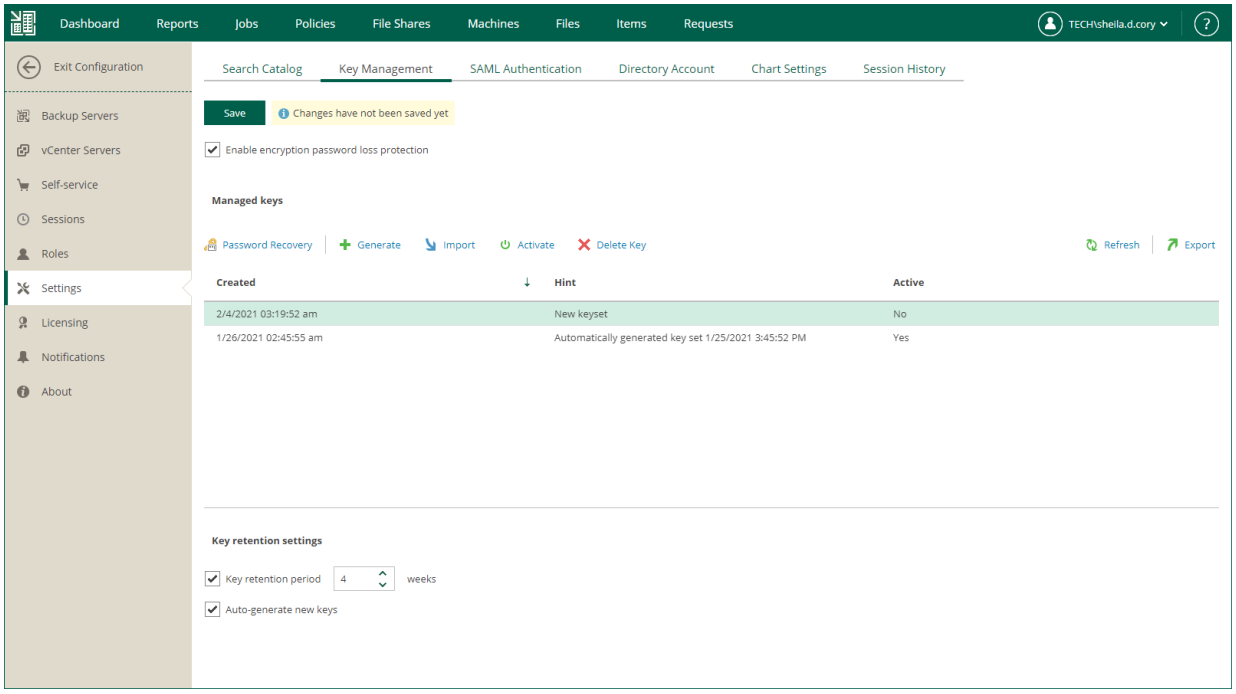
In some cases, government regulations and internal company policies require that you regularly change encryption keys. The shorter is the lifetime of an encryption key, the smaller amount of data is encrypted with this key and the higher is the level of encryption security.

Lifetime of Enterprise Manager keys is controlled by a key retention period. The key retention period defines for how long Enterprise Manager keys must remain in effect and must be used for encryption and decryption.

You can specify a retention period for an Enterprise Manager keyset.

To specify retention policy for Enterprise Manager keys:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select the necessary options:
   - If you want to set a retention period for Enterprise Manager keysets, select the **Key retention period** check box and specify the number of weeks for which Enterprise Manager keys must remain in effect (default is 4 weeks). After the retention period is over, and with key auto-generation is turned off, a user will receive a notification email and should then manually create and activate a new keyset. After a new keyset is ready, old keyset is marked as inactive.
   - If you want Veeam Backup Enterprise Manager to automatically generate a new keyset, select the **Auto-generate new keys** check box. After the current keyset expires, Veeam Backup Enterprise Manager will automatically generate a new keyset and mark it as active. During the next data synchronization session, Veeam Backup Enterprise Manager will propagate the newly created public Enterprise Manager key to all connected Veeam backup servers. The private Enterprise Manager key will remain on Veeam Backup Enterprise Manager and will be used for data decryption.
3. Click **Save** to save the settings.



Exporting and Importing Enterprise Manager Keyset

It is important to regularly back up your Enterprise Manager keys or save their copies in a safe place. If you lose a password for an encrypted backup or tape, you can unlock this backup or tape with the private Enterprise Manager key and the Enterprise Keys Restore wizard.

However, in some situations, a matching private Enterprise Manager key may be not available. This can happen, for example, if your Veeam Backup Enterprise Manager database has failed or you use a new installation of Veeam Backup Enterprise Manager and a new database. In this case, Veeam Backup Enterprise Manager will not find a matching private Enterprise Manager key in the database and will be unable to unlock the backup or tape encrypted with the public Enterprise Manager key.

You can create a backup copy of an Enterprise Manager keyset with the export operation in Veeam Backup Enterprise Manager. The exported keyset is saved as a file of the PEM format and contains private and public Enterprise Manager keys. You can save the exported keyset on the local disk or on a network share. An exported keyset can be imported back to Veeam Backup Enterprise Manager any time you need.

To export a keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select a keyset you want to back up and click **Export**.
3. Save the resulting PEM file on the local disk or in a network shared folder.

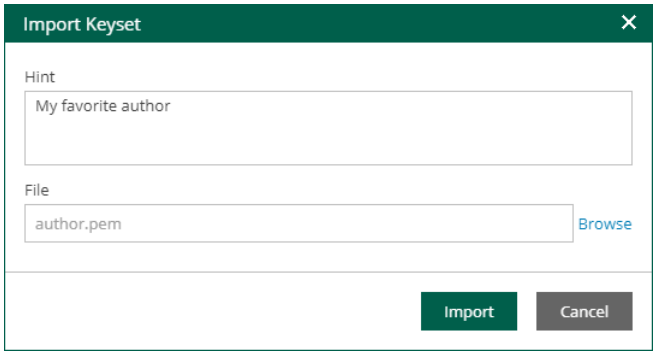
To import a previously exported keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, click **Import**.
3. Click **Browse** next to the **File** field and select a previously exported keyset.
4. In the **Hint** field, Veeam Backup Enterprise Manager displays a hint that you provided when creating the imported keyset.
5. Click **Import**.

When you import a keyset, it is saved to the Veeam Backup Enterprise Manager database and displayed in the keyset list in Veeam Backup Enterprise Manager.

NOTE

An imported keyset has the Inactive state. You must activate it to be able to use the keys from the keyset for backup encryption (for restore procedures, activation is not necessary). For more information, see Activating Enterprise Manager Keyset.



Deleting Enterprise Manager Keyset

You can delete an Enterprise Manager keyset in case it is no longer needed.

Only keys in the **Inactive** state can be deleted. You cannot delete keys that are currently active.

To delete a keyset:

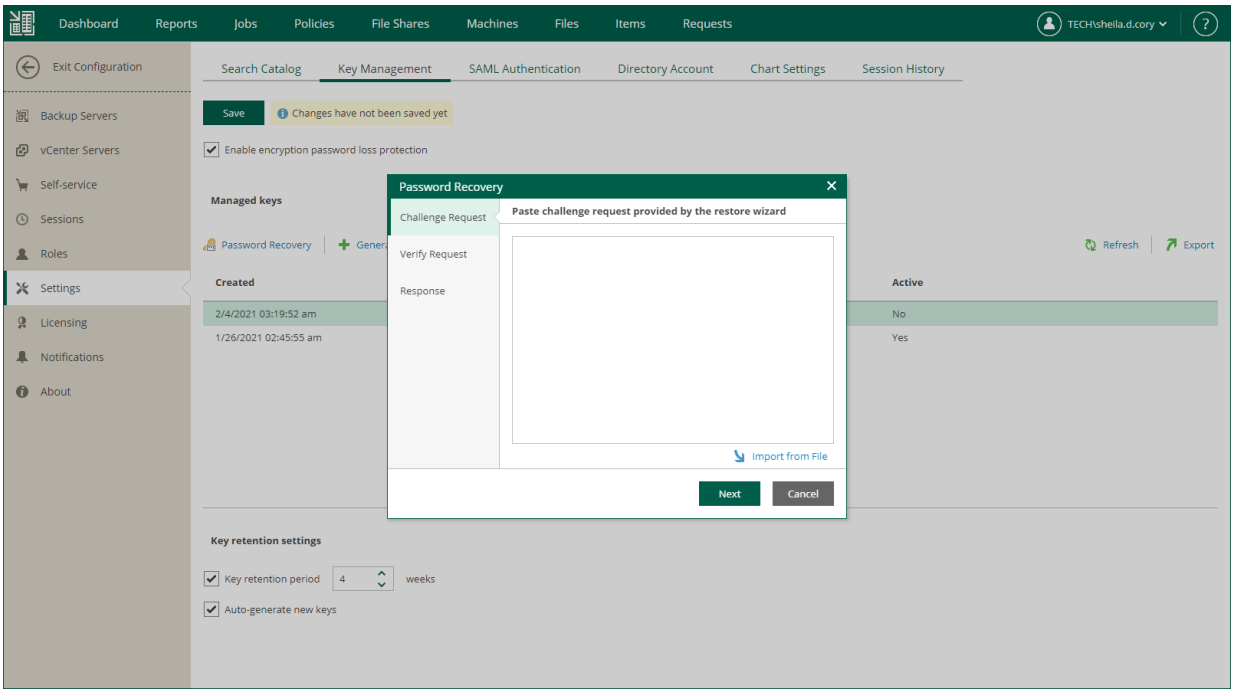
1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select the necessary keyset in the list and click **Delete Key**.

> **IMPORTANT**
>
> It is strongly recommended that you export a keyset before you delete it. If you delete a keyset and do not make its backup copy, you will not be able to restore data from a backup or tape encrypted with keys from this keyset in case a password is lost. For more information, see Exporting and Importing Enterprise Manager Keyset.

Handling Password Recovery Requests

When an encrypted backup file or tape media is imported to the Veeam backup server, a password is required to decrypt data. In some cases, however, a password can be lost or forgotten. Veeam Backup & Replication offers a way to restore data from encrypted backups or tapes even if a password is not available. For that, Veeam Backup Enterprise Manager administrator runs the **Password Recovery** wizard within the following context:

1. As a Veeam Backup Enterprise Manager Administrator, you receive a request for password restore, for example, by email.
2. Then you start the **Password Recovery** wizard by clicking the **Password Recovery** button in **Configuration > Key Management**, and insert the text of the request to the wizard.



3. Veeam Backup Enterprise Manager finds a matching public backup server key in Veeam Backup Enterprise Manager database and decrypts the signature with this key.
4. The wizard decrypts storage keys with the private Enterprise Manager key available on Veeam Backup Enterprise Manager, and generates a response. The response represents a text document and contains decrypted storage keys. Consider that the response is also encrypted and can be used only on the Veeam backup server where the request was issued.
5. Then you can send the response back to requester, for example, by email. The requester will input this response to the Enterprise Keys Restore wizard on the Veeam backup server where the request was issued; Veeam Backup & Replication will process the response, retrieve the decrypted storage keys and use them to unlock encrypted backups or tapes and retrieve their content.

IMPORTANT

In case your organization encrypts configuration backups of a Veeam backup server, and you want to be able to serve password restore request for these backups, ensure the original Veeam backup server and its public key (used for configuration backup encryption) are present on the Enterprise Manager server by the moment you receive such a request. Consider the following:

- If a Veeam backup server is removed from Enterprise Manager, its public key will be deleted from the Enterprise Manager database.
- If a new configuration database is created on Veeam backup server, then a new public key will be automatically generated for that Veeam backup server on Enterprise Manager, replacing its existing key.

For details on Enterprise Manager keysets, encryption passwords and password restore, see the Data Encryption section of the Veeam Backup & Replication User Guide.

Working with Virtual Lab Requests

The **Requests** tab allows you to create, approve and reject virtual lab requests, as well as prolong the time of virtual lab running which are part of the U-AIR process. The procedures are described in the following sections:

- Creating Virtual Lab Requests
- Approving Virtual Lab Requests

For more information, see Veeam Universal Application Item-Level Restore User Guide.

Creating Virtual Lab Requests

Users with the Portal Administrator role can create Virtual Lab requests directly from the Enterprise Manager web UI. For more information on roles, see Configuring Accounts and Roles.

Requests that are created in Enterprise Manager are approved automatically.

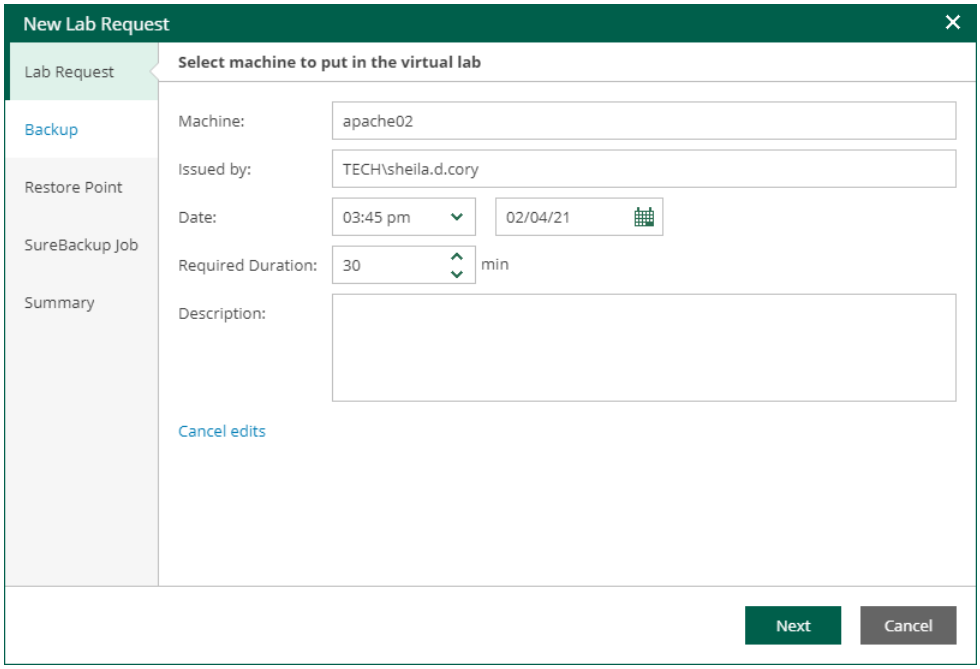
You can create a Virtual Lab request for VMs from the following sources:

- VM backups
- VM replicas
- Storage snapshots

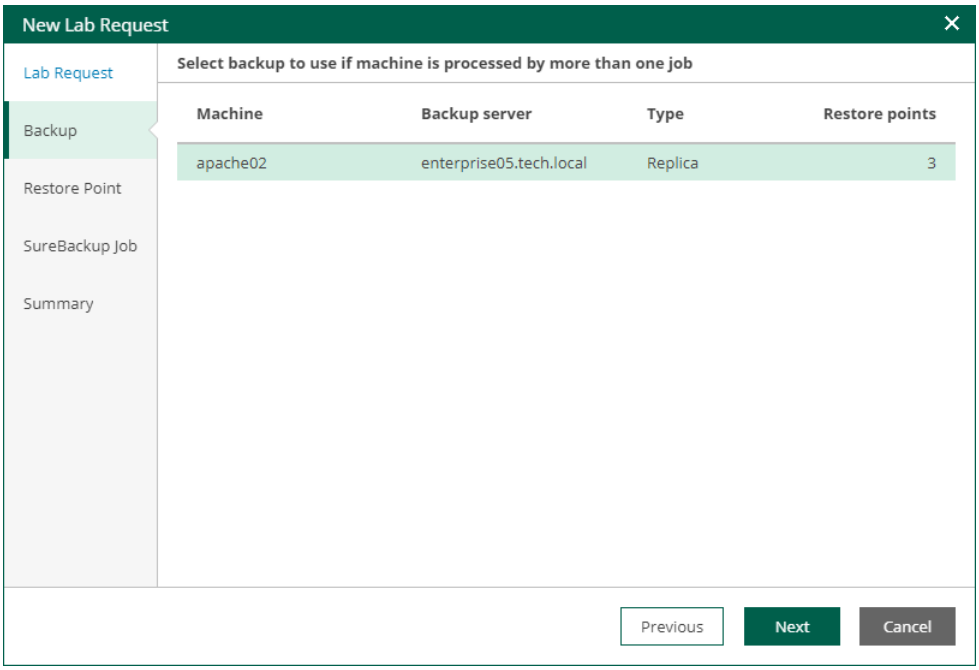
To create a Virtual Lab request:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Go to the **Requests** tab.
3. To open the **New Lab Request** wizard, click the **Create** link in the top left corner.
4. At the **Lab Request** step of the wizard, specify a name or IP address of the VM you need and other request settings.

   By default, lab usage duration is 30 minutes. If necessary, change this value. Optionally, specify a description for your request.

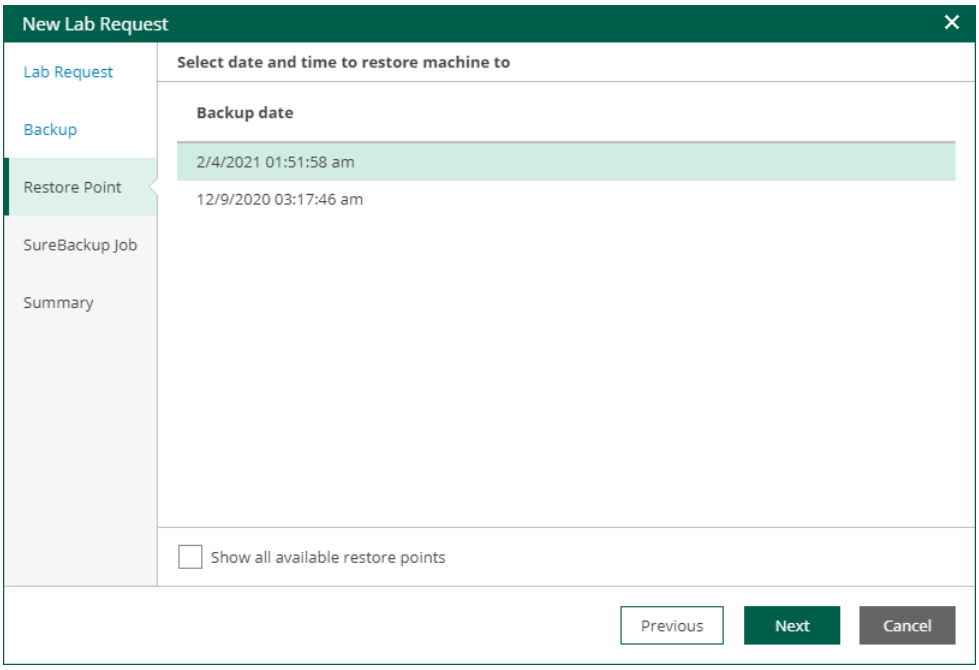


5. At the **Backup** step of the wizard, you can select the backup or replica to restore the VM from (if the VM is included in more than one job).



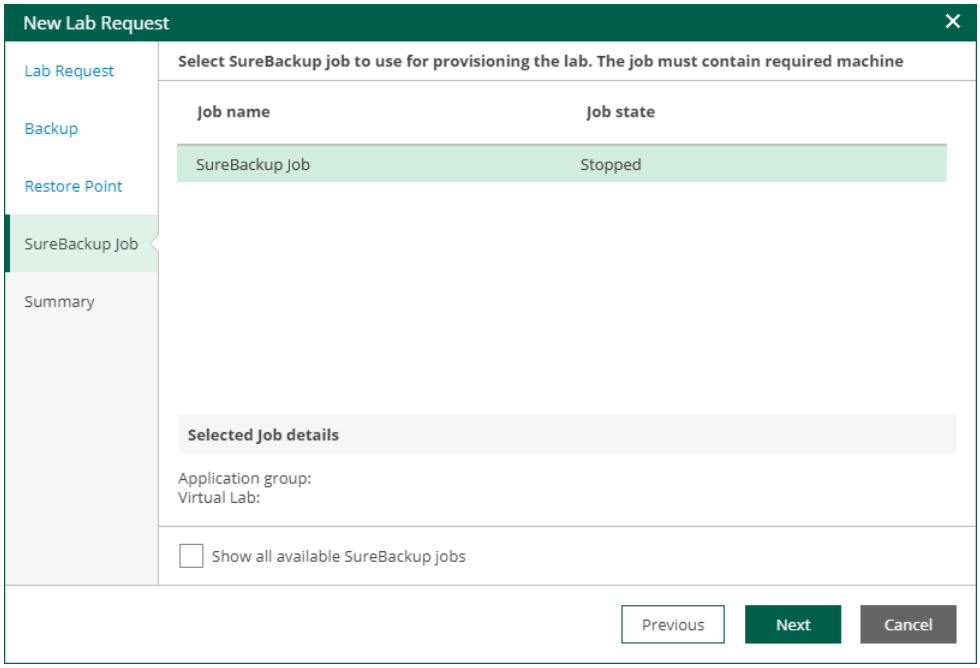
6. At the **Restore Point** step, select the restore point when the application was in the desired state. By default, Enterprise Manager will display restore points closest to the latest backup.

   If you want to display all restore points that are available for the selected backup, select the **Show all available restore points** check box.

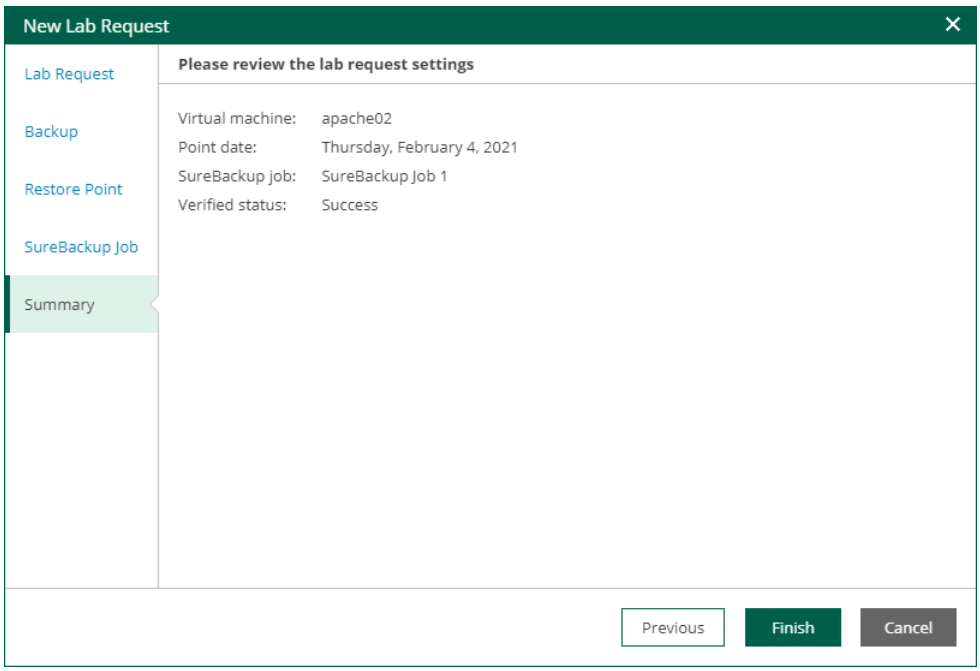


7. At the **SureBackup Job** step, select one of existing SureBackup jobs that you want to run to create an isolated sandbox in which the selected machine should be started. The application group and virtual lab used by this SureBackup job will be displayed in the **Selected Job details** section.

   By default, the list of jobs displays only those jobs that contain the selected machine. If you want to display all SureBackup jobs that were created, select the **Show all available SureBackup jobs** check box.



8. At the **Summary** step, review the settings you have configured for the virtual lab and click **Finish**. Veeam Backup & Replication will perform verification of the selected restore point.



Approving Virtual Lab Requests

When a user submits a request for a virtual lab through Universal Recovery Wizard or Virtual Lab Manager, the request is passed to Enterprise Manager and displayed on the **Requests** tab. Administrators working with Veeam Backup Enterprise Manager can approve submitted lab requests, reject them or prolong the time for which a requested virtual lab should be up.

> **IMPORTANT**
>
> To work with lab requests, the user must have the Portal Administrator role assigned in Veeam Backup Enterprise Manager. For more information, see Configuring Accounts and Roles.

To approve a lab request, select it in the list and click **Approve**. Then follow the **Edit Lab Request** wizard steps:

1. At the **Lab Request** step of the wizard, you can review and, if necessary, edit the virtual lab request (for example, change the time interval for which the lab should be up). To edit virtual lab request data, click the **Edit request** link at the bottom.
2. At the **Backup** step of the wizard, select a backup from which you want to restore items. Enterprise Manager scans all Veeam backup servers connected to it, searches for all backups with the machine specified at the previous step of the wizard, and displays these backups in the list.
3. At the **Restore Point** step of the wizard, select the restore point when the application was in the desired state. The list of restore points is formed depending on the choice the user made when submitting the virtual lab request. For example, if the user selected the **Last Friday night backup** option when creating the request, Enterprise Manager will display restore points created on the last Friday night, and a number of restore points closest to the matching point. If you want to display all restore points that are available for the selected backup, select the **Show all available restore points** check box.
4. At the **SureBackup Job** step of the wizard, select one of existing SureBackup jobs that you want to run to create an isolated sandbox in which the selected machine should be started. The application group and virtual lab used by this SureBackup job will be displayed in the **Selected Job details** section.

   By default, the list of jobs displays only those jobs that contain the selected machine. If you want to display all SureBackup jobs that were created, select the **Show all available SureBackup jobs** check box.
5. At the **Summary** step of the wizard, review the settings you have configured for the virtual lab and click **Finish**. Veeam Backup & Replication will perform verification of the selected restore point.

If the specified SureBackup job is already running, Veeam Backup Enterprise Manager will check the restore point to which machines from the application groups are started. If the point does not correspond to the point selected, Enterprise Manager will display a warning. In this case, you may need to start the SureBackup job to an earlier point in time to make sure the items you need are available there. To do this, open Veeam Backup & Replication console, and right-click the necessary SureBackup job and select **Start job to** from the shortcut menu.

If the SureBackup job is not running, Enterprise Manager will launch the selected SureBackup job, start the virtual lab and run the machine with the necessary application to the restore point selected.

Working with VMware vCloud Director

Veeam Backup Enterprise Manager allows you to perform the following operations with VMware vCloud Director (vCD) objects:

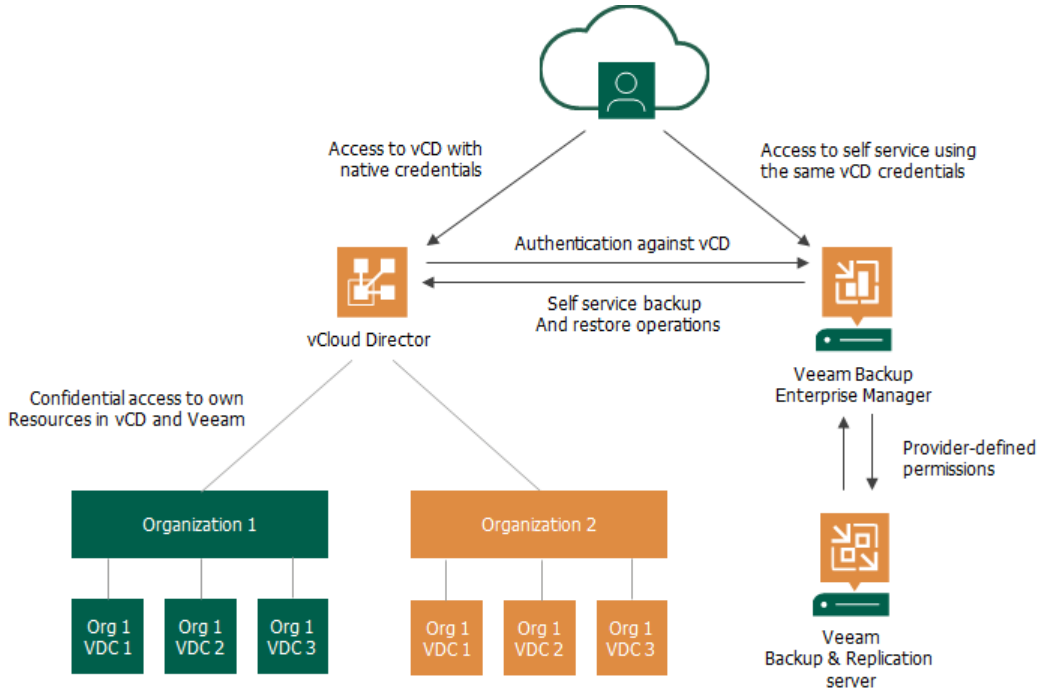
- Back up VMs, vApps and other containers
- Restore VMs and vApps
- Restore VM guest OS files
- Replicate vApps and other containers and fail over to their replicas

vCD service providers can allow self-service restore operations to their customers in the web UI based on Veeam Backup Enterprise Manager.

- Service provider administrators have administrative rights in Veeam Backup Enterprise Manager. Thus, they have access to the **Configuration** view of Enterprise Manager where they can configure vCD organization configurations, including repository quota and backup job template. These administrators typically have access to Veeam Backup & Replication console that controls vCD as part of backup infrastructure on the provider side.
- Members of vCD organizations do not need administrative rights for Veeam Backup Enterprise Manager — instead, they get access to Veeam Self-Service Backup Portal. There they can manage their vCD jobs, as well as restore VMs, files and application items within their scope.

How It Works

Veeam Backup Enterprise Manager uses native vCD authentication to authorize users that log in to Enterprise Manager. The authentication process and components interactions are shown in the figure below.



This approach helps to streamline administration and management tasks for service providers, as now they need to configure a tenant account only once in vCD, and then any change like a new password or a disable operation will be immediately reflected in Veeam Backup Enterprise Manager.

What Service Provider Administrators Can Do

Service provider administrators can perform the following operations:

- Configure settings for their tenants (vCD organizations), including backup job templates to be used, backup destination and repository quota.
- Restrict job scheduling for particular tenants, for example, prevent the jobs from running too often. Administrators can even completely prohibit the tenant's ability to schedule jobs, instead setting the required schedule themselves (manually or using a script).

Together with Veeam built-in load balancing, these capabilities allow administrators to ensure infrastructure is protected from excessive resource consumption.

For more information, see Managing Configurations for vCD Organizations.

What Members of vCD Organizations Can Do

Members of vCD organizations can use their vCD credentials to access Veeam Self-Service Backup Portal. Once they log in, Enterprise Manager identifies the resources included in their scope — the entities the user is allowed to see and manage — and automatically filters vCD objects when displaying them.

Members of vCD organizations can perform the following operations:

- Create new backup jobs for objects in their scope, based on the predefined templates. Organization members are allowed to configure essential job settings (such as VMs to backup, retention, schedule, notifications, and guest OS processing options).
- Modify or delete jobs.
- Enable or disable jobs.
- Start, stop, retry jobs.
- View statistics on vCD backups.
- Restore vCD VMs to the original vApps and vApps to the original vDC.
- Perform application item restore for SQL Server and Oracle databases.
- Restore files from indexed and non-indexed VMs guest file system.

To simplify job management for tenants, advanced job parameters (like backup mode and repository settings) are automatically populated from the job templates. These templates are assigned by the service provider administrator to the particular organization.

Managing Configurations for vCD Organizations

In Veeam Backup Enterprise Manager, users with the Portal Administrator role can manage configurations for vCloud Director (vCD) organizations. Each configuration defines a backup repository that can be used by the organization, repository quota and backup job settings. To specify multiple repositories per organization, add a separate configuration for each repository.

Before you manage vCD organization configurations, check prerequisites.

You can perform the following operations with vCD organizations:

- View the list of organization configurations
- Add a new configuration for a vCD organization
- Edit a vCD organization configuration
- Remove a vCD organization configuration
- Export a configuration report

Before You Begin

You can add configurations for vCD organizations created on multiple vCD servers that are added to the Veeam Backup Enterprise Manager infrastructure.

Before you manage vCD organization configurations, check the following prerequisites:

1. The version of vCD servers must be 9.5 or later.

   For more information on system requirements, see System Requirements.

2. All vCD servers must be added to the backup infrastructure of the same backup server.

   For more information, see the Adding VMware vCloud Director section of the Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > Multiple vCD servers are supported starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261 or later).

3. The backup server that contains the vCD servers in its infrastructure must be connected to Enterprise Manager. Make sure that the version of Veeam Backup & Replication installed on the backup server matches the version of Enterprise Manager.

   For more information, see Managing Backup Servers.

4. Enterprise Manager must complete data collection from the added backup server.

   For more information, see Collecting Data from Backup Servers.

5. The account that you will use to manage vCD organization configurations must be assigned the Portal Administrator role.

   For more information, see Configuring Accounts and Roles.

Managing Multiple vCD Servers

Starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261), you can add vCD organization configurations for multiple vCD servers. In this case, vCD organization members that work with Veeam Self-Service Backup Portal by the portal URL must specify the host of their vCD server when accessing the portal. They can also open the portal from the native vCD environment. For more information, see Accessing Veeam Self-Service Backup Portal.

Members of vCD organizations can access Veeam Self-Service Backup Portal by the following portal URLs:

- Full URL that contains the host address where the necessary vCD server resides:

  ```
  https://<EnterpriseManagerServer>:9443/vcloud/<vCDServer>/<OrgName>
  ```

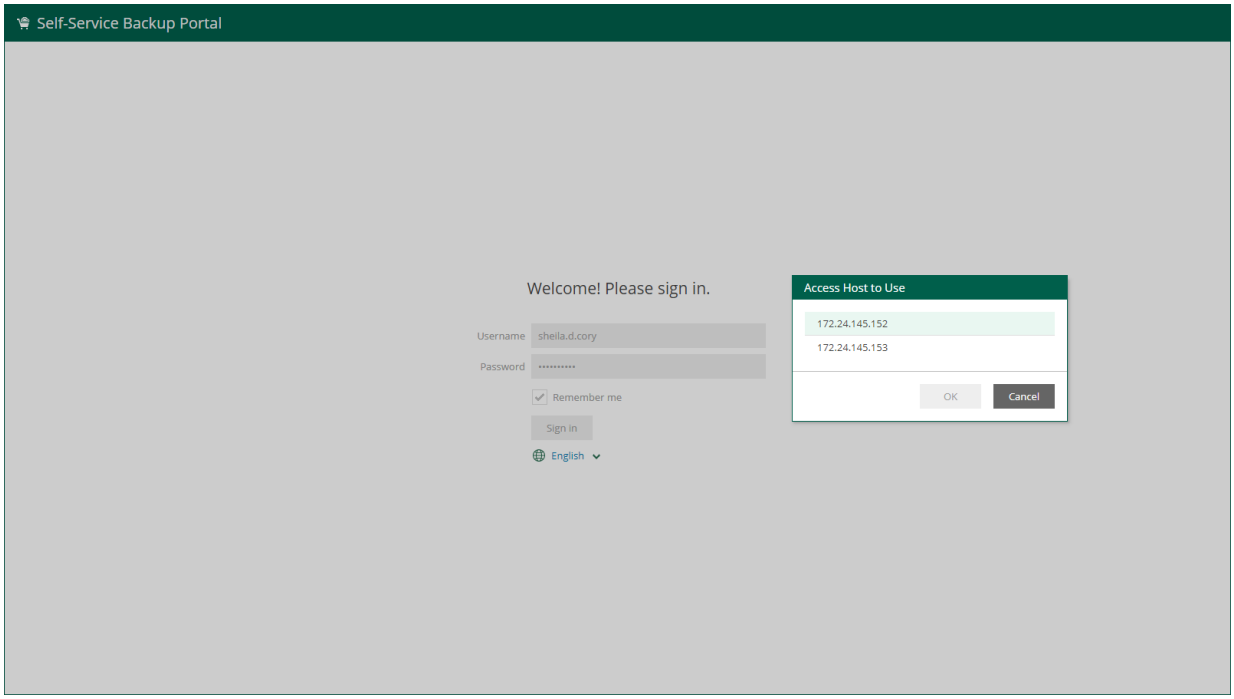
  In this case, Veeam Self-Service Backup Portal will open right after clicking the **Sign in** button.

- Shorter URL that does not contain the host address where the necessary vCD server resides:

```
https://<EnterpriseManagerServer>:9443/vcloud/<OrgName>
```

  In this case, after clicking the **Sign in** button, Veeam Self-Service Backup Portal will prompt to select a vCD host from the list of available vCD hosts.

If you do not want vCD organization members to see addresses of all vCD hosts added to the Enterprise Manager infrastructure, add each vCD server to a separate Enterprise Manager infrastructure.



Viewing Organization Configurations

In Veeam Backup Enterprise Manager, users with the Portal Administrator role can view the list of configurations for vCD organizations.

To view the list of organization configurations:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.

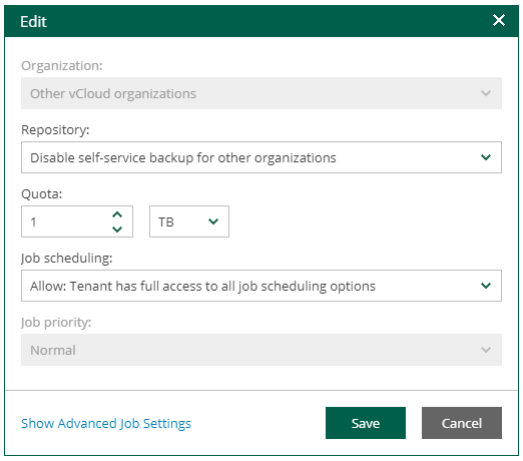
Veeam Backup Enterprise Manager offers a default configuration that you can use for vCD organizations. The configuration is applied to each vCD organization that does not have a specific configuration added for it.

The default configuration contains the following parameters:

- **Organization** – *Other vCloud organizations*
- **Repository** – *Disable self-service backup for other organizations*

  Initially the default configuration is not active. To enable it, select a repository for the configuration.
- **Quota** – *1 TB*
- **Job scheduling** – *Allow: Tenant has full access to all job scheduling*
- **Job priority** – *Normal*

For more information on configuration parameters, see Adding Organization Configuration.



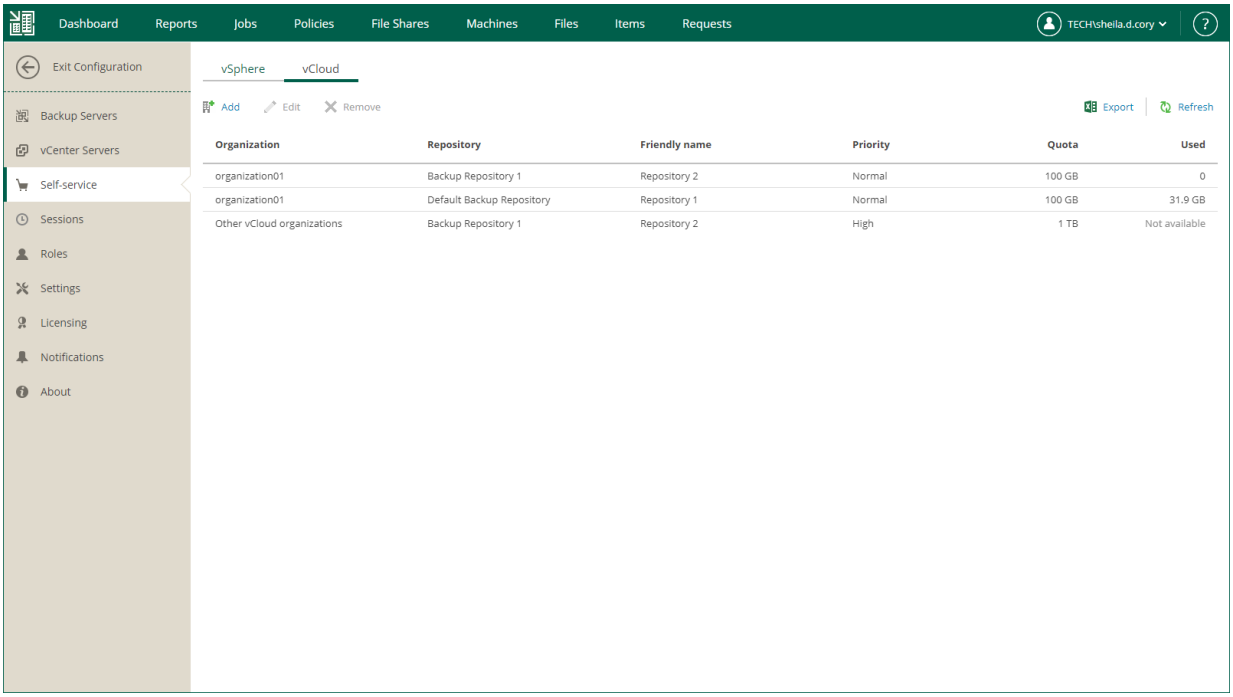
Adding Organization Configuration

Users with the Portal Administrator role can add a new configuration for a vCD organization. Each configuration defines a backup repository that can be used by the organization, repository quota and backup job settings. You can specify multiple repositories per organization. To do this, add a separate configuration for each repository.

Before you add a new configuration, check prerequisites.

To add a new organization configuration:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.



5. To add a new configuration, click **Add**.
6. From the **vCloud Director server** drop-down list, select a vCD server you need.

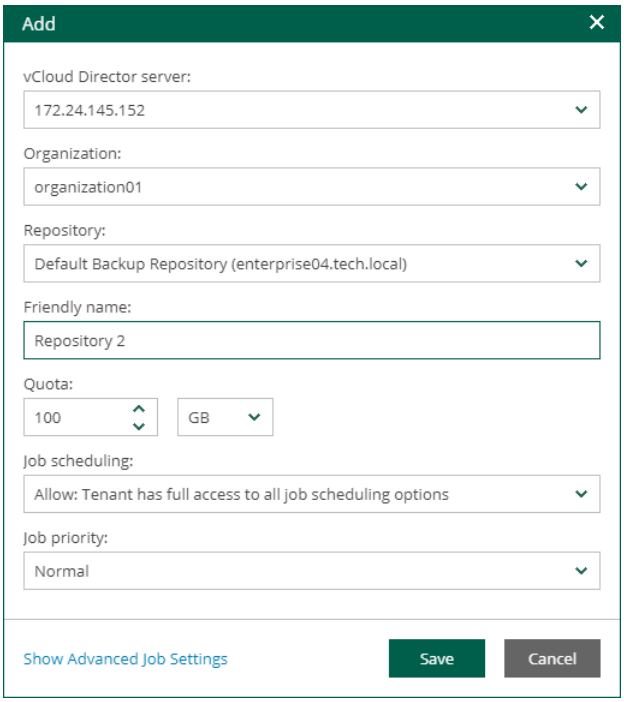
   The field is available if you have multiple vCD servers in the Enterprise Manager infrastructure and if you have Veeam Backup Enterprise Manager 11a (build 11.0.1.1261) installed.
7. From the **Organization** drop-down list, select an organization you need. The list contains organizations from the selected vCD server processed by the backup server that is added to Enterprise Manager.
8. From the **Repository** drop-down list, select a repository that will be used for backups. The list includes repositories configured on the backup server that has the vCD server added to its infrastructure.

   > **IMPORTANT**
   >
   > You cannot assign cloud-based repositories, as well as NetApp or Nimble storage systems storing snapshots created by snapshot-only jobs.
9. In the **Friendly name** field, specify a repository name that will be displayed to organization members.

10. In the **Quota** section, specify a repository storage quota. You can choose GB or TB from the drop-down list and enter the required quantity.
11. From the **Job scheduling** drop-down list, select one of the following options:
    a. *Allow: Tenant has full access to all job scheduling options*
    b. *Allow: Tenant can create daily and monthly jobs only*
    c. *Deny: Creates daily jobs with randomized start time within the backup window*

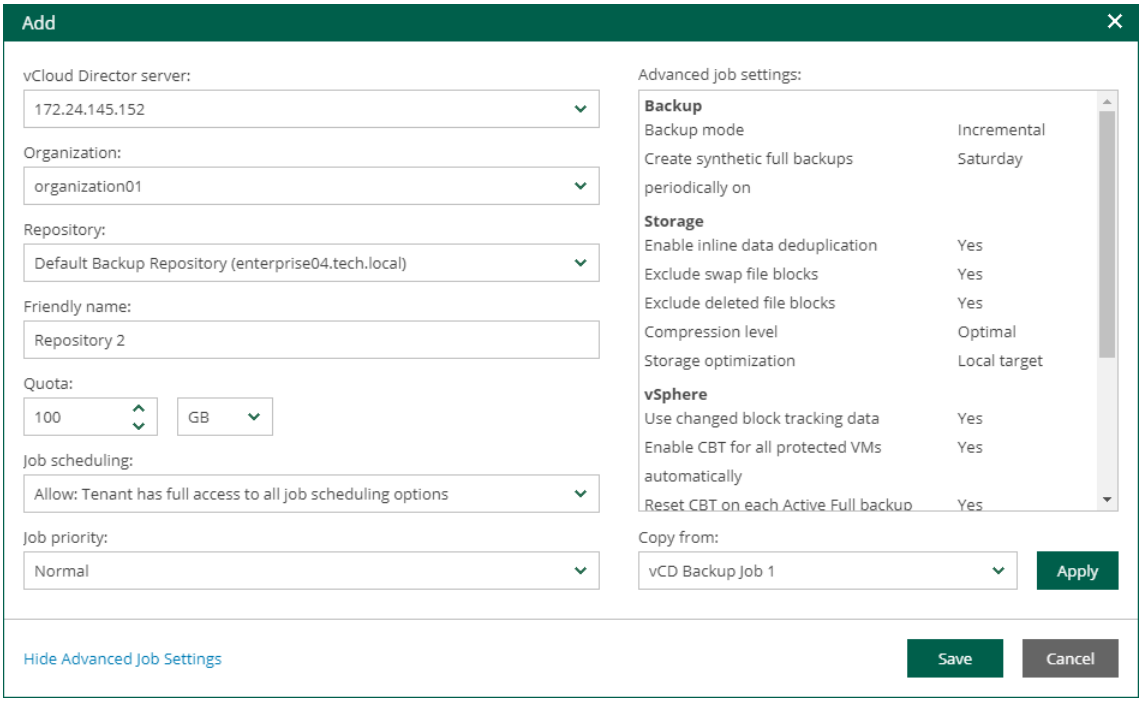
       For backup jobs of vCD organizations, the backup window settings are specified in Veeam Backup Enterprise Manager. Backup window settings specified for the job template that you will select from the advanced job settings do not affect organization jobs. For information on how to specify the backup window in Veeam Backup Enterprise Manager, see Customizing Chart Appearance.
    d. *Deny: Creates job with no schedule assigned*

    For more information on job scheduling, see Edit Job Schedule.



12. To specify what backup job will be used as a job template for the vCD organization:
    a. Click the **Show Advanced Job Settings** link.
    b. From the **Copy from** drop-down list, select backup job settings:
       - *Default job settings* — default vCD backup job settings as they are shown in the Veeam backup console
       - *<Job Name>* — specific vCD backup job configured in Veeam backup console

c. Click **Apply**.



> **IMPORTANT**
>
> The backup repository that is selected from the **Repository** drop-down list for the organization takes priority over the repository used by the selected job template.

13. If you do not use the **Show Advanced Job Settings** link, the default job settings will be applied to the template.

> **NOTE**
>
> To populate the list of job templates, you need at least one vCD backup job to be configured on the backup server.

14. To save the configuration, click **Save**.

Editing Organization Configuration

Users with the Portal Administrator role can edit vCloud Director (vCD) organization configurations.

Before you edit a configuration, consider the following recommendations:

- When you change a job template for a vCD organization, the new configuration will be applied only to the new jobs, existing jobs will not be affected.
- To make an existing backup job to store backups to another repository instead of the currently configured for the organization:

  a. Move already created backups of vCD objects to the new repository.

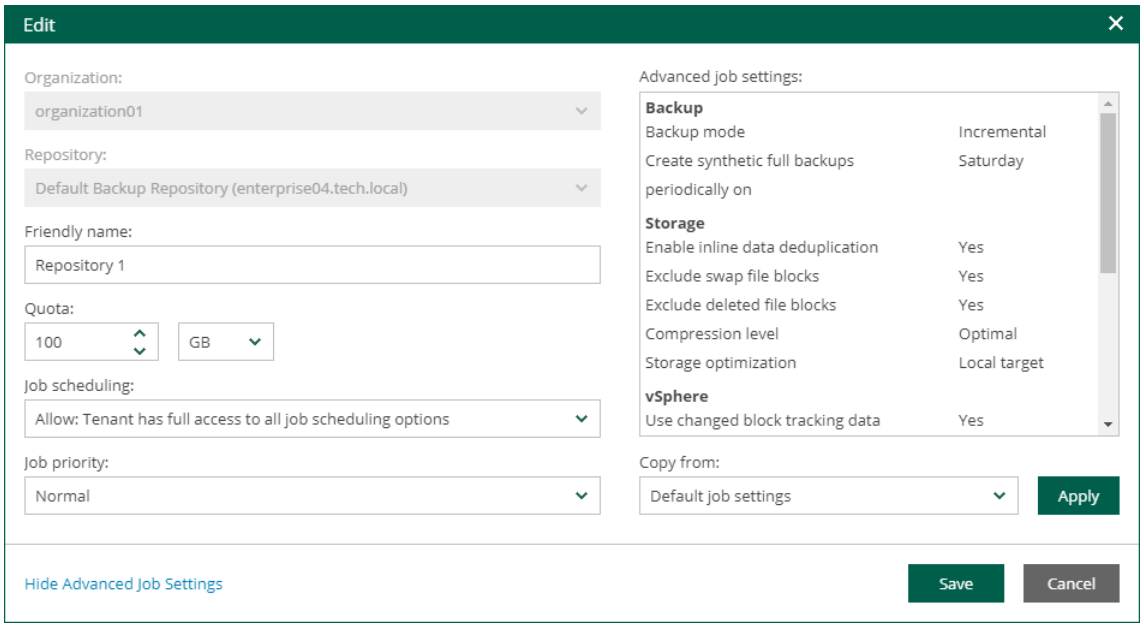
  b. Modify the backup job that is used as a template, and vCD organization configuration so that the job points to the new repository.

  Otherwise, data will be stored to the old repository, exceeding the quota.

To edit an organization configuration:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.
5. On the **vCloud** tab, select an organization configuration and click **Edit**.
6. To edit organization settings, follow the same steps as for adding a configuration.

   For more information, see Adding Organization Configuration.



Removing Organization Configuration

Users with the Portal Administrator role can remove vCloud Director (vCD) organization configurations. The removed configuration is still effective for the jobs created with this configuration. New vCD backup jobs created after this removal will use the default configuration until you add a new configuration for the organization.

To remove an organization configuration.

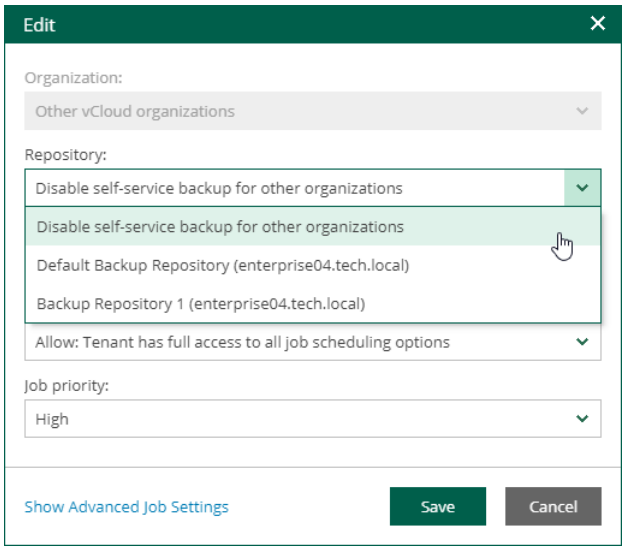
1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.
5. On the **vCloud** tab, select a configuration and click **Remove**.

Disabling Default Configuration

The default configuration cannot be removed from the list — instead, you can disable it.

To disable the default configuration:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.
5. On the **vCloud** tab, select the default organization configuration and click **Edit**.
6. From the **Repository** drop-down list, select *Disable self-service backup for other organizations*.

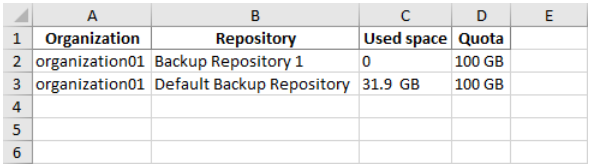


Exporting Configuration Report

Users with the Portal Administrator role can export a report with a list of configurations that were created for vCD organizations. The list does not include the default configuration. When you export the report, it is saved as an XLSX file.

To export a configuration report:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.
5. On the **vCloud** tab, click **Export**.



	A	B	C	D	E
1	**Organization**	**Repository**	**Used space**	**Quota**	
2	organization01	Backup Repository 1	0	100 GB	
3	organization01	Default Backup Repository	31.9 GB	100 GB	
4					
5					
6					

Veeam Self-Service Backup Portal

Veeam Self-Service Backup Portal is a web-based portal that provides members of vCloud Director (vCD) organizations with self-service operations for vCD VMs protection, including VM and file restore. These operations do not require to create specific user accounts or assign specific roles to them at the Veeam Backup Enterprise Manager level. The organization members access Veeam Self-Service Backup Portal with their native vCD credentials.

Required Permissions

Members of vCD organization can use Veeam Self-Service Backup Portal to backup and restore resources of their vCD organization. To authenticate users, Veeam Self-Service Backup Portal uses LDAP and local user authentication. SAML authentication is also supported if you access Veeam Self-Service Backup Portal from the vCD UI using Veeam Plug-in for VMware vCloud Director. For more information, see Accessing Veeam Self-Service Backup Portal.

The following organization members have access to Veeam Self-Service Backup Portal:

- vCD organization administrators.
- vCD organization members with the following rights granted in VMware vCloud Director:
  - *General: Administrator Control*
  - *General: Administrator View*
  - *Group / User: View*
- Any vCD organization members whose roles (or associated LDAP user roles) are defined in registry keys and with the *Group / User: View* right granted in VMware vCloud Director. For more information, contact Veeam Customer Support.

> **NOTE**
>
> vCD system administrators cannot access Veeam Self-Service Backup Portal since they are not vCD organization members.

Accessing Veeam Self-Service Backup Portal

Members of vCloud Director (vCD) organizations can access Veeam Self-Service Backup Portal in the following ways:

- Access by URL
- Access from vCD

For more information on access rights, see Required Permissions.

Accessing Veeam Self-Service Backup Portal by URL

To access Veeam Self-Service Backup Portal by URL:

1. Open your web browser and enter the following URL in the address bar:

   ```
   https://<EnterpriseManagerServer>:9443/vcloud/<vCDServer>/<OrgName>
   ```

   where:

   - `<EnterpriseManagerServer>` is a host name or IP address of the host where the Enterprise Manager server resides.
   - `<vCDServer>` is a host name or IP address of the host where the vCD server resides.

     This URL part is optional. If you do not specify a vCD host here, you may be asked to select the host when you log in to the portal.
   - `<OrgName>` is a name of the vCD organization.

   For example:

   ```
   https://vbr-em:9443/vcloud/172.17.53.16/TechCompanyOrg
   ```

2. From the drop-down list, select a display language.

   For more information on display languages, see Managing Languages.

   > **NOTE**
   >
   > You can select a display language for the portal if Veeam Backup Enterprise Manager 11a (build 11.0.1.1261 or later) is installed on the Enterprise Manager server.

3. In the **Username** and **Password** fields, specify credentials of a vCD account with proper rights.
4. To save the entered credentials for future access, select the **Remember me** check box.
5. Click **Sign in**.
6. From the list of hosts with vCD servers, select the one where your organization has been created.

   The list of hosts is displayed if multiple vCD servers are added to the Enterprise Manager infrastructure.

Accessing Veeam Self-Service Backup Portal from vCD

In the vCD environment, Veeam Self-Service Backup Portal is displayed in English by default. Starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261), when you access the portal by its URL, you can select a preferred language from the drop-down list on the login page. After you select the language here, you can work with the portal in the selected language from the vCD environment. For more information, see Accessing Veeam Self-Service Backup Portal by URL.

Before members of vCD organizations can access Veeam Self-Service Backup Portal from the vCD UI, the vCD system administrator must upload and configure Veeam Plug-in for VMware vCloud Director. For more information, see Uploading and Configuring Veeam Plug-in for VMware vCloud Director.

To access Veeam Self-Service Backup Portal from vCD:

1. Log in to vCloud Director Tenant Portal under a vCD account with proper rights.
2. From the **More** menu, select **Data Protection with Veeam**.

   If you have a connection error when accessing Veeam Plug-in for VMware vCloud Director, add the Veeam Backup Enterprise Manager certificate as trusted to your browser.

Uploading and Configuring Veeam Plug-in for VMware vCloud Director

Veeam Plug-in for VMware vCloud Director lets members of vCloud Director (vCD) organizations access Veeam Self-Service Backup Portal in the native vCD environment.

You can upload and configure Veeam Plug-in for VMware vCloud Director on vCloud Director Service Provider Admin Portal using a vCD system administrator account. When you upload the plug-in, you specify the scope — a set of vCD organizations that can use the plug-in.

If you need to modify the scope of vCD organizations after you configure the plug-in, update the plug-in configuration. For more information, see Updating Plug-in Configuration

Before You Begin

Before you start uploading Veeam Plug-in for VMware vCloud Director, check the following prerequisites:

- Veeam Plug-in for VMware vCloud Director requires Veeam Backup & Replication 11 or later to be installed on the backup server that has the vCD server in its infrastructure.
- Users of the plug-in must have access to the Veeam Backup Enterprise Manager and vCloud Director URLs.
- The Veeam Backup Enterprise Manager server should use a certificate issued by a Certificate Authority instead of a default self-signed certificate. In case of a self-signed certificate, users of the plug-in have to add the Enterprise Manager certificate as trusted to their browser before they access the plug-in. Otherwise, they will get a connection error.

  For more information on the Enterprise Manager certificate, see Updating Security Certificate.

Uploading and Configuring Plug-in

To upload and configure Veeam Plug-in for VMware vCloud Director:

1. Log in to vCloud Director Service Provider Admin Portal under a vCD system administrator account.

2. Upload Veeam Plug-in for VMware vCloud Director to the portal. You can find the plug-in file in the ISO installation image of Veeam Backup & Replication.

   For more information, see the Upload a Plug-in section of VMware vCloud Director documentation.

3. From the **More** menu, select **Data Protection with Veeam**.

   If the **Data Protection with Veeam** option is not available, log out from the vCloud Director Service Provider Admin Portal and log in again.

4. In the **Plug-in Configuration** section, specify the URL to the Veeam Backup Enterprise Manager website and click **Save**.

   > **NOTE**
   >
   > When you save the plug-in configuration, it is applied to all vCD organizations. For that, a separate operation is performed for each organization. If you have operation limits that are set through the vCloud Director API, the operations may fail with HTTP status 400.
   >
   > In this case, use the vCloud Director API to set the *QueuedOperationsPerOrg* and *QueuedOperationsPerUser* elements to zero until you save the plug-in configuration. For more information, see the OperationLimitsSettingsType section of VMware vCloud Director API documentation.

5. On the Enterprise Manager server in IIS Manager, recycle the VeeamBackup application pool.

   For more information, see the Recycling Settings for an Application Pool <recycling> section of Microsoft Docs.

Updating Plug-in Configuration

You can modify the scope of vCD organizations after you configure the plug-in. It may be useful, for example, if you create a new vCD organization and you want members of this organization to use the plug-in. To include or exclude vCD organizations, update the plug-in configuration.

To update the plug-in configuration:

1. Log in to vCloud Director Service Provider Admin Portal under a vCD system administrator account.
2. Modify the scope of vCD organizations.

   For more information, see the Publish or Unpublish a Plug-in from an Organization section of VMware vCloud Director documentation.

3. From the **More** menu, select **Data Protection with Veeam**.
4. In the **Plug-in Configuration** section, click **Save** to apply the changes to all vCD organizations.

Working with Veeam Self-Service Backup Portal

In Veeam Self-Service Backup Portal, members of vCD organizations can perform the following operations:

- On the Dashboard tab — view statistics on vCD backups.
- On the Jobs tab — examine and export job sessions data, search for jobs, create new jobs and edit jobs.
- On the VMs tab — search by a VM name, restore VMs and vApps to their original location (preserving or overwriting the production VM or vApp), and delete VM backups.
- On the Files tab — search for the files on the VM guest file system and restore the necessary files to the original location or download to the local machine.
- On the Items tab — perform application item-level restore (currently, for Microsoft SQL Server and Oracle databases).

Viewing Statistics on vCD Backups

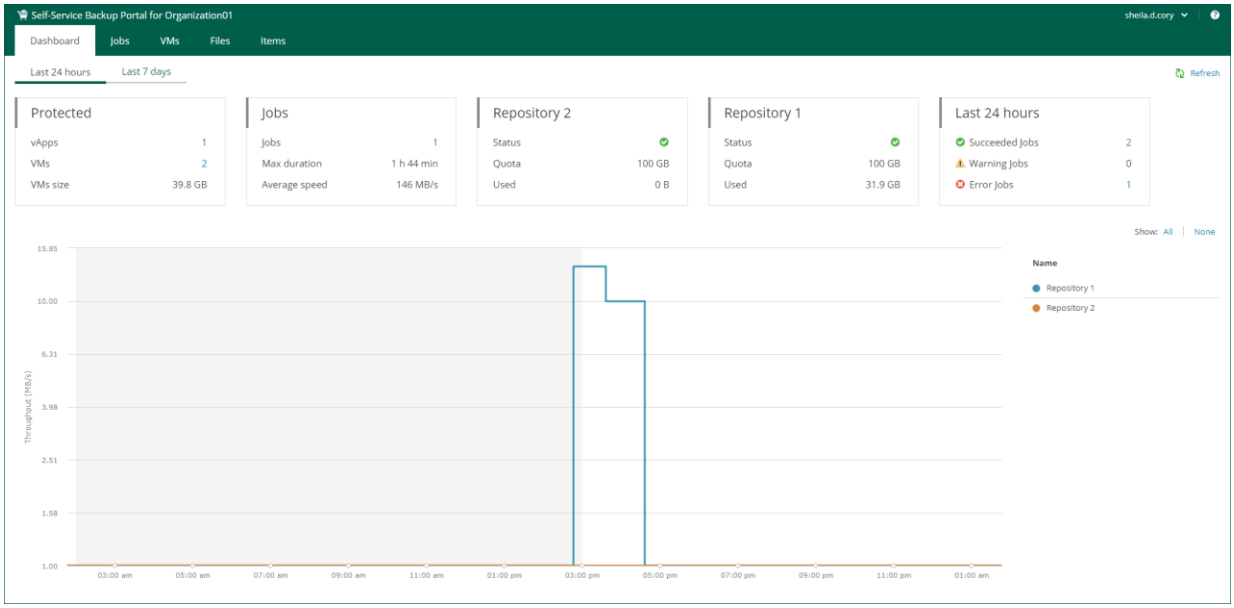
The **Dashboard** tab contains statistics on vCD backup jobs created by members of the vCD organization, including information on the VMs, job runs and backup repositories.

You can view the chart for one of the time ranges:

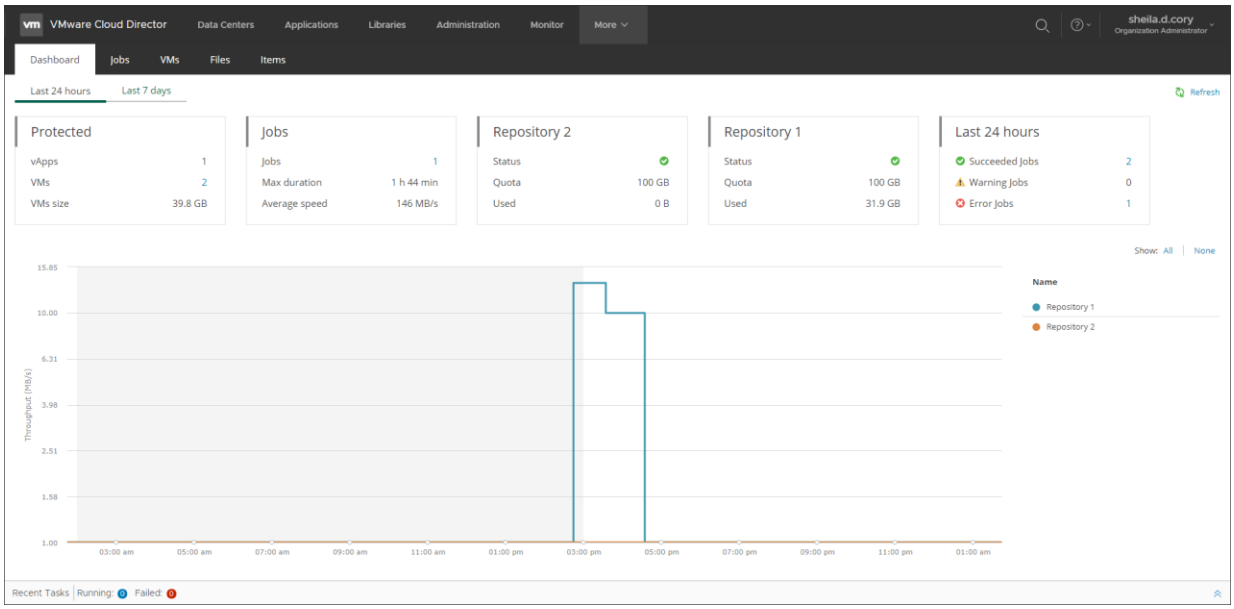
- Last 24 hours
- Last 7 days

To switch between the ranges, select a necessary tab in the top left corner.

Veeam Self-Service Backup Portal accessed by URL



Veeam Self-Service Backup Portal accessed from vCD using Veeam Plug-in for VMware vCloud Director



The **Protected** widget contains the following information:

- *vApps* — the number of vApps for which restore points were successfully created during the specified period
- *VMs* — the number of VMs for which restore points were successfully created during the specified period
- *VMs size* — total size of source VMs successfully processed

The **Jobs** widget contains the following information:

- *Jobs* — the number of jobs created by currently logged in administrator
- *Max duration* — maximum job duration
- *Average speed* — average data transfer speed

The **Backup Storage / <Repository name>** widgets display statistics about backup repositories available to the organization. Each widget represents a single repository and contains the following information:

- *Status* — a status of the backup repository assigned to the organization:
  - *Green* — more than 10% of storage space is free
  - *Yellow* — less than 10% of storage space is free
  - *Red* — no free space on backup storage
- *Quota* — storage quota
- *Used* — used storage size

The **Last 24 hours / Last 7 days** widget reports on the job session results for the selected period.

To visualize on-going jobs data, the **Dashboard** tab also comprises a chart showing date and time when jobs were performed, and the network throughput rate during the job.

> **NOTE**
>
> The dashboard displays only vCD backup jobs of the current vCD organization.

The highlighted part of the chart represents the configured backup window if this option is specified in the chart settings. For more information, see Customizing Chart Appearance.

Managing vCD Backup Jobs

On the **Jobs** tab, members of the vCD organization can perform the following operations with vCD backup jobs:

- Create a new vCD backup job
- Start, stop or retry a job
- Disable or enable a job
- Edit a job

Creating vCD Backup Jobs

To create a new vCD backup job:

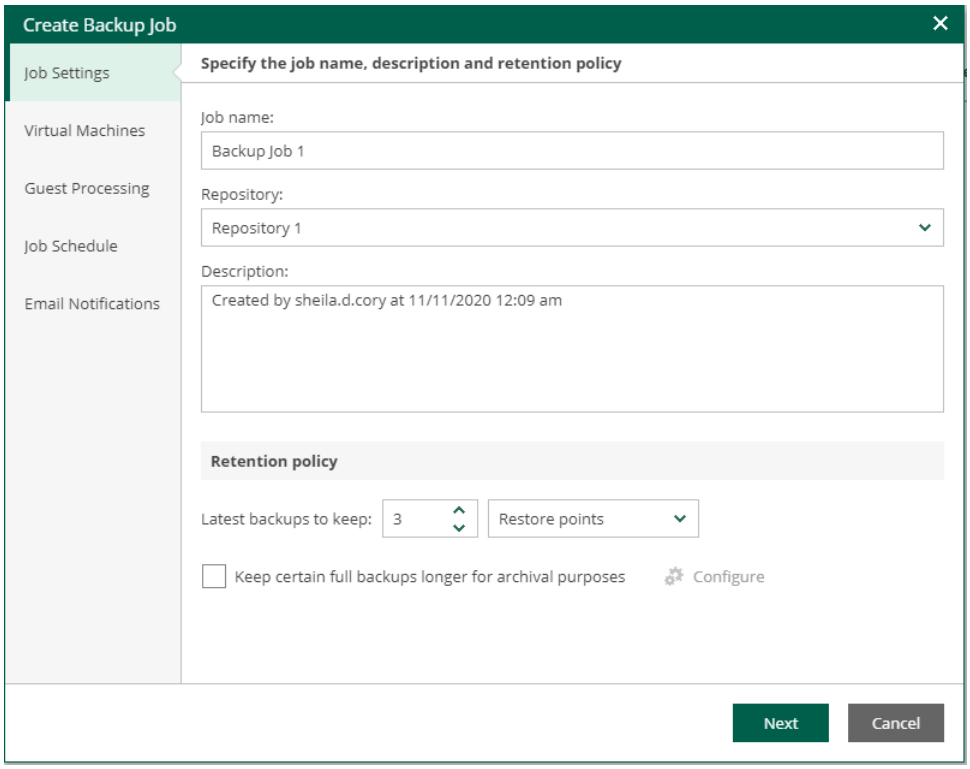
1. Log in to the portal under a vCD account with proper rights.

   For more information on user rights, see Required Permissions.

2. On the **Jobs** tab, click **Create**.
3. At the **Job Settings** step, specify a job name, repository, job description and retention policy.

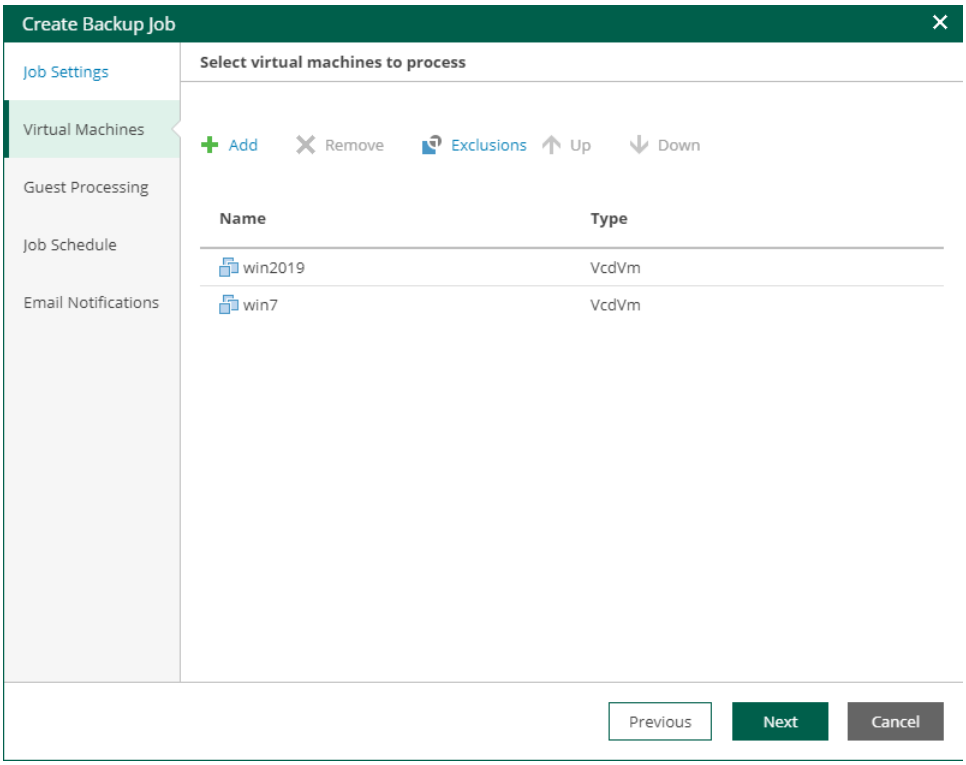
   For more information, see Edit Job Name and Retention Settings.

   > **NOTE**
   >
   > You can select a repository only if more than one configuration is added for the organization. For more information, see Adding Organization Configuration.



4. At the **Virtual Machines** step, add VMs, vApps and vDCs of the organization, and define their processing order.

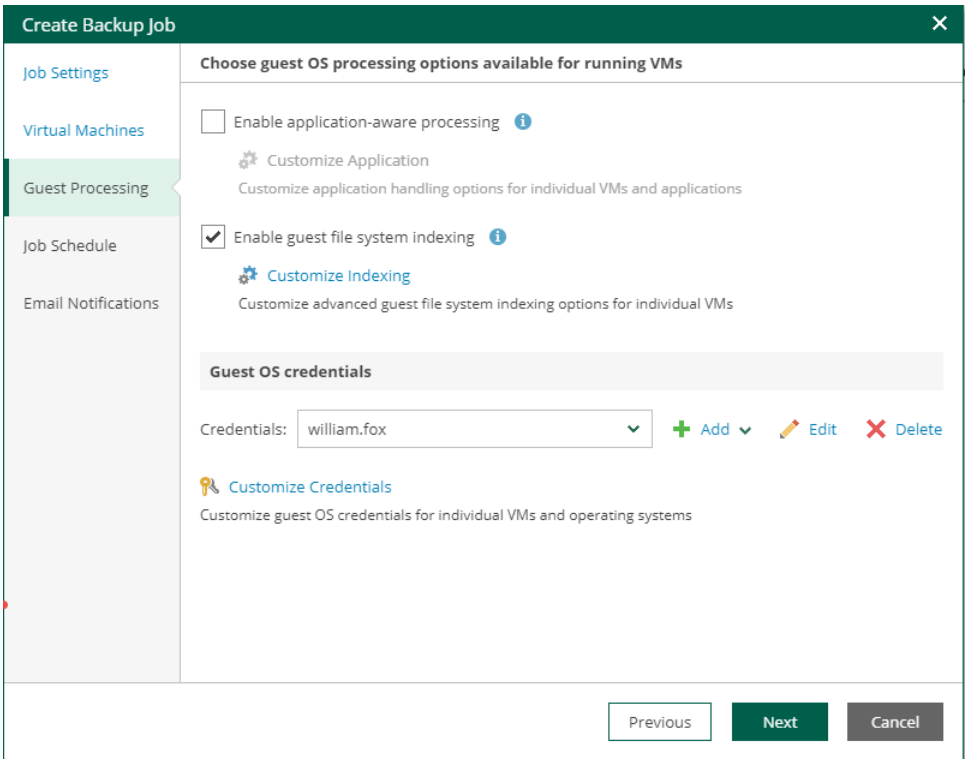
   For more information, see Edit List of Virtual Machines and Change VM Processing Order.



5. At the **Guest Processing** step, you can configure transactionally consistent backup, transaction log handling settings, and enable guest file system indexing.

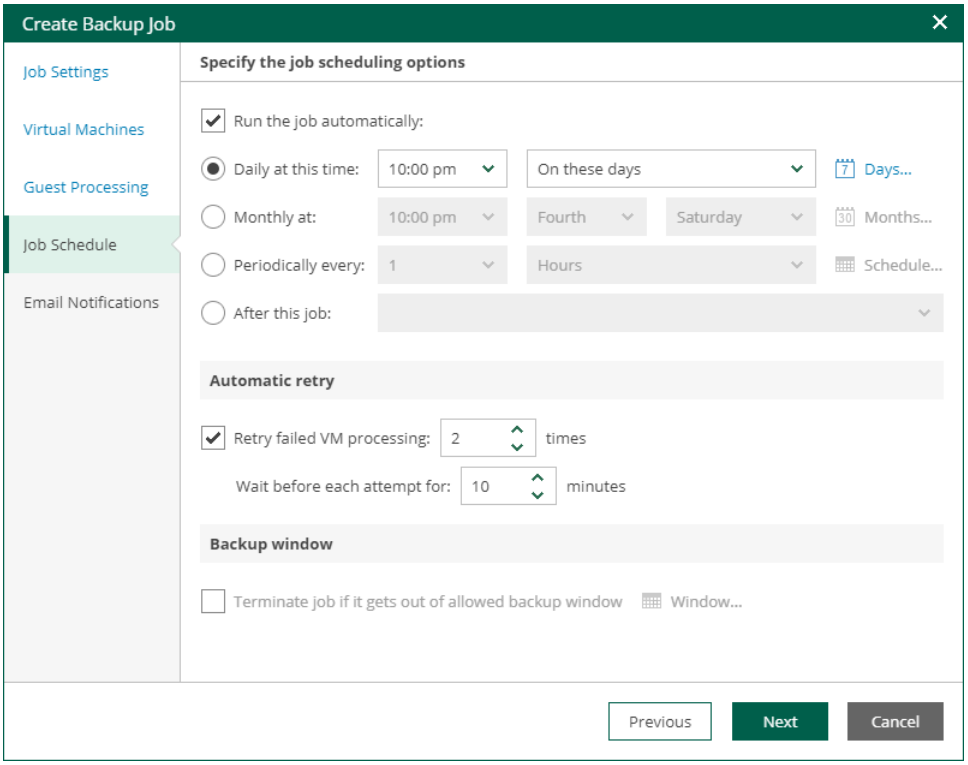
   For more information, see Configure Guest Processing Settings.

> **NOTE**
>
> vCD system administrators can access guest OS credentials available for their organizations. They can also supply new credentials for guest OS processing.



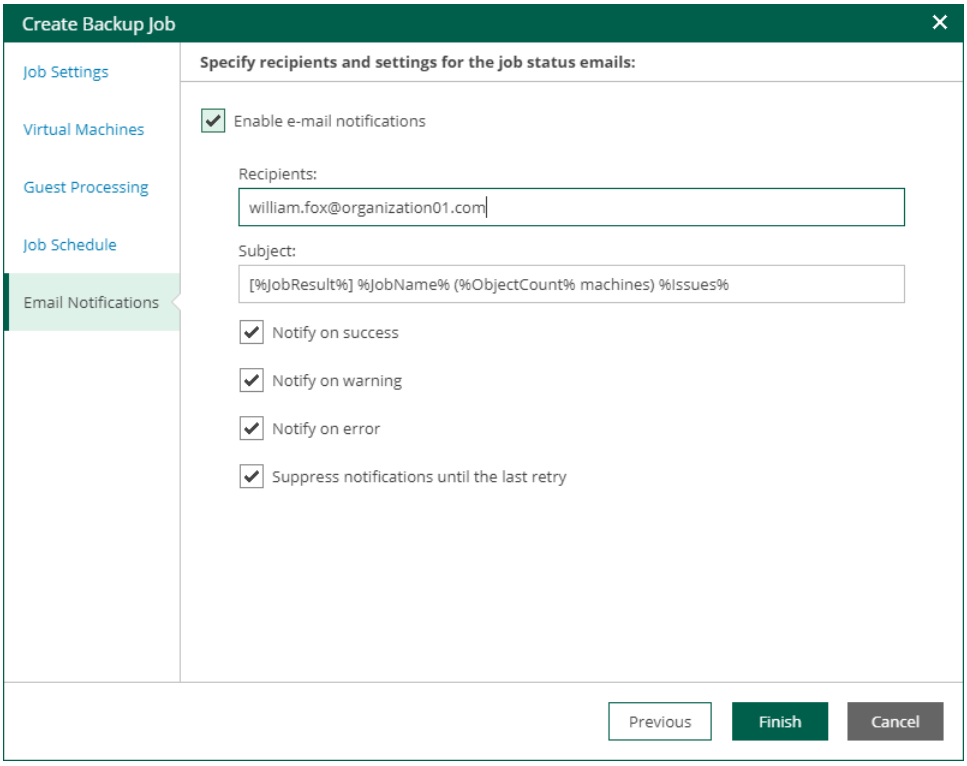
6. At the **Job Schedule** step, you can specify job scheduling options.

   For more information, see Edit Job Schedule.



7. At the **Email Notifications** step, configure notifications as required.

   For more information, see the Notification Settings section of the Veeam Backup & Replication User Guide.



8. To create a job, click **Finish**.

   Remaining settings are obtained from the job configuration specified for the organization. For more information, see Adding Organization Configuration.

The jobs you create are shown in Veeam Backup & Replication console under the **Jobs** node and in Veeam Backup Enterprise Manager on the **Jobs** tab. The jobs have the *<vCloud Director_org_name>* prefix.

> **NOTE**
>
> Organization members cannot see the jobs with VMs from their vCD organization if the jobs are created using Veeam Backup & Replication. To view these jobs, tenants can map their organization jobs using a PowerShell command. For more information, see the Set-VBRvCloudOrganizationJobMapping section of the Veeam Backup & Replication PowerShell Reference. Tenants can map jobs of their own organization only.

Managing vCD Backup Jobs

You can perform management actions with vCD backup jobs as described in the procedures for ordinary jobs in Veeam Backup Enterprise Manager:

- Starting, stopping and retrying jobs
- Enabling and disabling jobs
- Editing job settings

To delete a job, select it on the **Jobs** tab and then on the toolbar click **Job > Delete**. After deletion, this job will be removed and no longer appear in the web portal, Veeam Backup & Replication console and in Veeam Backup Enterprise Manager.

Considerations and Limitations

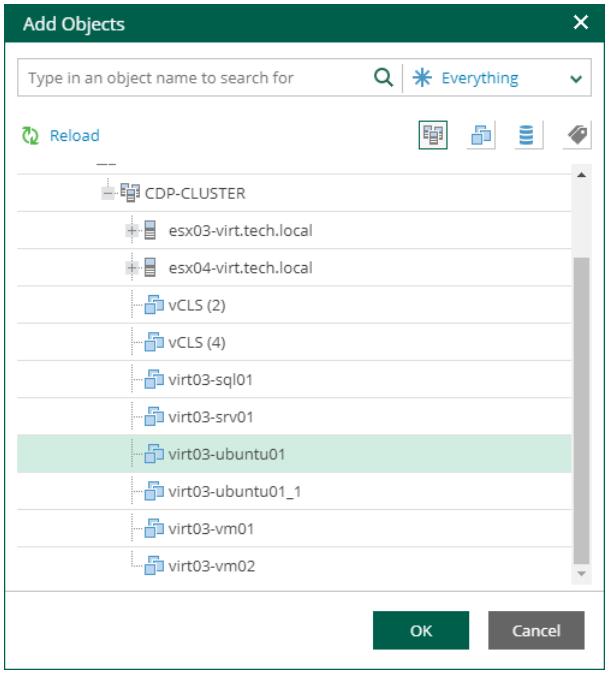
- Job cloning is not available.
- The following limitations apply to scenario involving VM backup and subsequent restore using Veeam Self-Service Backup Portal:

  a. You create a backup job that will process a VM added explicitly (that is, not as a part of a vApp container).

  b. This job runs creating a number of restore points.

  c. Then you restore this VM to the original location by using the portal.

  After restore, the VM identifier changes in vCD hierarchy. Due to this reason, the backup job cannot locate this VM any longer. So, you need to edit job settings, adding this VM anew. To ensure that job configuration will store this VM with the new metadata (not the old one from vCD hierarchy cache), you should first click **Reload** in the **Add Objects** window.



  d. At the next job run, a new full backup will be created for this VM. However, if you try to perform file-level restore with the portal from the restore points created initially for that VM (on step 2), the restore operation will fail, as that VM identifier does not exist any longer.

Managing vCD VMs and vApps

On the **VMs** tab, members of the vCD organization can perform the following tasks:

- Browse VMs and vApps
- Restore VMs
- Restore vApps
- Restore VM disks
- Delete VMs and vApps from Backups

Restoring VMs

You can restore vCD VMs to the original (production) vApp.

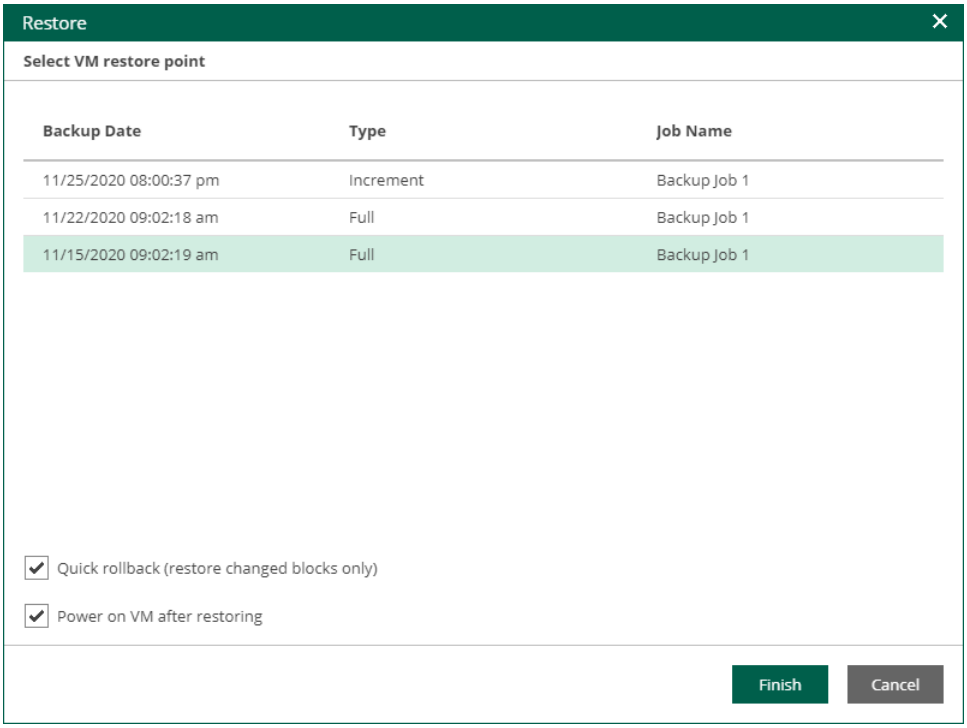
To restore a VM:

1. On the **VMs** tab, select the necessary VM backup in the list of VMs. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Restore VM** and select the option you need:
   - Select **Overwrite** to restore the VM from the backup to the original vApp, replacing the production VM.

     In this case, the restored VM hard disks are assigned the storage policies of the original VM hard disks.
   - Select **Keep** to keep both VMs in the original vApp. The VM from the backup will be located next to the original production VM and will have the same name with the *_restored* suffix.

     In this case, the restored VM hard disks are assigned the storage policy of the VM.
3. Select the restore point that will be used to restore the VM.
4. [Optional] Instead of restoring an entire machine from a backup file, you can instruct Enterprise Manager to recover only those data blocks that are necessary to revert the machine to the selected restore point. To do this, select the **Quick rollback** check box. Quick rollback significantly reduces the recovery time and has little impact on the production environment.

   For more information on quick rollback, see the Quick Rollback section of the Veeam Backup & Replication User Guide.
5. [Optional] To start a machine immediately after recovery, select the **Power on machine after restoring** check box.



6. Click **Finish**.
7. Click **Yes** in the message window to confirm the operation.

To view the VM restore progress, on the **Machines** tab, click **History**.

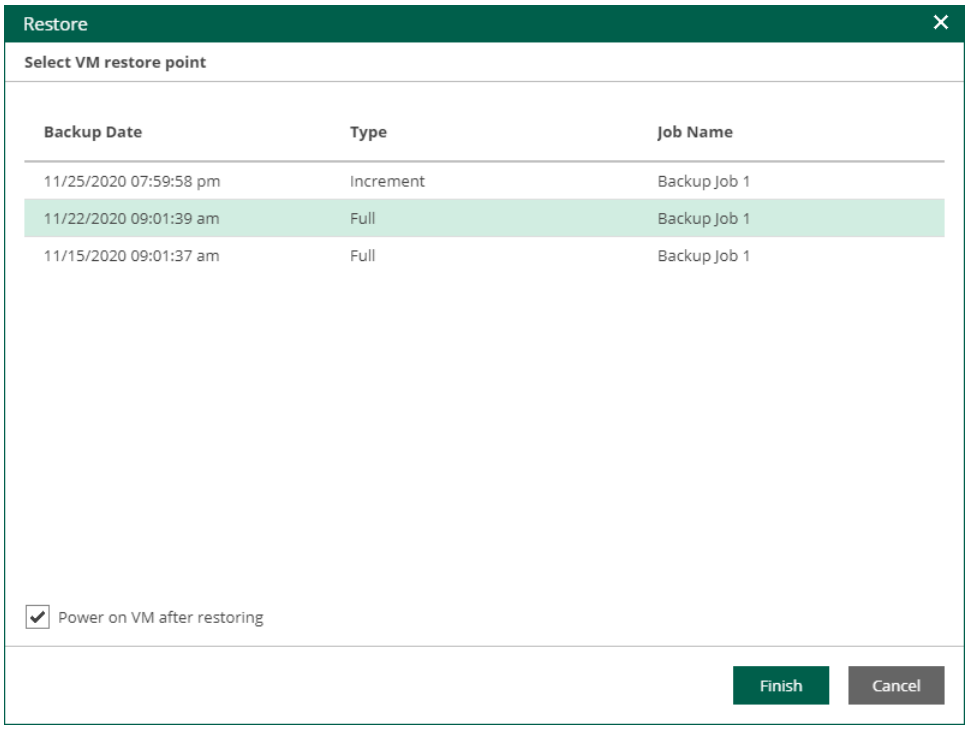
> **IMPORTANT**
>
> Restore of a standalone VM to the original location with the **Keep** option selected results in an unpredictable behavior and possible failure of the restore job.

Restoring vApps

You can restore a vApp to the original vDC.

To restore a vApp:

1. On the **VMs** tab, select a vApp. To quickly find the necessary vApp, use the search field at the top of the window.
2. Click **Restore vApp** and select the option you need:
   - Select **Overwrite** if you want to restore the vApp from the backup to the original vDC, replacing the production vApp.
   - Select **Keep** if you want to keep the original vApp in the original vDC. The vApp from the backup will be located next to the original production vApp and will have the same name with the *_restored* suffix. Names of VMs in the vApp will remain the same.
3. Select the restore point that will be used to restore the vApp.
4. [Optional] To start VMs in the restored vApp immediately after recovery, select **Power on VM after restoring**.



5. Click **Finish**.
6. Click **Yes** in the message window to confirm the operation.

To view the VM restore progress, on the **Machines** tab, click **History**.

IMPORTANT

Restore job of a vApp with a standalone VM will return an ordinary and not standalone VM.

Restoring Virtual Disks

You can restore individual virtual disks from backups of vCloud Director VMs.

To restore a virtual disk:

1. On the **VMs** tab, select a VM with disks you want to restore. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Virtual Disks**.
3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Performing Virtual Disk Restore.

Deleting VMs and vApps from Backups

You can delete a VM from the vApp. If the selected VM is the last one in its vApp, the VM will be deleted from the backup with its vApp. If this vApp is the last one in its backup, the whole backup will be deleted.

If you delete a VM that has GFS backups, they will not be deleted. You can delete them in Veeam Backup Enterprise Manager. For more information, see Deleting Machine from Backups.

To delete a VM:

1. On the **VMs** tab, select a VM. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Delete**.
3. Click **Yes** to confirm the deletion.

When you remove data for deleted VMs from per-VM backup chains, it does not mark the space as available but deletes backup files since they contain data for one VM only.

When you remove data for deleted VMs from regular backup chains, the space is not freed up on the backup repository. It is marked as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.

Restoring Guest OS Files

On the **Files** tab, members of the vCD organization can browse the guest OS file system in a VM backup, search for guest OS files and restore necessary files. You can restore files from indexed and non-indexed guest OS file systems.

To restore guest OS files, follow the steps described in Performing 1-Click File Restore.

NOTE

- When you restore from non-indexed guest OS file system, mount operation is performed using mount server associated with the backup repository that stores the backup file.
- Before you restore files from a non-Windows VM, make sure that an FLR helper appliance is configured on the backup server. For more information, see Preparing for File Search and Restore (non-Windows machines).

Restoring Application Items

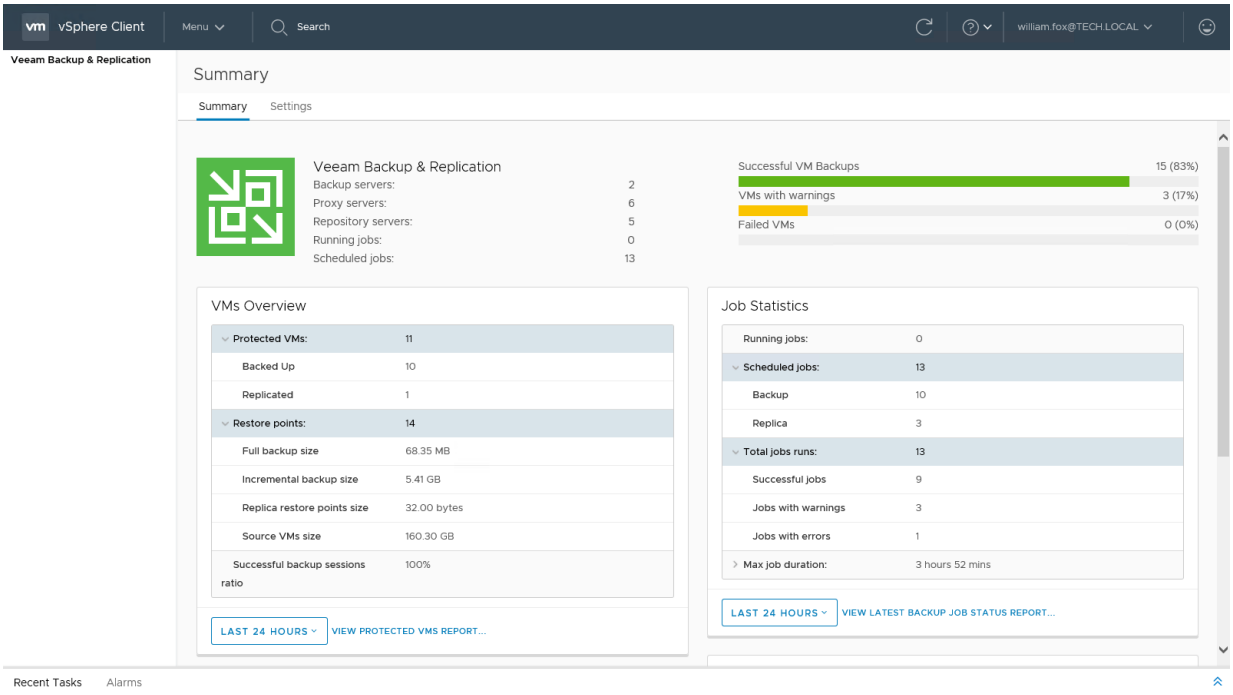
On the **Items** tab, members of the vCD organization can perform item-level recovery of SQL Server databases and Oracle databases from application-aware backups.

To restore application items, open the **Items** tab and follow the steps described in the Restore Procedure for SQL Server databases and Restore Procedure for Oracle databases.

Information on these restore operations will be available in the Delegated Restore Permissions Overview report from the Veeam Backup Overview report pack available in Veeam ONE.

Controlling Backup Infrastructure with vSphere Web Client Plug-in

The vSphere Web Client plug-in for Veeam Backup & Replication facilitates vSphere administrators' daily routine of managing backup infrastructure in the organization. This plug-in allows authorized personnel to view detailed information on the status of Veeam Backup & Replication infrastructure and create restore points ad-hoc, using no other tool but vSphere Web Client.



In particular, vSphere administrators can view success, warning, failure counts for all jobs, as well as cumulative information on used and available storage space, and statistics on processed VMs. They can easily identify unprotected VMs and perform capacity planning, as well as create restore points for selected VMs using VeeamZIP and Quick Backup functions, all directly from vSphere Web Client.

Getting Started

The vSphere Web Client plug-in is installed from the **vCenter Servers** section of the **Configuration** view in Enterprise Manager. To access the **Configuration** view, log in to Enterprise Manager using an account with the Portal Administrator role.

Before installing the vSphere Web Client plug-in, make sure the following requirements are met:

- The plug-in supports vSphere Web Client v5.1.0 build 880146 and later. For vSphere Web Client versions 5.1.0 build 880146 – 6.5 (including), the plug-in is available with the flex/flash interface. Starting with vSphere Web Client version 6.7, the plug-in offers HTML 5 user interface. The older versions of the client do not support the HTML 5 interface.
- Single Sign-On Service must be running on a server with FQDN (to be accessible from Enterprise Manager server over HTTPS).
- Account used to install the plug-in must have sufficient access rights for vCenter server (must belong to the same domain in case of cross-domain access):
  - **Extension > Register extension** – to install the plug-in
  - **Extension > Unregister extension** – to uninstall the plug-in

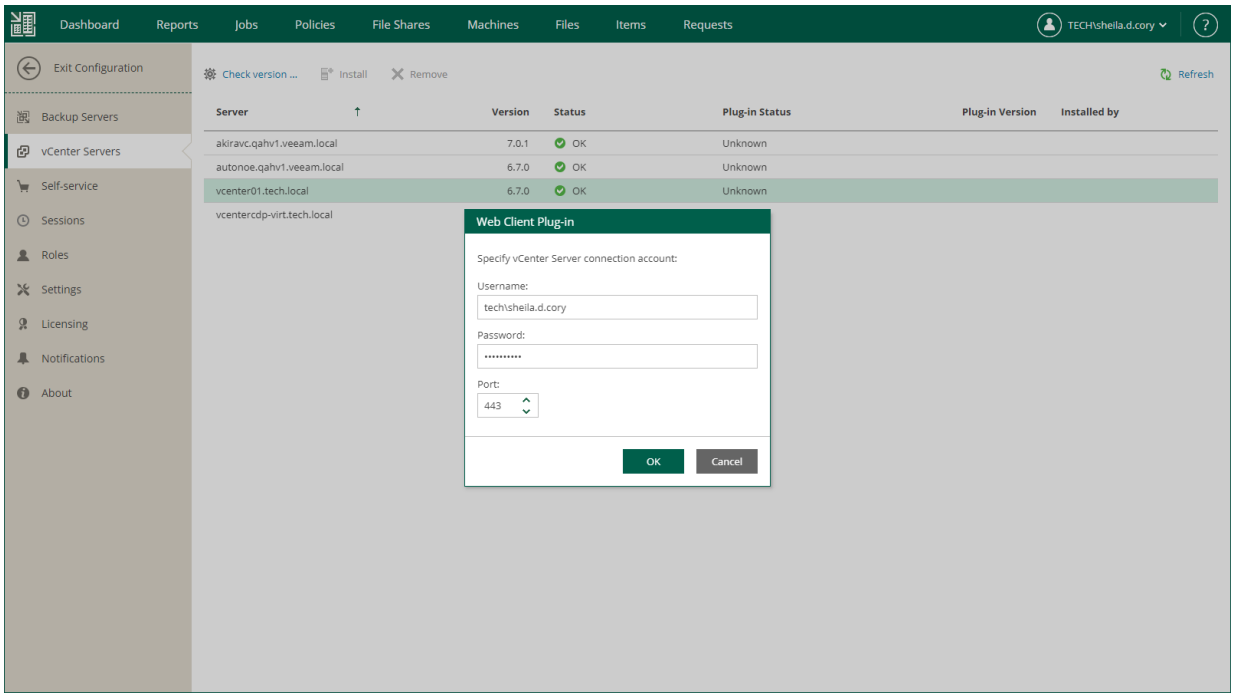
For more information on vSphere Web Client, see this VMware article.

Installing vSphere Web Client Plug-in

To install Veeam plug-in for vSphere Web Client, do the following:

1. In the Enterprise Manager **Configuration** view, go to the **vCenter Servers** section.
2. Select the vCenter server you need, and click **Check version**.
3. In the **Web Client Plug-in** window, enter a user name and password to connect to vCenter Server, and specify connection port (default is 443). Veeam Backup Enterprise Manager will use these credentials to access vCenter Server and check if Veeam plug-in has been already installed there. If discovered, plug-in version will be displayed in the **Plug-in Version** column.
4. If the connection to vCenter Server is successful, and the plug-in has not been installed yet, then the **Install** link will become active. Click it to install the plug-in.

5. After installation, the plug-in will be displayed in the list of vCenter Servers and plug-ins.



Removing vSphere Web Client Plug-in

To remove Veeam plug-in for vSphere Web Client, do the following:

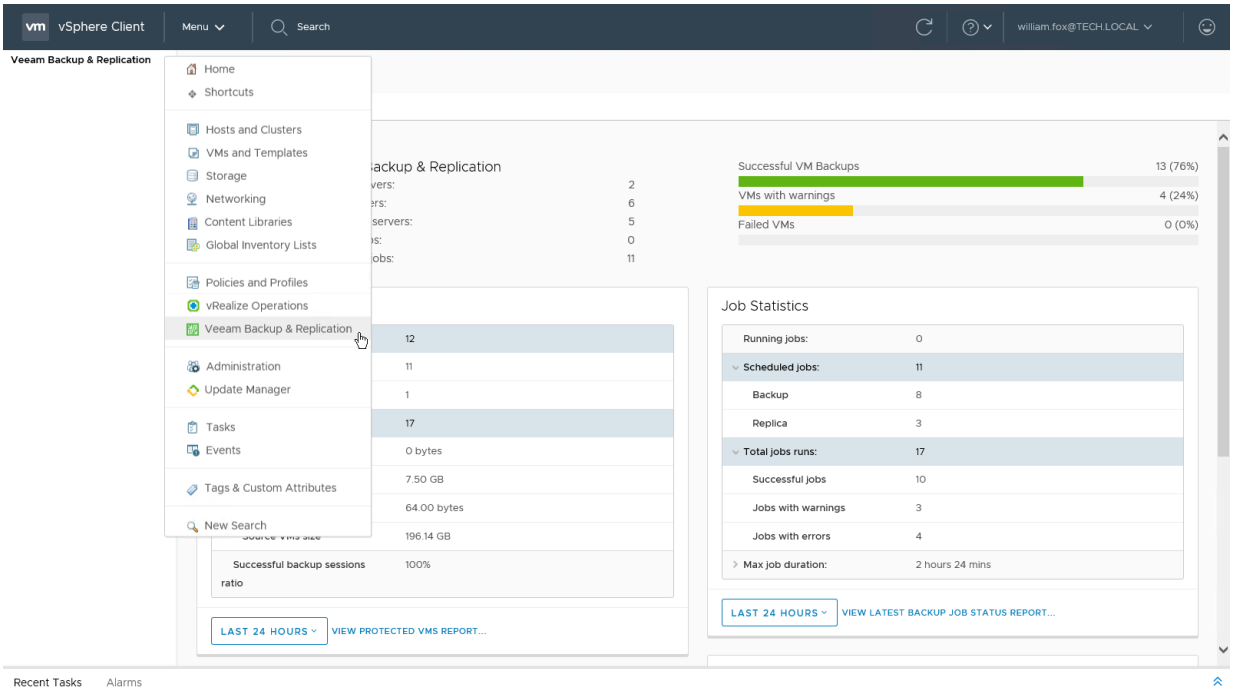
1. In the Enterprise Manager **Configuration** view, go to the **vCenter Servers** section.
2. Select the vCenter server you need, and click **Remove**.
3. In the displayed window, click **Yes** to confirm the removal.

Accessing Plug-in from vSphere Web Client

To access the plug-in from VMware vSphere Web Client, launch the vSphere Web Client and select **Veeam Backup & Replication** from the menu.

IMPORTANT

- To successfully obtain statistics from Veeam Backup Enterprise Manager, the accounts used to connect to Enterprise Manager (that is, the account currently logged in to the web client, or specific account configured in the Veeam plug-in settings) should have the Portal Administrator or Portal User role. For more information, see Configuring Accounts and Roles.
- To open Veeam ONE reports (optional capability), these accounts should be also included in the Veeam ONE Users or Veeam ONE Administrators group on the machine where Veeam ONE Server component is installed.



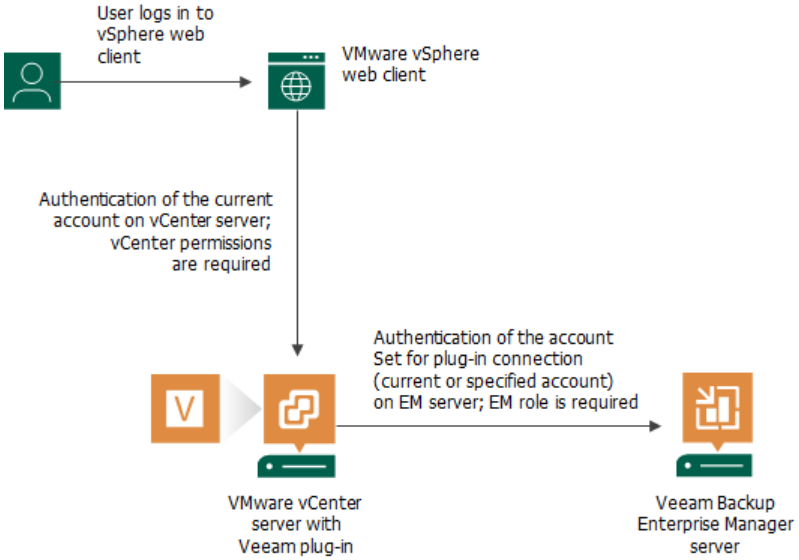
Configuring Plug-in Settings

When using the plug-in, consider that authentication process includes the following stages:

1. A user logs in to vSphere Web Client. To work with a VMware vCenter server where Veeam plug-in runs, this user account requires the following minimal privileges on vCenter level: *VirtualMachine.Interact.Backup*, *Task.Create*, *Task.Update*.

2. Veeam plug-in connects to Veeam Backup Enterprise Manager which verifies its account. You can configure Veeam plug-in to use the account currently logged in, or to use specific account for that connection. For details, see the procedure description below.

   Whatever account is used, to perform the necessary backup operation (VeeamZIP or Quick Backup) it should have sufficient security permissions. They are granted by assigning a security role — Portal Administrator or Portal User. For more information, see Configuring Accounts and Roles.



To configure a connection to the Veeam Backup Enterprise Manager server and (optionally) Veeam ONE server:

1. Open Veeam plug-in for vSphere Web Client.

2. On the **Settings** tab, check the plug-in version and specify the following Veeam Backup Enterprise Manager connection properties:

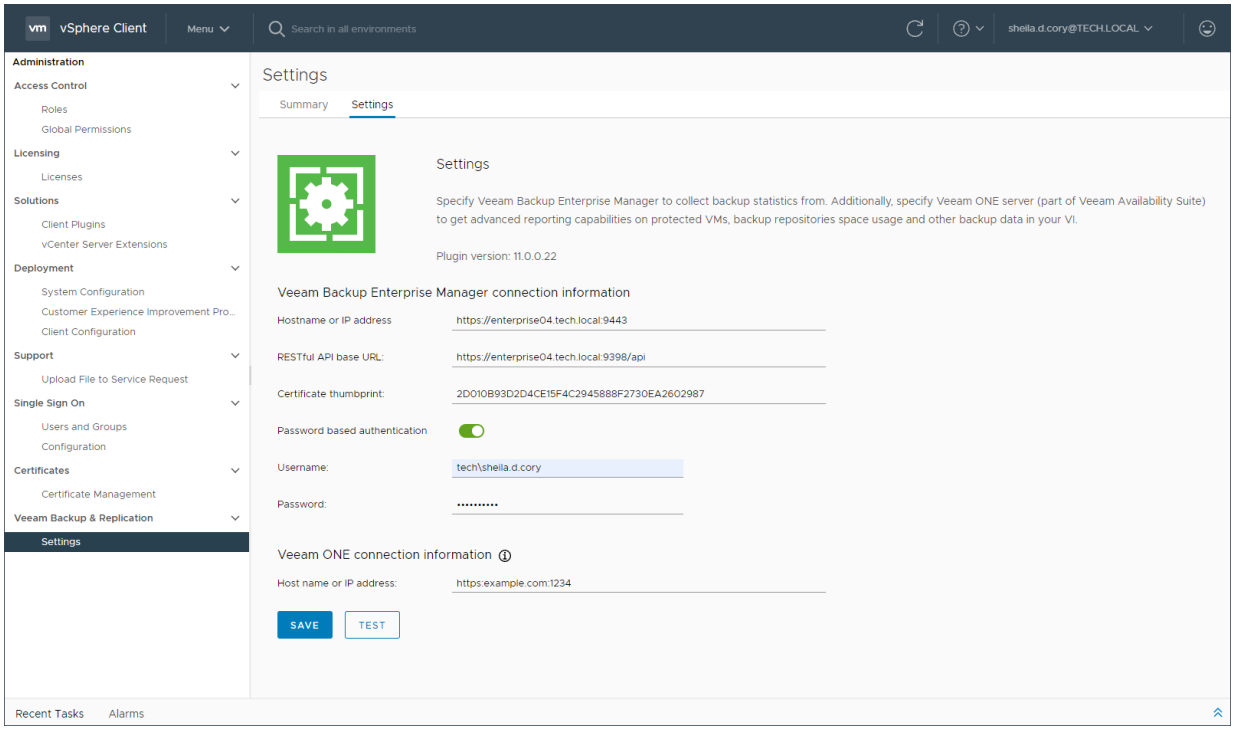
   - Host name or IP address of the Veeam Backup Enterprise Manager server
   - Base URL of Veeam Backup Enterprise Manager REST API
   - Thumbprint of the certificate used to connect to Veeam Backup Enterprise Manager REST API

   > **TIP**
   >
   > You can get the connection properties on the Veeam Backup Enterprise Manager website. To do this, log in to the website with a Portal Administrator account and go to **Configuration** > **About**. For more information, see Viewing Information About Enterprise Manager.

3. If you plan to connect to Enterprise Manager using a specific account, select the **Password based authentication** option and provide a user name and password. If this option is not selected, connection to Enterprise Manager will be performed using the account currently logged in.

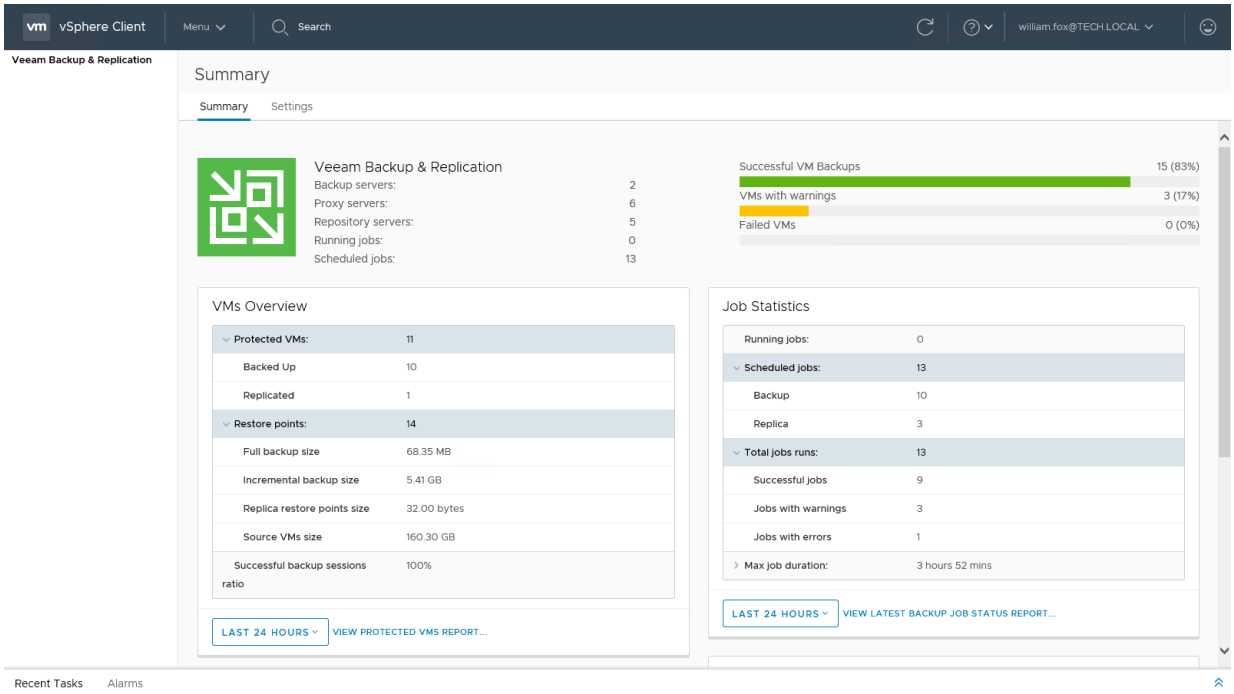
   Make sure the account intended for connection has an appropriate Enterprise Manager role assigned.

4. If you have Veeam ONE deployed in your environment, you can specify Veeam ONE server name and connection port. Default is HTTP port 1239.
5. To test the connection, click **Test**.
6. To apply the specified settings, click **Save**.



Examining Backup Infrastructure

All components of the Veeam Backup & Replication infrastructure — backup servers, proxy servers, and repository servers — are listed on top of the **Summary** page, as well as the count of running and scheduled jobs.



Next to the list, there are three key indicators that inform you how the VMs were protected during the specified period:

- Successful VM backups
- VMs with Warnings
- Failed VMs

In the dashboard pane under the summary information, you can explore backup infrastructure in more details.

- The **VMs overview** widget gives you the information on how your VMs are protected: number of protected VMs (backed up or replicated), number of restore points available, source VM size, full and incremental backup size, replica restore point size, and successful backup sessions ratio. To maximize the widget, click the **Full screen** icon in the widget's top right corner; to change reporting period, click the gear icon and select the time period you need:
  - Last 24 hours
  - Last 7 days
  - Last 14 days

  Additionally, if Veeam ONE is installed, you can click the link and examine the **Protected VMs** report that provides a list of VMs which are protected by Veeam Backup & Replication, and which are not.
- In the **Jobs statistics** widget, all running jobs are displayed, as well as scheduled jobs and max job duration. Additionally, if Veeam ONE is installed, you can click the link and examine the **Latest BU Job Statistics** report.

- In the **Repositories** widget, detailed information for each backup repository is displayed, including repository name, overall capacity, free space and backup size. Additionally, if Veeam ONE is installed, you can click the link and examine the **Capacity Planning for Repositories** report. It gives you an estimation of when the repositories may run out of space.
- The **Processed VMs** widget shows a graphical representation of how the jobs ran (1-week, 2-weeks, 1-month filters can be applied).

Creating Restore Points with VeeamZIP and Quick Backup

vSphere administrators can quickly create a restore point for a selected VM using VeeamZIP (full backup) or Quick Backup (incremental backup) right from VMware vSphere web client, with no need to use Veeam backup management console. To utilize these capabilities, a user account should be able to go through authentication process, so it must meet the requirements specified in Configuring Plug-in Settings.

Configuring VeeamZIP Settings

To configure the settings for VeeamZIP (VBK file creation), do the following:

1. In vSphere Web Client, open **vCenter Inventory**.
2. In the inventory tree, select a VM.
3. Click the **Configure** tab and select **VeeamZIP**.
4. In the **Destination** section, select the Veeam backup server to process the VM and the repository where to store the VeeamZIP file.

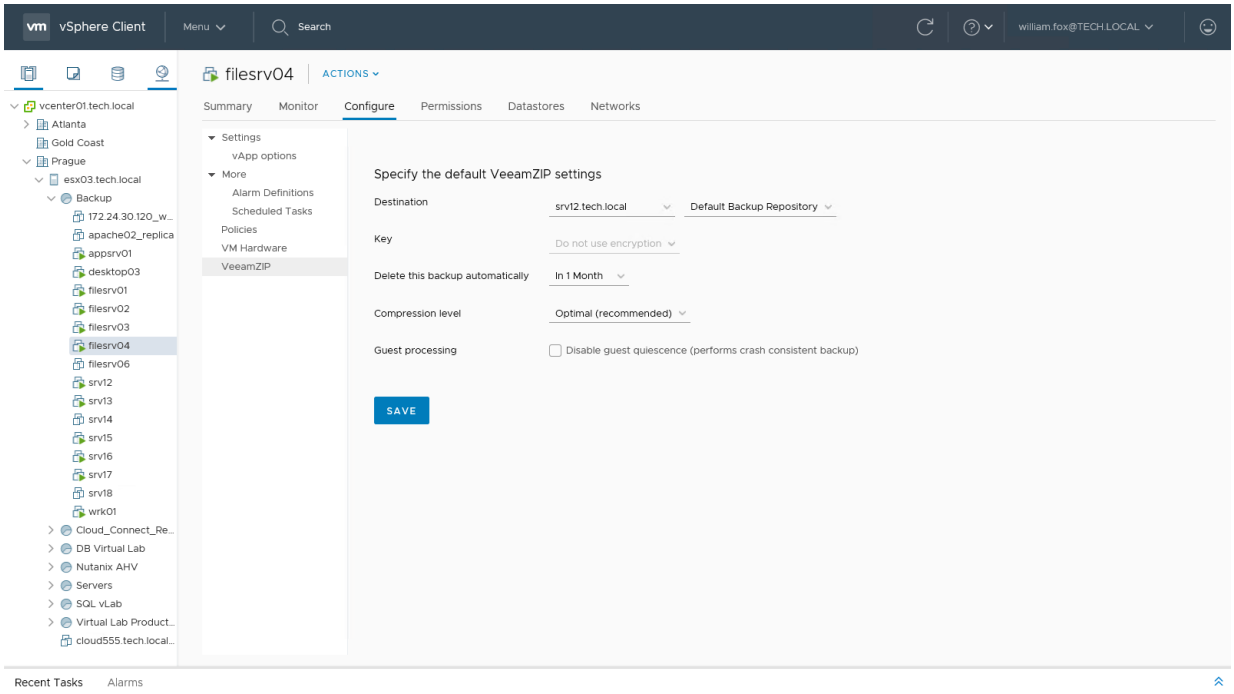
> **NOTE**
>
> To be visible in this list, Veeam backup server should be added to Veeam Backup Enterprise Manager. Connected repositories from Veeam backup infrastructure will be shown automatically.

5. In the **Key** section, specify the encryption key, if necessary.
6. In the **Delete this backup automatically** section, specify whether the resulting backup file should be automatically deleted after a certain time interval.
7. In the **Compression level** section, select the necessary compression level for the backup.
8. By default, the **Disable guest quiescence** option is selected, meaning that guest OS quiescence is deactivated. So, if you want a crash-consistent backup, leave it that way.

   If you want, however, an application-consistent backup, then clear the **Disable guest quiescence** check box, and Veeam will create a transactionally consistent image of VMs using VMware Tools quiescence for guest OS.

> **NOTE**
>
> For more information about guest OS quiescence, see the *Transaction Consistency* section of the Veeam Backup & Replication User Guide.

9. Click **Save**. The specified settings will be stored as default settings for the currently logged on user account and will be used for VeeamZIP backup.



Creating Full VM Backup with VeeamZIP

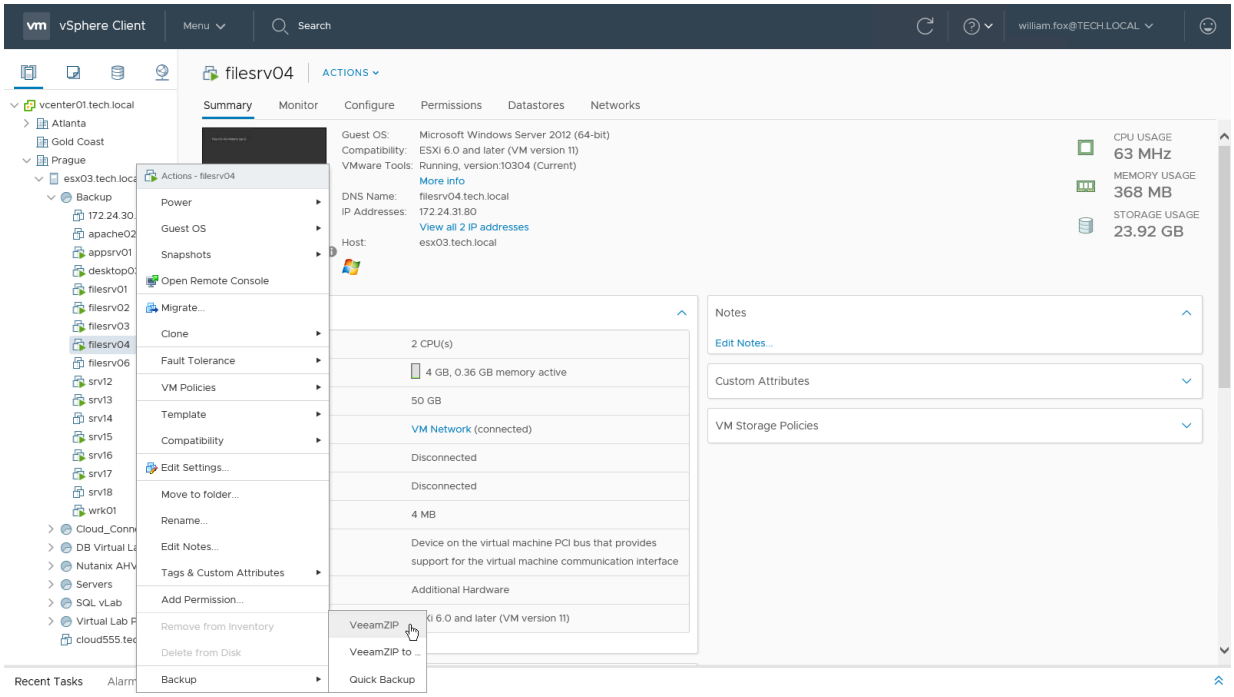
You can use Veeam plug-in for vSphere Web Client to create an ad-hoc VeeamZIP backup of a VM. To create a full VM backup with VeeamZIP:

1. In vSphere Web Client, open **vCenter Inventory**.

2. In the inventory tree, right-click the VM that you want to back up and select one of the following options:

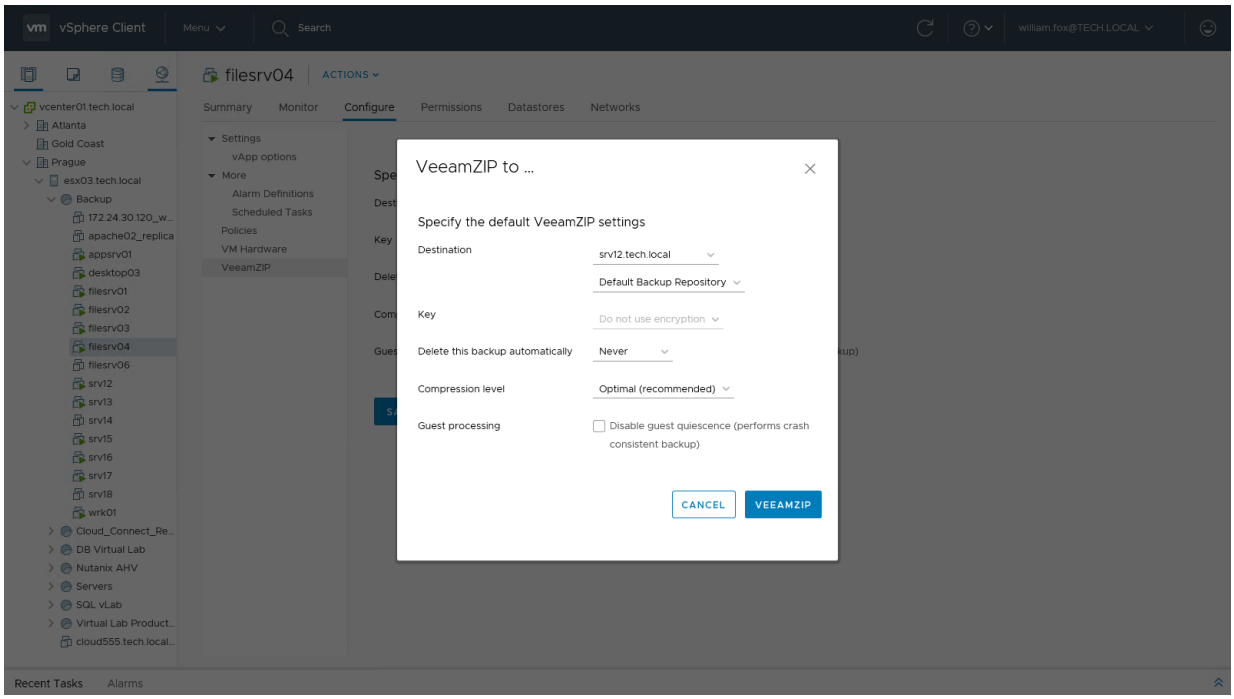
   - Select **Backup** > **VeeamZIP** if you want to create a backup using the default VeeamZIP settings specified earlier. Alternatively, use the **Actions** > **Backup** > **VeeamZIP** option.

     Veeam will start the VeeamZIP backup process using the default VeeamZIP settings.



   - Select **Backup** > **VeeamZIP to** if you want to create a backup with new VeeamZIP settings. Alternatively, use the **Actions** > **Backup** > **VeeamZIP to** option.

     If you select this option, Veeam plug-in will display the **VeeamZIP to** window offering to specify VeeamZIP settings. Specify settings in the same way as described in the Configuring VeeamZIP Settings section and click **VeeamZIP**. Veeam will save the specified settings as default settings for VeeamZIP backup and start the VeeamZIP backup process.



You can view the backup creation progress in the **Recent Tasks** pane of vSphere Web Client.

Creating Incremental VM Backup with Quick Backup

You can also create an incremental backup for selected VM with a single click, using Quick Backup capability. Quick Backup can be run for any VM that meets the following requirements:

1. A backup job processing the VM exists on the Veeam backup server which is added to Veeam Backup Enterprise Manager.
2. There is a full backup file for this VM in the backup repository.

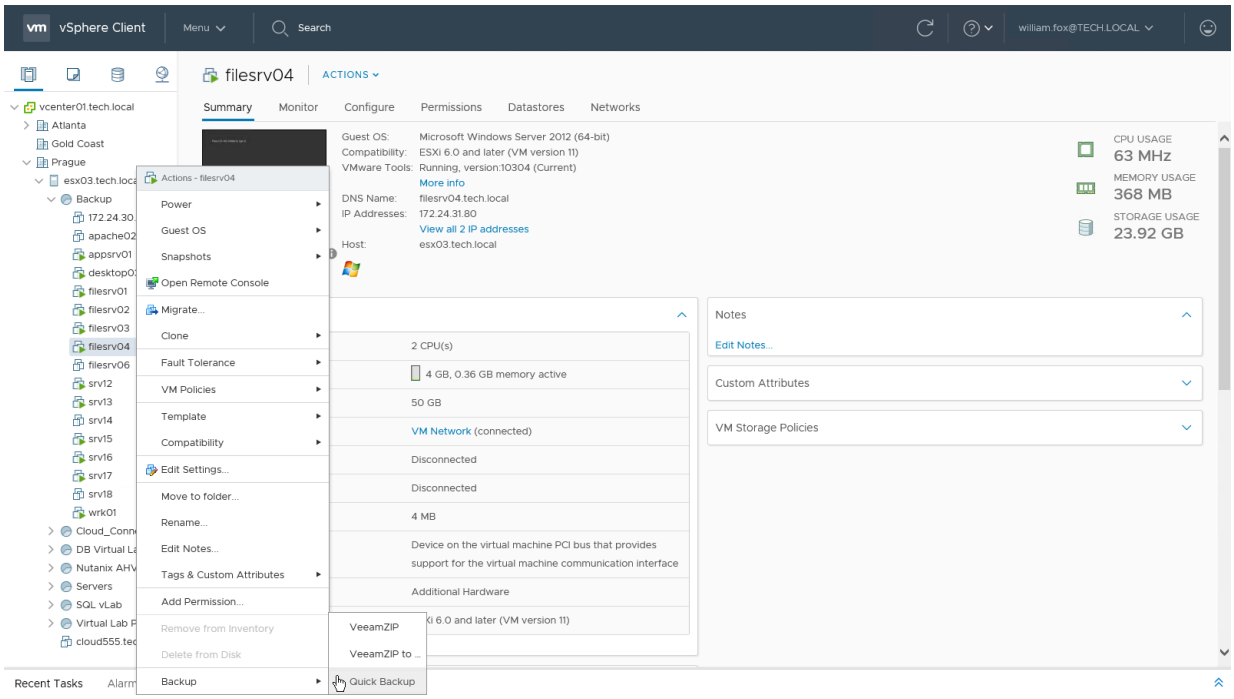
To perform quick backup:

1. In the **vCenter Inventory**, select the necessary VM.
2. Right-click the VM and select **Quick Backup**. Alternatively, you can use the **Actions** menu command.

This will trigger a backup job processing the selected VM to create a new incremental restore point (VIB file) for the latest full backup found in the repository for this VM. Details of a running quick backup task can be seen in the **Recent Tasks** pane on the right.

To learn more about VeeamZIP and Quick Backup, refer to the Veeam Backup & Replication User Guide.

> **NOTE**
>
> A Quick Backup or VeeamZIP job fails to start if the *Location* property of the VM and backup repository do not match — for example, if you try to use a repository with location set to Sydney to back up a VM with location set to Helsinki. To read more about location settings, refer to the Veeam Backup & Replication User Guide.



vSphere Self-Service Backup Portal

Veeam Backup & Replication allows backup administrators to delegate VM backup and restore operations to VMware vSphere users. For that, Veeam Backup & Replication offers the vSphere Self-Service Backup Portal — a web tool based on Veeam Backup Enterprise Manager. With vSphere Self-Service Backup Portal, users can create and manage backup jobs that process vSphere VMs and restore data from backups created with these jobs. All operations are performed from the web UI without the need to deploy the Veeam Backup & Replication console on the user machine.

To define what VMs vSphere users can back up and restore, Veeam Backup Enterprise Manager offers the concept of delegation mode. The delegation mode specifies conditions that must be met to allow a user to add a VM to the backup job. The administrator can choose from 3 delegation modes based on vSphere tags, vSphere roles or VM privileges. For more information, see Configuring Delegation Mode.

In terms of vSphere Self-Service Backup Portal, a vSphere user that works with the portal is considered a tenant. To access the portal, a tenant uses the tenant account created by the Enterprise Manager administrator. The administrator can create tenant accounts for a separate vSphere user and a group of users. The tenant account settings define storage quota available to the tenant on the backup repository and settings for backup jobs created by the tenant. For more information, see Managing Tenant Accounts.

To simplify backup job management for tenants, advanced job settings (such as backup settings and storage settings) and schedule settings are automatically populated from job templates. The administrator can assign a separate template to each tenant account.

When working with vSphere Self-Service Backup Portal, administrators and tenants perform the following tasks:

- Administrator tasks
- Tenant tasks

Administrator Tasks

To let tenants work with vSphere Self-Service Backup Portal, the Veeam Backup Enterprise Manager administrator performs the following tasks:

1. Configures the delegation mode

   The default delegation mode allows tenants to access VMs with the *VirtualMachine.Interact.Backup* privilege. The administrator can change the delegation mode, if necessary.

2. Creates and manages tenant accounts

   By default, Veeam Backup Enterprise Manager offers a group tenant account for users of the domain that includes the Enterprise Manager server. Each user can access the portal and use a 30 GB quota on the default backup repository to create VM backups. Users can create backup jobs with default advanced settings and custom schedule. The administrator can edit settings of the default account and create other accounts to configure granular access to storage quotas and backup settings.

> **NOTE**
>
> Administrators perform tasks with vSphere Self-Service Backup Portal using the **Self-service** section in the **Configuration** view of the Enterprise Manager UI. If a vCloud Director server is added to your Veeam backup infrastructure, the working area of the **Self-service** tab will display two inner tabs: **vSphere** and **vCloud**. To work with vSphere Self-Service Backup Portal, make sure the **vSphere** tab is opened. The **vCloud** tab is used to work with VMware vCloud Director organizations and their configurations. For more information, see Working with VMware vCloud Director.

Tenant Tasks

Tenants access the vSphere Self-Service Backup portal using the portal URL obtained from the Veeam Backup Enterprise Manager administrator. Tenants can log in to the portal under a domain user account or single sign-on account. For more information, see Accessing Portal.

Tenants can use the portal to work with vSphere VMs that are available to them according to the selected delegation mode. VM backup settings are defined by the properties of the tenant account.

Tenants can use vSphere Self-Service Backup Portal to perform the following operations:

- Create and manage backup jobs that process vSphere VMs.
- View VM backup statistics.
- Restore vSphere VMs to the original location.
- Restore files from indexed and non-indexed guest OS file systems of vSphere VMs.
- Perform item-level restore for Microsoft SQL Server and Oracle databases.

For more information, see Using vSphere Self-Service Backup Portal.

Configuring Delegation Mode

To define what VMs tenants of vSphere Self-Service Backup Portal can back up and restore, the Enterprise Manager administrator can configure the delegation mode. The delegation mode specifies conditions that must be met to allow a tenant to add a VM to the backup job.

> **NOTE**
>
> If you have configured a single sign-on service to access vSphere Self-Service Backup Portal, you must use the delegation mode based on vSphere tags only. For more information on single sign-on, see SAML Authentication Support.

To configure a delegation mode:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter server as part of its infrastructure.
4. If a vCloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. In the **Delegation Mode** window, select a delegation mode:
   - **vSphere tags** — to allow tenants to work with VMs to which the specified tags are assigned. If you select this option, you must specify the necessary tags in the properties of the tenant account. You can specify tags for each tenant account individually. For more information, see Adding Tenant Account and Editing Tenant Account.
   - **vSphere role** — to allow tenants to work with VMs that are available to the specified vSphere role.

     To specify a vSphere role:

     i. Next to the **vSphere role** option, click **Select Role**.

     Alternatively, if you have already selected a role before, click the name of the currently selected role.

     ii. In the **Select Role** window, select the required vSphere role.

     iii. Click **OK**.
   - **VM privilege** — to allow tenants to work with VMs for which they have the specified vSphere privilege.

     To select a vSphere privilege:

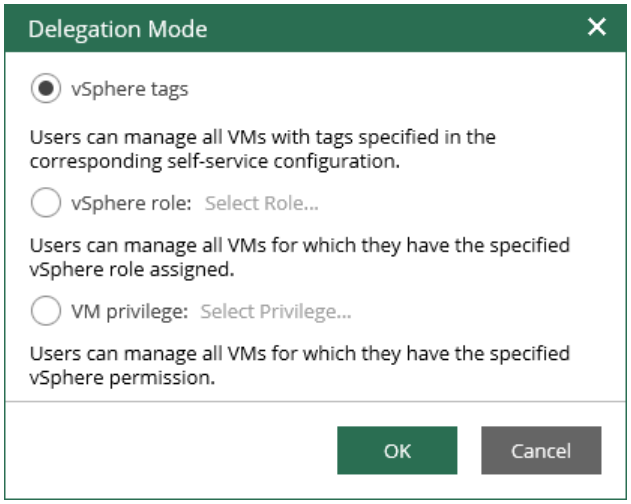
     i. In the **VM privilege** field, click the name of the currently selected privilege. By default, the *VirtualMachine.Interact.Backup* privilege is selected.

     ii. In the **Select Privilege** window, select the required privilege.

     iii. Click **OK.**
6. Click **OK**.

NOTE

If you change the delegation mode when tenants already work with vSphere Self-Service Backup Portal, tenants can lose access to VMs that were available to them according to the original delegation mode. Make sure that the necessary tags, roles or privileges are configured in VMware vSphere.



Managing Tenant Accounts

Veeam Backup Enterprise Manager offers the following types of vSphere Self-Service Backup Portal tenant accounts: User, Group, External User and External Group.

Type	Description	How to Sign In	Name Format
User	AD user	By specifying a user name and password	*DOMAIN\Username* Domain is optional
Group	AD group	By specifying a user name and password	*DOMAIN\Groupname* Domain is optional
External User	IdP user	By using single sign-on*	*Username@Suffix*
External Group	IdP group	By using single sign-on*	Free-form string

* For more information on the single sign-on capability, see SAML Authentication Support.

> **NOTE**
>
> You cannot create a vSphere Self-Service Backup Portal tenant account for a local user account.

Veeam Backup Enterprise Manager administrators can perform the following tasks with the tenant accounts:

- Add a new tenant account
- Edit an already created tenant account
- Export a report on the created tenant accounts
- Remove a tenant account

Adding Tenant Account

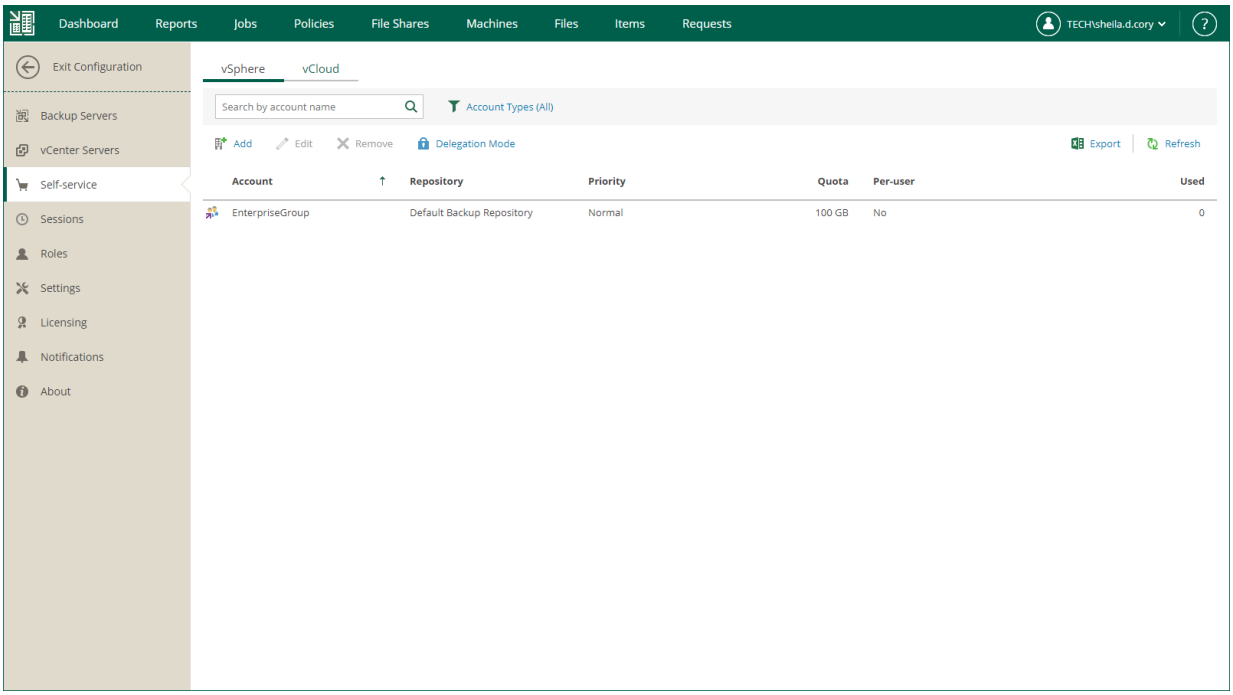
Veeam Backup Enterprise Manager offers the default Domain Users account for vSphere Self-Service Backup Portal tenants. It is a group account that includes all users from the Enterprise Manager server domain. To configure granular access to storage quotas and backup settings, the Enterprise Manager administrator can add new tenant accounts.

> **NOTE**
>
> If you plan to provide a user with access to vSphere Self-Service Backup Portal only, and not to the main Enterprise Manager UI, you do not need to configure an account for this user in the **Roles** tab of the **Configuration** view.

To add a tenant account for vSphere Self-Service Backup Portal:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter server as part of its infrastructure.
4. If a vCloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Click **Add**.



6. From the **Type** drop-down list, select a type of the account: *User*, *Group*, *External User* or *External Group*. For more information, see Managing Tenant Accounts.
7. In the **Account** field, specify an account name in the *DOMAIN|Username* or *Username@Suffix* format depending on the account type. For more information, see Managing Tenant Accounts.

> **NOTE**
>
> You cannot create a vSphere Self-Service Backup Portal tenant account for a local user account.

8. From the **Repository** drop-down list, select a target repository that will contain VM backups created by the tenant. The list includes repositories configured on Veeam backup servers added to Veeam Backup Enterprise Manager.

   Backup repository settings specified at this step will take priority over backup repository settings prescribed by the selected job template.

   > **NOTE**
   >
   > You cannot assign to tenants Veeam Cloud Connect repositories, as well as NetApp or Nimble storage systems storing snapshots created by Veeam snapshot-only jobs.

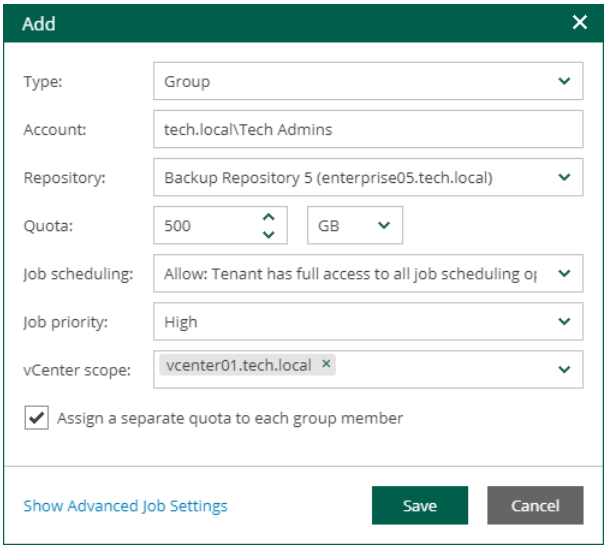
9. In the **Quota** field, specify the repository storage quota for the tenant account. Choose *GB* or *TB* from the drop-down list and enter the required quota size.
10. From the **Job scheduling** drop-down list, select how the job scheduling will be organized. The following options are available:
    - *Allow: Tenant has full access to all job scheduling options*
    - *Allow: Tenant can create daily and monthly jobs only*
    - *Deny: Creates daily jobs with randomized start time within the backup window*

      For tenant backup jobs, the backup window is defined by backup window settings specified in Veeam Backup Enterprise Manager. Backup window settings specified for the job template that you will select at the step 12 do not affect tenant jobs. For information on how to specify the backup window in Enterprise Manager, see Customizing Chart Appearance.
    - *Deny: Creates job with no schedule assigned*

    For more information on job scheduling, see Edit Job Schedule.
11. From the **Job priority** drop-down list, select a normal or high priority for backup jobs of the tenant.
12. If you have multiple vCenter Servers in your infrastructure and want to provide the tenant account with access to VMs of specific vCenter Servers only, from the **vCenter scope** drop-down list, select the necessary vCenter Servers. By default, the *All vCenter Servers* options is selected.
13. If you have selected the delegation mode that is based on vSphere tags, in the **vSphere tags** field, specify tags assigned to VMs that will be available to the tenant.

    For more information on delegation modes, see Configuring Delegation Mode.

14. [Optional] If you add a tenant account of the Group or External Group type, select the **Assign a separate quota to each group member** check box to provide each user of the group with individual quota on the backup repository. Each user will be able to work with backup jobs and VM backups created by this user only. Backups and jobs of other users will not be displayed.



15. [Optional] Specify advanced settings for backup jobs of the tenant:

    a. Click the **Show Advanced Job Settings** link.

    b. In the **Advanced job settings** section, view the currently used backup job settings.

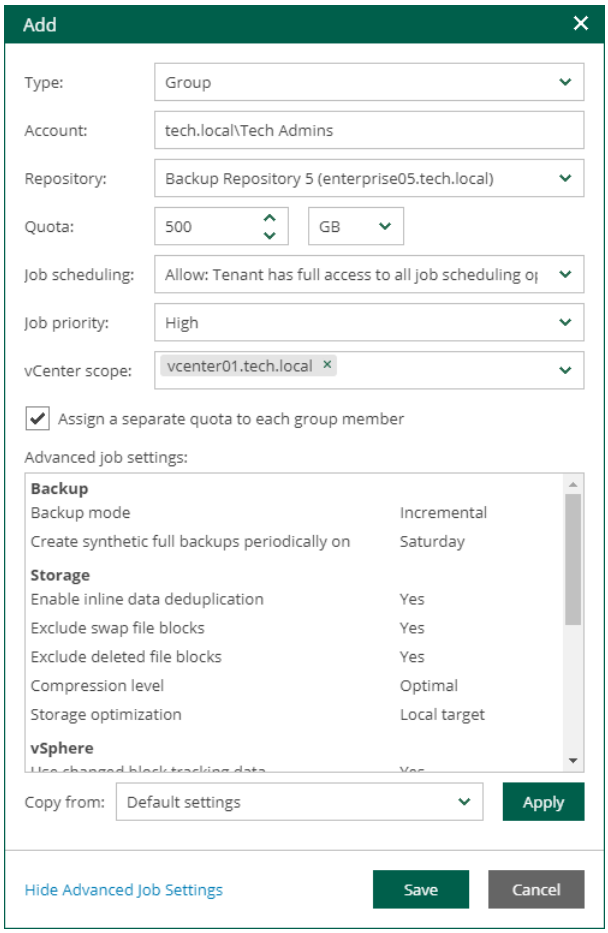
    c. From the **Copy from** list, select the backup job settings that will be applied to tenant jobs. You can select from the following options:

    - *Default settings* — this option is selected by default. With this option selected, tenant backup jobs will be configured with the default settings as they are shown in the Veeam backup console. For more information, see the Creating Backup Jobs section of the Veeam Backup & Replication User Guide.
    - *<Job name>* — an existing backup job for vSphere VMs. With this option selected, the backup job will be used as a template for tenant backup jobs. The job must be configured in advance on the Veeam backup server added to Veeam Backup Enterprise Manager. When a tenant creates a backup job on the vSphere Self-Service Backup Portal, Enterprise Manager will copy job settings from the template and apply these settings to the job.

    d. Click **Apply**.

> **NOTE**
>
> To populate the list of job templates, you must have at least one vSphere backup job configured in the Veeam backup console.

16. Click **Save**.



Editing Tenant Account

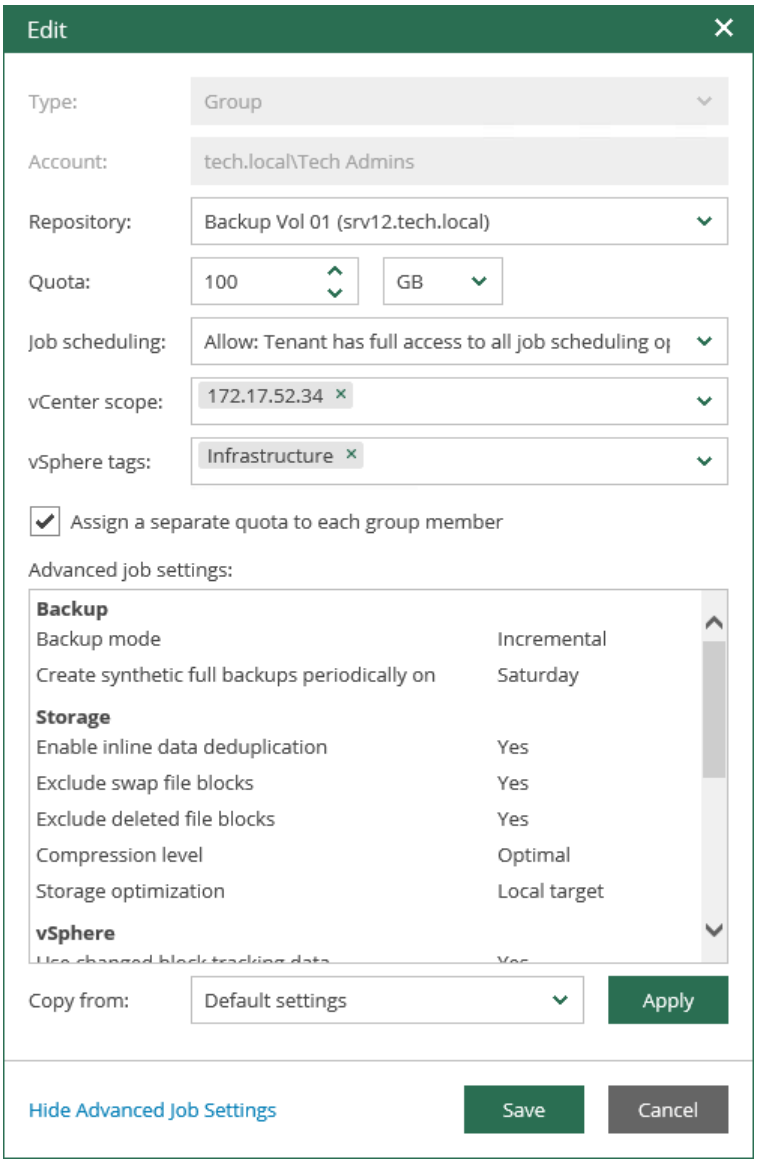
The Veeam Backup Enterprise Manager administrator can edit tenant accounts configured for vSphere Self-Service Backup Portal. For example, the administrator changes backup scheduling settings or other settings for tenant backup jobs.

To change settings of a tenant account:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter server as part of its infrastructure.
4. If a vCloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Select the account you need and click **Edit**.
6. In the **Edit** window, edit tenant account settings as required. For more information, see Adding Tenant Account.

7. Click **Save**.



NOTE

Make sure to establish a proper connection between the Veeam backup server and Enterprise Manager server. Otherwise, changes of the tenant account settings will not be saved to the Veeam configuration database.

Consider the following recommendations for modifying tenant account settings for vSphere Self-Service Backup Portal:

- If you plan to modify job template for a tenant account, remember that the new settings will be applied only to the new jobs created by the tenant; the changes will not affect existing jobs.
- If you want an existing backup job to create backups in another backup repository instead of the repository that is currently specified in the properties of the tenant account, do the following:
    a. In Veeam Backup Enterprise Manager, specify the new backup repository in the properties of the tenant account.
    b. Move vSphere VM backups created by the tenant to the new repository.

c. In Veeam Backup & Replication, specify the new backup repository in the properties of tenant backup jobs.

Otherwise, tenant backup jobs will continue creating backups in the former repository.

Exporting List of Tenant Accounts

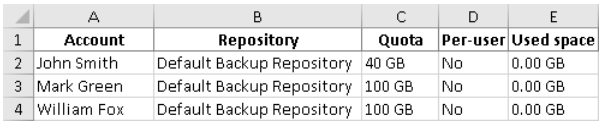
The Veeam Backup Enterprise Manager administrator can generate a report on tenant accounts configured for vSphere Self-Service Backup Portal. This report includes information on the account name, backup repository used by the account, storage quota allocated to the account, and space used by the account.

To generate a report:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter server as part of its infrastructure.
4. If a vCloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Click the **Export** link in the top right corner.

The report is saved to the `excelreport.xls` file.



	A	B	C	D	E
1	**Account**	**Repository**	**Quota**	**Per-user**	**Used space**
2	John Smith	Default Backup Repository	40 GB	No	0.00 GB
3	Mark Green	Default Backup Repository	100 GB	No	0.00 GB
4	William Fox	Default Backup Repository	100 GB	No	0.00 GB

Removing Tenant Account

The Veeam Backup Enterprise Manager administrator can remove tenant accounts configured for vSphere Self-Service Backup Portal.

To remove a tenant account:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter server as part of its infrastructure.
4. If a vCloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Select the account you want to remove.
6. Click **Remove**.
7. In the **Remove configuration** window, select necessary options:
   - To delete backup jobs created by the tenant, select the **Delete jobs** check box.
   - To delete all backups created by the tenant, select the **Delete backup files** check box.
8. To confirm the removal, click **Yes**.

Using vSphere Self-Service Backup Portal

vSphere Self-Service Backup Portal is a tool for VMware vSphere users that facilitates operations with delegated VM protection, including VM restore and files restore. These operations do not require access to the Veeam Backup & Replication console. For backup and restore operations, tenants access vSphere Self-Service Backup Portal.

Accessing Portal

To access vSphere Self-Service Backup Portal:

1. Open your web browser and enter the following address in the address bar:

   ```
   https://<EnterpriseManagerServer>:9443/backup
   ```

   For example:

   ```
   https://vbr-em:9443/backup
   ```

2. From the drop-down list, select a language that you want to use as the display language.

   For more information, see Managing Languages.

3. Log in using your credentials:

   - To log in with Enterprise Manager credentials:

     i. In the **Username** and **Password** fields, specify credentials of the domain user for which the Enterprise Manager administrator created a vSphere Self-Service Backup Portal tenant account. The username must be provided in the *DOMAIN|Username* format.

     ii. To save the entered credentials for future access, select the **Remain signed in** option.

     iii. Click **Sign in**.

   - To log in with single sign-on, click **Use Single Sign-On (SSO)**. You will be redirected to the login webpage of the single sign-on service. Complete the sign-in procedure on the login page. If the account is already authenticated in the single sign-on service, you will immediately access the Enterprise Manager website.

     > **NOTE**
     >
     > The **Use Single Sign-On (SSO)** option is available if SAML authentication is configured for Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.

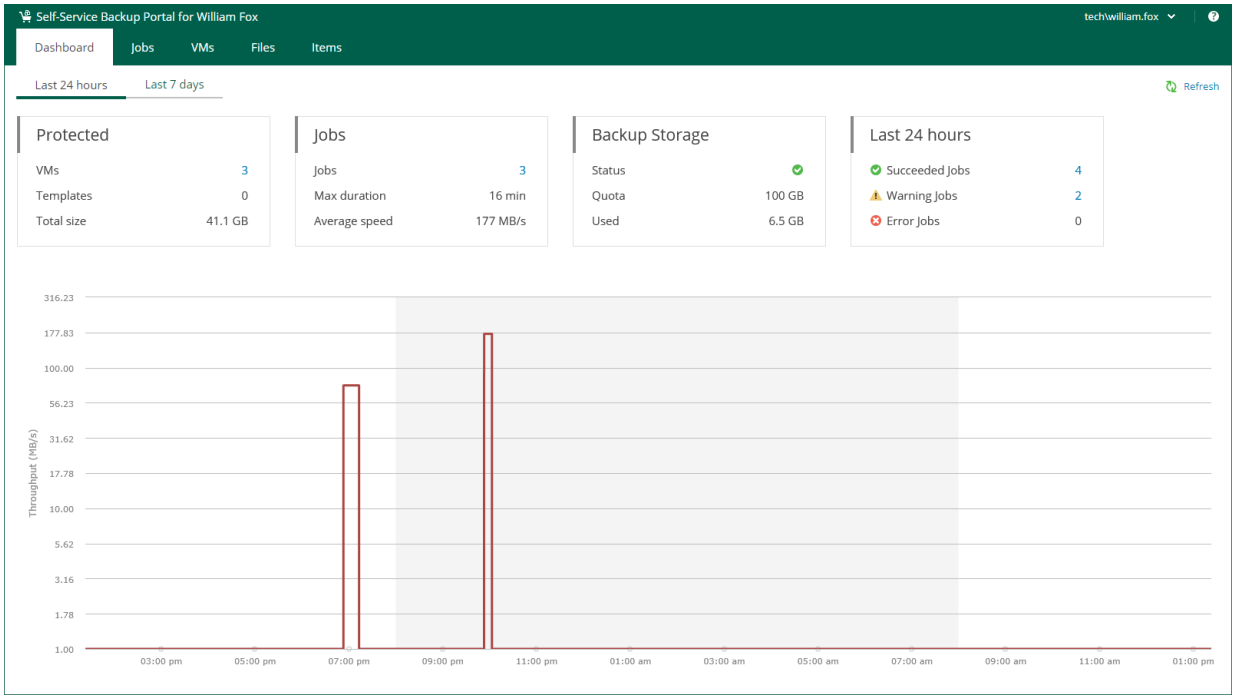
Working with Portal

You can use vSphere Self-Service Backup Portal to perform the following operations:

- View statistics on backups of vSphere VMs. For more information, see Viewing Self-Service Backup Portal Statistics.
- Work with backup jobs that process vSphere VMs: create and edit backup jobs; examine and export backup job session data; start, stop and retry backup jobs. For more information, see Managing Backup Jobs.
- Perform backup and restore operations with vSphere VMs. For more information, see Managing VMs.
- Search for files in guest file systems of backed-up VMs and restore the necessary files to the original location or download them to a local machine. For more information, see Restoring Guest OS Files.
- Perform item-level restore of Microsoft SQL Server and Oracle databases. For more information, see Restoring Application Items.

Viewing Self-Service Backup Portal Statistics

The **Dashboard** tab contains statistics on tenant backup infrastructure, including information about protected VMs, backup jobs, backup storage and the number of jobs that completed successfully, finished with warnings and errors. You can view statistics for the last 24 hours or last 7 days. To switch between the views, click **Last 24 hours** or **Last 7 days** in the top left corner of the working area.



The **Protected** block displays the following information:

- **VMs** – number of VMs successfully processed during the selected period. At least one restore point was created for these VMs.
- **Templates** – number of virtual machine templates successfully protected during the specified period.
- **Total size** – total size of successfully protected VMs and templates.

The **Jobs** block displays the following information:

- **Jobs** – number of jobs created by the currently logged-in user.
- **Max duration** – maximum job duration.
- **Average speed** – average data transfer speed.

The **Backup Storage** block displays the following information:

- **Status** – status of the backup storage assigned to the user: *Green* – more than 10% of storage space is free; *Yellow* – less than 10% of storage space is free; *Red* – no free space on backup storage.
- **Quota** – storage quota assigned to the user.
- **Used** – storage quota used by the user.

The **Last 24 hours** / **Last 7 days** block reports on job session results for the selected period.

To visualize on-going job data, the **Dashboard** tab also comprises a graph showing time and date when jobs were performed, and the network throughput rate during the job.

The highlighted part of the graph represents the configured backup window if this option was specified in the dashboard settings. For more information, see Customizing Chart Appearance.

Managing Backup Jobs

In the **Jobs** tab of Self-Service Backup Portal, you can perform the following operations with backup jobs:

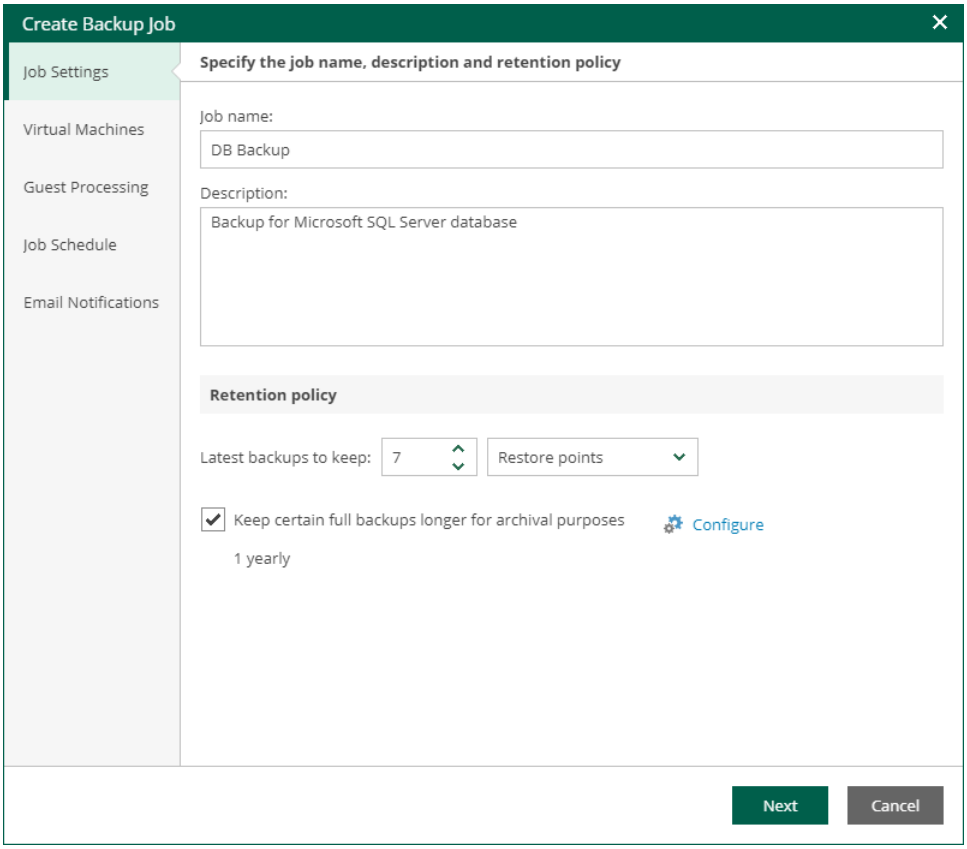
- Create a new backup job for vSphere VMs
- Start, stop and retry jobs
- Enable and disable jobs
- Edit backup job settings
- Delete backup jobs

Creating Backup Job

To create a new vSphere backup job:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal and click **Create**.
2. At the **Job Settings** step of the wizard, specify the backup job name, description and retention policy settings. The retention policy defines how many restore points are kept in the backup repository and can be used for data restore.

   For more information, see the Retention Policy section of the Veeam Backup & Replication User Guide.



3. At the **Virtual Machines** step of the wizard, select which vSphere VMs the job will process. For more information, see Edit the List of Virtual Machines.
4. At the **Guest Processing** step of the wizard, select the guest OS processing options and guest OS credentials. For more information, see Configure Guest Processing Settings.

5. At the **Job Schedule** step of the wizard, configure the backup job scheduling options. For more information, see Schedule the Job.

   You can configure backup job scheduling options only if the Enterprise Manager administrator allowed this in the properties of the tenant account. For more information, see Adding Tenant Account.

6. At the **Email Notifications** step of the wizard, select the **Enable e-mail notifications** check box and configure notification settings:

   a. In the **Recipients** field, enter email addresses of recipients separated by comma.

   b. [Optional] In the **Subject** field, specify the subject for notification emails.

   c. Select the **Notify on success**, **Notify on error** and/or **Notify on warning** options to receive email notification if the job completes successfully, fails or completes with a warning.

   d. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.

7. Click **Finish**.

The backup job will create backups in the backup repository that the Enterprise Manager administrator selected as the target repository in the properties of the tenant account. Advanced job settings such as the backup settings and storage settings will be obtained from the job template assigned to the tenant by the administrator. For more information, see Editing Tenant Account.

Editing Backup Job

You can edit a backup at any time you need. For example, you may want to change scheduling settings for the job or add VMs to the job.

To edit backup job settings, do the following:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal.
2. In the working area, select the job you want to edit and click **Edit**.
3. In the **Edit** window, edit backup job settings as required. You will follow the same steps as you have followed when creating the job. For more information, see Creating Backup Job.

Removing Backup Job

You can permanently remove a backup job from the configuration database. To remove a job, do the following:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal.
2. In the working area of the **Jobs** tab, select the job you want to delete.
3. Click **Delete**.

Information about the deleted job will be removed from the Veeam Backup & Replication configuration database (and the Enterprise Manager database as well), and the job will no longer appear in the UI. If you agreed to delete backup files created with the job, they will be removed from backup repository.

> **IMPORTANT**
>
> For vSphere Self-Service Backup Portal tenants, the job cloning operation is not available.

Managing VMs

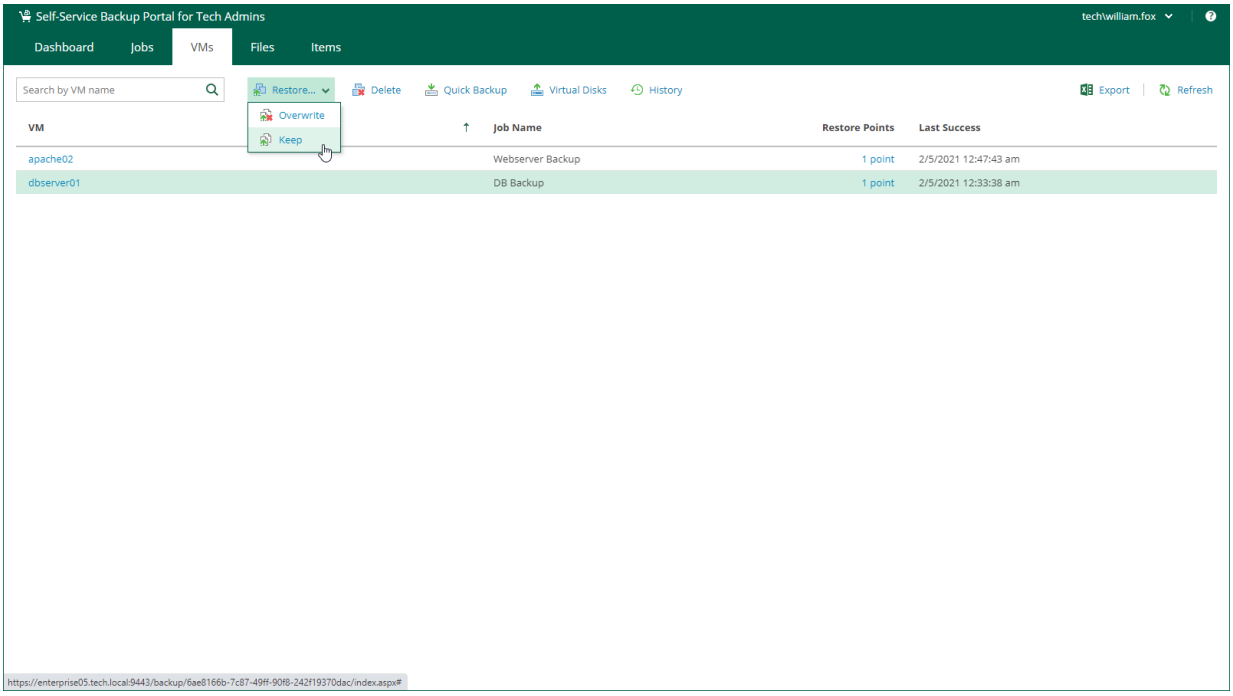
You can use vSphere Self-Service Backup Portal to perform the following operations with backed-up VMs:

- Search VMs and view VMs details
- Restore VMs
- Restore VM disks
- Delete VMs

Restoring VMs

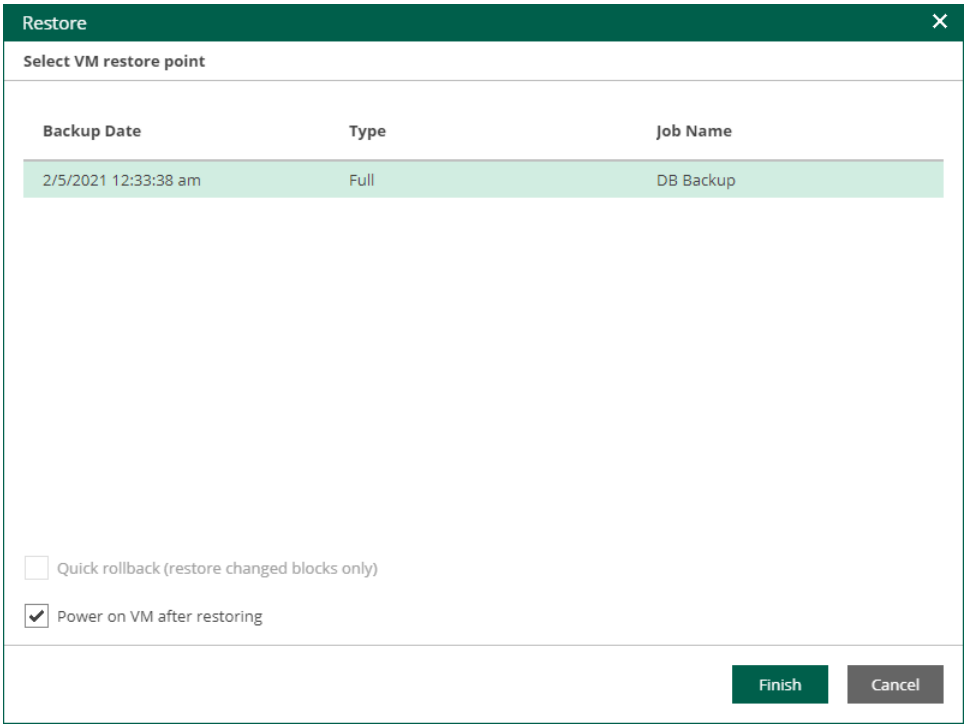
You can restore vSphere VMs to the original (production) location using flexible restore options. To restore a VM, do the following:

1. On the **VMs** tab, select the necessary VM in the list of VMs. You can also use the search field to search for the necessary VM by a VM name.
2. Click **Restore** and select the option you need:
   - Select the **Overwrite** option if you want to replace the VM in the original location with the VM in the backup. The current state of the VM will be deleted.
   - Select the **Keep** option if you want to save the current state of the VM. The restored VM will be located next to the original VM and will have the same name with the *_restored* suffix added to the VM name.



3. In the **Restore** window, select the restore point that will be used to restore the VM.
4. You can select additional options for the VM restore:
   - Select the **Quick rollback** check box if you want to restore only the changed data. This option is available only for VMs that were protected with the Changed Block Tracking (CBT) option.
   - Select the **Power on VM after restoring** check box if you want to turn on the VM once it is restored.

- Select the **Restore VM tags** check box if you want to restore vSphere tags of the VM.



5. Click **Finish**.
6. Veeam Backup Enterprise Manager will display a message notifying that the VM from the backup will replace the original VM if this VM is present in the original location. Click **Proceed** to start the VM restore operation.

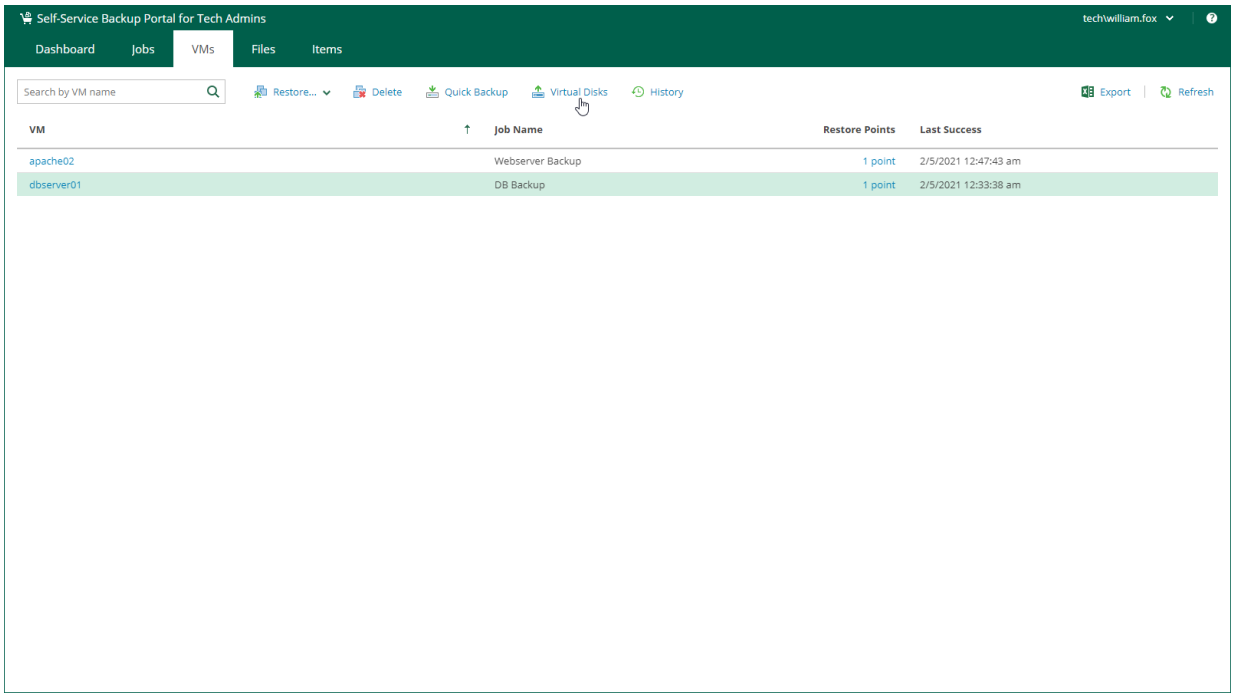
You can view the VM restore progress. To do this, on the **VMs** tab, click **History**.

Restoring Virtual Disks

You can restore individual virtual disks from backups of vSphere VMs:

1. On the **VMs** tab, select the backup of the VM whose disks you want to restore. You can also use the search field to search for the necessary VM by a VM name.
2. Click **Virtual Disks**.

3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Performing Virtual Disk Restore.



Deleting VMs

You can delete a VM on **vSphere Self-Service Backup Portal. This operation may be useful if you want to delete data of the backed-up VM from the backup repository.**

When you delete a VM, Veeam Backup Enterprise Manager removes records about the VM from the UI and configuration database. In addition, Enterprise Manager removes data of the deleted VM from the backup.

To delete a VM, on the **VMs** tab, select the necessary VM and click **Delete**. Then press **Yes** in the **Delete VM** window.

The deleted VM is not removed from the list of VMs immediately. The VM will be removed from the list after records about the VM are removed from the configuration database on the Veeam backup server.

Restoring Guest OS Files

The **Files** tab of vSphere Self-Service Backup Portal allows you to browse the guest OS file system in a VM backup and restore individual files. You can restore files from indexed and non-indexed guest OS file systems.

To restore guest OS files, follow the steps described in Performing 1-Click File Restore.

NOTE

- When you restore from non-indexed guest OS file system, mount operation is performed using mount server associated with the backup repository that stores the backup file.
- Before you restore files from a non-Windows VM, make sure that an FLR helper appliance is configured on the backup server. For more information, see Preparing for File Search and Restore (non-Windows machines).

Restoring Application Items

The **Items** tab of vSphere Self-Service Backup Portal allows you to perform item-level recovery from application-aware backups of Microsoft SQL Server databases and Oracle databases.

To restore application items, follow the steps described in the following sections:

- To restore Microsoft SQL Server databases, see Restore Procedure for SQL Server.
- To restore Oracle databases, see Restore Procedure for Oracle.

Appendix A. License Update Session Data

The table below lists the messages that can appear in the automatic license update session log. Similar messages are received as pop-ups after you force the immediate update. Recommendations for users (if applicable) are provided in the **Comment** field.

Message	Reason	Comment
"New license key has been received" "New license key has been installed" "License key has been auto-updated"	This sequence of messages means automatic license key update procedure has completed successfully.	You can open the License Information dialog in Veeam backup console or the Licensing section in Enterprise Manager to examine the details.
"License key type is not supported at the moment"	License key generation failed due to currently unsupported license type.	Currently, automatic update is supported only for licenses associated with *Hosting Rental* contract type.
"License key is invalid"	License signature (identifier) is invalid.	Contact your Veeam sales representative.
"Your existing license key is up to date"	License expiration date is more than 7 days from now.	This message could probably been issued due to an accidental attempt to update the license manually. Select to update the license key automatically, and the system will notify you on time.
"Your contract has expired, so the license key cannot be updated automatically. Please contact your Veeam sales representative to renew your contract."	Your contract has expired and needs to be renewed.	Contact your Veeam sales representative for contract renewal.
"General license key generation error has occurred"	Web licensing server did not return a new key upon request due to some other reason.	Wait for 24 hours (Veeam will re-try to update the key). Retries will take place for 1 month after key expiration date.

Appendix B. Configuring AD FS for SAML Authentication

Active Directory Federation Service (AD FS) is a hosted identity provider implemented as a feature in the Windows Server OS. It provides single sign-on capabilities for Active Directory (AD) users. If AD FS is used as the identity provider in the organization, to let AD users log in to the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal using the single sign-on service, an IT administrator must register the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal as service providers in AD FS.

To add a service provider in AD FS:

1. Obtain the service provider metadata exported from Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.
2. In AD FS, add a Relying Party Trust using the service provider metadata.
3. Edit the Claim Issuance Policy for the added Relying Party Trust to add an issuance transform rule with the following properties:
   - **Claim rule template** = *Transform an Incoming Claim*
   - **Incoming claim type** = *UPN*
   - **Outgoing claim type** = *NameID*
   - **Outgoing name ID format** = *Persistent Identifier*
4. [Optional] To provide single sign-on capabilities to AD groups, add to the Claim Issuance Policy an issuance transform rule with the following properties:
   - **Claim rule template** = *Send Group Membership as a Claim*
   - **User's group** = *<Name>*

     where *<Name>* is a name of the AD group that includes users that will access the service provider.

     When a user that belongs to the specified group attempts to access the service provider, the identity provider will issue an authentication assertion confirming that the user belongs to the group.
   - **Outgoing claim type** = *Group*

     Alternatively, if a different value is specified for the **Group claim type** option of advanced SAML settings in Enterprise Manager, the same value must be specified as the outgoing claim type in AD FS.
   - **Outgoing claim value** = *<Name>*

     where <Name> is a name of the group that will be returned to the service provider in authentication assertions.

     This value can be different from the **User's group** value, for example, if you do not want the service provider to display AD group names. This value must be the same as the name of the account of the External Group type added in Enterprise Manager. For more information, see Configuring Accounts and Roles and Adding Tenant Account.

   For example, you want to provide single sign-on capabilities to users that belong to the *Backup* AD group. In Enterprise Manager, you have the *EnterpriseUsers* account of the External Group type, and the default group claim type is specified in advanced SAML settings.

To allow these users to log in to Enterprise Manager with the single sign-on service, you must create an issuance transform rule with the following properties:

- **Claim rule template** = *Send Group Membership as a Claim*
- **User's group** = *Backup*
- **Outgoing claim type** = *Group*
- **Outgoing claim value** = *EnterpriseUsers*

Veeam Explorers

Version 11

User Guide

October, 2021

© 2021 Veeam Software.

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

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

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

Contents

CONTACTING VEEAM SOFTWARE 9
ABOUT THIS DOCUMENT 10
VEEAM EXPLORERS OVERVIEW 11
VEEAM EXPLORER FOR MICROSOFT ACTIVE DIRECTORY 12
Planning and Preparation 13
System Requirements 14
Used Ports 15
Required Permissions 16
Required Backup Job Settings 17
Considerations and Limitations 18
Launching Application and Exploring Backups 20
Understanding User Interface 21
Browsing, Searching and Viewing Items 23
Standalone Databases Management 26
Adding Standalone Databases 27
Removing Standalone Databases 28
Data Restore 29
Restoring Objects 30
Restoring Containers 38
Using 1-Click Restore 46
Data Export 49
Exporting Objects 50
Exporting Containers 51
Using 1-Click Export 53
Data Compare 54
Comparing Active Directory Containers 55
Comparing Object Attributes 57
Enabling Extended Logging 59
VEEAM EXPLORER FOR MICROSOFT SQL SERVER 60
Planning and Preparation 61
System Requirements 62
Used Ports 64
Required Permissions 67
Required Backup Job Settings 68
Considerations and Limitations 69
Launching Application and Exploring Backups 71

Understanding User Interface 72
Understanding Mounting 74
Understanding Veeam SQL Restore Service 75
Viewing Database Information 76
General Application Settings 77
Configuring Staging SQL Server 78
Enabling Extended Logging 81
Standalone Databases Management 82
Adding Standalone Databases 83
Removing Standalone Databases 85
Data Restore 86
Restoring Single Database 87
Restoring Multiple Databases 97
Restoring Database Schema and Data 102
Restoring Latest or Point-in-Time State 112
Data Publishing 117
Publishing to Specified Server 118
Publishing Latest or Point-in-Time State 125
Unpublishing Databases 130
Exporting as BAK 131
Refreshing Database Status 133
Instant Recovery 134
How It Works 135
Instant Recovery of Multiple Databases 136
Instant Recovery of Latest State 143
Instant Recovery of Point-in-Time State 145
Instant Recovery to Another Server 151
Switchover 160
Managing Instant Recovery Session 162
Data Export 166
Export as MDF 167
Export as BAK 179
Database Schema and Data Export 191
SQL Server Database Operations 199
VEEAM EXPLORER FOR ORACLE 202
Planning and Preparation 203
System Requirements 204
Used Ports 205
Required Permissions 208

Required Backup Job Settings 209
Considerations and Limitations 210
Launching Application and Exploring Backups 213
Understanding User Interface 214
Understanding Mounting 216
Viewing Database Information 217
General Application Settings 219
Configuring Staging Oracle Server 220
Enabling Extended Logging 224
Exploring Oracle Backups 225
Exploring Application-Enabled Backups 226
Exploring Non-Application Enabled Backups 227
Exploring RMAN Backups 232
Data Restore 233
Restoring Single Database and Data Guard 234
Restoring Latest or Point-in-Time State 242
Restoring Multiple Databases 246
Restoring RMAN Backups 254
Data Publishing 264
Publishing to Specified Server 265
Publishing Latest or Point-in-Time State 272
Unpublishing Databases 277
Exporting as RMAN Backup 278
Refreshing Database Status 279
Instant Recovery 280
How It Works 281
Instant Recovery of Multiple Databases 282
Instant Recovery of Latest State 290
Instant Recovery of Point-in-Time State 292
Instant Recovery to Another Server 298
Switchover 308
Managing Instant Recovery Session 310
Data Export 315
Export as RMAN Backup 316
Export Database Files 325
VEEAM EXPLORER FOR MICROSOFT EXCHANGE 333
Planning and Preparation 334
System Requirements 335
Used Ports 336

Required Permissions 338
Required Backup Job Settings 340
Considerations and Limitations 341
Launching Application and Exploring Backups 342
Understanding User Interface 343
Browsing, Searching and Viewing Items 345
General Application Settings 349
Configuring Extensible Storage Engine 350
Configuring SMTP Settings 351
Configuring Advanced Settings 352
Standalone Databases Management 353
Adding Microsoft Exchange Stores 354
Adding Veeam Backup for Microsoft Office 365 Server 355
Adding Veeam Backup for Microsoft Office 365 Service Provider 356
Removing Standalone Databases 358
Data Restore 359
Restore to Office 365 Organizations 360
Restore to On-Premises Microsoft Servers 376
1-Click Restore 387
Data Export 395
Exporting to Custom Location 396
Using 1-Click Export 398
Receiving Export Reports 401
Data Compare 403
Compare to Office 365 Organizations 404
Compare to On-Premises Microsoft Servers 408
Saving Microsoft Exchange Items 411
Sending Microsoft Exchange Items 413
VEEAM EXPLORER FOR MICROSOFT SHAREPOINT 415
Planning and Preparation 416
System Requirements 417
Used Ports 418
Required Permissions 420
Required Backup Job Settings 422
Staging SQL Server 423
Considerations and Limitations 424
Launching Application and Exploring Backups 428
Understanding User Interface 429
Browsing, Searching and Viewing Items 431

General Application Settings 435
Configuring Staging SQL Server 436
Configuring Custom Lists 439
Configuring SMTP Settings 442
Configuring Advanced Settings 443
Standalone Databases Management 444
Adding Microsoft SharePoint Databases 445
Adding Veeam Backup for Microsoft Office 365 Databases 446
Adding Veeam Backup for Microsoft Office 365 Server 447
Adding Veeam Backup for Microsoft Office 365 Service Provider 448
Removing Standalone Databases 450
Data Restore 451
Restoring Microsoft SharePoint Sites 452
Restoring Microsoft SharePoint Document Libraries and Lists 460
Restoring Microsoft SharePoint Documents and List Items 468
Data Export 476
Exporting Microsoft SharePoint Data 477
Importing Microsoft SharePoint Data 478
Saving Microsoft SharePoint Documents and Libraries 479
Sending Microsoft SharePoint Documents and Libraries 480
Appendix A: Unsupported SharePoint Lists 482
VEEAM EXPLORER FOR MICROSOFT ONEDRIVE FOR BUSINESS 486
Planning and Preparation 487
Launching Application and Exploring Backups 488
Understanding User Interface 489
Browsing, Searching and Viewing Items 491
General Application Settings 495
Configuring SMTP Settings 496
Configuring Advanced Settings 497
Standalone Databases Management 498
Adding Veeam Backup for Microsoft Office 365 Databases 499
Adding Veeam Backup for Microsoft Office 365 Server 500
Adding Veeam Backup for Microsoft Office 365 Service Provider 501
Removing Standalone Databases 503
Restoring Microsoft OneDrive Data 504
Restoring Single OneDrive 505
Restoring Multiple OneDrives 510
Copying Microsoft OneDrive Data 516
Step 1. Launch Restore Wizard 517

Step 2. Select Authentication Method 518
Step 3. Log In to Office 365 520
Step 4. Specify Target User 521
Step 5. Specify Target Folder 522
Step 6. Specify Restore Options 523
Saving Microsoft OneDrives 524
Saving Microsoft OneDrive Documents and Folders 526
Sending Microsoft OneDrive Documents 527
VEEAM EXPLORER FOR MICROSOFT TEAMS 529
Planning and Preparation 530
System Requirements 531
Used Ports 532
Required Permissions 533
Considerations and Limitations 534
Launching Application and Exploring Backups 535
Understanding User Interface 536
Browsing, Searching and Viewing Items 538
General Application Settings 543
Configuring SMTP Settings 544
Configuring Advanced Settings 545
Standalone Databases 546
Adding Veeam Backup for Microsoft Office 365 Databases 547
Adding Veeam Backup for Microsoft Office 365 Server 548
Adding Veeam Backup for Microsoft Office 365 Service Provider 549
Removing Standalone Databases 551
Data Restore 552
Restoring Teams 553
Restoring Channels and Tabs 562
Restoring Posts 570
Restoring Files 576
Data Export 583
Exporting Multiple Posts 584
Exporting Individual Posts 586
Saving Posts 588
Saving Files 590
Sending Posts and Files 592

Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

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

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

About This Document

This document provides general information on how to use the Veeam Explorers suite consisting of the following applications:

- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Oracle
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft OneDrive for Business
- Veeam Explorer for Microsoft Teams

Information in this document is applicable to each Veeam Explorer that comes as part of Veeam Backup & Replication 11 or Veeam Backup for Microsoft Office 365 5.0 until it is replaced with a newer version of the product.

Intended Audience

This user guide is intended for IT administrators, consultants, analysts and any other IT professionals.

Veeam Explorers Overview

Veeam Explorers Suite extends the functionality of Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 and allows you to restore or export your data from backup or replica files.

Veeam Explorers Suite consists of the following applications:

- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Oracle
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft OneDrive for Business
- Veeam Explorer for Microsoft Teams

Veeam Explorers are distributed as part of Veeam Backup & Replication and Veeam Backup for Microsoft Office 365, and you do not need to install them separately. You also do not need to purchase any additional license to use Veeam Explorers: the available feature set for each Veeam Explorer depends entirely on the installed edition of Veeam Backup & Replication or Veeam Backup for Microsoft Office 365. For information about how to deploy Veeam products, see the following sections:

- Deployment section of the Veeam Backup & Replication User Guide
- Deployment section of the Veeam Backup for Microsoft Office 365 User Guide

To recover VMware VM data directly from storage snapshots, use Veeam Explorer for Storage Snapshots, as described in Veeam Explorer for Storage Snapshots.

Veeam Explorer for Microsoft Active Directory

Veeam Explorer for Microsoft Active Directory allows you to restore and export Active Directory objects and containers from backups created in Veeam Backup & Replication.

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft Active Directory.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft Active Directory.

Component	Requirement
Microsoft Active Directory Domain Services	For more information about supported operating systems, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

IMPORTANT

Consider the following:

- Database files created by the domain controller can be opened for object recovery with Veeam Explorer for Active Directory only if Veeam Explorer is installed on a Windows machine with the same OS version or higher that the version of that domain controller OS.
- To open database files, Veeam Explorer for Microsoft Active Directory uses a service dynamic link library (`esent.dll`) which is installed with Microsoft Active Directory Domain Services and can be found in the *%SystemRoot%* directory. The `Esent.dll` file on a machine with Veeam Explorer must be of the same version as that of Microsoft Active Directory Domain Services that was used to create database files.

Used Ports

The following table lists network ports that must be opened to manage inbound/outbound traffic.

From	To	Protocol	Port	Notes
Veeam Backup Server / Standalone Console	**Microsoft Active Directory VM Guest OS**	TCP	135	Manages communication between the domain controller and Veeam backup server.
		TCP, UDP	389	Utilized for LDAP connections.
		TCP	636, 3268, 3269	
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	The dynamic RPC range that is used by the runtime coordination process which is deployed on a VM guest OS for application-aware image processing (when working over the network, not over VIX API). For more information, see this Microsoft article.

Required Permissions

The following table lists required permissions for user accounts to back up and restore Microsoft Active Directory data.

Operation	Required Roles and Permissions
Backup	For more information, see the Required Permissions section of the Veeam Backup & Replication User Guide.
Restore	The account being used must be a member of the *Domain Admins* group and the *Exchange Organization Management* group.

Assigning Role with PowerShell

To assign the **Organization Management** role via PowerShell, run the following cmdlet.

```
Add-RoleGroupMember "Organization Management" -Member "<user_name>"
```

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft Active Directory.

General

- When Veeam Explorer for Microsoft Active Directory is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup and Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft Active Directory does not support restore via *PSDirect*, *VIX* or *Sphere API*.
- Data can only be restored back to the original domain. Cross-domain restore is not supported.
- Veeam Explorer for Microsoft Active Directory supports restore of both mailbox-enabled objects (including *hard-deleted items* and *Online Archives*), and *mail-enabled objects* for the following Microsoft Exchange versions: *Microsoft Exchange Server 2019*, *Microsoft Exchange Server 2016*, *Microsoft Exchange Server 2013*, *Microsoft Exchange Server 2010 SP1* and higher. For other Microsoft Exchange versions, restore of *mailbox-enabled* objects is not supported (only *mail-enabled* objects can be restored).
- To restore passwords, Veeam Explorer for Microsoft Active Directory uses the registry database. To restore passwords, make sure the *System registry hive* is available. The default location of the hive is *%systemroot%|System32|Config*. When restoring an Active Directory database from the Active Directory backup using *Veeam file-level restore*, the registry hive will be located automatically. When restoring from an imported backup or from VeeamZIP backups, make sure that the system registry hive and the *.dit* file are located in the same directory.
- If you plan to restore database items from an *Active Directory Domain Services* server running *Microsoft Windows ReFS*, consider that a Veeam backup server or a management console must be installed on *Microsoft Windows Server 2012* or higher. To restore from a server running *Microsoft Windows ReFS 3.x*, a Veeam backup server or a management console must be installed on *Microsoft Windows Server 2016*.
- Restore of *Group Policy objects*, *AD-integrated DNS records* and objects from the *Configuration partition* is supported in the *Enterprise* and *Enterprise Plus* editions only.
- To restore security attributes such as *objectSID* and *objectGUID*, Veeam uses existing tombstone objects on the target Active Directory server. Make sure that the **AD Recycle Bin** feature is disabled in the target domain. If no tombstone objects exist on the target server, Active Directory will assign new *objectSID* and *objectGUID* attributes to objects restored from the backup file.
- To restore business-critical objects for which the tombstone object is missing, you can perform authoritative restore of the entire domain from the old DC backups. For more information on tombstone objects, see this Microsoft article.
- Always use backups that are newer than the tombstone lifetime interval for the Active Directory forest. To determine a tombstone lifetime interval, you can use *ADSIEdit* or *Dsquery*. For more information. see this Microsoft article.
- When you move an object from one domain to another within a forest (for example, using the *Movetree.exe* utility or any other 3rd party tool), no tombstone for this object will remain in the source Active Directory; such an object cannot be fully recovered to the original domain.

Export

- Veeam uses *Lightweight Data Interchange Format* to save Active Directory objects and containers to *.ldf* files. You can make an *.ldf* file available to the Active Directory Domain Services server by importing it with the *ldifde* utility. For more information. see this Microsoft article.
- Veeam Explorer for Microsoft Active Directory does not support exporting passwords.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Active Directory and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created in Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

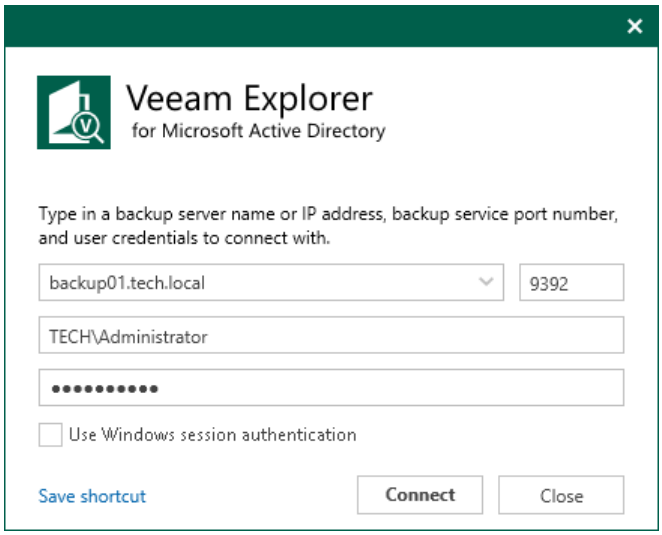
- Go to **Start**, click **Veeam Explorer for Microsoft Active Directory** and manually open Active Directory databases, as described in the Adding Standalone Microsoft Active Directory Databases section.

When starting the application from the **Start** menu, specify the following:

- The domain name or IP address of the backup server to which you want to connect
- The port number
- User credentials

  The account must be a member of the *Local Administrator* group on a target server. To use the account under which Veeam Explorer for Microsoft Active Directory is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



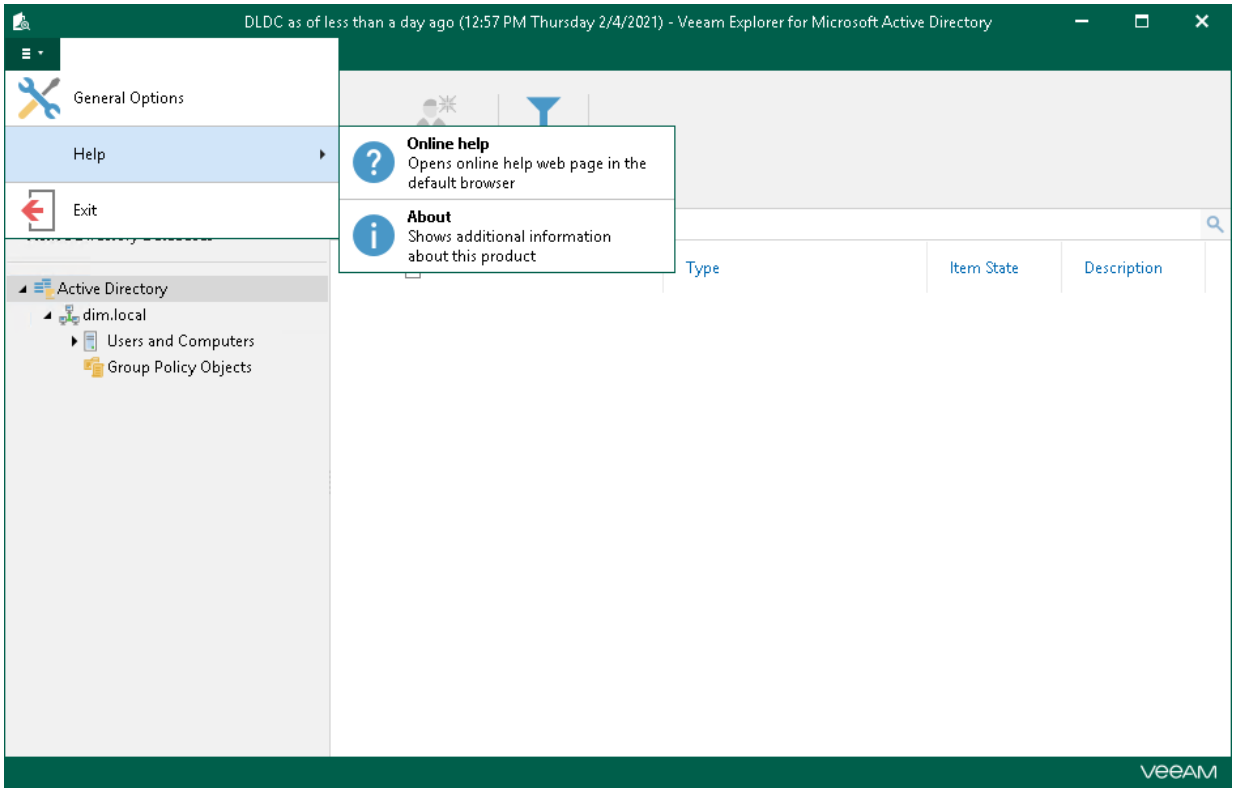
Understanding User Interface

Veeam Explorer for Microsoft Active Directory provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

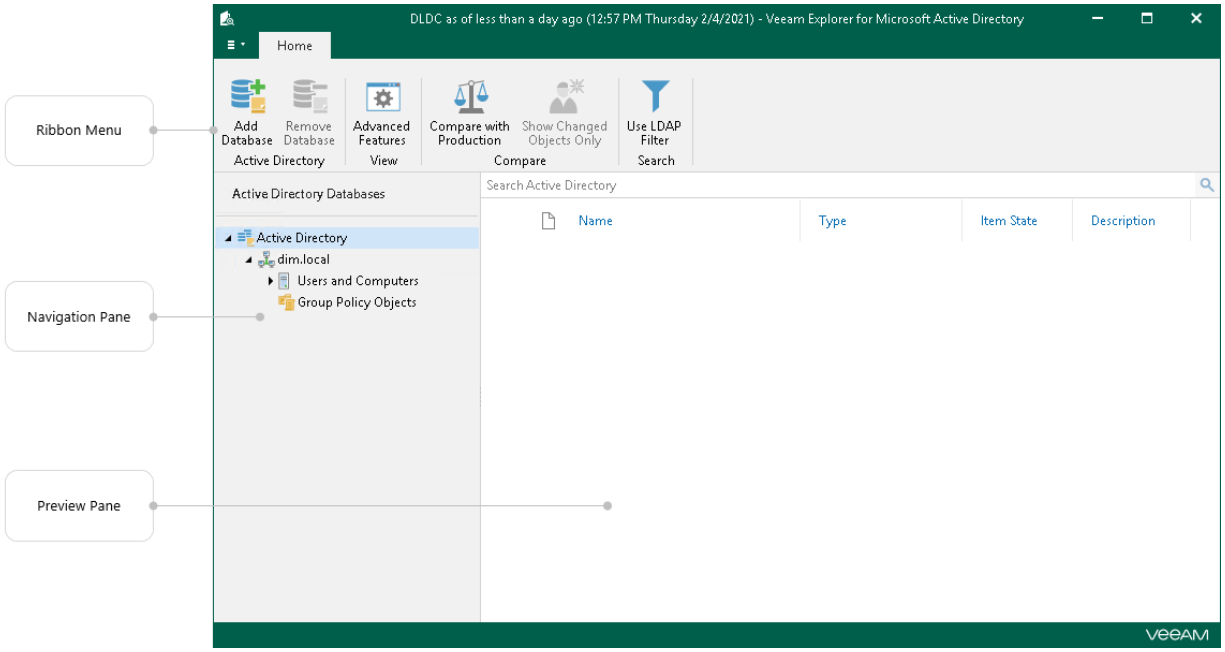
- **General Options**. Allows you to configure program options.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows information about the product.
- **Exit**. Closes the program.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

Continue with this section to learn more about:

- Browsing backup content
- Searching for objects in a backup file

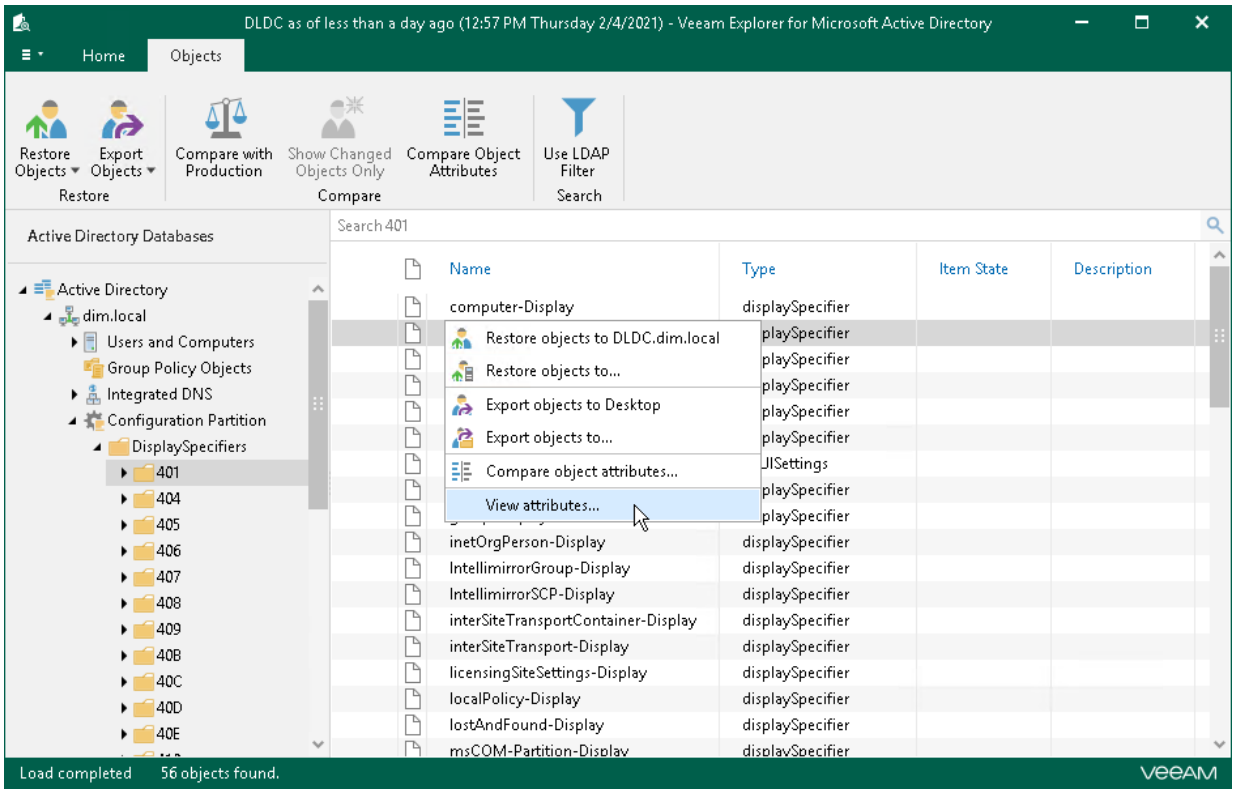
Browsing

To view the contents of a backup file, use the navigation pane which shows you the database structure containing your active directory objects.

After you select an object in the navigation pane, you can see its content in the preview pane.

Right-click an object and select **View attributes** to view object attributes. To copy necessary attributes to the clipboard, select an attribute and press **CTRL+C** on the keyboard. Multiple selection is also supported.

> **NOTE**
>
> Due to organizational and security purposes, recovery of *Domain Controllers* objects is not supported.



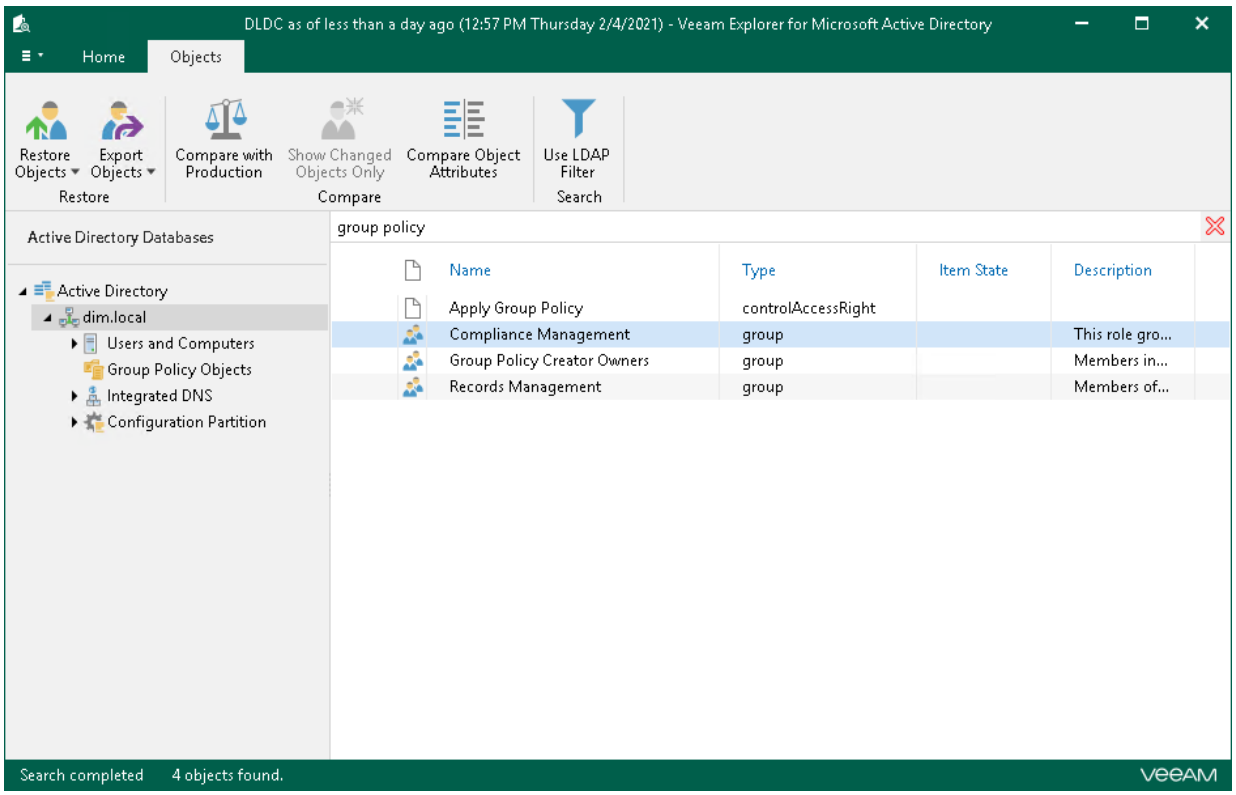
Searching

The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find your data.
2. Enter a search query to the search field at the top of the preview pane and click the search button.

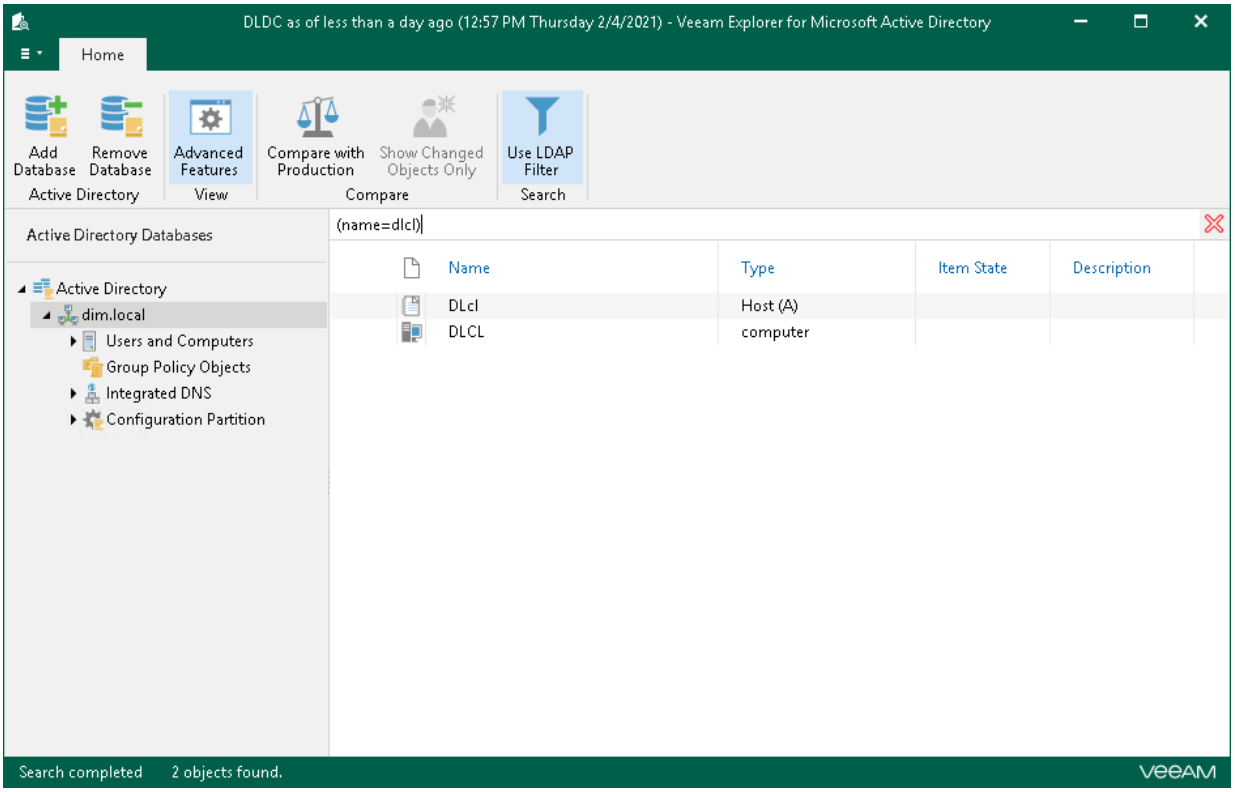
> **NOTE**
>
> To find the exact phrase, use double quotes. For example, *"group policy"*.



Using LDAP Queries

To use the LDAP search query, do the following:

1. In the preview pane, select a container.
2. On the ribbon menu, click **Use LDAP Filter**.
3. In the search field, enter an LDAP query and click the search button.



Standalone Databases Management

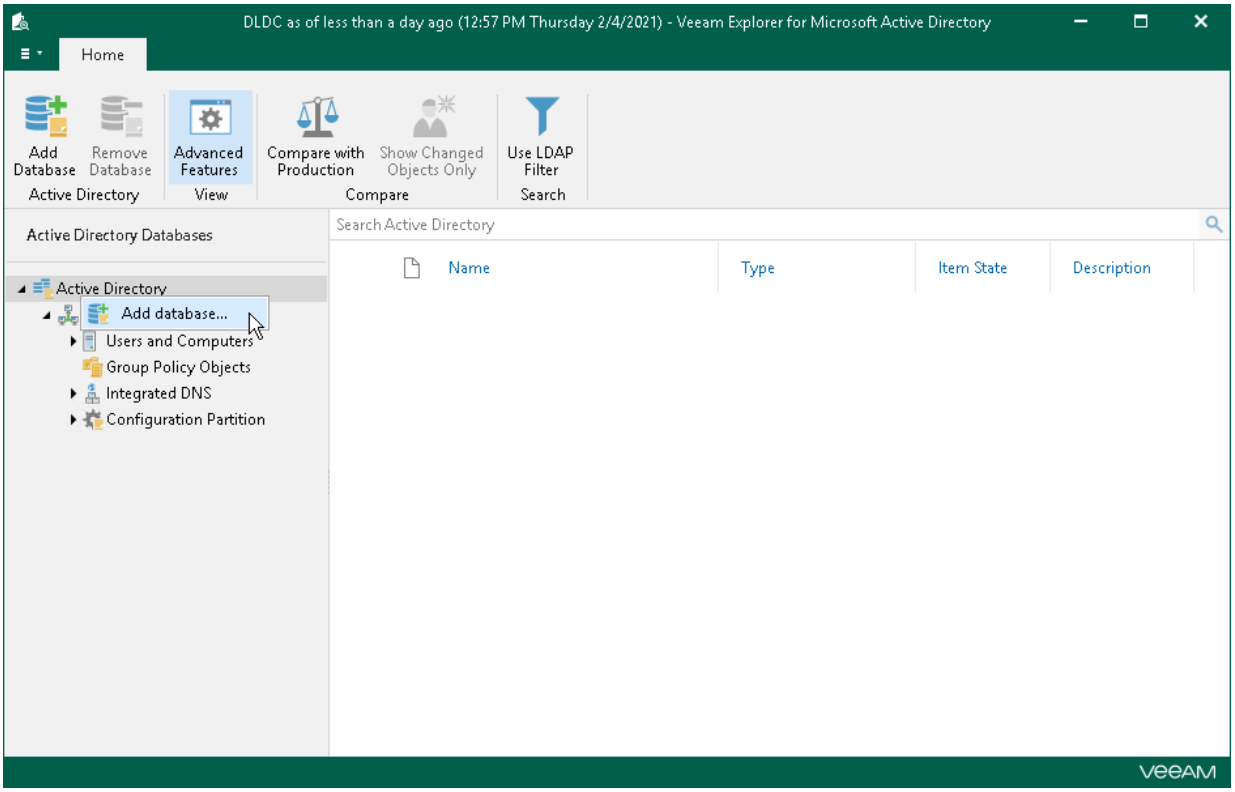
Continue with this section to learn more about adding and removing Microsoft Active Directory databases.

> **IMPORTANT**
>
> Make sure the database you are adding to the Veeam Explorer scope was not locked by another process.

Adding Standalone Databases

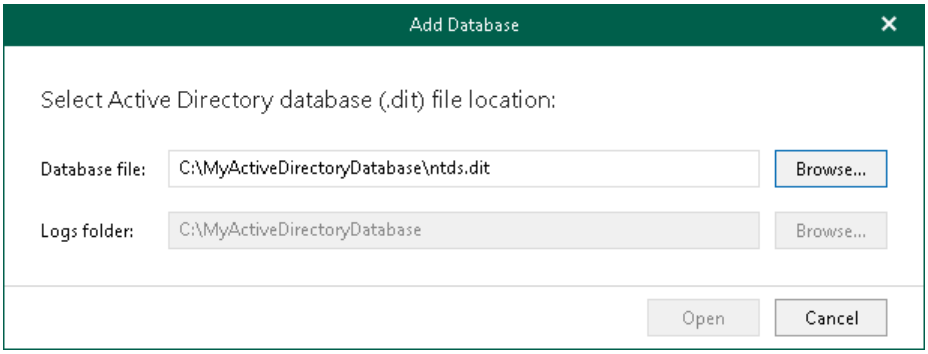
To add a standalone Active Directory database manually, do the following:

1. Select the root **Active Directory** node in the navigation pane and click **Add Database** on the toolbar or right-click the **Active Directory** node and select **Add database**.



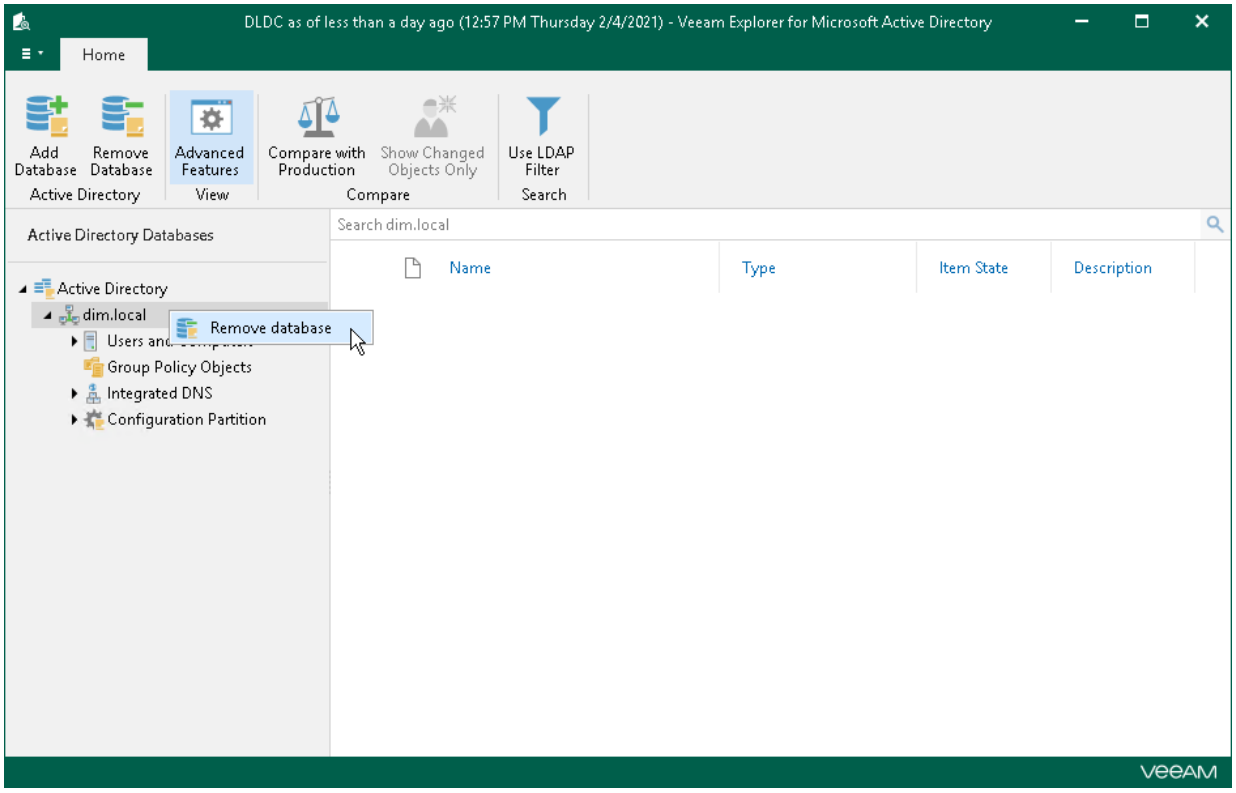
2. Specify the location of the Active Directory database file and folder that contains associated transaction log files (*Edb.log* and *Edb.chk*).

   By default, the Active Directory database file (`NTDS.DIT`) is located in the `%SystemRoot%\NTDS` directory. Make sure that the system registry hive is located in the same place.



Removing Standalone Databases

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove database**.



Data Restore

Continue with this section to learn more about restoring Active Directory objects and containers.

> **TIP**
>
> Before restoring data, make sure to read Considerations and Limitations.

Restoring Objects

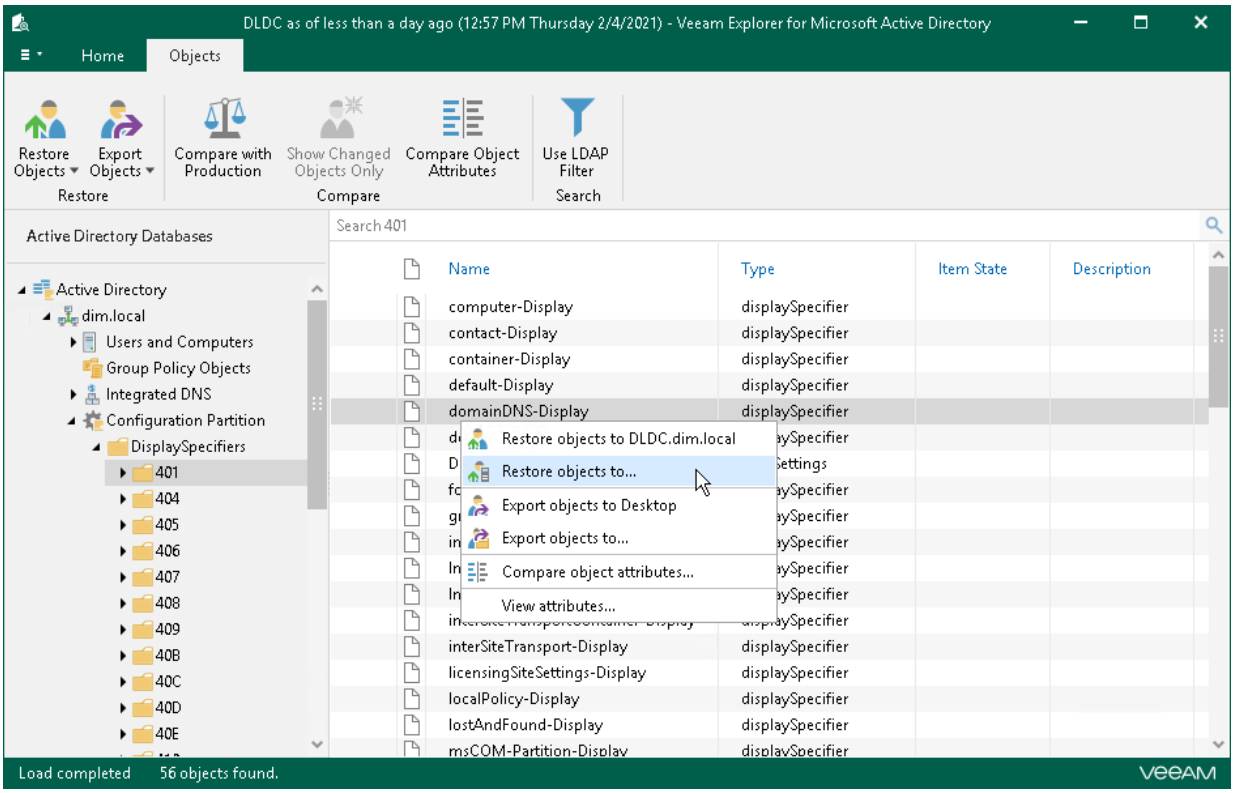
To restore Active Directory objects, do the following:

1. Launch the Restore wizard.
2. Specify connection parameters.
3. Specify the restore location.
4. Specify password restore options.
5. Specify the account state.
6. Specify restore options.
7. Specify attributes to restore.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the preview pane, select an object.
2. On the **Objects** tab, select **Restore Objects** > **Restore objects to** *<server_name>* or right-click an object and select **Restore objects to** *<server_name>*.



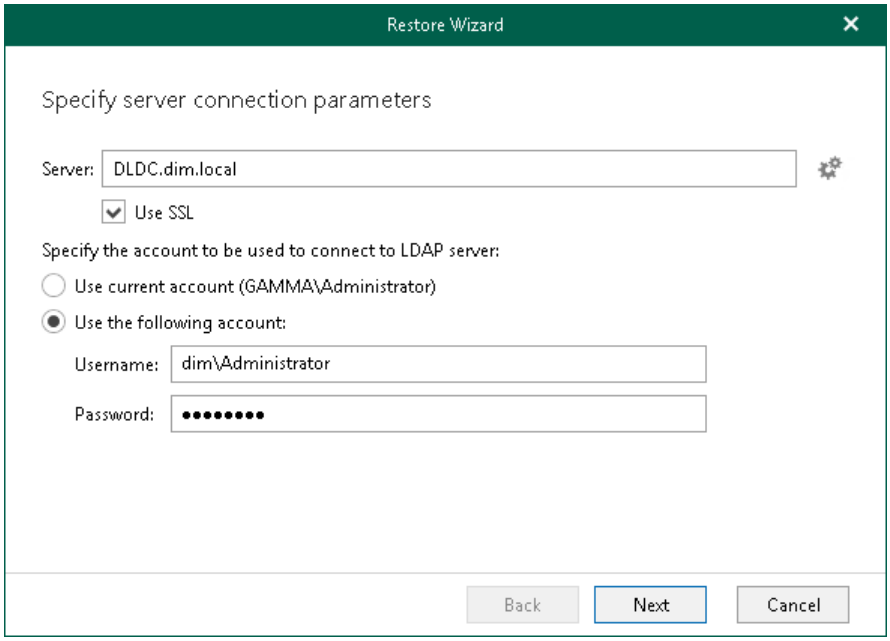
Step 2. Specify Connection Parameters

At this step of the wizard, specify the following:

- A target production server to which you want to restore your data.

  Select the **Use SSL** check box to establish a secure SSL connection.

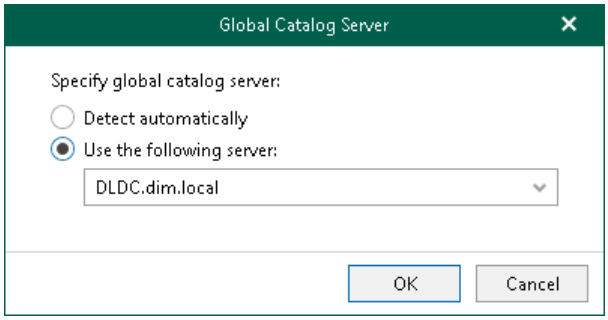
- User credentials to connect to the LDAP server.



Global Catalog Server

To specify a Global Catalog server, click the button on the right side of the **Server** field and choose either of the following options:

- **Detect automatically**. To detect a server automatically.
- **Use the following server**. To choose a server from the list.

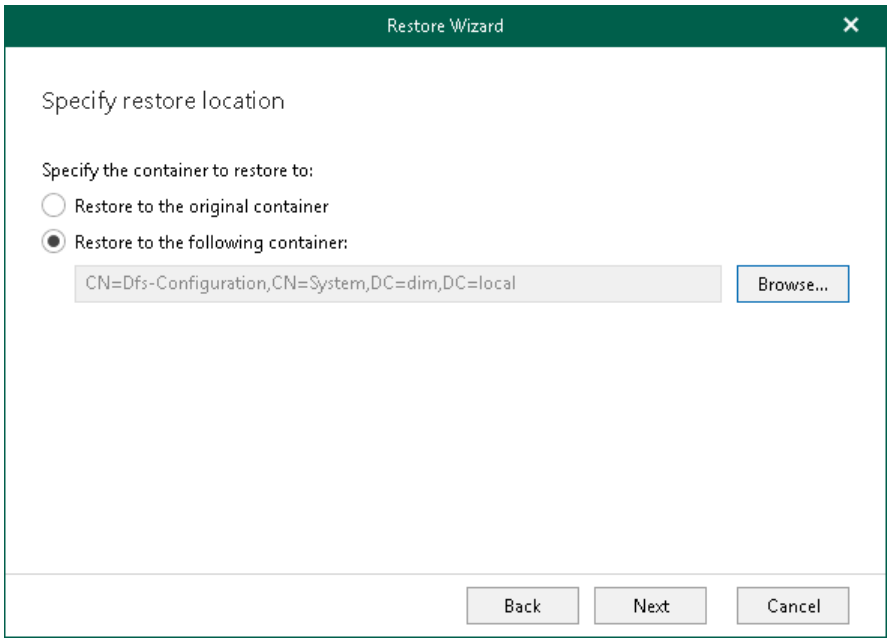


Step 3. Specify Restore Location

At this step of the wizard, select a container to which you want to restore the objects.

You can select the following:

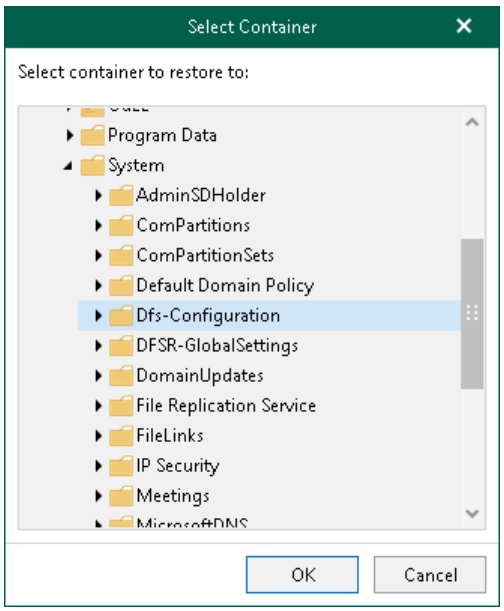
- **Restore to the original container**. To restore data to the original container in your production environment.
- **Restore to the following container**. To select a different container, as described in Browsing Container.



> **TIP**
>
> If a container that is being restored was not found in the production environment, it will be restored anew.

Browsing Container

To select a different container, click **Browse** and choose a container you want to use.



Step 4. Specify Password Restore Options

At this step, select one of the following options:

- **Restore password**. To restore the password from the backup file.
- **Set password to**. To set a new password.
- **Do not restore password**. To skip restoring the password.

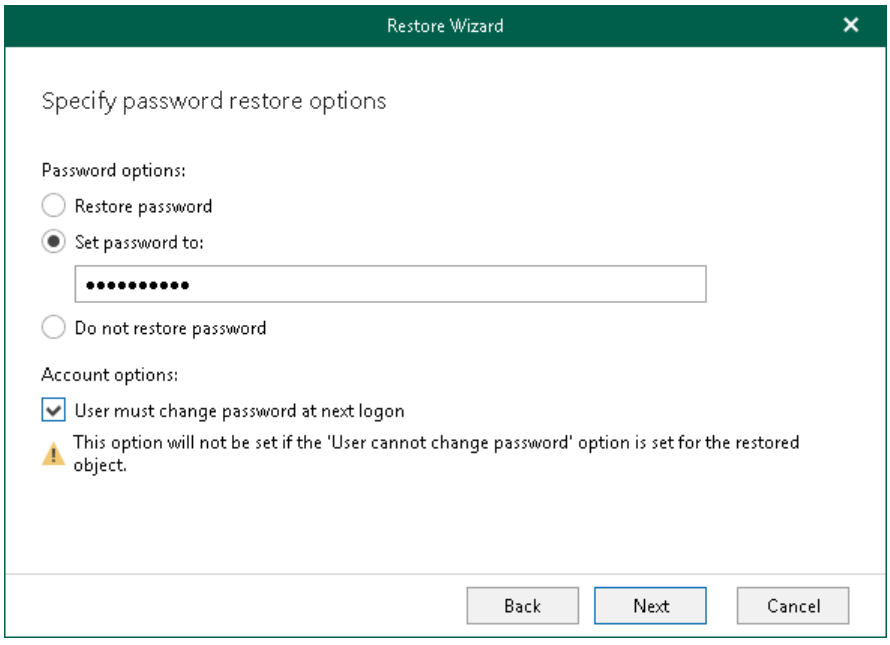
  This option will not make any changes to the currently configured passwords in your environment.

Consider the following:

- When providing a new password, check that it complies with the password policy in your production environment.
- If you select **Restore password** or **Set password to** options, you may also request a user to change the password at next log on.

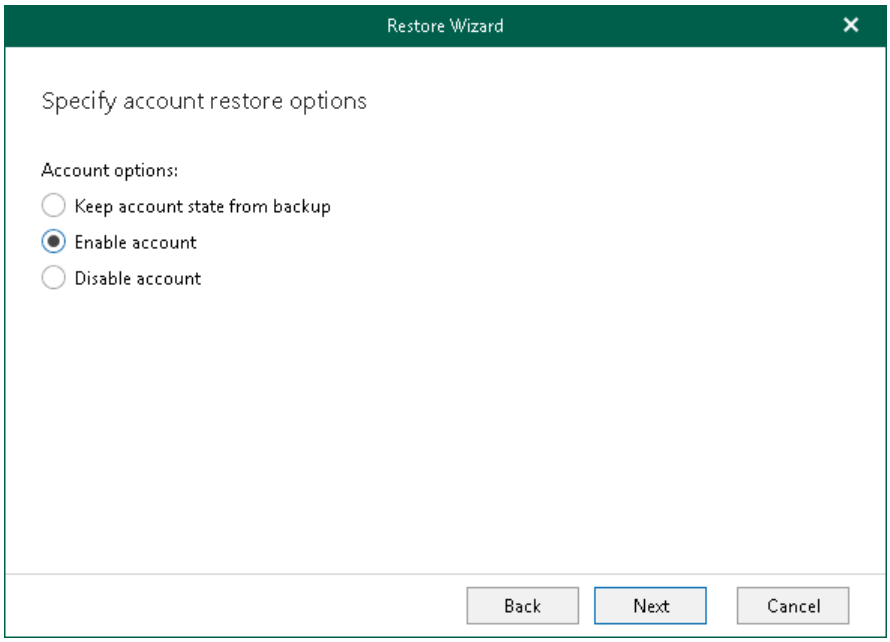
  Mind that this setting will not take effect if a user is not allowed to change the password due to security limitations.
- When restoring multiple accounts, a new password will be set for all the accounts altogether.
- To restore account passwords, Veeam Explorer for Microsoft Active Directory uses registry database. Make sure that the *System* registry hive is available.

  The default location is `%systemroot%\System32\Config`.
- When restoring Active Directory database from an Active Directory backup file using Veeam file-level restore, the registry hive will be located automatically. Otherwise, make sure the system registry hive is located in the same folder as `.DIT` file.



Step 5. Specify Account State

At this step of the wizard, specify whether you want to keep the account state as it is in the backup file or select **Enabled** or **Disabled** to assign a state you need.



Step 6. Specify Restore Options

At this step of the wizard, specify restore options.

You can select the following:

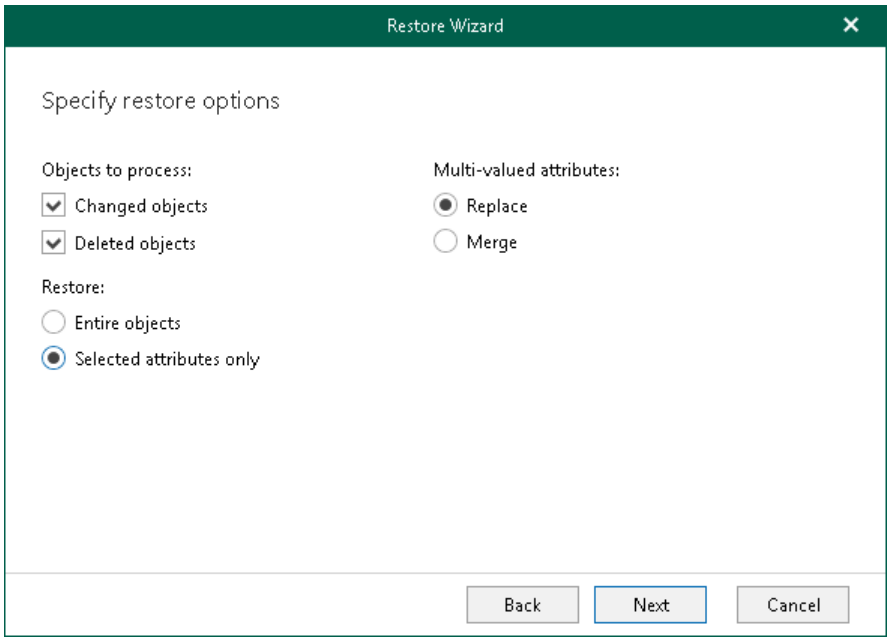
- **Objects to process**:
  - **Changed objects**. To restore changed objects.
  - **Deleted objects**. To restore deleted objects.
- **Restore**:
  - **Entire objects**. To restore entire objects collection.
  - **Selected attributes only**. To select particular attributes.

    When selecting **Selected attributes only**, you will be offered to choose the attributes you want to restore in the next step.
- **Multi-valued attributes**:
  - **Replace**. To replace production data with that of a backup file.
  - **Merge**. To merge existing data with that of a backup file.

  By default, multi-valued attributes will be replaced, not merged.

NOTE

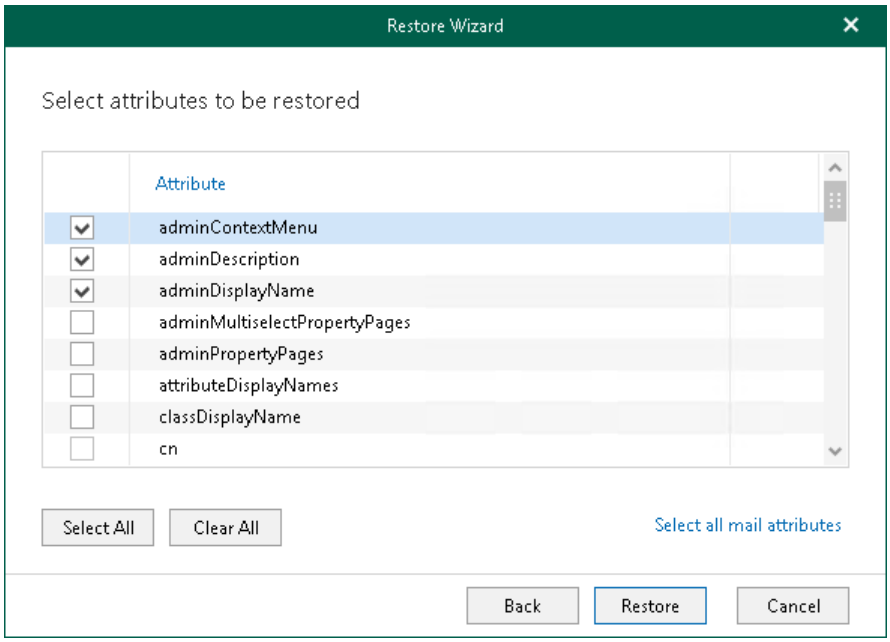
- When working with Active Directory 2016, this dialog will also include the **Restore expiration time** option, which allows you to restore expiration time for linked attributes.
- Users cannot change recovery settings for disabled attributes. Such attributes will be either restored or skipped according to the default configuration.



Step 7. Specify Attributes to Restore

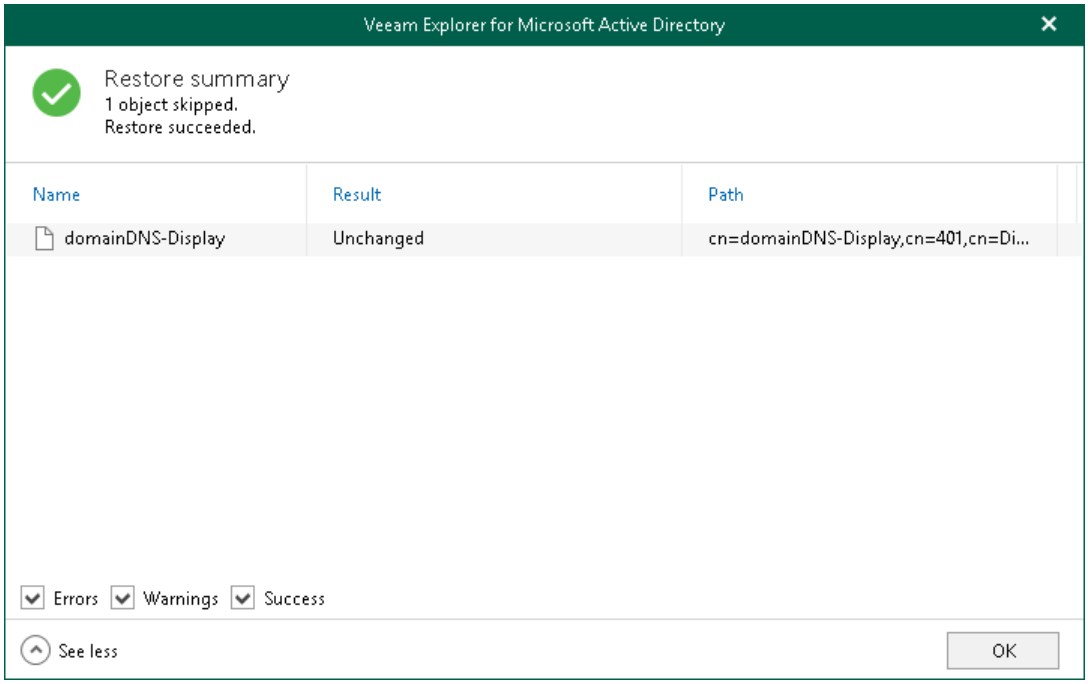
At this step of the wizard, select attributes you want to restore.

This step is available only if you have chosen the **Selected attributes only** option at the previous step.



After the restore process is complete, review the results shown in the **Restore summary** dialog.

You can select whether to display all types of notifications or only those you need by selecting/deselecting the corresponding check boxes in the lower-left corner of the dialog.



Restoring Containers

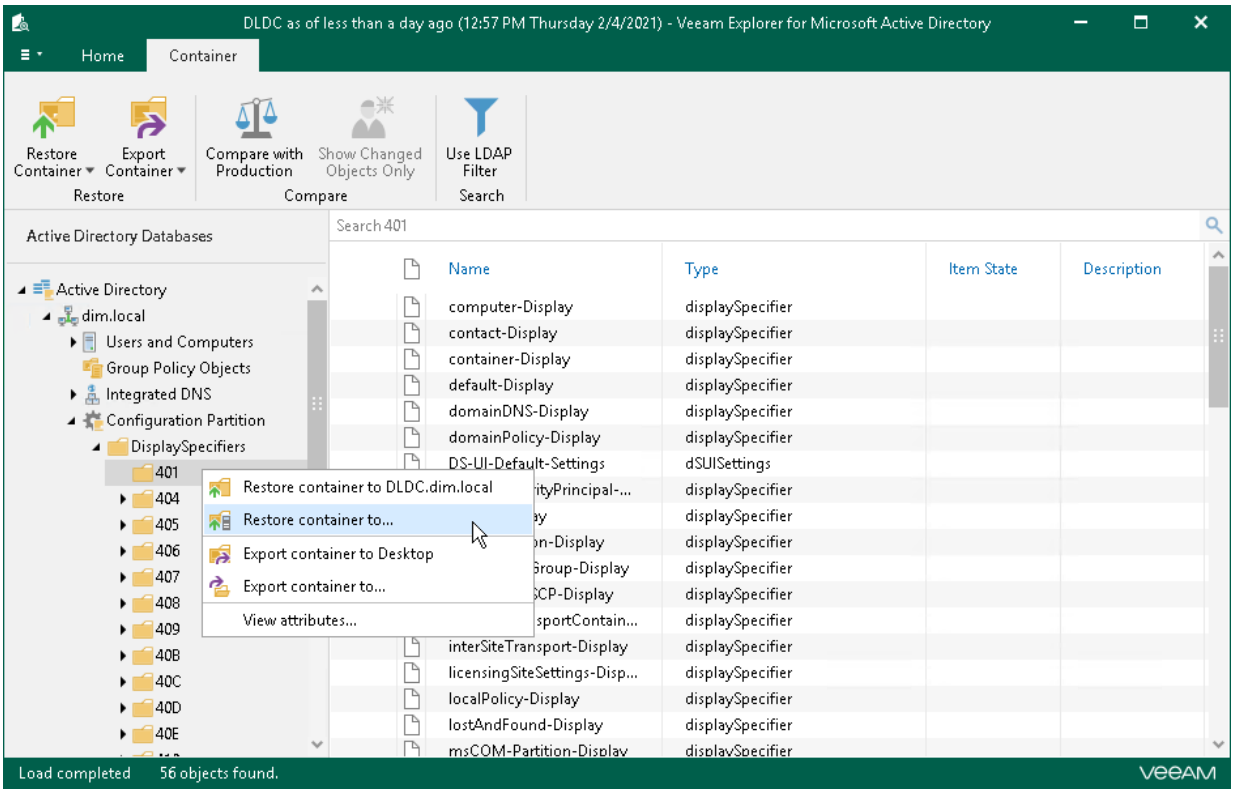
To restore Active Directory containers, do the following:

1. Launch the Restore wizard.
2. Specify connection parameters.
3. Specify the restore location.
4. Specify password restore options.
5. Specify the account state.
6. Specify restore options.
7. Specify attributes to restore.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the preview pane, select an object.
2. On the **Container** tab, select **Restore Container** > **Restore container to** or right-click a container and select **Restore container to**.



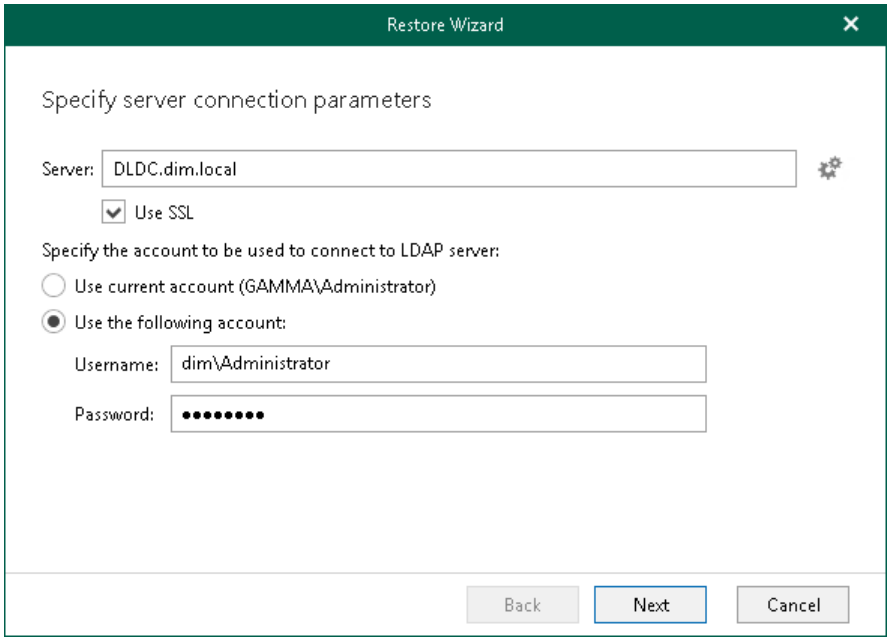
Step 2. Specify Connection Parameters

At this step of the wizard, specify the following:

- A target production server to which you want to restore your data.

  Select the **Use SSL** check box to establish a secure SSL connection.

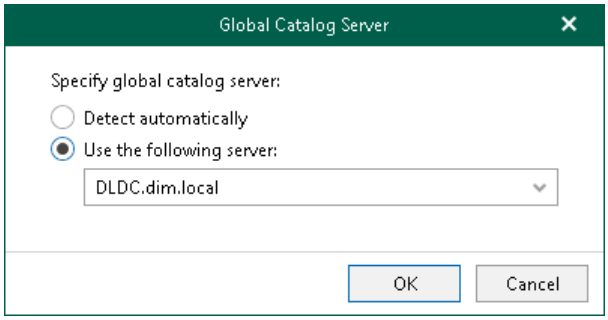
- User credentials to connect to the LDAP server.



Global Catalog Server

To specify a Global Catalog server, click the button on the right side of the **Server** field and choose either of the following options:

- **Detect automatically**. To detect a server automatically.
- **Use the following server**. To choose a server from the list.

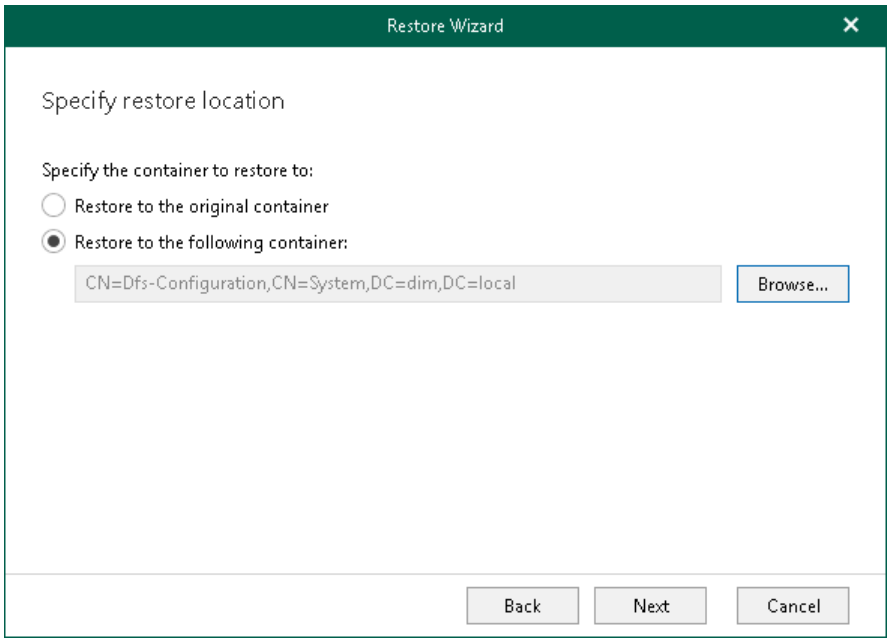


Step 3. Specify Restore Location

At this step of the wizard, select a container to which you want to restore the objects.

You can select the following:

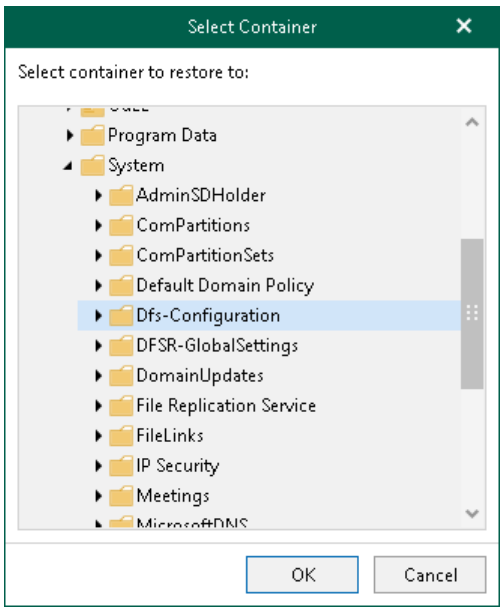
- **Restore to the original container**. To restore data to the original container in your production environment.
- **Restore to the following container**. To select a different container, as described in Browsing Container.



> **TIP**
>
> If a container that is being restored was not found in the production environment, it will be restored anew.

Browsing Container

To select a different container, click **Browse** and choose a container you want to use.



Step 4. Specify Password Restore Options

At this step, select one of the following options:

- **Restore password**. To restore the password from the backup file.
- **Set password to**. To set a new password.
- **Do not restore password**. To skip restoring the password.

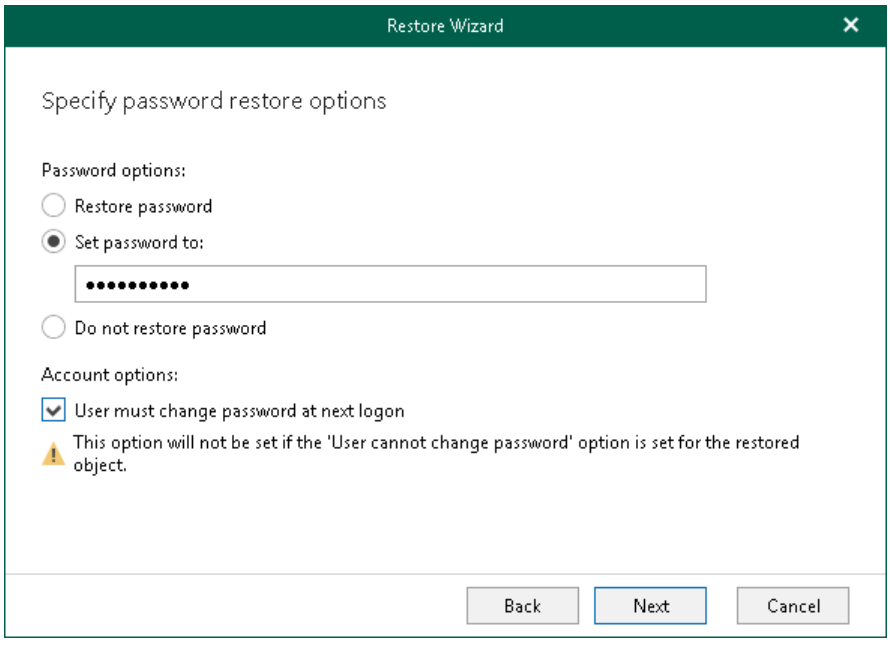
  This option will not make any changes to the currently configured passwords in your environment.

Consider the following:

- When providing a new password, check that it complies with the password policy in your production environment.
- If you select **Restore password** or **Set password to** options, you may also request a user to change the password at next log on.

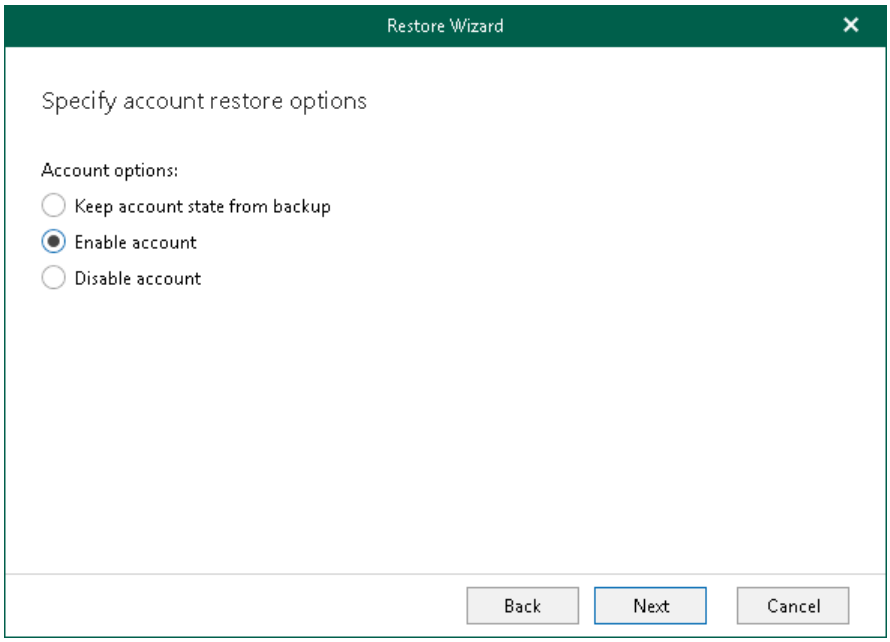
  Mind that this setting will not take effect if a user is not allowed to change the password due to security limitations.
- When restoring multiple accounts, a new password will be set for all the accounts altogether.
- To restore account passwords, Veeam Explorer for Microsoft Active Directory uses registry database. Make sure that the *System* registry hive is available.

  The default location is `%systemroot%\System32\Config`.
- When restoring Active Directory database from an Active Directory backup file using Veeam file-level restore, the registry hive will be located automatically. Otherwise, make sure the system registry hive is located in the same folder as `.DIT` file.



Step 5. Specify Account State

At this step of the wizard, specify whether you want to keep the account state as it is in the backup file or select **Enabled** or **Disabled** to assign a state you need.



Step 6. Specify Restore Options

At this step of the wizard, specify restore options.

You can select the following:

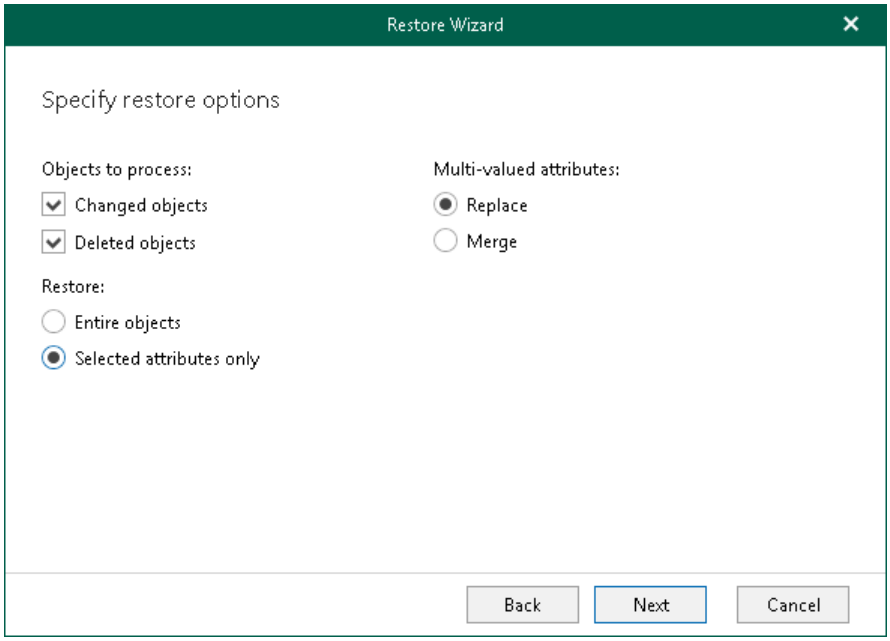
- **Objects to process**:
  - **Changed objects**. To restore changed objects.
  - **Deleted objects**. To restore deleted objects.
- **Restore**:
  - **Entire objects**. To restore entire objects collection.
  - **Selected attributes only**. To select particular attributes.

    When selecting **Selected attributes only**, you will be offered to choose the attributes you want to restore in the next step.
- **Multi-valued attributes**:
  - **Replace**. To replace production data with that of a backup file.
  - **Merge**. To merge existing data with that of a backup file.

  By default, multi-valued attributes will be replaced, not merged.

NOTE

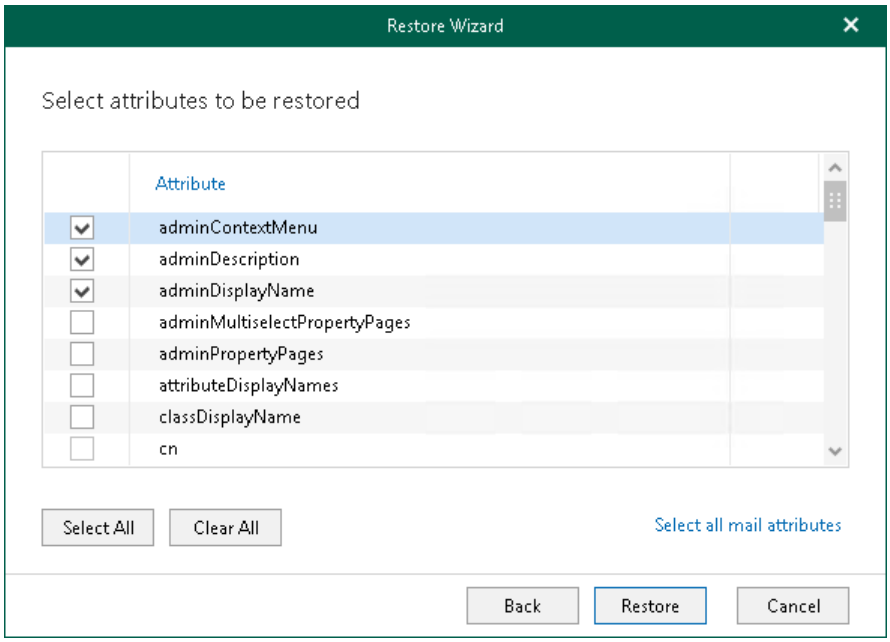
- When working with Active Directory 2016, this dialog will also include the Restore expiration time option which allows you to restore expiration time for linked attributes.if an attribute being restored expires during the restore session, then such an attribute will not be restored.
- Users cannot change recovery settings for disabled attributes. Such attributes will be either restored or skipped according to the default configuration.



Step 7. Specify Attributes to Restore

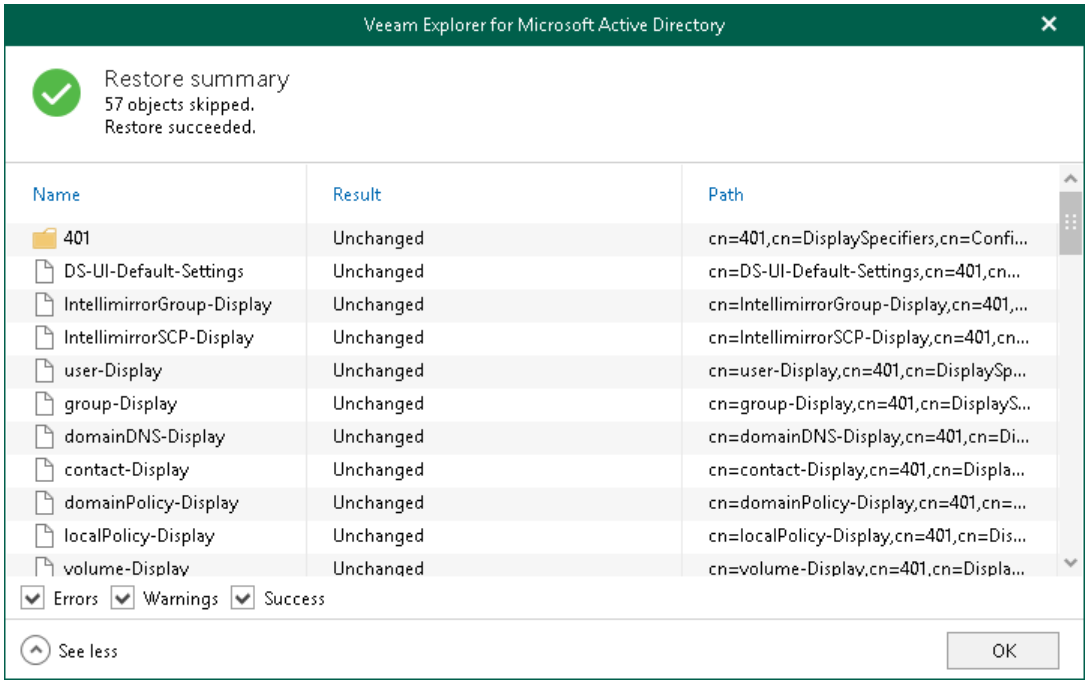
At this step of the wizard, select attributes you want to restore.

This step is available only if you have chosen the **Selected attributes only** option at the previous step.



After the restore process is complete, review the results shown in the **Restore summary** dialog.

You can select whether to display all types of notifications or only those you need by selecting/deselecting the corresponding check boxes in the lower-left corner of the dialog.



Using 1-Click Restore

The 1-Click Restore feature allows you to quickly recover Active Directory objects and containers back to the original domain in your production environment.

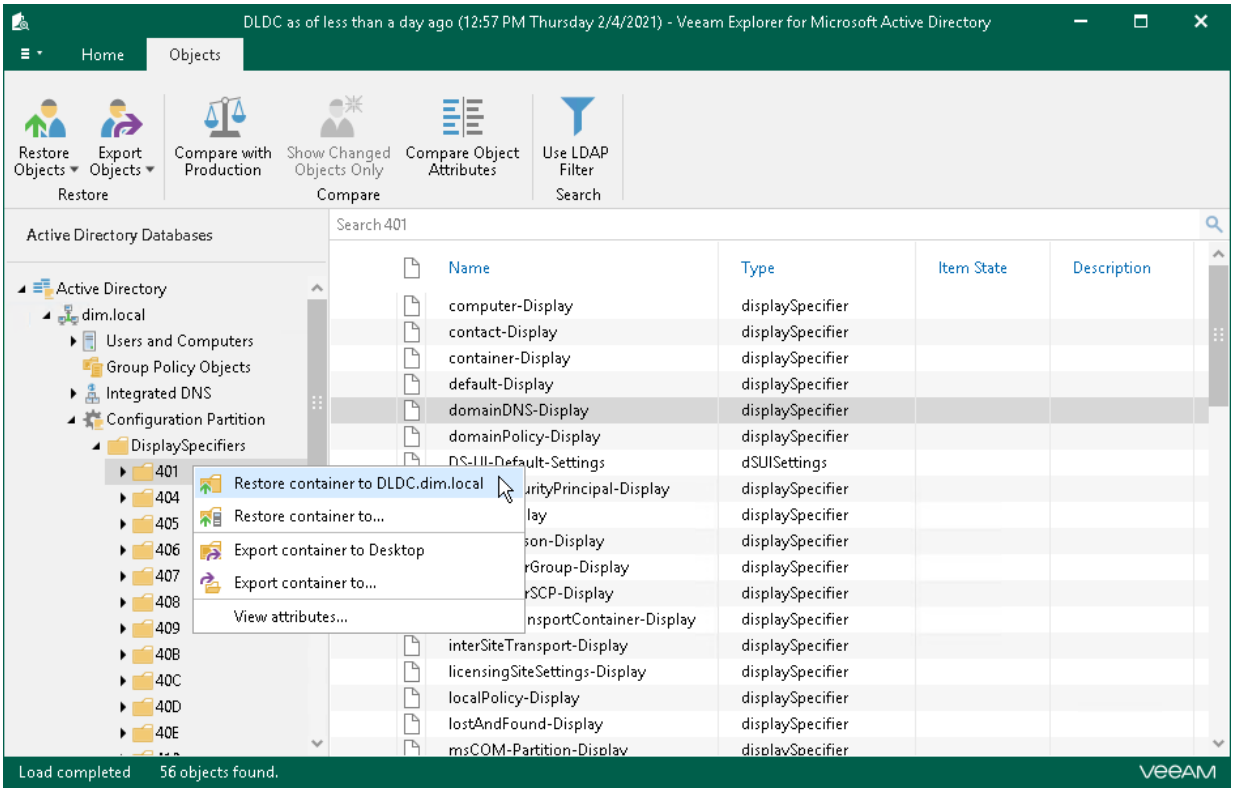
Consider the following:

- Both changed and deleted objects will be restored.
- All the attributes will be restored.
- Attribute values and security descriptors will be replaced with that of a backup file.

Restoring Containers

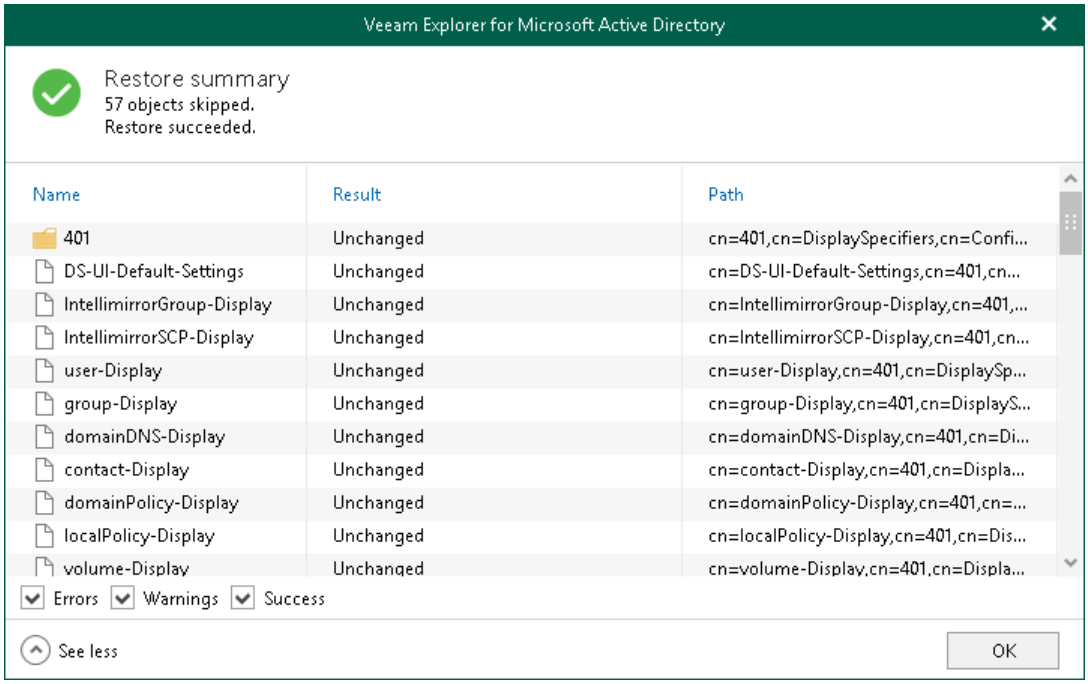
To restore a container, do the following:

1. In the navigation tree, select a container.
2. On the **Container** tab, select **Restore Container** > **Restore container to** *<server_name>* or right-click a container and select **Restore container to** *<server_name>*.



After the restore process is complete, review the results shown in the **Restore Summary** dialog.

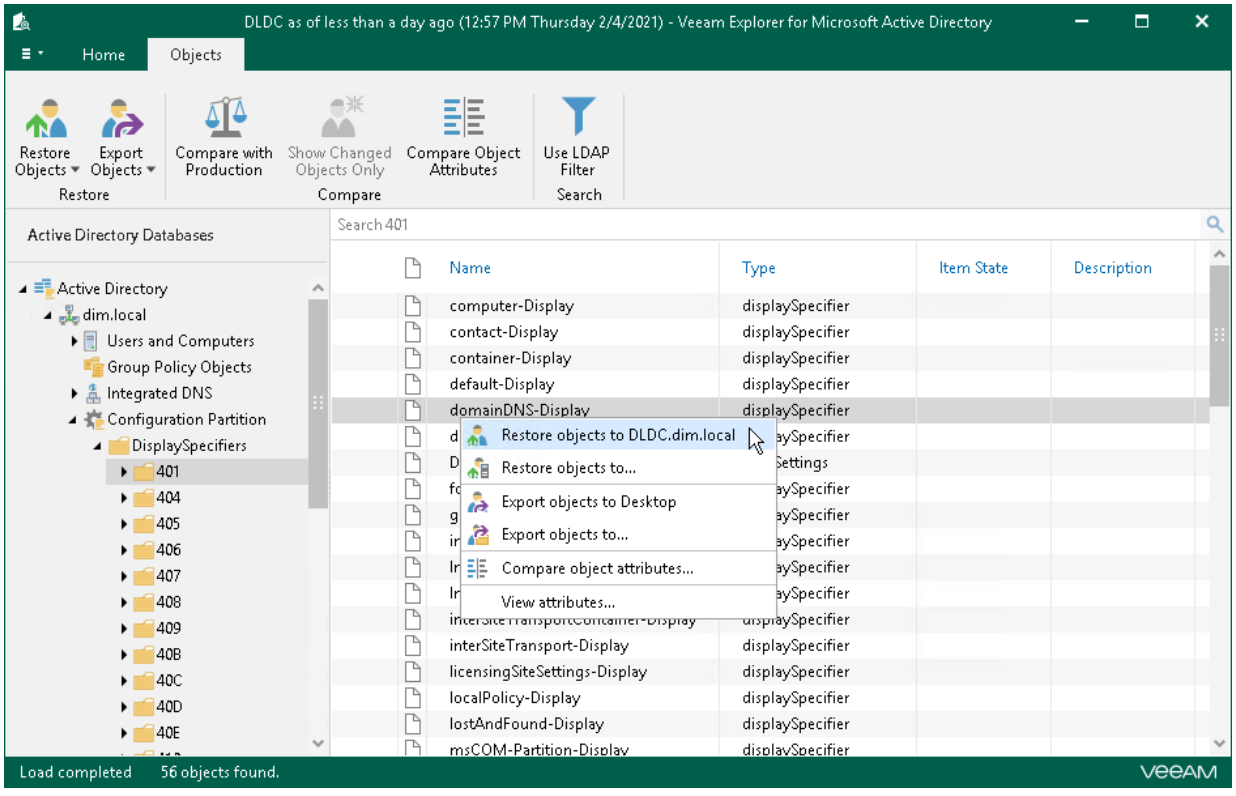
You can select whether to display all types of notifications or only those you need by selecting/deselecting the corresponding check boxes in the lower-left corner of the dialog.



Restoring Objects

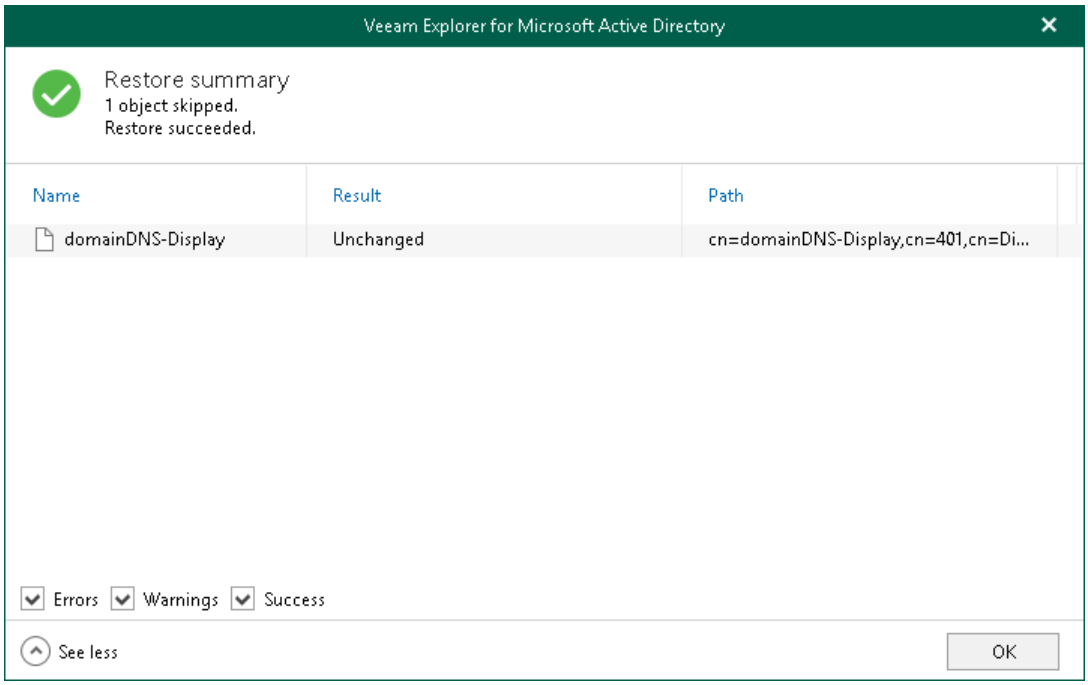
To restore an object, do the following:

1. In the preview pane, select objects.
2. On the **Objects** tab, select **Restore Objects** > **Restore objects to** *<server_name>* or right-click an object and select **Restore objects to** *<server_name>*.



After the restore process is complete, review the results shown in the **Restore Summary** dialog.

You can select whether to display all types of notifications or only those you need by selecting/deselecting the corresponding check boxes in the lower-left corner of the dialog.



Data Export

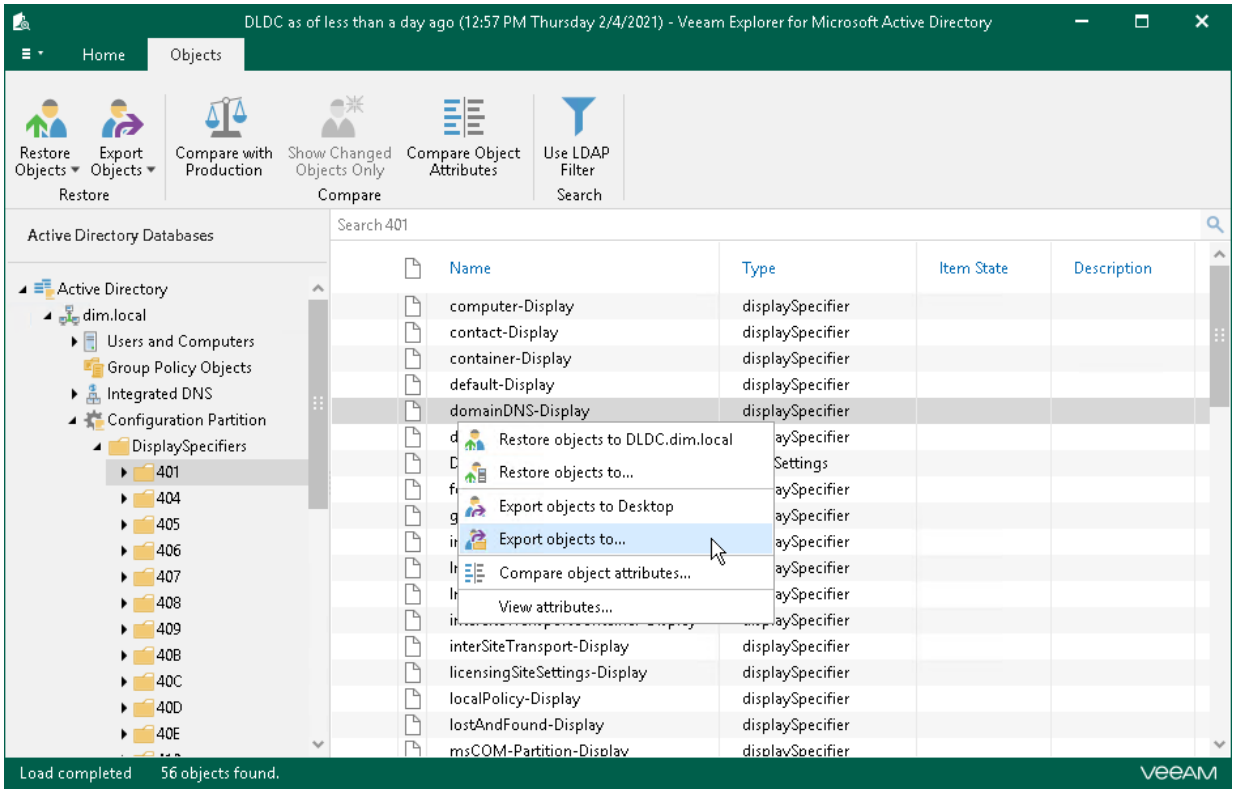
Continue with this section to learn more about exporting Active Directory objects and containers.

> **TIP**
>
> Before exporting data, make sure to read Considerations and Limitations.

Exporting Objects

To export Active Directory objects, do the following:

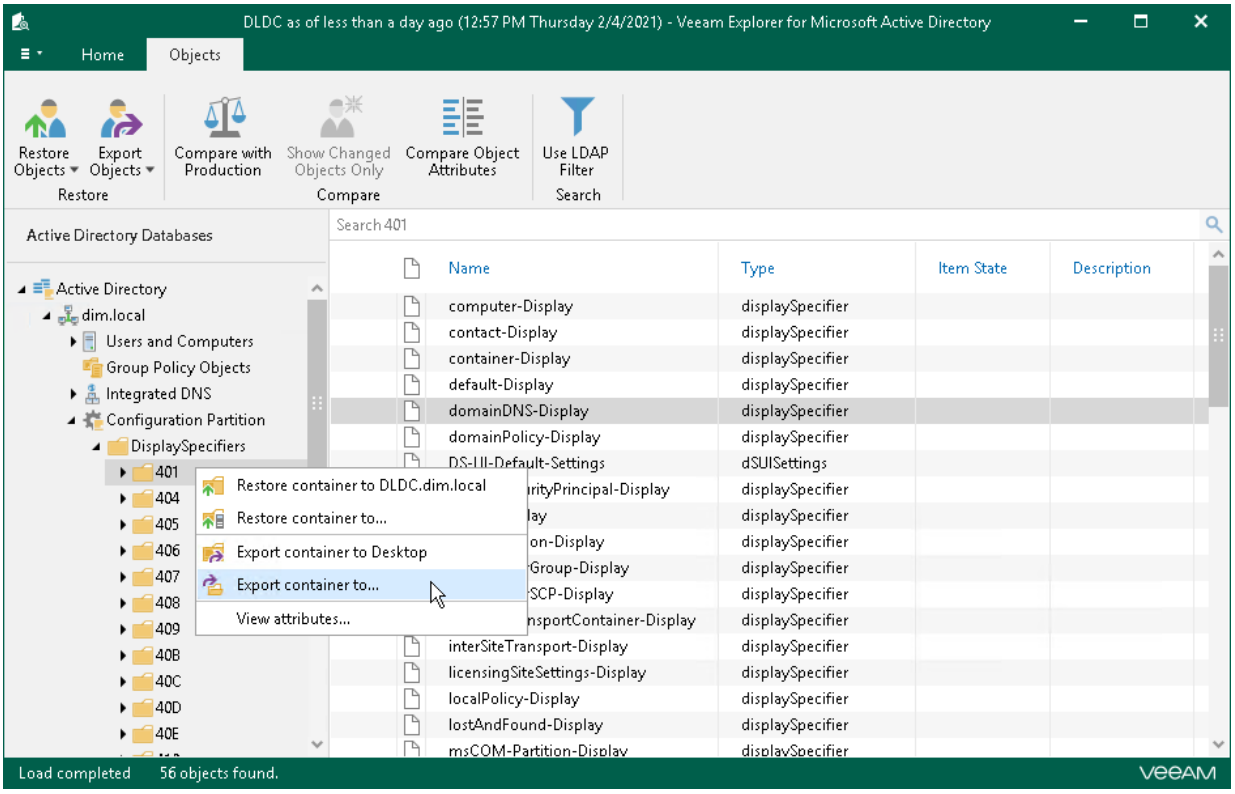
1. In the preview pane, select an object.
2. On the **Objects** tab, select **Export Objects** > **Export objects to** or right-click an object and select **Export objects to**.
3. Specify the destination folder and click **Save**.



Exporting Containers

To export containers and its content, do the following:

1. In the preview pane, select a container.
2. On the **Container** tab, select **Export Container** > **Export container to** or right-click a container and select **Export container to**.



3. In the **Export Container** window, in the **Export to** field, specify the destination location.

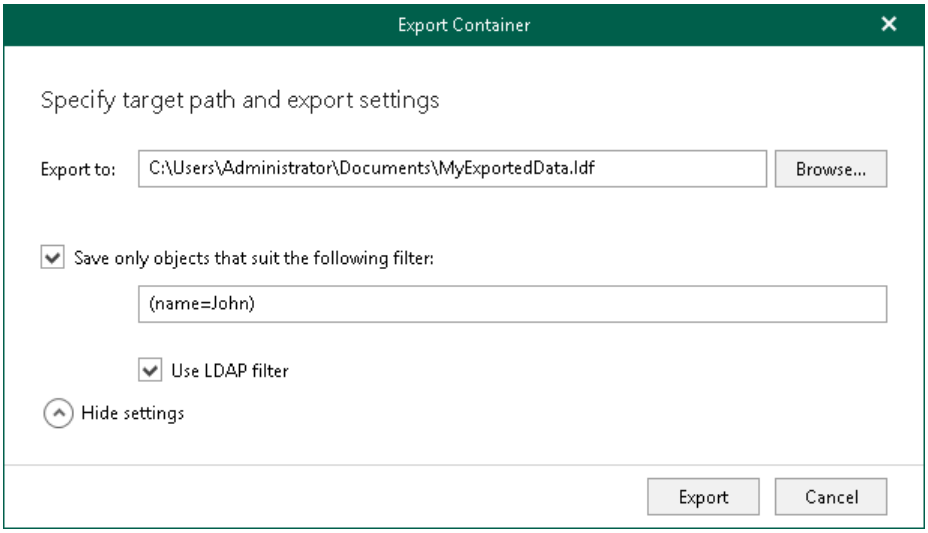
   To save only objects included in the selected container and meet specific filtering criteria, click **Show settings** to set the filter.

4. [Optional] Select the **Save only objects that suit the following filter** check box and enter filtering criteria.

   If necessary, select the **Use LDAP filter** check box to switch to the LDAP filtering mode.

5. Click **Export**.

   All the nested containers (if any) will be preserved during the export.

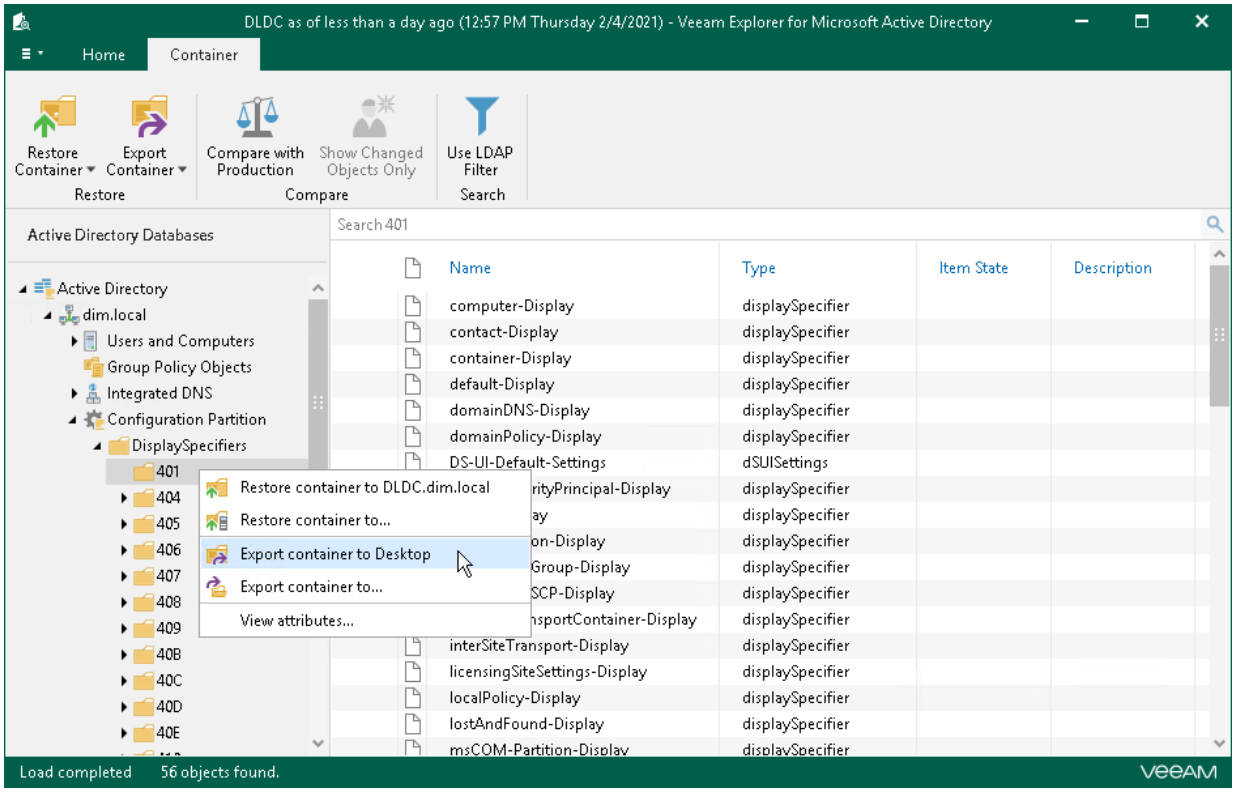


Using 1-Click Export

To export a container or object to a default location, do the following:

1. Select a container or object.
2. On the **Container** tab, select **Export Container** > **Export Container to <target_folder>** or **Export Objects** > **Export Object to <target_folder>** respectively or use the associated context menu command.

> **NOTE**
>
> The **<target_folder>** destination depends on the location you have been using during the last export operation.



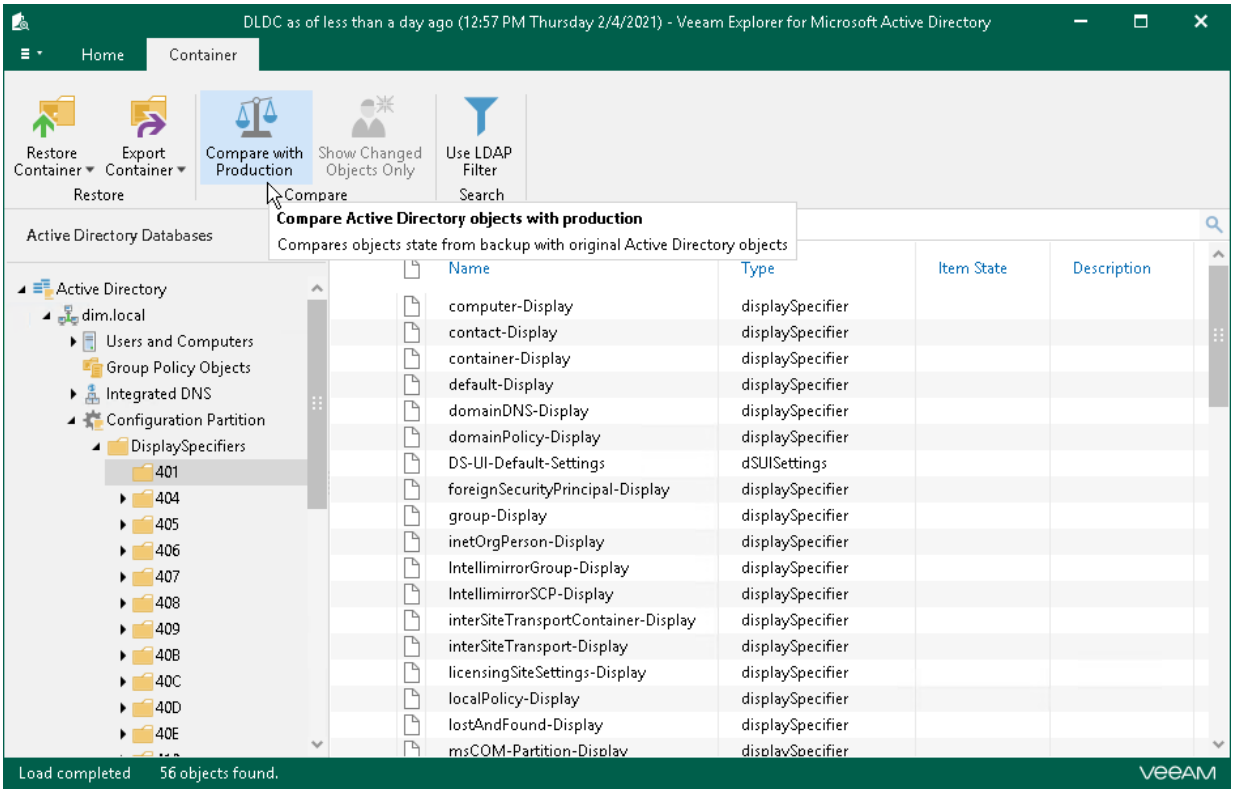
Data Compare

This section explains how to use Veeam Explorer for Microsoft Active Directory to compare data in a backup file with that of the production state.

Comparing Active Directory Containers

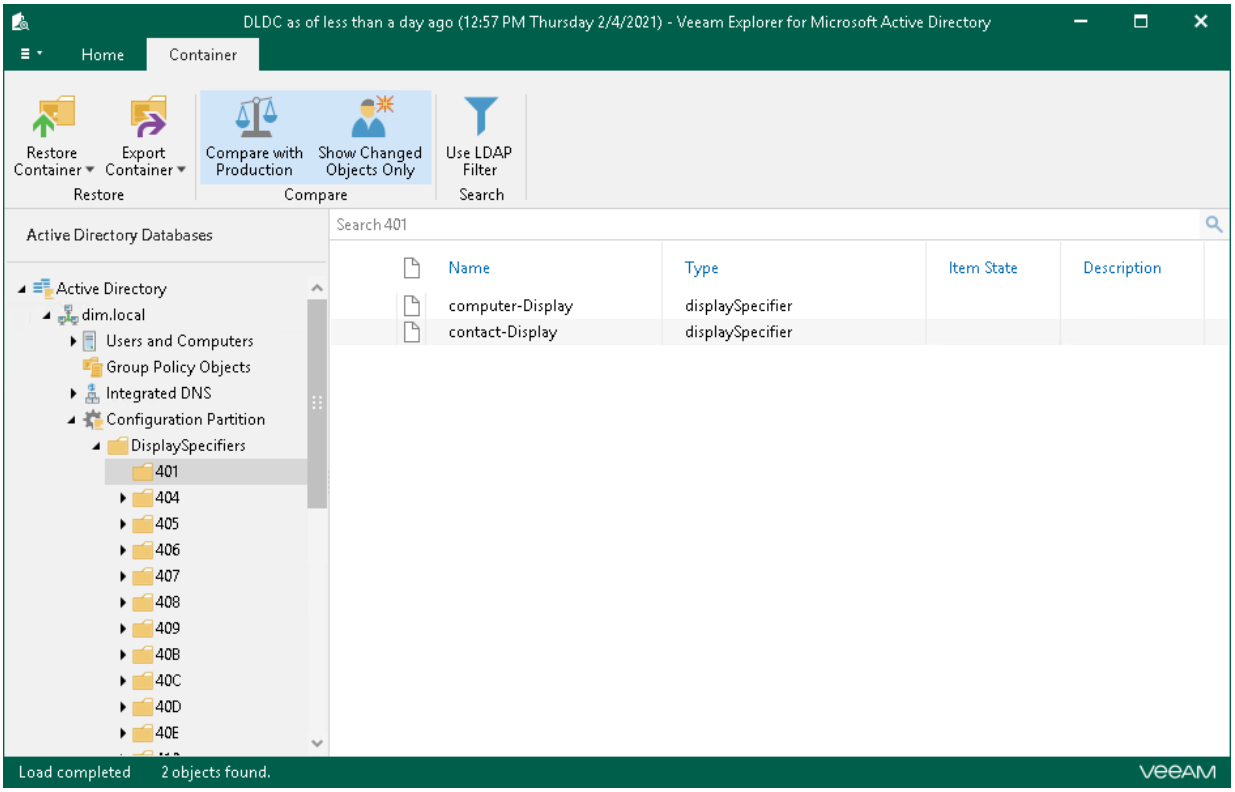
To compare Active Directory containers, do the following:

1. In the navigation pane, select a container.
2. On the **Home** tab, select **Compare with Production** to detect changed, moved or deleted objects since the last Active Directory backup.



3. Click **Show Changed Items Only** on the toolbar to view only those items that have been changed since the last backup.

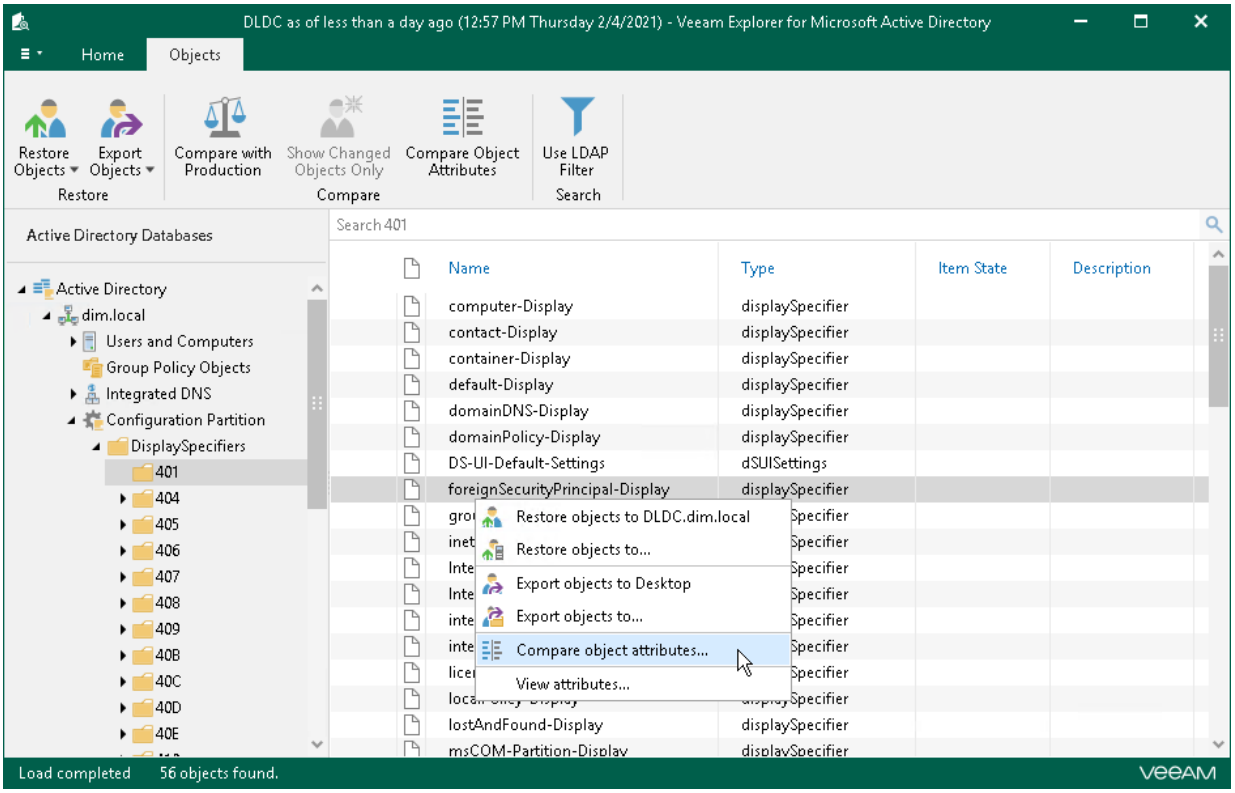
   The following figure shows user accounts the attributes of which have been changed since the last time they were backed up. Veeam can also combine item states to represent the most accurate state of an object. For example, if object attributes have been changed and the object was moved to a different location, the object status in this case will be shown as *Moved*, *Changed*.



Comparing Object Attributes

To compare Active Directory objects attributes, do the following:

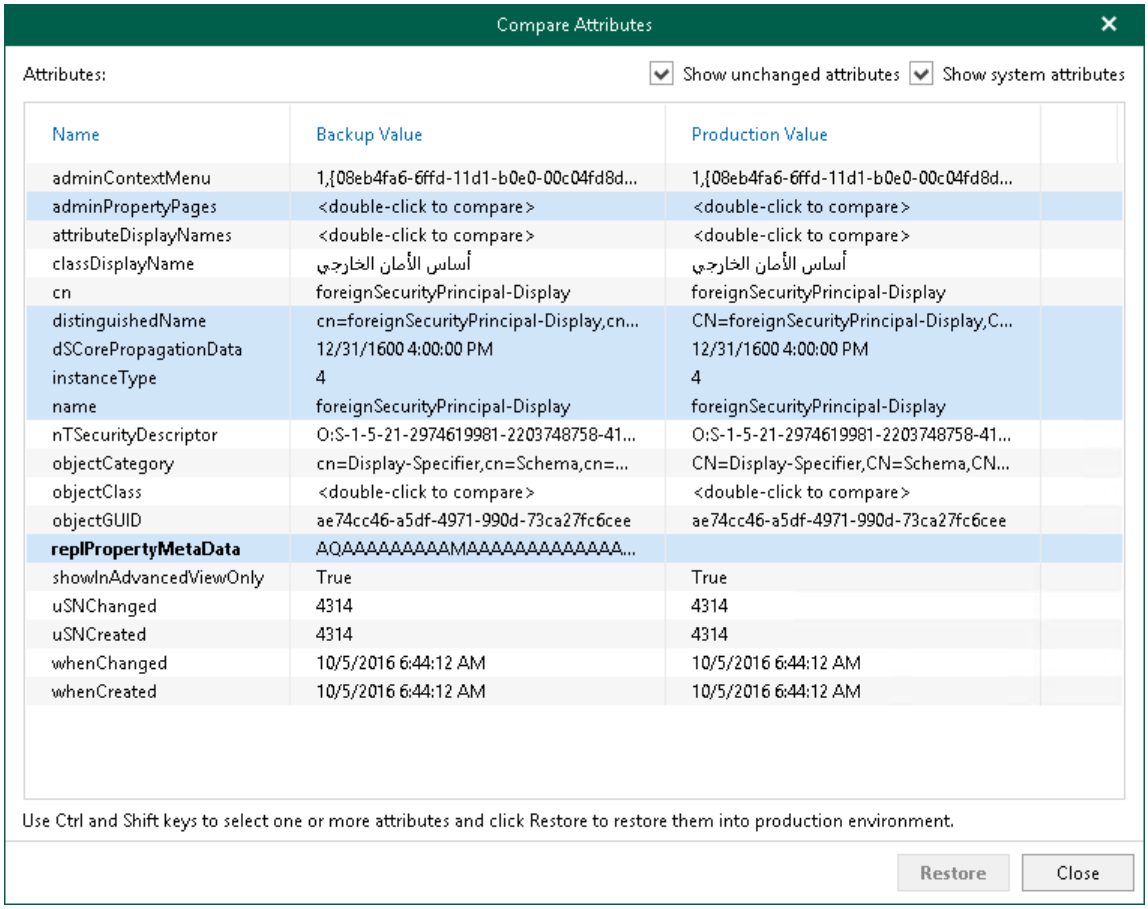
1. In the navigation pane, select a container.
2. In the preview pane, select an object.
3. On the **Objects** tab, select **Compare object attributes** or right-click an object and select **Compare object attributes**.



4. Review changed attributes.

   To show unchanged attributes, select **Show unchanged attributes** at the top-right corner. To show system properties, select **Show system attributes**.

To restore an attribute, select it and click **Restore**. Multiple selection is also supported.



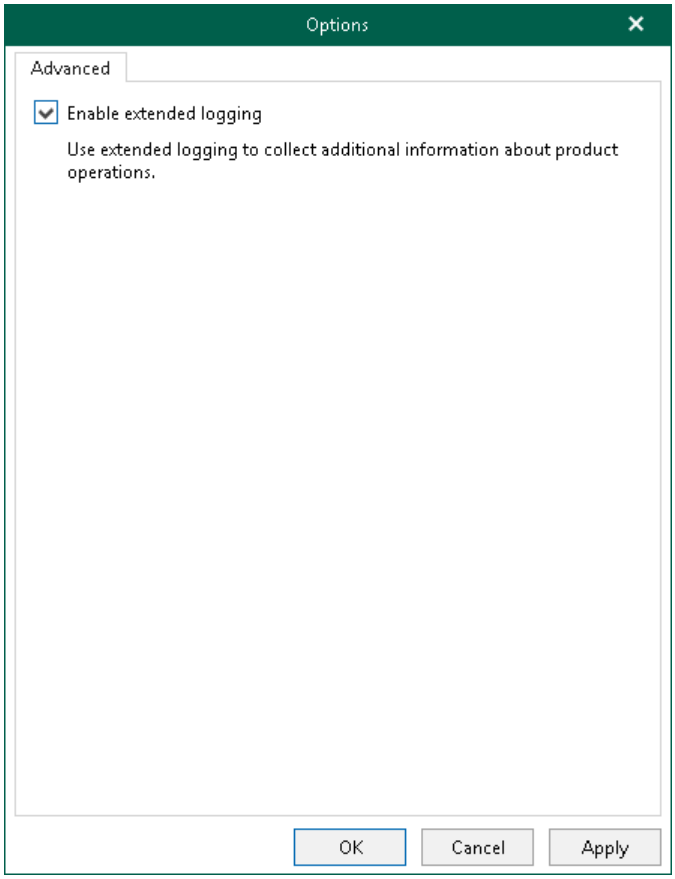
Enabling Extended Logging

Log files are used to troubleshoot a variety of different situations when certain processes may have gotten unexpected results while being executed.

By default, logs are collected in the default mode. In certain cases, you may need to enable the extended logging mode to collect logs that contain more details on specific operations.

To configure extended logging mode, do the following:

1. Go to the main menu and click **General Options**.
2. On the **General** tab, select the **Enable extended logging** check box and click **OK**.
3. Go back to the application, perform necessary actions and then review the logs to see the details.



Veeam Explorer for Microsoft SQL Server

Veeam Explorer for Microsoft SQL Server allows you to restore and export Microsoft SQL Server databases and schema objects from backups created in Veeam Backup & Replication.

In This Section

- Planning and Preparation
- Launching Application and Exploring Backups
- General Application Settings
- Standalone Databases Management
- Data Restore
- Data Publishing
- Instant Recovery
- Data Export
- SQL Server Database Operation Selection

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft SQL Server.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft SQL Server.

Component	Requirement
Microsoft SQL Server	For more information about supported versions of Microsoft SQL Server, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

> **NOTE**
>
> AlwaysOn Availability Groups are supported for Microsoft SQL Server 2012 and higher.

Consider the following:

- By default, the **AUTO_CLOSE** option for SQL Server databases is set to **False**.

  If **AUTO_CLOSE** is enabled, your databases might be skipped from processing.
- To restore database items from an SQL Server that is running Microsoft Windows ReFS, the Veeam backup server or a management console must be installed on Microsoft Windows Server 2012 or higher.
- To restore data from a server that is running Microsoft Windows ReFS 3.x, the Veeam backup server or a management console must be installed on Microsoft Windows Server 2016.
- Nodes participating in AlwaysOn Availability Groups are supported, but using *Availability Group Listeners* as staging servers is not recommended.

Staging SQL Server Requirements

Consider the following:

- Make sure that the staging Microsoft SQL Server has the same or later version as the original SQL Server.
- An SQL Server included in Microsoft SQL Server Failover Cluster cannot be used as a staging system.
- Mind domain trusts configuration when planning to add databases to the Veeam Explorer scope manually. For more information, see Configuring Staging SQL Server.
- The following *Microsoft SQL Server Express Editions* can be used as a staging system:
  - *Microsoft SQL Server 2012 Express Edition.*

    For Microsoft Windows 2008 R2 and Windows 7.
  - *Microsoft SQL Server 2016 Express Edition.*

    For other higher versions.

  Both editions come as part of the Veeam Backup & Replication distribution package.
- An SQL Server instance can be used as a staging system.

NOTE

Databases that exceed 10 GB cannot be attached to the Microsoft SQL Server 2012/2016 Express Edition due to Express Edition limitations. For more information, see the following Microsoft articles:

- For Microsoft SQL Server 2012 Express Edition
- For Microsoft SQL Server 2016 Express Edition

Used Ports

The following tables list network ports that must be opened to manage inbound/outbound traffic.

Backup

From	To	Protocol	Port	Notes
Veeam Backup Server / Guest Interaction Proxy (Enterprise and Enterprise Plus editions)	**Microsoft SQL Server VM Guest OS**	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on a VM guest OS.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC range that is used by the runtime coordination process which is deployed on a VM guest OS for application-aware processing.[1]
		TCP	6167	**For Microsoft SQL Server transaction logs shipping** Port used by the runtime process on a VM guest OS from which transaction logs are collected.
Microsoft SQL Server VM Guest OS	**Veeam Backup Server / Guest Interaction Proxy (Enterprise and Enterprise Plus editions)**	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC range used by the runtime coordination process that is deployed on a VM guest OS for application-aware processing.[1] For more information, see this Microsoft article.
	Log Shipping Server	TCP	2500 to 3300	**For Microsoft SQL Server transaction logs shipping** Default range of ports used by the Veeam Data Mover Service for data transfer over the network.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Restore

From	To	Protocol	Port	Notes
Veeam Backup Server / Standalone Console / Mount server associated with the backup repository (only when restoring from Enterprise Manager)	**Target Server, Staging Server**	TCP, UDP	135, 445	Ports used to deploy the runtime coordination process on a target guest OS.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC range used by the runtime coordination process that is deployed on a target guest OS.[1] For more information, see this Microsoft article.
		TCP	6160	Port used to communicate with the installer service.
		TCP	1433, 1434	Ports used to communicate with the Microsoft SQL Server installed on a VM during application-item restore. For more information, see this Microsoft article.
		UDP	1434	Port used by the Microsoft SQL Server Browser service. For more information, see this Microsoft article.
		TCP	1025 to 1034	Default RPC range for the runtime component installed on a target or staging SQL Server VM to support restore. This port range is opened only during application item restore.
Target Server, Staging Server	**Mount server associated with the backup repository**	TCP	3260 to 3270	Port range opened by Veeam Backup & Replication to manage iSCSI traffic during restore to the target VM. This port range is opened only during application item restore. For more information, see Mount Operations.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure

dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Required Permissions

The following table lists required permissions for user accounts to back up and restore Microsoft SQL Server data.

Operation	Required Roles and Permissions
Backup	For more information, see the Required Permissions section of the Veeam Backup & Replication User Guide.
Restore, Instant Recovery	The account being used must be a member of the *Local Administrator* group and must be granted the *sysadmin* role on a target Microsoft SQL Server. For more information about Microsoft SQL Server roles, see this Microsoft article.

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Configuring Transaction Logs

For more information about configuring transaction logs, see the Microsoft SQL Server Transaction Log Settings section of the Veeam Backup & Replication User Guide.

Recovery Model

> **NOTE**
>
> To be able to restore your data as of a point in time or as of a state before undesired transactions, make sure the recovery model for the database is set to **full** or **bulk-logged**.

The following table lists database logging models and applicable Veeam options.

SQL DB Logging Model	Veeam Options		
	Truncate logs	**Do not truncate logs**	**Backup logs periodically**
Simple	Databases are skipped from processing.	Applicable option.	Databases are skipped from processing. Log files do not grow (and do not need to be backed up).
Full	Applicable option. Veeam performs "backup to NUL" for log files on guest.	Applicable but not recommended to use without native or 3rd party means of log truncation or backup – otherwise, logs will increase in size.	Applicable option. Log backup files (.BAK) are copied from the temporary folder on SQL Server to Veeam repository. As soon as data is copied to target, BAK files are deleted from source.
Bulk-logged	Applicable option. Veeam performs "backup to NUL" for log files on guest.	Applicable but not recommended to use without native or 3rd party means of log truncation or backup – otherwise, logs will increase in size.	Applicable option. Log backup files (.BAK) are copied from the temporary folder on SQL Server to Veeam repository. As soon as data is copied to target, BAK files are deleted from source.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft SQL Server.

General

- When Veeam Explorer for Microsoft SQL Server is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft SQL Server does not support restore via *PSDirect*, *VIX* or *Sphere API*.
- Table-level recovery is supported only for database tables with no external dependencies.
- To restore an encrypted database, consider reading this Veeam Knowledge Base article.
- The *Replace* logic is not supported when restoring schema objects.
- To restore a database from the AlwaysOn availability group node as of the selected transaction state, the nodes of such a group must be located in the same time zone.

Publishing

- During publishing, Veeam Explorer for Microsoft SQL Server mounts VMs disks from the backup file to the target machine (under the *C:|VeeamFLR* directory), retrieves required database files and attaches associated databases directly to your SQL Server instance so that you can perform required operations using Microsoft SQL tools such as Microsoft SQL Server Management Studio.

  When publishing to a cluster, all VMs disks become part of the target cluster.
- You can publish the same database more than once.
- After you unpublish a database, Veeam Explorer for Microsoft SQL Server detaches such a database from the target SQL Server but the restore point will continue to remain on the target machine for the next 15 minutes.
- If a Veeam Explorer for Microsoft SQL Server session has been terminated in any way other than by clicking **Exit** in the main menu (or by clicking the **X** button in the upper-right corner), then all the published databases will continue to remain attached to the target SQL Server with the *Recovery pending* state.
- If published databases have been renamed manually via SQL tools (for example, in *Microsoft SQL Management Studio*), then Veeam Explorer for Microsoft SQL Server will not be able to unpublish such databases properly. In this case, all the renamed databases will continue to remain attached to the target SQL Server and you will have to remove them manually using the SQL tools.
- Veeam Explorer for Microsoft SQL Server does not back up published databases.
- Upon closing the Veeam Explorer console, all the published databases will be detached from the target SQL Server instance automatically. The corresponding mount points will also be dismounted from under the `C:\VeeamFLR` directory.

Instant Recovery

- To restore an encrypted database, consider reading this Veeam Knowledge Base article.
- If you perform instant recovery of a database from the AlwaysOn availability group node, Veeam Explorer restores it as a standalone database.
- For desktop versions of Microsoft Windows (7, 8, 8.1, 10), you must perform instant recovery of multiple databases one by one. The limitation occurs because desktop versions of Microsoft Windows OS do not allow more than 20 incoming concurrent TCP/IP connections. For details, see Microsoft Windows 10 License Terms.

  As a workaround, you can perform instant recovery of multiple databases in parallel using the Restore-VESQLIRDatabase PowerShell cmdlet.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft SQL Server and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created in Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

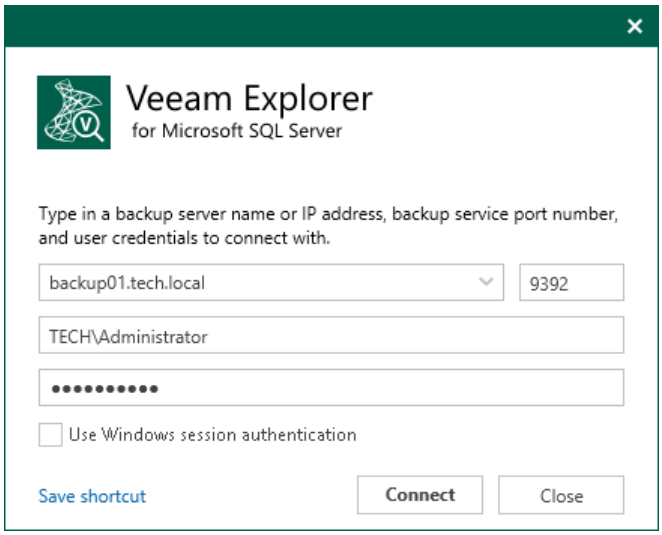
- Go to **Start**, click **Veeam Explorer for Microsoft SQL Server** and manually open Microsoft SQL databases, as described in the Adding Standalone Microsoft SQL Databases section.

If you open Veeam Explorer for Microsoft SQL Server from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

- The domain name or IP address of the backup server to which you want to connect
- The port number
- User credentials

  The account must be a member of the *Local Administrator* group on a target server. To use the account under which Veeam Explorer for Microsoft SQL Server is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



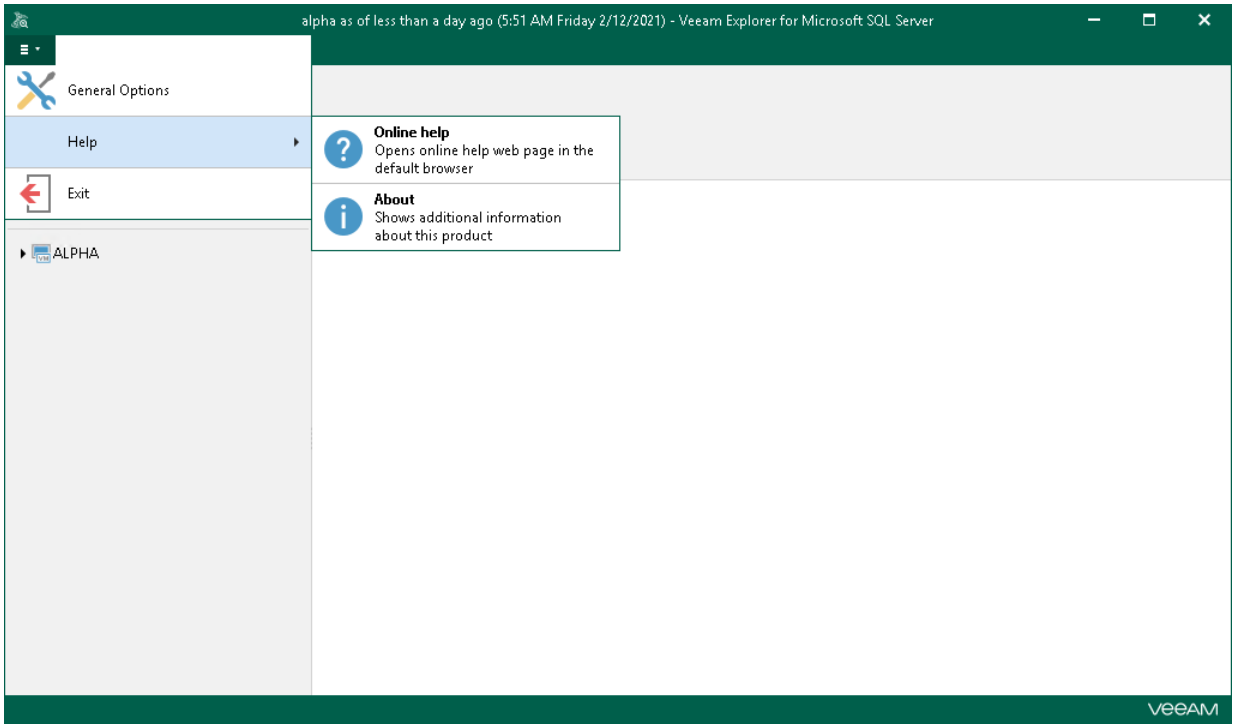
Understanding User Interface

Veeam Explorer for Microsoft SQL Server provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

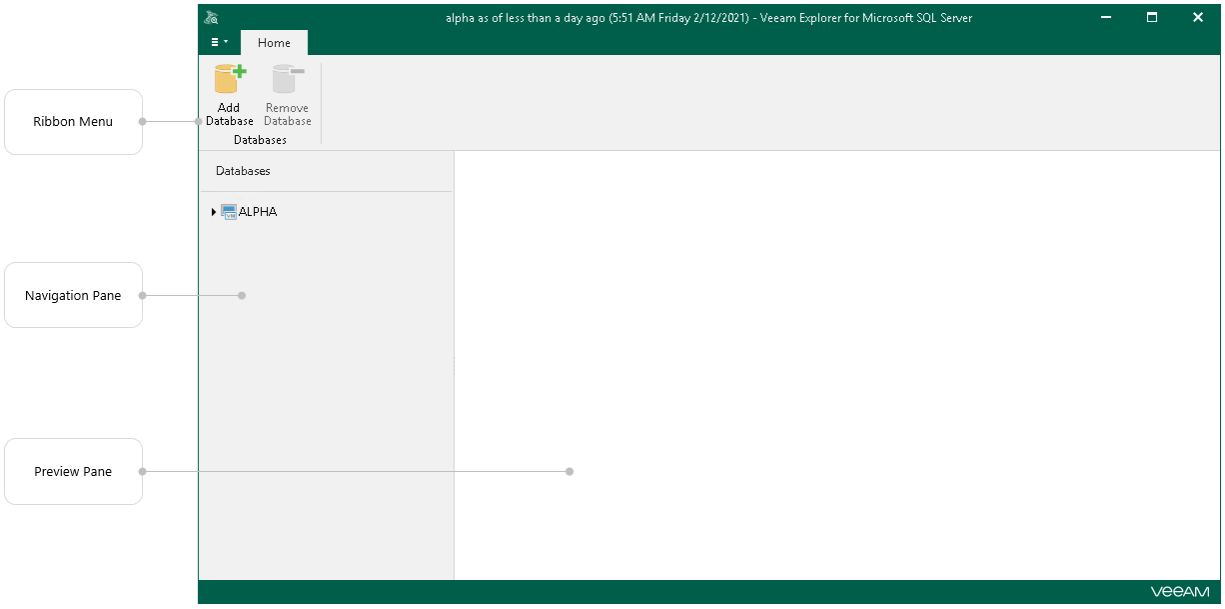
- **General Options**. Allows you to configure program options.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows information about the product.
- **Exit**. Closes the program.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your SQL databases.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Understanding Mounting

When restoring your data, Veeam Explorer requires an additional mount point to be created to display SQL Server transactions.

Mounting is performed by the *Veeam Mount Service* component which is deployed on a backup repository machine or any other machine you define in the backup repository settings.

During mounting, *Veeam Mount Service* retrieves a VM file system from the backup file, attaches it to the hard drive of a target machine and creates a mount point.

To mount a VM file system on to machines with the Microsoft Windows operating system, Veeam uses the iSCSI protocol. The original virtual machine or staging SQL Server acts as an iSCSI initiator and a mount server that is associated with the backup repository acts as an iSCSI target. The iSCSI mount point is non-persistent and only exists during the recovery process.

> **NOTE**
>
> When using fine-tune restore or point-in-time state restore, Veeam always uses a staging SQL Server to mount the VM file system.

Understanding Veeam SQL Restore Service

The *Veeam SQL Restore Service* runtime component is used to support restore activities on a VM guest operating system during the restore session. It checks the valid rights assignments required for database restore, gets information about the databases and performs required file operations including database and transaction logs copy.

After the recovery session is ended, the service is stopped and removed from the guest operating system.

All service activities are logged to the `Veeam.SQL.Service_<timestamp>.log` file stored in the `Temp` folder which is located in the system directory.

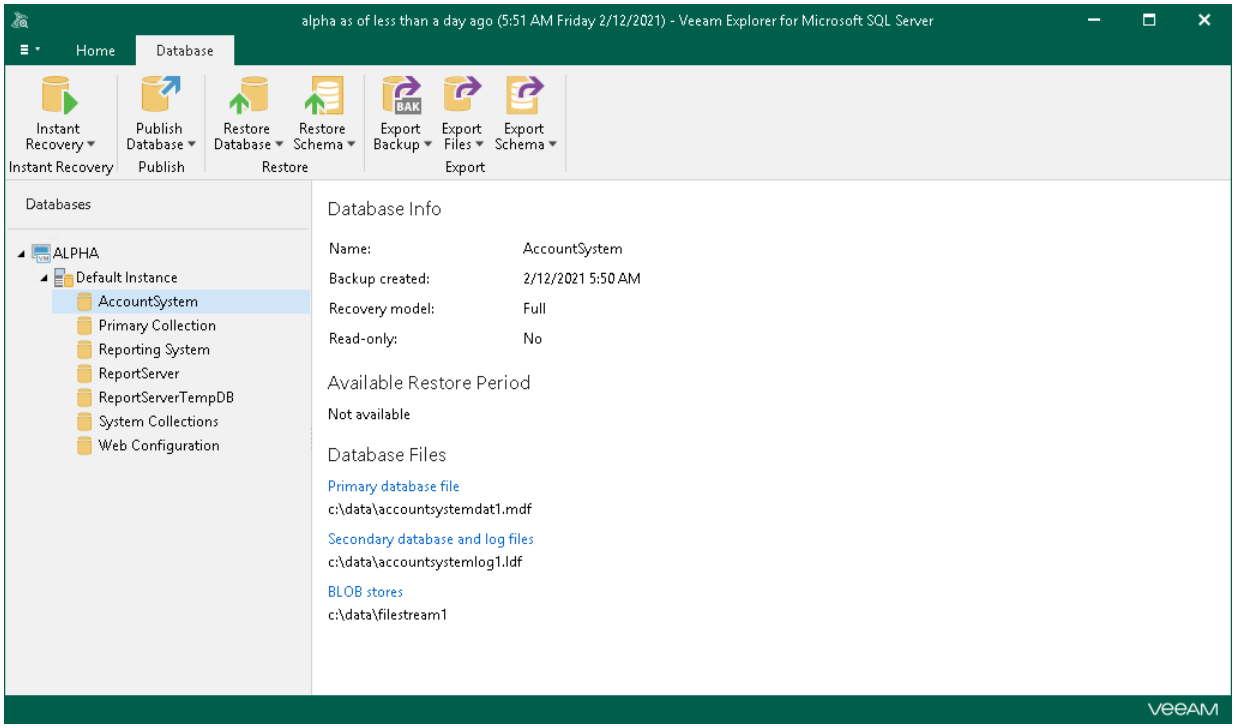
The *Veeam SQL Restore Service* component requires the Local System account.

Inbound\outbound traffic management between Veeam Explorer for Microsoft SQL Server and the *Veeam SQL Restore Service* component is performed via the RPC protocol. For more information, see Used Ports.

> **NOTE**
>
> When restoring to the local server instance, *Veeam SQL Restore Service* component is not installed on the SQL Server VM.

Viewing Database Information

To get information about databases, select a database in the navigation pane and review database info in the preview pane.



General Application Settings

Continue with this section to learn more about configuring required application settings and components.

Configuring Staging SQL Server

A staging Microsoft SQL Server is required in the following cases:

- When exporting data, as described in Data Export.
- When using the fine-tune restore, as described in Data Restore and Data Publishing.
- When adding standalone Microsoft SQL Server databases to Veeam Explorer, as described in Adding Standalone Databases.

A machine used as a staging SQL Server for the data export, data restore and data publishing operations can reside in the same domain as the machine hosting Veeam Explorer, as well as in a trusted domain or untrusted domain.

For the add standalone database operation, consider the following:

- A machine used as a staging SQL Server can reside in the same domain as the machine hosting Veeam Explorer or in a trusted domain. You cannot use a staging server that belongs to an untrusted domain to add a standalone database to Veeam Explorer.
- Both *Windows authentication* and *SQL Server authentication* methods are supported for the staging SQL Server. If you want to use *Windows authentication*, complete the following steps to configure delegation settings:
  a. In **Active Directory Users and Computers**, select a staging SQL Server.
  b. Open server properties and go to the **Delegation** tab.
  c. Select the **Trust this computer for delegation to specified services only** and **Use any authentication protocol** options for the *cifs* service on a computer with Veeam Explorer.
  d. Restart the staging SQL Server VM.
  e. Select a domain user account that you want to use when connecting to the staging SQL Server VM and make sure the **Account is sensitive and cannot be delegated** check box is not selected.

To configure a staging server, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **Staging Server** tab, select the **Use this helper SQL Server for advanced recovery functionality** check box and do the following:
   a. In the **SQL Server name** drop-down list, select a server that you want to use as your staging SQL Server.

      You can click **Browse** to locate a server using the built-in browser, as described in Browsing for Servers.
   b. Under the **Specify user account to connect to Windows server** section, select the following:
      - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Microsoft SQL Server running.
      - **Use the following account**. To connect to the specified server under a custom user account.

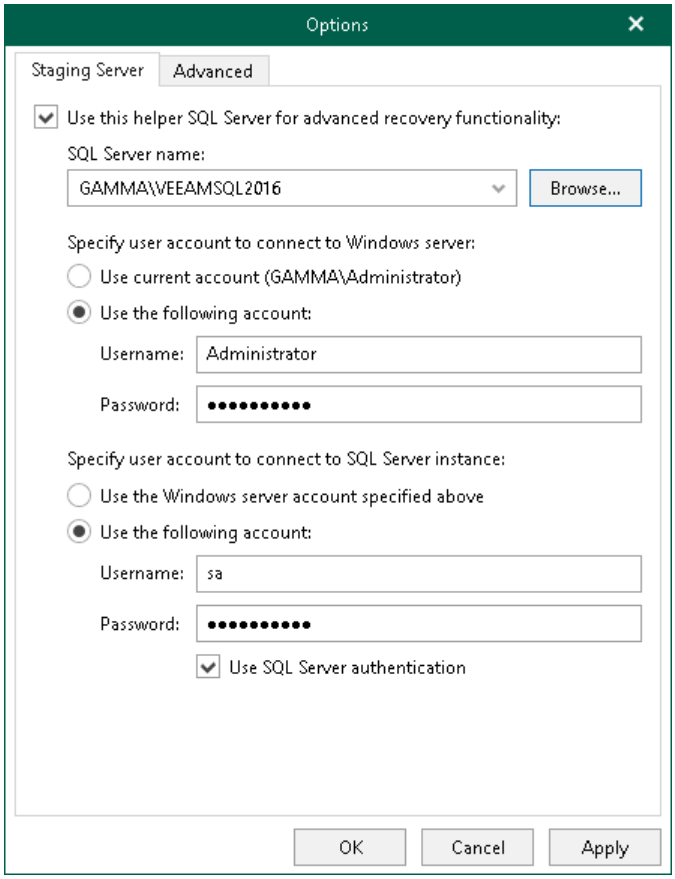
        When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.

c. Under the **Specify user account to connect to SQL Server instance** section, select the following:

- **Use the Windows server account specified above**. To connect to the specified instance under the user account that you have specified under the **Specify user account to connect to Windows server** section.
- **Use the following account**. To connect to the specified instance under a custom user account.

  When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.

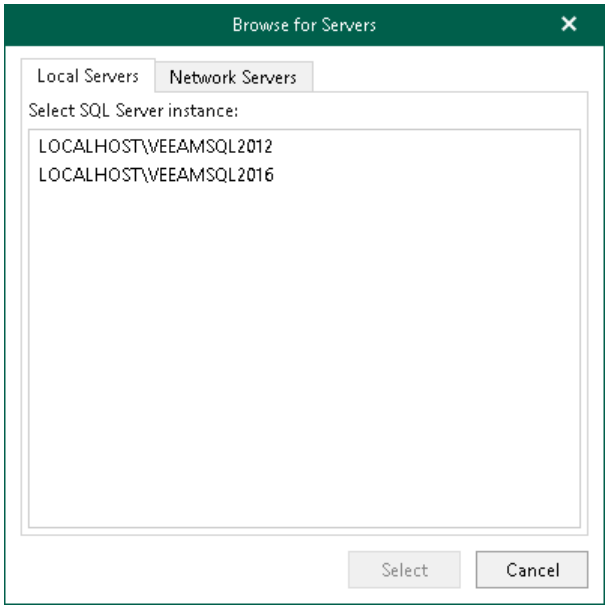
  To use SQL Server authentication, select the **Use SQL Server authentication** check box.



Browsing for Servers

To browse for a server, do the following:

- On the **Local Servers** tab, select a local SQL Server that is located on the compute with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL Server over the network.

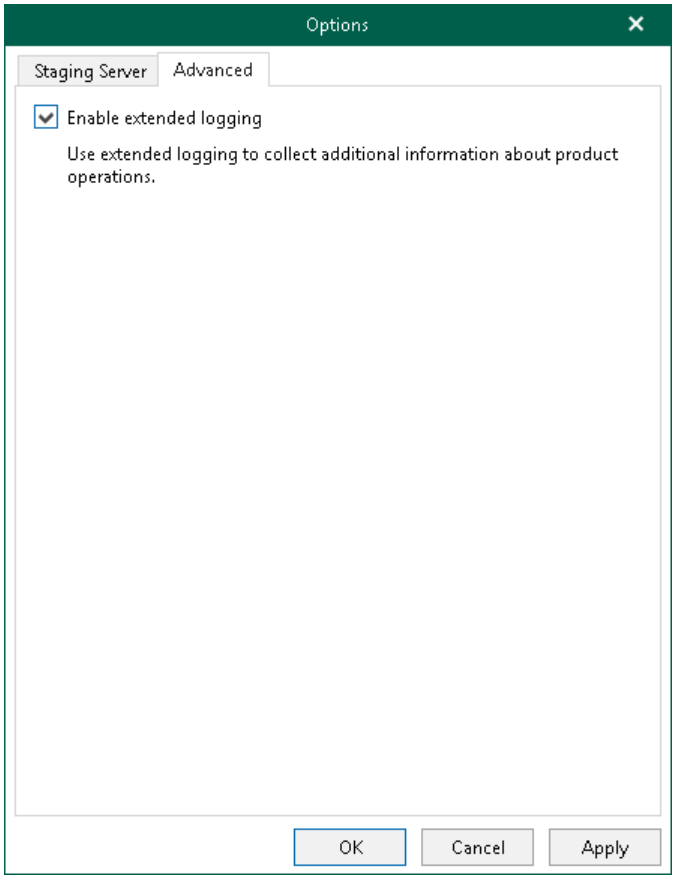


Enabling Extended Logging

Veeam Explorer for Microsoft SQL Server allows you to enable extended logging mode to collect logs that contain more details on specific operations.

To enable extended logging mode, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box.
3. After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs.



Standalone Databases Management

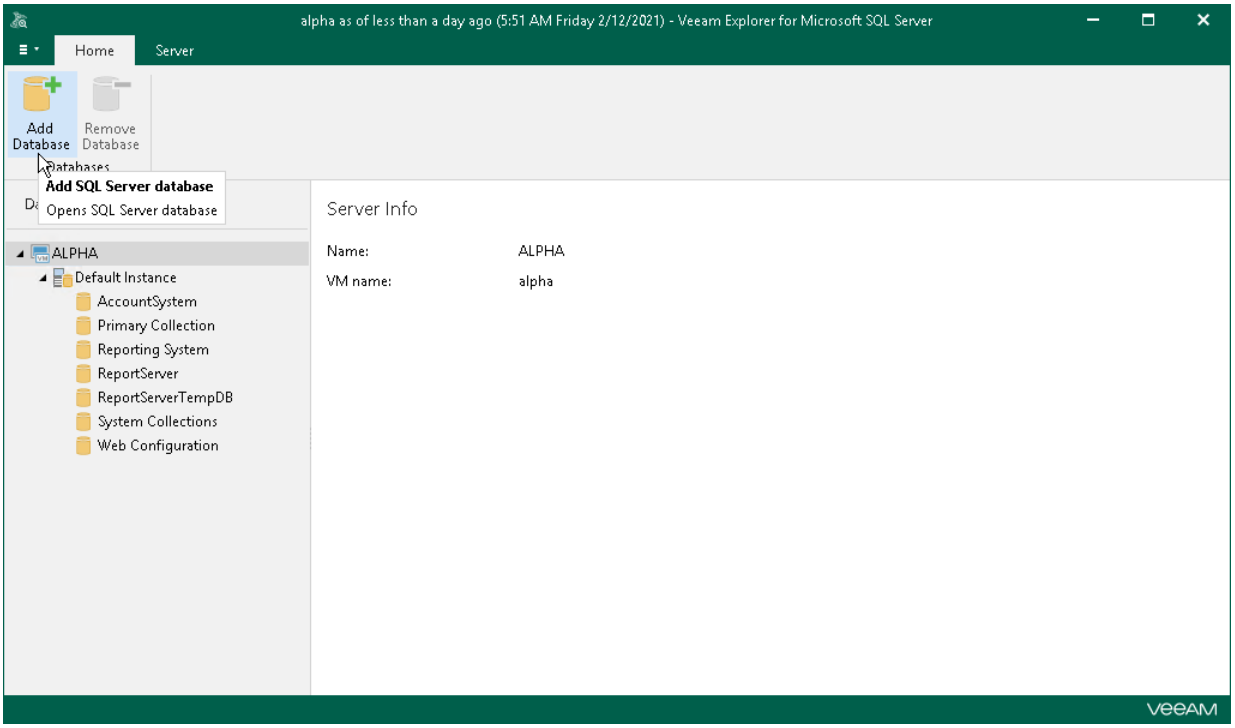
Continue with this section to learn more about adding and removing Microsoft SQL databases.

Adding Standalone Databases

> **NOTE**
>
> Before you add a standalone Microsoft SQL database, you must configure a staging SQL Server. For more information, see Configuring Staging SQL Server.

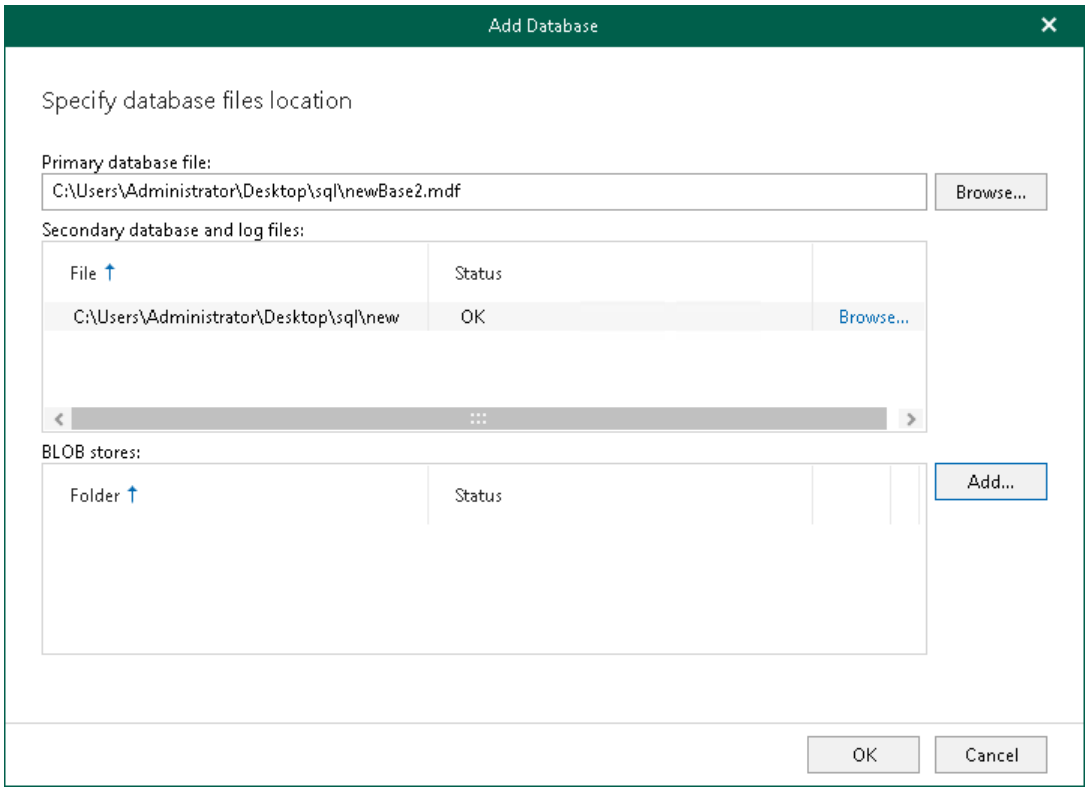
To add a standalone Microsoft SQL database manually, do the following:

1. On the **Home** tab, click **Add Database**.



2. Specify the location of a primary database file, a secondary database file and associated log files. If necessary, specify the BLOB store location.

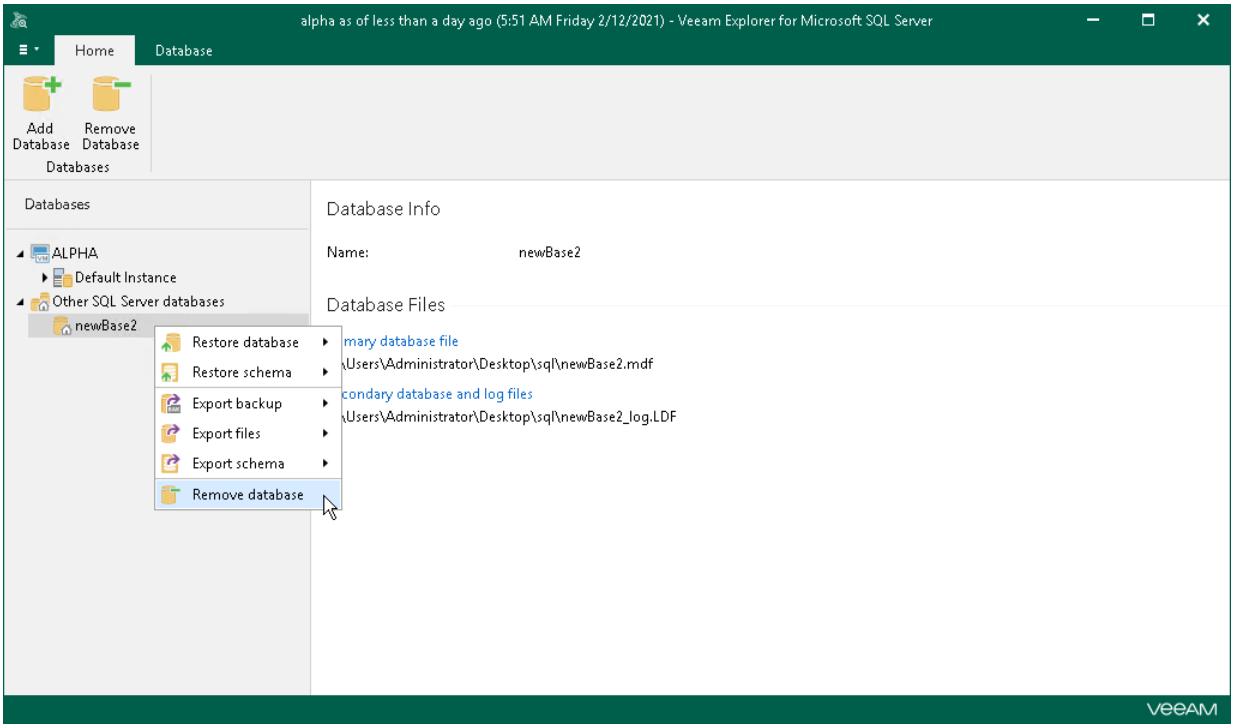
   Manually added databases will be displayed in the navigation pane under the **Other SQL Server Databases** node.



Removing Standalone Databases

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove database** or select a database in the navigation pane and click **Remove Database** on the **Home** tab.

> **NOTE**
>
> You can only remove databases that have been added to the application scope manually.



Data Restore

Continue with this section to learn more about restoring Microsoft SQL Server databases.

> **TIP**
>
> Before restoring data, make sure to read Considerations and Limitations.

Restoring Single Database

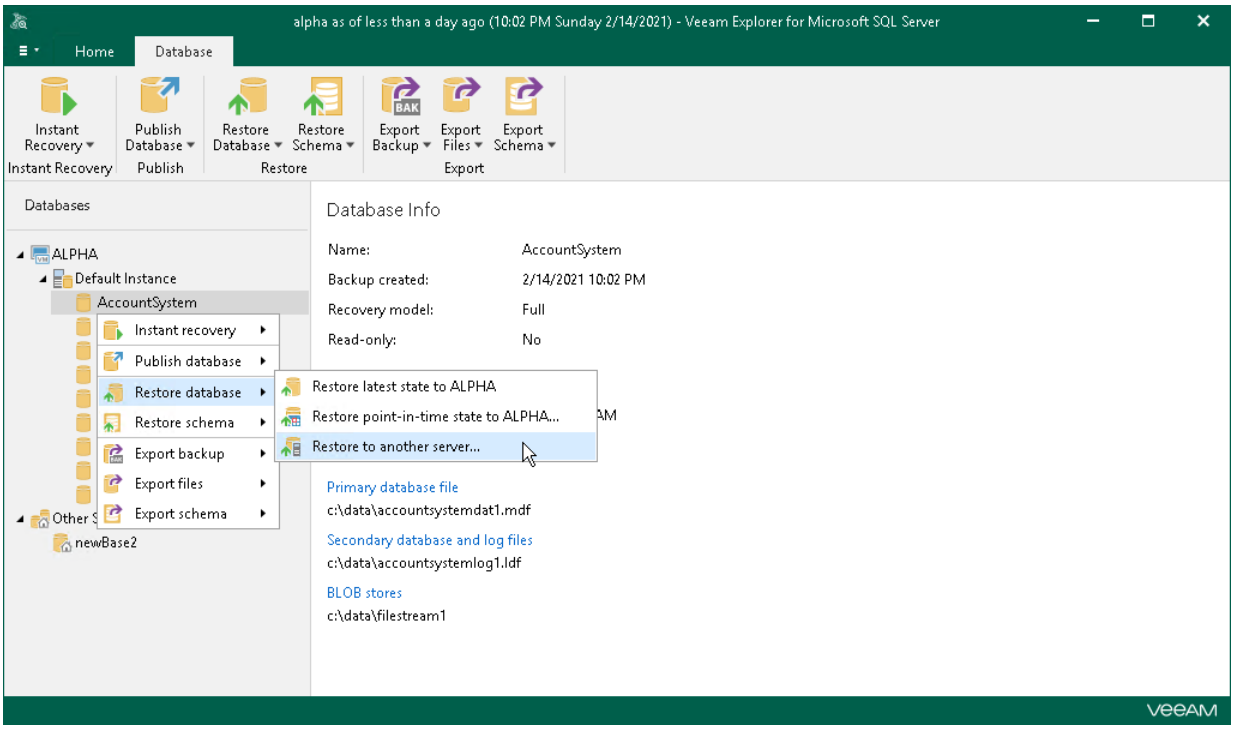
To restore a single Microsoft SQL Server database, do the following:

1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify AlwaysOn restore options.
6. Specify files location.
7. Specify the recovery state.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Restore Database** > **Restore to another server** or right-click a database and select **Restore database** > **Restore to another server**.



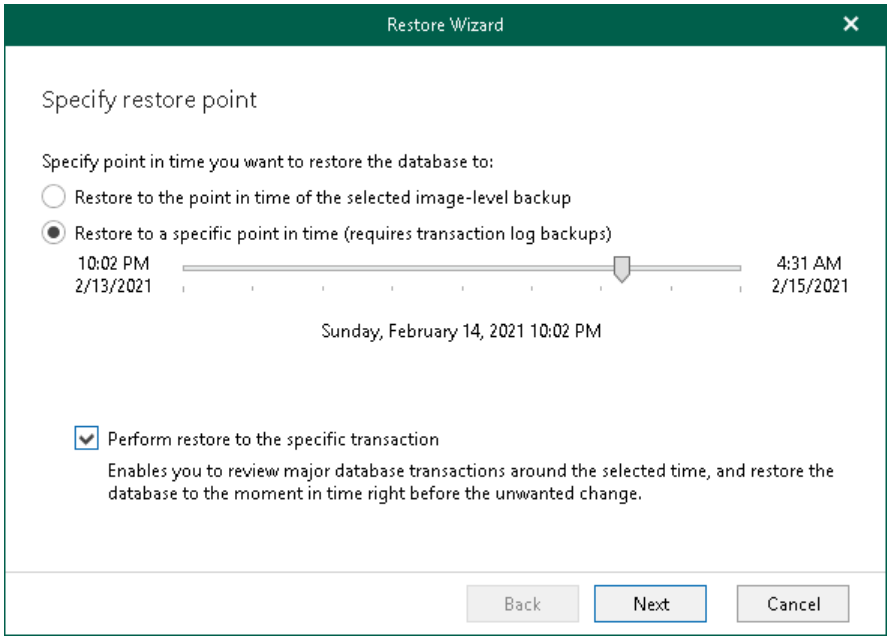
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL Server. For more information, see Configuring Staging SQL Server.

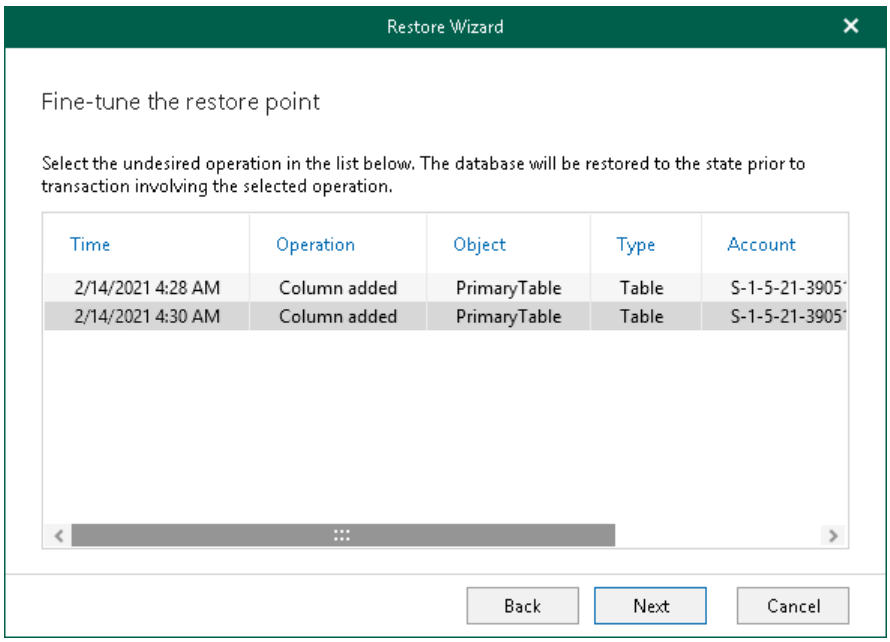


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to recover your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target Server

At this step of the wizard, specify the following:

- A production SQL Server VM name and/or SQL Server instance to which you want to restore your database.

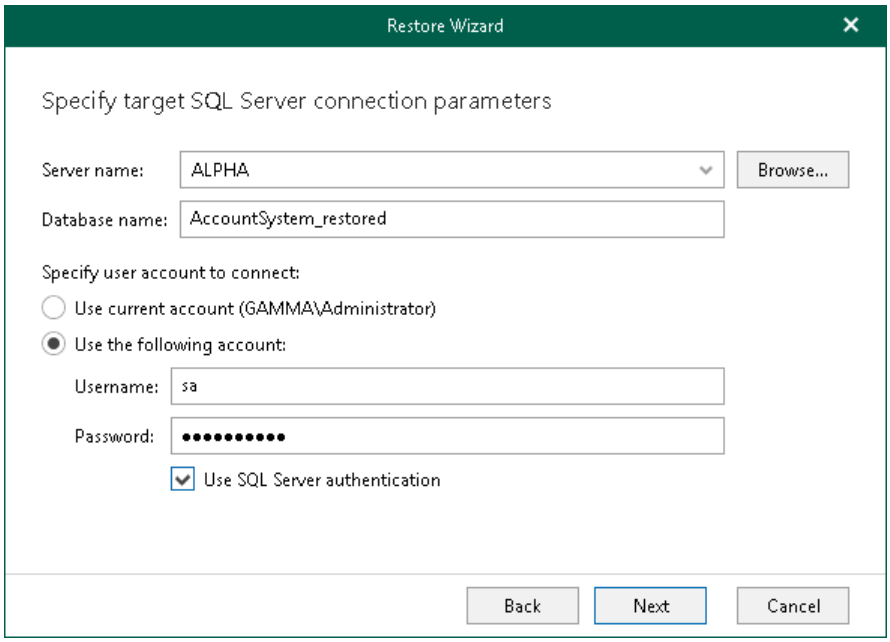
  Use the `server_name\instance` format. You can select a server or instance from the drop-down list or use the **Browse** button on the left, as described in Browsing for Servers.

- A name for the database that is being restored.
- The user account to connect to the target SQL Server.

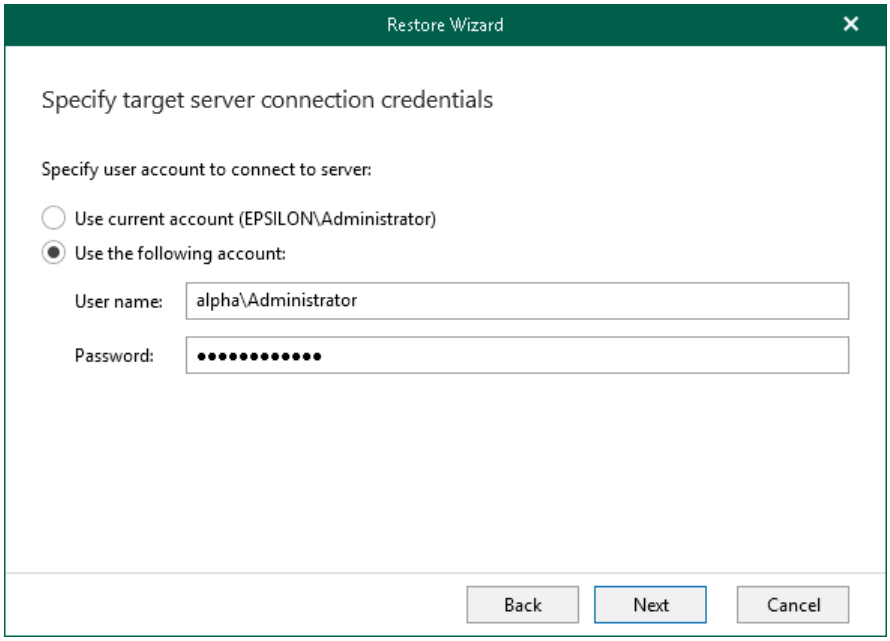
  Select the **Use SQL Server authentication** check box to use SQL authentication. If not selected, Veeam Explorer will use Windows authentication.

  Make sure the account you are using has been granted the **sysadmin** role on a target SQL Server VM.

> **IMPORTANT**
>
> Make sure that the administrative share (for example, `\\myserver\ADMIN$`) on a target machine is available. **Read** and **Write** are minimum required, **Full Control** is recommended.



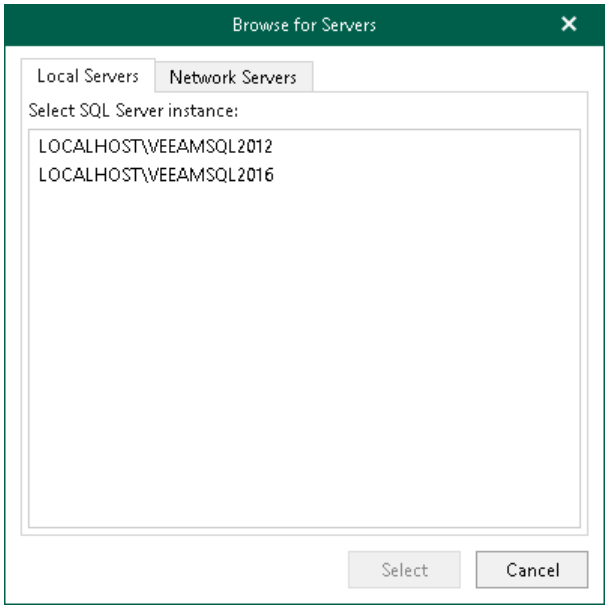
When selecting the **Use SQL Server authentication** check box and providing your SQL Server account, you will be asked to provide a target production server account in the next step, as shown below.



Browsing for Servers

To browse for a server, do the following:

- On the **Local Servers** tab, select a local SQL Server that is located on a machine with Veeam Explorer.
- On the **Network Server** tab, select an SQL Server over the network.



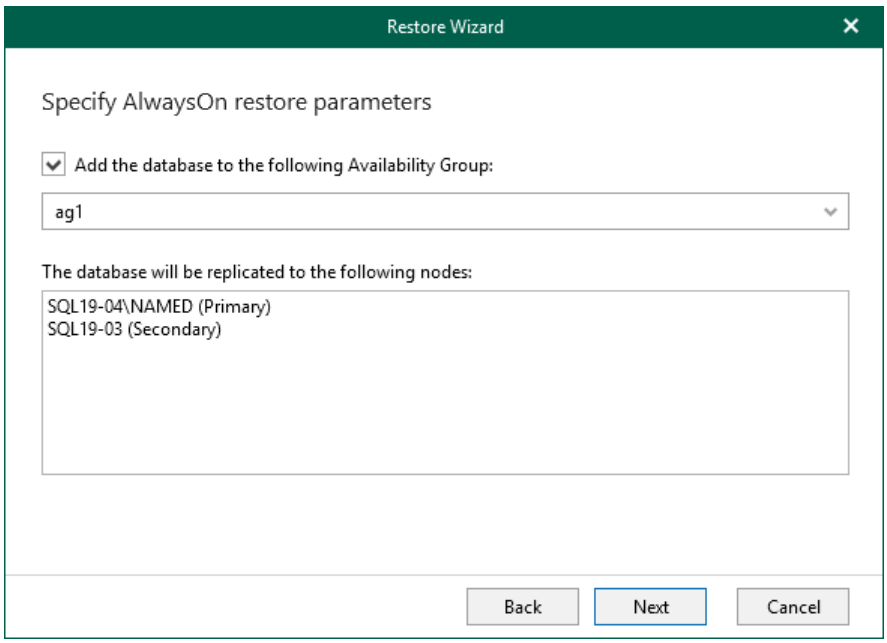
Step 5. Specify AlwaysOn Restore Options

If the specified target SQL Server supports AlwaysOn Availability Groups, you will be offered to specify AlwaysOn restore options. To use the AlwaysOn capabilities for the restored database, do the following:

1. Select the **Add the database to the following Availability Group** check box and select an availability group from the drop-down list.
2. In the **The database will be replicated to the following nodes** list, review information about the primary and secondary nodes of the availability group.

   During the restore process, Veeam Explorer for Microsoft SQL Server will restore the database to the primary server and then replicate it to secondary nodes.

If you do not plan to use the AlwaysOn capabilities when restoring a database, clear the **Add the database to the following Availability Group** check box.

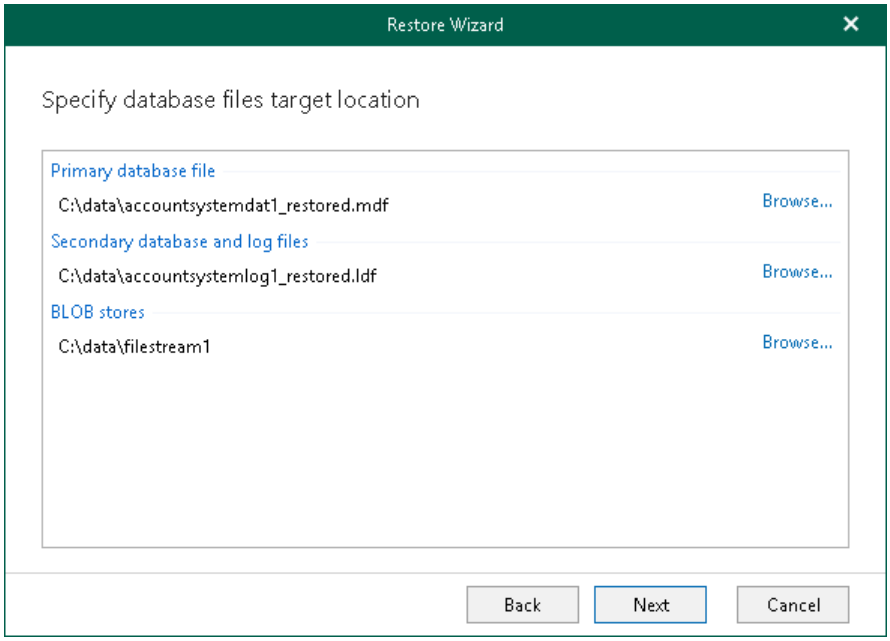


Step 6. Specify Files Location

At this step of the wizard, specify database files location.

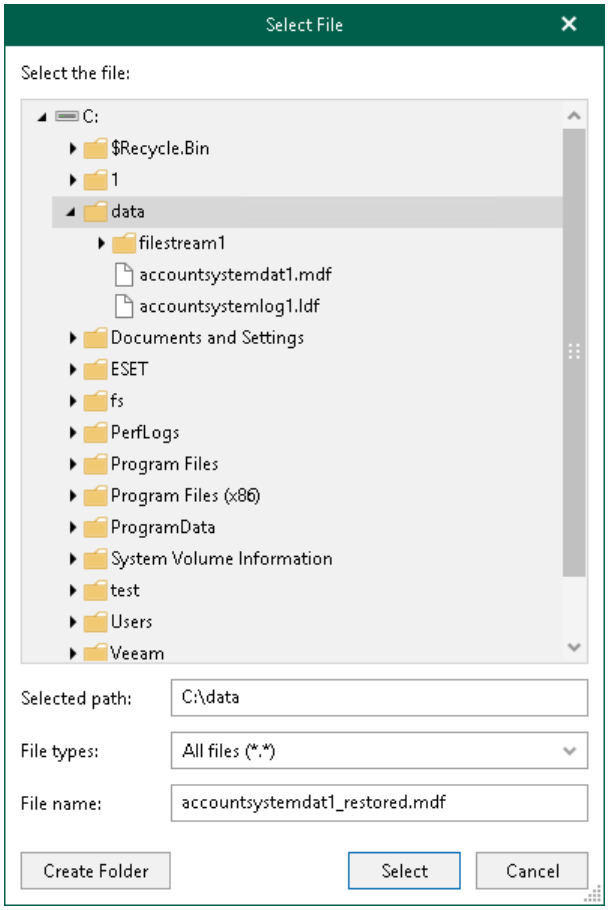
Click **Browse** to specify the path for the primary database file, secondary database and log files, as described in Selecting Files.

> **NOTE**
>
> Make sure the account you are using has **Read** and **Write** permissions.



Selecting Files

In the **Select File** dialog, select a database file or folder for the database being restored and click **OK**.



Step 7. Specify Recovery State

At this step of the wizard, select recovery state:

- **Default (RECOVERY)**

  Rolls back (*undo*) any uncommitted changes.

- **NORECOVERY**

  Skips the undo phase so that uncommitted or incomplete transactions are held open.

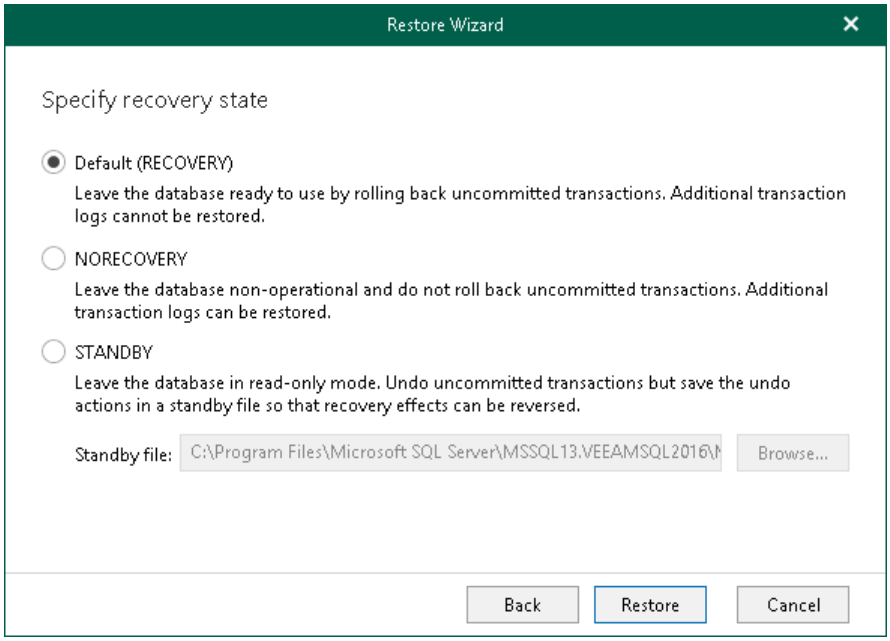
  This allows further restore stages to carry on from the restore point. When applying this option, the database will be in a *norecovery* state and inaccessible to users.

- **STANDBY**

  The database will be in *standby* state and therefore available for read operations. You can also provide a standby file with uncommitted transactions.

For more information on recovery modes, see this Microsoft article.

> **NOTE**
>
> This step is unavailable if the **Add the database to the following group** check box is selected at the Specify AlwaysON Restore Options step.



Restoring Multiple Databases

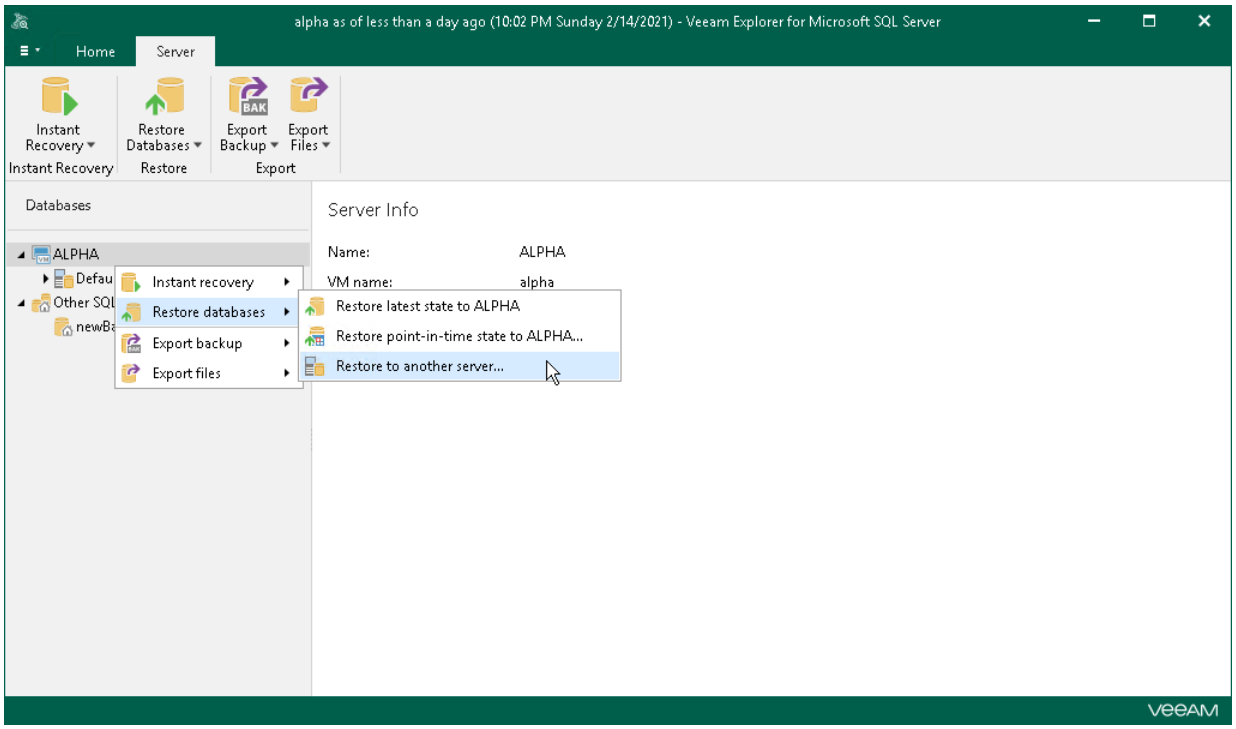
To restore multiple Microsoft SQL Server databases, do the following:

1. Launch the Restore wizard.
2. Specify a restore point.
3. Specify the target server.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select an instance or server.
2. On the **Server/Instance** tab, select **Restore Databases** > **Restore to another server** or right-click a database and select **Restore databases** > **Restore to another server**.

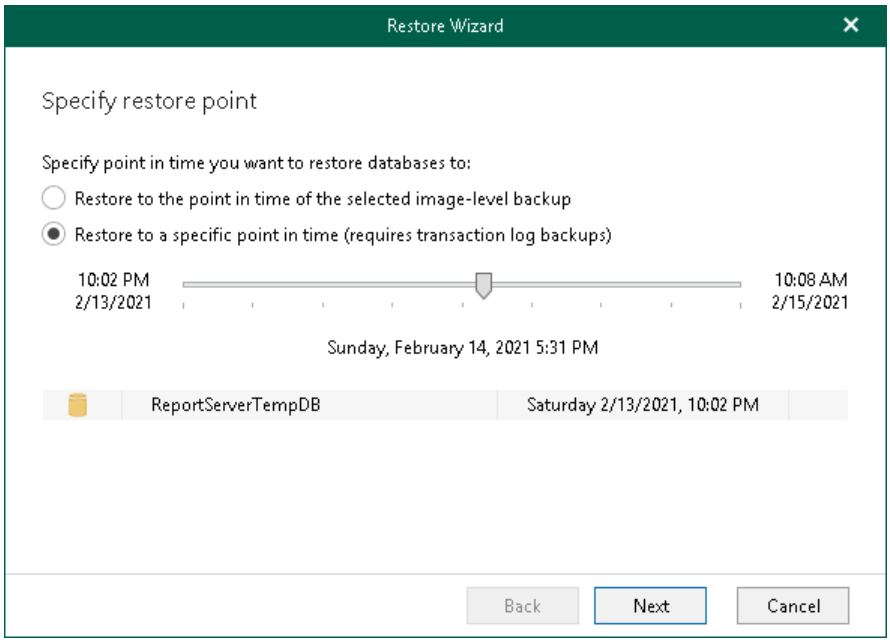


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.



Step 3. Specify Target Server

At this step of the wizard. specify the following:

- A production SQL Server VM name and/or SQL Server instance to which you want to restore your database.

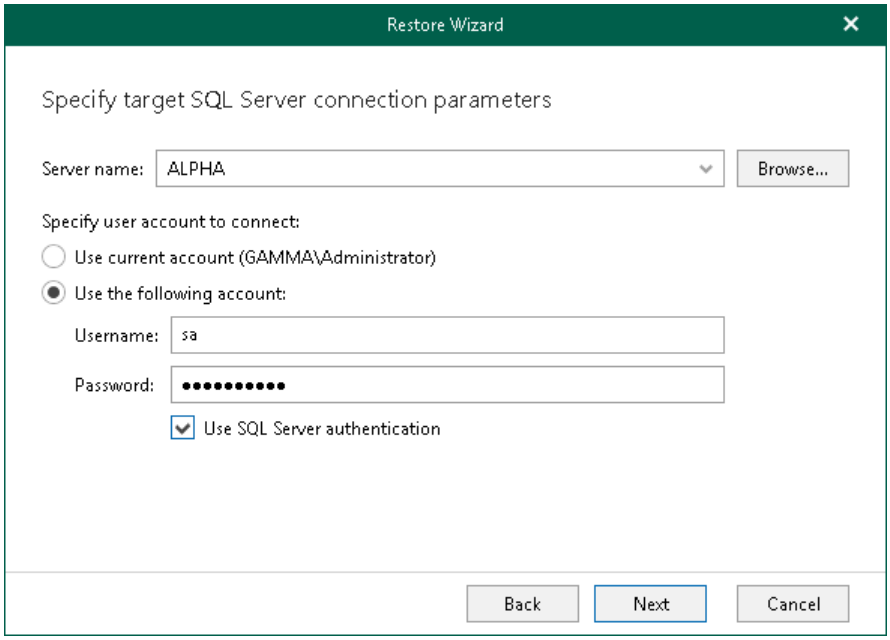
  Use the `server_name\instance` format. You can select a server or instance from the drop-down list or use the **Browse** button on the left, as described in Browsing for Servers.

- The user account to connect to the target SQL Server.

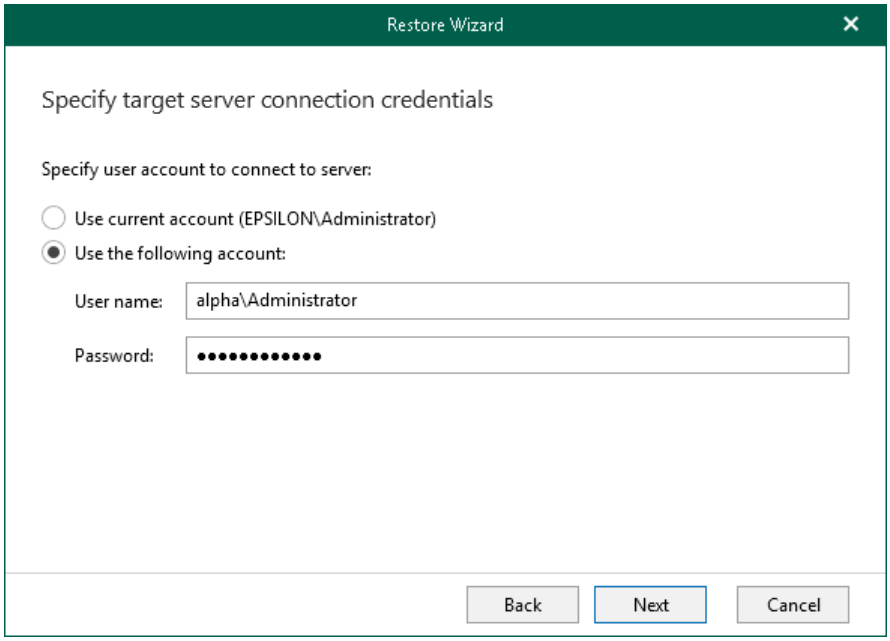
  Select the **Use SQL Server authentication** check box to use SQL Server authentication. If not selected, Veeam will use Windows authentication.

  Make sure the account you are using has been granted the **sysadmin** role on a target SQL Server.

> **IMPORTANT**
>
> Make sure that the administrative share (for example, `\\myserver\C$`) on a target machine is available. **Read** and **Write** are minimum required permissions, **Full Control** is recommended.



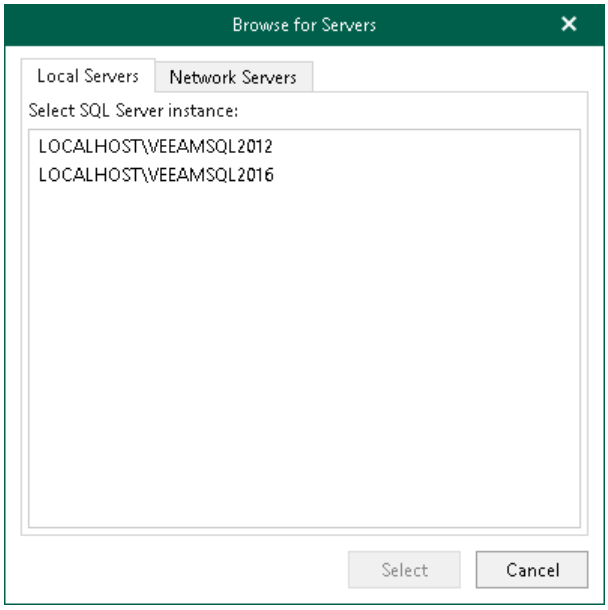
When selecting the **Use SQL Server authentication** check box and providing your SQL Server account, you will be asked to provide a target production server account in the next step, as shown below.



Browsing for Servers

To browse for a server, do the following:

- On the **Local Servers** tab, select a local SQL Server that is located on a machine with Veeam Explorer.
- On the **Network Server** tab, select an SQL Server VM over the network.



Restoring Database Schema and Data

To restore database schema and data, do the following:

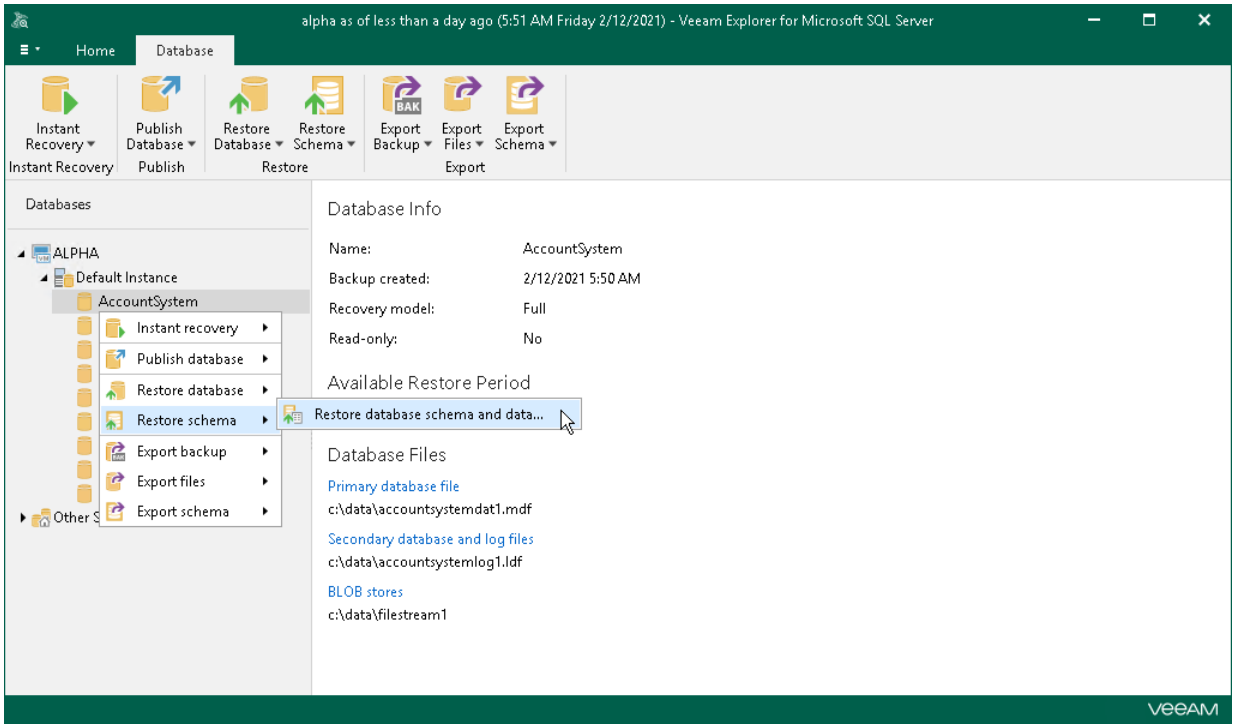
1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify target SQL server settings.
5. Select database objects.
6. Specify names for restored objects.
7. Specify directory names for file tables.
8. Specify additional restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Restore Schema** > **Restore database schema and data** or right-click a database and select **Restore schema** > **Restore database schema and data**.

> **IMPORTANT**
>
> Consider the following:
>
> - A staging SQL Server is required to perform a restore of database schema and data. For more information, see Configuring Staging SQL Server.
> - FILESTREAM must be enabled on a staging SQL Server to restore file tables. For more information on enabling FILESTREAM, see this Microsoft article.

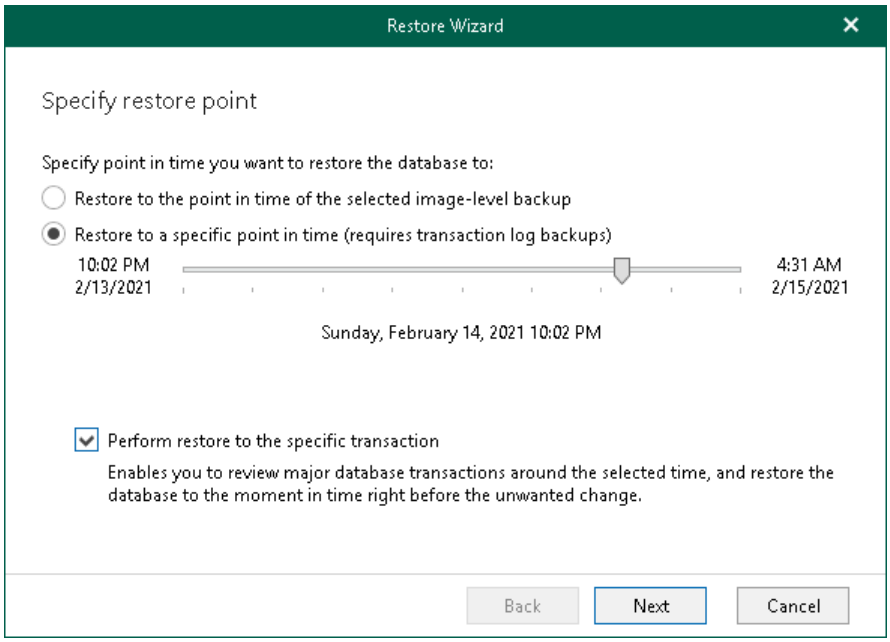


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

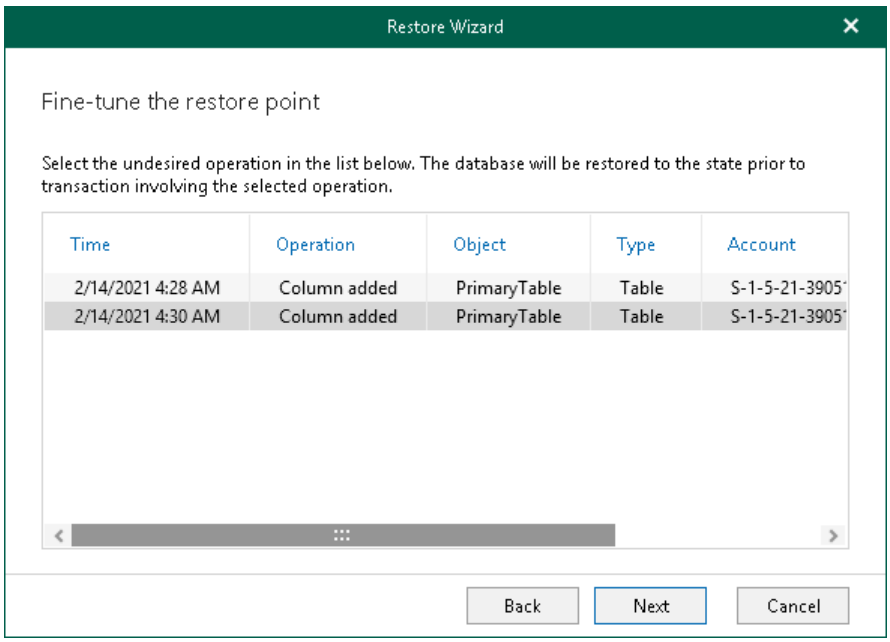


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to recover your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target SQL Server Settings

At this step of the wizard, specify the target SQL Server connection parameters:

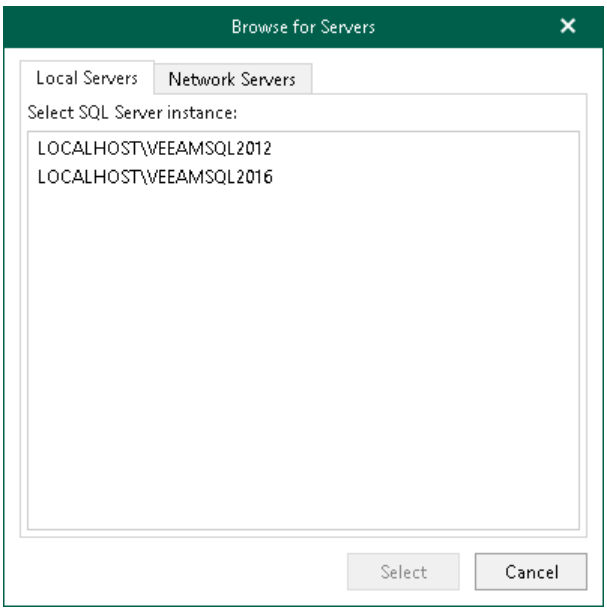
1. At the **Server name** field, specify the target SQL Server instance to which you want to restore your database.

   You can specify the instance name in the `server_name\instance` format. Also, you can select an instance from the drop-down list or use the **Browse** button on the right.

   To browse for another servers and SQL Server instances:

   a. Click the **Browse** button.

   b. You can select an SQL Server instance residing on the local machine on the **Local Servers** tab or click the **Network Servers** tab and select an instance on another server. Veeam Explorer displays servers from your network where Microsoft SQL Server is installed.

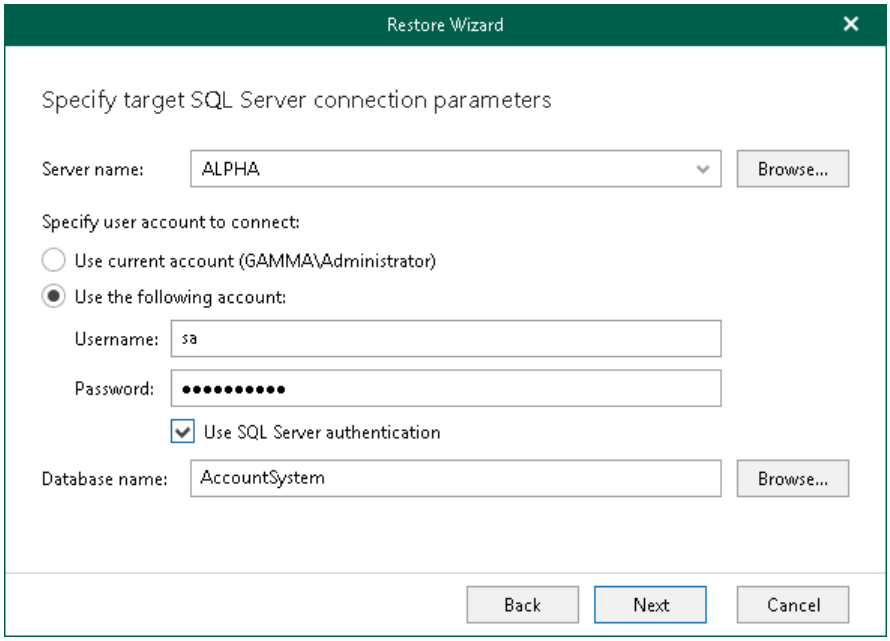


2. At the **Specify user account to connect** field, specify a user account that will be used connect to the target SQL Server machine.

   Select the **Use SQL Server authentication** check box to use SQL authentication. If not selected, Veeam Explorer will use Windows authentication.

   Make sure the account you are using has been granted the **sysadmin** role on the target SQL Server machine.

3. At the **Database name** field, specify the target database name. Click **Browse** to select a database to which you want to restore the schema.

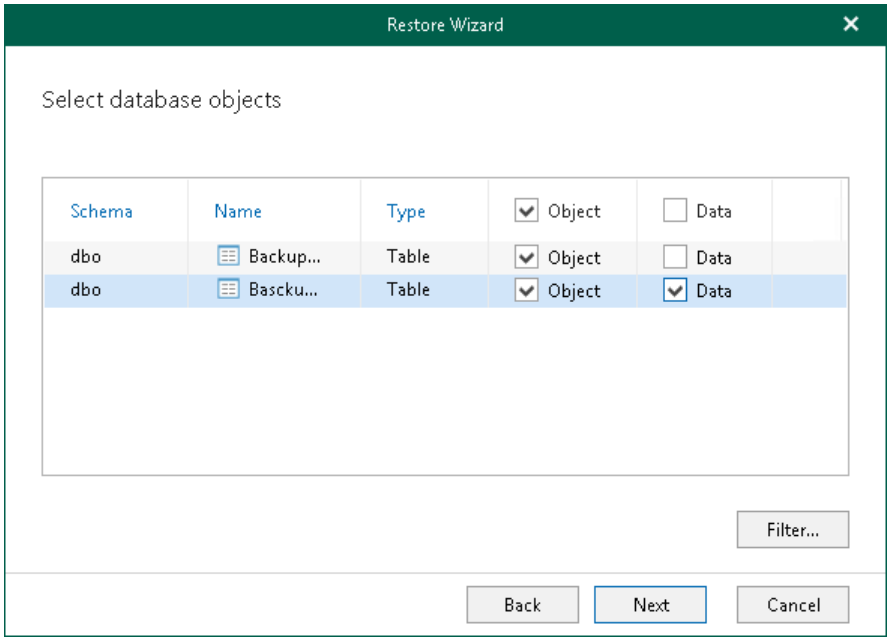


Step 5. Select Database Objects

At this step of the wizard, specify database objects you want to restore.

Use the **Object** and **Data** check boxes to specify what database objects and data should be restored.

To display only specific objects, click **Filter** and select the object type.

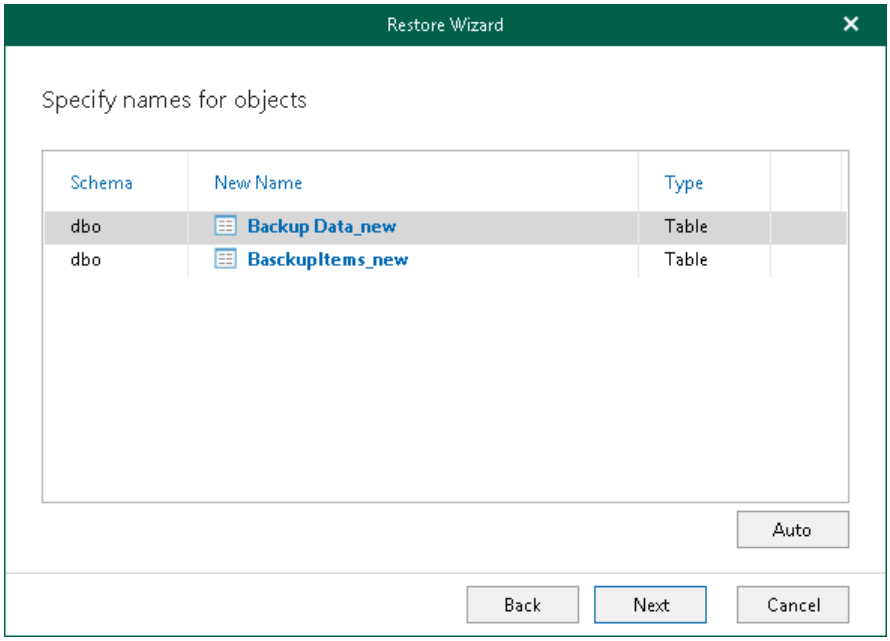


Step 6. Specify Names for Objects

At this step of the wizard, specify a new name for the object.

To specify a new name, select a database and provide a new name.

To assign a default name to the object that already exists, click **Auto**. In this case, the *_new* suffix will be added.



Step 7. Specify Directory Names for File Tables

At this step of the wizard, specify directory names for file tables.

The following options are available:

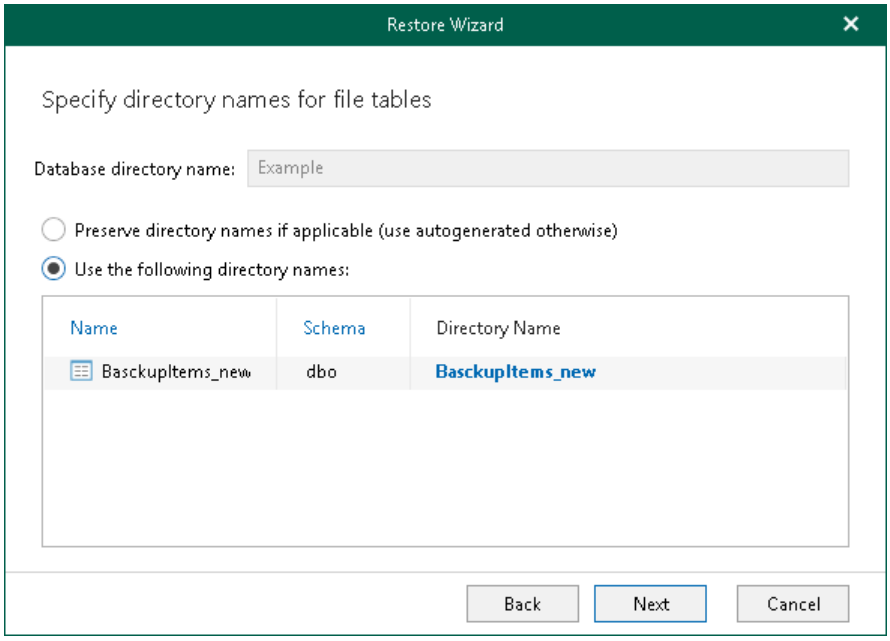
- **Preserve directory names if applicable (use autogenerated otherwise)**.

  To use the original names.

  If such names already exist on a target server, Veeam will add *_new* suffix to each name. For example, *<existing_name>_new*.

- **Use the following directory names**.

  To provide a different name under the **Directory Name** column.



Step 8. Specify Additional Restore Options

At this step of the wizard, specify additional restore options and click **Restore**.

- Select how the file groups should be restored for selected schema objects:
  - **Preserve filegroup if applicable**

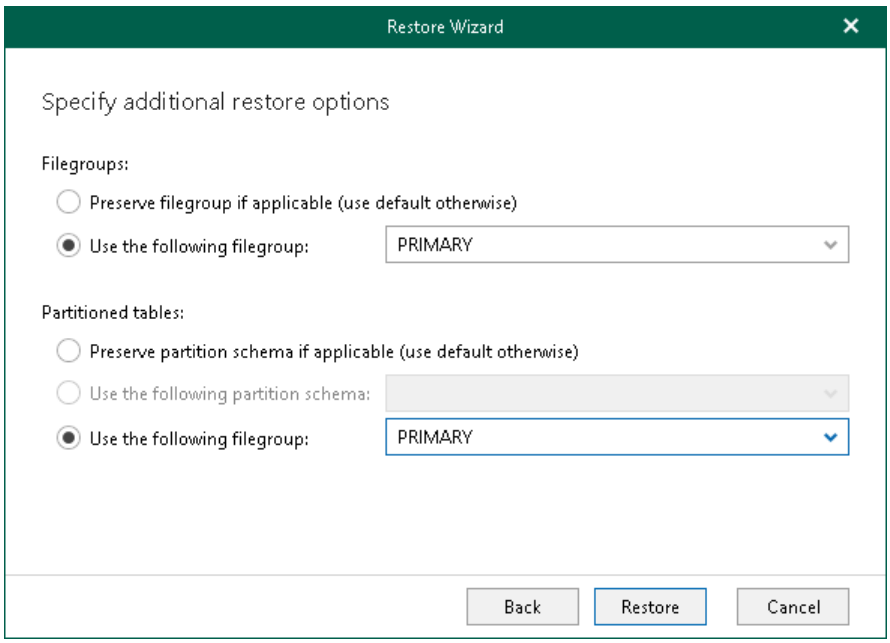
    To preserve the file group state.
  - **Use the following filegroup**

    To select a file group on a target SQL Server instance.
- Select how partitioned tables should be restored:
  - **Preserve partition schema if applicable**

    To restore tables to the original partition schema.
  - **Use the following partition schema**

    To select a partition schema on a target SQL Server instance.
  - **Use the following filegroup**

    To select a file group on a target SQL Server instance.



Restoring Latest or Point-in-Time State

This section explains how to select a state as of which you want to restore your databases.

You can select either of the following states:

- *The latest available state*

  To restore your data as of the latest state in your backup file.

- *The point-in-time state*

  To restore your data as of the selected point-in-time state (requires log backup).

The data will be restored in the following manner:

- Database files will be copied to the original location and then mounted to the original SQL Server.
- If a database with the same name already exists on a target SQL Server, it will be replaced with the database from a backup file.

Restore Point-in-Time State

To restore SQL Server databases as of the point-in-time state, do the following:

1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

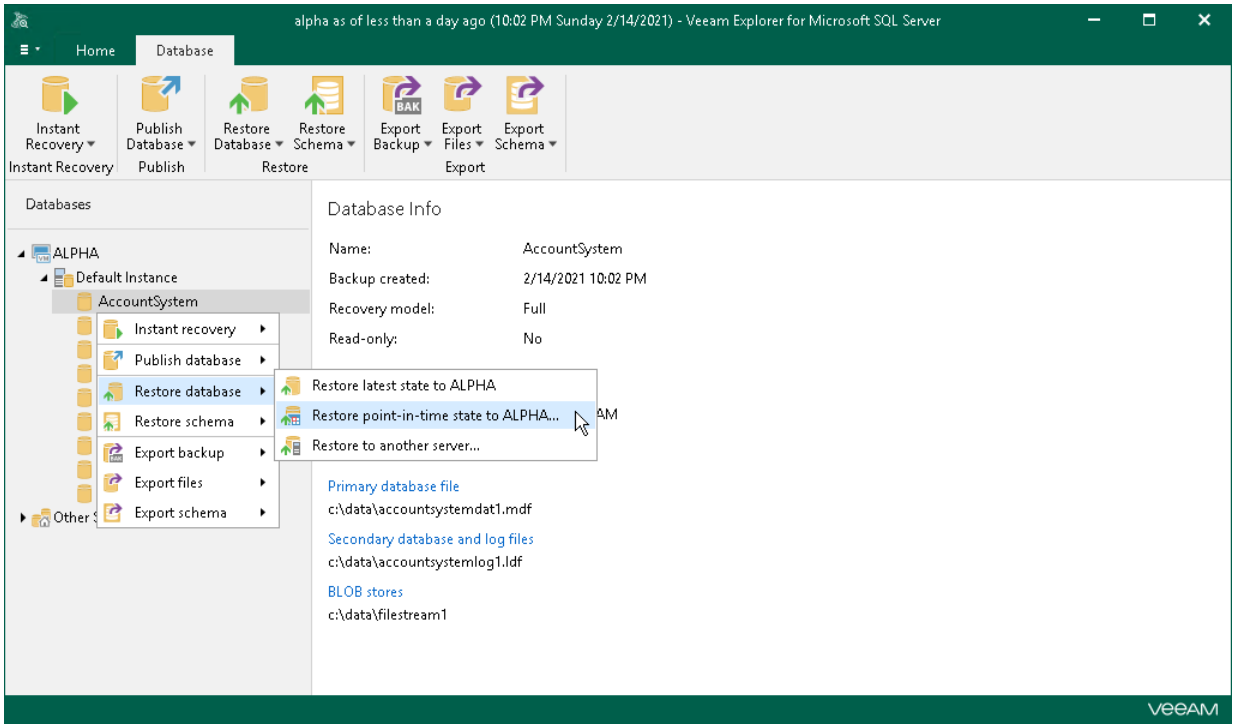
1. In the navigation pane, select a database or an instance.

   You can select the root instance node to restore all the available databases at once.

2. On the **Database** tab, select **Restore Database > Restore point-in-time state to *<server_name>*|*<instance_name>*** or right-click a database and select **Restore database > Restore point-in-time state to *<server_name>*|*<instance_name>***.

When restoring multiple databases, consider that depending on the database recovery model the following cases are possible:

- Some databases might be restored as of the different time interval.
- Some databases cannot be restored if there are no transaction logs available for the specified period.



Step 2. Specify Restore Point

At this step of the wizard, specify a state to which you want to restore your database:

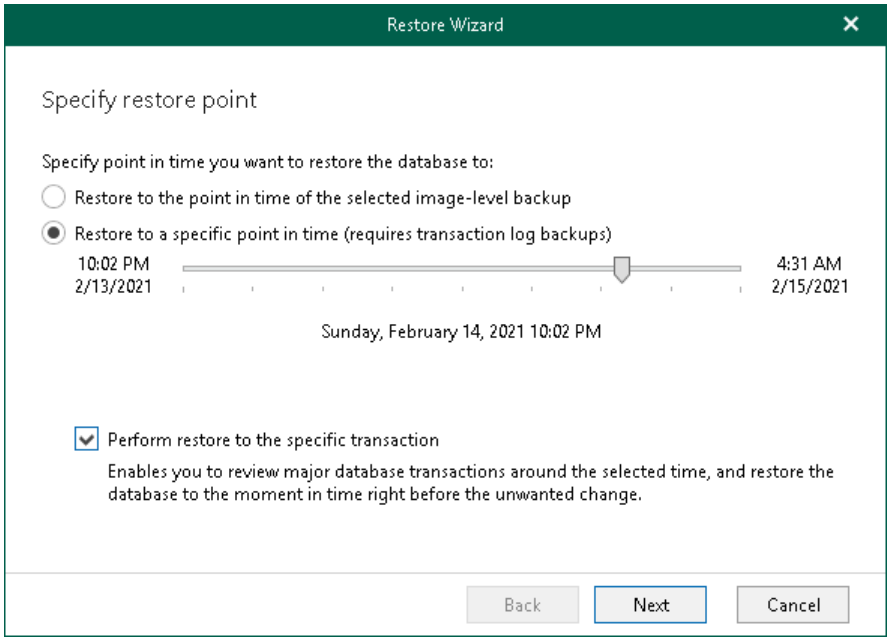
1. In the **Specify point in time you want to restore the database to** section, select one of the following options:
   - **Restore to the point in time of the selected image-level backup**. Select this option to load database files as per date of the current restore point.
   - **Restore to a specific point in time**. Select this option to load database files as per selected point in time. Use the slider control to choose a point you need.

     This option is available in case the following conditions are met:

     - [For restore from a backup created by a backup job] The backup is created by a job that is set to back up transaction logs or process transaction logs in the copy only mode.
     - [For restore from a backup created by a backup copy job] The backup is created by a job that is set to process transaction logs.
     - The recovery model for the database is set to *full* or *bulk-logged*.
2. [Optional] Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions. If you select this option, you will be able to specify an exact transaction at the next step of the wizard.

   This option requires a staging SQL Server. For more information, see Configuring Staging SQL Server.

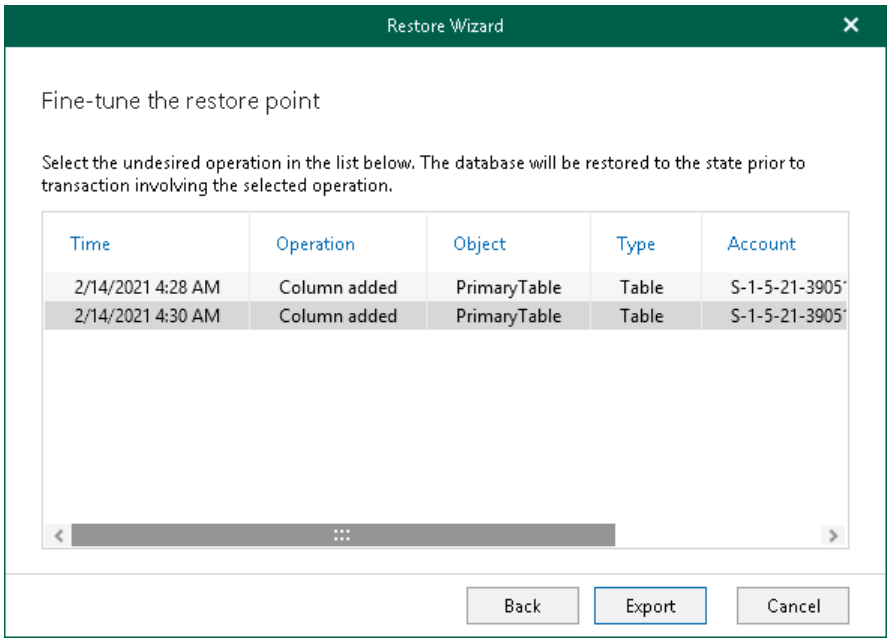
   This option is unavailable when restoring multiple databases.



Step 3. Fine-Tune Restore Point

This step is available if you have selected the **Perform restore to the specific transaction** check box at the previous step of the wizard. At this step, select an operation prior to which you want to recover your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.



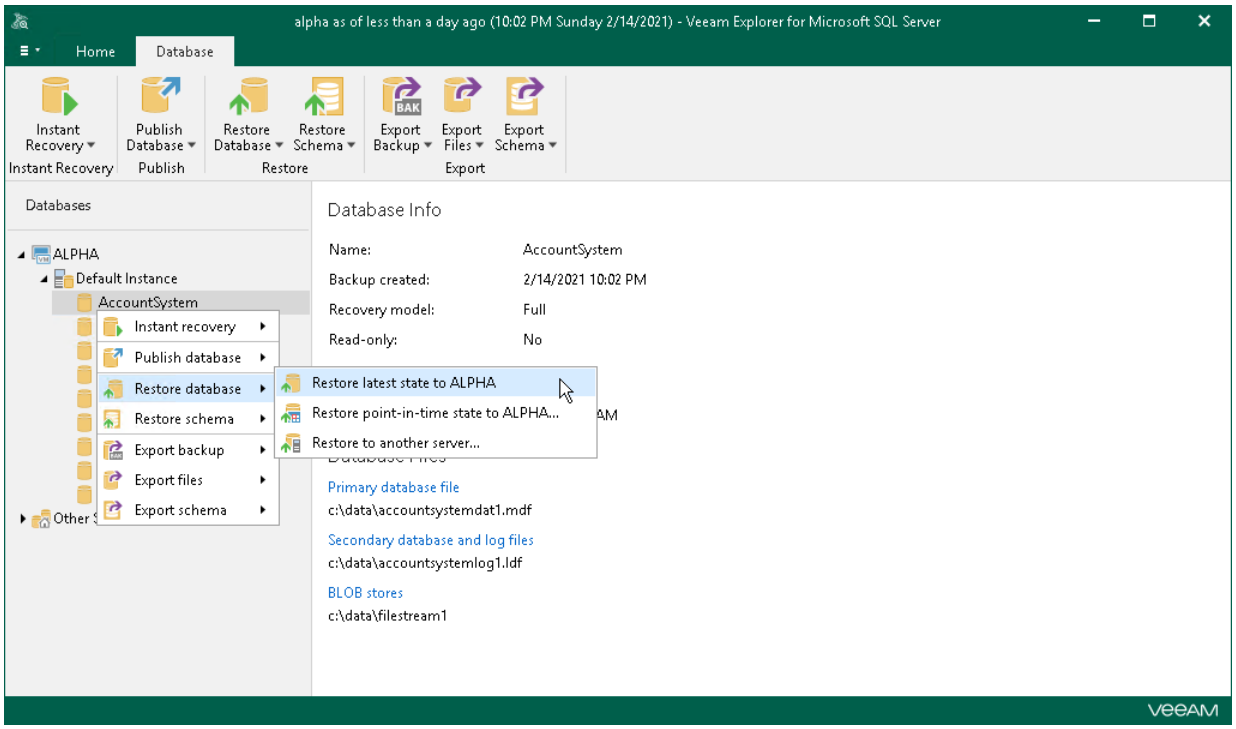
Restore Latest State

To restore your data as of the latest available state, do the following:

1. In the navigation pane, select a database or an instance.

   You can select the root instance node to restore all the available databases at once.

2. On the **Database** tab, select **Restore Database > Restore latest state to <server_name>\<instance_name>** or right-click a database and select **Restore Database > Restore latest state to <server_name>\<instance_name>**.



Data Publishing

Publishing databases allows you to temporarily attach large SQL Server databases to the target Microsoft SQL Server without having to restore them.

Publishing databases typically occurs faster than using standard restore features and might be convenient in certain cases, for example, when your time to perform disaster-recovery operations is limited.

> **TIP**
>
> Before publishing data, make sure to read Considerations and Limitations.

Publishing to Specified Server

Publishing to the specified server allows you to select a target SQL server to which you can publish your databases.

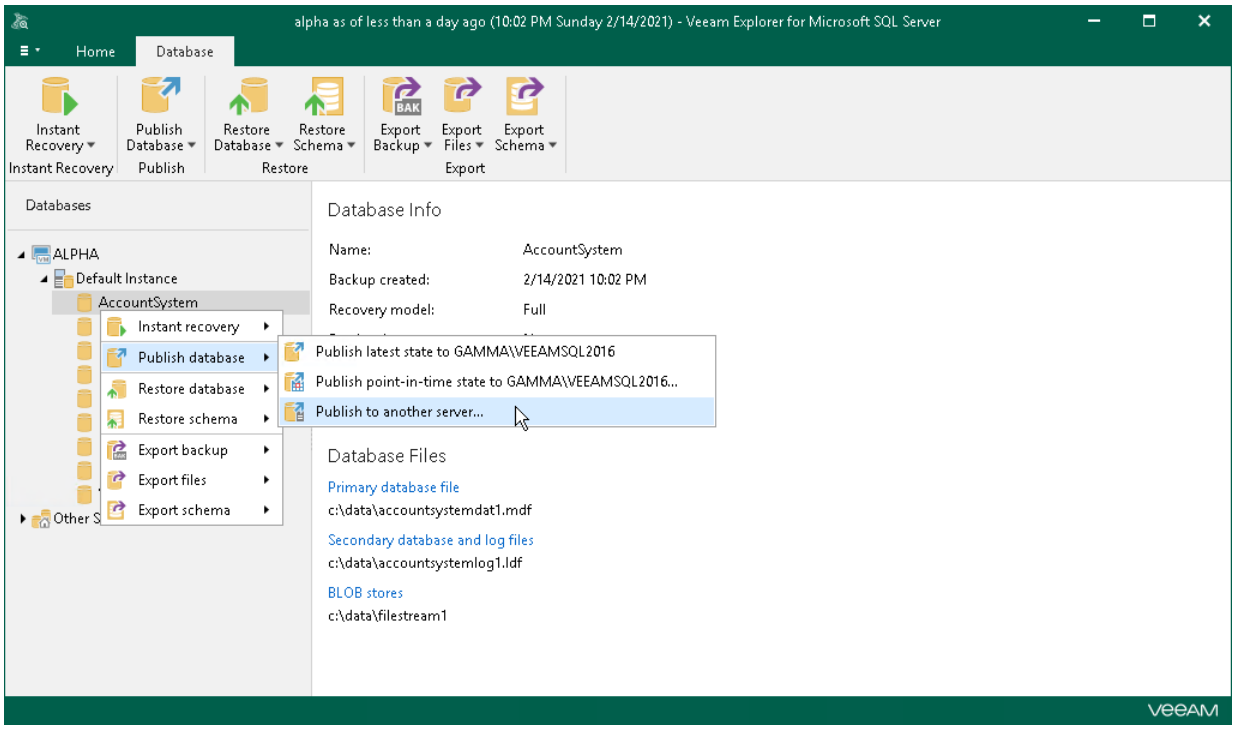
To publish data, do the following:

1. Launch the Publish Database wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.

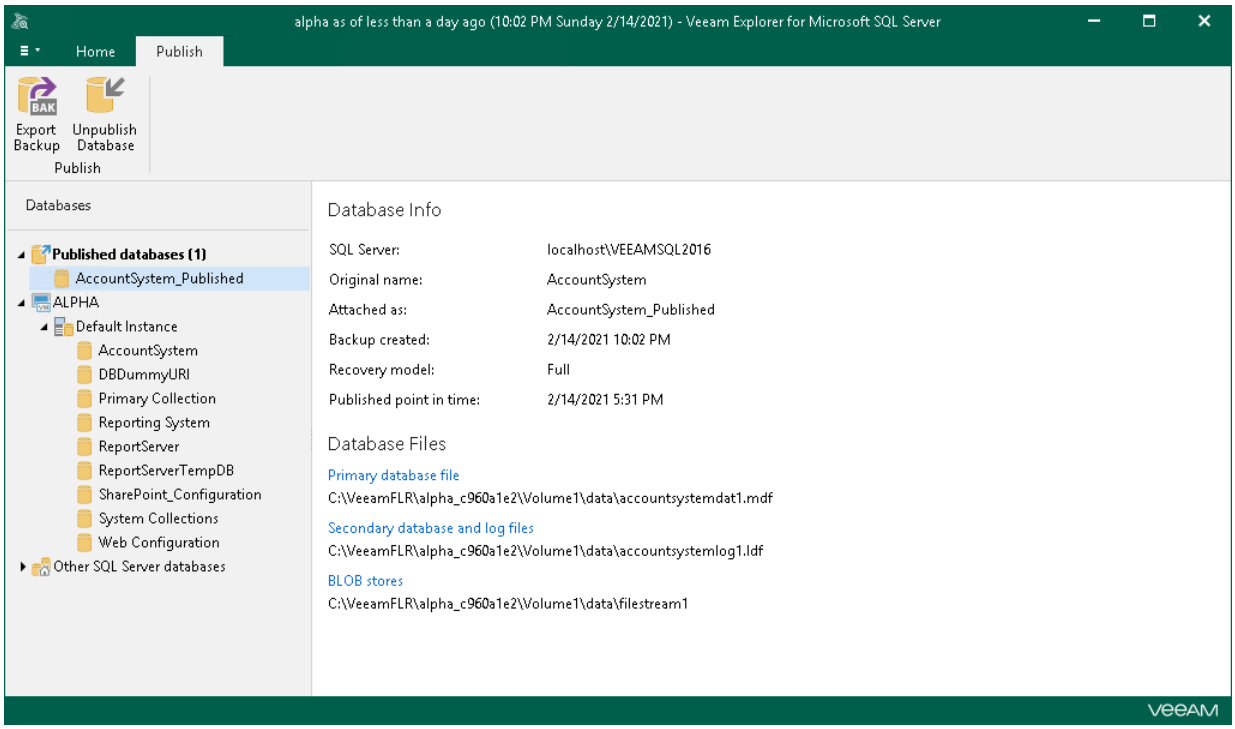
Step 1. Launch Publish Database Wizard

To launch the **Publish Database** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish to another server** or right-click a database and select **Publish database** > **Publish to another server**.

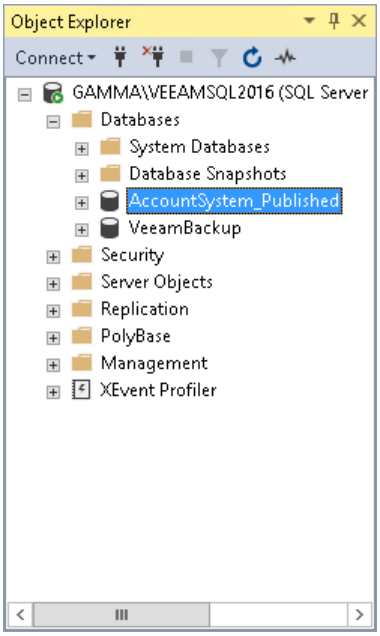


After you complete the wizard steps, a new **Published databases** node appears at the top of the navigation pane. Under this node, you can find the databases that have been published during the current session of Veeam Explorer for Microsoft SQL Server.



To work with published databases, open a SQL tool you prefer, for example, *Microsoft SQL Management Studio* and locate your published databases.

The figure below demonstrates a published database (*AccountSystem_Published*) available in the **Object Explorer** window of your *Microsoft SQL Server Management Studio* console. This database is also being referenced by Veeam Explorer for Microsoft SQL Server under its **Published databases** node.



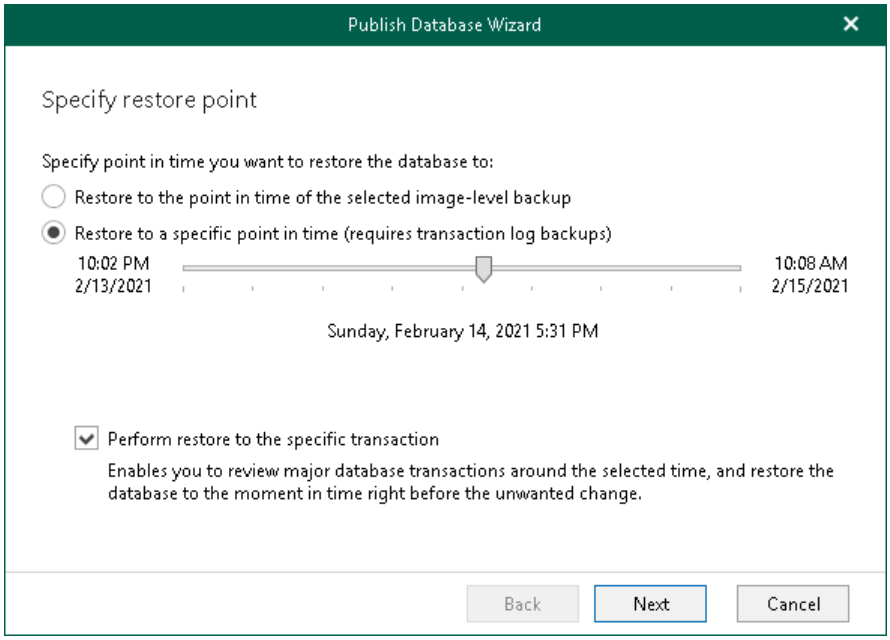
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

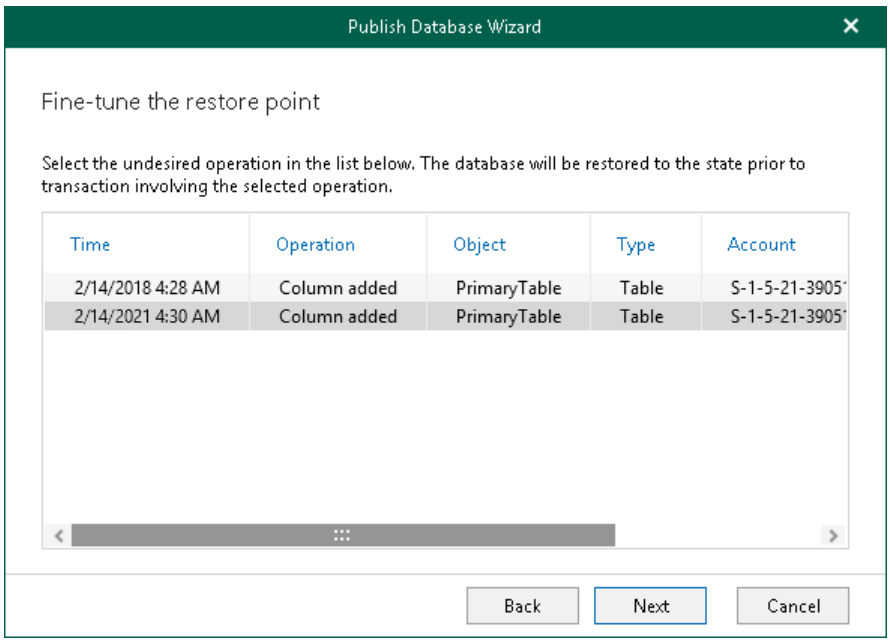


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target Server

At this step of the wizard, do the following:

- In the **Server name** field, specify a target SQL server name/SQL server instance/SQL cluster to which you want to restore your database.

  Use the `server_name\instance` format. You can select a server/instance/cluster from the drop-down list or use the **Browse** button on the left, as described in Browsing for Servers.

- In the **Database name** filed, specify a new name under which you want to publish your database.

  Consider that if you leave the original database name, Veeam Explorer for Microsoft SQL Server will overwrite the associated database on the target server.

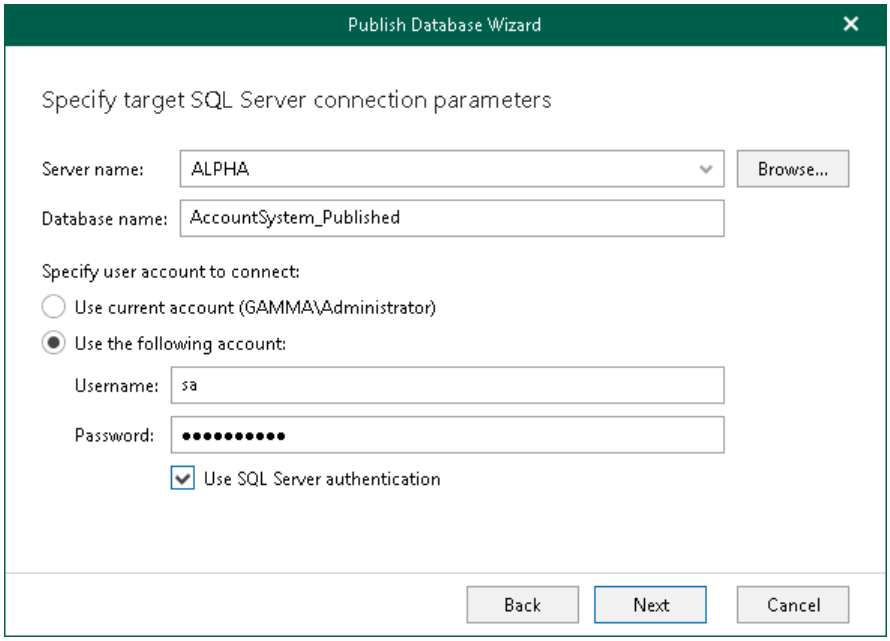
- Under the **Specify user account to connect to server** section, select either of the following options:

  - **User current account**. To use the current account under which Veeam Explorer for Microsoft SQL Server is running.
  - **User the following account**. To use a custom account.

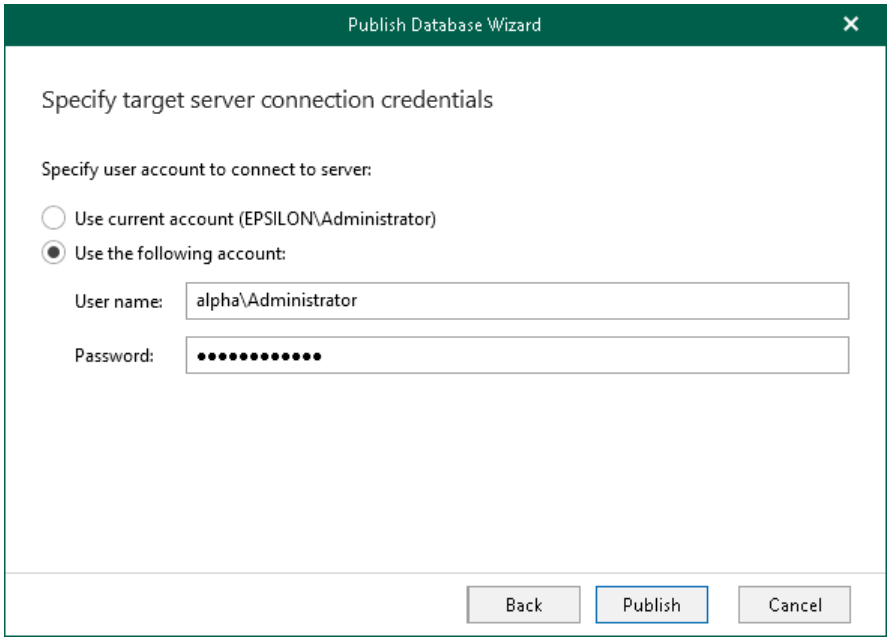
    Make sure the account you are using has been granted the **sysadmin** role on the target server.

- Select the **Use SQL Server authentication** check box to use SQL authentication.

> **NOTE**
>
> Make sure that the administrative share for example, `\\myserver\ADMIN$`) on a target machine is available; **Read** and **Write** are minimum required, **Full Control** is recommended.



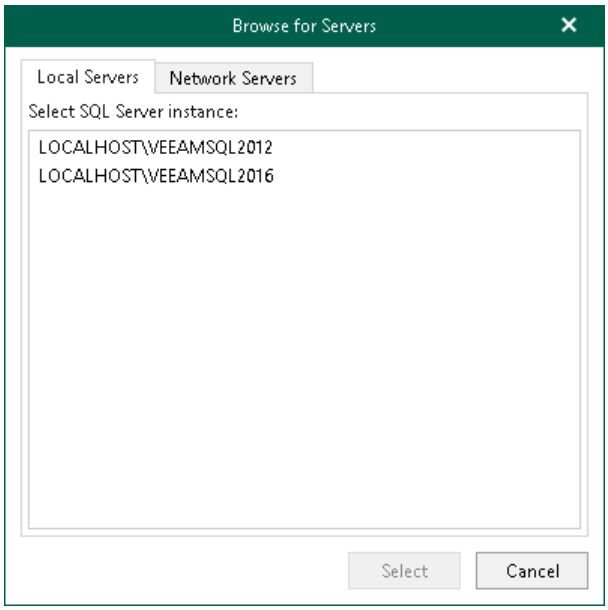
When selecting the **Use SQL Server authentication** check box and providing a SQL server account, you will be asked to provide a target server account in the next step, as shown below.



Browsing for Servers

To browse for a server to which you want to restore your databases, do the following:

- On the **Local Servers** tab, select a local SQL server/instance/cluster that is located on a machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Server** tab, select a SQL server/instance/cluster over the network.



Publishing Latest or Point-in-Time State

This section explains how to select a state as of which you want to publish your databases.

You can select either of the following states:

- *The latest available state*

  To publish your data as of the latest state in your backup file.

- *The point-in-time state*

  To publish your data as of the selected point-in-time state (requires a log backup).

These options are available only after the initial publising of a database, as described in Publishing to Specified Server.

When you unpublish a database, both options continue to remain until you close the application so that you can quickly republish a database if needed.

Publishing Point-in-Time State

Publishing a point-in-time state allows you to obtain a required database state and unroll specified transactions if needed.

To publish databases as of the point-in-time state, do the following:

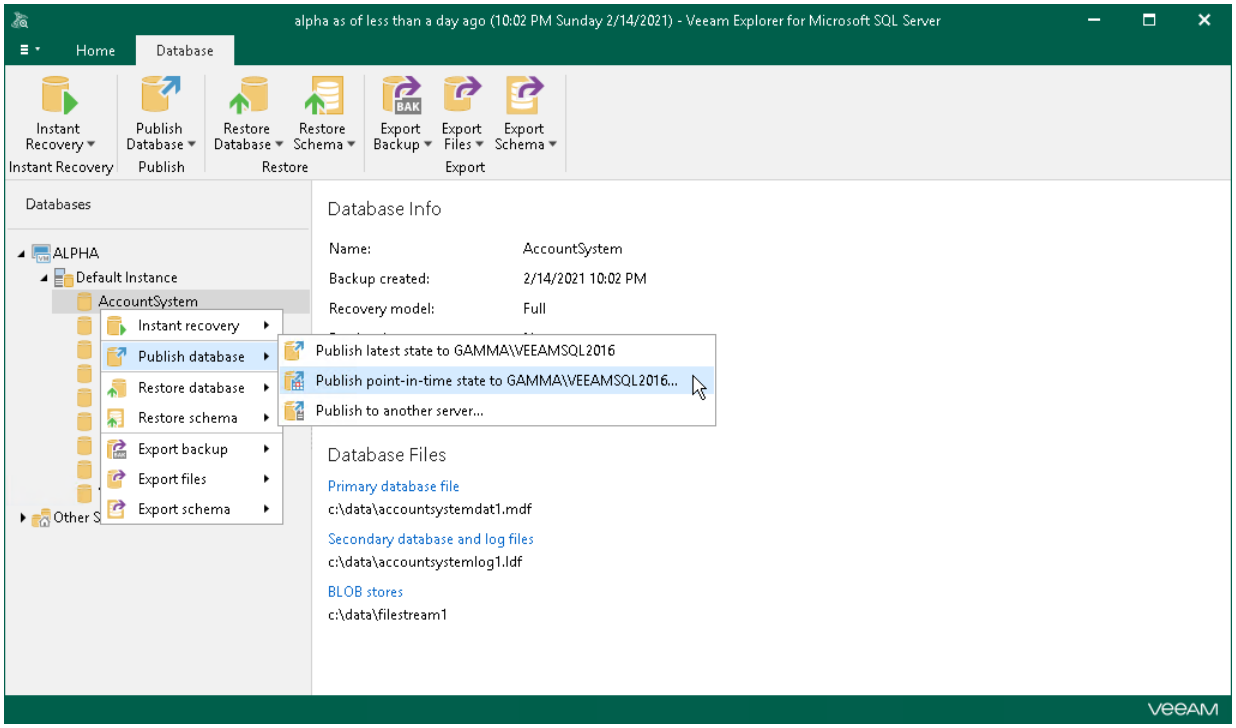
1. Launch the Publish Database wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Publish Database Wizard

To launch the **Publish Database** wizard, do the following:

1. In the navigation pane, right-click a database.
2. On the **Database** tab, select **Publish Database** > **Publish point-in-time state to <server_name>\<instance_name>** or right-click a database and select **Publish database** > **Publish point-in-time state to <server_name>\<instance_name>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



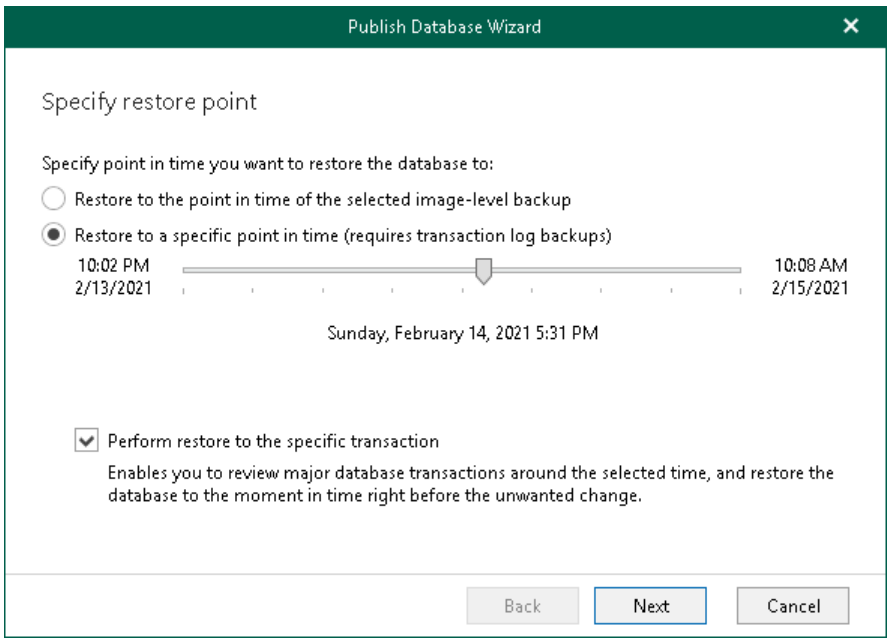
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL Server. For more information, see Configuring Staging SQL Server.

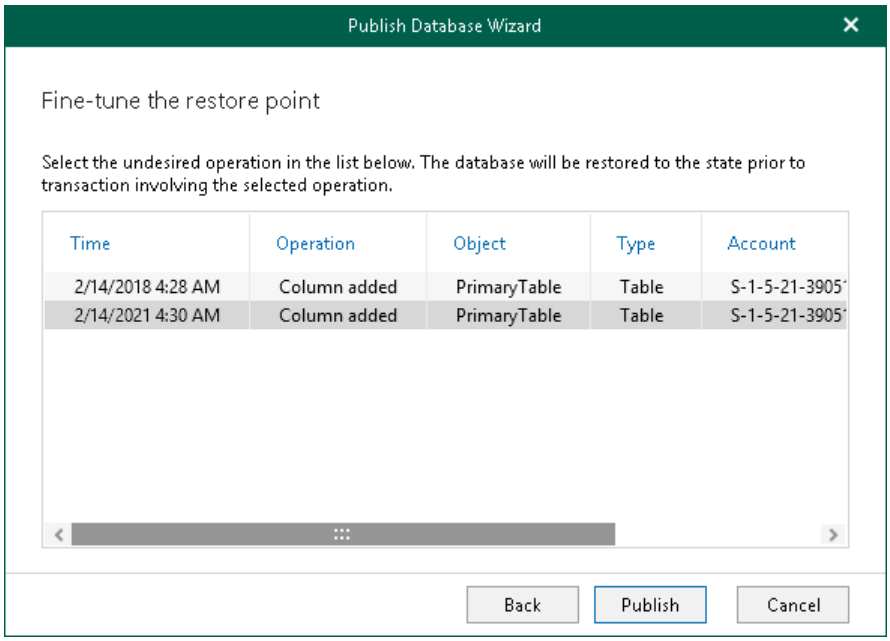


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



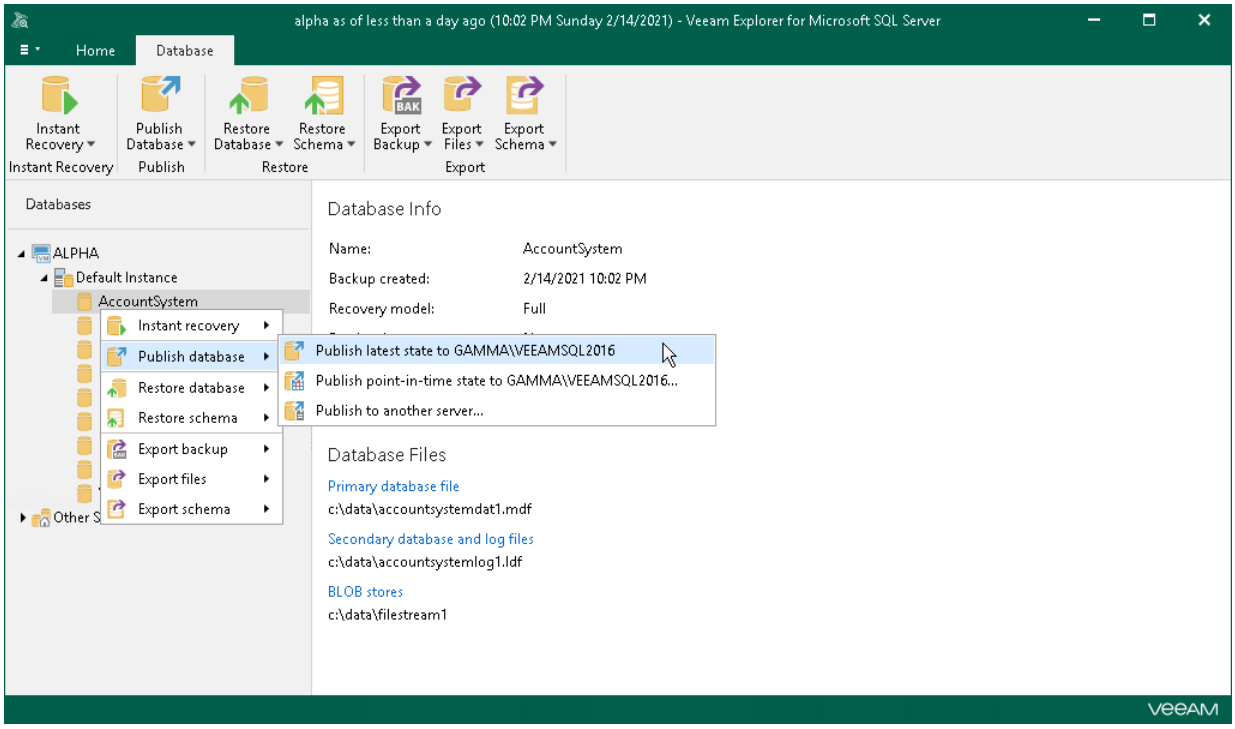
Publishing Latest State

Veeam Explorer for Microsoft SQL Server allows you to republish an unpublished database. When republishing a database, it will be attached to the target SQL server as of the latest state.

To republish a database as of the latest available state, do the following:

1. In the navigation pane, right-click a database.
2. On the **Database** tab, select **Publish Database** > **Publish latest state to <server_name>\<instance_name>** or right-click a database and select **Publish database** > **Publish latest state to <server_name>\<instance_name>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



Unpublishing Databases

Once you have done working with published SQL databases, you may want to unpublish (detach) these databases from the target SQL server.

Detachment occurs in the following manner:

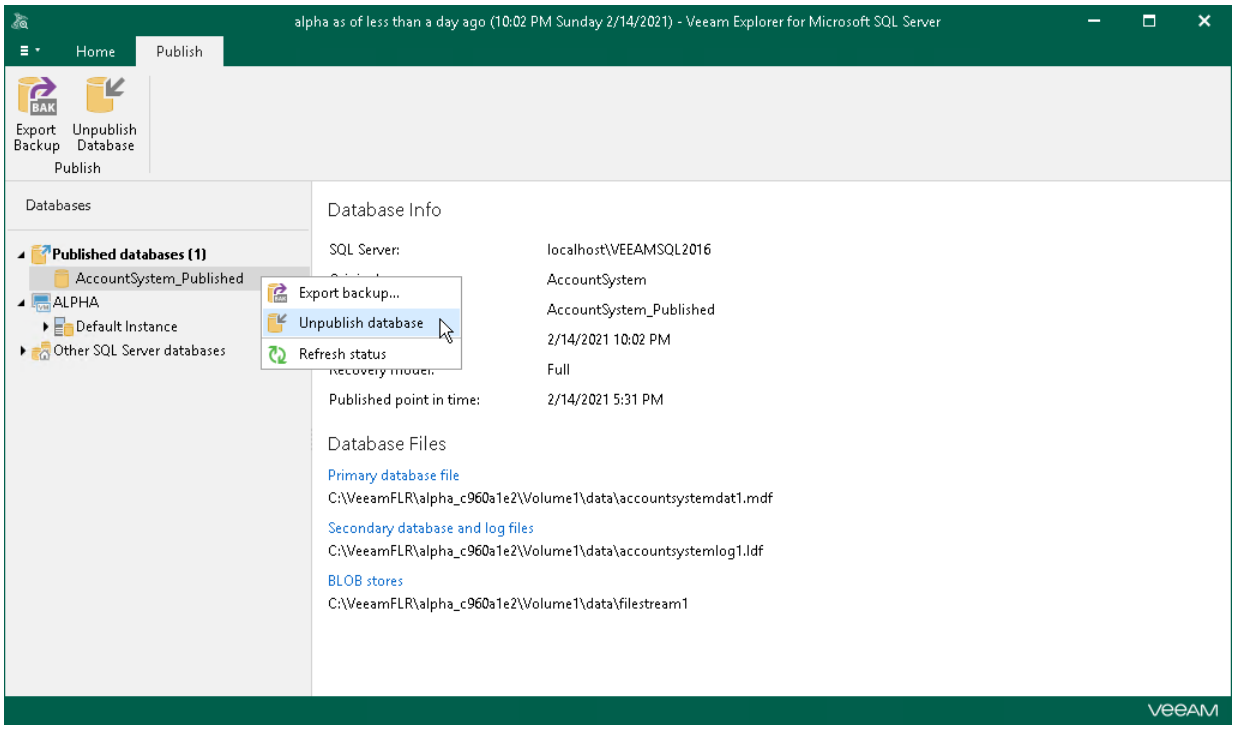
- Upon closing the Veeam Explorer for Microsoft SQL Server console, all published databases will be detached from the target SQL server automatically. The corresponding mount points will also be dismounted from under the *C:\VeeamFLR* directory.
- On manual unpublishing, databases will be detached at once but the restore point will remain mounted on the target machine for the next 15 minutes.

To unpublish a database manually, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Unpublish Database**.

Alternatively, in the navigation pane, right-click a published database and select **Unpublish database**.

To detach more than one published database simultaneously, right-click the root **Published databases** node and select **Unpublish databases** or select the root **Published databases** node and click **Unpublish Databases** on the **Publish** tab.

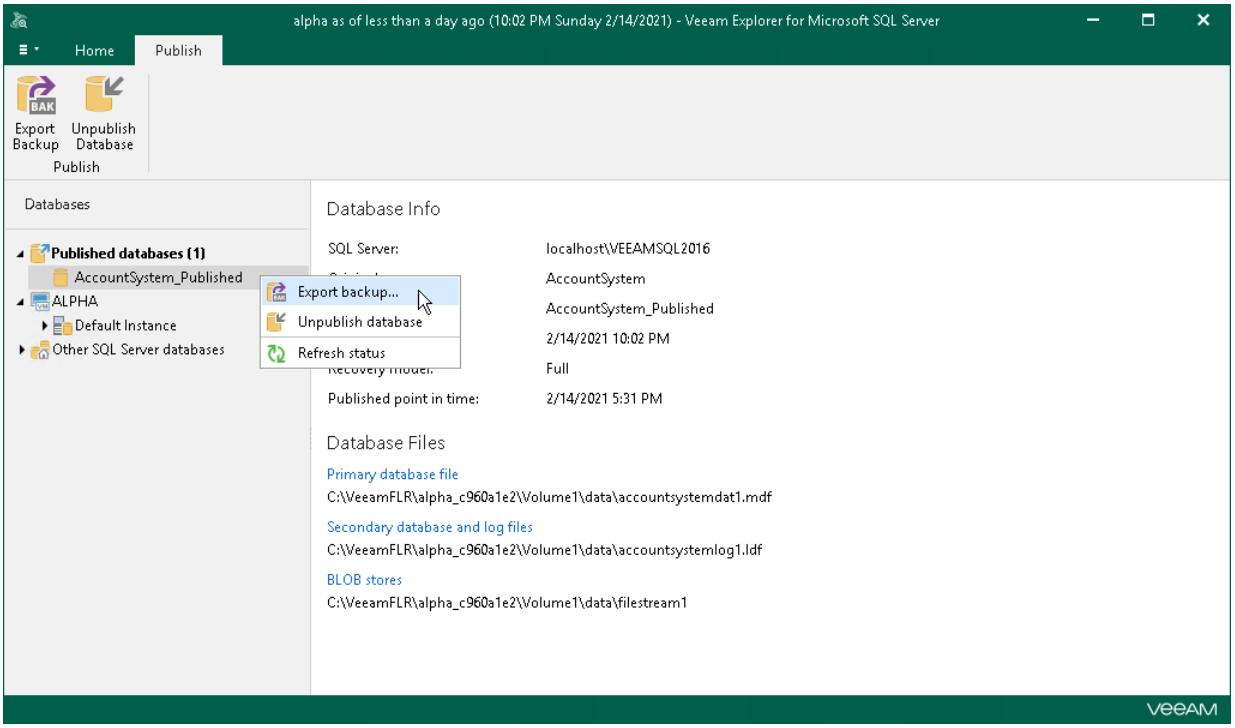


Exporting as BAK

To save changes that have been made while working with your published database to a local computer, you can use the export feature. This feature will export modified databases as BAK, preserving all the changes that have been done during the publishing session.

To export a published database, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Export backup** or right-click a database and select **Export backup**.

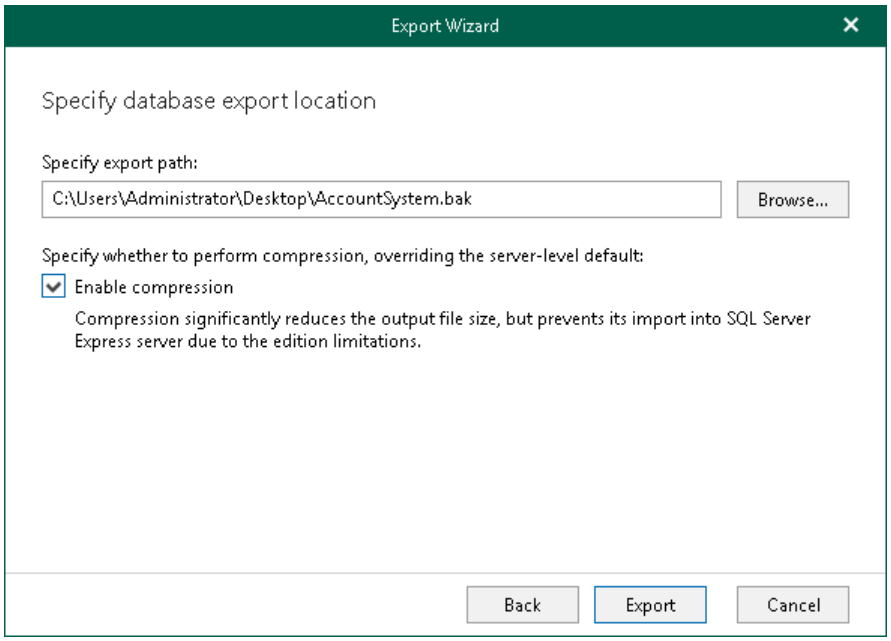


2. In the **Export** wizard, click **Browse** next to the **Specify export path** field to specify the location where to export your data.

   To compress data, select the **Enable compression** check box. Compression will be applied according to your SQL server configuration.

NOTE

Compression is unavailable for Microsoft SQL Server 2005 and all Express Editions of Microsoft SQL Server.

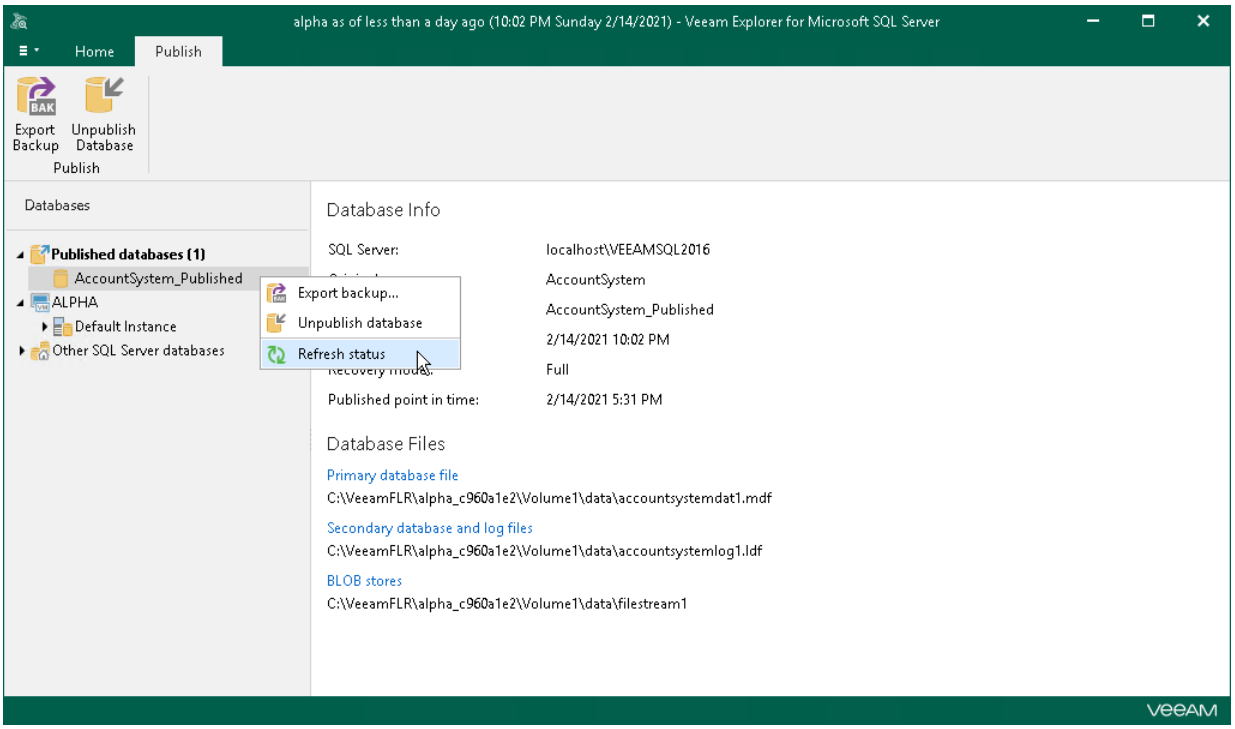


Refreshing Database Status

While the databases are attached to the target SQL server, Veeam Explorer for Microsoft SQL Server synchronizes each published database state to verify its availability. By default, synchronization occurs every five seconds.

If something went wrong with any of the published databases, the question mark appears next to each of such databases indicating the database unavailability. In the **Database Info** section, you will also see the notification message describing the problem.

To refresh a published database state manually, in the navigation pane, under the **Published databases** node, right-click a published database and select **Refresh status**.



Instant Recovery

Instant recovery combines capabilities of the data restore and data publishing features. If you want databases to be online as quickly as possible, you can use the **Instant Recovery** option and restore databases in the background.

> **IMPORTANT**
>
> Before performing instant recovery, make sure to read Considerations and Limitations.

How It Works

To perform instant recovery, Veeam Explorer for Microsoft SQL Server uses the *Veeam Explorers Recovery Service* that runs in the background. This removes the necessity to keep Veeam Explorer running during an entire instant recovery session. Once you have started an instant recovery session, you can close Veeam Explorer and then launch it later when necessary.

When you start an instant recovery session in Veeam Explorer for Microsoft SQL Server, the following happens:

1. Veeam Explorer uses backup files to start two iSCSI mount sessions in parallel:
    - The first mount is used to publish the database on the target production server and attach it to the target SQL Server instance.
    - The second mount is used to copy database files to the target server in the background.
2. While the published database is online, all changes in database files that occur after publishing are saved in cache on the mount server.
3. After all database files are copied to the target server, Veeam Explorer uses the cache to synchronize changes in database files.
4. After the synchronization, you can switch over to the up-to-date copy of the database on the production server. Depending on the option you choose, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization. During switchover, Veeam Explorer does the following:
    a. Stops the published database.
    b. Uses the cache to synchronize differences between the published database and the copied database files.
    c. Drops the published database.
    d. Starts the recovered database.

Instant recovery session is resilient to network disruption, backup server or mount server crash. If anything disrupts the restore process, the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch retry after the server or network is up.

Instant Recovery of Multiple Databases

You can perform instant recovery of multiple Microsoft SQL Server databases hosted on a server or a certain SQL Server instance. You can perform instant recovery to the original server or any other server in your network where SQL Server is installed.

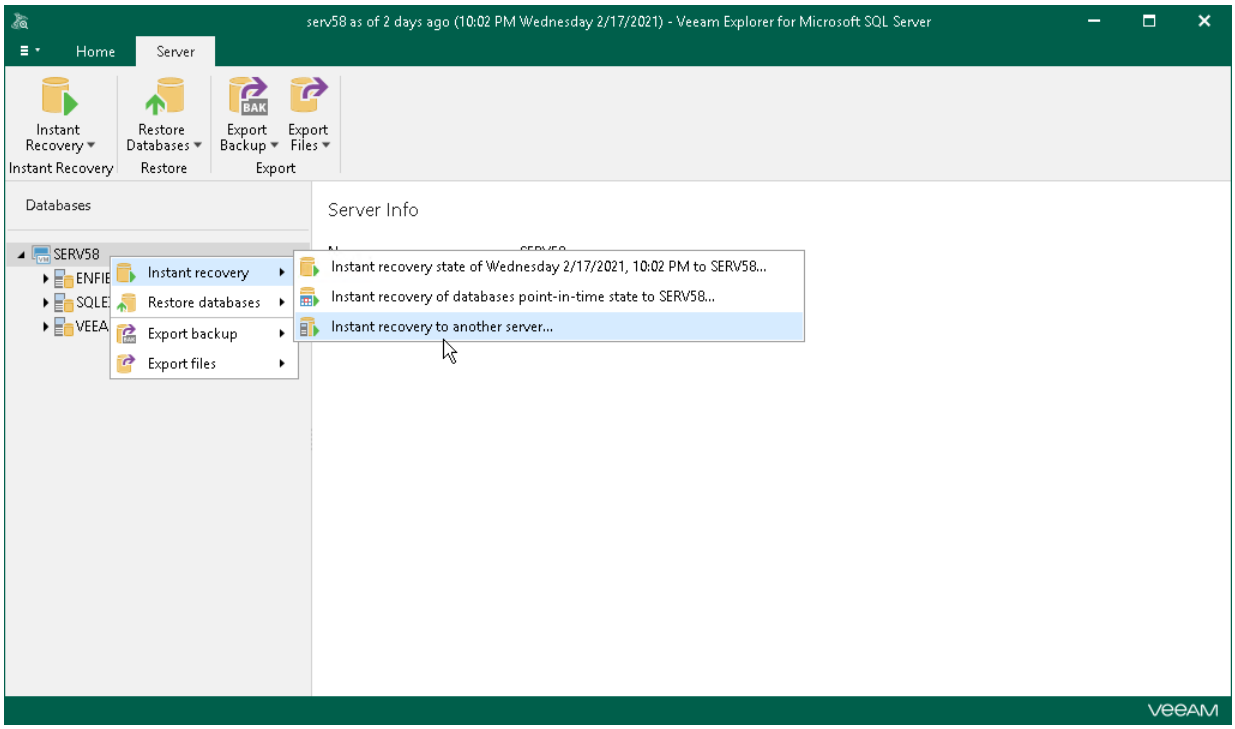
To perform instant recovery of multiple databases, do the following:

1. Launch the Instant Recovery wizard.
2. Specify restore point.
3. Specify target server.
4. Specify switchover settings.
5. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To perform instant recovery of multiple databases, do the following:

1. In the navigation tree of Veeam Explorer for Microsoft SQL Server, select a server or an SQL Server instance.
2. On the **Database** or the **Instance** tab, select one of the following options:
   - **Instant Recovery** > **Instant Recovery of databases latest state to** ***<original server/instance>*** or right-click the server or an instance and select **Instant recovery** > **Instant recovery of databases latest state to** ***<original server/instance>***.
   - **Instant Recovery** > **Instant Recovery of databases point-in-time state to** ***<original server/instance>*** or right-click a server or an instance and select **Instant recovery** > **Instant recovery of databases point-in-time state to** ***<original server/instance>***.
   - **Instant Recovery** > **Instant Recovery to another server** or right-click a server or an instance and select **Instant recovery** > **Instant recovery to another server**.



Step 2. Specify Restore Point

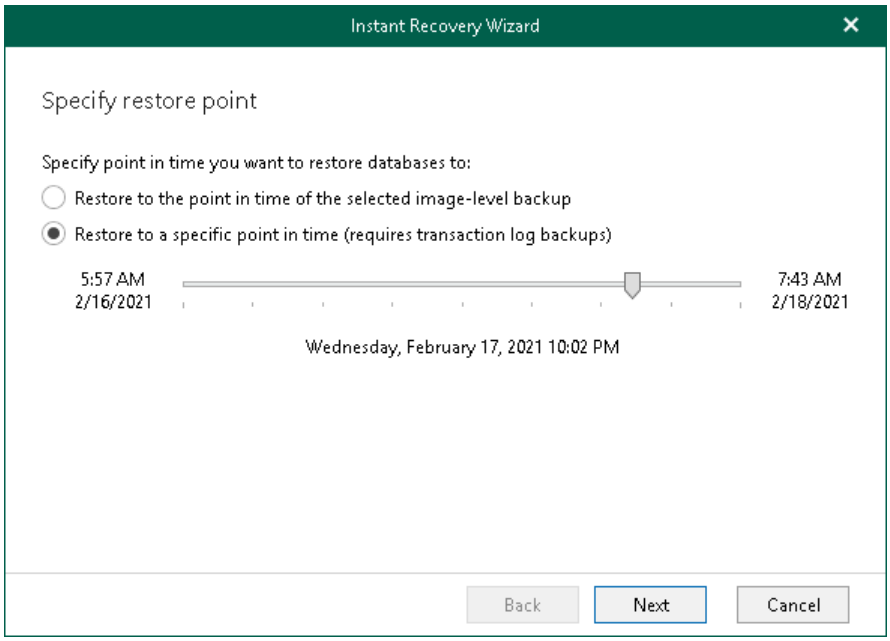
At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a required point in time.

  If some of the databases do not have transaction log backups for the specified time, they will be displayed below with their own time point.

> **NOTE**
>
> If you have selected to perform instant recovery of databases latest state to original server/instance, skip this step and go to Specify Switchover Settings.



Step 3. Specify Target Server

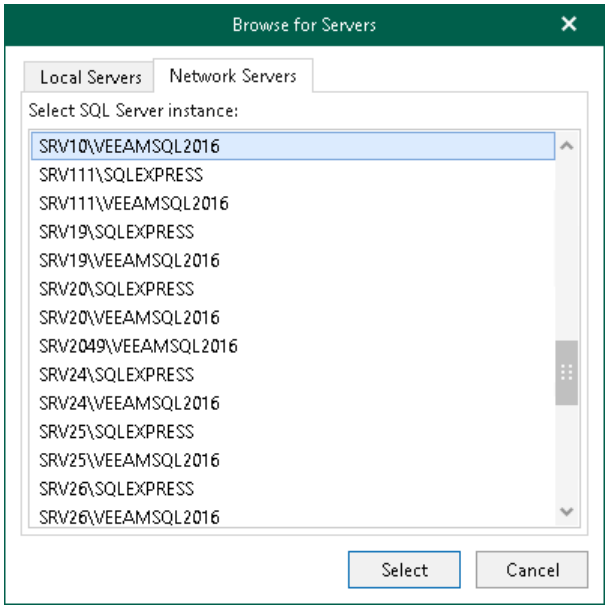
[For instant recovery to another server] At this step of the wizard, specify credentials to access the target server.

1. In the **Server name** field, specify the target instance to which you want to restore the database. Use the `server\instance` or `IP_address\instance` format. You can select an instance from the drop-down list or use the **Browse** button on the right.

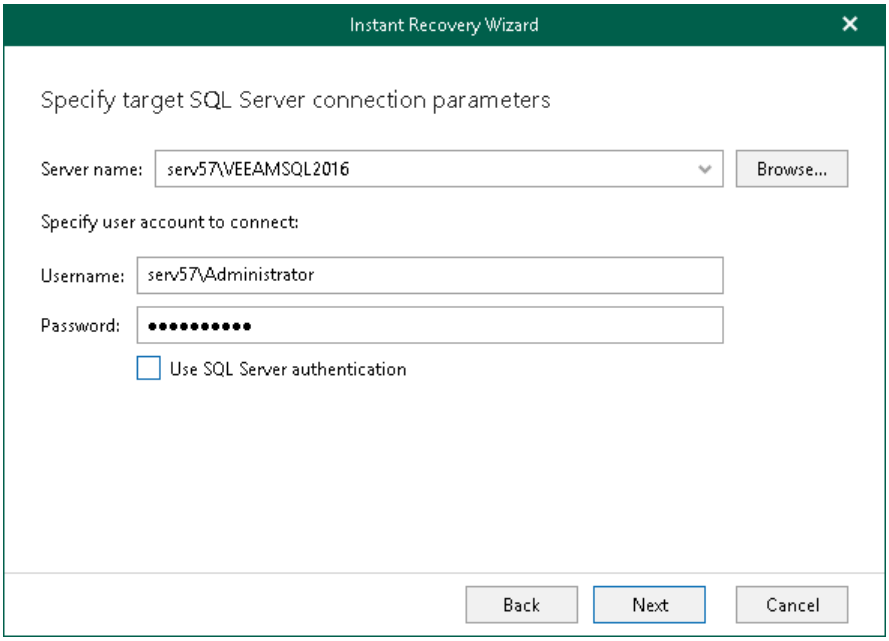
   To browse for another servers and SQL Server instances:

   a. Click the **Browse** button.

   b. You can select an SQL Server instance residing on the local machine on the **Local Servers** tab or click the **Network Servers** tab and select an instance on another server. Veeam Explorer displays servers from your network where SQL Server is installed.



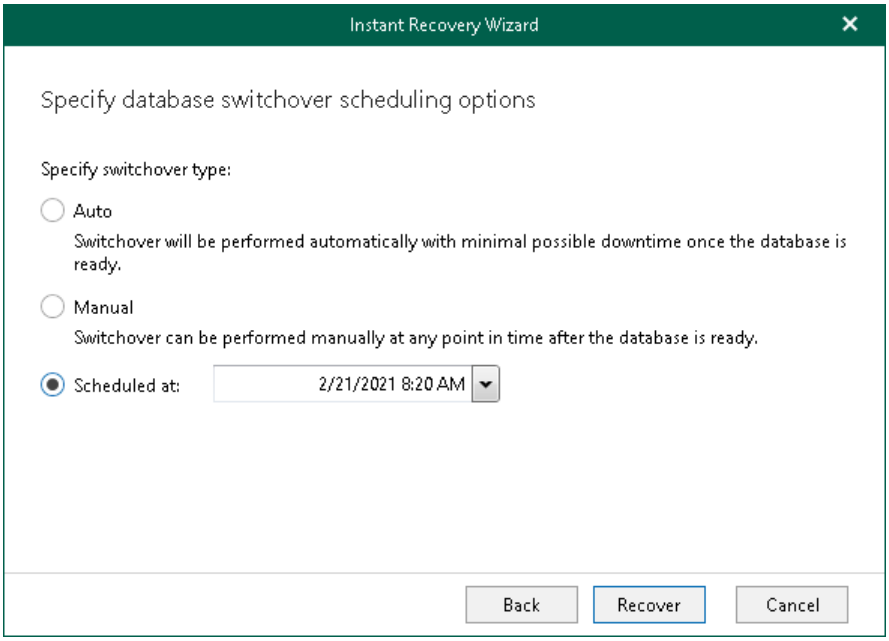
2. In the **Specify user account to connect** field, specify credentials which will be used to connect to the target SQL Server instance.
   - Select the **Use SQL Server authentication** check box to use SQL Server authentication. If not selected, Veeam Explorer will use Windows authentication.
   - Make sure the account has been granted the sysadmin role privileges on a target SQL server.
   - Make sure that the account has at least **Read** and **Write** permissions on the administrative share (i.e., `\\myserver\ADMIN$`) on the target server.



Step 4. Specify Switchover Settings

At this step of the wizard, you can specify a switchover option and define a schedule.

1. In the **Specify switchover type** field, select one of the following options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.



2. Click **Recover** to start instant recovery.

Step 5. Finalize Instant Recovery Session

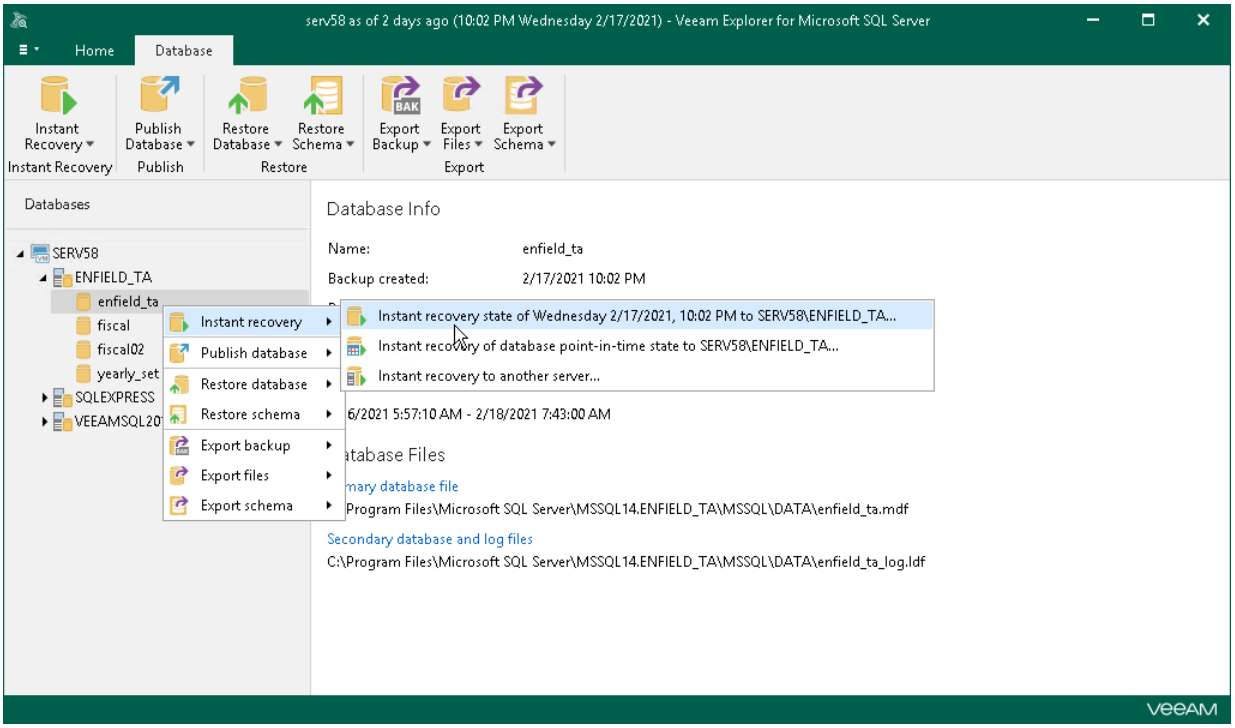
Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

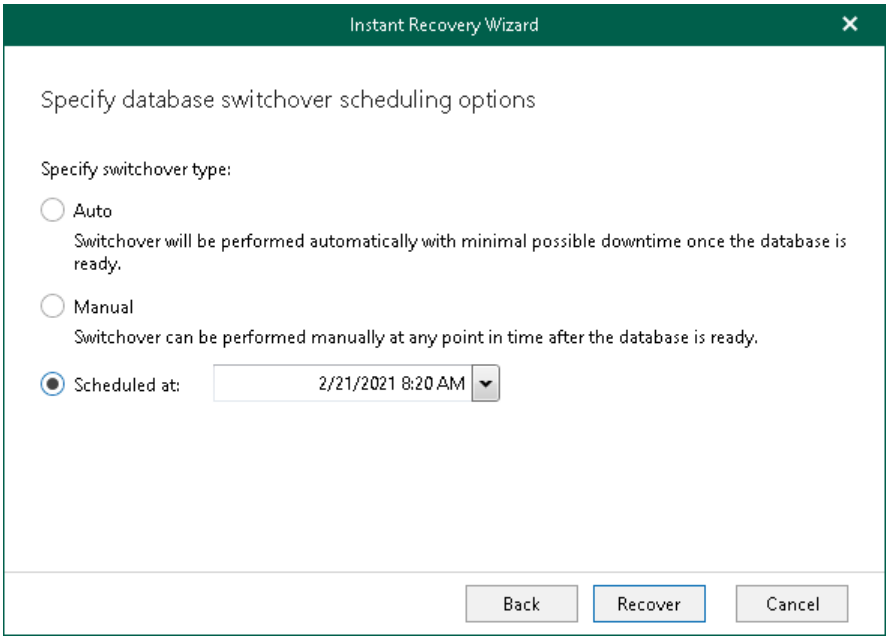
Instant Recovery of Latest State

To perform instant recovery of a single database to the latest state, do the following:

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of the latest state** or right-click a database and select **Instant recovery > Instant recovery of the latest state to** *<original instance>*.



3. In the **Instant Recovery** wizard, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.



4. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.

5. Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

   If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Instant Recovery of Point-in-Time State

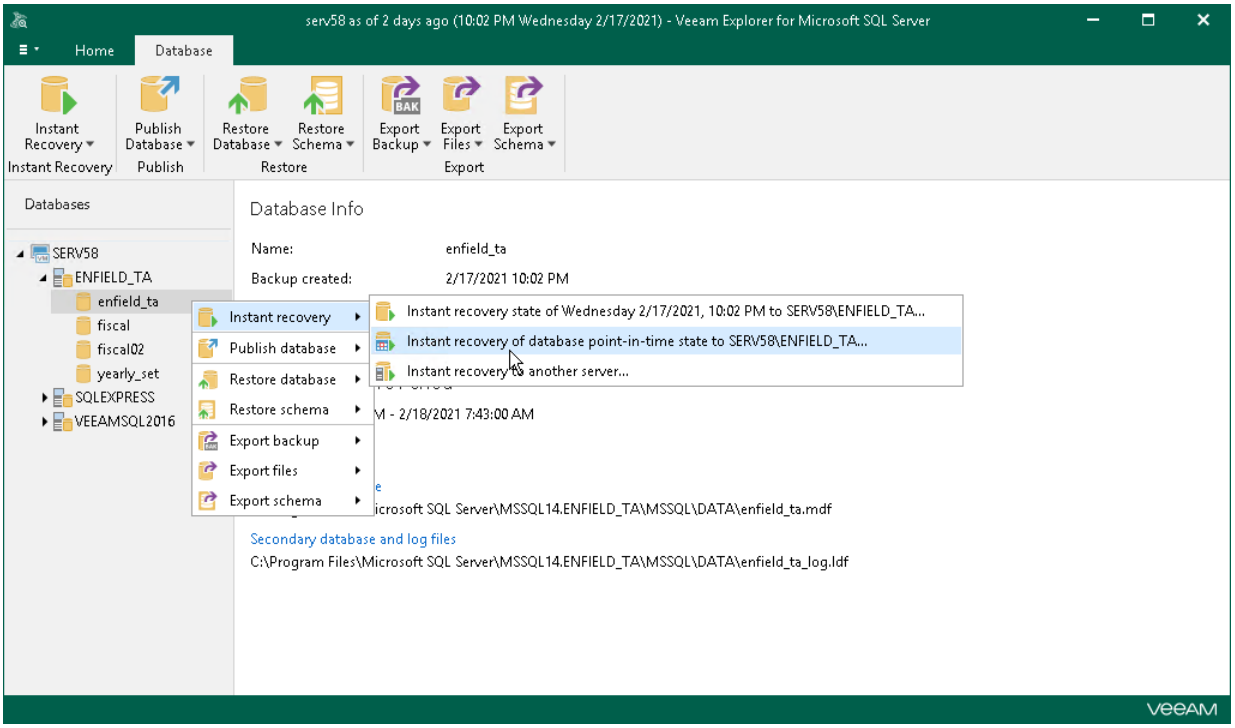
To perform instant recovery of a database to a selected point-in-time state, perform the following steps:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify a switchover option.
5. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery** wizard, do the following:

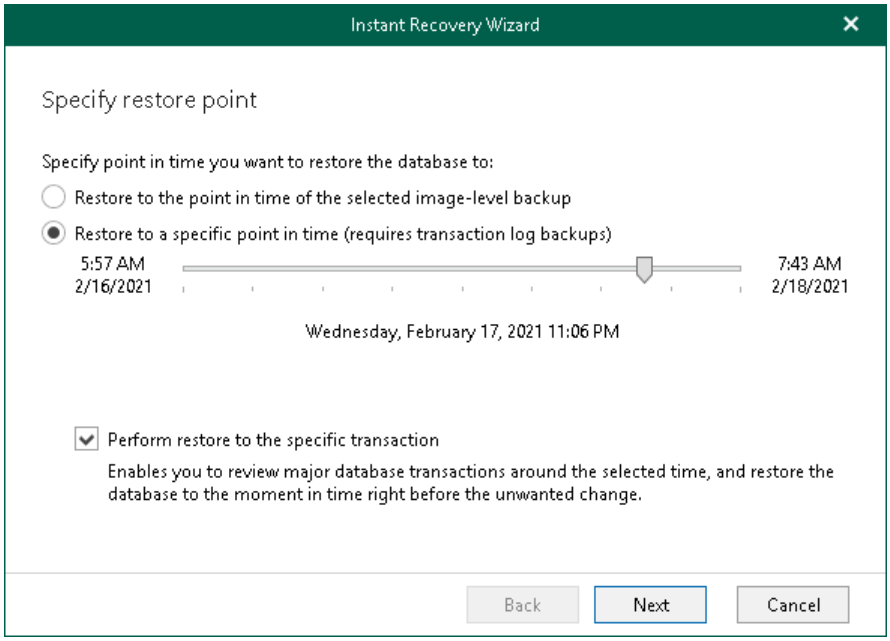
1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of database point-in-time state** or right-click a database and select **Instant recovery > Instant recovery of database point-in-time state to *<original_instance>***.



Step 2. Specify Restore Point

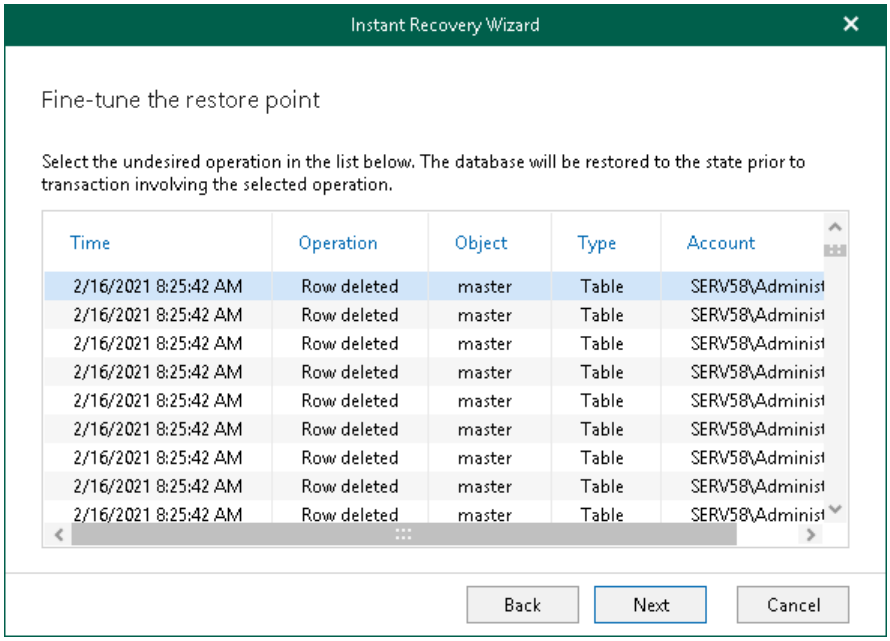
At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging server where Microsoft SQL Server is deployed. For more information, see Configuring Staging SQL Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database and click **Next**.



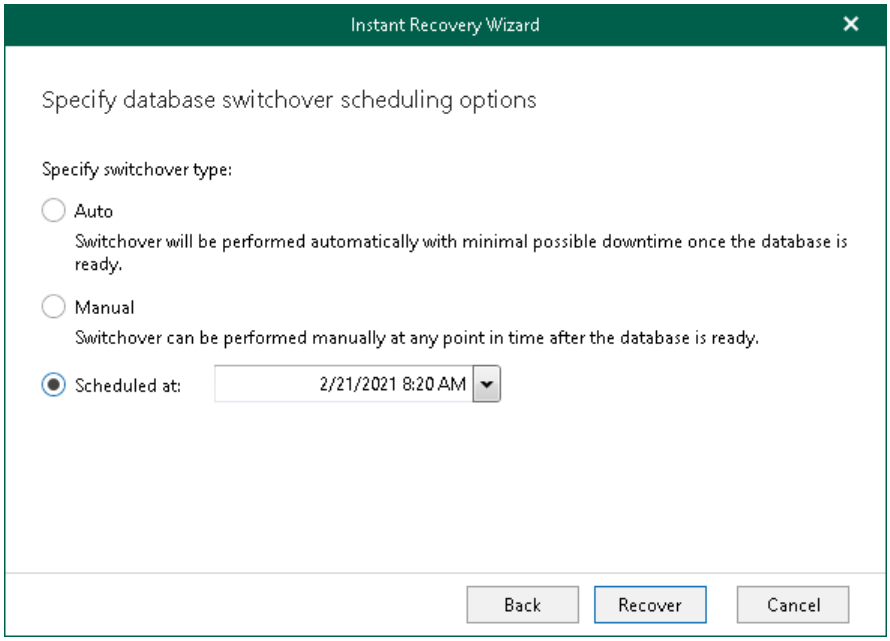
Step 4. Specify Switchover Option

At this step of the wizard, specify a database switchover option. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



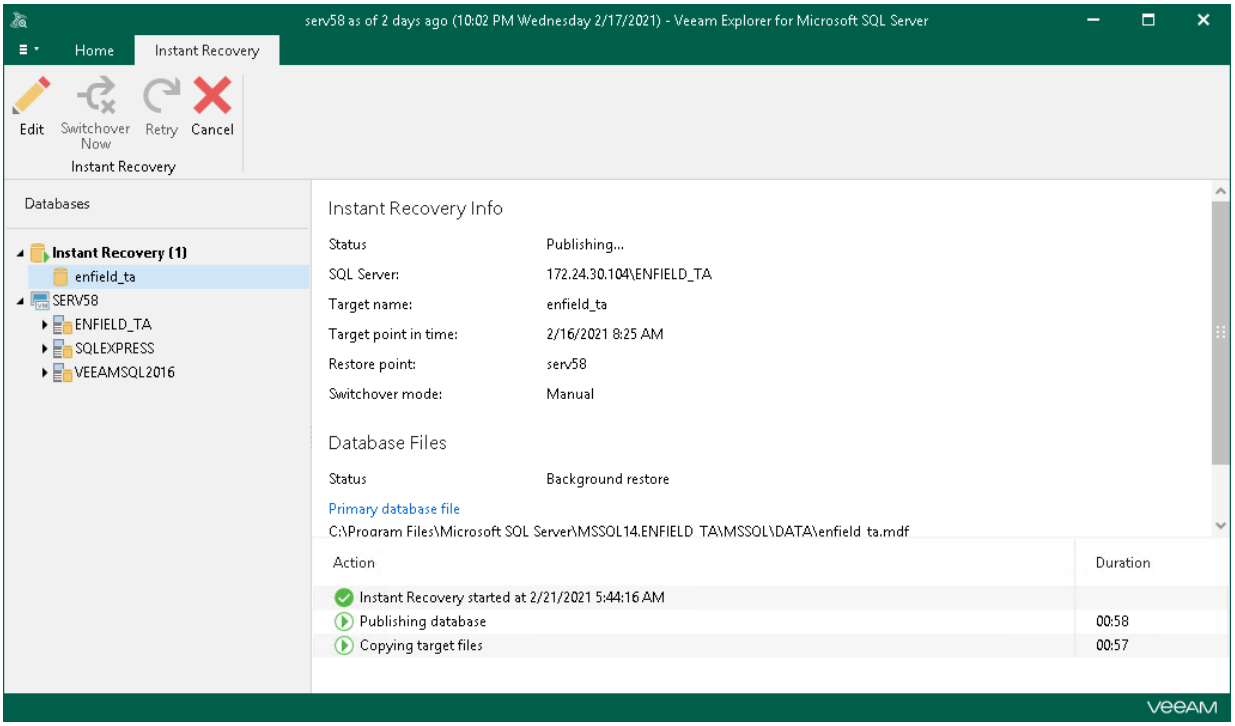
Step 5. Finalize Instant Recovery Session

After you finish steps of the Instant Recovery wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery and start manual switchover (if you selected the **Manual** switchover option).

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery to Another Server

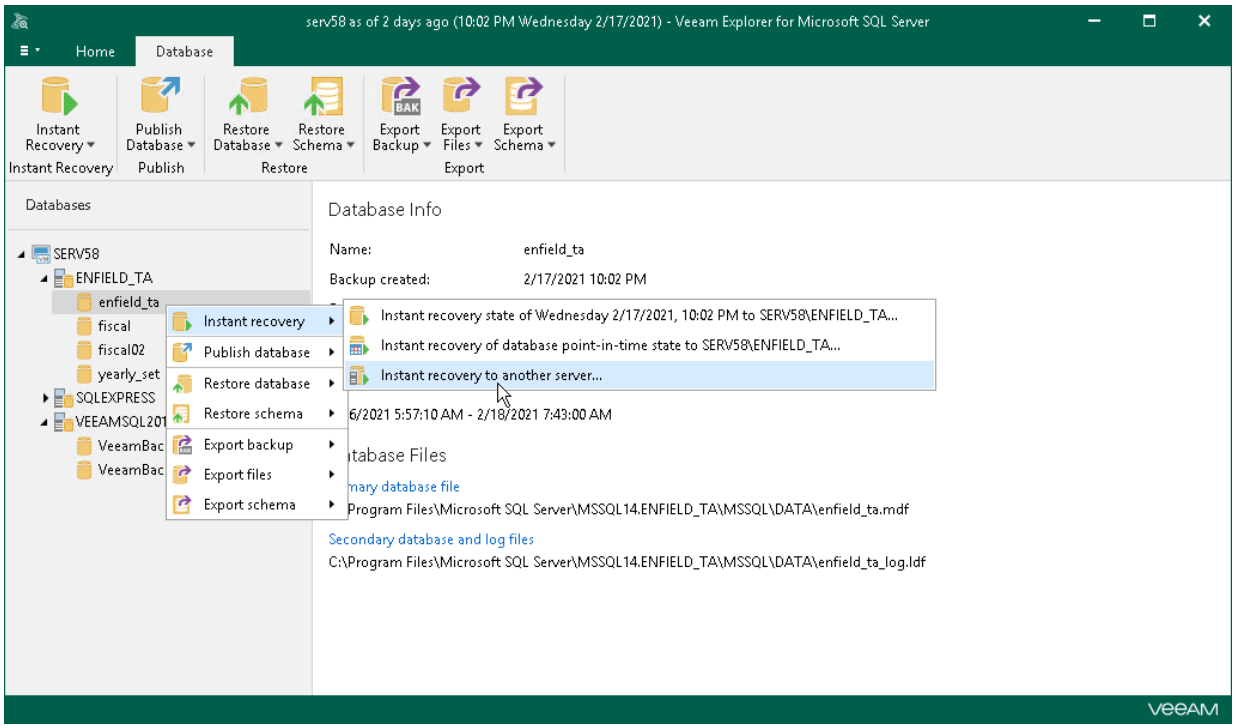
To perform instant recovery of a database to another server, perform the following steps:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify database files location.
6. Specify a switchover option.
7. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery** wizard, do the following:

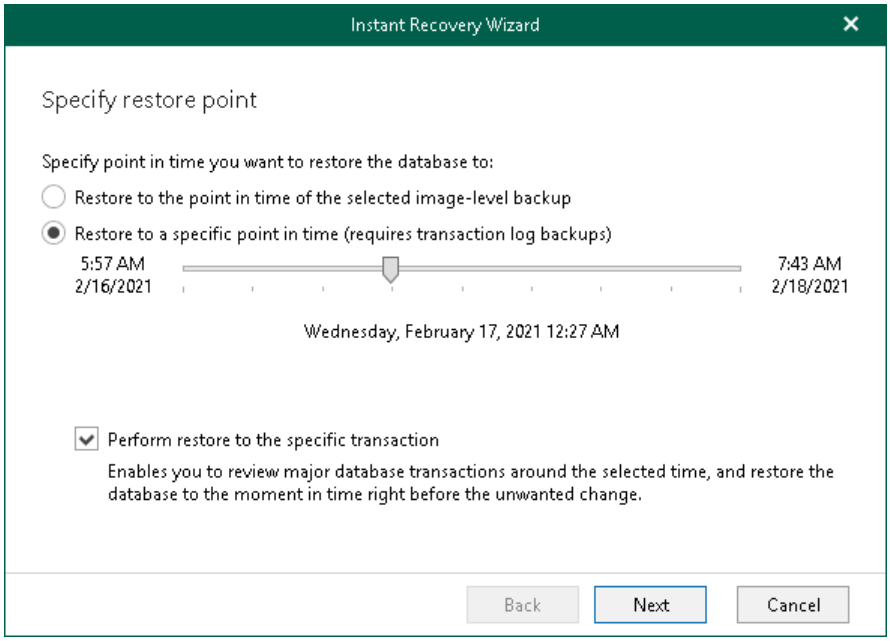
1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery to another server** or right-click a database and select **Instant recovery > Instant recovery to another server**.



Step 2. Specify Restore Point

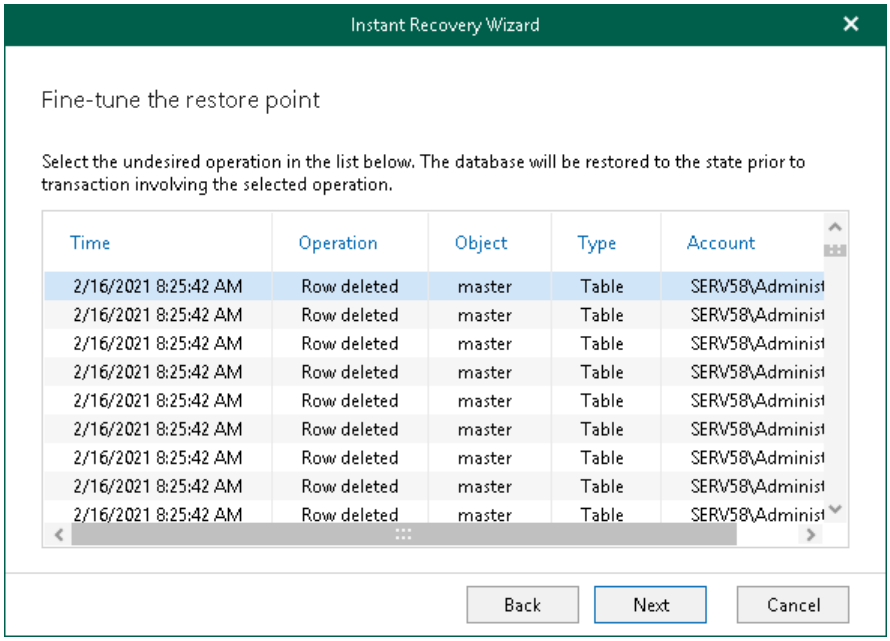
At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging server where Microsoft SQL Server is deployed. For more information, see Configuring Staging SQL Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.



Step 4. Specify Target Server

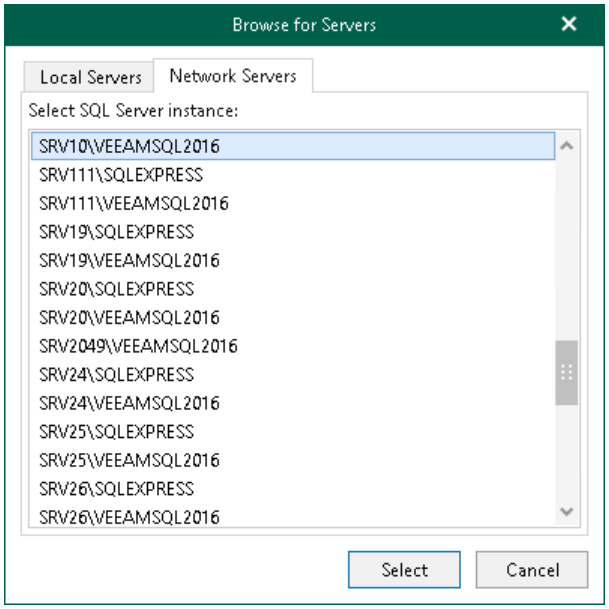
At this step of the wizard, specify credentials to access the target server.

1. In the **Server name** field, specify the target instance to which you want to restore the database. Use the `server\instance` or `IP_address\instance` format. You can select an instance from the drop-down list or use the **Browse** button on the right.

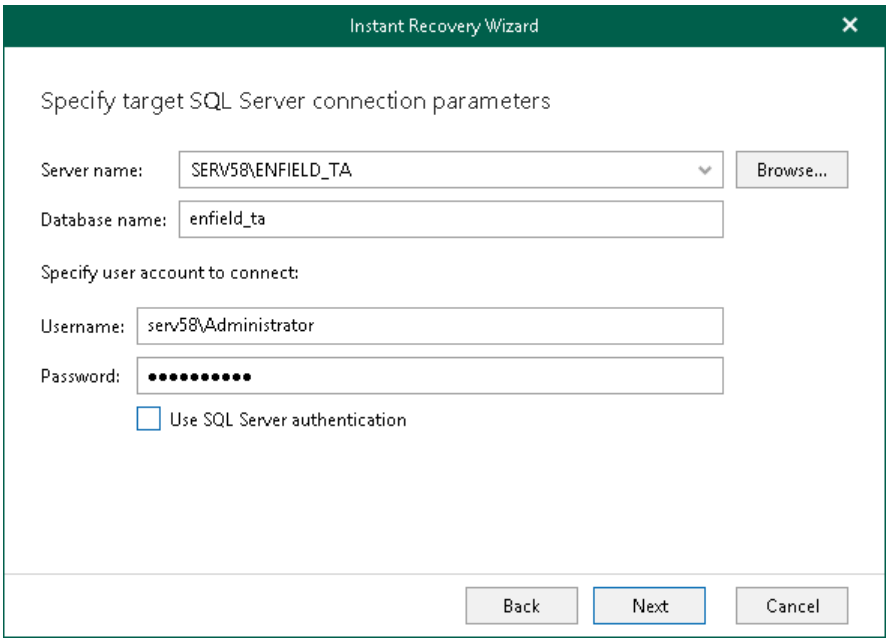
   To browse for other servers and SQL Server instances:

   a. Click the **Browse** button.

   b. You can select an SQL Server instance residing on the local machine on the **Local Servers** tab or click the **Network Servers** tab and select an instance on another server. Veeam Explorer display servers from your network where SQL Server is installed.



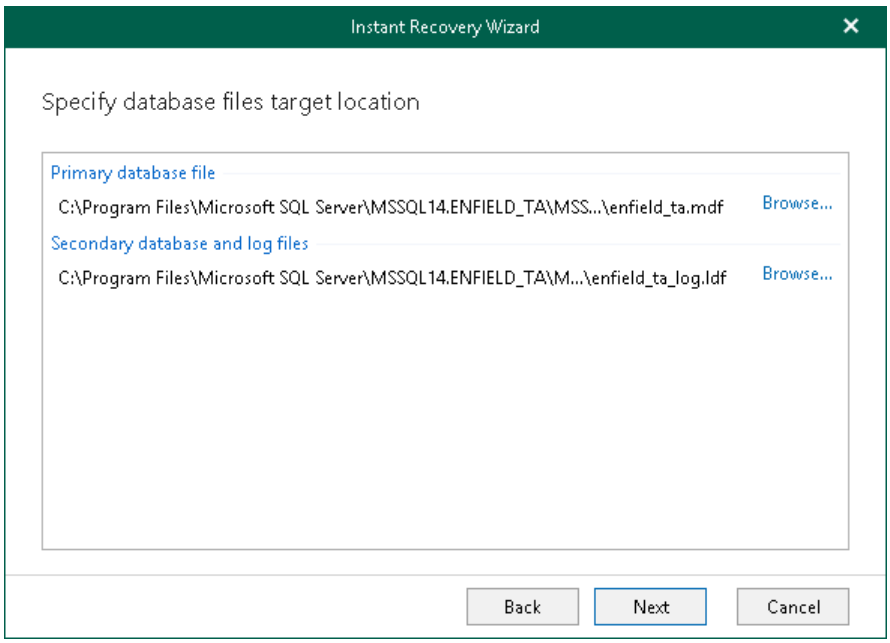
2. In the **Database name** field, specify a name for the restored database.
3. In the **Specify user account to connect** field, specify credentials which will be used to connect to the target SQL Server instance.
   - Select the **Use SQL Server authentication** check box to use SQL Server authentication. If not selected, Veeam Explorer will use Windows authentication.
   - Make sure the account has been granted the sysadmin role privileges on a target SQL server.
   - Make sure that the account has at least **Read** and **Write** permissions on the administrative share (i.e., `\\myserver\ADMIN$`) on the target server.



Step 5. Specify Database File Location

At this step of the wizard, specify the location for database files (control files, data files, log files and temp files).

To edit the path, click the path row and specify the location you want to use. If specified folders don't exist, Veeam Explorer will create these folders.



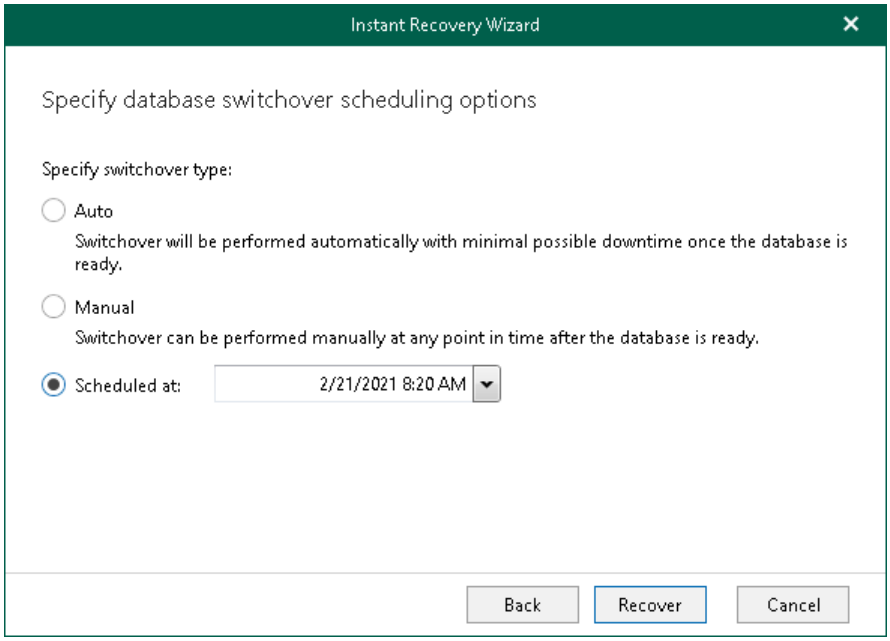
Step 6. Specify Switchover Option

At the last step of the wizard, specify database switchover options.

To select a switchover option and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 7. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Switchover

The switchover option becomes available after all the database files are copied to the target server and all database files are synchronized. During switchover, the published mount is detached from the target SQL Server instance and the copied database is attached to this instance. Note that if you have selected to restore to the original server, the restored database will replace the original database.

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

During the switchover, Veeam Explorer performs the following:

1. Detaches the published database from the SQL Server instance.
2. Uses the cache to synchronize changes between the published database and the copied database files.
3. Drops the published database.
4. Attaches the recovered database to the SQL Server instance.

Note that the database will be offline between the steps 1–4.

Auto Switchover

The Auto switchover option ensures minimal period of downtime.

As soon as database files are copied from the mount server, Veeam Explorer checks the size of the cache that contains changes that has been made to the database since the publishing. Depending on the cache size, the following happens:

- If the cache size is smaller than 100 MB, Veeam Explorer starts the switchover.
- If the cache size is larger than 100 MB, Veeam Explorer uses the cache to synchronize changes and checks the cache size once again. If the cache size is smaller than 100 MB, Veeam Explorer starts the switchover. If the cache size is larger than 100 MB again, another cycle of synchronization is performed. Synchronization is relaunched until the cache size is smaller than 100 MB.

Manual Switchover

After database files are copied from the mount server, Veeam Explorer checks the size of the cache that contains changes that has been made to the database since the publishing. The cache size is performed every minute. If the cache size is larger than 100 MB or it has been 5 minutes since the last synchronization, Veeam Explorer starts to synchronize the changes between the published database and the copied database files.

After the synchronization is finished, you can launch the switchover manually. For details, see Starting Switchover Manually.

If you launch the switchover during the synchronization process, the switchover starts only after the synchronization if finished.

Scheduled Switchover

After database files are copied from the mount server, Veeam Explorer checks the size of the cache that contains changes that has been made to the database since the publishing. The cache size is performed every minute. If the cache size is larger than 100 MB or it has been 5 minutes since the last synchronization, Veeam Explorer starts to synchronize the changes between the published database and the copied database files.

After the synchronization is finished, Veeam Explorer waits for the scheduled date and time to start the switchover.

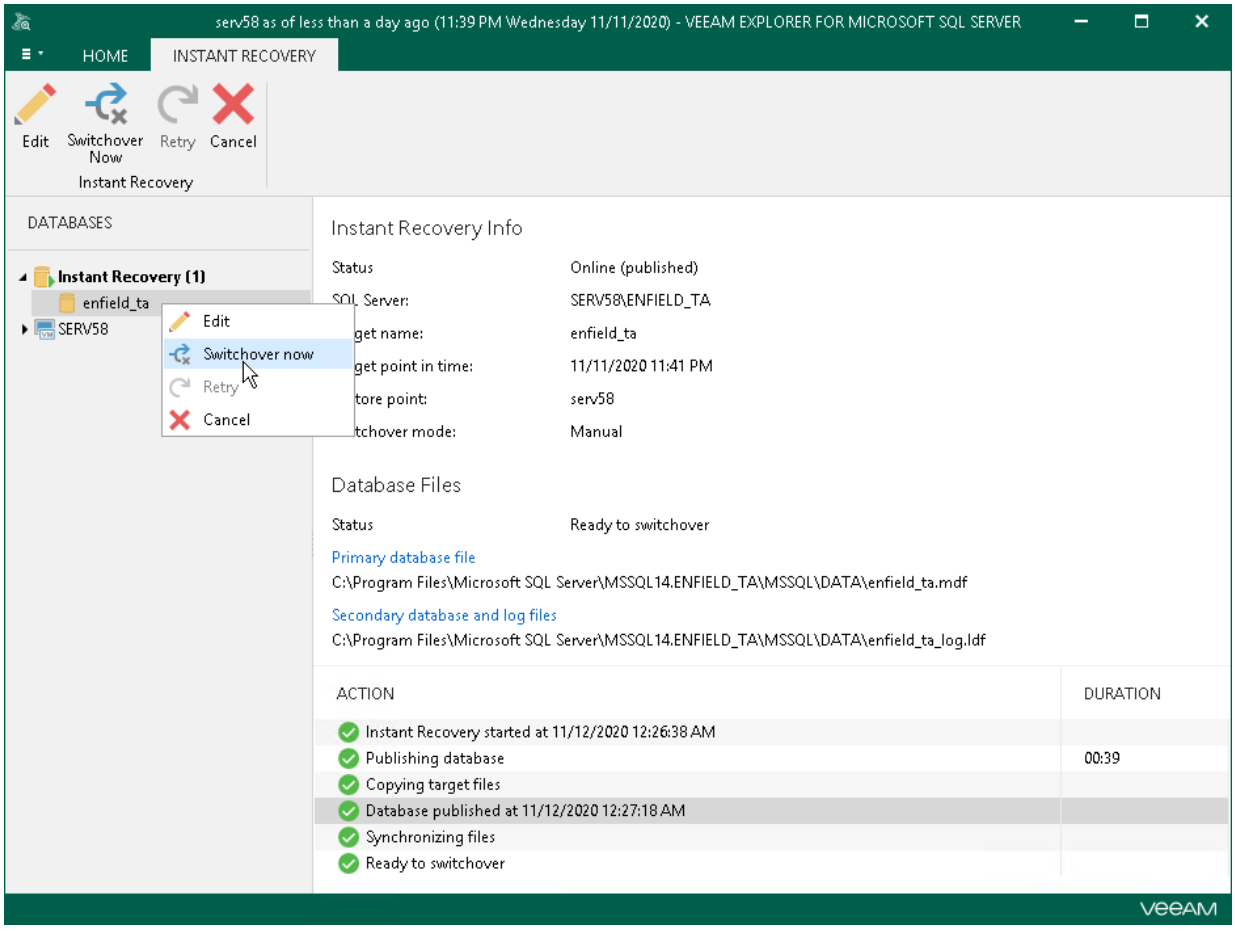
If the switchover scheduled period starts during the synchronization process, the switchover starts only after the synchronization if finished

Starting Switchover Manually

If you have selected the *Manual* switchover option in the **Instant Recovery** wizard, you can start the switchover at any time if the database is in the *Ready to switchover* state.

To start the switchover manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Switchover Now** or right-click the database and select **Switchover now**.



Managing Instant Recovery Session

After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session which shows the progress of the recovery process.

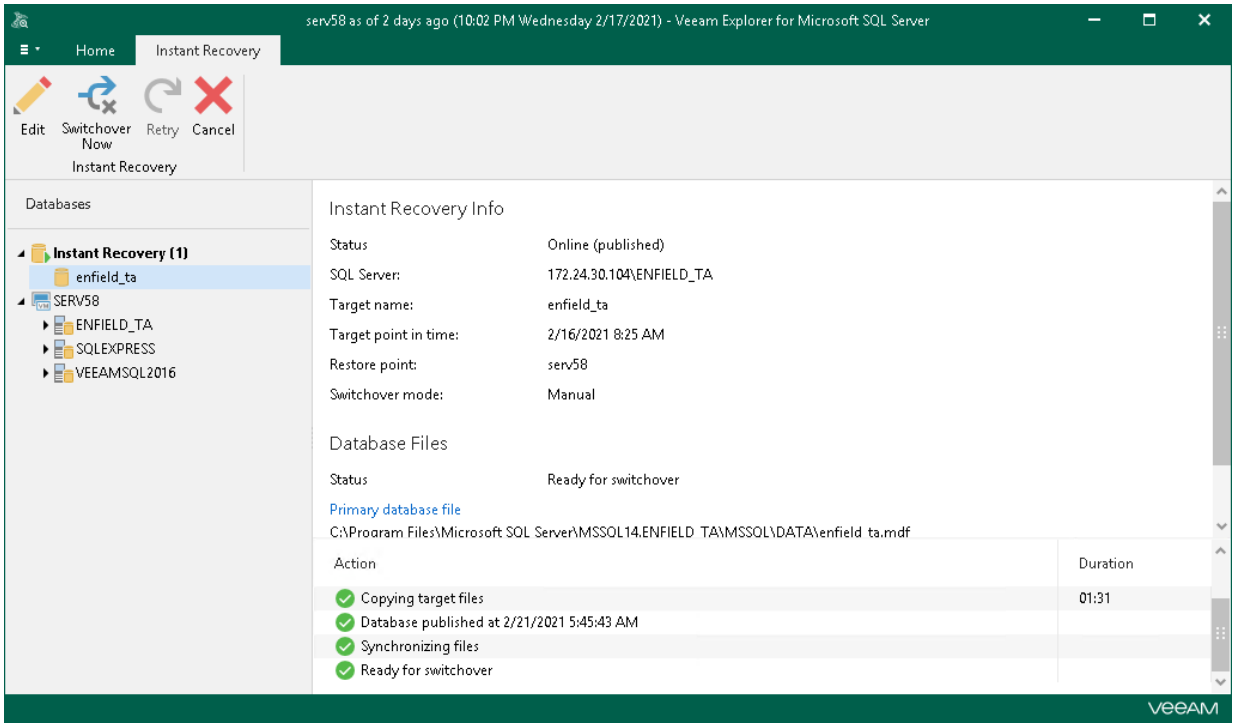
Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Also, in the **Instant Recovery** session view, you can do the following:

- Edit switchover settings.
- Retry instant recovery (in case instant recovery session fails for any reason).
- Cancel instant recovery.

> **NOTE**
>
> An instant recovery session closes automatically after the switchover.

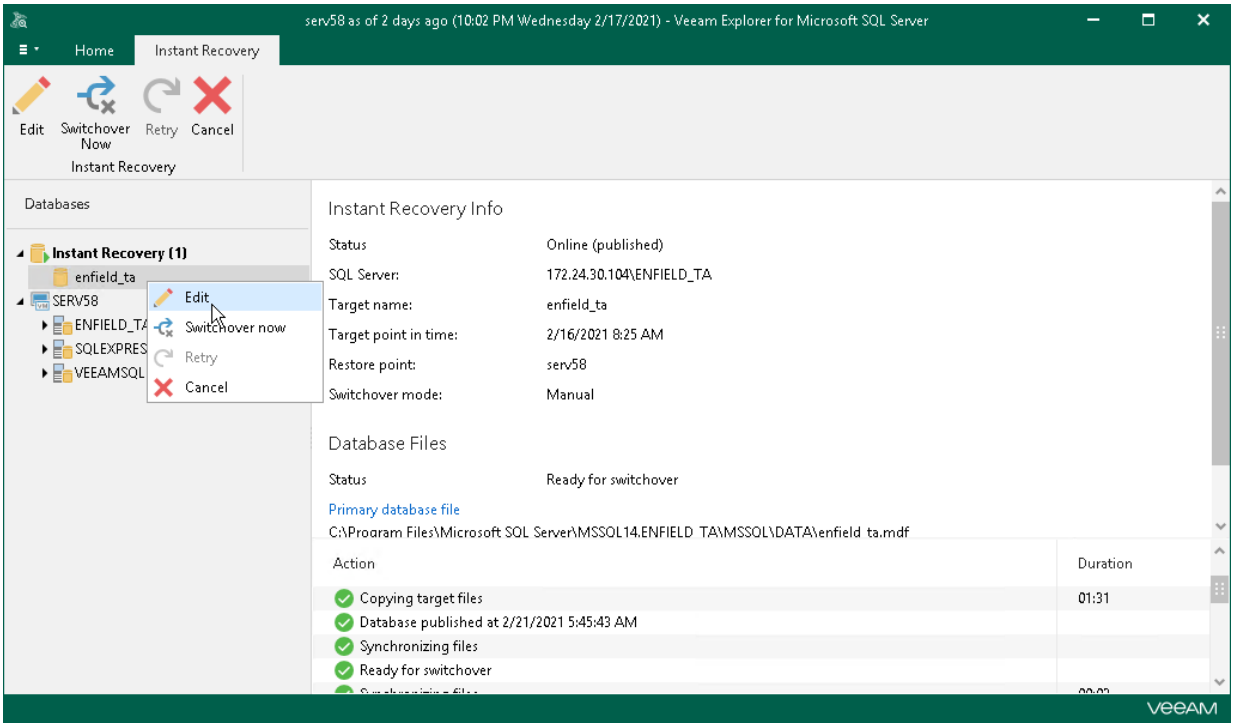


Editing Instant Recovery Settings

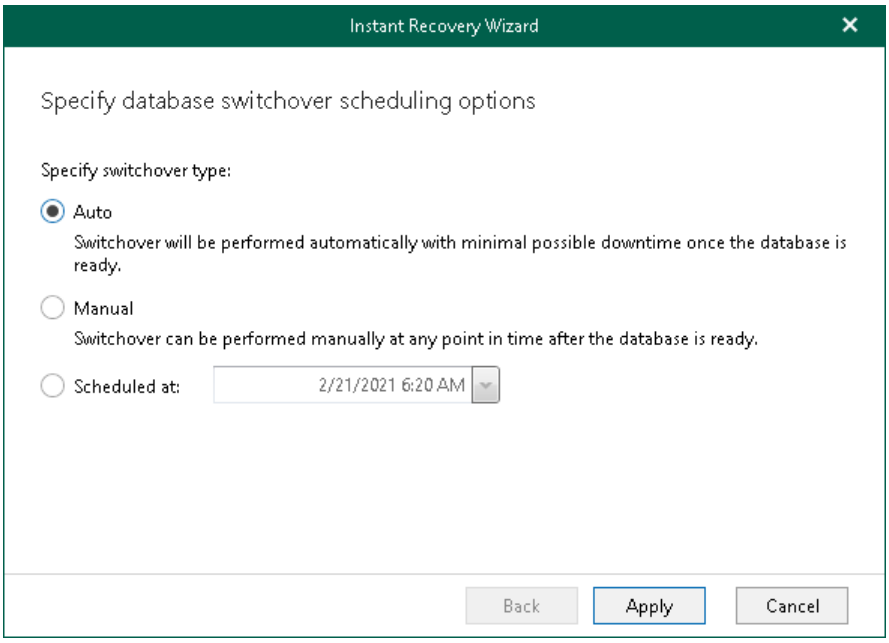
If you have started an instant recovery session and want to change the switchover settings, you can edit the instant recovery settings.

To change switchover settings of an instant recovery session, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Edit** or right-click the database or instance and select **Edit**.



3. Change the switchover option and click **Apply**.

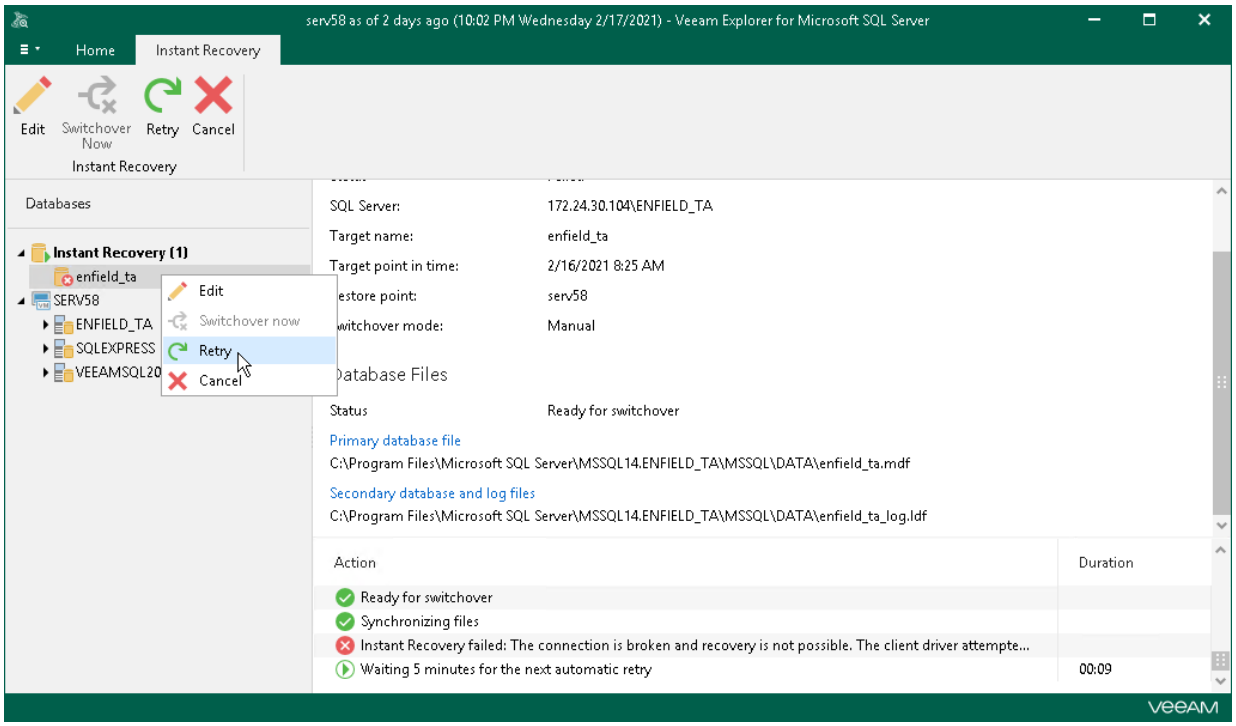


Recovery Retry

If anything disrupts the restore process (the target or mount server crashes or the network is down), the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch the retry manually after the server or network is up.

To start the retry process manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select the database.
2. On the **Instant Recovery** tab, click **Retry**.

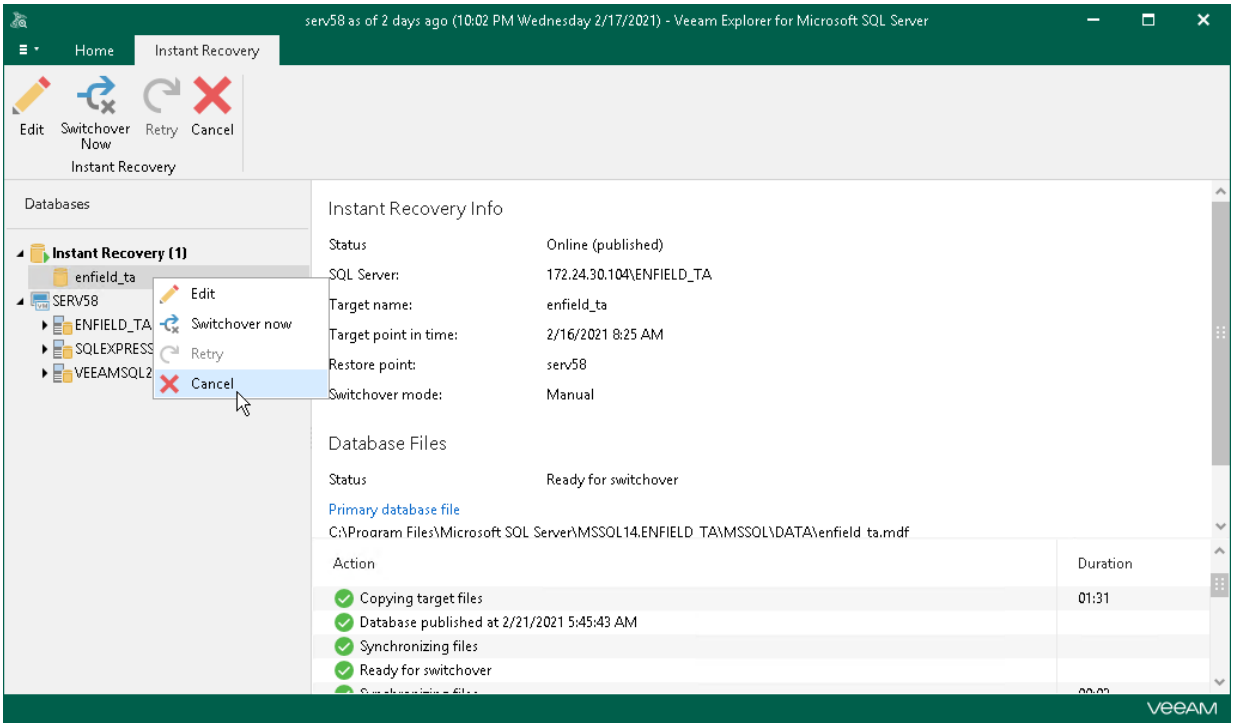


Cancelling Instant Recovery

If you have done working with published databases and don't want to switchover, you can cancel the instant recovery process.

To cancel the instant recovery process, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Cancel** or right-click the database and select **Cancel**.



NOTE

You do not need to cancel the instant recovery session if switchover is already performed. The session closes automatically after the switchover.

Data Export

Continue with this section to learn more about exporting Microsoft SQL Server databases.

Export as MDF

Continue with this section to learn more about exporting databases files as MDF.

Exporting Single Database

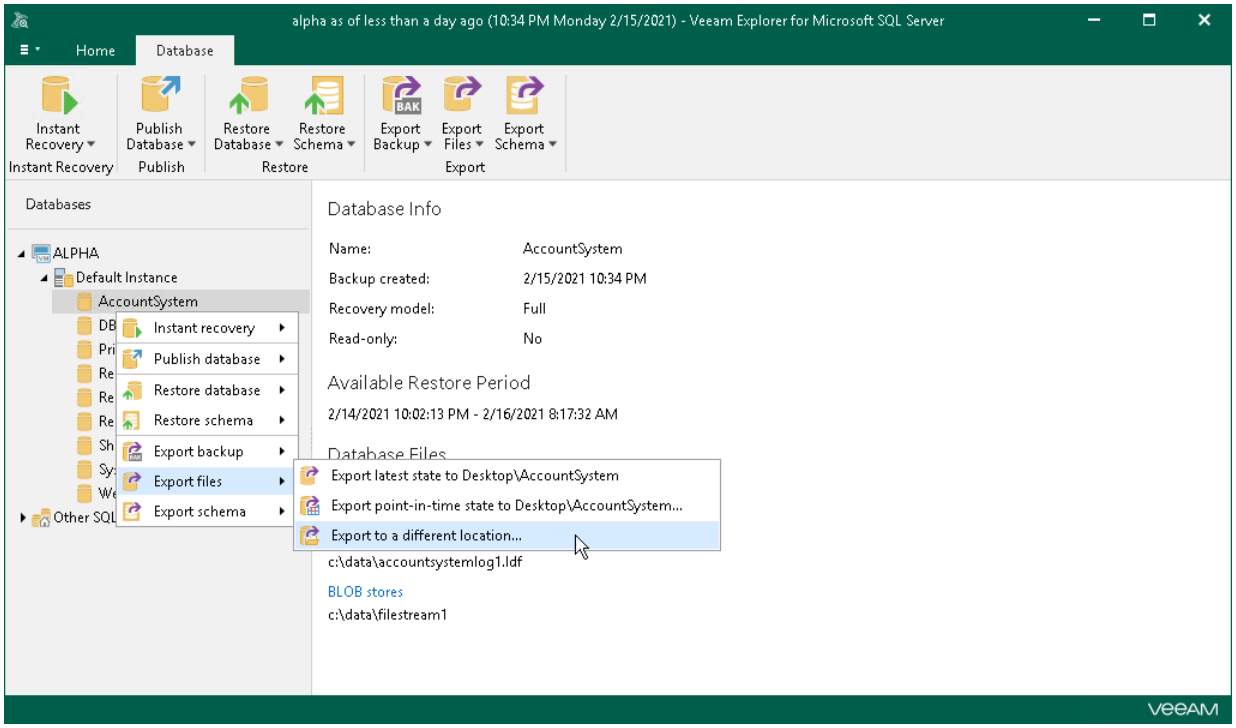
To export a single SQL database, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify files location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** (or **Server/Instance**) tab, select **Export Files** > **Export to a different location** or right-click a database and select **Export files** > **Export to a different location**.



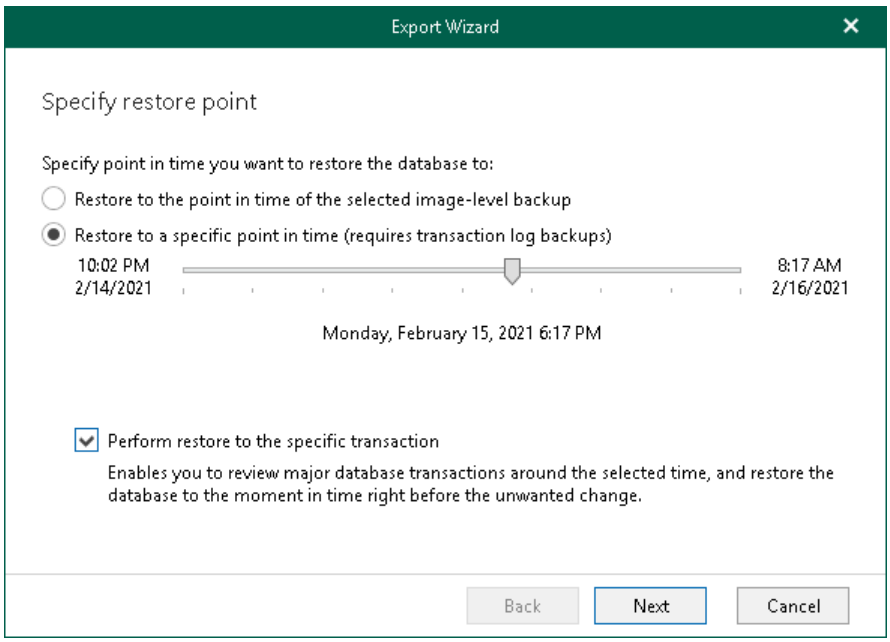
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

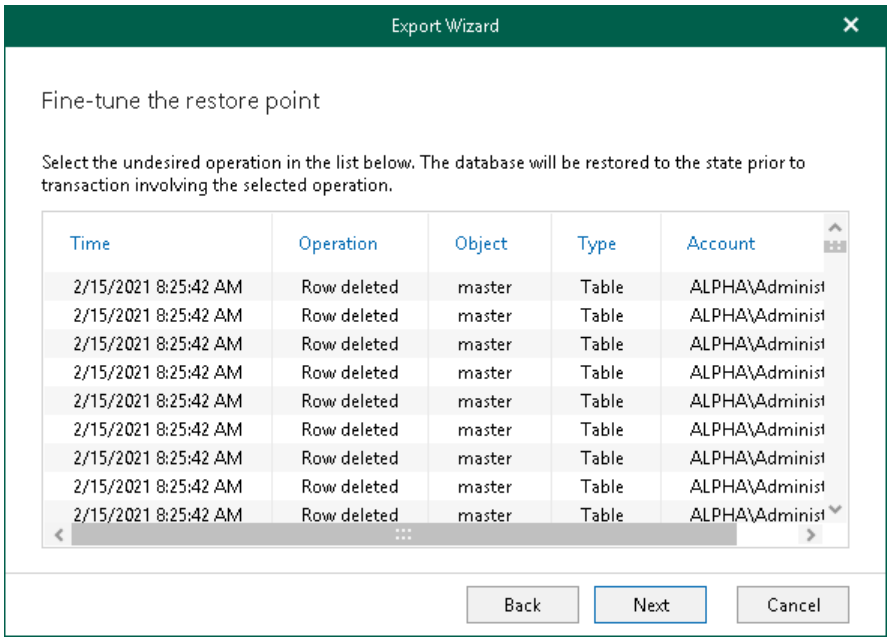


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.

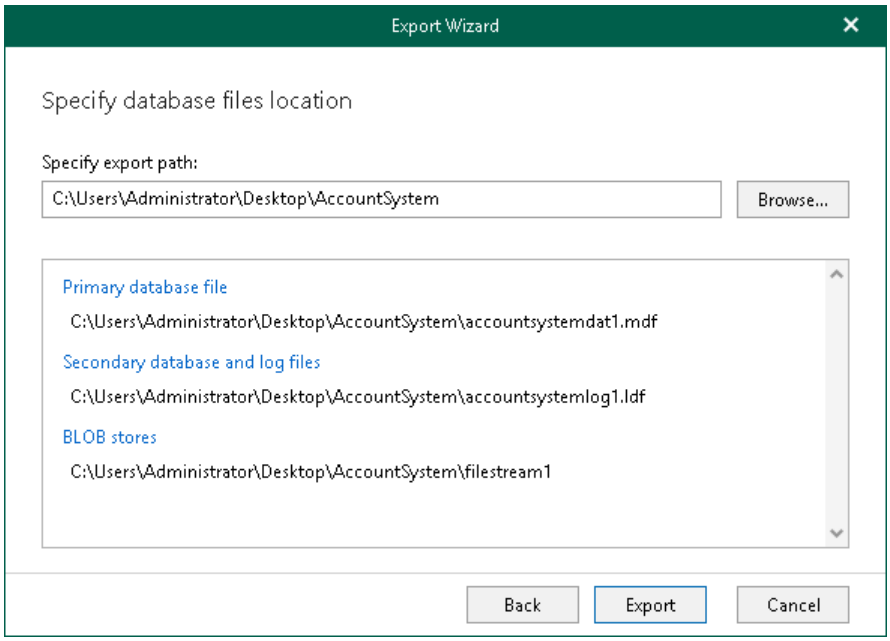


Step 4. Specify Files Location

At this step of the wizard, specify a path to the directory where you want to export database files.

Click **Browse** to specify the path manually.

> **NOTE**
>
> The account you are using must have a sufficient permission level to access the selected directory (Read and Write as minimum recommended).



Exporting Multiple Databases

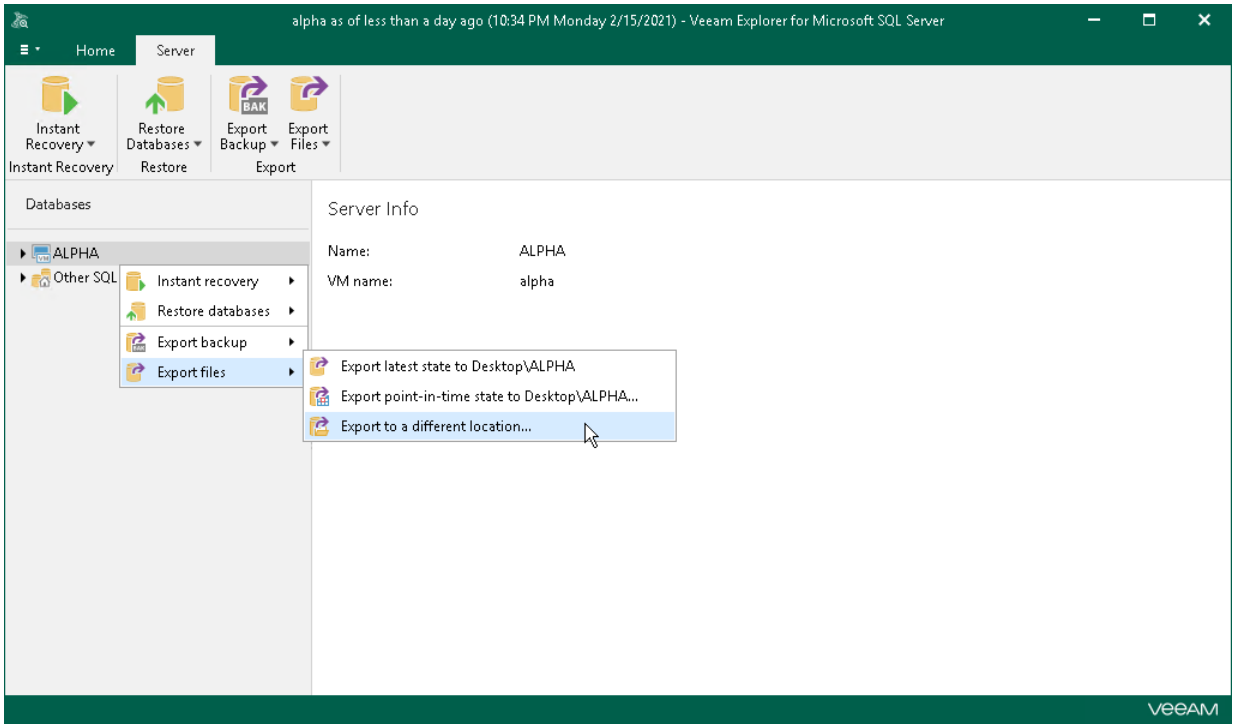
To export all SQL databases to a custom location, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Specify database files location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a server or instance.
2. On the **Server/Instance** tab, select **Export Files** > **Export to a different location** or right-click a database and select **Export files** > **Export to a different location**.



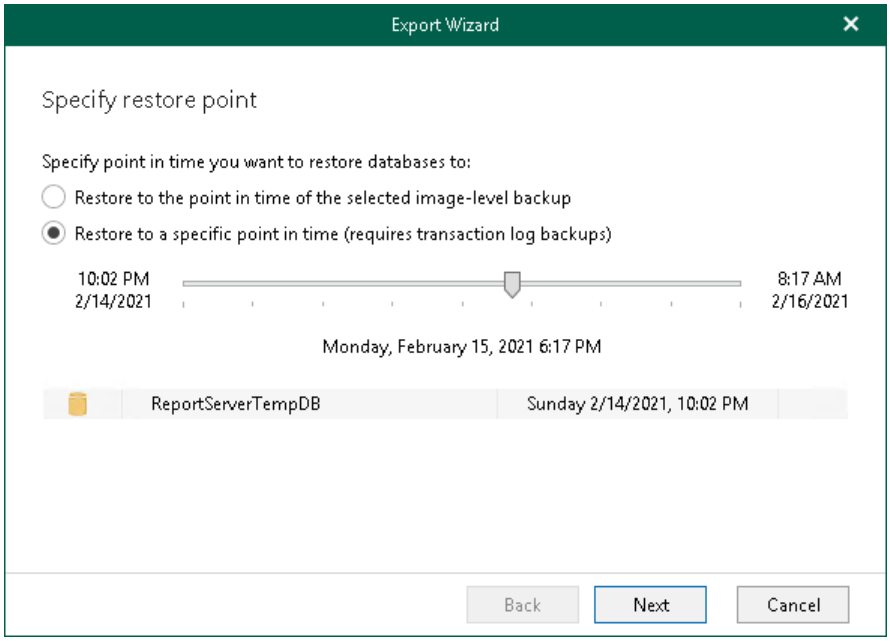
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

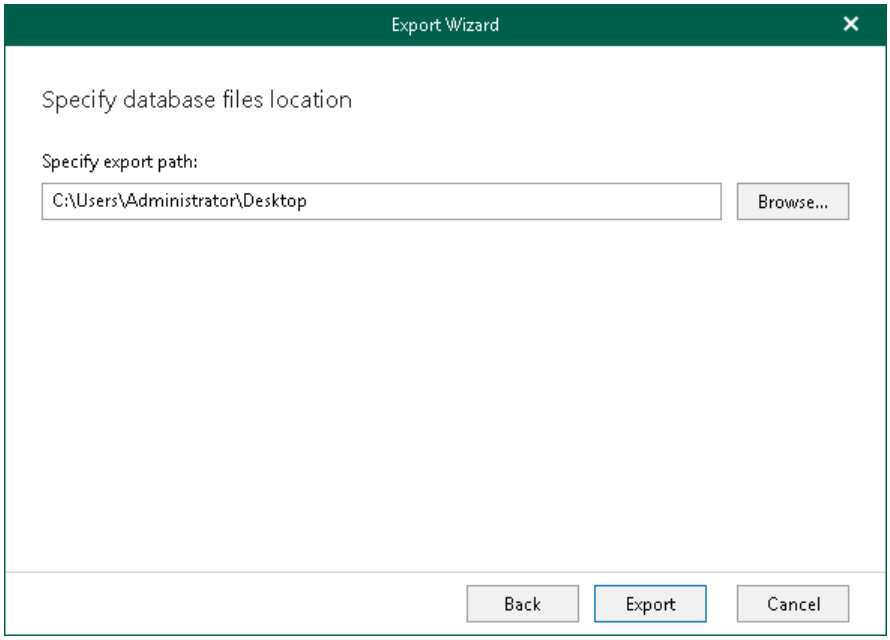
  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.



Step 3. Specify Database Files Location

At this step of the wizard, specify a path to the directory where you want to export database files.



Exporting Latest or Point-in-Time State

Continue with this section to learn more about exporting your data as of a latest or point-in-time state.

Exporting Point-in-Time State

To export data as of a point-in-time state, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

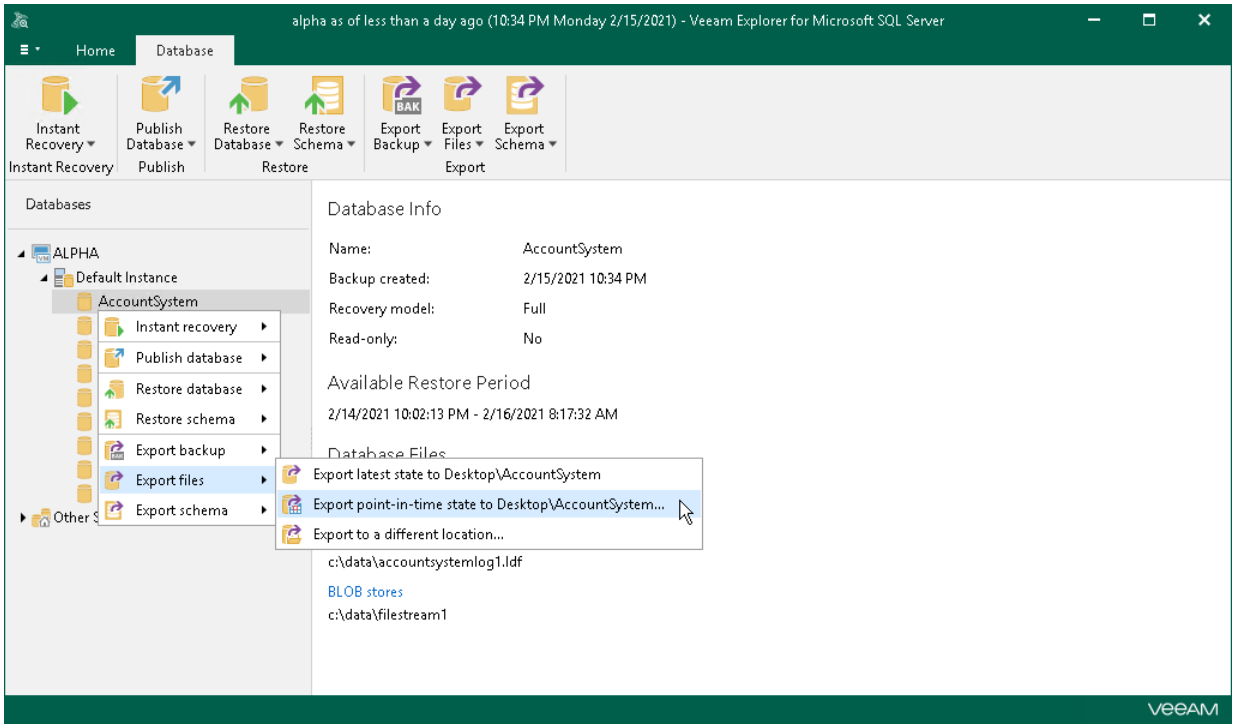
Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database, server or instance.

   You can select the root instance node to export all the available databases at once.

2. On the **Database** (or **Server/Instance**) tab, select **Export Files** > **Export point-in-time state to Desktop\<db_name>** or right-click a database and select **Export files** > **Export point-in-time state to Desktop\<db_name>**.



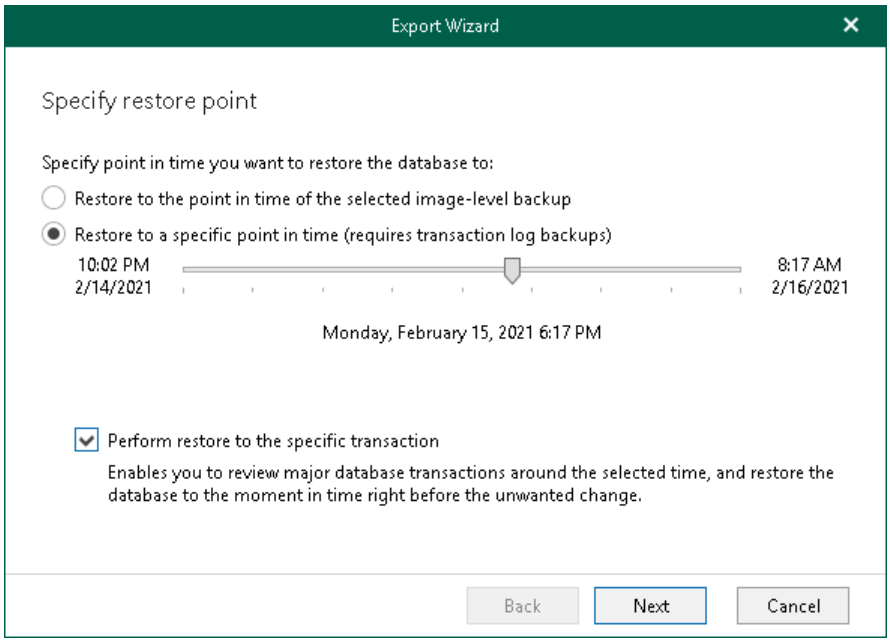
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

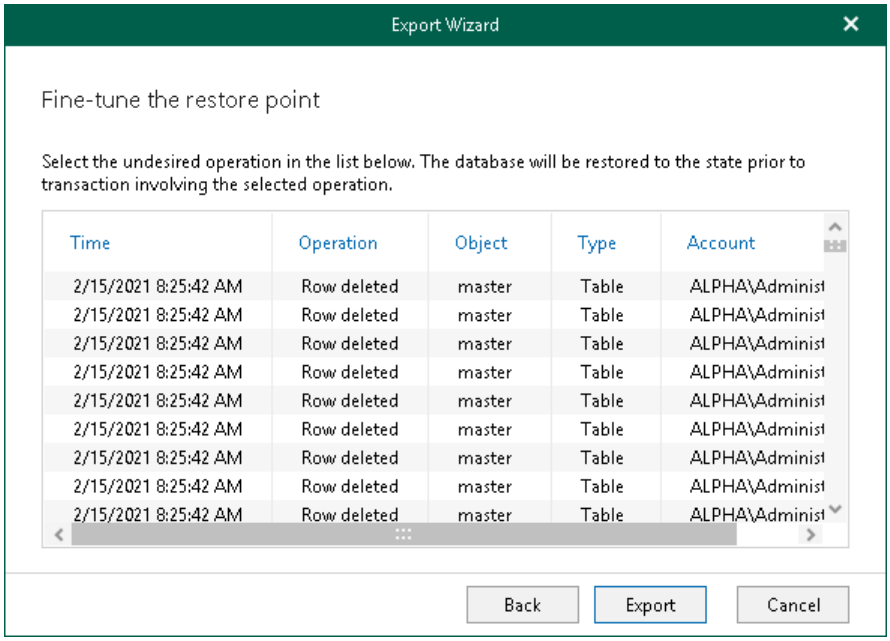


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



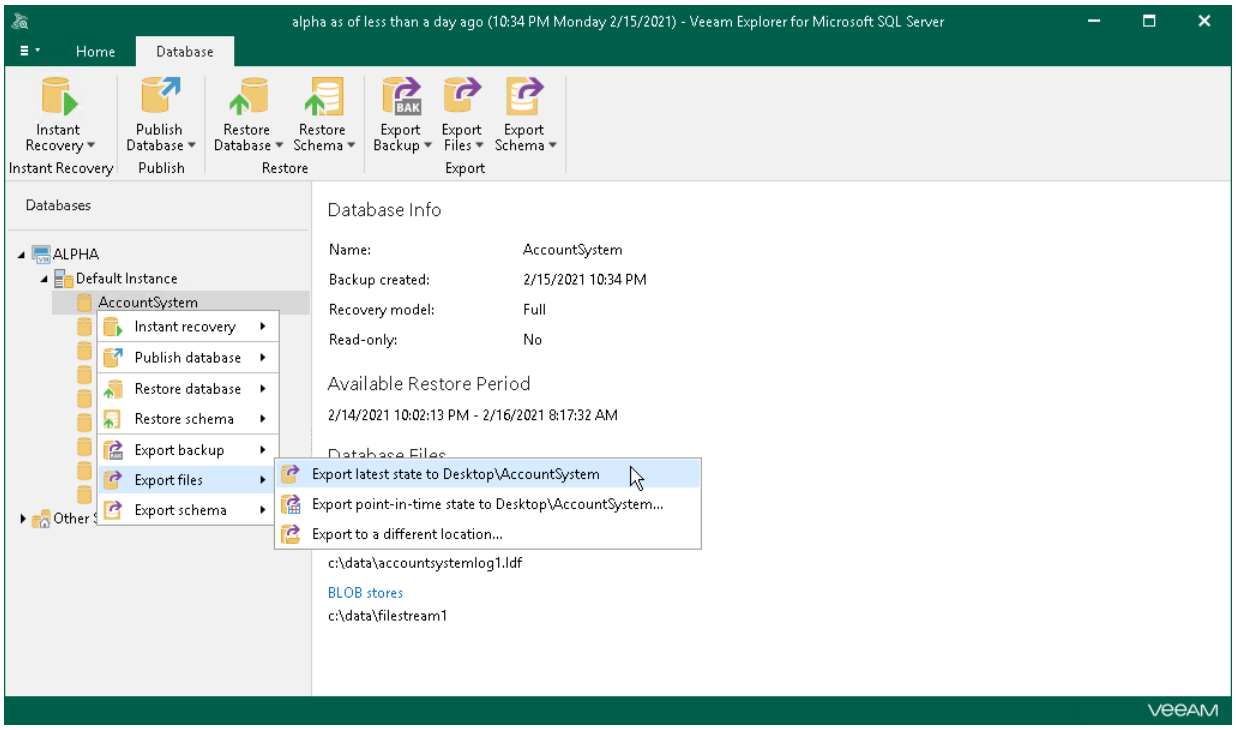
Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database or instance.

   You can select the root instance node to export all the available databases at once.

2. On the **Database** (or **Server/Instance**) tab, select **Export Files** > **Export latest state to Desktop\<db_name>** or right-click a database and select **Export files** > **Export latest state to Desktop\<db_name>**.



Export as BAK

Continue with this section to learn more about exporting databases files as BAK.

> **IMPORTANT**
>
> To export database files as BAK, make sure to configure a staging SQL server, as described in Configuring Staging SQL Server.

Exporting Single Database

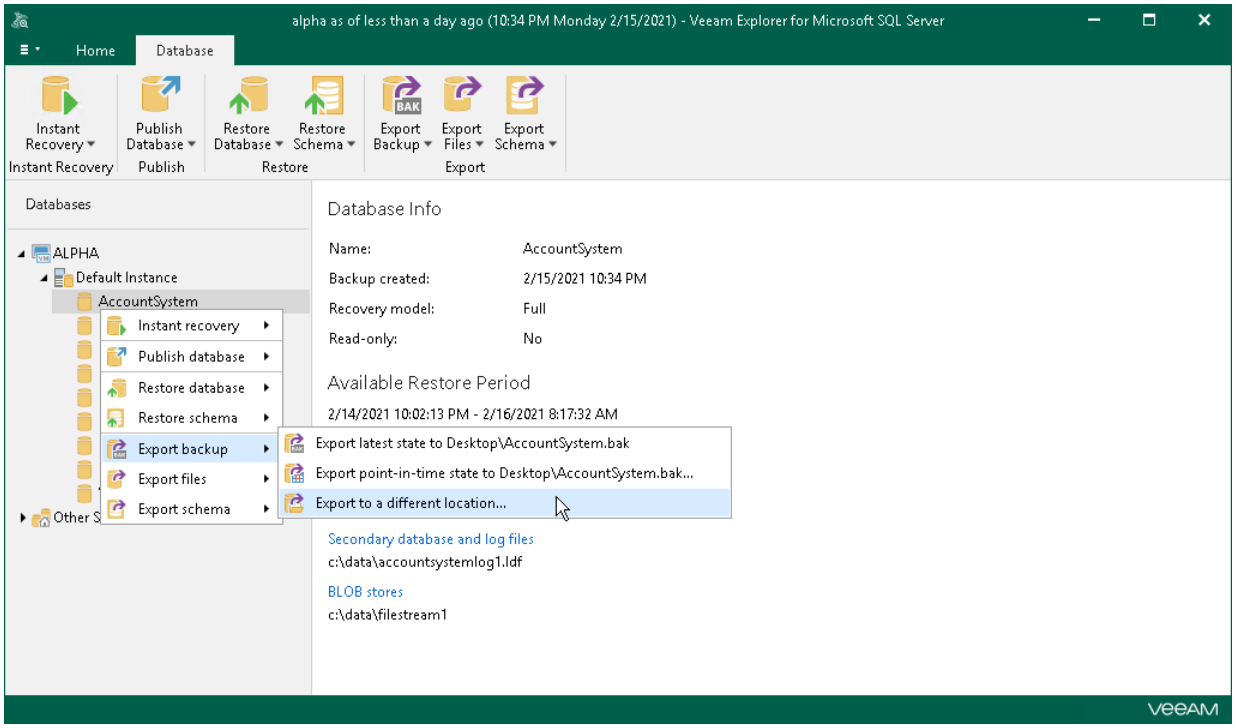
To export a single SQL database, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the database export location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** (or **Server/Instance**) tab, select **Export Backup** > **Export to a different location** or right-click a database and select **Export backup** > **Export to a different location**.



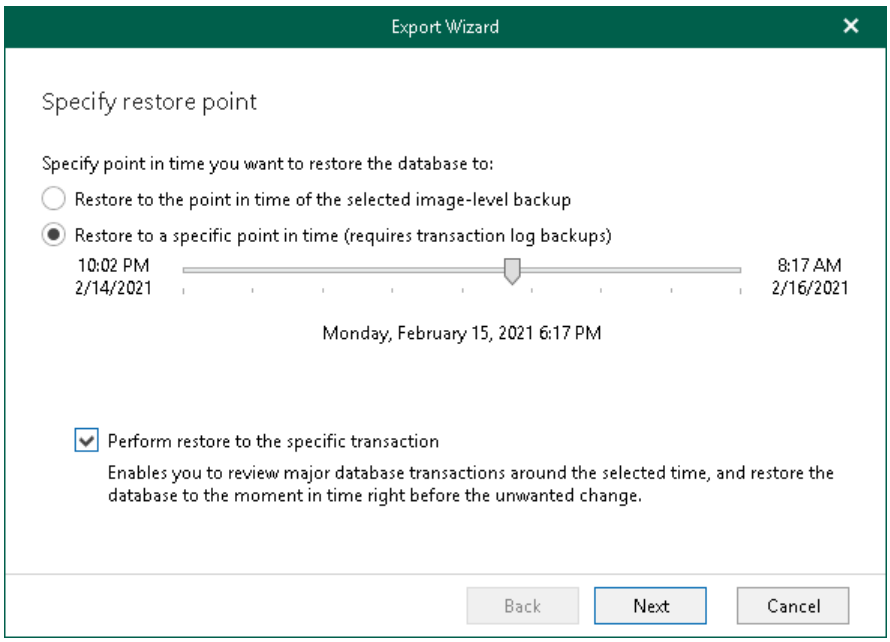
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

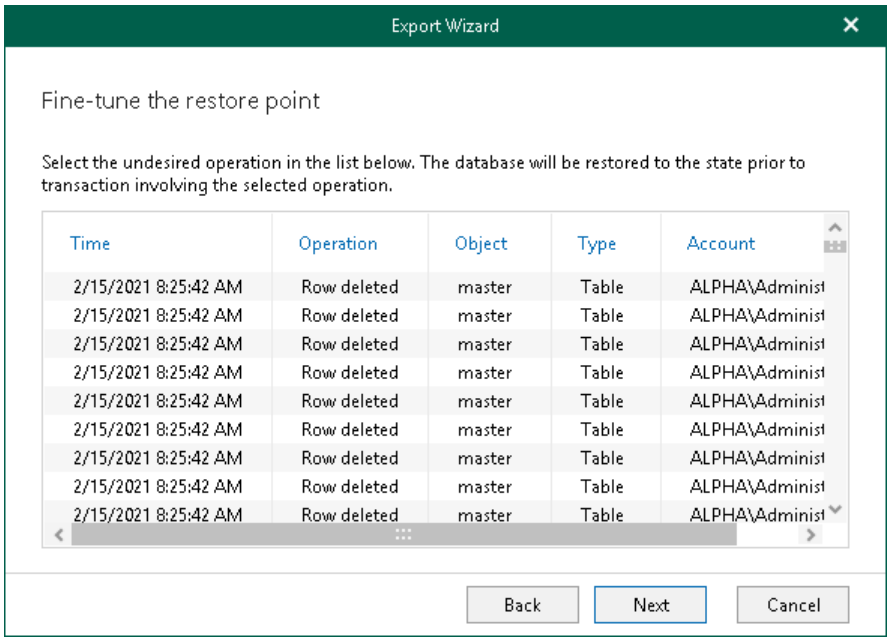


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.

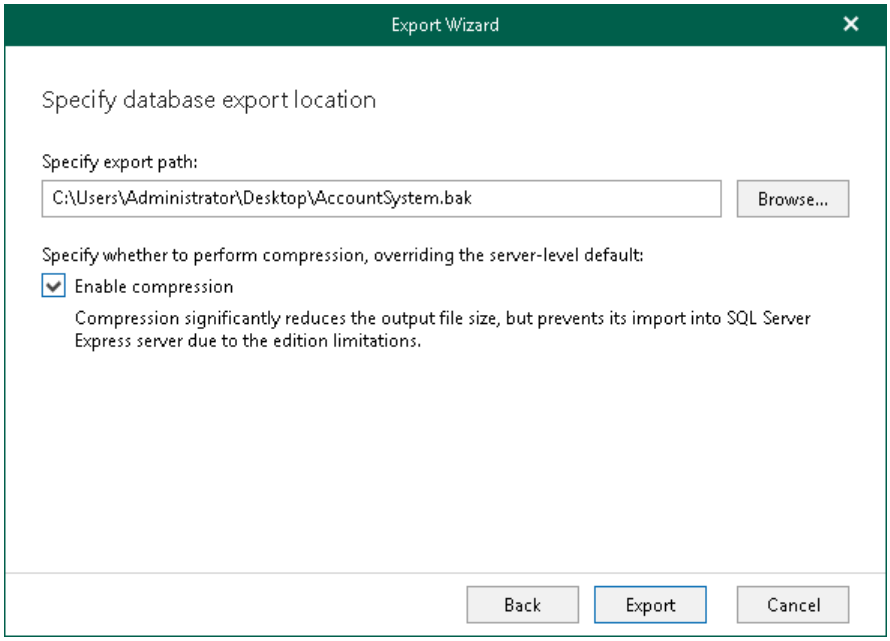


Step 4. Specify Database Export Location

At this step of the wizard, specify the path to the destination directory.

You can select **Enable compression** check box to reduce the output file size.

> **NOTE**
>
> Compression is unavailable for Microsoft SQL Server 2005 and all Express Editions of Microsoft SQL Server.



Exporting Multiple Databases

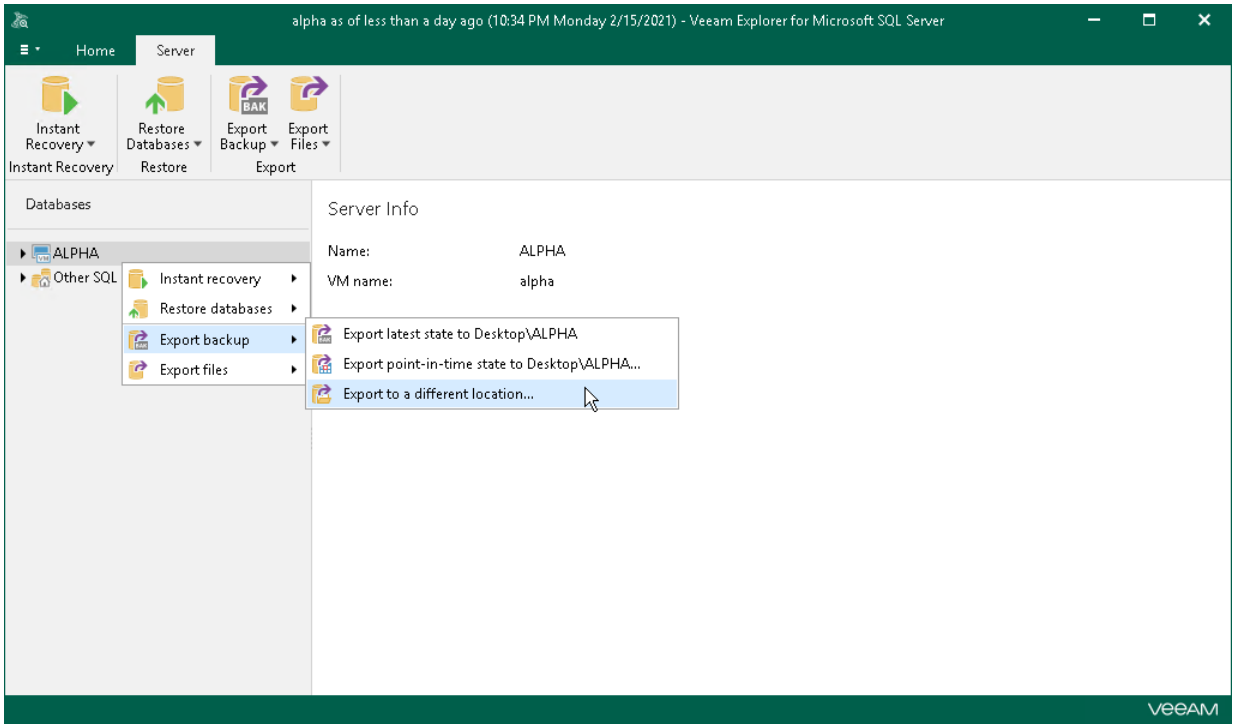
To export multiple SQL databases as BAK, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Specify the database export location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a server or instance.
2. On the **Server/Instance** tab, select **Export Backup** > **Export to a different location** or right-click a database and select **Export backup** > **Export to a different location**.



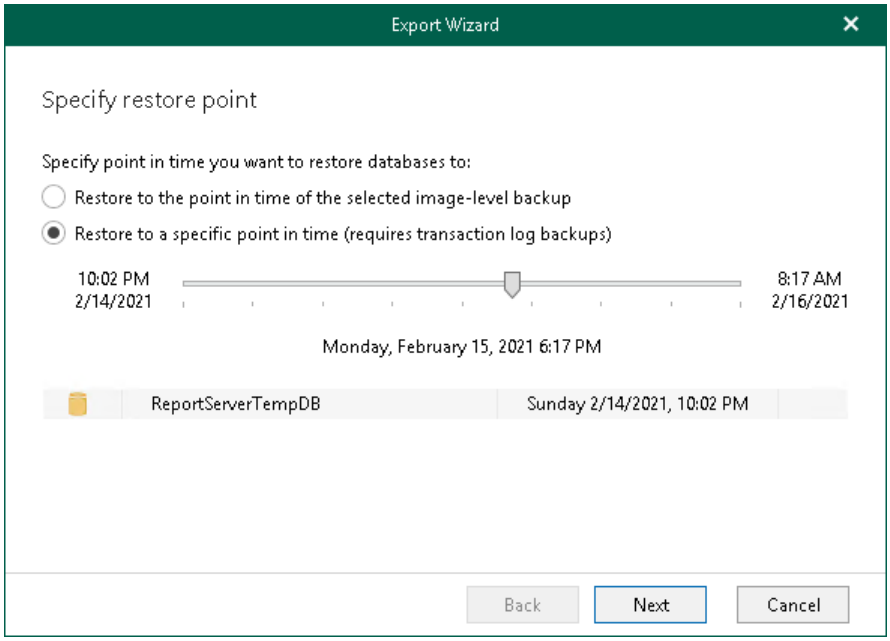
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.

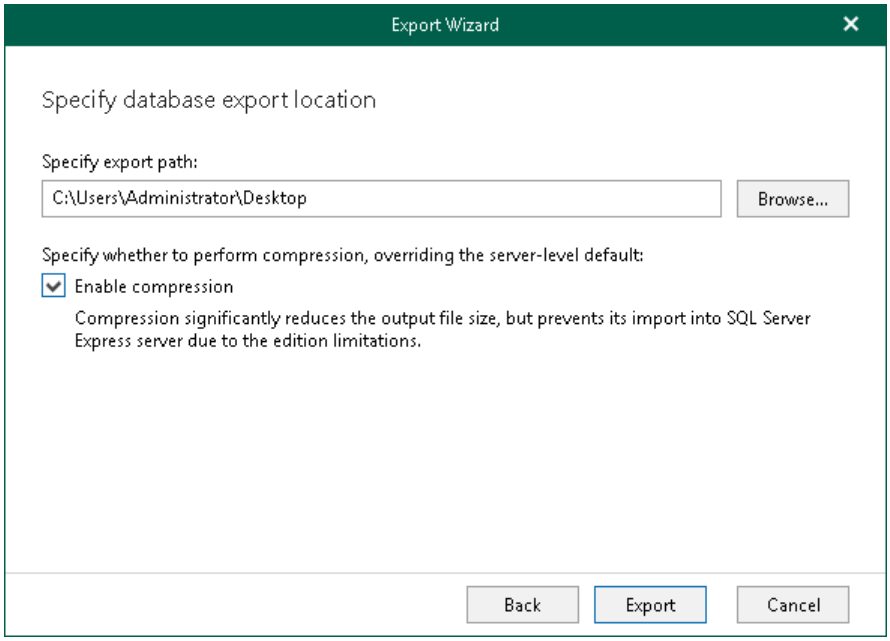


Step 3. Specify Database Export Location

At this step of the wizard, specify the path to the destination directory.

You can select **Enable compression** check box to reduce the file size.

> **NOTE**
>
> Compression is unavailable for Microsoft SQL Server 2005 and all Express Editions of Microsoft SQL Server.



Exporting Latest or Point-in-Time State

Continue with this section to learn more about exporting your data as of a latest or point-in-time state.

Exporting Point-in-Time State

To export data as of a point-in-time state, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

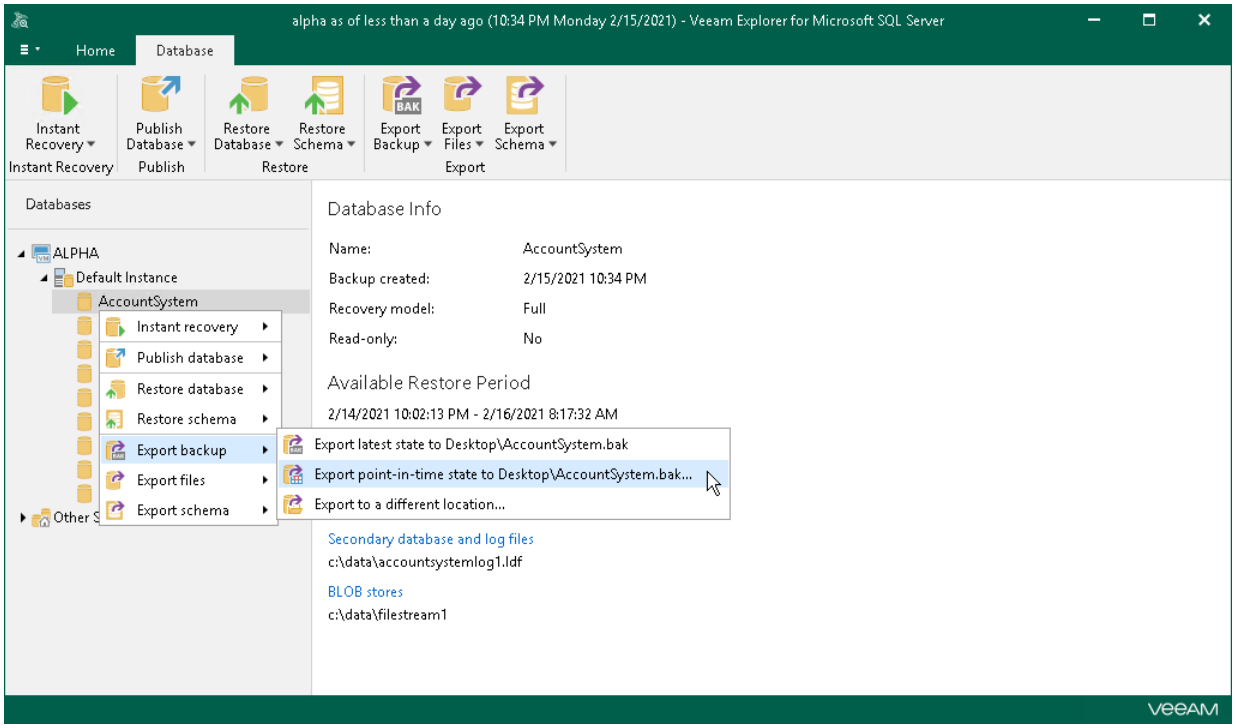
Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database, server or instance.

   You can select the root instance node to export all the available databases at once.

2. On the **Database** (or **Server/Instance**) tab, select **Export Backup** > **Export point-in-time state to Desktop\<db_name>.bak** or right-click a database and select **Export backup** > **Export point-in-time state to Desktop\<db_name>.bak**.



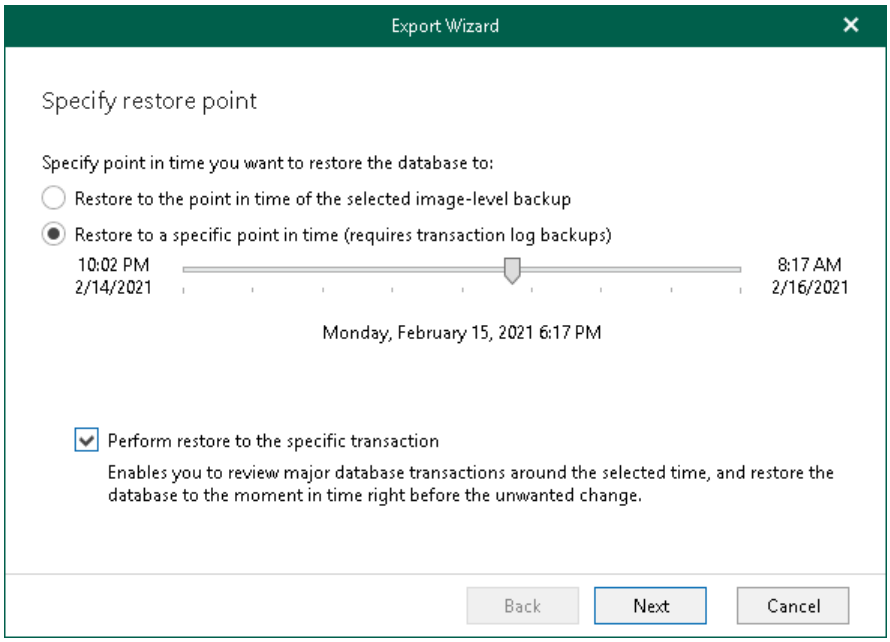
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

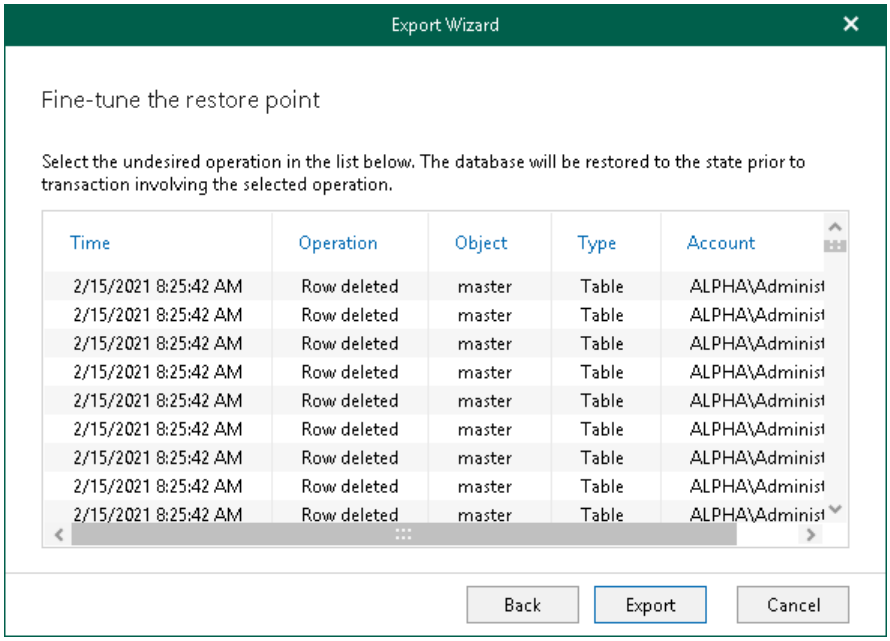


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



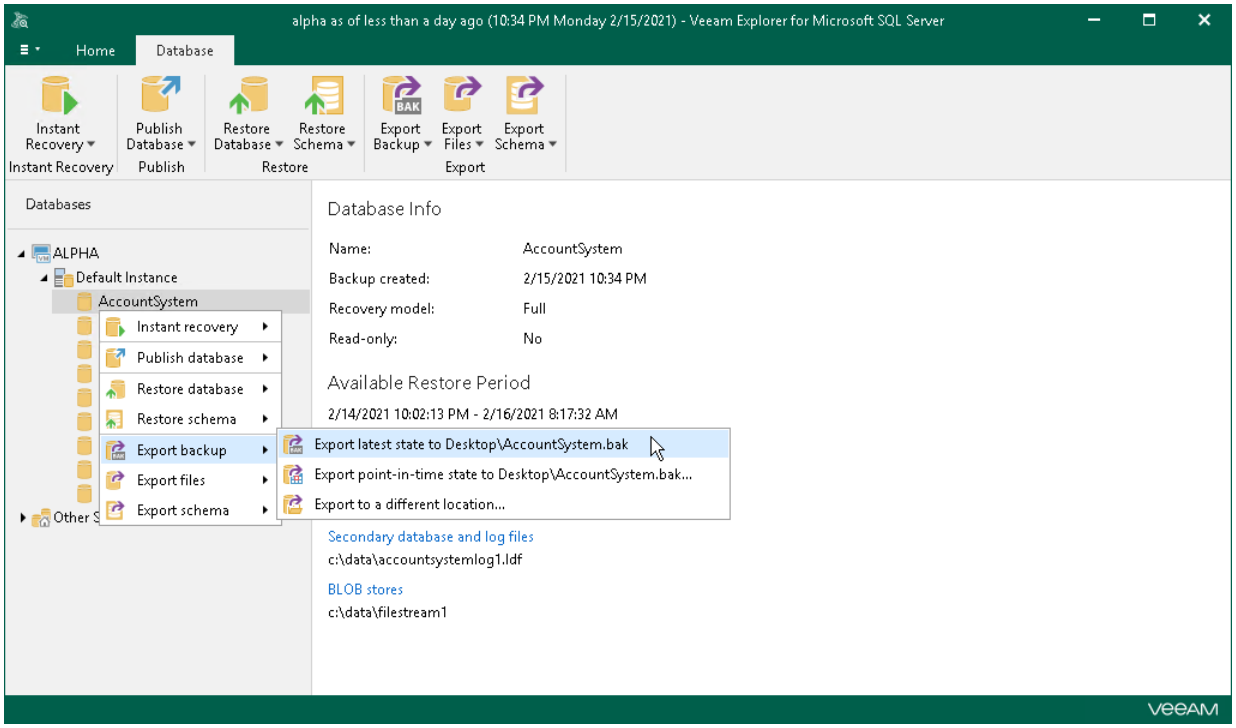
Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database or instance.

   You can select the root instance node to export all the available databases at once.

2. On the **Database** (or **Server/Instance**) tab, select **Export Backup** > **Export latest state to Desktop\<db_name>.bak** or right-click a database and select **Export backup** > **Export latest state to Desktop\<db_name>.bak**.



Database Schema and Data Export

Topics in this section provide information on how to use Veeam Explorer for Microsoft SQL Server to export your database schema and data.

> **NOTE**
>
> Export of schema and data for multiple databases is not supported.

Exporting to Custom Location

To export database schema and data, do the following:

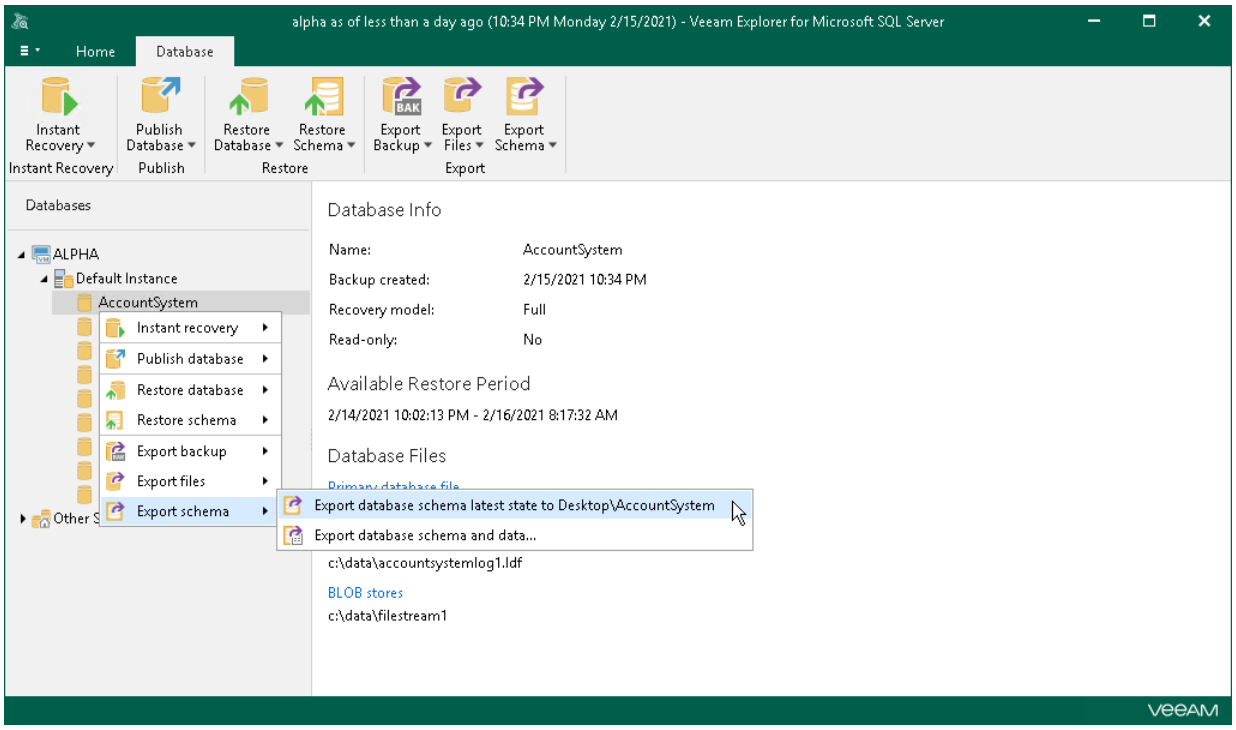
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Select database objects.
5. Specify names for objects.
6. Specify the destination folder.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** (or **Server/Instance**) tab, select **Export Schema** > **Export database schema and data** or right-click a database and select **Export schema** > **Export database schema and data**.

> **TIP**
>
> To import data tables, use the standard SQL server **bcp.exe** utility. For more information, see this Microsoft article.



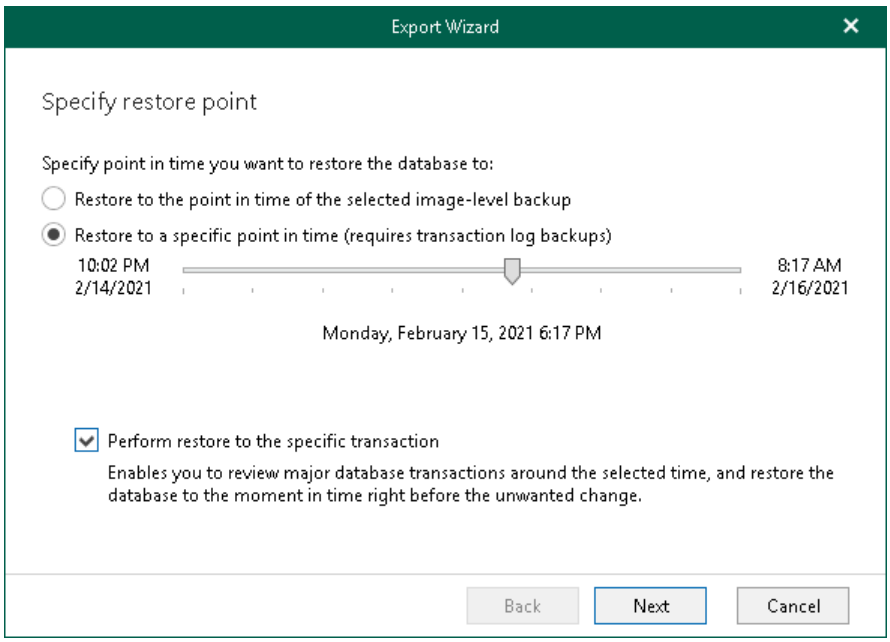
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

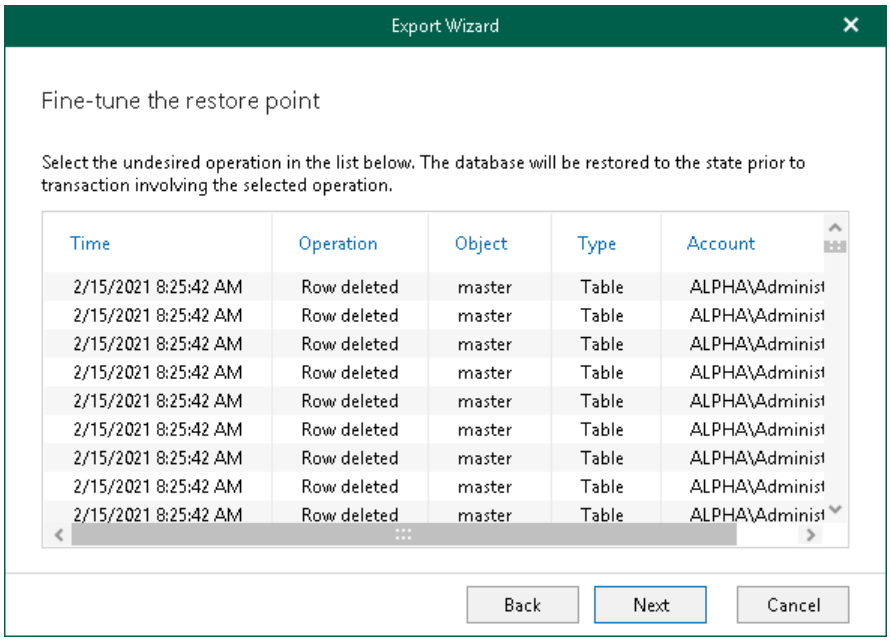


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

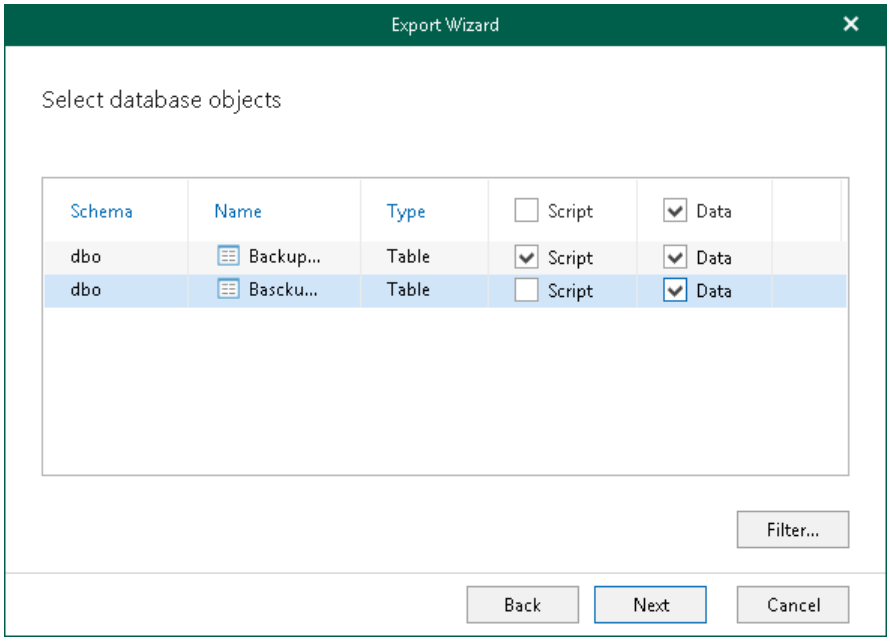
> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Select Database Objects

At this step of the wizard, select database objects to restore.

To display only specific objects, click **Filter** and select an object type you want to be shown in the list.

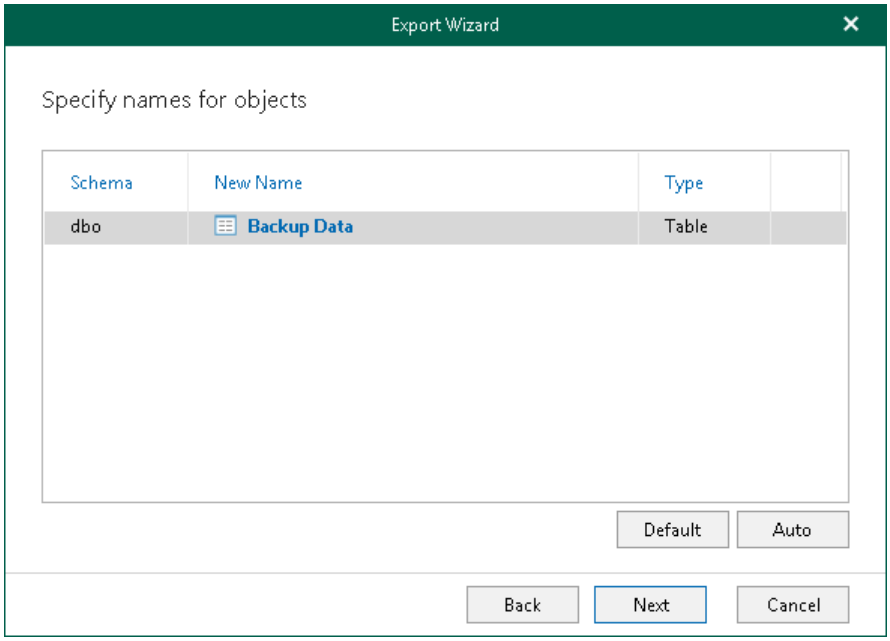


Step 5. Specify Names for Objects

At this step of the wizard, specify the name to be assigned to the object.

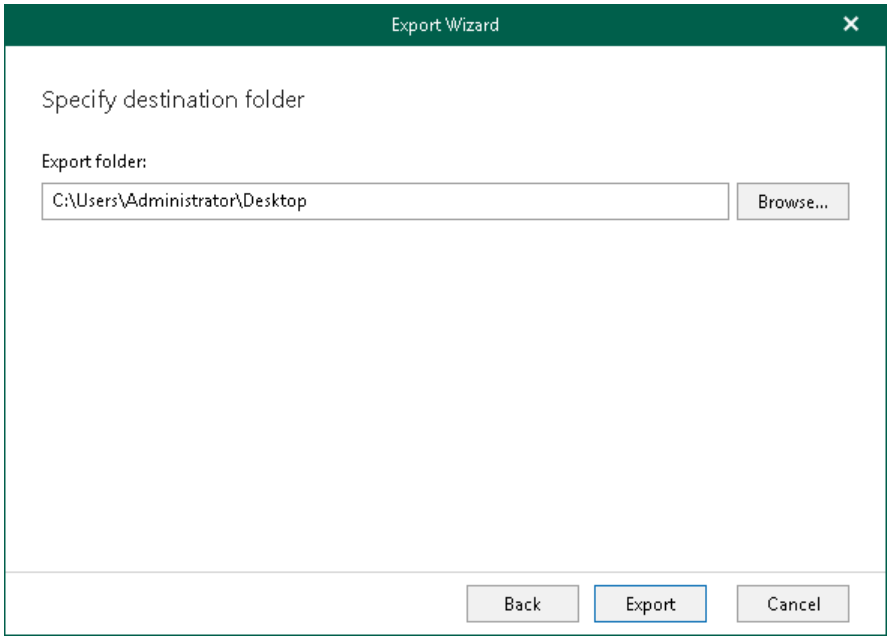
To specify a new name, select a database and provide a new name.

To assign a default name with the *_new* suffix, click **Auto**.



Step 6. Specify Destination Folder

Specify the destination folder to which you want to export selected database schema objects.

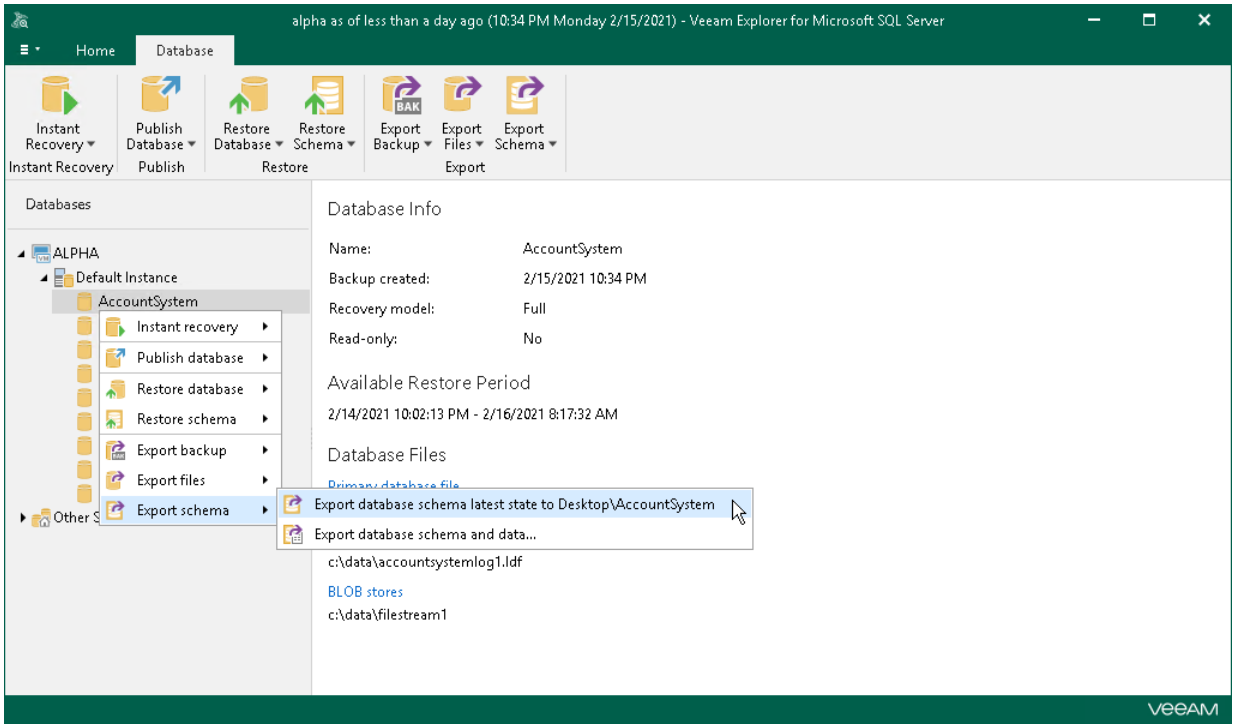


Using 1-Click Export

Veeam Explorer for Microsoft SQL Server allows you to quickly export database schema state as of the current restore point

To export database schema to the default location, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Schema** > **Export database schema latest state to Desktop\<db_name>** or right-click a database and select **Export schema** > **Export database schema latest state to Desktop\<db_name>**.



SQL Server Database Operations

The following table lists SQL Server database operations and their corresponding display names that appear in the fine-tune dialog.

Entity	Operation	Display Format	Constraints
Table	CREATE	<date_time> Created[/Modified] <table_name> Table <table ID> <initiator>	
	DROP	<date_time> Deleted <table_name> Table <table ID> <initiator>	
	ALTER	<date_time> Column added <table_name> Table <table ID> <initiator>	
	INSERT INTO	<date_time> Inserted row <table_name>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	DELETE FROM	<date_time> Deleted row <table_name>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	UPDATE	<date_time> Modified <table_name>>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	TRUNCATE	<date_time> Truncated Table <initiator>	Table name and ID will not be displayed for deleted table.
	BULK INSERT	<date_time> Inserted row <table_name>[/table_ID] Table <initiator>	
View	CREATE	<date_time> Created <view_name> View <initiator>	
	DROP	<date_time> Deleted <view_name> Table <initiator>	

Entity	Operation	Display Format	Constraints
	ALTER	<date_time> Modified <view_name> View <initiator>	
Index	CREATE	<date_time> Created <index_name> Index <initiator>	
	DROP	<date_time> Deleted <index_name> Index <initiator>	
	ALTER	<date_time> Modified <index_name> Index <initiator>	
Procedure	CREATE	<date_time> Created <procedure_name> Procedure <initiator>	
	DROP	<date_time> Deleted <procedure_name> Table <initiator>	
	ALTER	<date_time> Modified <procedure_name> Procedure <initiator>	
Function	CREATE	<date_time> Created <function_name> Function <initiator>	
	DROP	<date_time> Deleted <function_name> Table <initiator>	
	ALTER	<date_time> Modified <function_name> Function <initiator>	
Schema	CREATE	<date_time> Created <schema_name> Schema <initiator>	
	DROP	<date_time> Deleted <schema_name> Schema <initiator>	
	ALTER	<date_time> Modified <schema_name> Schema <initiator>	Schema cannot be detected.
User	CREATE	<date_time> Created <user_name> User <initiator>	

Entity	Operation	Display Format	Constraints
	DROP	<date_time> Deleted <user_name> User <initiator>	
	ALTER	<date_time> Modified <user_name> User <initiator>	
Trigger	CREATE	<date_time> Created <trigger_name> Trigger <initiator>	
	DROP	<date_time> Deleted <trigger_name> Trigger <initiator>	
	ALTER	<date_time> Modified <trigger_name> Trigger <initiator>	

Veeam Explorer for Oracle

Veeam Explorer for Oracle allows you to restore and export Oracle databases and Data Guard from backups created by Veeam Backup & Replication.

In This Section

- Planning and Preparation
- Launching Application and Exploring Backups
- General Application Settings
- Exploring Oracle Backups
- Data Restore
- Data Publishing
- Instant Recovery
- Data Export

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Oracle.

System Requirements

This section lists system requirements for Veeam Explorer for Oracle.

Component	Requirement
Oracle on Windows OS / Oracle on Linux OS	For more information on supported operating systems, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

Used Ports

The following tables list network ports that must be opened to manage inbound/outbound traffic.

Backup

Oracle on Windows

From	To	Protocol	Port	Notes
Veeam Backup Server	**Oracle Server Guest OS**	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on a VM guest OS.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC range used by the runtime coordination process that is deployed on a VM guest OS for application-aware processing.[1] For more information, see this Microsoft article.
		TCP	6167	**For archived logs shipping** Port used by the runtime coordination process on a VM guest OS from which archived logs are collected.
Oracle Server VM Guest OS	**Veeam Backup Server**	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC range used by the runtime coordination process that is deployed on a VM guest OS for application-aware processing.[1]
	Log Shipping Server	TCP	2500 to 3300	**For archived logs shipping** Default range of ports used for data transfer over the network.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Oracle on Linux

From	To	Protocol	Port	Notes
Veeam Backup Server	**Oracle on Linux Server Guest OS**	TCP	22	Default SSH port used as a control channel.
		TCP	2500 to 3300	Default range of ports used for managing data transfer over the network.
		TCP	6167	**For archived logs shipping** Port used by the runtime process on the VM guest OS from which archived logs are collected.
Oracle Server VM Guest OS	**Log Shipping Server**	TCP	2500 to 3300	**For archived logs shipping** Default range of ports used for managing data transfer over the network.

Restore

From	To	Protocol	Port	Notes
Veeam Backup Server / Standalone Console	**Mount Service**	TCP	6170	Port used for connections to the mount service.
	Oracle on Windows Server	TCP	49152 to 65535	Recommended dynamic RPC port range for Microsoft Windows 2008 and newer. For more information, see this Microsoft article.
		TCP	1025 to 1075	Default range of ports for the runtime component installed on the VM guest OS to support restore operations. Port is opened only during application item restore.
	Oracle on Linux Server	TCP	22	Default SSH port used as a control channel.

From	To	Protocol	Port	Notes
Backup Repository Server	**Oracle on Linux Server**	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) VM on the target Oracle on Linux server.
Oracle on Linux Server	**Veeam Backup Server**	TCP	22	Default SSH port used as a control channel.
	Backup Repository Server	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) VM on the target Oracle on Linux server.
Mount Service	**Oracle on Windows Server**	TCP	6160, 11731	Ports used by the Veeam Installer Service for connections to a target Oracle on Windows server.

Make sure to open the following ports when using a staging Oracle server.

From	To	Protocol	Port	Notes
Target VM / Staging Oracle Server	**Veeam Explorer for Oracle**	TCP	3260 to 3270	Range of ports opened by Veeam Backup & Replication to manage iSCSI traffic during restore to the target VM. This port range is opened only during application item restore.

Required Permissions

The following table lists required permissions for user accounts to back up and restore Oracle data.

Operation	Required Roles and Permissions
Backup	For more information, see the Required Permissions section of the Veeam Backup & Replication User Guide.
Restore / Accessing Staging Server	To restore data, make sure to configure user accounts as follows: • When restoring to a Windows-based VM, the account must be a member of the *Local Administrator* group. In addition, if *ASM* is used, then such an account must be a member of the *ORA_ASMADMIN* group (for Oracle 12 and higher). • When restoring to a Linux-based VM, the account must be a Linux user and have membership in the following groups: *OSASM* [if *ASM* is used] (typically *asmadmin*), *OSDBA* (typically dba), *Oracle Inventory group* (typically *oinstall*).

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware image processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication user guide.

If your backups were created without application-aware image processing, you can explore them, as described in Exploring non-Application Enabled Backups.

The application-specific information is retrieved according to the following:

- If the **application-aware image processing** option is enabled, Veeam Explorer obtains application-specific Oracle database information from the Oracle VM backup metadata located in the Veeam backup server configuration database.
- If the **application-aware image processing** option is disabled, Veeam Explorer requires a staging Oracle server to mount a selected image-level Oracle VM backup (with databases and redo logs) and collect required information using the guest scan and Oracle infrastructure analysis.

> **IMPORTANT**
>
> Make sure to have your database in the **OPEN** state during backup. Otherwise, the following warning message will appear in the backup job session: "*Oracle database instance state is not valid for property collection*".

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Oracle.

General

- When Veeam Explorer for Oracle is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup and Replication Global Notification settings.
- [Restore to Linux server] Restore with Veeam Explorer for Oracle is not supported if the SQL*Plus environment on the target Oracle server is configured to use `glogin.sql` or `login.sql` profile files. For details, see the Configuring SQL*Plus section of the SQL*Plus User's Guide.
- [For refreshable PDB] Data restore, data publishing and instant recovery are not supported for refreshable PDBs.
- Mount of Btrfs disks will fail if you want to perform instant recovery, data restore or data publish to the original server. The issue occurs due to restriction for mounting 2 Btrfs disks with identical IDs to the same machine.
- Mount operations with fuse are not supported on kernel versions 4.0.0 – 4.1.33. Make sure to upgrade the kernel to version 4.1.37 or higher.

Restore from Image-Level Backups

- Veeam Explorer for Oracle does not support restore via *PSDirect*, *VIX* or *Sphere API*.
- 1-Click restore to the original location from storage snapshots is not supported.
- A point in time restore is not supported for replicas and backups stored in the DR site by backup copy jobs, nor it is supported for backups stored in a cloud repository. Such repositories cannot be used as a destination location for archived logs.
- Restore of databases from the current restore point is only supported for backups created by Veeam backup job, replication job, VeeamZIP and for imported backup and storage snapshots.
- If OS authentication on a target Oracle server is disabled, the restore of databases with enabled ASM will not be possible.
- If OS authentication on a staging Oracle server is disabled, the restore of databases with enabled ASM as of the selected transaction state will not be possible.
- Make sure that both the backed-up Oracle machine and the target server to which you are restoring have the same OS patch version.

Restore from RMAN Backups

> **IMPORTANT**
>
> Restore from RMAN backups is not be possible if OS authentication is disabled on the target Oracle server.

Restore of Oracle Real Application Clusters (RAC)

To restore RAC databases from RMAN backups, make sure you apply the following restore settings. Otherwise, the databases will be restored as standalone databases.

- **Restore to original server**: You must perform the restore with original name and settings.
- **Restore to another server**:
  - You must perform the restore with original name and settings.
  - The Oracle Home and Oracle directory structure must remain the same.
  - You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
  - For Oracle ASM, the file system structure of the restored database must remain the same.

Restore of Data Guard Databases

Data restore with Veeam Explorer for Oracle from backups of Data Guard databases created by Veeam Plug-in for Oracle RMAN has experimental support. You can restore Data Guard databases from Veeam Plug-in backups with the following limitations:

- **Restore to original server**
  - You can restore Data Guard primary databases as primary databases only to the original location with the original name and settings.
  - You can restore Data Guard standby databases as standby databases only to the original location with the original name and settings.

    A restore with different settings will fail due to Data Guard limitations.
- **Restore to another server**
  - Make sure that the copy of the original cluster already exists in the duplicated environment.
  - You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
  - You can restore Data Guard primary databases as primary databases only with the original name and settings.
  - You can restore Data Guard standby databases as standby databases only to the original location with original name and settings.

    A restore with different settings will fail due to Data Guard limitations.

Restore of Oracle Databases

When restoring to another server with the original name and settings, consider the following:

- The Oracle Home and Oracle directory structure must remain the same.
- You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
- For Oracle ASM, the file system structure of the restored database must remain the same.

Publishing from Image-Level Backups

- Make sure that the target Oracle server to which you publish your databases is of the same version as the database in the backup.
- If the database that you publish is part of the ASM group, make sure that the target Oracle server also has an ASM group properly configured.

Instant Recovery

- Instant recovery is supported for image-level backups only. You cannot perform instant recovery from RMAN backups.
- If OS authentication on a target Oracle server is disabled, the instant recovery of databases will not be possible.
- If OS authentication on a staging Oracle server is disabled, the instant recovery of databases as of the selected transaction state will not be possible.
- Make sure that both the backed-up Oracle machine and the target server to which you are restoring have the same OS patch version.
- Instant recovery is not supported if `tnsnames.ora` and `listener.ora` are stored in a non-default location.
- Instant recovery of the entire Oracle Data Guard is not supported. However, you can restore individual Data Guard databases.

Instant Recovery Process

- Veeam Explorer requires 512 MB RAM for instant recovery process for each database.
- During an instant recovery process, if you add a new pluggable database to the container, instant recovery session fails.
- During an instant recovery process, if you add a new tablespace or datafile to the published database while the database files are being copied, the instant recovery session fails.

Launching Application and Exploring Backups

To open Veeam Explorer for Oracle and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created in Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

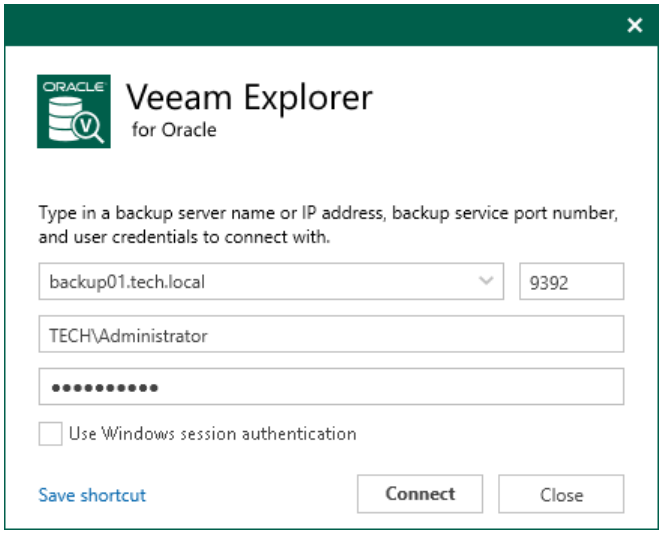
- Go to **Start** and click **Veeam Explorer for Oracle**.

If you open Veeam Explorer for Oracle from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

- The domain name or IP address of the backup server to which you want to connect
- The port number
- User credentials

  The account must be a member of the *Local Administrator* group on a target server. To use the account under which Veeam Explorer for Microsoft SQL Server is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



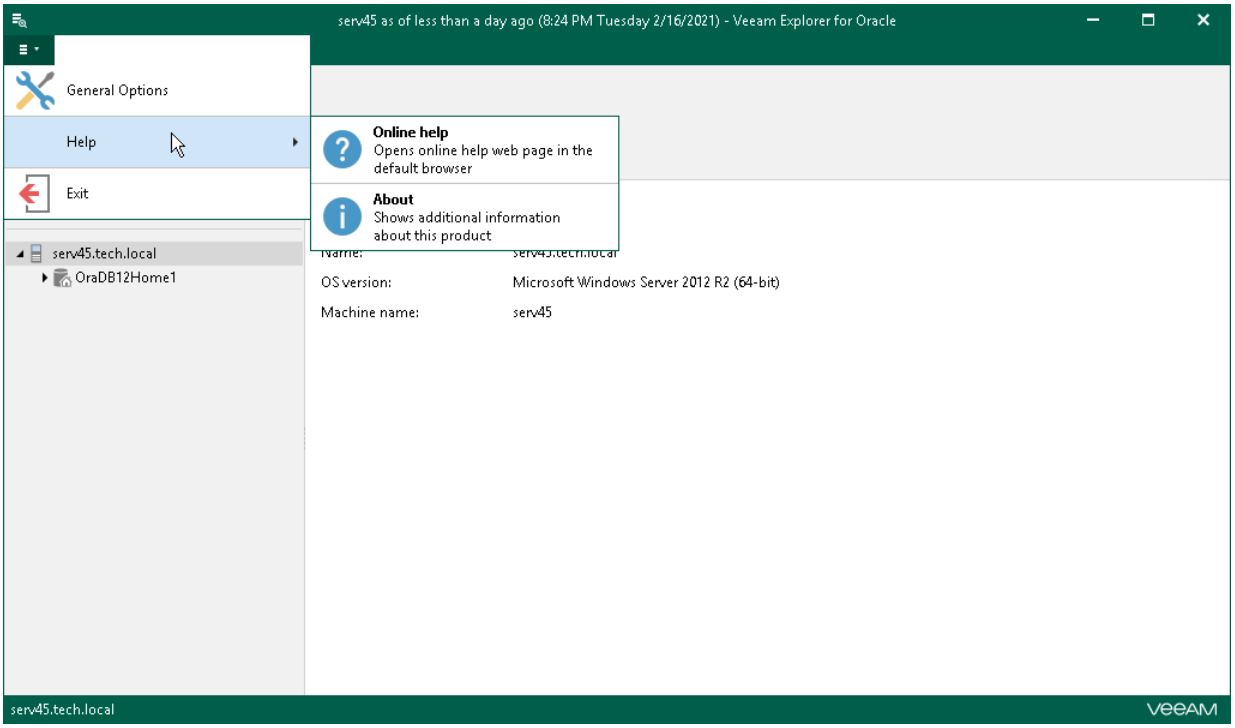
Understanding User Interface

Veeam Explorer for Oracle provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

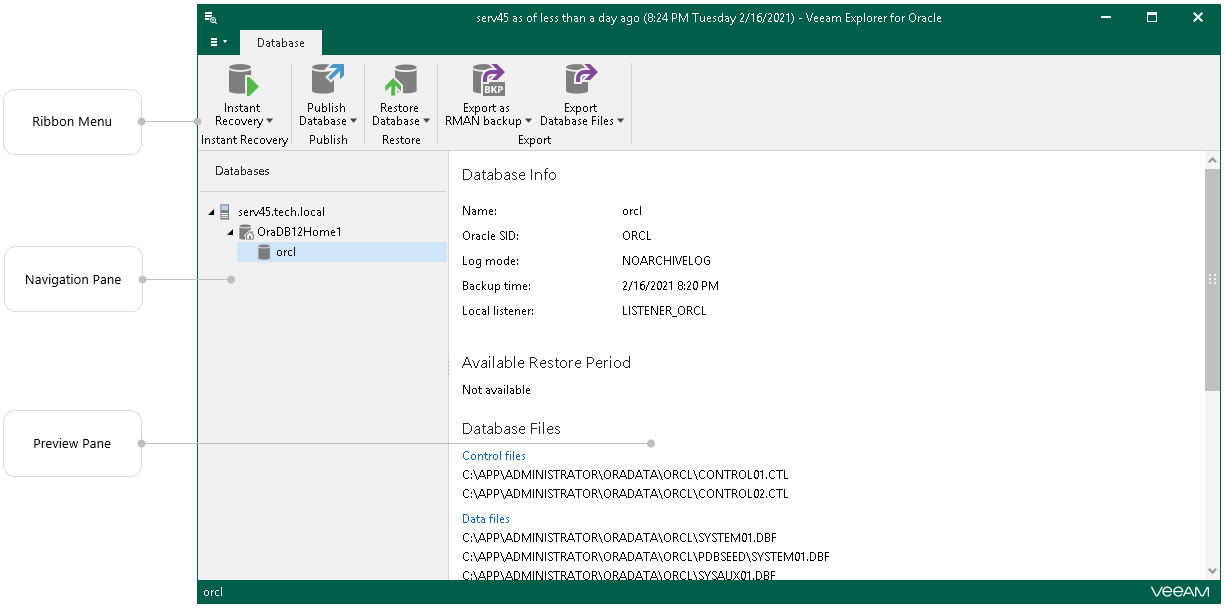
- **General Options**. Allows you to configure program options.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows information about the product.
- **Exit**. Closes the program.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Understanding Mounting

When restoring your data, Veeam Explorer requires an additional mount point to be created to display the list of available transactions.

Mounting is performed by the *Veeam Mount Service* component which is deployed on a backup repository machine or any other machine you define in the backup repository settings. For more information on configuring mount server settings, see the Mount Server section of the Veeam Backup & Replication User Guide.

During mounting, *Veeam Mount Service* retrieves a VM file system from the backup file, attaches it to the hard drive of a target machine and creates a mount point.

Mounting is done as follows:

- To mount a VM file system on machines with the Microsoft Windows operating system, Veeam uses the iSCSI protocol.

  The original virtual machine or the staging server acts as an iSCSI initiator and the mount server that is associated with the backup repository acts as an iSCSI target. The iSCSI mount point is non-persistent and only exists during the recovery process.

- To mount a VM file system on machines with Linux, Veeam uses *fuse*.

> **NOTE**
>
> When using fine-tune restore, Veeam requires a staging Oracle server to mount the VM file system.

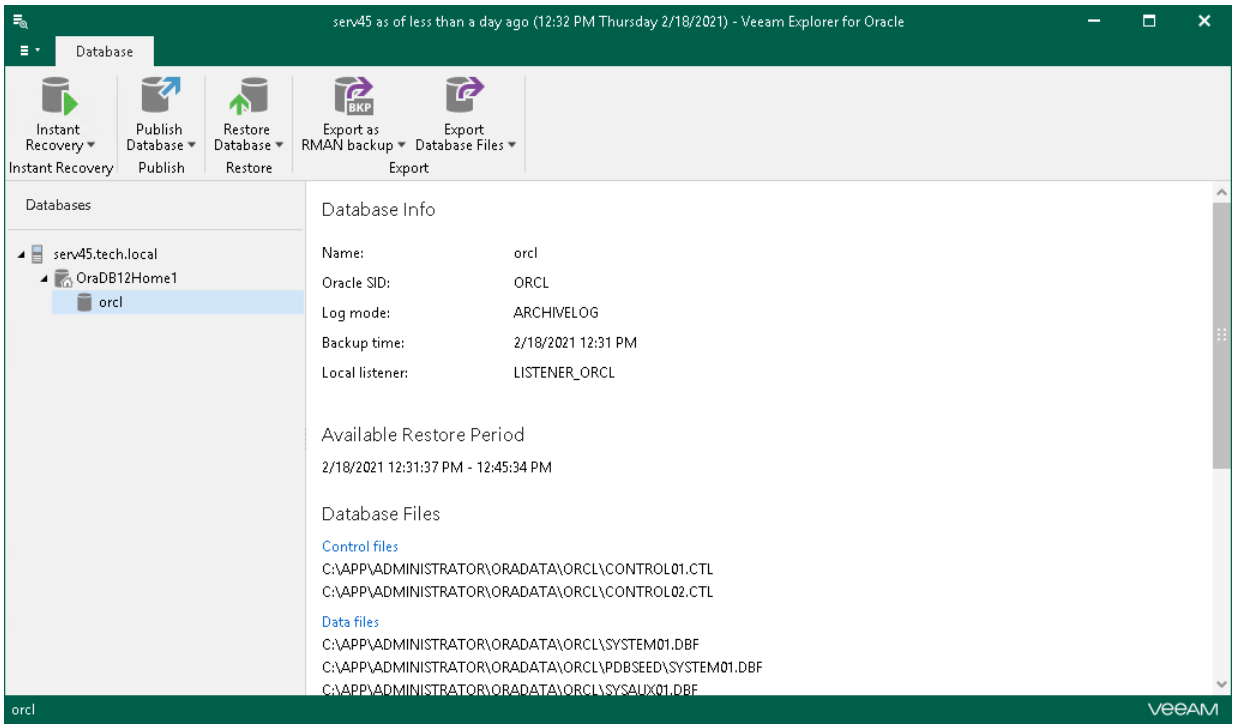
Viewing Database Information

To view Oracle database information, select a database or Data Guard in the navigation pane and review its properties in the preview pane.

Viewing Oracle Database Information

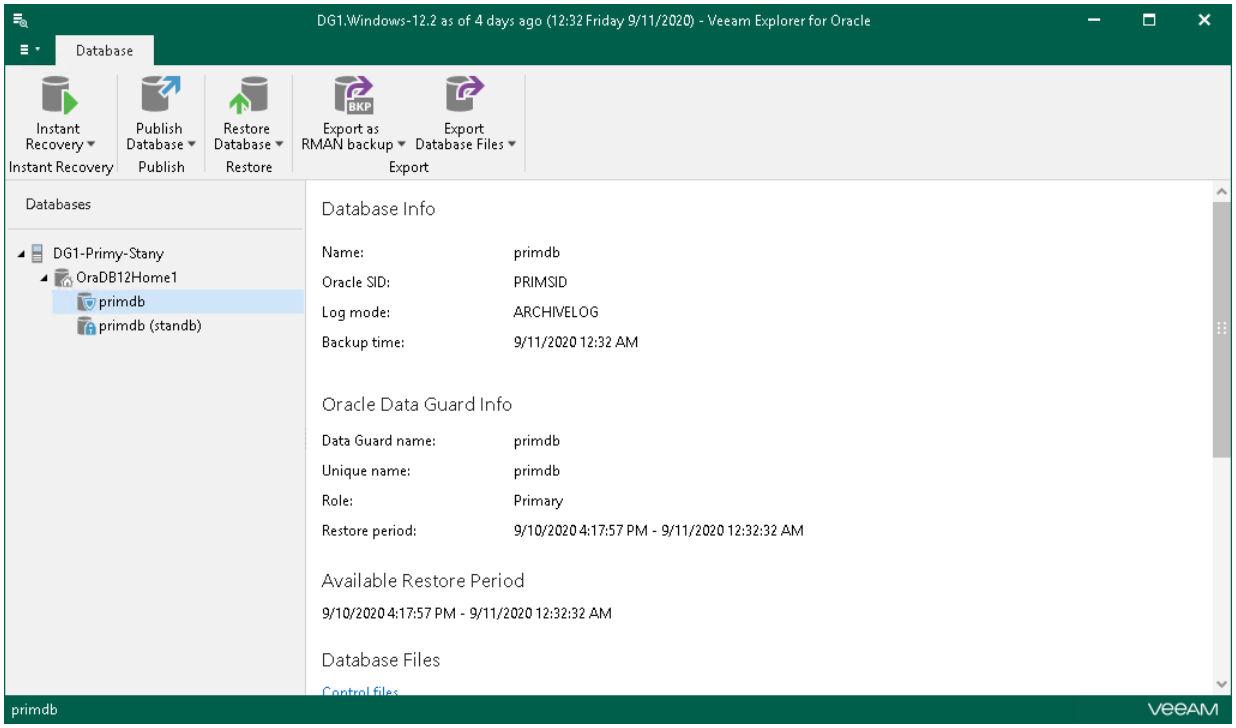
The following figure shows the standalone database information view.

If the current restore point was created with Oracle Automatic Storage Management (ASM), file paths will be displayed with the '+' prefix.



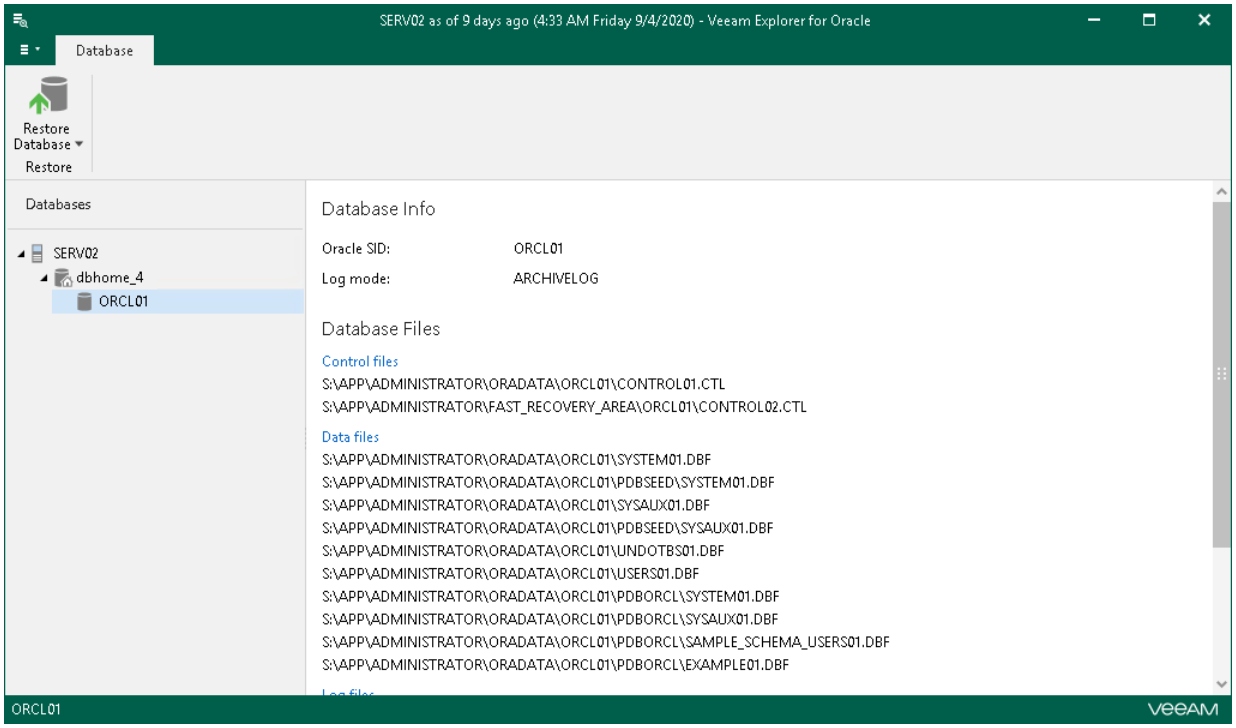
Viewing Oracle Data Guard Information

The following figure shows the Data Guard information view.



Viewing Oracle RMAN Database Information

The following figure shows the RMAN database information view.



General Application Settings

Continue with this section to learn more about configuring required application settings and components.

Configuring Staging Oracle Server

This section explains how to configure a staging Oracle server.

A staging Oracle server is required in the following cases:

- If you use the *point-in-time state* option of databases for restore, export, publishing and instant recovery operations.
- To explore backups created without application-aware image processing. For more information, see Exploring Oracle Backups.

Consider the following:

- A staging server must be of the same Oracle version as both the source and target Oracle servers.
- If you plan to restore databases with *Automatic Storage Management* enabled, both staging and target servers must have ASM enabled.
- Oracle Database Express Edition cannot be used as a staging system.

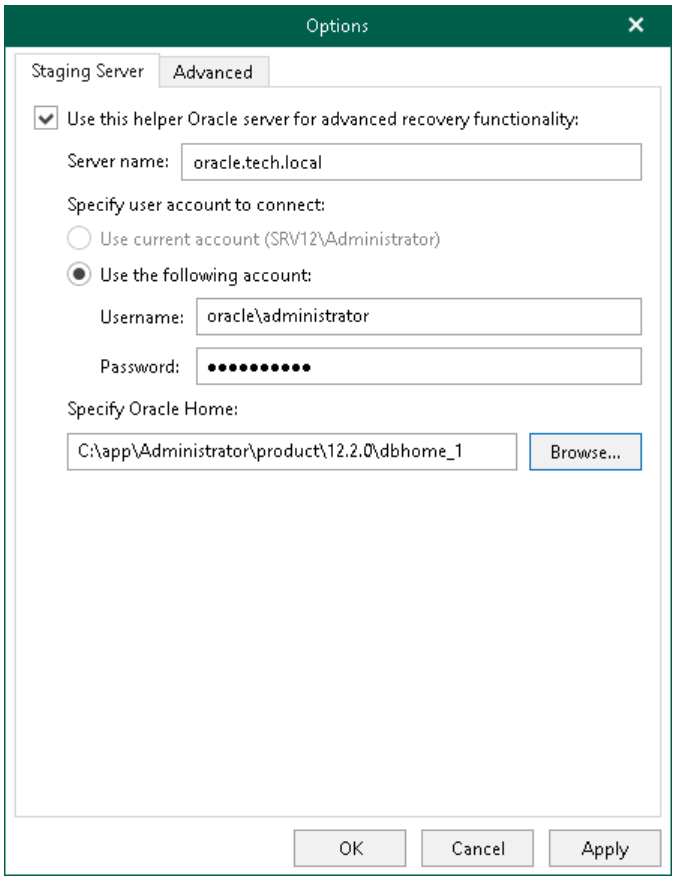
For Windows-based VM

To configure a staging server for Windows-based machines, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Staging Server** tab, select the **Use this helper Oracle server for advanced recovery functionality** check box and do the following:
   a. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
   b. Under the **Specify user account to connect to server** section, select the following:
      - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Oracle running.
      - **Use the following account**. To connect to the specified server under a custom user account.

        When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.
3. Specify the path to Oracle Home.

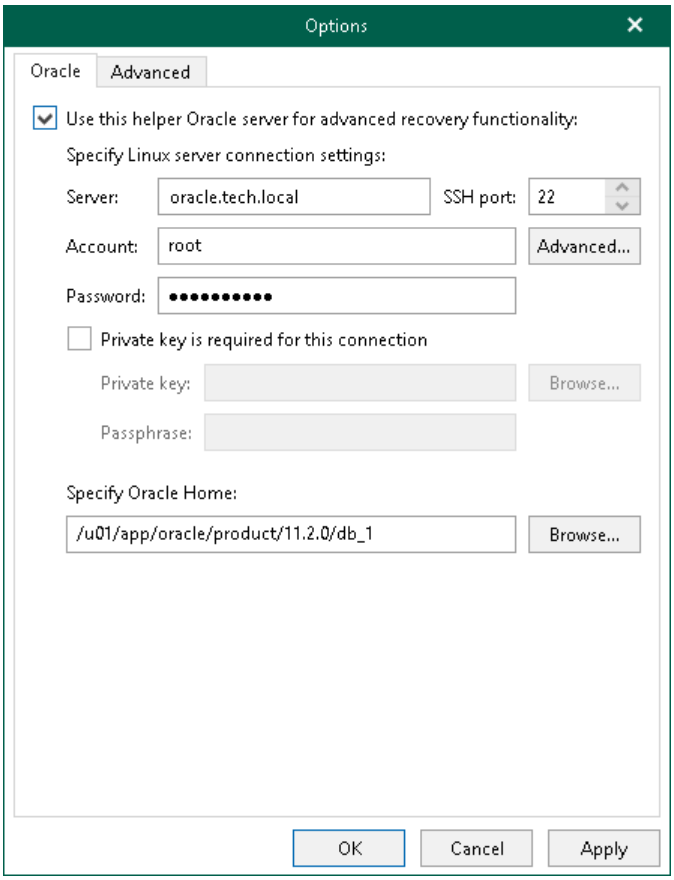
   Click **Browse** to browse for Oracle Home.



For Linux-based VM

To configure a staging server for Linux-based machines, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Oracle** tab, select the **Use this helper Oracle server for advanced recovery functionality** check box and do the following:
   a. In the **Server** field, specify the name of the Oracle server to which you want to restore data.
   b. In the **SSH-port** field, specify the port number.
   c. In the **Account** field, specify a user account under which to connect to the specified server.
   d. In the **Password** field, specify the password.
   e. If the private key is required to connect to the selected server, do the following:
      i. Select the **Private key is required for this connection** check box.
      ii. In the **Private key** filed, specify a key. To select a key, click **Browse** and select a key.
      iii. In the **Passphrase** field, enter the passphrase.
3. Specify the path to Oracle Home.



4. If you specify data for a non-root account that does not have root permissions on a Linux server, click **Advanced** to grant sudo rights to this account.

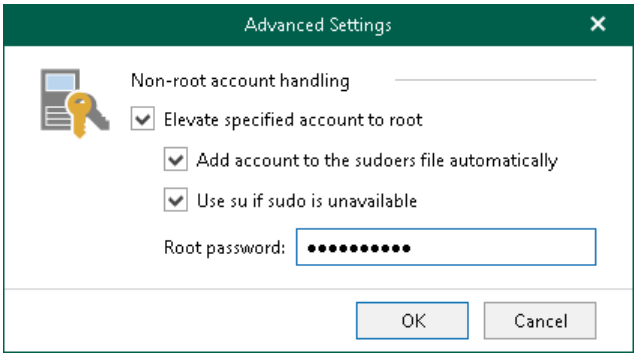
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

   b. To add the user account to the sudoers file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the sudoers file.

   c. When registering a Linux-based VM, you have an option to failover to using the su command for distros where the sudo command is not available.

      To enable the failover, select the **Use su if sudo is unavailable** check box and in the **Root password** field, enter the password for the root account.

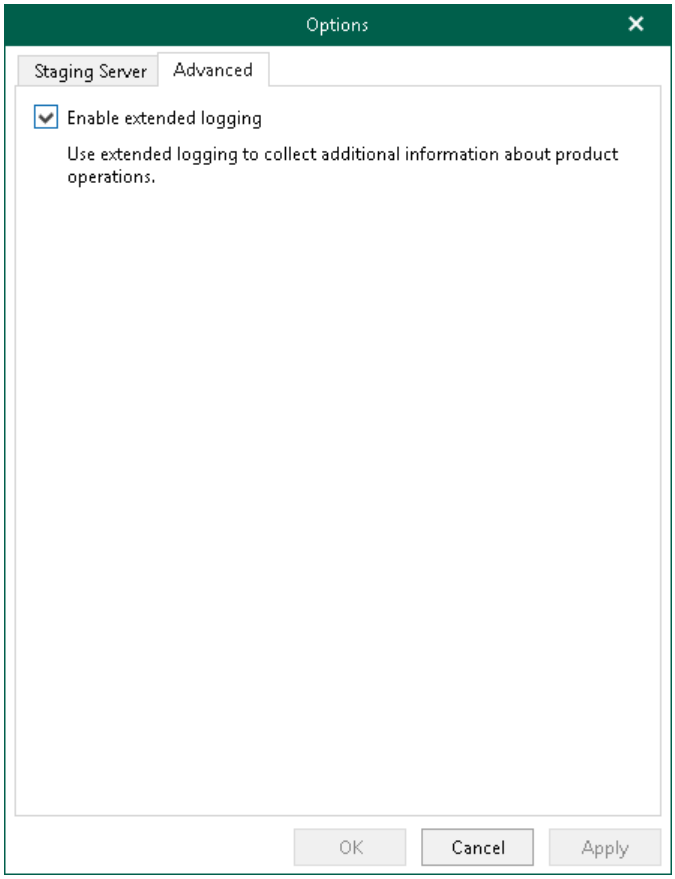


Enabling Extended Logging

Veeam Explorer for Oracle allows you to enable extended logging mode to collect logs that contain more details on specific operations.

To enable extended logging mode, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box.
3. After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs.



Exploring Oracle Backups

Continue with the section to learn more about:

- Exploring Application-Enabled Backups
- Exploring Non-Application Enabled Backups
- Exploring RMAN Backups

Exploring Application-Enabled Backups

For more information about exploring backups created with application-aware image processing, see the Restoring Application Items section of the Veeam Backup & Replication User Guide.

Exploring Non-Application Enabled Backups

If a backup file you are exploring was created without application-aware image processing, the heuristic analysis must be performed to mount required restore points and find existing Oracle databases in these points.

> **NOTE**
>
> The heuristic analysis requires a staging Oracle server to be configured in advance. For more information, see Configuring Staging Oracle Server.

To explore backups created without application-aware image processing, do the following:

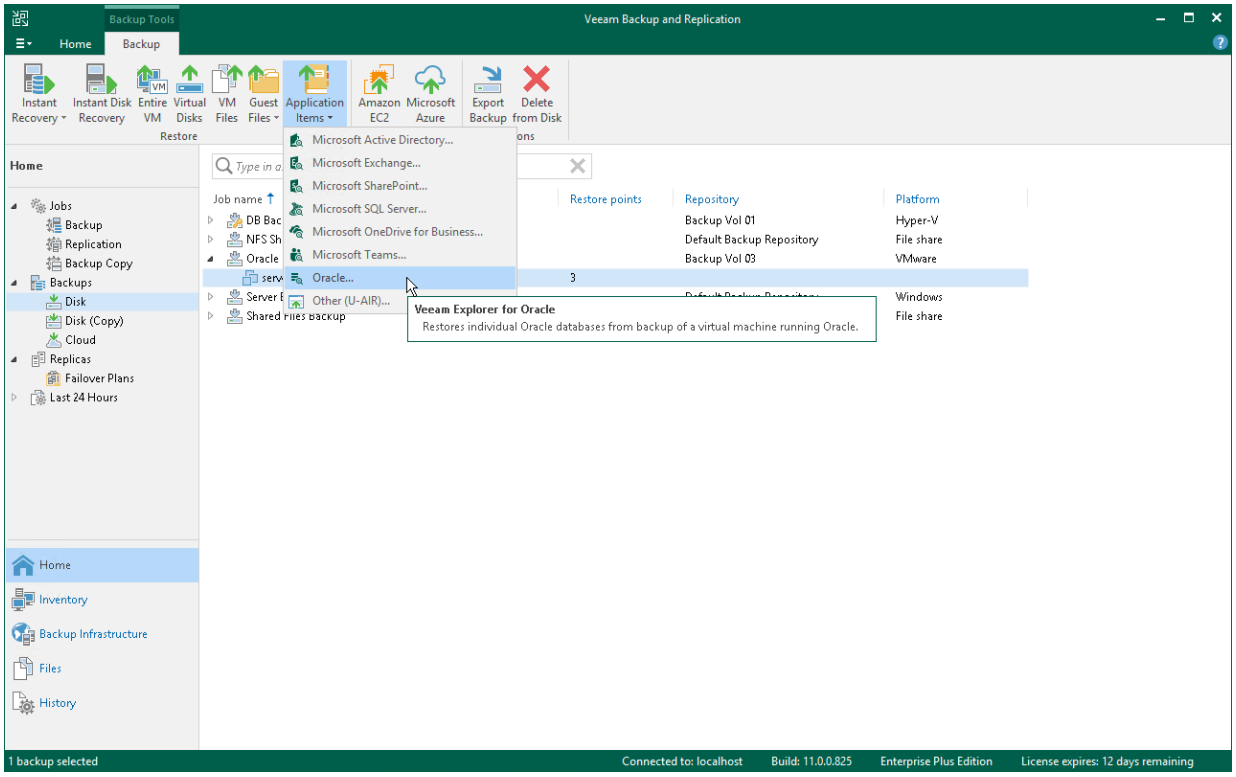
1. Launch the Heuristic Analysis wizard.
2. Specify the target server.
3. Specify heuristic settings.

Step 1. Launch Heuristic Analysis Wizard

To launch the **Heuristic Analysis** wizard, do the following:

1. In the Veeam Backup & Replication console, select the necessary backup and click **Application Items** > **Oracle** (or **Windows**) on the ribbon.
2. At the **Restore Point** step of the **Oracle Database Restore** wizard, select a restore point to explore.
3. Complete subsequent steps of the wizard and click **Browse**.

Veeam Backup & Replication will launch Veeam Explorer for Oracle and display the **Heuristic Analysis** wizard.



Step 2. Specify Target Server

At this step of the **Heuristic Analysis** wizard, specify credentials to access the target Oracle server.

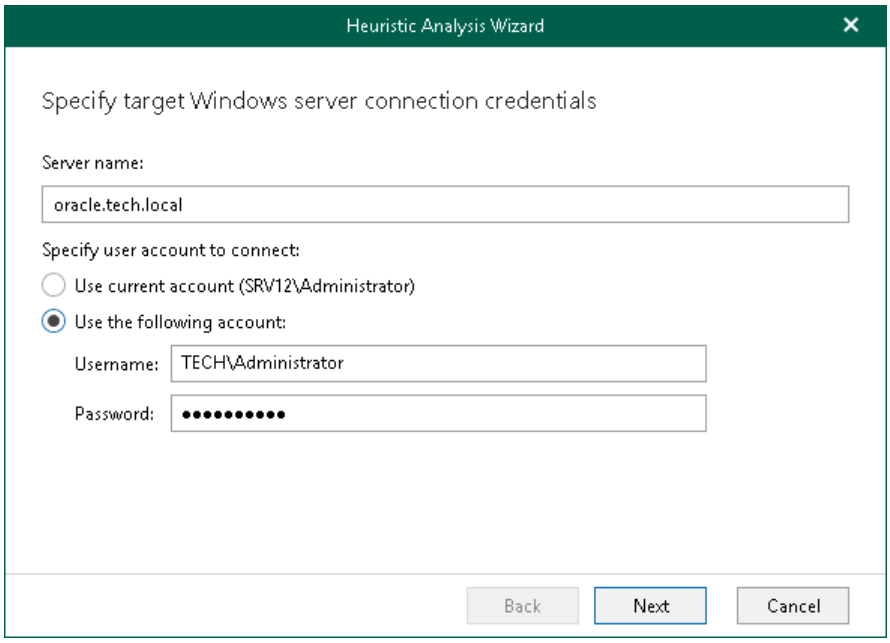
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify a server name to which you want to restore data.
2. Under the **Specify user account to connect to server** section, select one of the following:
   - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**. To connect to the specified server under a custom user account.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account has been granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.

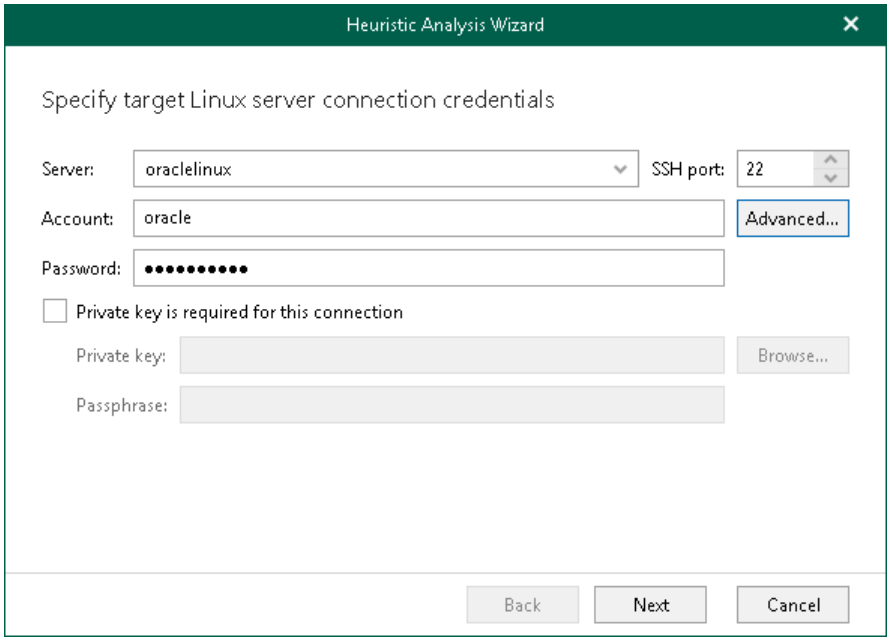


Linux-Based Oracle Server

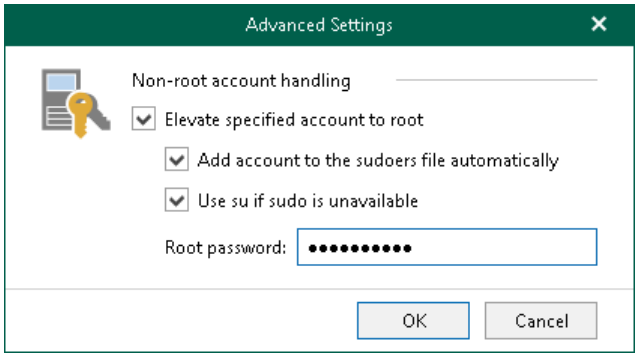
For a Linux-based Oracle server, do the following:

1. In the **Server** field, select a server to which you want to restore data.
2. In the **SSH port** field, specify the port number of the selected server.
3. In the **Account** filed, enter the user account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If the private key is required to connect to the selected server, do the following:
   a. Select the **Private key is required for this connection** check box,
   b. In the **Private key** filed, specify a key. To select a key, click **Browse** and select a key.
   c. In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



You can use the native Veeam Explorer abilities to elevate your account to **root** and add it to the **sudoers** file. To do this, click **Advanced** and select corresponding check boxes.



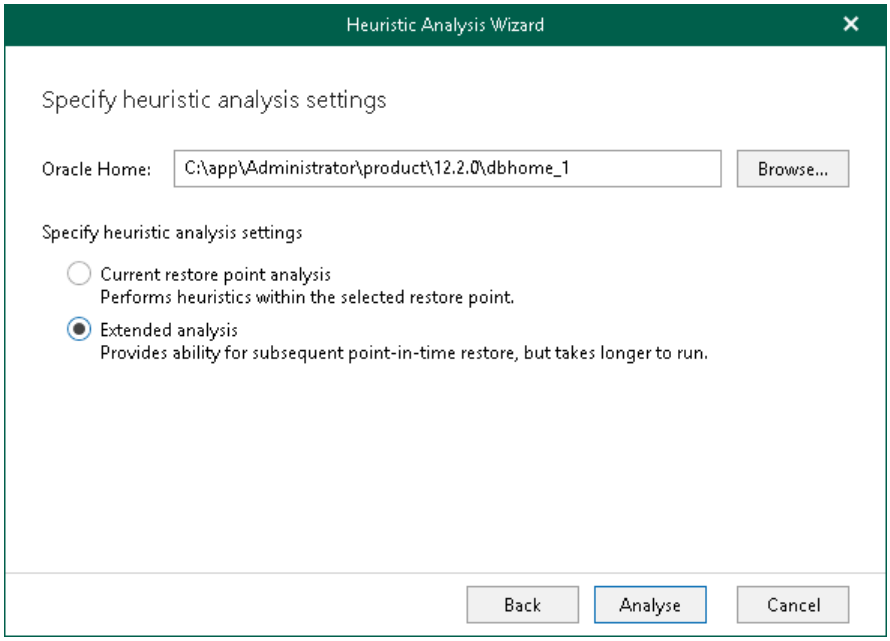
Step 3. Specify Heuristic Settings

At this step of the wizard, specify the following:

- **Oracle Home**. To attach a database, apply log files (if required) and make a consistency check of the database.
- **Heuristic analysis settings**:
  - **Current restore point analysis**. To search for available Oracle databases within the selected restore point only.
  - **Extended analysis**. To search for available Oracle databases within multiple restore points.

    Typically, Veeam Explorer for Oracle scans three restore points; the current restore point that you select when opening Veeam Explorer, and two other restore points that come before and after the current restore point.

Once analysis is complete, Veeam Explorer for Oracle will load available Oracle databases to the program scope automatically.

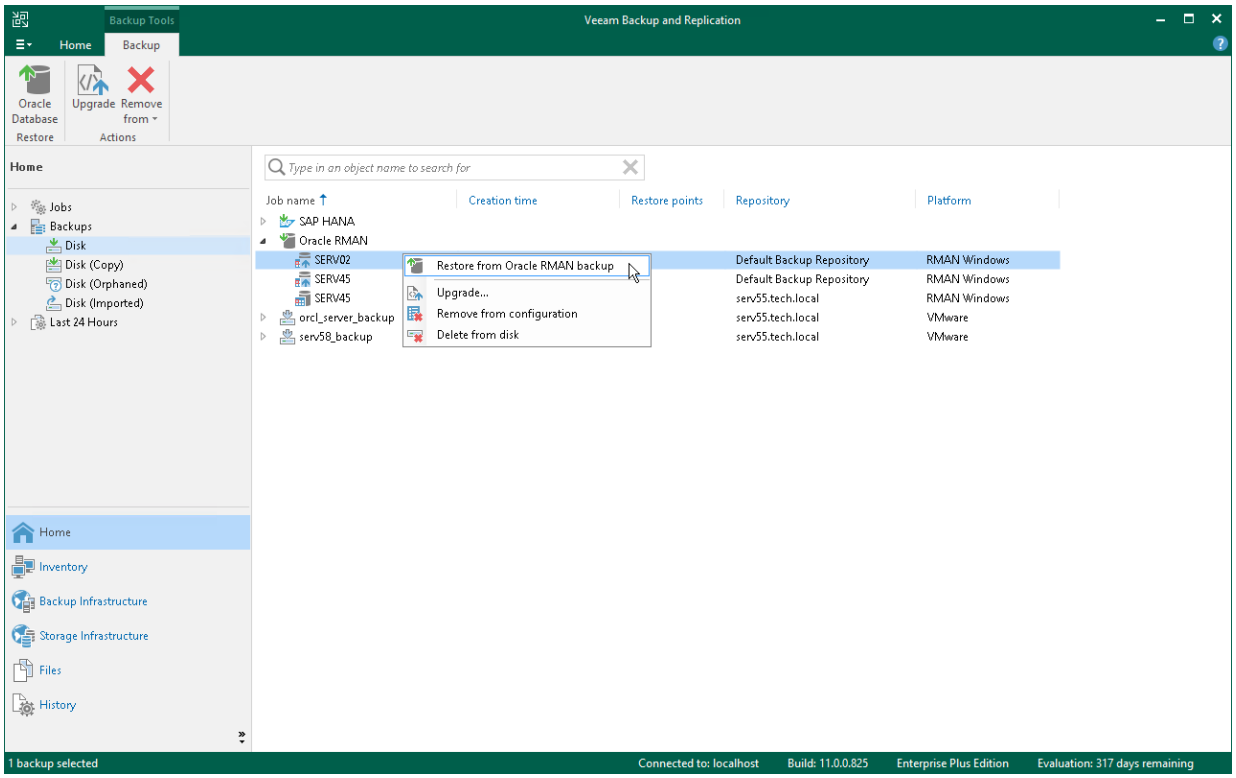


Exploring RMAN Backups

This section explains how to explore backups created with the Oracle RMAN Plug-in. For more information, see Veeam Plug-in for Oracle RMAN.

To load RMAN backups, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Go to the **Backups** > **Disk** node.
3. Right-click an RMAN backup and select **Restore from Oracle RMAN backup**.



Data Restore

Continue with this section to learn more about restoring Oracle databases and Data Guard.

Before restoring data, make sure to read Considerations and Limitations.

> **IMPORTANT**
>
> Make sure to install a bash shell on a target Oracle server to perform a restore.

Restoring Single Database and Data Guard

This section explains how to restore Oracle databases and Oracle Data Guard back to the production environment.

Consider that when restoring Data Guard to another server as described in this section, databases from Data Guard will be restored as standalone Oracle databases preserving no Data Guard infrastructure. To restore Data Guard infrastructure altogether, use either a latest state restore, or point-in-time restore. For more information, see Restoring Latest State and Restoring Point-in-Time State respectively.

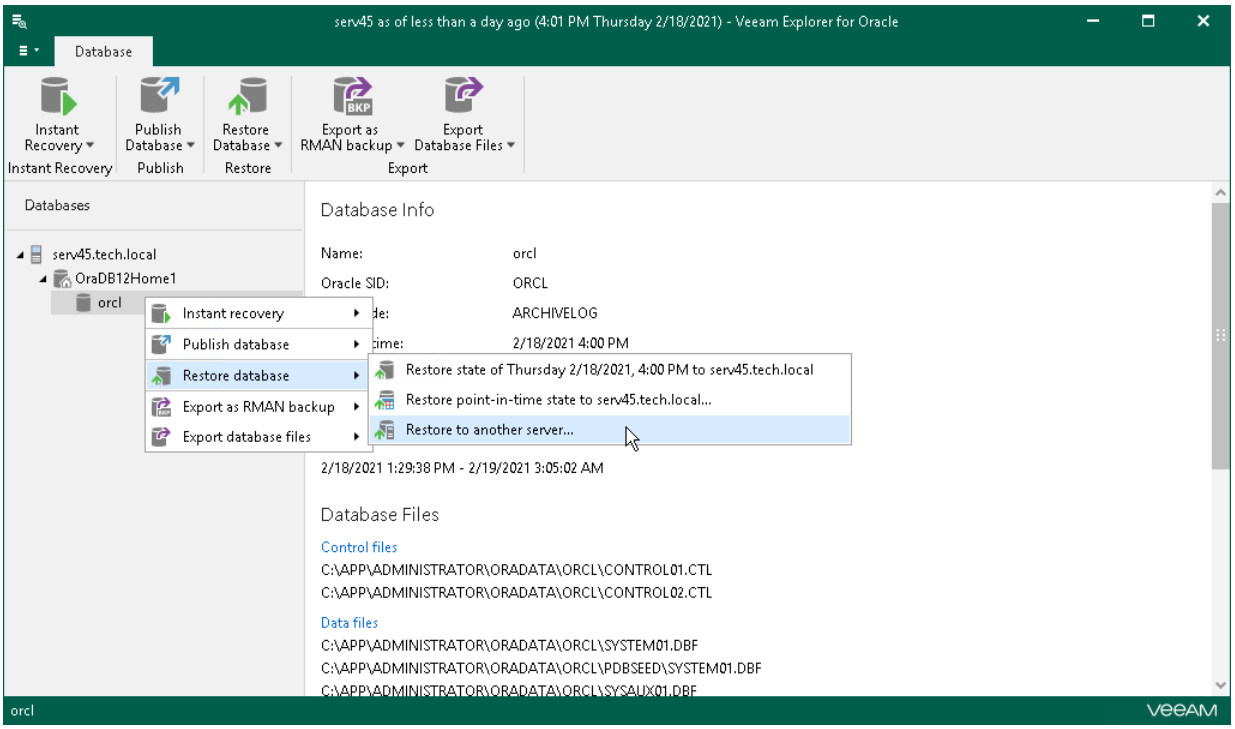
To restore data, do the following:

1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify Oracle settings.
6. Specify database files location.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation tree, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore to another server** or right-click a database or Data Guard and select **Restore database** > **Restore to another server**.



Step 2. Specify Restore Point

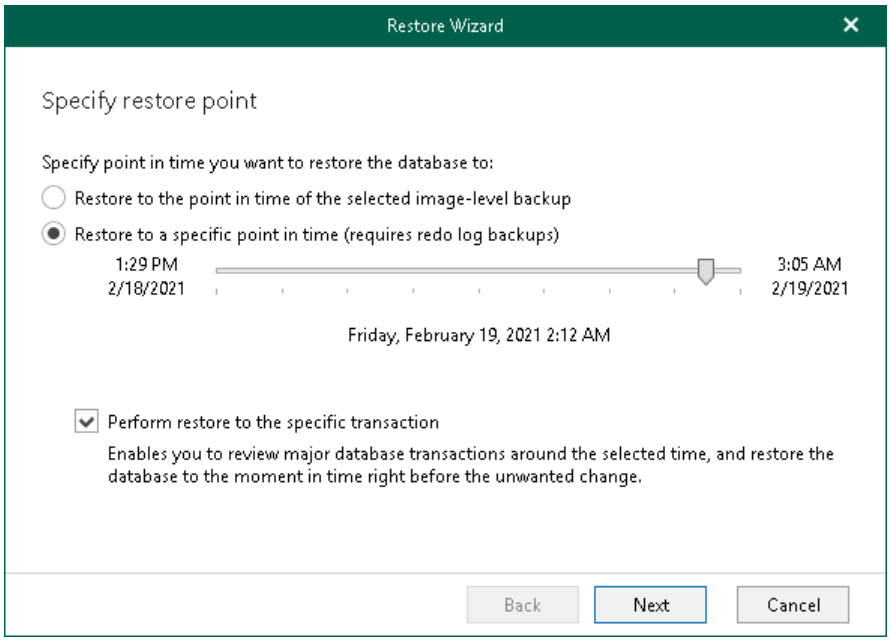
At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

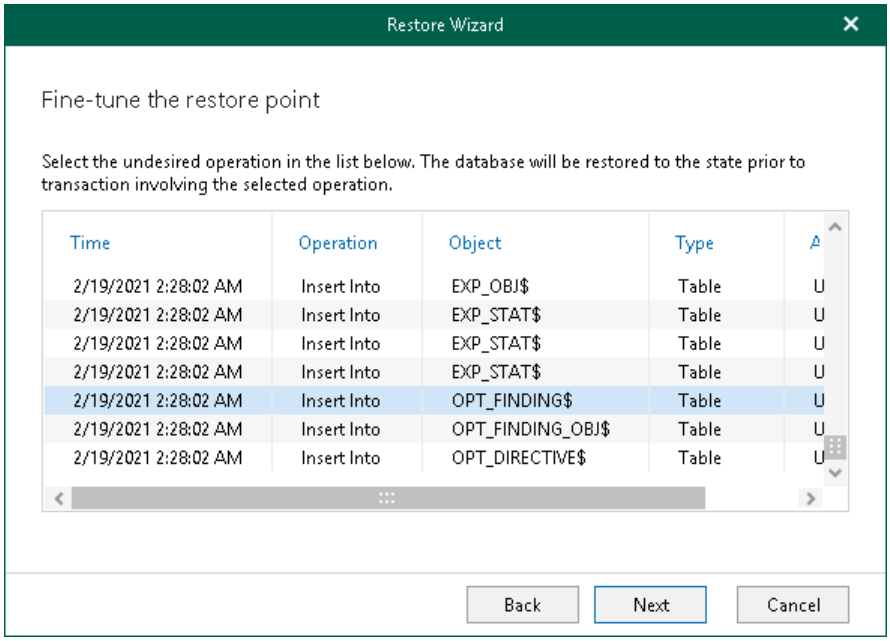
Consider the following:

- The **Restore to a specific point in time** option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
- The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore your database.



Step 4. Specify Target Server

At this step of the wizard, specify credentials to access the target Oracle server.

Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

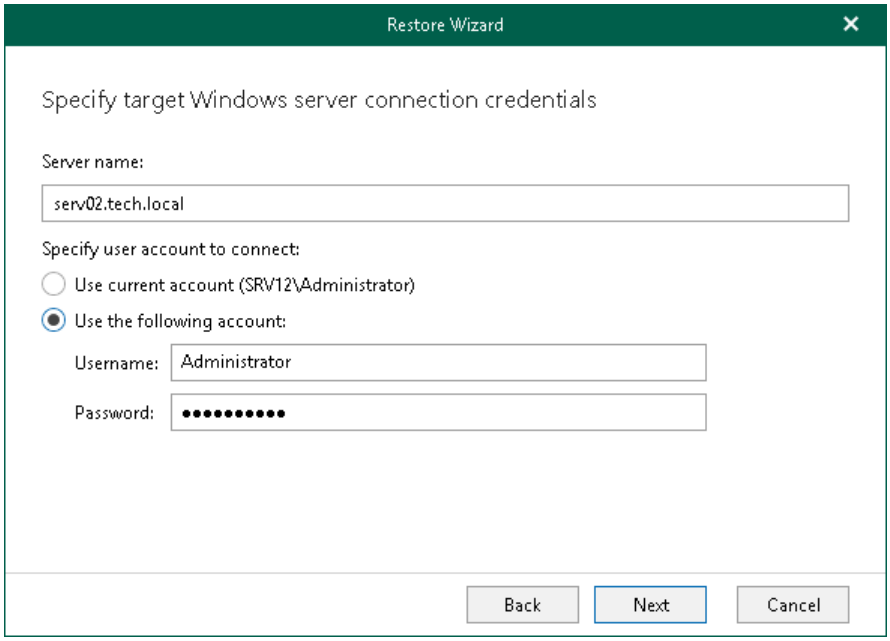
1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. Under the **Specify user account to connect to server** section, select either of the following options:
   - **Use current account**

     Select this option to connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**.

     Select this option to connect to the specified server using a custom user account.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



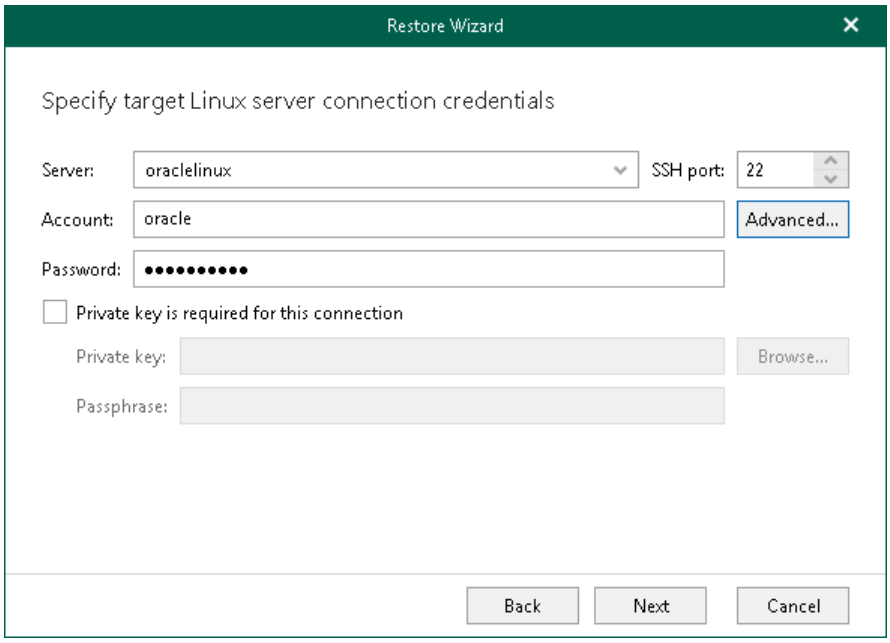
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

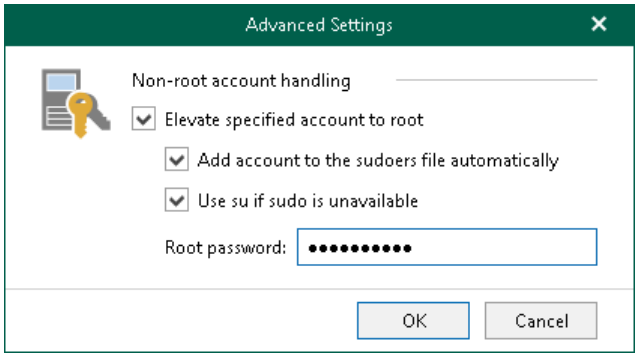
1. In the **Server** drop-down list, select an Oracle server to which you want to restore data.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



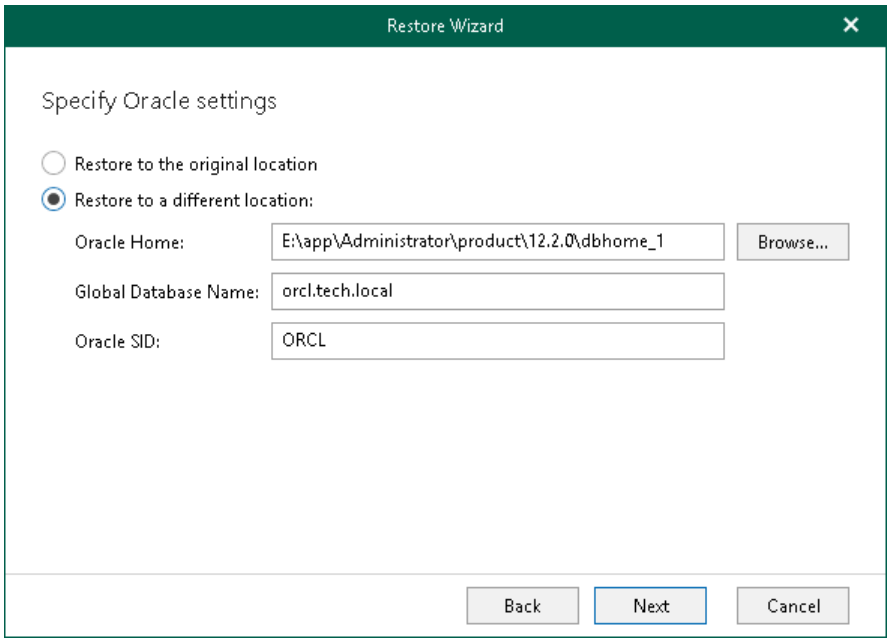
Use the native Veeam Explorer for Oracle abilities to elevate your account to *root* and add it to the *sudoers* file. To do this, click **Advanced** and select corresponding check boxes.



Step 5. Specify Oracle Settings

At this step of the wizard, select a location to which you want to restore databases:

- **Restore to the original location**. To restore a database back to the original location.
- **Restore to a different location**. To restore a database to the custom location, specify **Oracle Home**, **Global Database Name** and **Oracle SID**. To locate the Oracle home folder, click **Browse** and select a folder you want to use.



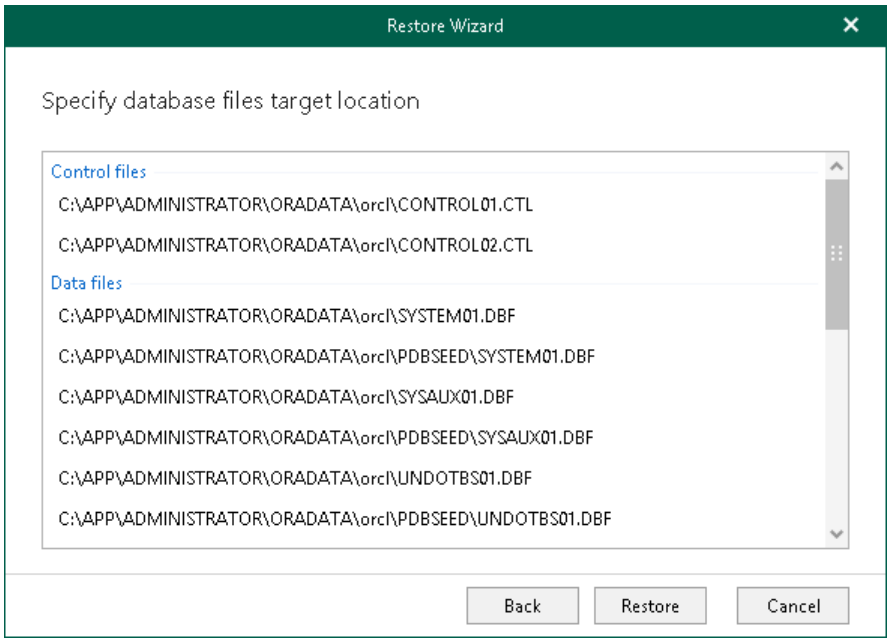
NOTE

If the account specified in step 4 is not the Oracle Home user, you will be asked to provide a password to access the target Oracle Home. Applicable to Oracle 12c and later versions.

Step 6. Specify Database Files Location

At this step of the wizard, specify the location for database files.

To edit the path, click the path row and provide the location you want to use.



Restoring Latest or Point-in-Time State

This section explains how to select a state as of which to restore Oracle databases or Data Guard, including a point-in-time restore — to revert the database to a state before an undesired transaction or before a point of failure.

The behavior in case of a latest or point-in-time state restore is as follows:

- Data Guard will be restored starting from the primary node. Once the primary node is restored, Veeam Explorer for Oracle will use it to restore standby nodes.
- Database files will be copied to the original location and then mounted to the original Oracle home.
- Databases from the backed up ASM group will be restored back to the original ASM group.
- All existing databases on the target Oracle server will be replaced with databases from the backup files.

Consider that restoring a latest or point-in-time state to the original Oracle server from storage snapshots is not supported. Use the **Restore to another server** command, as described in Restoring Database and Data Guard.

Restoring Point-in-Time State

To restore Oracle databases or Data Guard as of the selected point-in-time state, do the following:

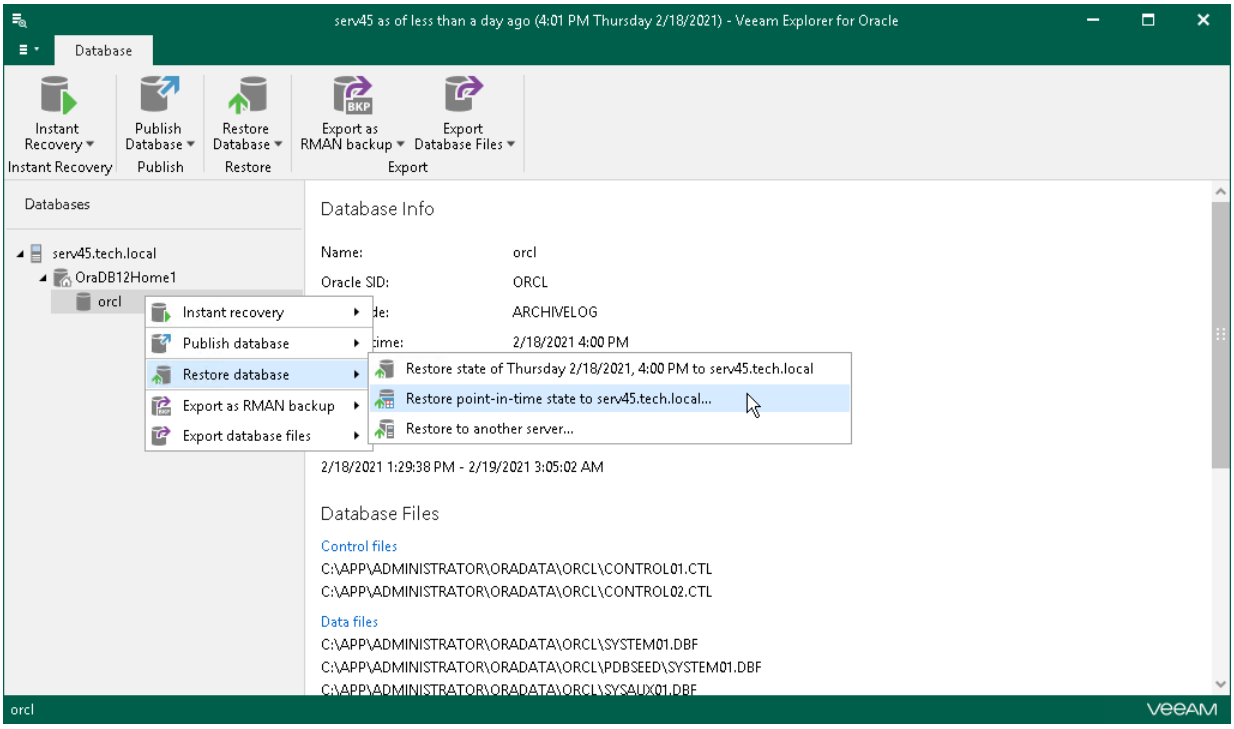
1. Launch Restore Wizard
2. Specify Restore Point
3. Fine-tune Restore Point

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore point-in-time state** or right-click a database or Data Guard and select **Restore database** > **Restore point-in-time state**.

> **IMPORTANT**
>
> A point in time restore is only possible if the *ARCHIVELOG* mode in enabled.



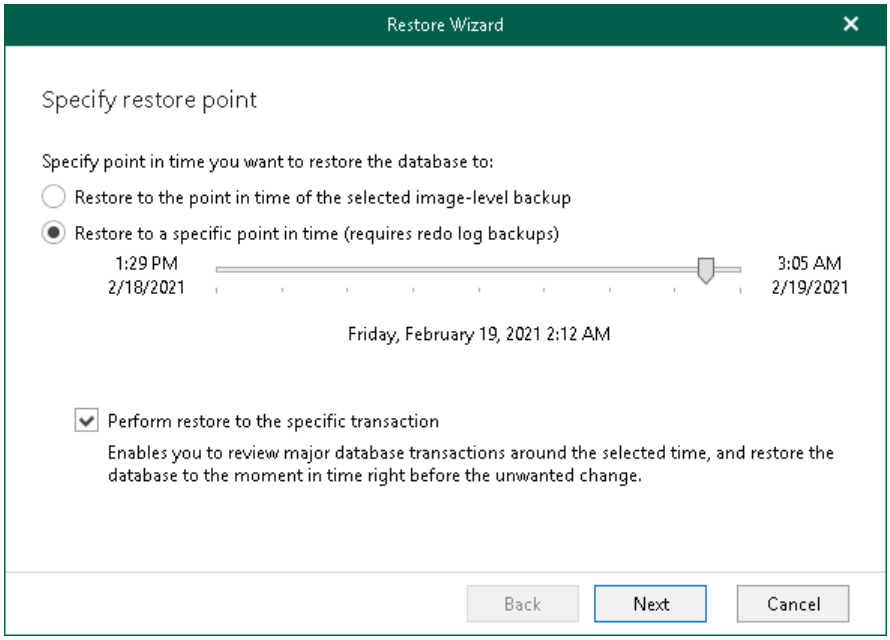
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain selected database files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

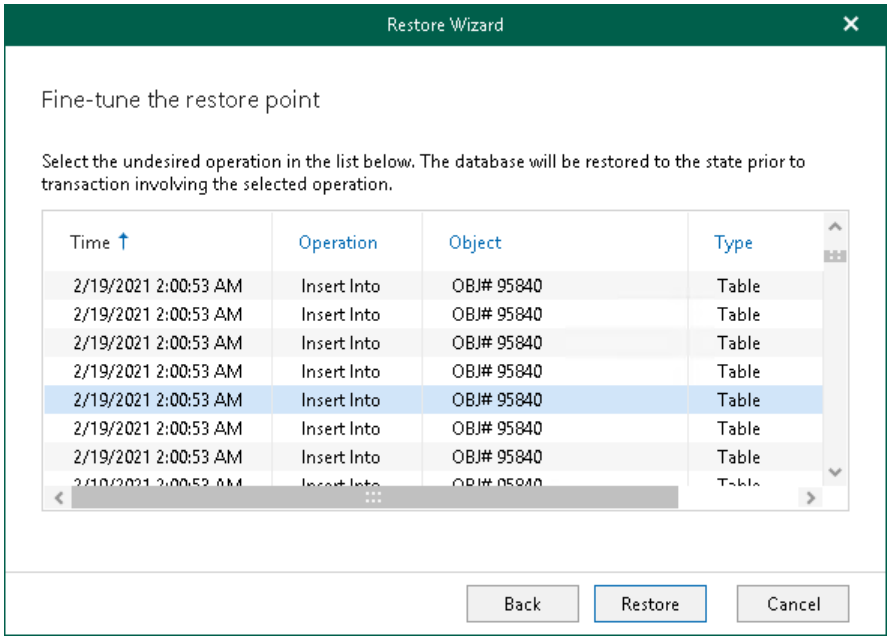
Consider the following:

- The **Restore to a specific point in time** option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
- The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

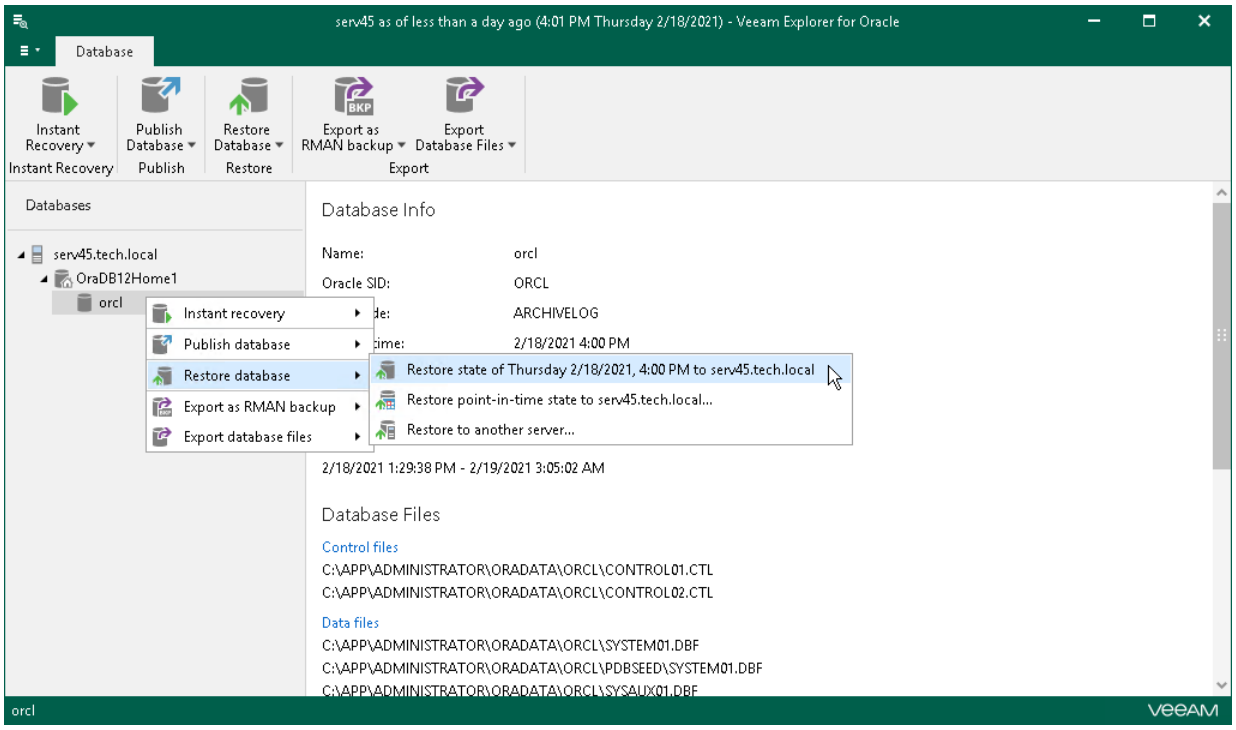
At this step of the wizard, select an operation prior to which you want to recover your database.



Restoring Latest State

To restore Oracle databases or Data Guard as of the latest available state, do the following:

1. In the navigation pane, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore state of <point_in_time> to <server_name>** or right-click a database and select **Restore database** > **Restore state of <point_in_time> to <server_name>**.



Restoring Multiple Databases

With Veeam Explorer for Oracle, you can restore multiple databases of the Oracle home or the server to the original server or to another server with different settings. For instructions, see:

- Restoring Databases to Another Server
- Restoring Databases to Latest or Point-in-Time State

Restoring Databases to Another Server

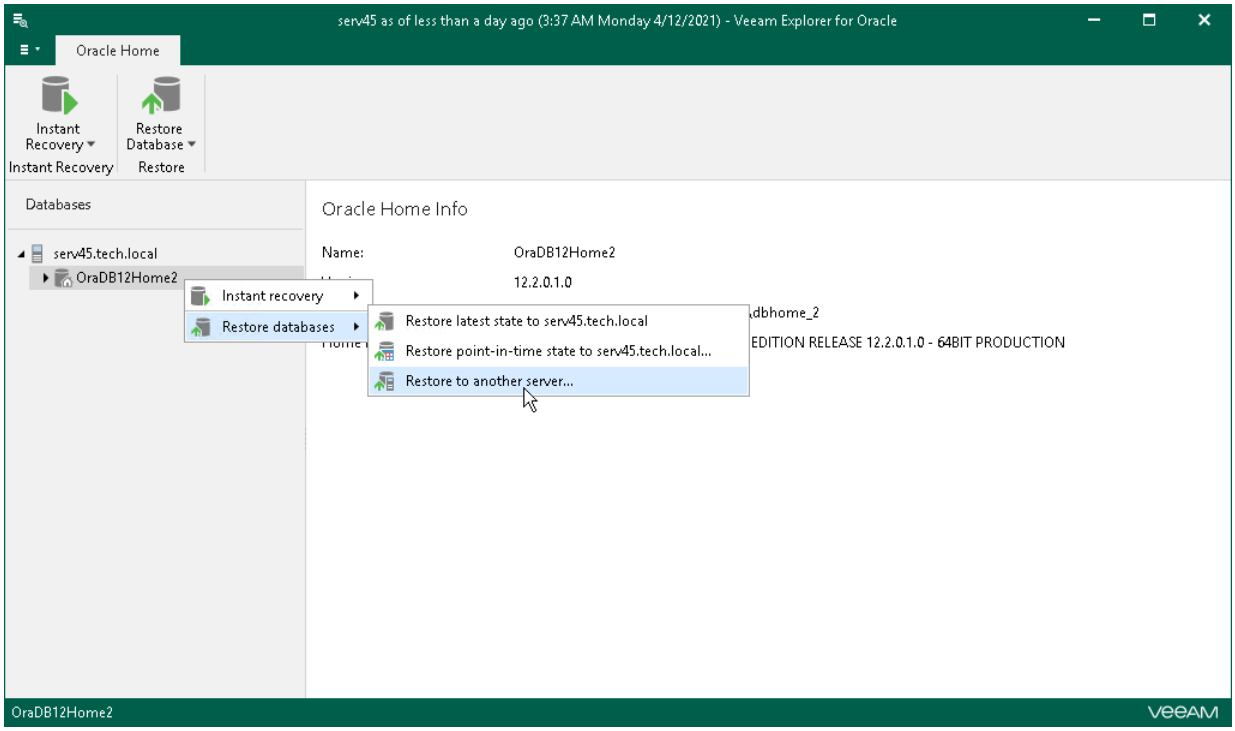
To restore multiple Oracle databases, do the following:

1. Launch the Restore wizard
2. Specify a restore point
3. Specify a target server
4. Specify Oracle settings

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation tree, select an Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Database** > **Restore to another server** or right-click a database or Data Guard and select **Restore database** > **Restore to another server**.

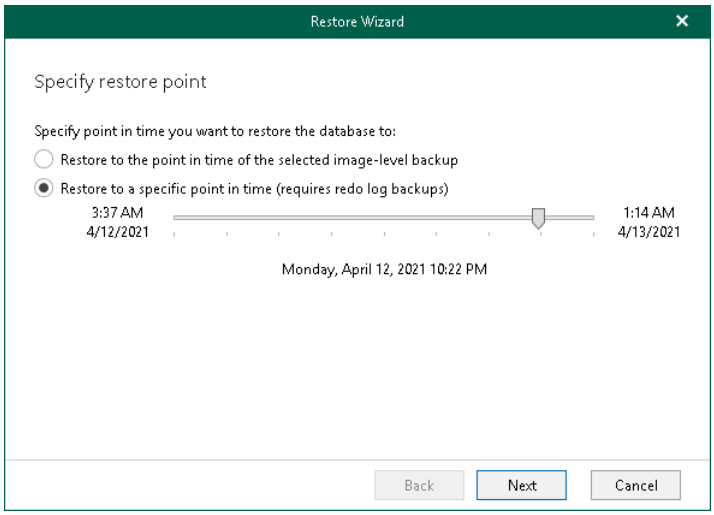


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore the databases:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a necessary point in time.



Step 3. Specify Target Server

At this step of the wizard, specify credentials to access the target Oracle server.

Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

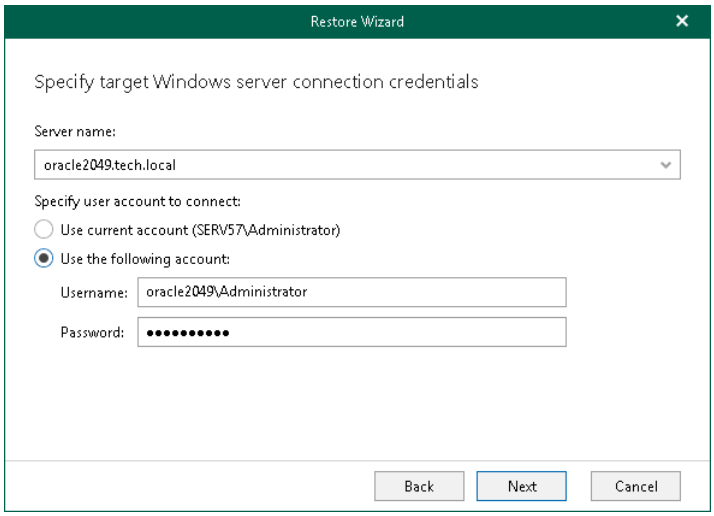
1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. Under the **Specify user account to connect to server** section, select either of the following options:
   - **Use current account**

     Select this option to connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**.

     Select this option to connect to the specified server using a custom user account.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



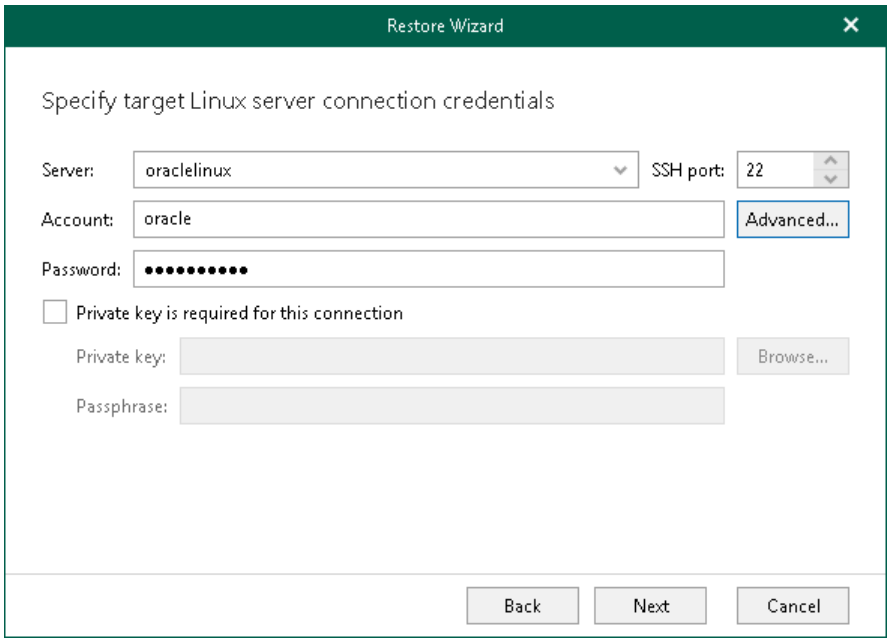
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

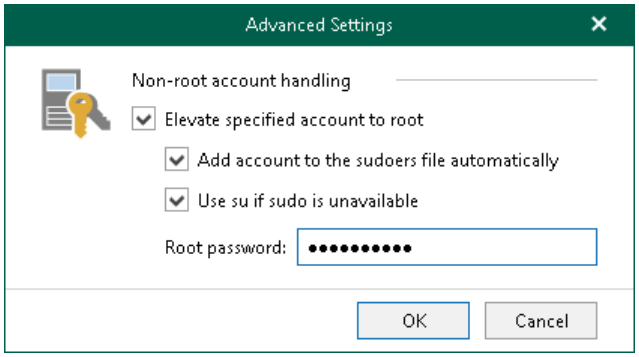
1. In the **Server** drop-down list, select an Oracle server to which you want to restore data.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



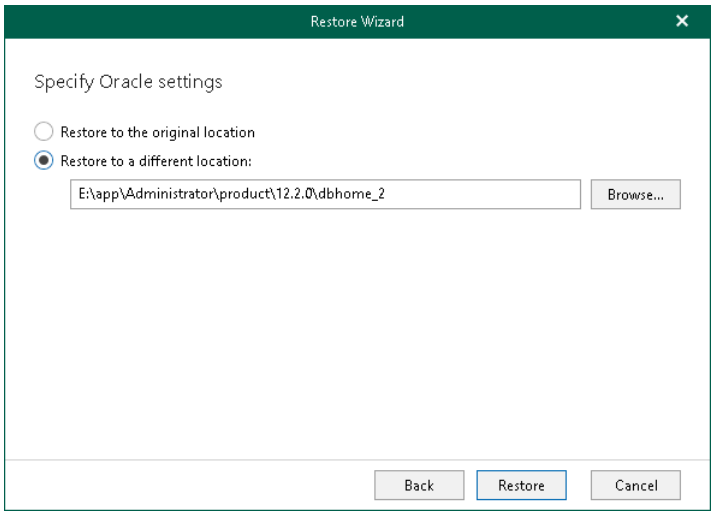
Use the native Veeam Explorer for Oracle abilities to elevate your account to *root* and add it to the *sudoers* file. To do this, click **Advanced** and select corresponding check boxes.



Step 4. Specify Oracle Settings

At this step of the wizard, select a location to which you want to restore databases and launch the restore.

1. At the **Specify Oracle settings** field, select one of the following:
   - **Restore to the original location:** Veeam Explorer checks if there are suitable Oracle home directories. If yes, the databases are restored to these home directories. If no, the databases will not be restored and Veeam Explorer will issue an error that suitable home directories has not been found.
   - **Restore to a different location**: Veeam Explorer restores all databases to the custom location. To specify the Oracle home directory, click **Browse** and select a folder that you want to use.
2. Click **Restore**.



NOTE

If the account specified in step 3 is not the Oracle Home user, you will be asked to provide a password to access the target Oracle Home. Applicable to Oracle 12c and later versions.

Restoring Databases to Latest or Point-in-Time State

With Veeam Explorer for Oracle, you can restore the latest or point-in-time state of multiple Oracle databases. In this scenario, all selected databases on the original Oracle server will be replaced with databases from the latest or earlier backup files.

Mind the following:

- Data Guard will be restored starting from the primary node. Once the primary node is restored, Veeam Explorer for Oracle will use it to restore standby nodes.
- Database files will be copied to the original location and then mounted to the original Oracle home.
- Databases from the backed up ASM group will be restored back to the original ASM group.

Consider that restoring a latest or point-in-time state to the original Oracle server from storage snapshots is not supported. Use the **Restore to another server** command, as described in Restoring Databases to Another Server.

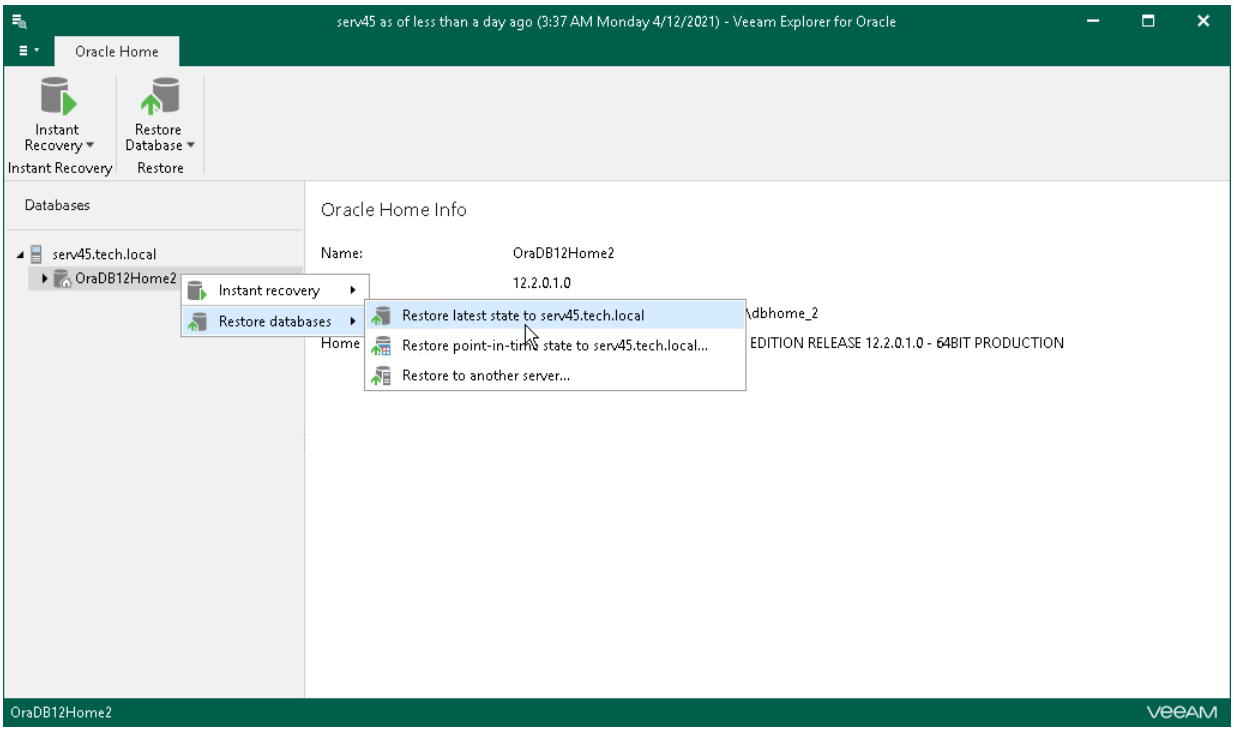
For instructions, see:

- Restoring Databases to Latest State
- Restoring Databases to Point-in-Time State

Restoring Databases to Latest State

To restore multiple databases to the latest state to the original server, do the following:

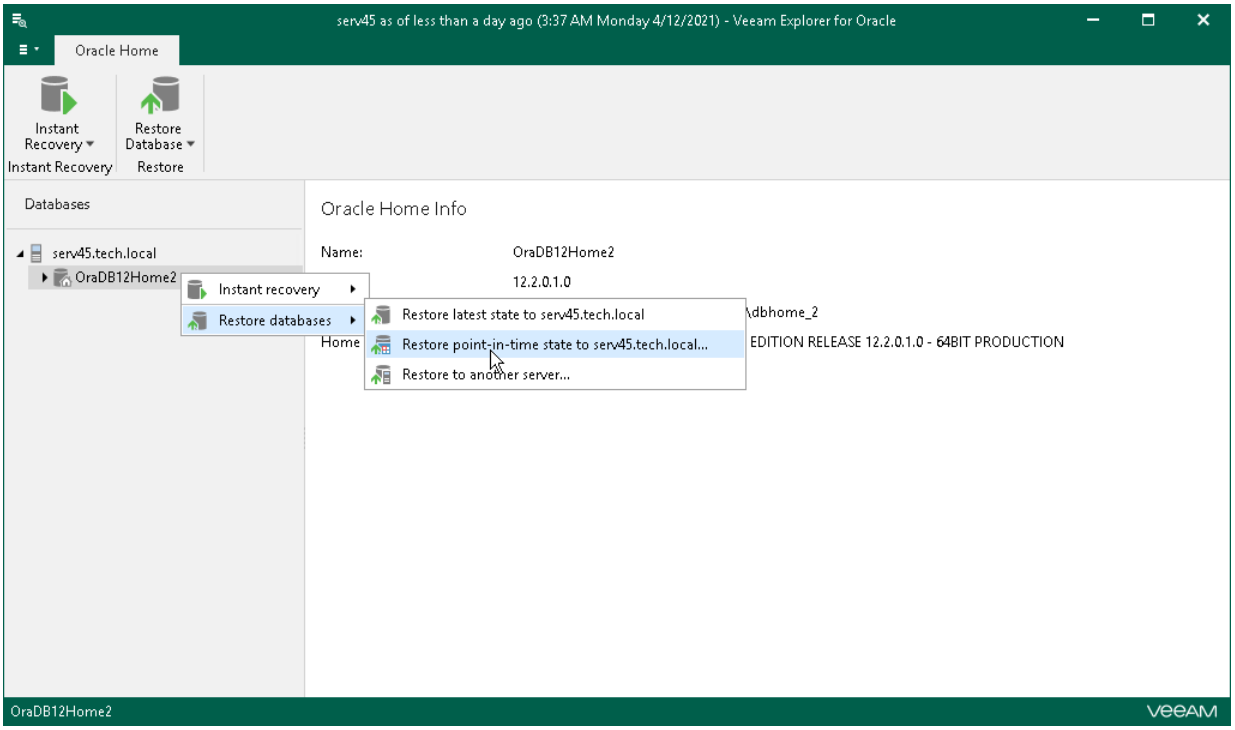
1. In the navigation pane, select an Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Database** > **Restore latest state** or right-click a database and select **Restore databases** > **Restore latest state**.



Restoring Databases to Point-in-Time State

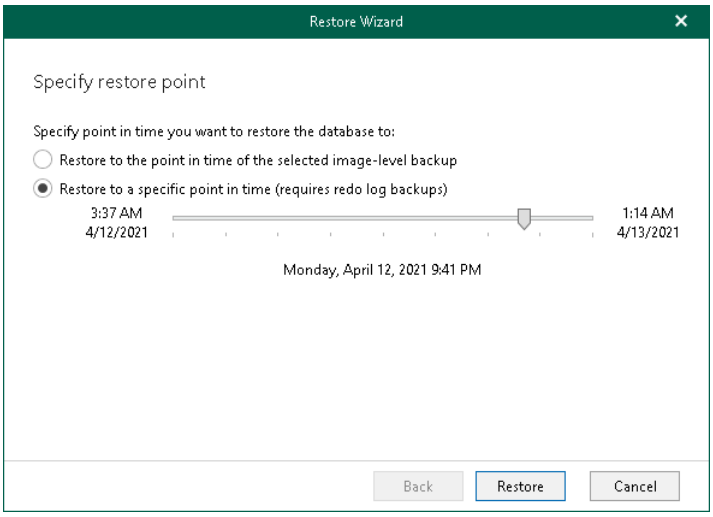
To restore multiple databases to a point-in-time state to original server, do the following:

1. In the navigation pane, select an Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Database** > **Restore state of <point_in_time>** or right-click a database and select **Restore databases** > **Restore point-in-time state**.



3. At this step of the **Restore** wizard, select a state as of which you want to restore the databases:
   - Select the **Restore to the point in time** of the selected image-level backup option to load database files as per date when the current restore point was created.
   - Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

     Use the slider to choose a necessary point in time.



Restoring RMAN Backups

This section explains how to restore backups created with Veeam Plug-in for Oracle RMAN. For more information, see the Veeam Plug-in for Oracle RMAN section of the Veeam Plug-ins for Enterprise Applications User Guide.

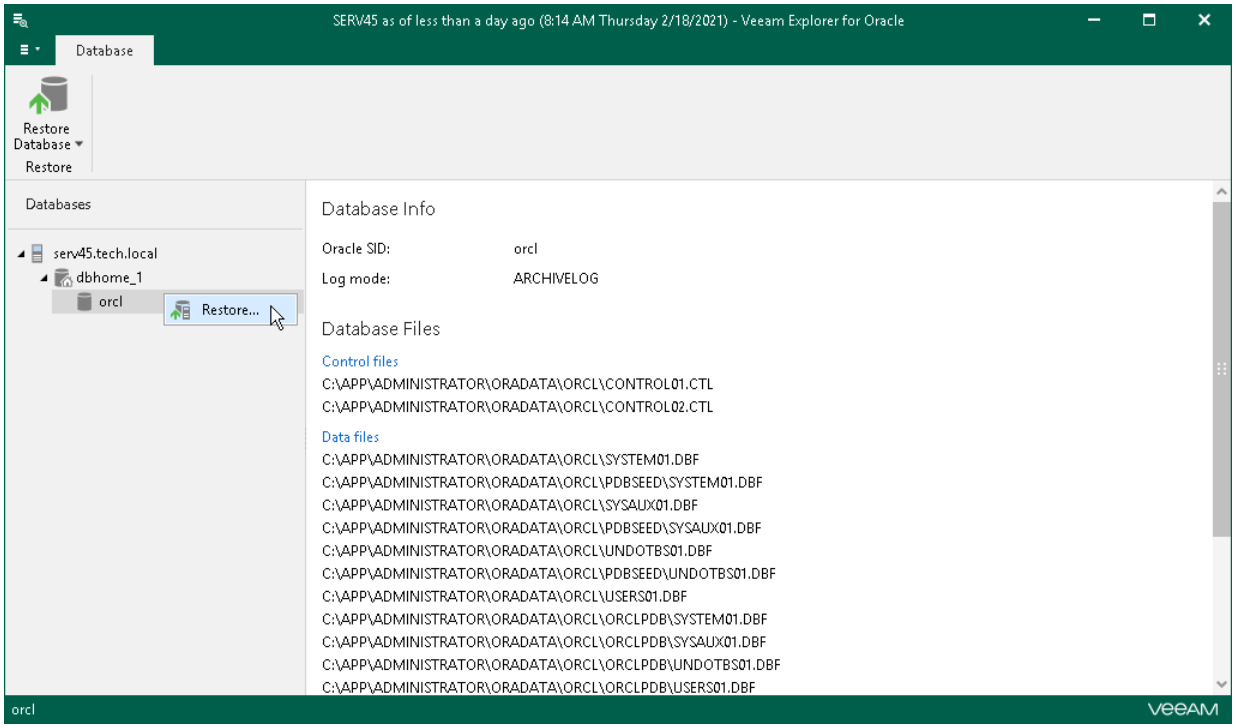
To restore RMAN backups, do the following:

1. Launch the Restore wizard.
2. Specify the recovery type.
3. Specify the target server.
4. Specify Oracle settings.
5. Specify home user password.
6. Specify point in time.
7. Specify database files location.
8. Configure channel allocation.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. Open an RMAN backup, as described in Exploring RMAN Backups.
2. In the navigation pane, select a database.
3. On the **Database** tab, select **Restore Database** > **Restore** or right-click a database and select **Restore**.



Step 2. Specify Recovery Type

At this step of the wizard, select a recovery type:

- **Recover database to specific point in time**

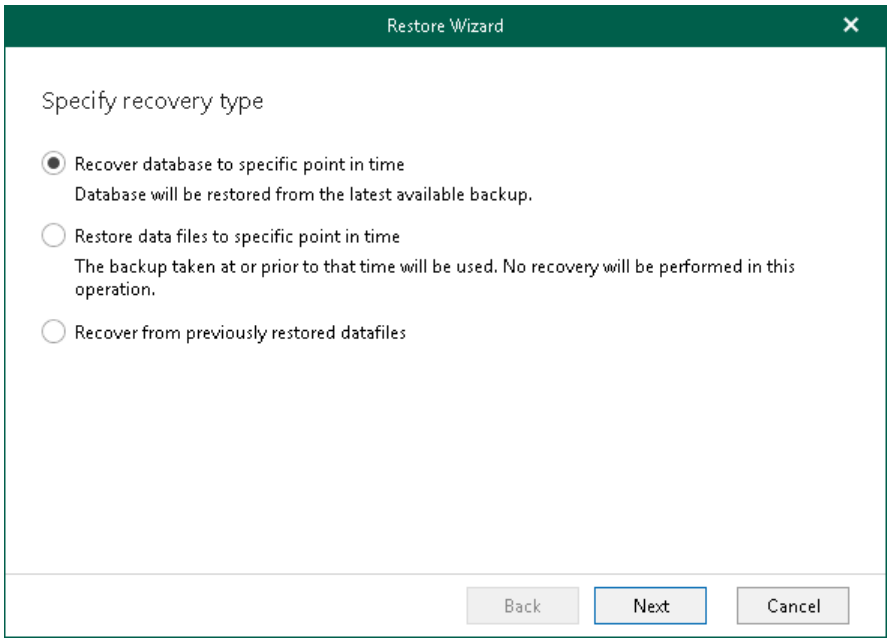
  Select this option to restore databases as of the latest available state.

- **Restore data files to specific point in time**

  Select this option to restore only datafiles as of the specific point-in-time state without applying log files.

- **Recover from previously restored datafiles**

  Select this option to apply log files to restored datafiles.



Step 3. Specify Target Server

At this step of the wizard, specify credentials to access the target Oracle server.

Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

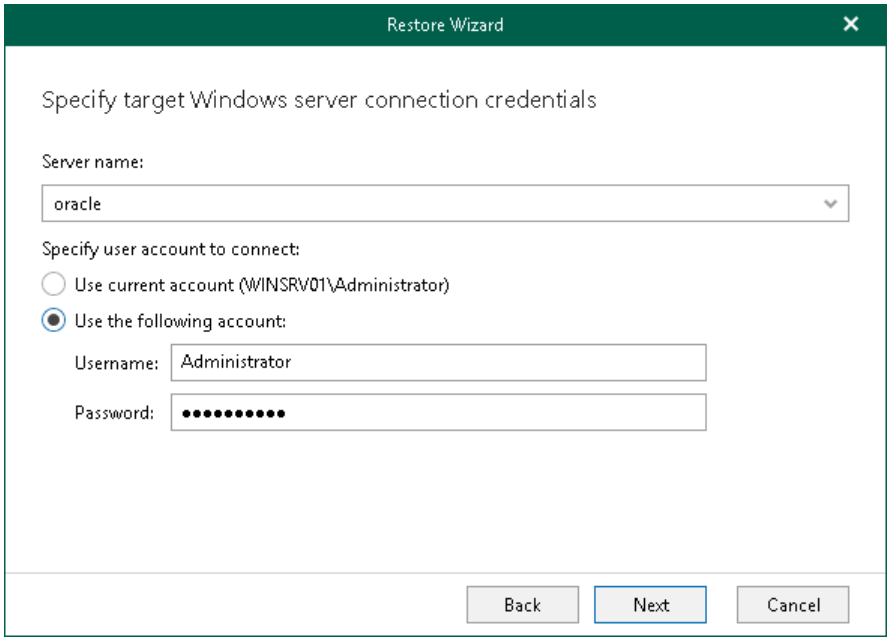
1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. Under the **Specify user account to connect to server** section, select either of the following options:
   - **Use current account**

     Select this option to connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**.

     Select this option to connect to the specified server using a custom user account.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.



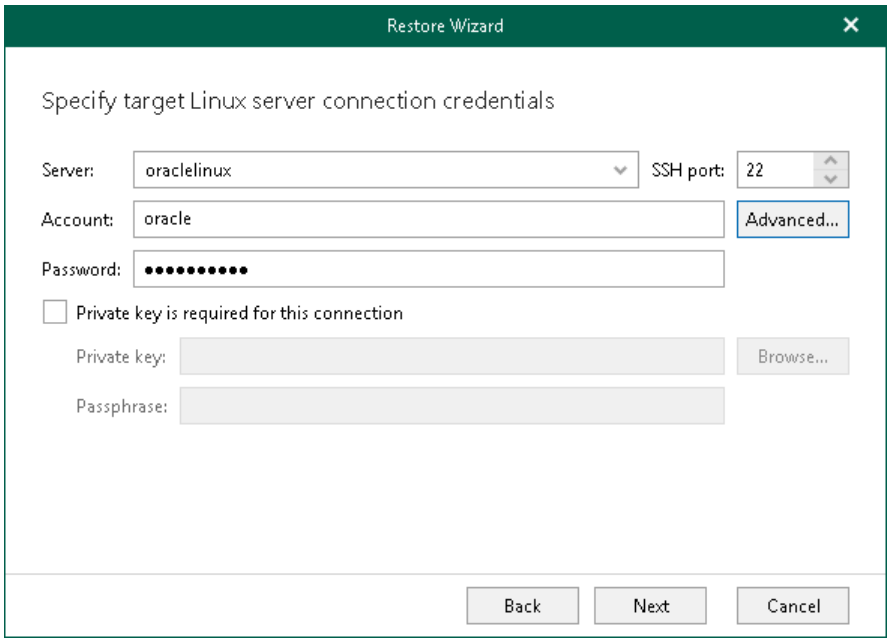
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

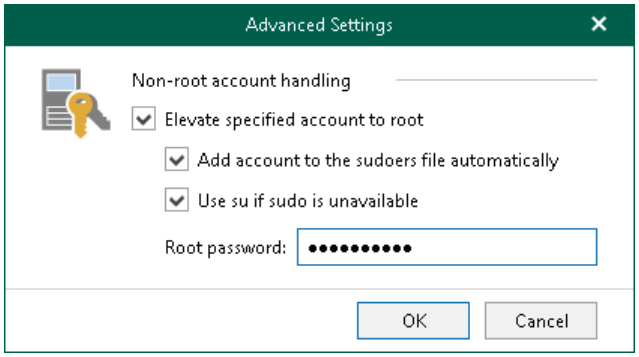
1. In the **Server** drop-down list, select an Oracle server to which you want to restore data.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



You can use the native Veeam Explorer abilities to elevate your account to **root** and add it to the **sudoers** file. To do this, click **Advanced** and select corresponding check boxes.



Step 4. Specify Oracle Settings

At this step of the wizard, select either of the following options:

- **Restore with the original name and settings**

  Select this option to restore data using the original name and settings.

- **Restore with different name and settings**

  Select this option to choose custom settings:

  - In the **Oracle Home** field, specify Oracle Home.

    You can click **Browse** to select a folder.

  - In the **Global Database Name** field, specify the name under which to restore a database.

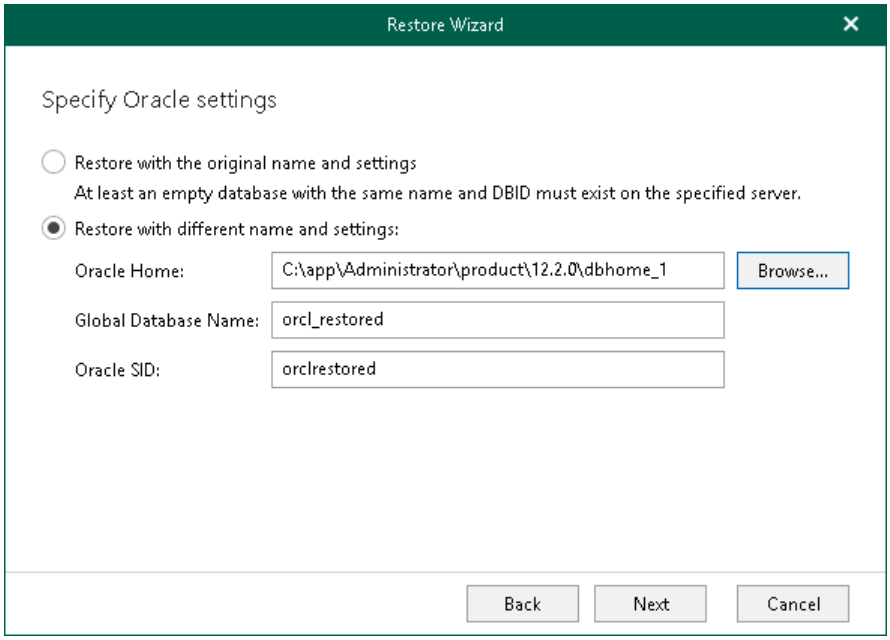
    This field is available only if you have selected the **Recover database to specific point in time** option in the Specify Recovery Type step.

  - In the **Oracle SID** field, specify a SID.

NOTE

Consider the following:

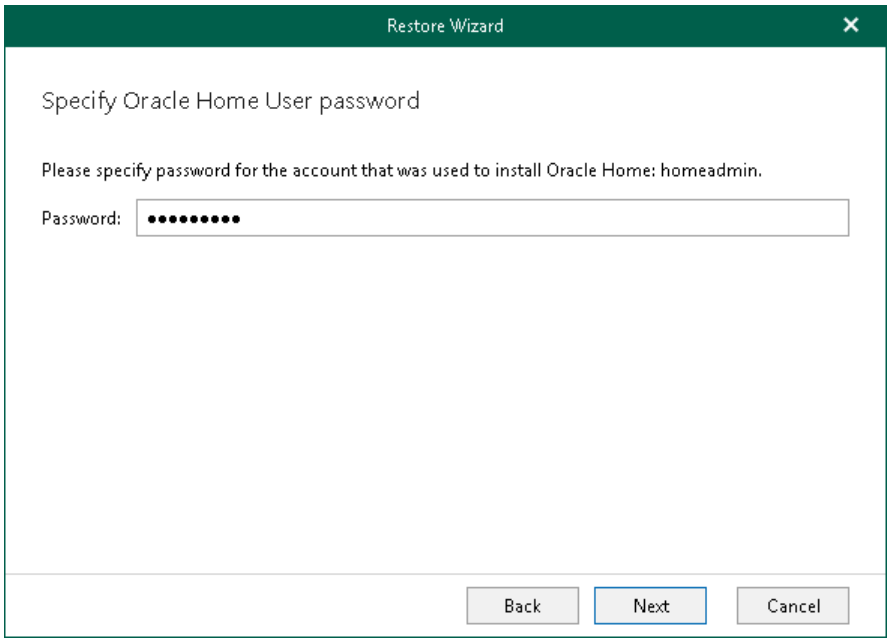
- To use the **Restore with different name and settings** option, make sure that *Controlfile Autobackup* is enabled. For more information, see the Oracle Environment Planning section of the Veeam Plug-in for Oracle RMAN User Guide.
- An existing Oracle SID (if any) will be replaced with that from the backup when selecting the **Restore with different name and settings** option.



Step 5. Specify Home User Password

This step of the wizard is available if the account specified in step 3 is not the Oracle Home user.

At this step of the wizard, specify the password for the *Oracle Home* user.



Step 6. Specify Point in Time

At this step of the wizard, do the following:

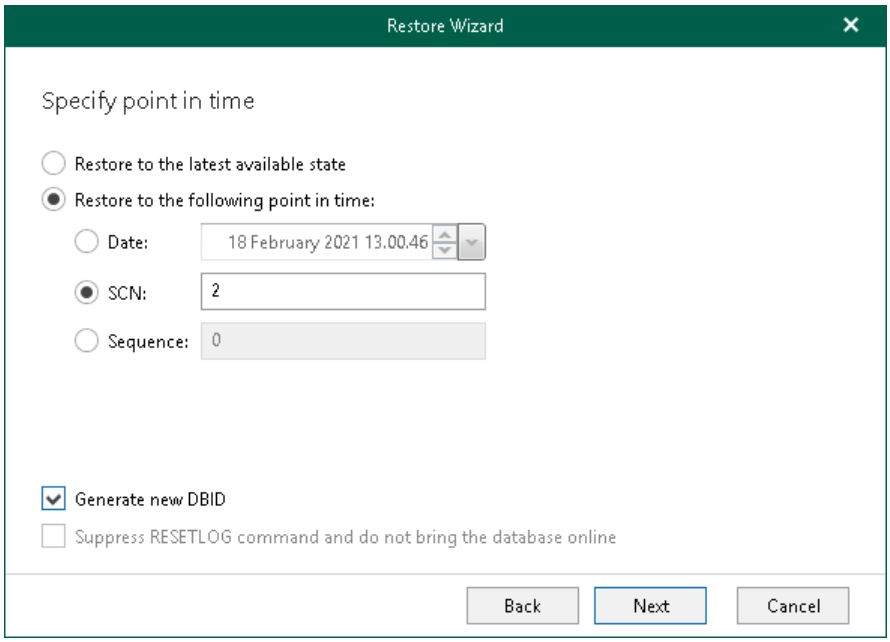
- Select the **Recover to the latest available** option to restore data as of the latest available state.
- Select the **Recover to the following point in time** option to select a state as of which you want to restore data:
  - **Date**. Select a date as of which you want to restore data.
  - **SCN**. Specify SCN (System Change Number).
  - **Sequence**. Specify the sequence.
- Select the **Generate new DBID** check box to generate a new DBID in addition to the new database name.

  This check box is available only when using the **Restore with different name and settings** option at the Specify Oracle Settings step.
- Select the **Suppress RESETLOG command and do not bring the database online** check box to skip the OPEN RESETLOGS operation if it was required by the database. The database in this case remains in the *mount* state.

  This check box is available only when using the **Restore with the original name and settings** option at the Specify Oracle Settings step.

TIP

For more information, see Oracle documentation.



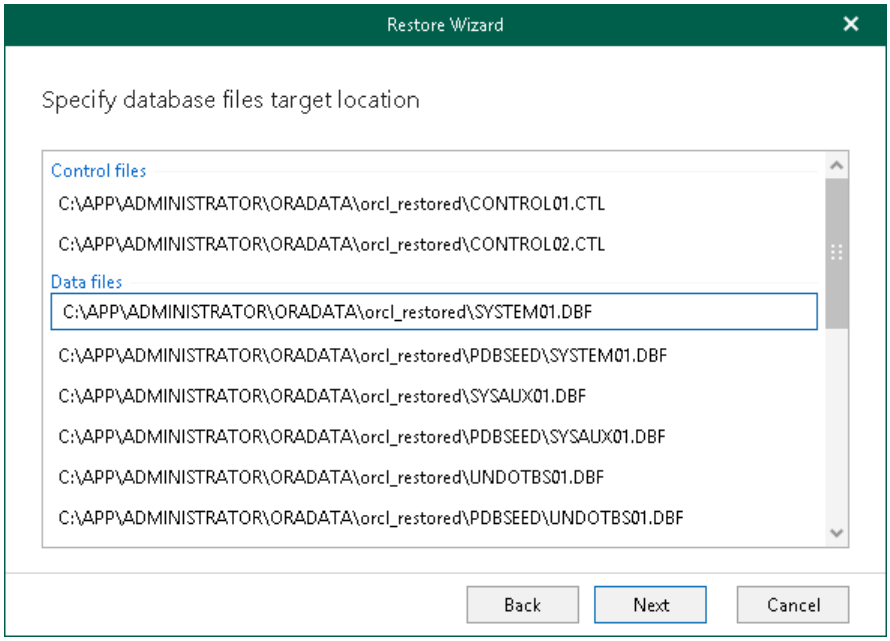
Step 7. Specify Database Files Location

At this step of the wizard, specify the location to which you want to restore data files.

Consider the following:

- When restoring with the **Restore with the original name and settings** option, only the location for *Data files* will be available for editing.
- When restoring with the **Restore with different name and settings** option, the location for the following files will be available for editing:
  - *Control files*
  - *Data files*
  - *Log files*
  - *Temp files*

To change the location, click the path row and specify the path.



Step 8. Configure Channel Allocation

At this step of the wizard, specify channels allocation.

Channels are used to restore data in multiple threads per session. Using multiple threads allows Veeam Explorer for Oracle to reduce the amount of time needed to complete restore sessions. For more information about allocating channels, see Oracle documentation.

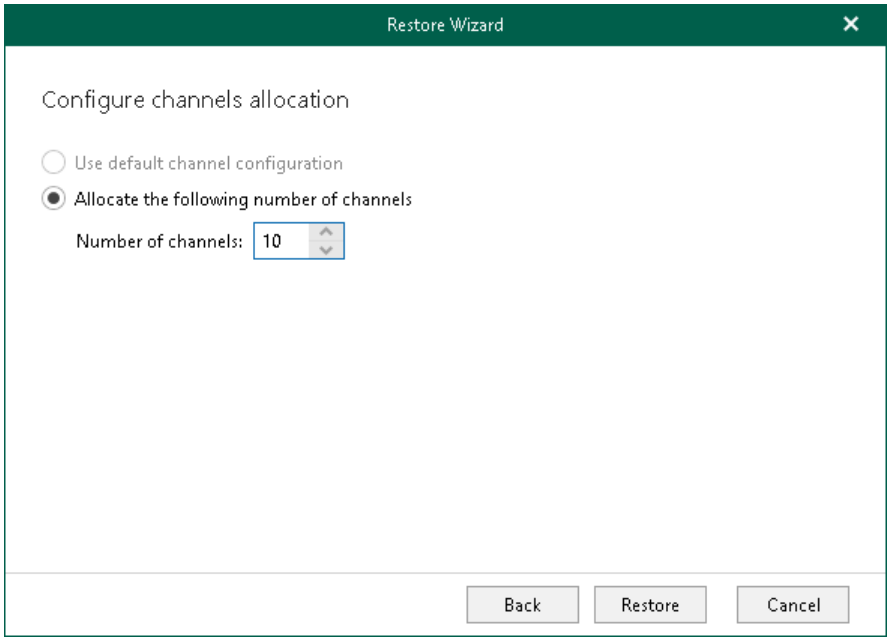
The following options are available:

- **Use default channel configuration**

  Select this option to use the default channel configuration defined in the RMAN plug-in settings.

- **Allocate the following number of channels**

  Select this option to specify the number of channels to be used when restoring your data.



Data Publishing

Publishing databases allows you to temporarily attach large Oracle databases to the target Oracle server without having to restore them.

Publishing databases typically occurs faster than using standard restore features and might be convenient in certain cases, for example, when your time to perform disaster-recovery operations is limited.

During publishing, Veeam Explorer for Oracle does the following:

1. Mounts VM disks from the backup file to the target Oracle server.

   Mounting is done to the *C:\VeeamFLR* directory for Windows-based servers and the */tmp* directory for Linux-based servers.

2. Retrieves required database files.

3. Attaches associated databases directly to the target Oracle server so that you can perform required operations using Oracle tools.

Before restoring data, make sure to read Considerations and Limitations.

Publishing to Specified Server

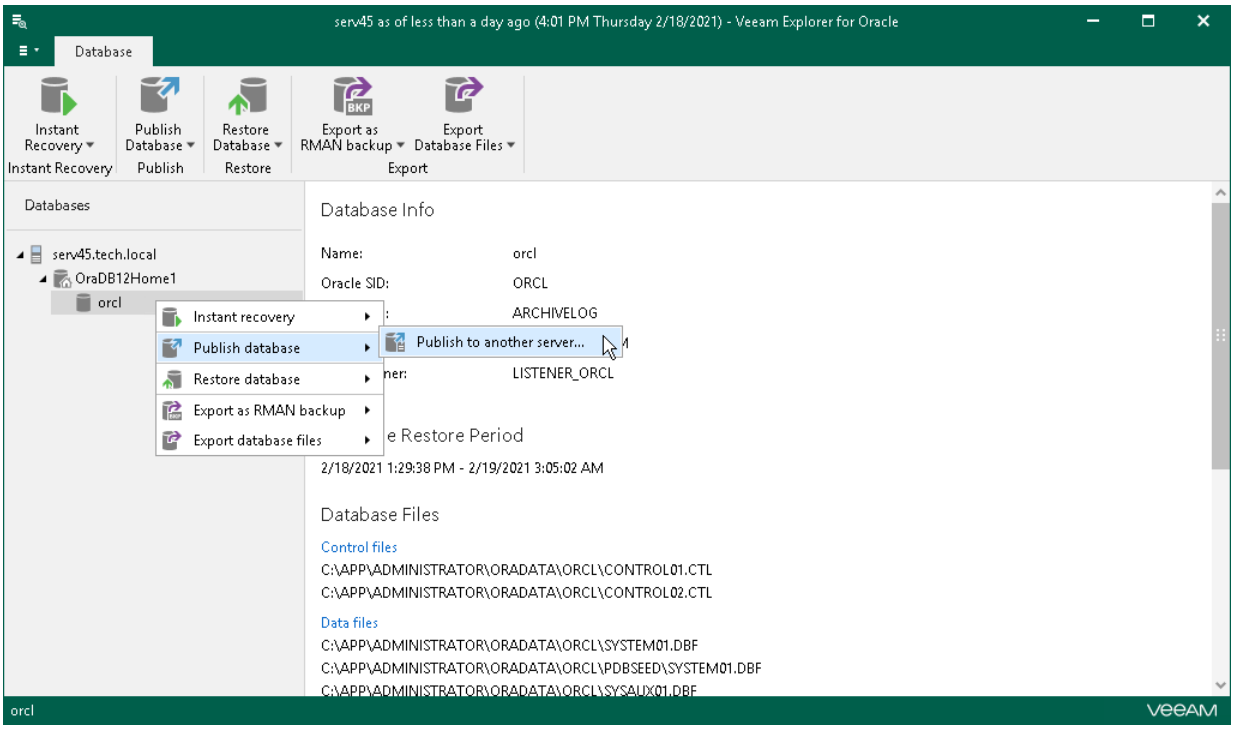
To publish a database to the specified Oracle server, do the following:

1. Launch the Publish wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target Oracle server.
5. Specify Oracle settings.

Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish to another server** or right-click a database and select **Publish database** > **Publish to another server**.



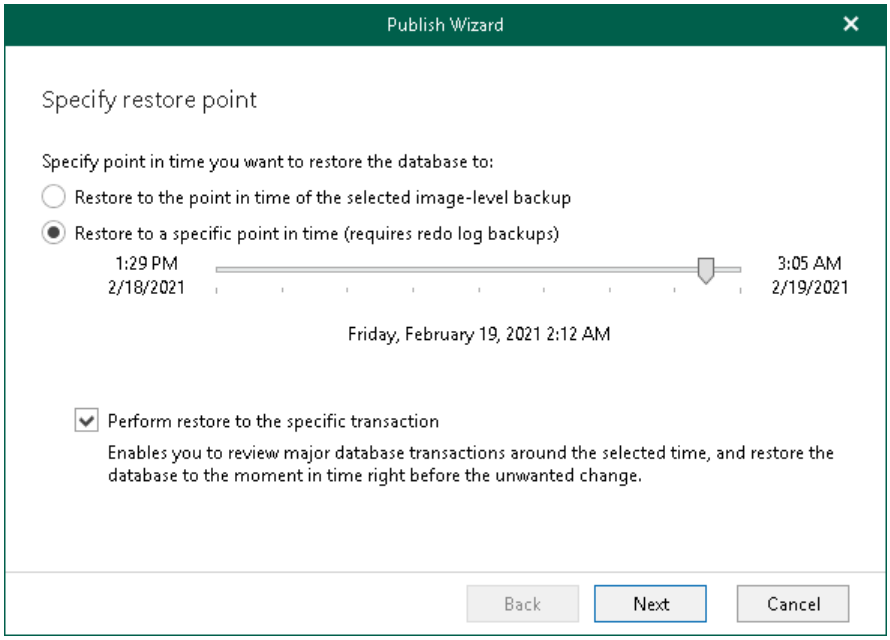
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

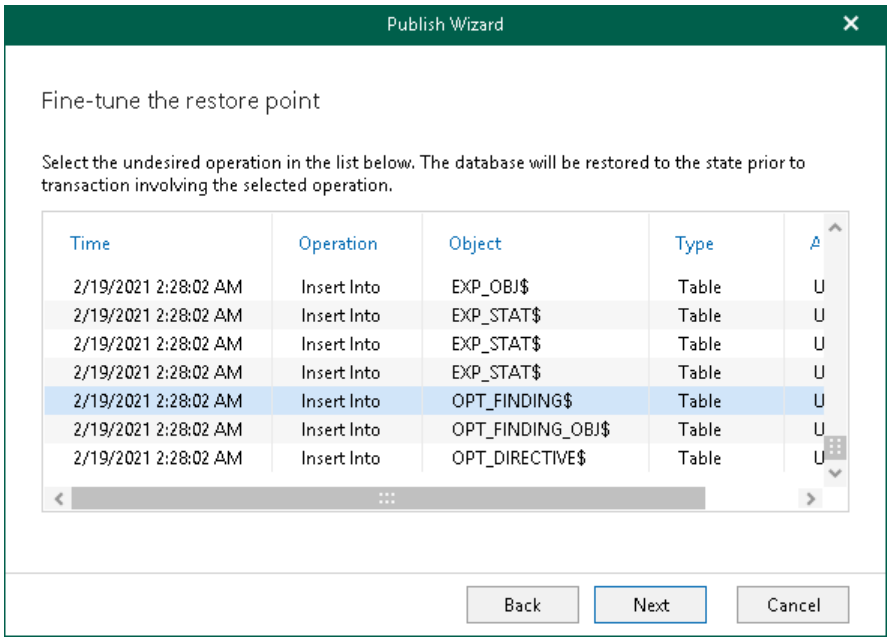
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target Oracle Server

At this step of the wizard. specify credentials to access the target Oracle server.

Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

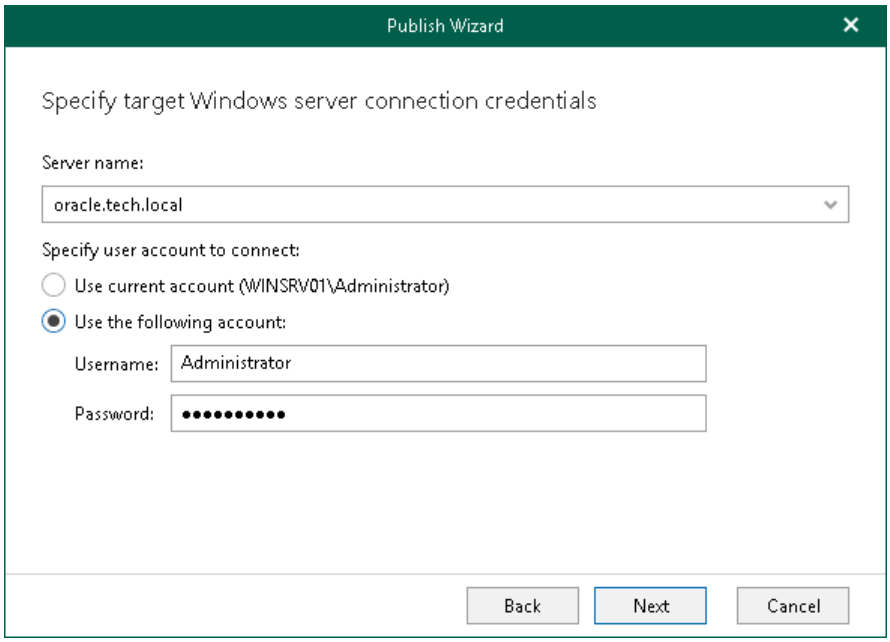
1. In the **Server name** drop-down list, specify the name of the Oracle server to which you want to restore data.
2. In the **Specify user account to connect** section, select either of the following options:
   - **Use current account**

     Select this option to connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**.

     Select this option to connect to the specified server using a custom user account.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account has been granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



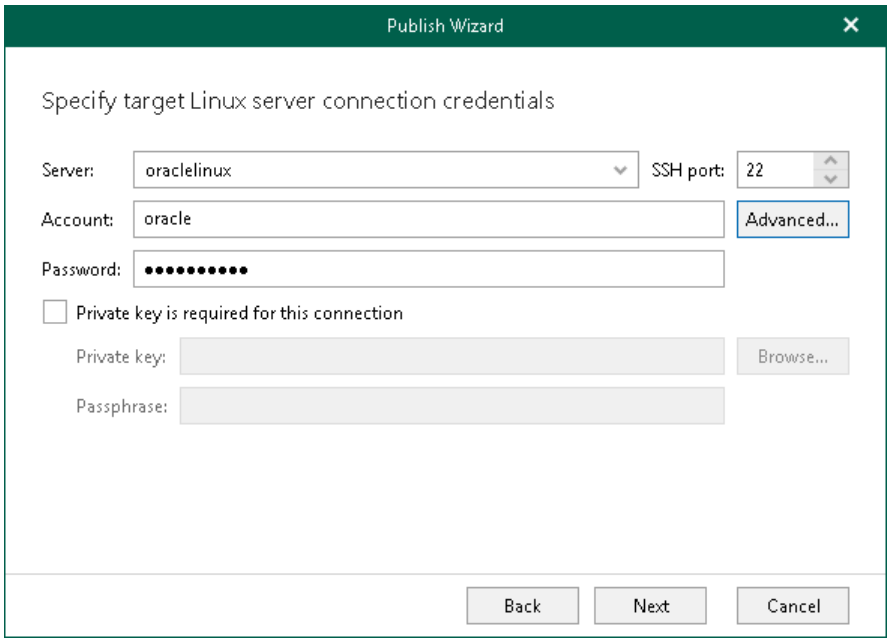
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

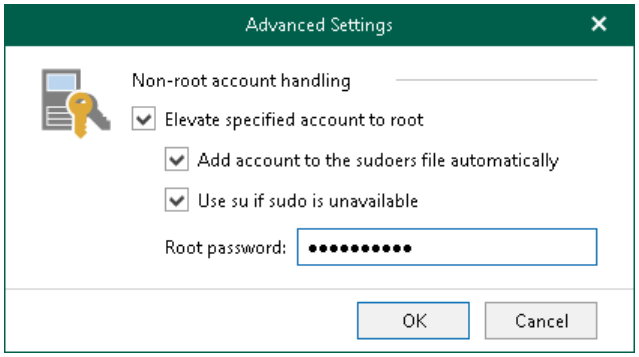
1. In the **Server** drop-down list, select an Oracle server to which you want to restore data.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



Use the native Veeam Explorer for Oracle abilities to elevate your account to **root** and add it to the **sudoers** file. To do this, click **Advanced** and select corresponding check boxes.



Step 5. Specify Oracle Settings

At this step of the wizard, select either of the following options:

- **Restore to the original location**. To publish a database to the original location.
- **Restore to a different location**. To select a custom location for database publishing.

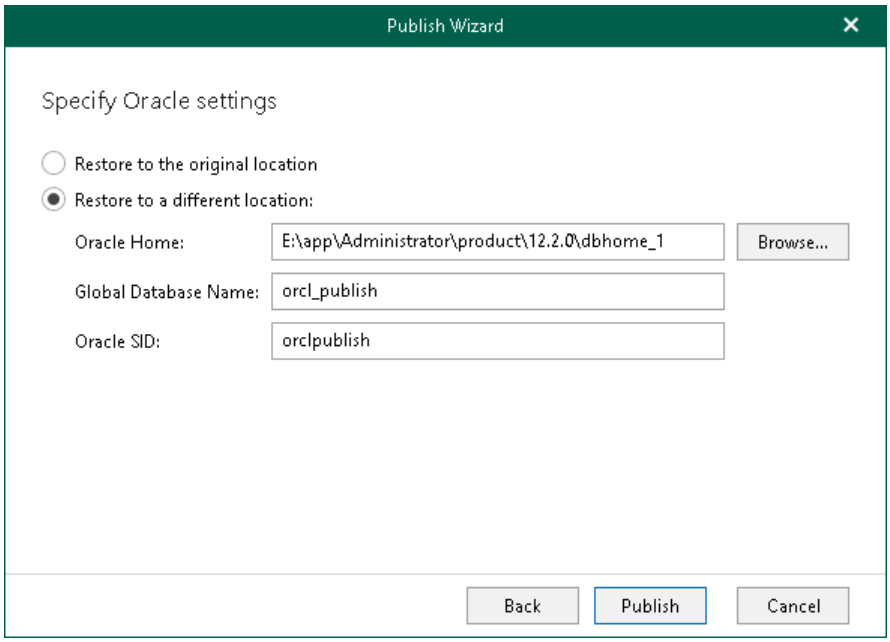
  When selecting this option, specify the following:

  - **Oracle Home**. Specify Oracle Home. You can click **Browse** to select a folder.
  - **Global Database Name**. Specify the name under which the database is going to be published.
  - **Oracle SID**. Specify the SID, which is populated automatically when the **Global Database Name** value is being set. You can also assign a value that is different from **Global Database Name**.

  The figure below shows an example of publishing a database with the *delme_published* name.

After you complete this step, a new **Published databases** node appears at the top of the navigation pane in Veeam Explorer for Oracle. Under this node you can find the databases that have been published during the current session.

> **NOTE**
>
> Veeam Explorer for Oracle only shows 8 characters of the published database name in its console. As per example, once published, the name of the published database in the navigation pane will be displayed as *delme_pu.*



Publishing Latest or Point-in-Time State

This section explains how to select a state as of which to publish Oracle databases.

You can select either of the following states:

- **The latest available state**

  To publish data as of the latest state in the backup file.

- **The point-in-time state**

  To publish data as of the selected point-in-time state (requires a log backup).

These options are available only after the initial publishing of a database to the target Oracle server, as described in Publishing to Specified Server.

When you unpublish a database, both options continue to remain until you close the application so that you can quickly republish a database if required.

Publishing Point-in-Time State

Publishing a point-in-time state allows you to load a required database state and unroll specified transactions if needed.

To publish a database as of the point-in-time state, do the following:

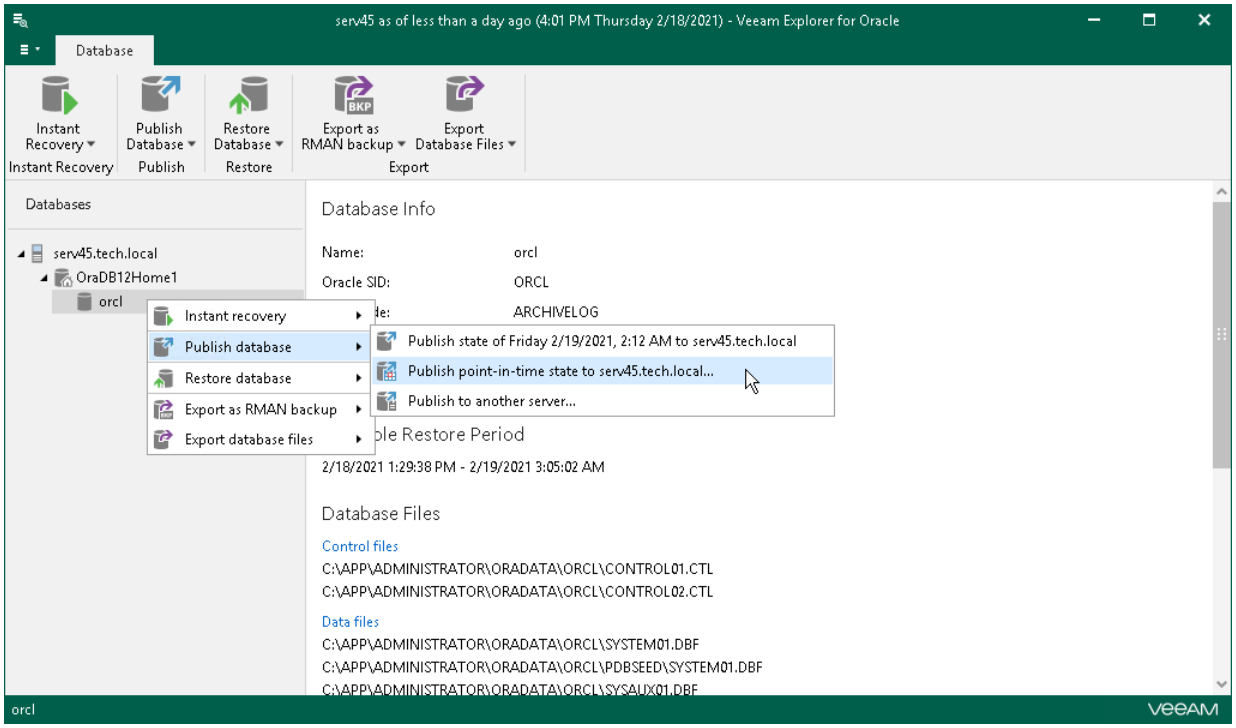
1. Launch the Publish wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, right-click a database.
2. On the **Database** tab, select **Publish Database** > **Publish point-in-time state to <server_name>** or right-click a database and select **Publish database** > **Publish point-in-time state to <server_name>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



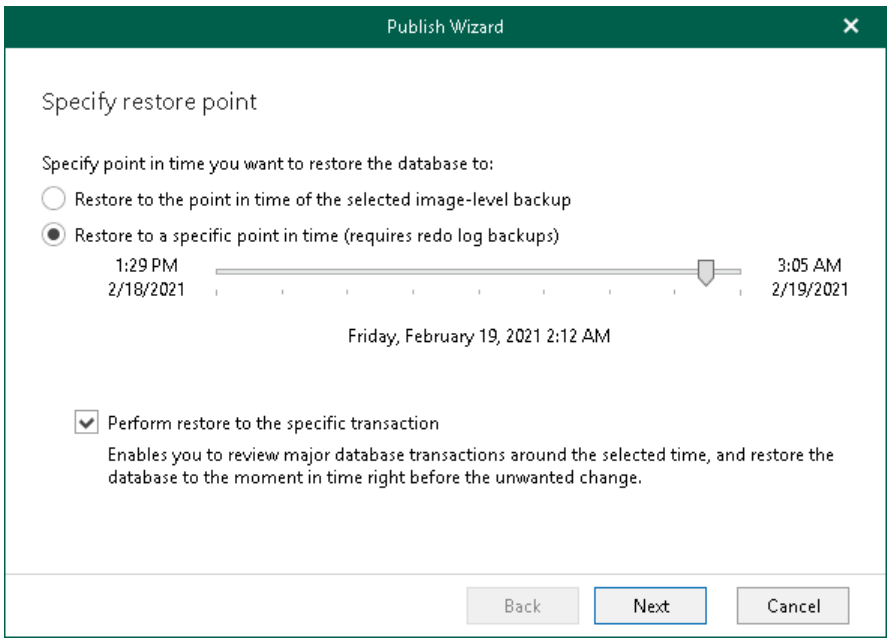
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

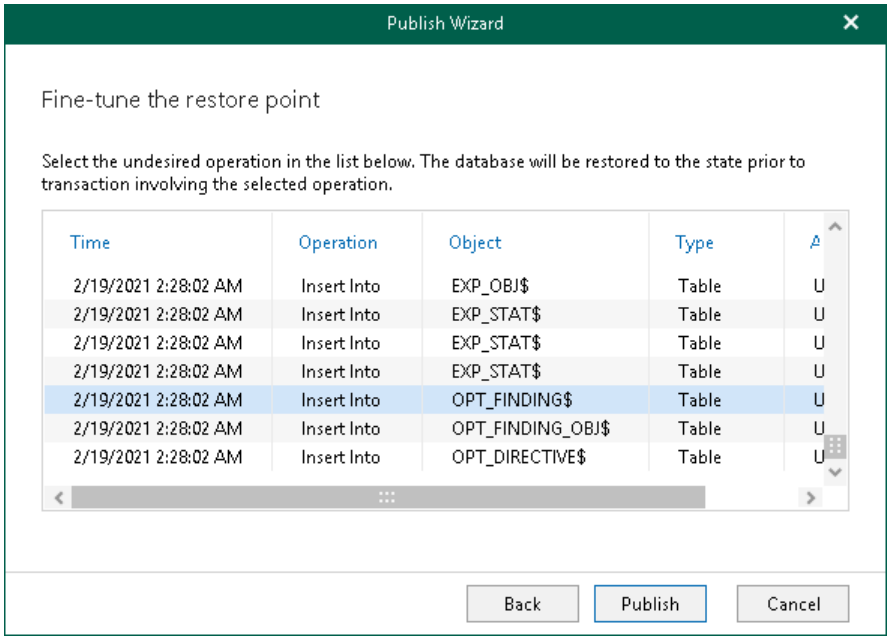
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database and click **Publish**.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



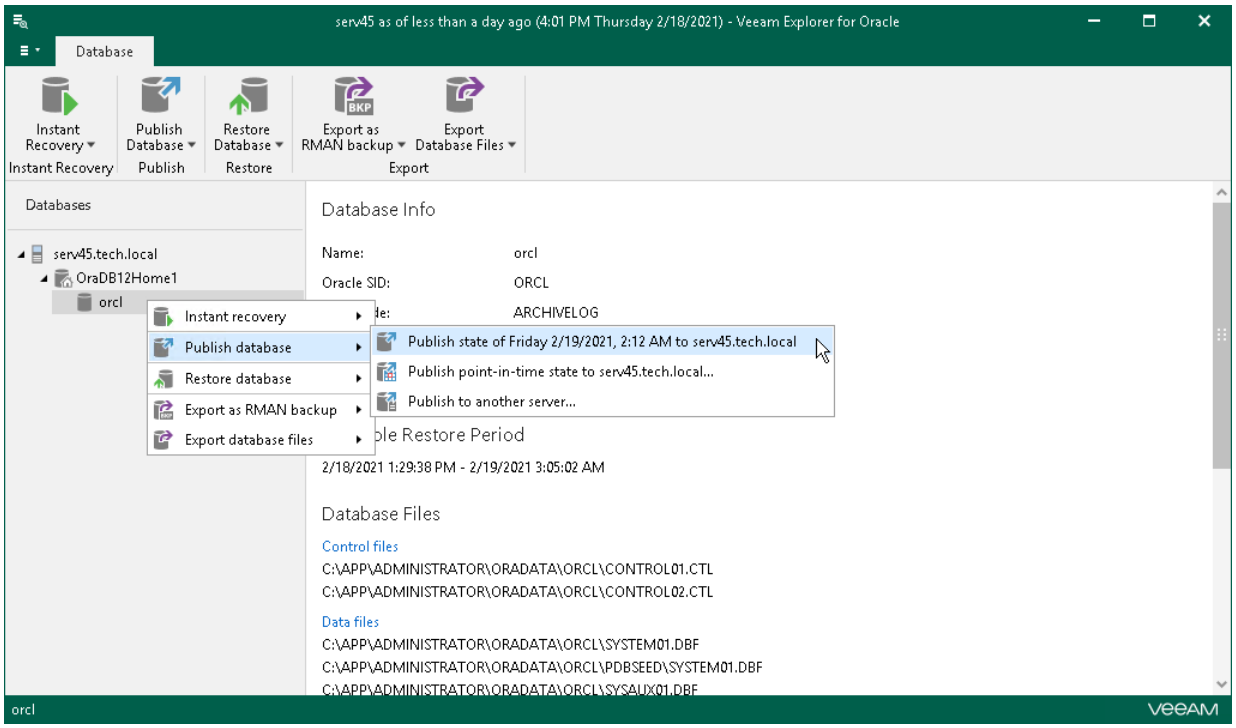
Publishing Latest State

Veeam Explorer for Oracle allows you to republish an unpublished database anew. When republishing a database, it will be attached to the target Oracle server as of the latest available state.

To republish a database as of the latest state, do the following:

1. In the navigation pane, right-click a database.
2. On the **Database** tab, select **Publish Database** > **Publish state of <point_in_time> to <server_name>** or right-click a database and select **Publish database** > **Publish state of <point_in_time> to <server_name>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



Unpublishing Databases

Once you have done working with published databases, you may want to unpublish (detach) these databases from the target Oracle server.

Detachment occurs in the following manner:

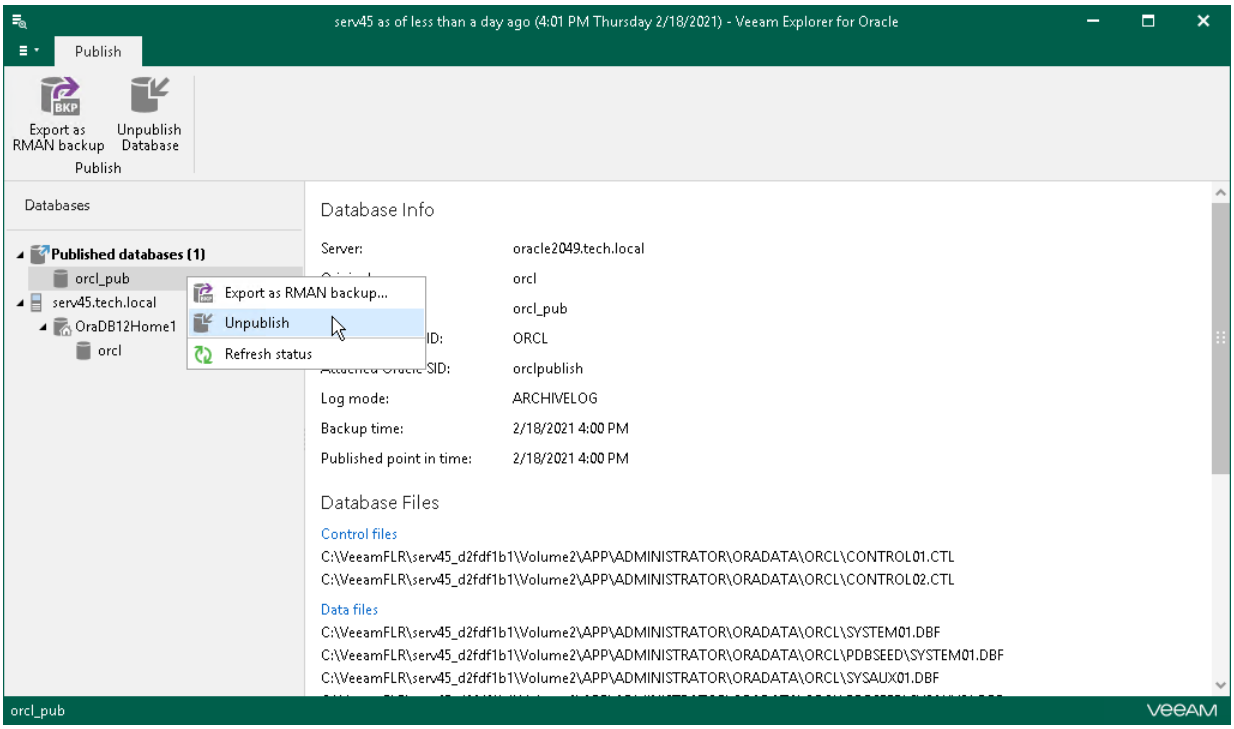
- Upon closing the Veeam Explorer for Oracle console, all published databases will be detached from the target Oracle server automatically. The corresponding mount points will also be dismounted from under the *C:|VeeamFLR* directory for Windows-based servers and the */tmp* directory for Linux-based servers.
- On manual unpublishing, databases will be detached at once but the restore point will remain mounted on the target server for the next 15 minutes.

To unpublish a database manually, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Unpublish Database**.

Alternatively, in the navigation pane, right-click a published database and select **Unpublish**.

To detach more than one published database simultaneously, right-click the root **Published databases** node and select **Unpublish databases** or select the root **Published databases** node and click **Unpublish Databases** on the **Publish** tab.



Exporting as RMAN Backup

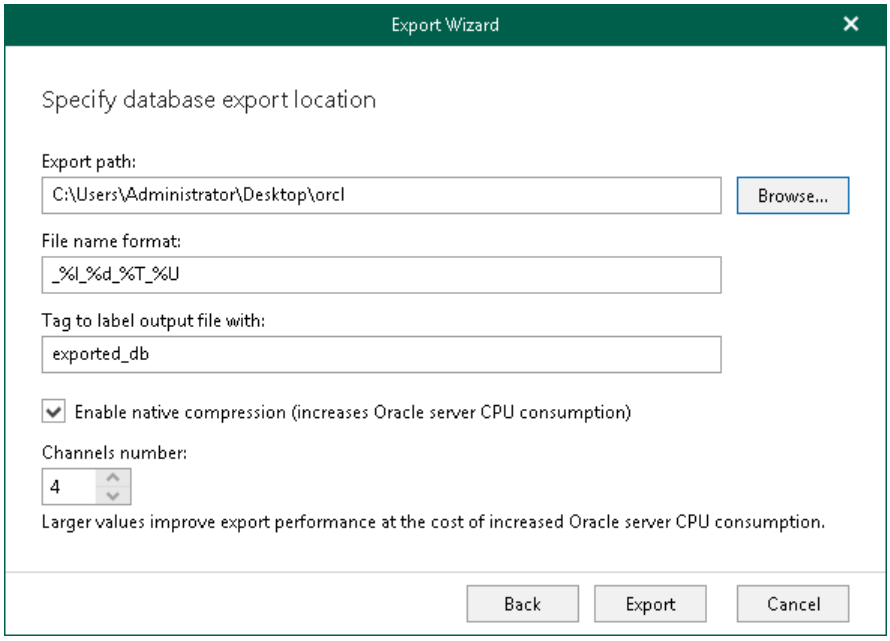
Once published, the database can be exported as an RMAN backup so that you can save the changes you may have made on the target server. For example, after publishing a database, you may have added a column or alter some values. In order to save these modifications before you unpublish the database, you can use the export feature.

To export a database, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Export as RMAN backup** or right-click a published database and select **Export as RMAN backup**.
3. In the **Export** wizard, in the **Export path** field, specify the location to which you want to export database files.

   If the folder you are specifying does not exist, it will be created.
4. In the **File name format** field, specify the format according to which your files will be named after the export.

   For more information, see this Oracle article.
5. In the **Tag to label output file with** field, specify a new tag name.
6. To compress files using native Oracle compression, select the **Enable native compression** check box.
7. In the **Channels number** numeric field, specify the number of channels to be used when retrieving Oracle databases from the backup.
8. Click **Export**.

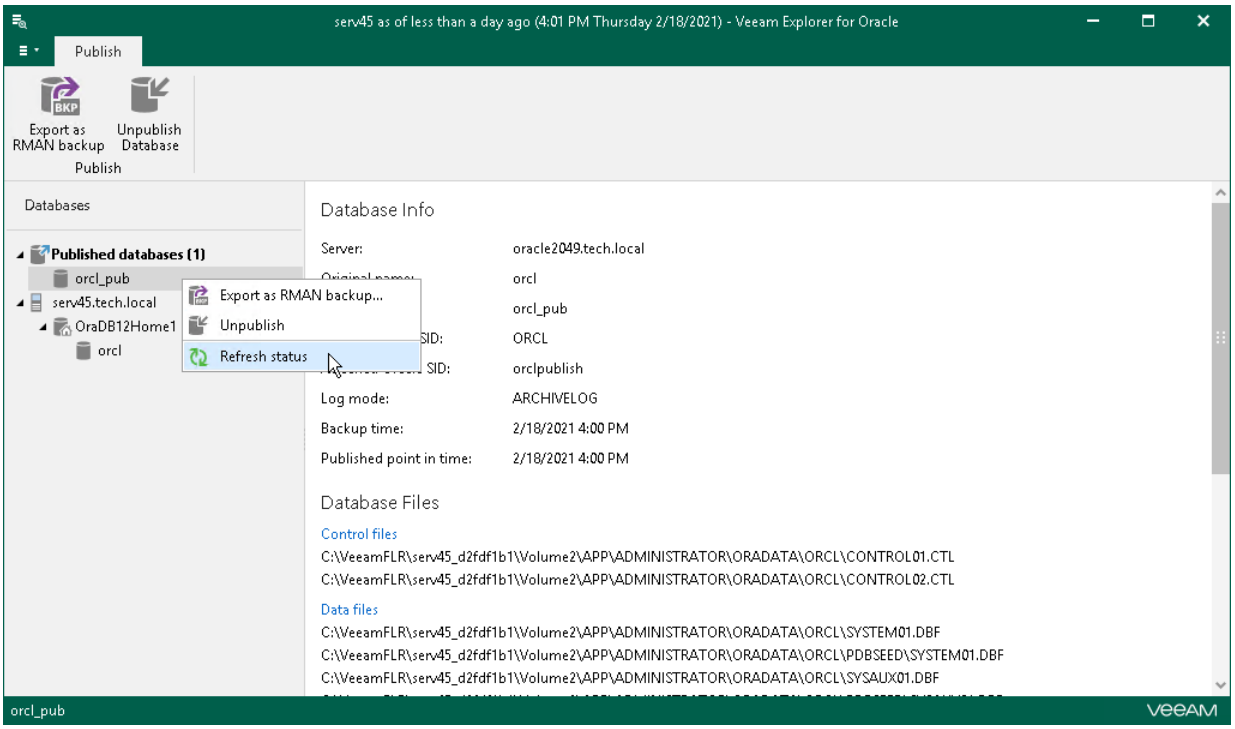


Refreshing Database Status

While databases are attached to the target Oracle server, Veeam Explorer for Oracle synchronizes each published database state to verify its availability. By default, synchronization occurs every five seconds.

If something went wrong with any of the published databases, the question mark appears next to each of such databases indicating the database unavailability. In the **Database Info** section, you will also see the notification message describing the problem.

To refresh a published database state manually, in the navigation pane, under the **Published databases** node, right-click a published database and select **Refresh status**.



Instant Recovery

Instant recovery combines capabilities of the data restore and data publishing features. If you want the database to be online as quickly as possible, you can use the **Instant Recovery** option and restore it in the background.

> **IMPORTANT**
>
> Before performing instant recovery, make sure to read Considerations and Limitations.

How It Works

To perform instant recovery, Veeam Explorer for Oracle uses the *Veeam Explorers Recovery Service* that runs in the background. This removes the necessity to keep Veeam Explorer running during an entire instant recovery session. Once you have started an instant recovery session, you can close Veeam Explorer and then launch it later when necessary.

When you start the instant recovery session in Veeam Explorer for Oracle, the following happens:

1. Veeam Explorer uses backup files to publish the database on the target production server directly from backup.
2. While the published database is online, Veeam Explorer starts to create a copy of the database on the target Oracle server.
3. All changes in database files that occur after publishing are saved in cache.
4. After all database files are copied to the target server, Veeam Explorer uses archived redo logs to synchronize changes in database files.
5. After the synchronization, you can switch over to the up-to-date copy of the database on the production server. Depending on the option you choose, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization. During switchover, Veeam Explorer does the following:
    a. Stops the published database.
    b. Uses redo logs to synchronize differences between the published database and the copied database files.
    c. Drops the published database.
    d. Starts the recovered database.

Instant recovery session is resilient to network disruption, backup server or mount server crash. If anything disrupts the restore process, the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch retry after the server or network is up.

Instant Recovery of Multiple Databases

You can you Veeam Explorer for Oracle to perform instant recovery of multiple databases hosted on a server or a certain Oracle server. You can perform instant recovery to the original server or to any other server in your network where Oracle Database is installed.

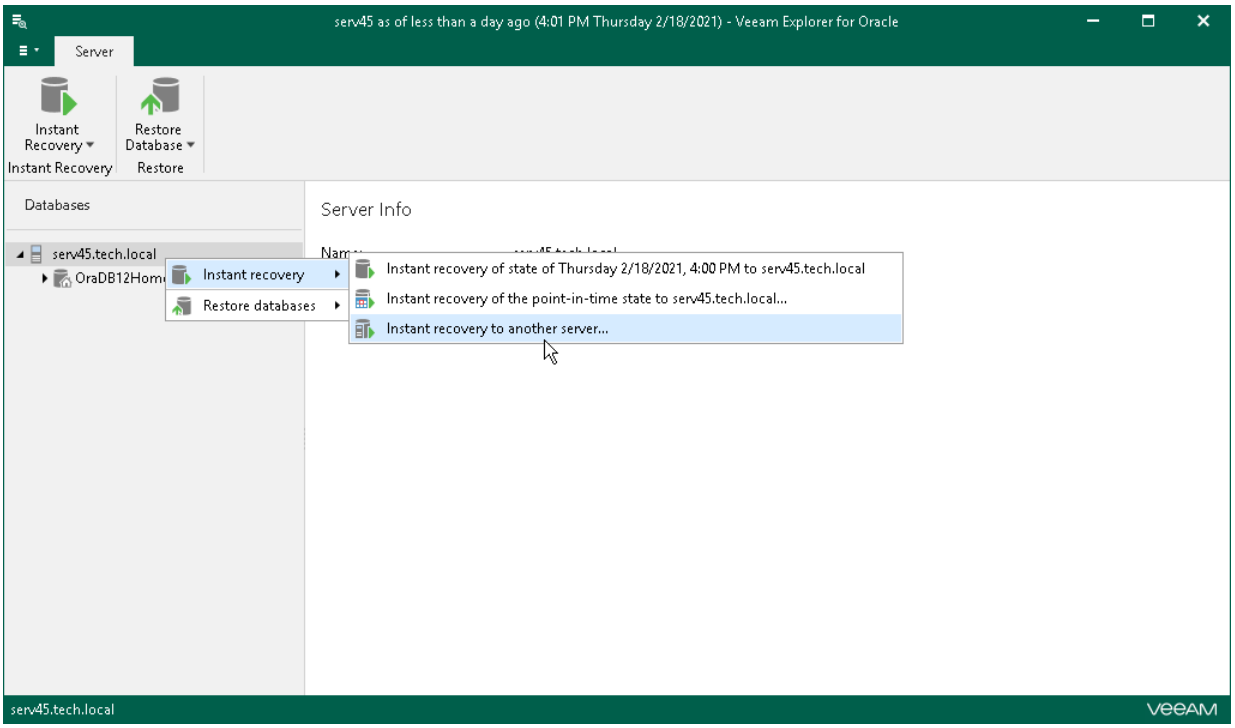
To perform instant recovery of multiple databases, do the following:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Specify the target server.
4. Specify oracle settings.
5. Specify switchover settings.
6. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To perform instant recovery of multiple databases, do the following:

1. In the navigation tree of Veeam Explorer for Oracle, select a server or Oracle home.
2. On the **Server** or the **Oracle Home** tab, select one of the following options:
   - **Instant Recovery** > **Instant Recovery of the latest state to** ***<original server>*** or right-click the server or Oracle home and select **Instant recovery** > **Instant recovery of the latest state to** ***<original server>***.
   - **Instant Recovery** > **Instant Recovery of the point-in-time state to** ***<original server>*** or right-click a server or Oracle home and select **Instant recovery** > **Instant recovery of the point-in-time state to** ***<original server>***.
   - **Instant Recovery** > **Instant Recovery to another server** or right-click a server or Oracle home and select **Instant recovery** > **Instant recovery to another server**.



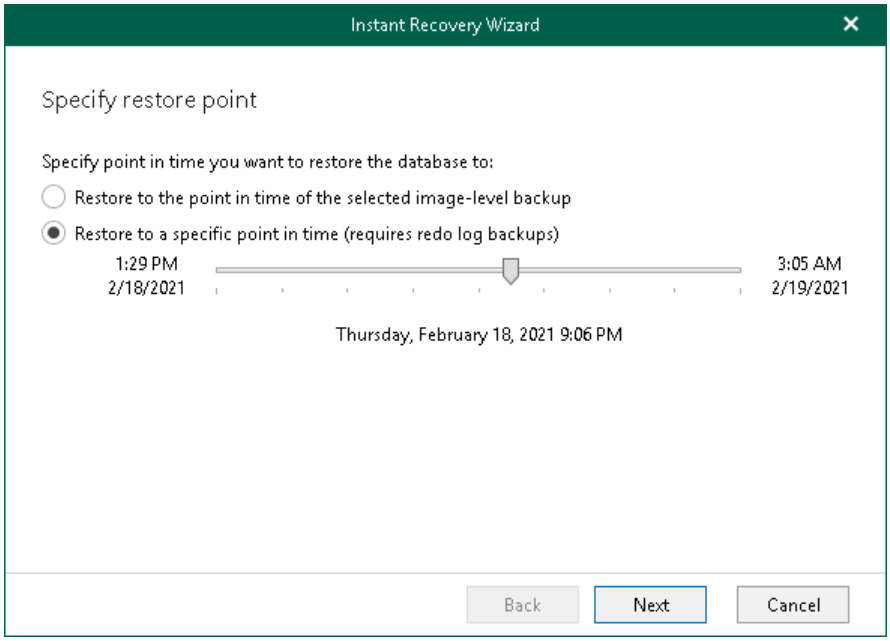
Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a required point in time.

> **NOTE**
>
> If you have selected to perform instant recovery of databases latest state to original server, skip this step and go to Step 5. Specify Switchover Settings.



Step 3. Specify Target Server

This step of the wizard is available if you select the instant recovery to another server option. At this step, specify credentials to access the target Oracle server.

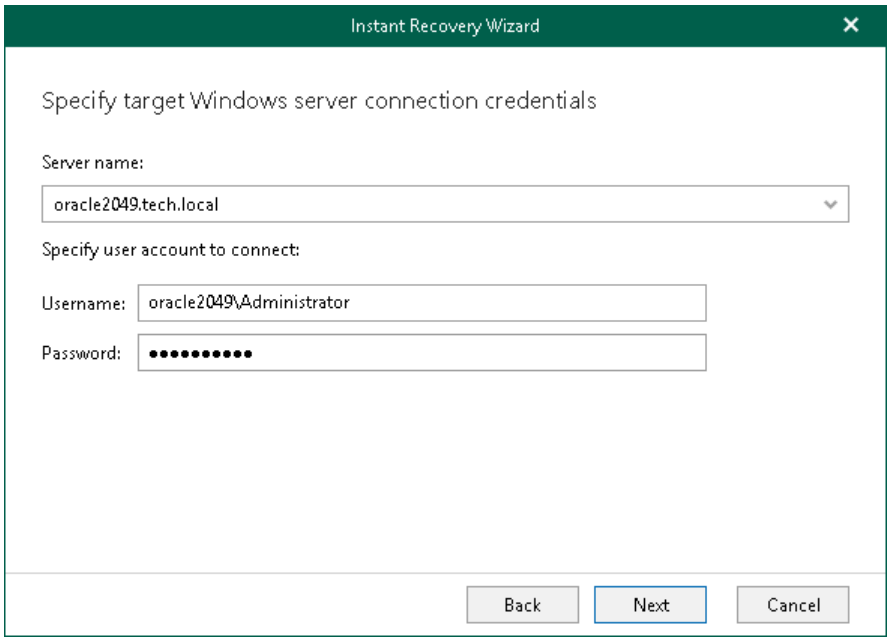
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. Under the **Specify user account to connect** specify credentials that will be used to connect to the specified server.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases (**Read** and **Write** are minimum required, **Full Control** is recommended).
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



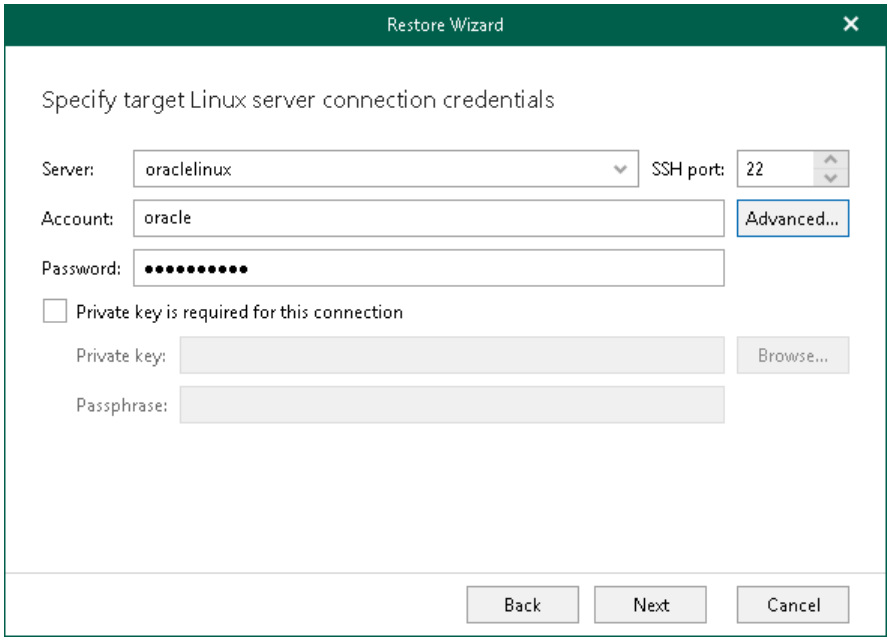
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

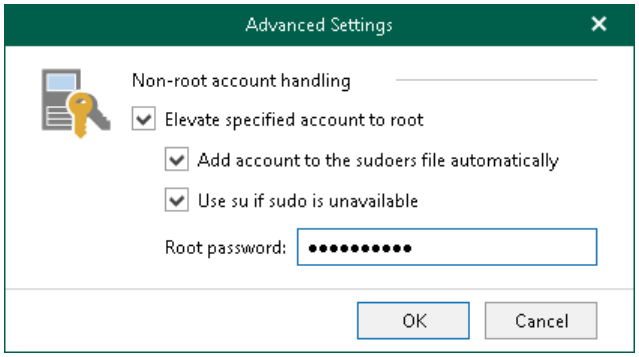
1. In the **Server** drop-down list, specify an Oracle server to which you want to restore data. You can specify the DNS name of the target Oracle server or select an Oracle server from the list.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



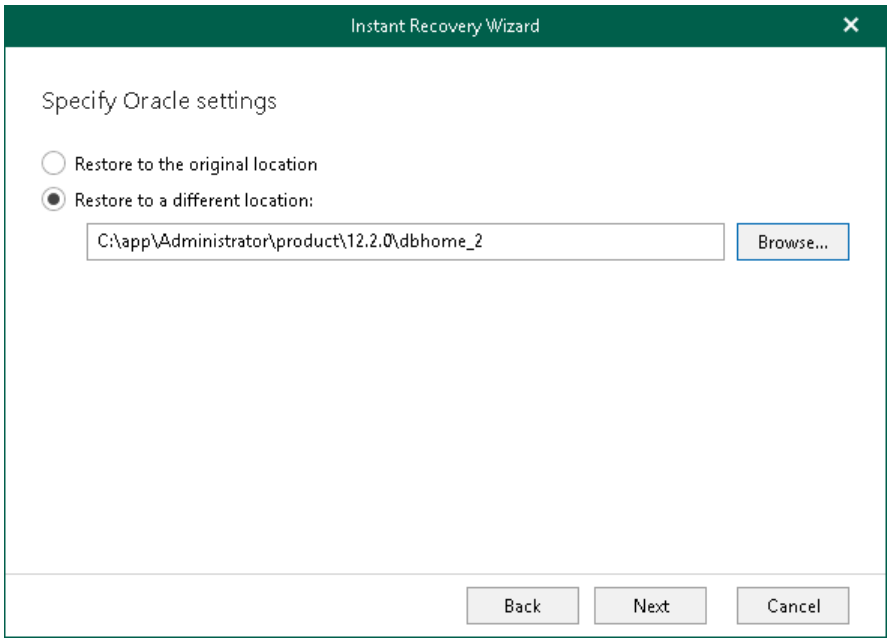
Use the native Veeam Explorer for Oracle abilities to elevate your account to *root* and add it to the *sudoers* file. To do this, click **Advanced** and select corresponding check boxes.



Step 4. Specify Oracle Settings

The **Specify Oracle settings** step of the wizard is available if you select the instant recovery to another server option. At this step of the wizard, select a location to which you want to restore databases:

- **Restore to the original location**. To restore databases back to the original location.
- **Restore to a different location**. To restore databases to the custom location, specify the **Oracle Home** for restored databases. To locate Oracle Home folder, click **Browse** and select a folder you want to use.



NOTE

If the account specified in step 3 is not the Oracle Home user, you will be asked to provide a password to access the target Oracle Home. Applicable to Oracle 12c and later versions.

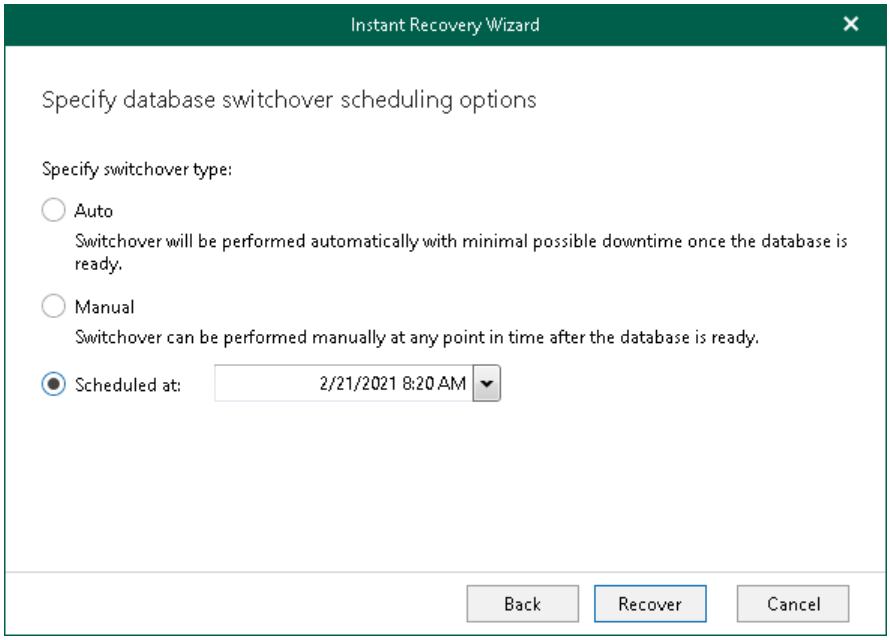
Step 5. Specify Switchover Settings

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.



Step 6. Finalize Instant Recovery Session

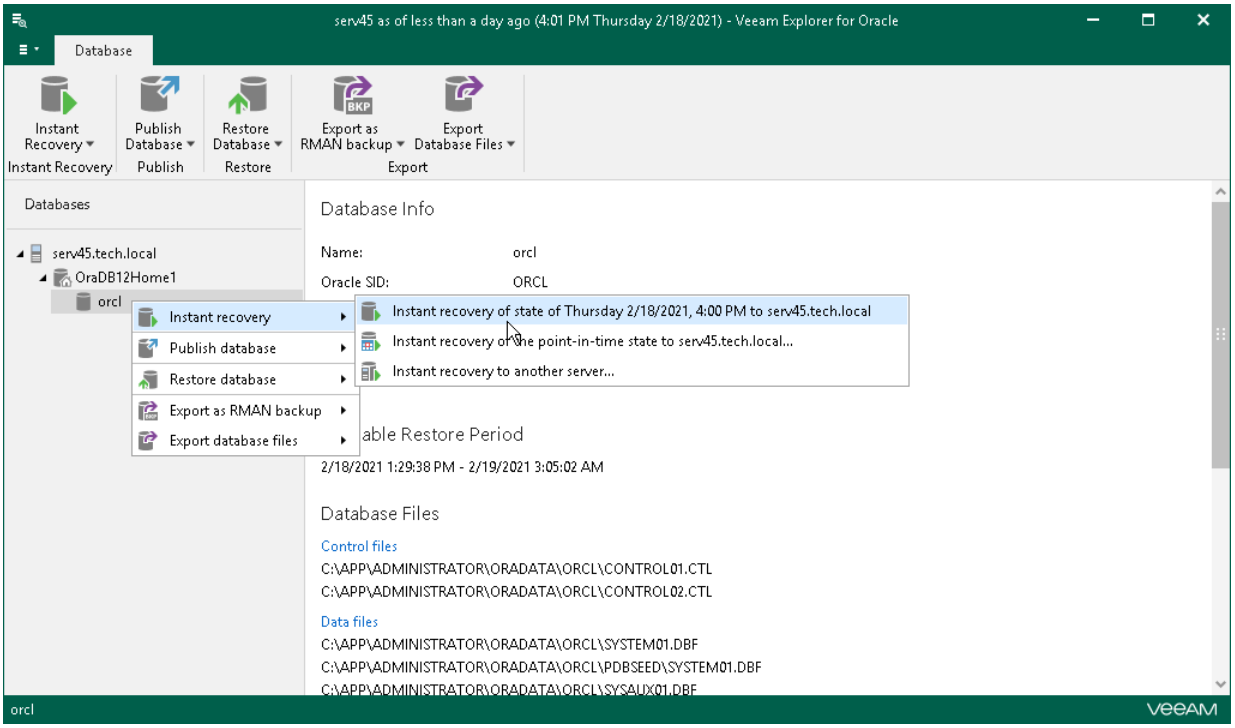
Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Instant Recovery of Latest State

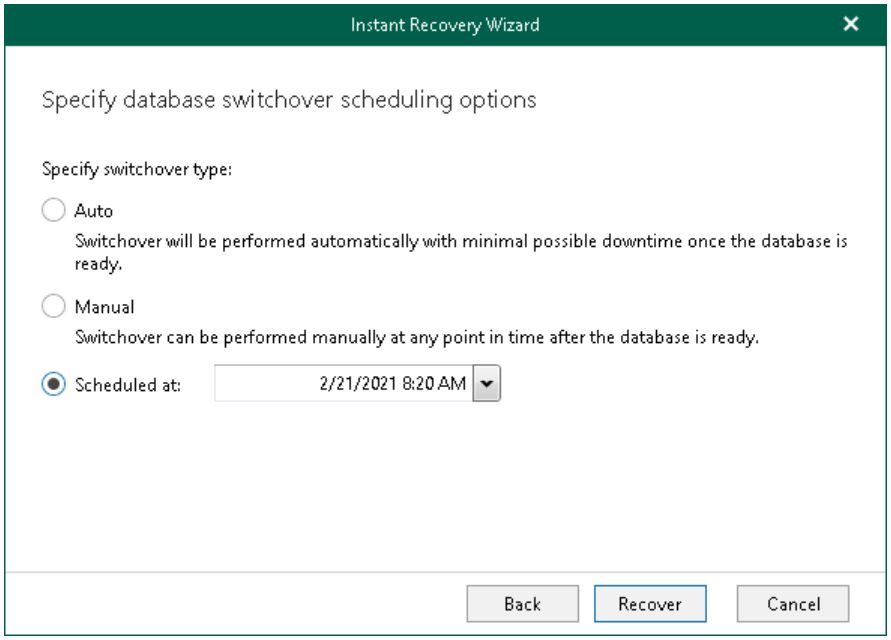
To perform instant recovery of a database to the latest state, do the following:

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant Recovery of state to <*original server*>** or right-click a database and select **Instant Recovery > Instant recovery of state to <*original server*>**.



3. In the **Instant Recovery** wizard, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.

- **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.



4. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.

5. Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

   If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Instant Recovery of Point-in-Time State

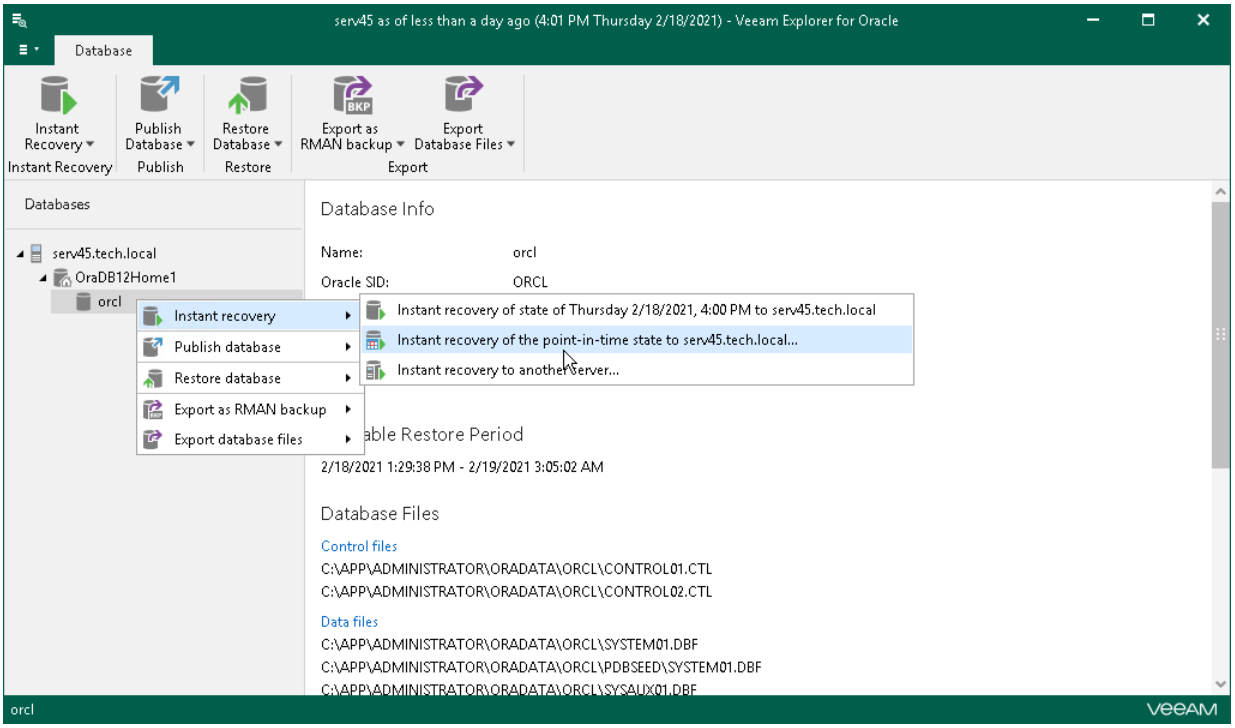
To perform instant recovery of a database to a selected point-in-time state, perform the following steps:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify a switchover option.
5. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery** wizard, do the following:

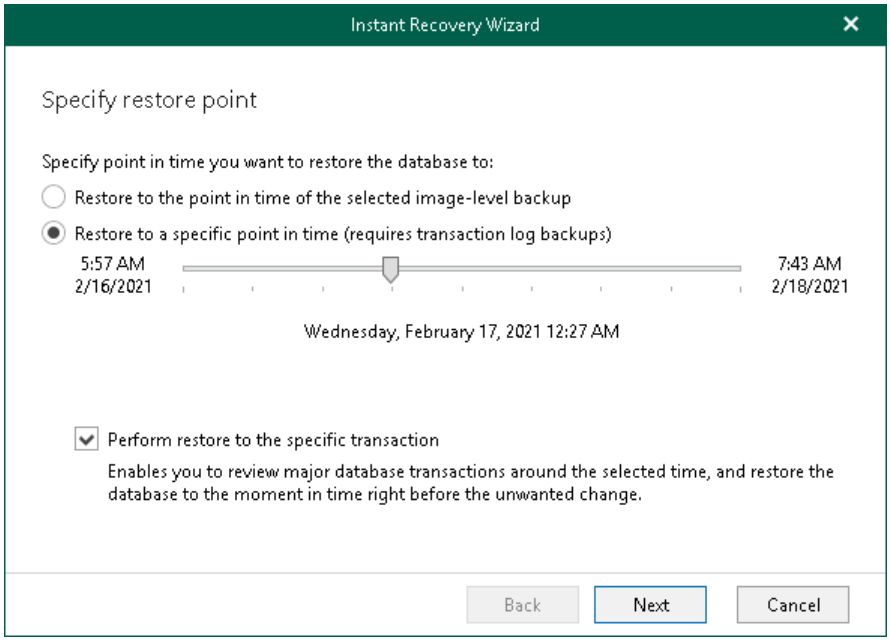
1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of point-in-time state to** *<original server>* or right-click a database and select **Instant recovery > Instant recovery of point-in-time state to** *<original server>*.



Step 2. Specify Restore Point

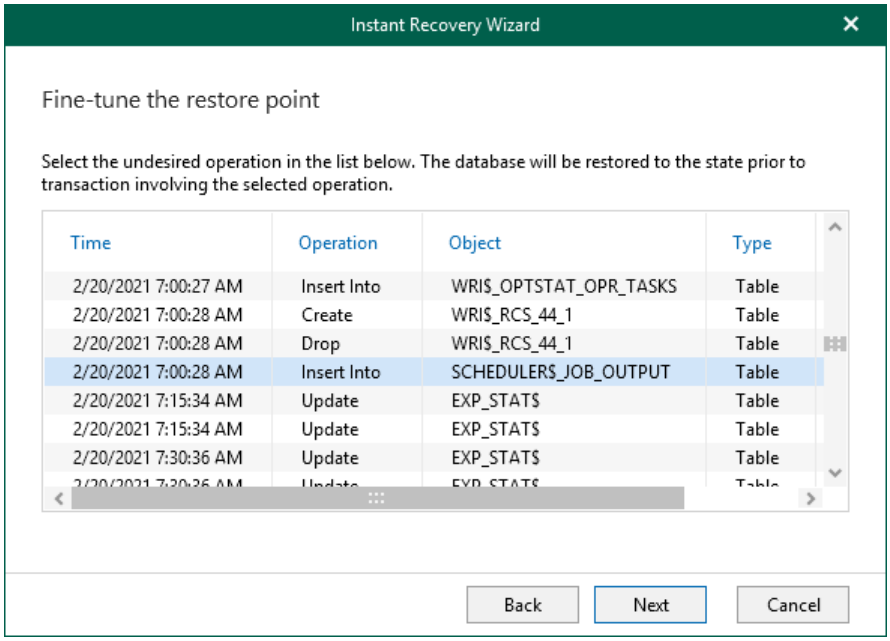
At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.



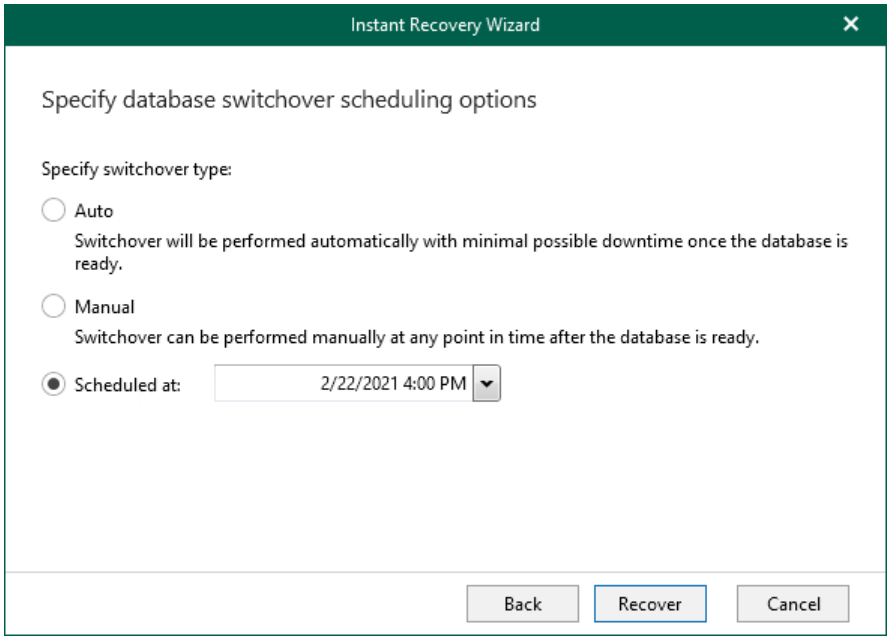
Step 4. Specify Switchover Option

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.



Step 5. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Instant Recovery to Another Server

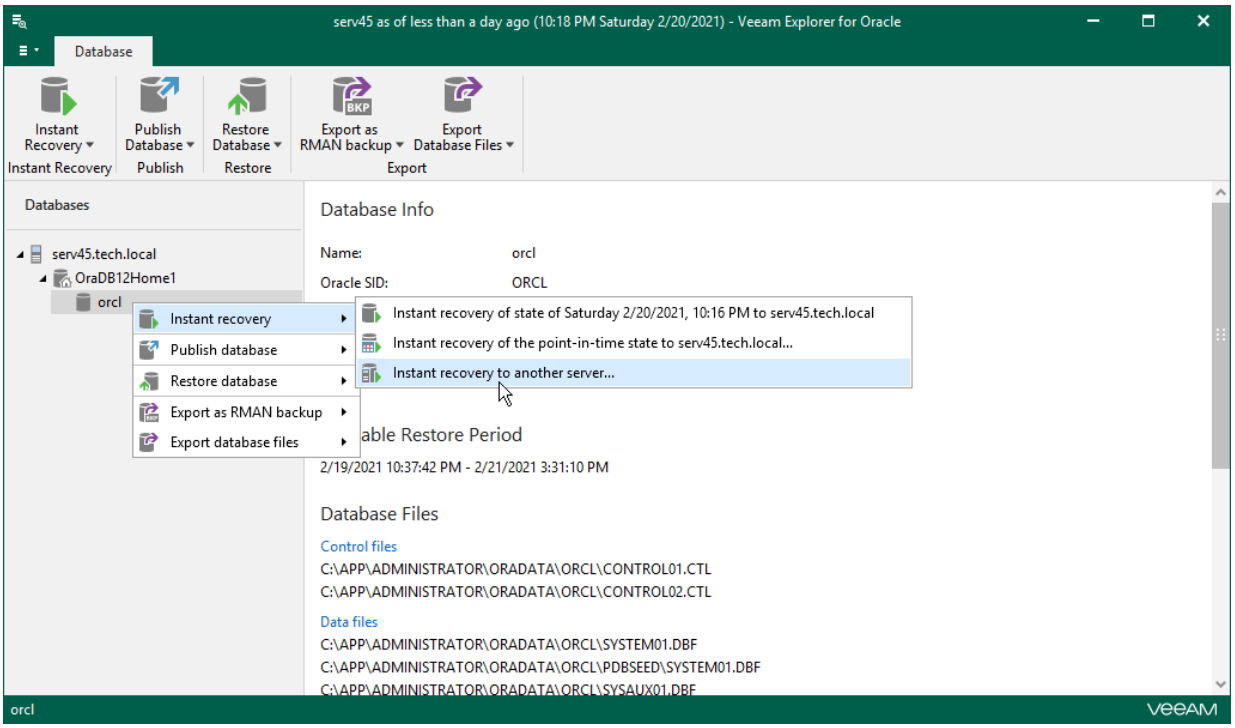
To perform instant recovery of a database to another server, perform the following steps:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify Oracle settings.
6. Specify database files location.
7. Specify a switchover option.
8. Finalize the instant recovery session.

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery** wizard, do the following:

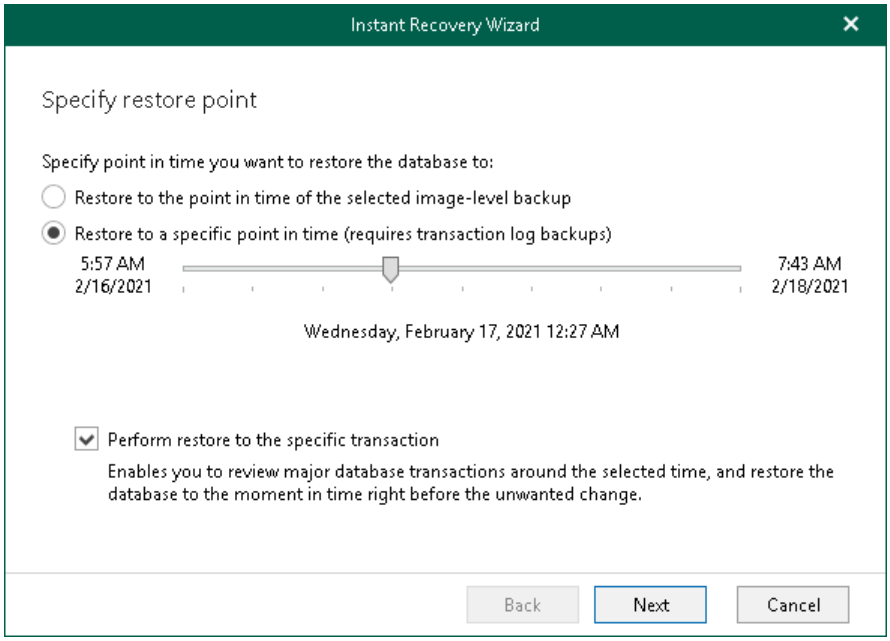
1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant Recovery to another server** or right-click a database and select **Instant recovery > Instant recovery to another server**.



Step 2. Specify Restore Point

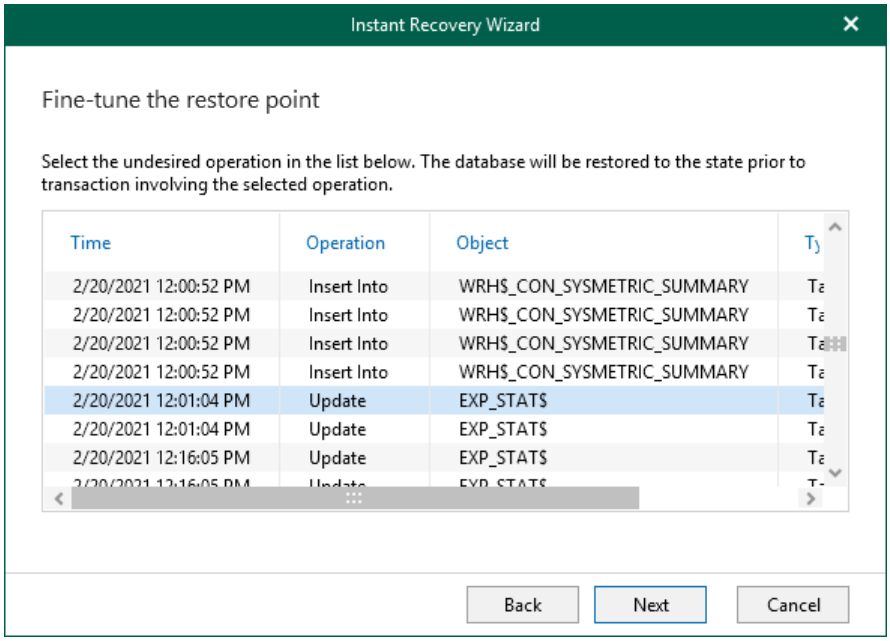
At this step of the **Instant Recovery** wizard, select a state as of which you want to restore the database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.



Step 4. Specify Target Server

At this step of the wizard, specify credentials to access the target Oracle server.

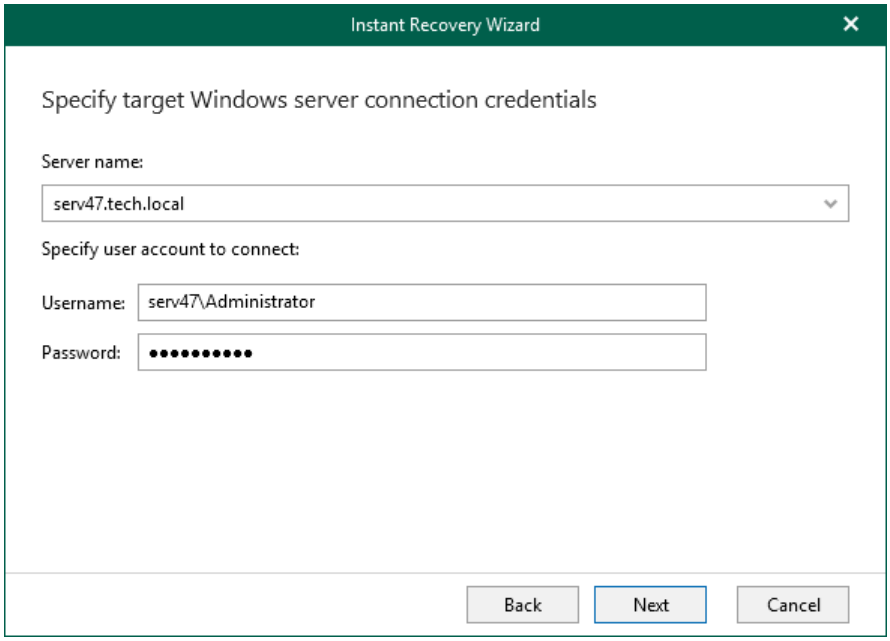
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. Under the **Specify user account to connect** specify credentials that will be used to connect to the specified server.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases (**Read** and **Write** are minimum required, **Full Control** is recommended).
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



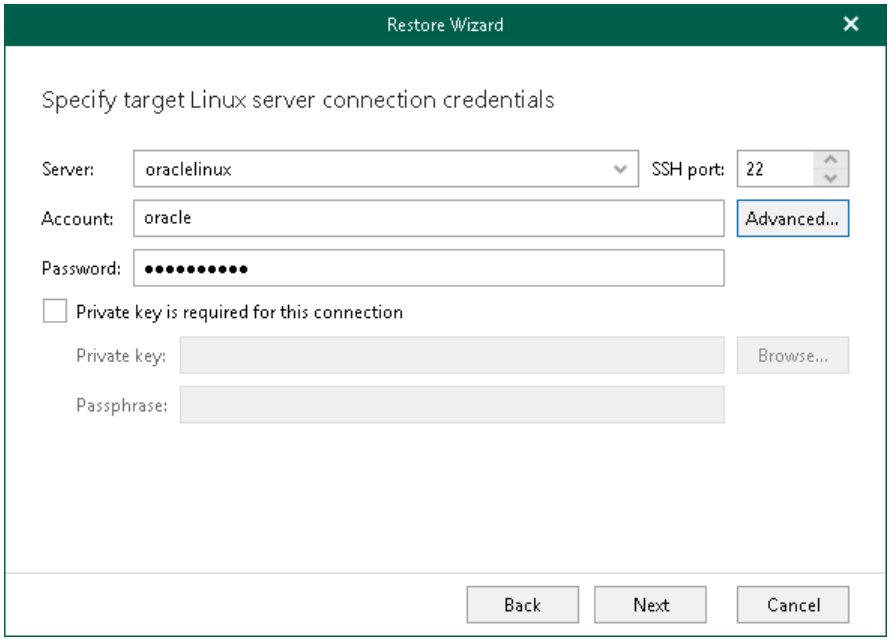
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

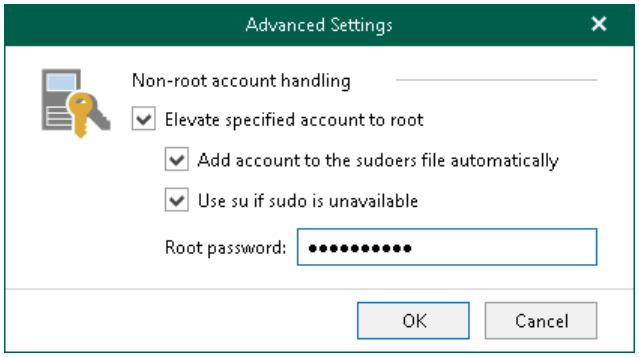
1. In the **Server** drop-down list, specify an Oracle server to which you want to restore data. You can specify the DNS name of the target Oracle server or select an Oracle server from the list.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   - Select the **Private key is required for this connection** check box.
   - In the **Private key** filed, specify a key.

     To select a key, click **Browse** and select a key.
   - In the **Passphrase** field, enter the passphrase.

Consider that the user account must be a member of the **dba** group.



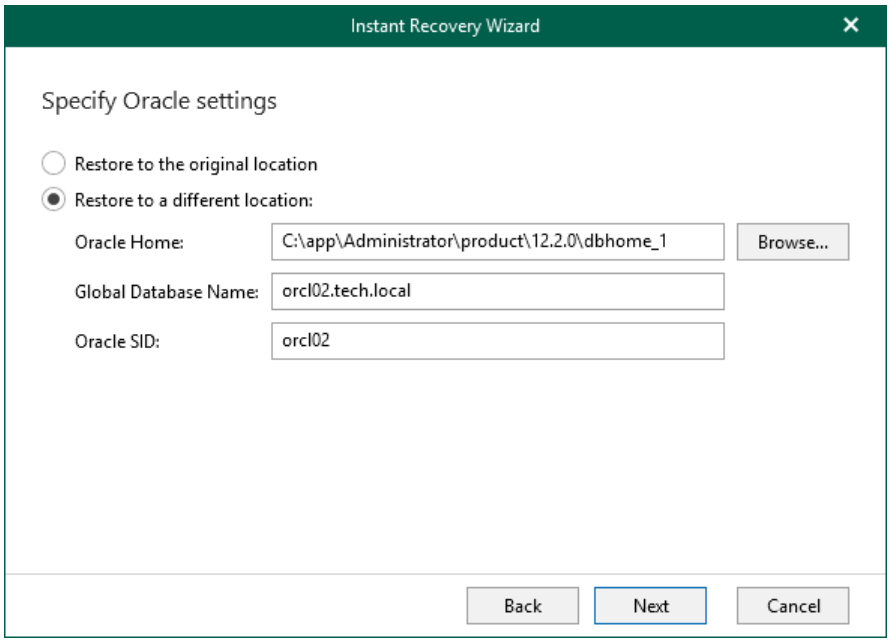
Use the native Veeam Explorer for Oracle abilities to elevate your account to *root* and add it to the *sudoers* file. To do this, click **Advanced** and select corresponding check boxes.



Step 5. Specify Oracle Settings

At this step of the wizard, select a location to which you want to restore databases:

- **Restore to the original location**. To restore a database back to the original location.
- **Restore to a different location**. To restore a database to the custom location specify **Oracle Home**, **Global Database Name** and **Oracle SID**. To locate Oracle Home folder, click **Browse** and select a folder you want to use.



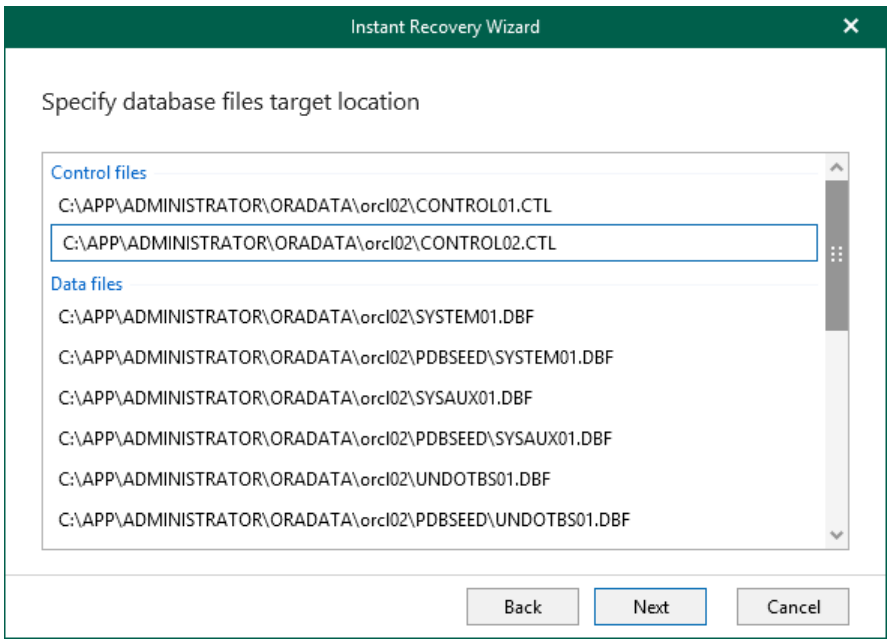
NOTE

If the account specified in step 4 is not the Oracle Home user, you will be asked to provide a password to access the target Oracle Home. Applicable to Oracle 12c and later versions.

Step 6. Specify Database File Location

At this step of the wizard, specify the location for database files (control files, data files, log files and temp files).

To edit the path, click the path row and provide the location you want to use. If specified folders do not exist, Veeam Explorer will create these folders.



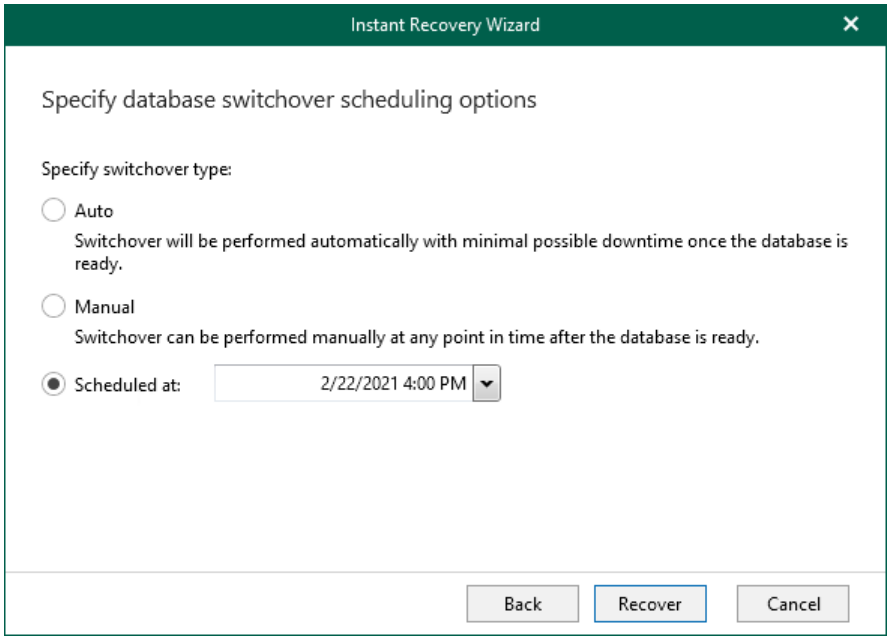
Step 7. Specify Switchover Option

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.



Step 8. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Switchover

The switchover option becomes available after all the database files are copied to the target server. During switchover, the mounted database is switched to its complete copy in a target server. Note that if you have selected to restore to the original server, the restored database will replace the original database.

Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

During the switchover, Veeam Explorer performs the following:

1. Detaches the published database from the Oracle server.
2. Uses archived redo logs to synchronize changes between the published database and the copied database files.
3. Drops the published database.
4. Attaches the recovered database to the Oracle server.

Note that the database will be offline between the steps 1-4.

Auto Switchover

The Auto switchover option ensures minimal period of downtime.

As soon as database files are copied from backup files, Veeam Explorer uses archived redo logs to find differences between the published database and the recovered database. Depending on the size of differences in archived redo logs, the following happens:

- If the size of differences in archived redo logs is smaller than 10 MB, Veeam Explorer starts the switchover. In this case, the databases are synchronized during the switchover.
- If the size of differences in archived redo logs is larger than 10 MB, Veeam Explorer uses redo logs to synchronize the changes.

  After synchronizations, checks the size of differences in archived redo logs once again. If the size is smaller than 10 MB, Veeam Explorer starts the switchover. If the size is larger than 10 MB again, another cycle of synchronization is performed. Synchronization is relaunched until the size of differences in logs is smaller than 10 MB.

Manual Switchover

After database files are copied from backup files, Veeam Explorer uses archived redo logs to find differences between the published database and the recovered database. Veeam Explorer checks the size of differences every minute. If the size is larger than 10 MB or it has been 5 minutes since the last synchronization, Veeam Explorer starts to synchronize the changes between the published database and the copied database files.

After the synchronization is finished, you can launch the switchover manually. For details, see Starting Switchover Manually.

If you launch the switchover during the synchronization process, the switchover starts only after the synchronization if finished.

Scheduled Switchover

After database files are copied from backup files, Veeam Explorer uses archived redo logs to find differences between the published database and the recovered database. Veeam Explorer checks the size of differences every minute. If the size is larger than 10 MB or it has been 5 minutes since the last synchronization, Veeam Explorer starts to synchronize the changes between the published database and the copied database files.

After the synchronization is finished, Veeam Explorer waits for the scheduled date and time to start the switchover.

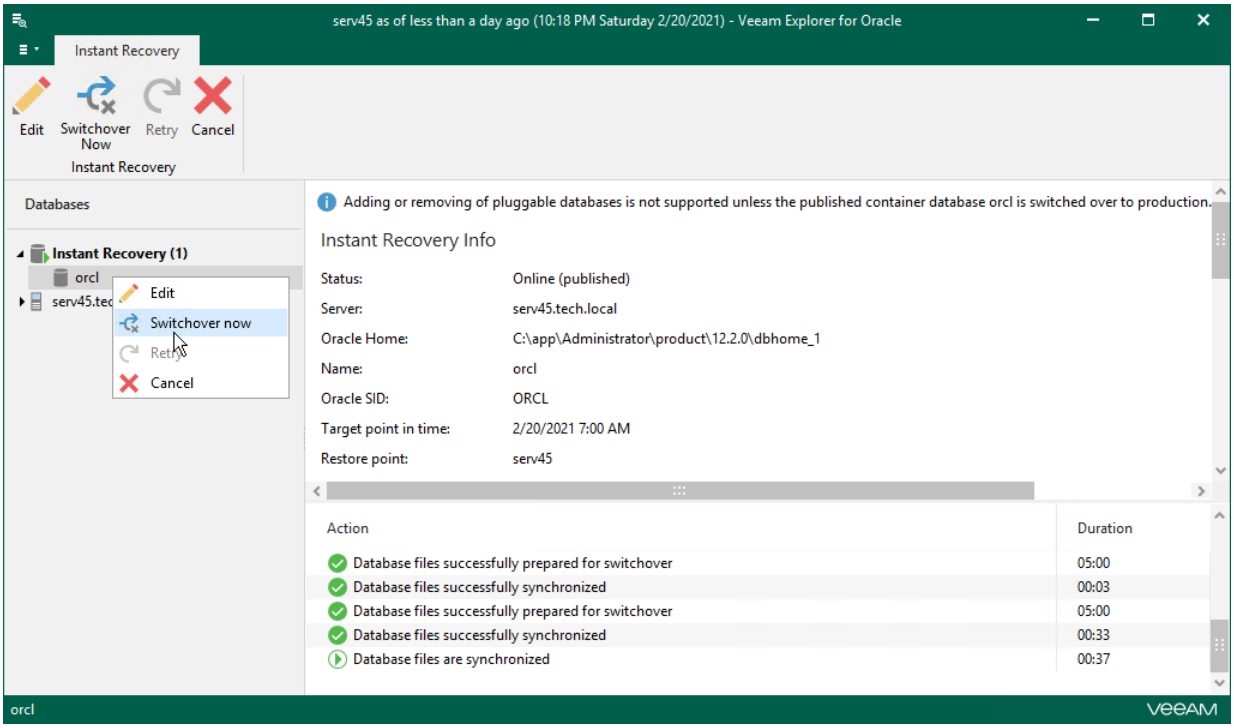
If the switchover scheduled period starts during the synchronization process, the switchover starts only after the synchronization if finished

Starting Switchover Manually

If you have selected the *Manual* switchover option in the **Instant Recovery** wizard, you can start the switchover at any time if the database is in the *Ready to switchover* state.

To start the switchover manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Switchover Now** or right-click the database and select **Switchover now**.



Managing Instant Recovery Session

After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Oracle starts an instant recovery session which shows the progress of the recovery process.

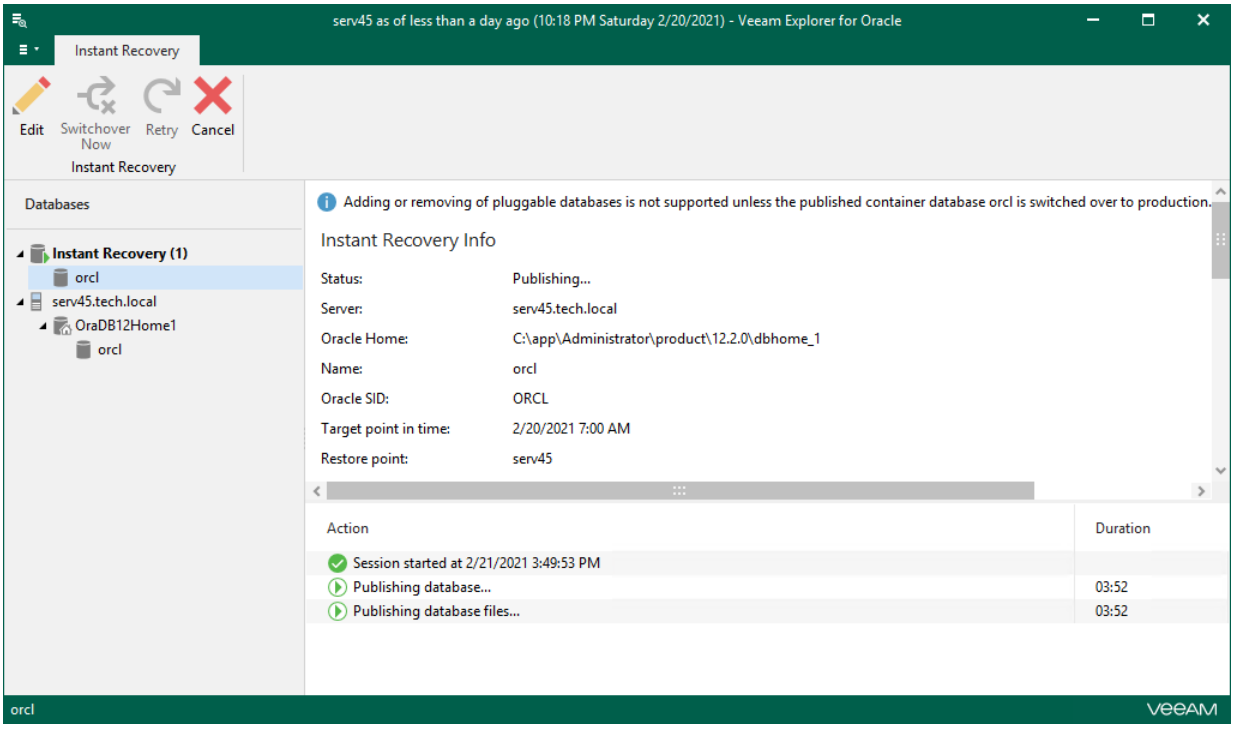
Depending on the option you choose in the **Instant Recovery** wizard, the switchover starts manually, automatically according to a specified schedule or immediately after synchronization.

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Also, in the **Instant Recovery** session view, you can do the following:

- Edit switchover settings.
- Retry instant recovery (in case instant recovery session fails for any reason).
- Cancel instant recovery.

> **NOTE**
>
> An instant recovery session closes automatically after the switchover.

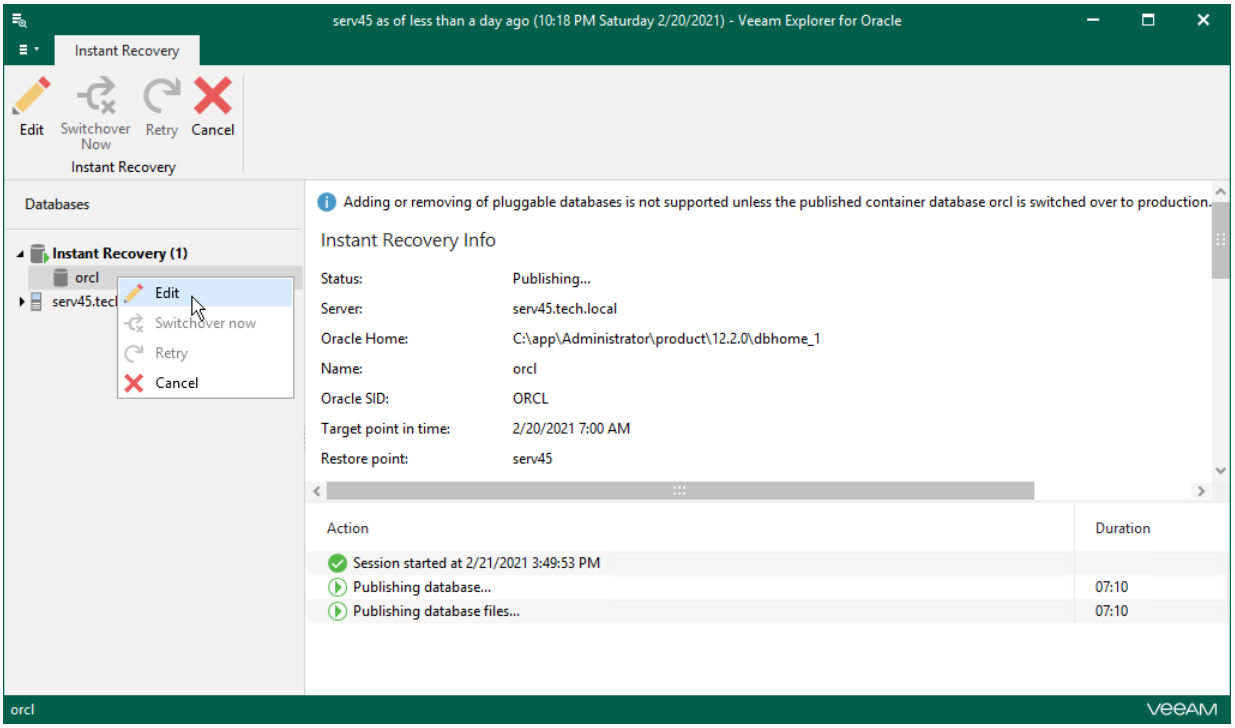


Editing Instant Recovery Settings

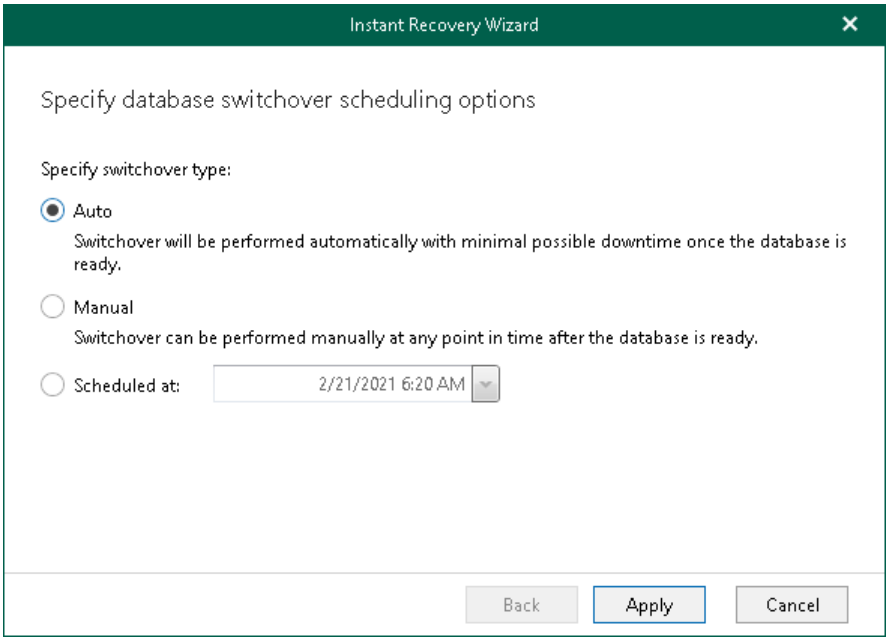
If you have started an instant recovery session and want to change the switchover settings, you can edit the instant recovery settings.

To change switchover settings of an instant recovery session, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Edit** or right-click the database or instance and select **Edit**.



3. Change the switchover option and click **Apply**.

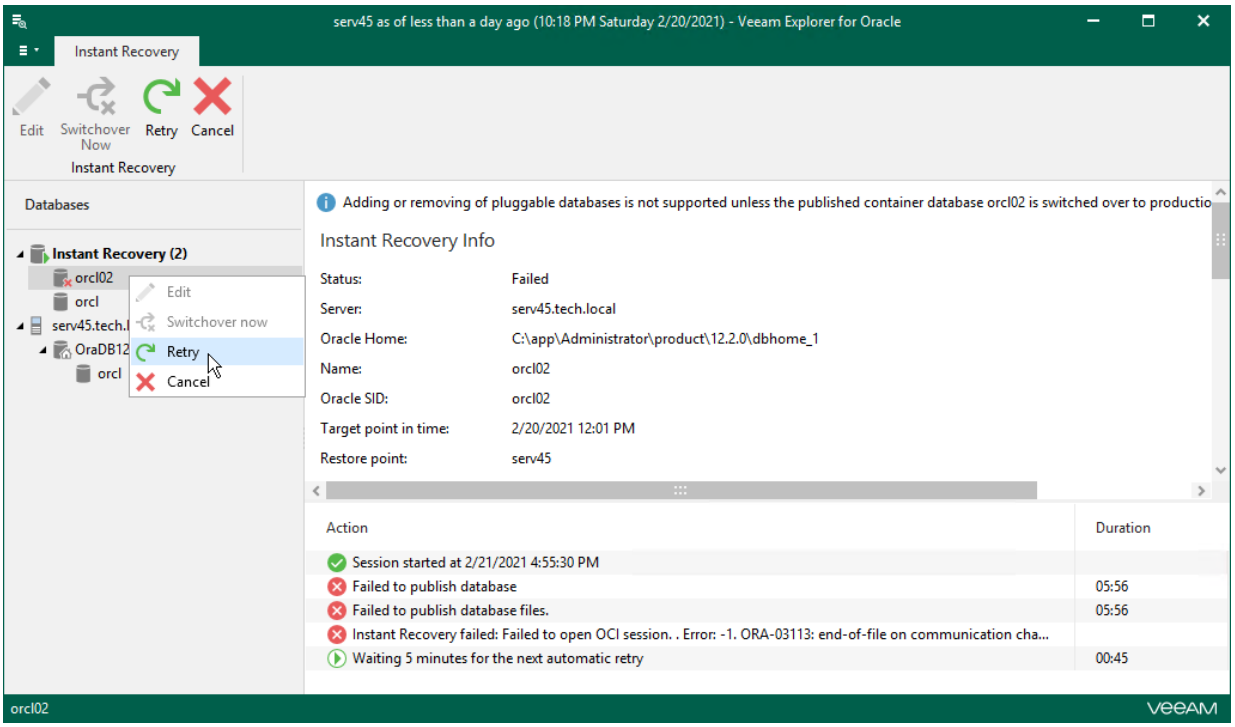


Recovery Retry

If anything disrupts the restore process (the target or mount server crashes or the network is down), the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch the retry manually after the server or network is up.

To start the retry process manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select the database.
2. On the **Instant Recovery** tab, click **Retry**.

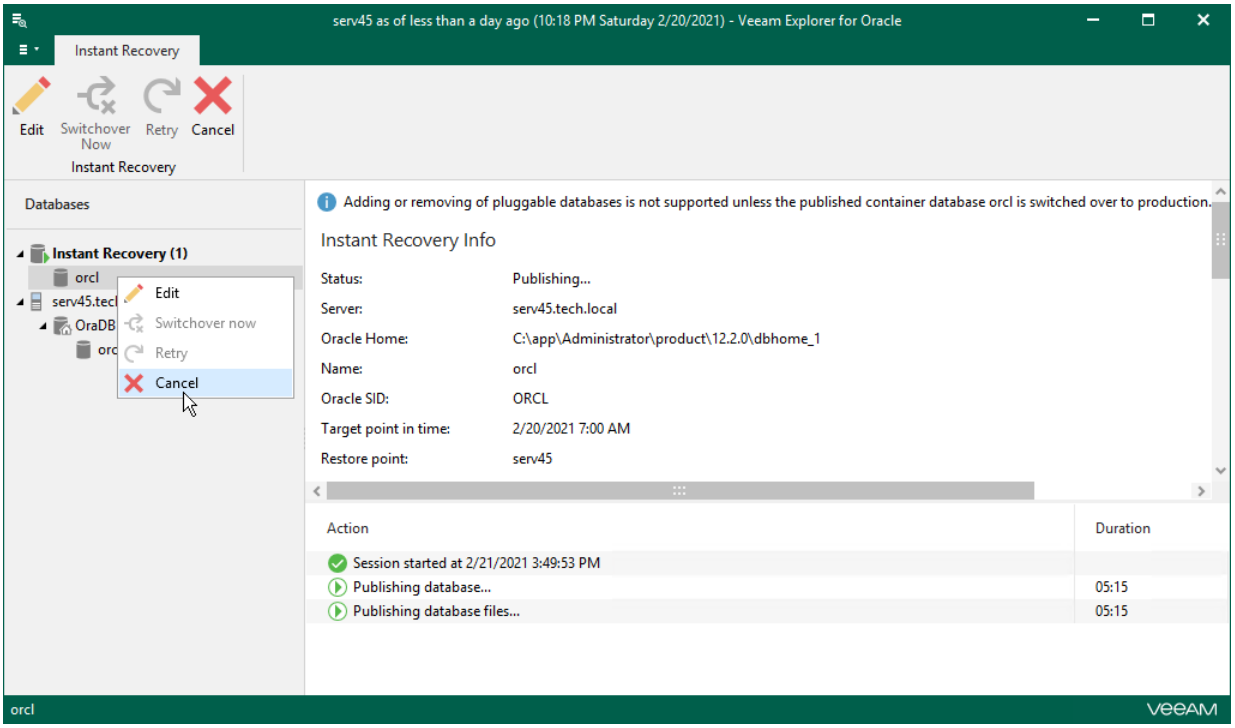


Cancelling Instant Recovery

If you have done working with published databases and don't want to move the published database to the original database, you can cancel the instant recovery process.

To cancel the instant recovery process, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Cancel** or right-click the database and select **Cancel**.



> **NOTE**
>
> You do not need to cancel the instant recovery session if switchover is already performed. The session closes automatically after the switchover.

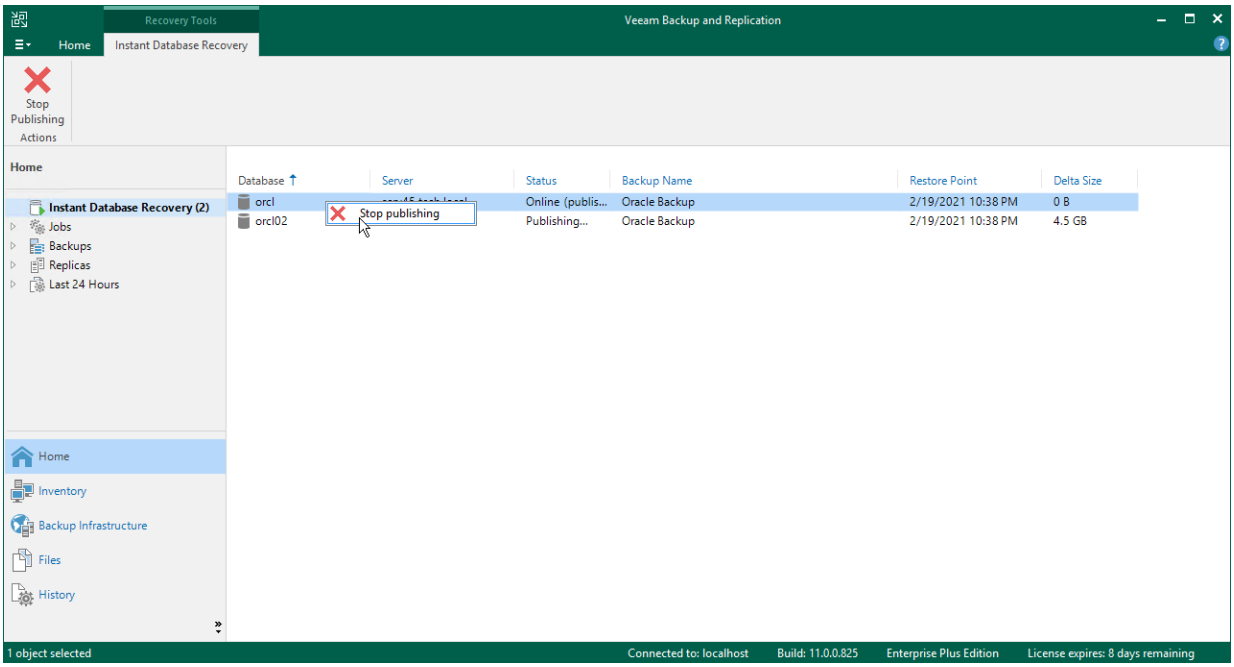
Stopping Publishing

After you finish steps of the **Instant Recovery** wizard, you can see the **Instant Database Recovery** session in the Veeam Backup & Replication console.

In the Veeam Backup & Replication console, you can stop publishing the database. If you stop publishing the database, the instant recovery session will be canceled.

To stop publishing the database:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the navigation pane, select **Instant Database Recovery**.
3. Right-click the database and select **Stop publishing**.



Data Export

Continue with this section to learn more about exporting Oracle databases.

Export as RMAN Backup

In Veeam Explorer for Oracle, you can export Oracle databases as RMAN backups.

During the export, Veeam Explorer for Oracle does the following:

- Uses native Oracle RMAN to retrieve Oracle databases from the backup that is being explored.

  The retrieved databases are then saved onto a staging server as RMAN backups.

  When exporting published databases, then such databases are saved directly to the server onto which they are published.

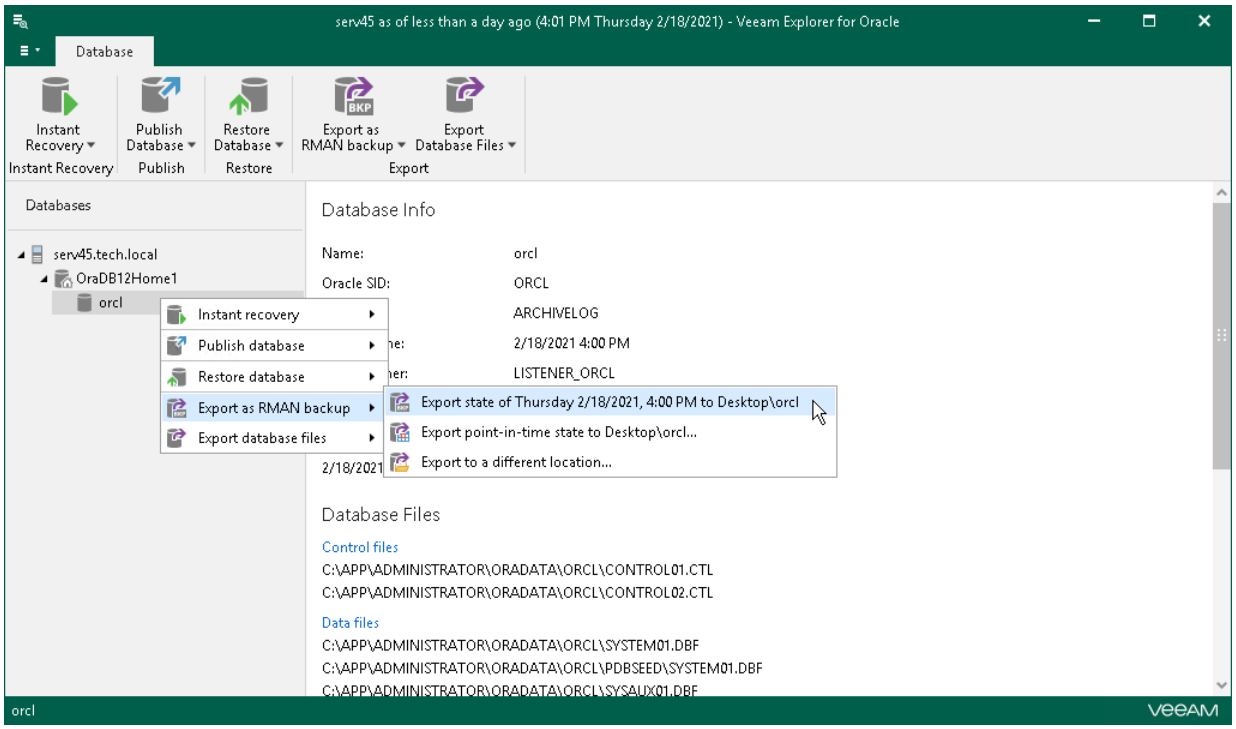
- Copies the saved RMAN backups to the target location.

Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup > Export state of <point_in_time> to Desktop\<db_name>** or right-click a database and select **Export as RMAN backup > Export state of <point_in_time> to Desktop\<db_name>**.
3. Wait until the export process is complete.

Consider that Veeam Explorer for Oracle exports files in the following format: *_%I_%d_%T_%U*. For more information, see this Oracle article. To set a different export format, use Exporting to Custom Location.



Exporting Point-in-Time State

To export data as of the point-in-time state, do the following:

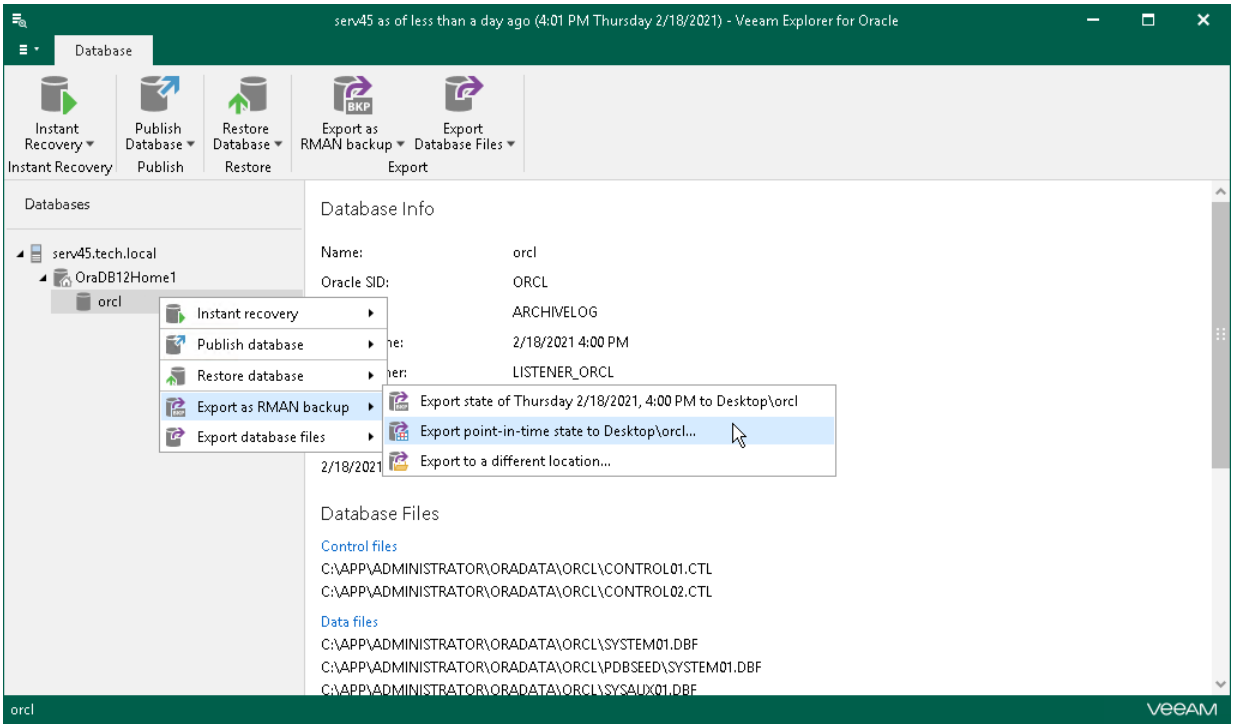
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup** > **Export point-in-time state to Desktop\<db_name>** or right-click a database and select **Export as RMAN backup** > **Export point-in-time state to Desktop\<db_name>**.

Consider that Veeam Explorer for Oracle exports files in the following format: *_%I_%d_%T_%U*. For more information, see this Oracle article. To set a different export format, use Exporting to Custom Location.



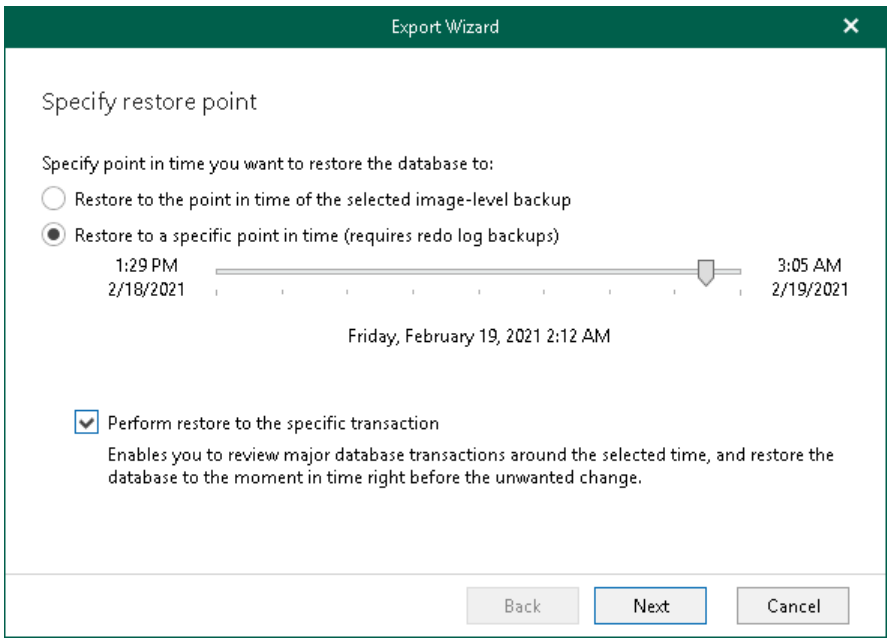
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

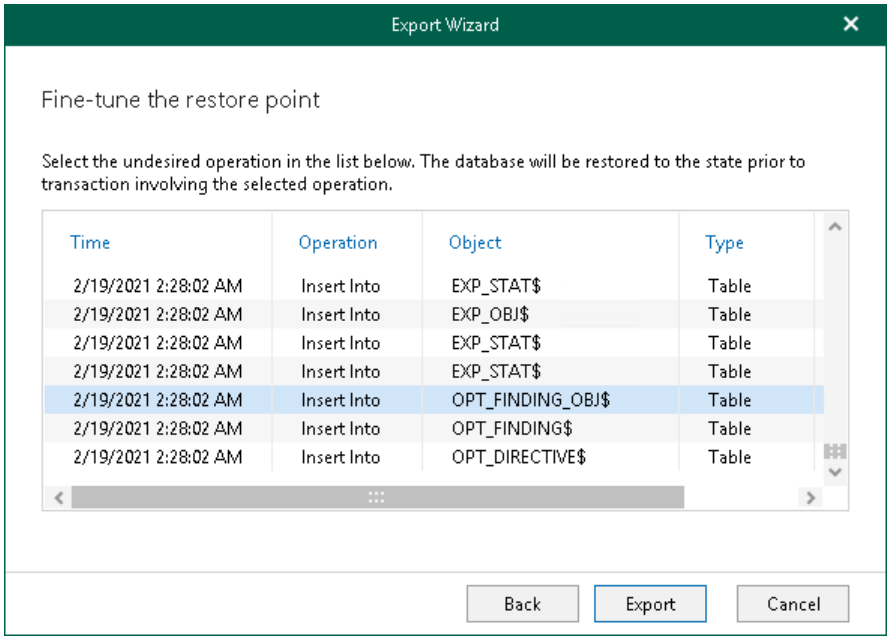
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Exporting to Custom Location

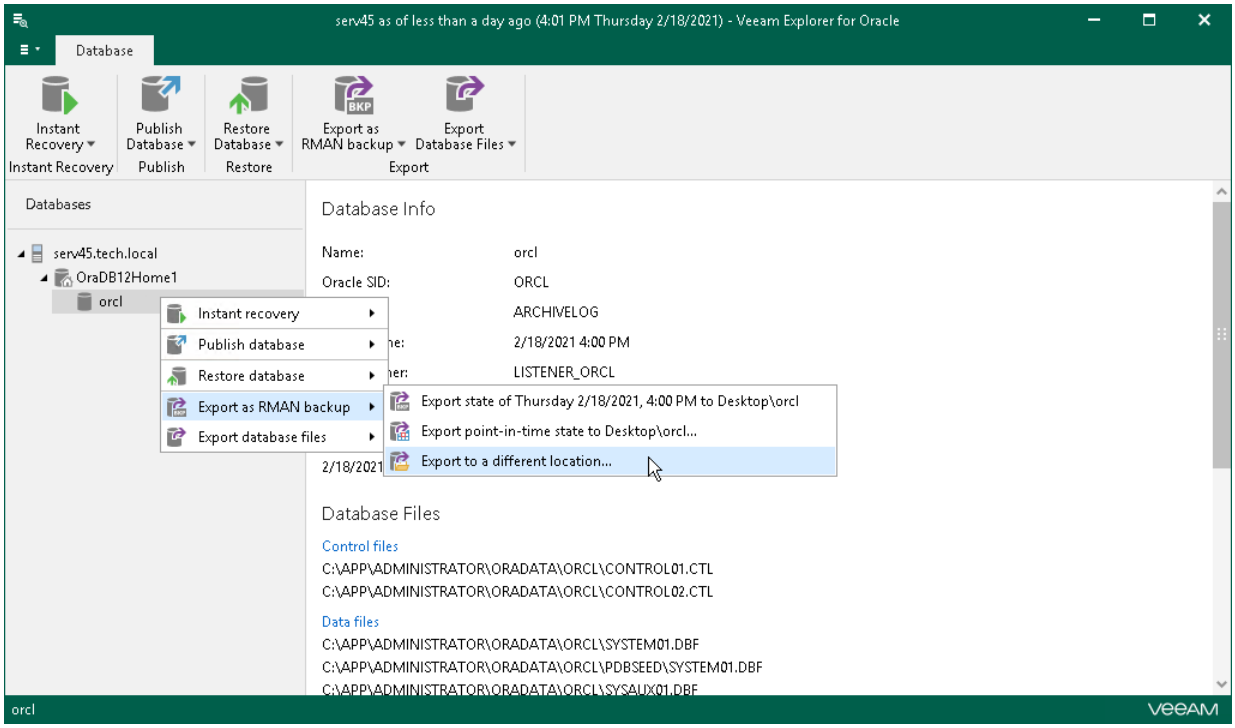
To export a database to a custom location, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup** > **Export to a different location** or right-click a database and select **Export as RMAN backup** > **Export to a different location**.



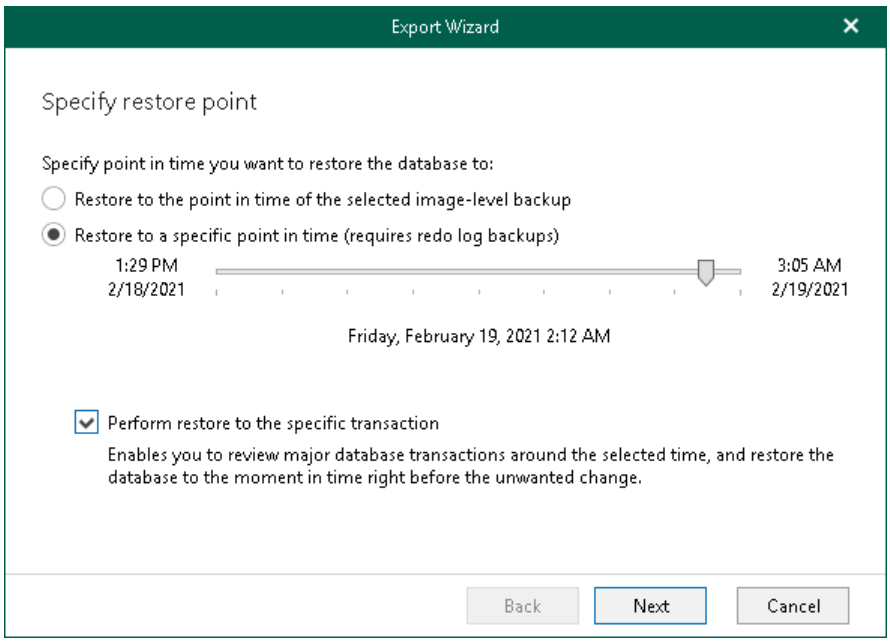
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

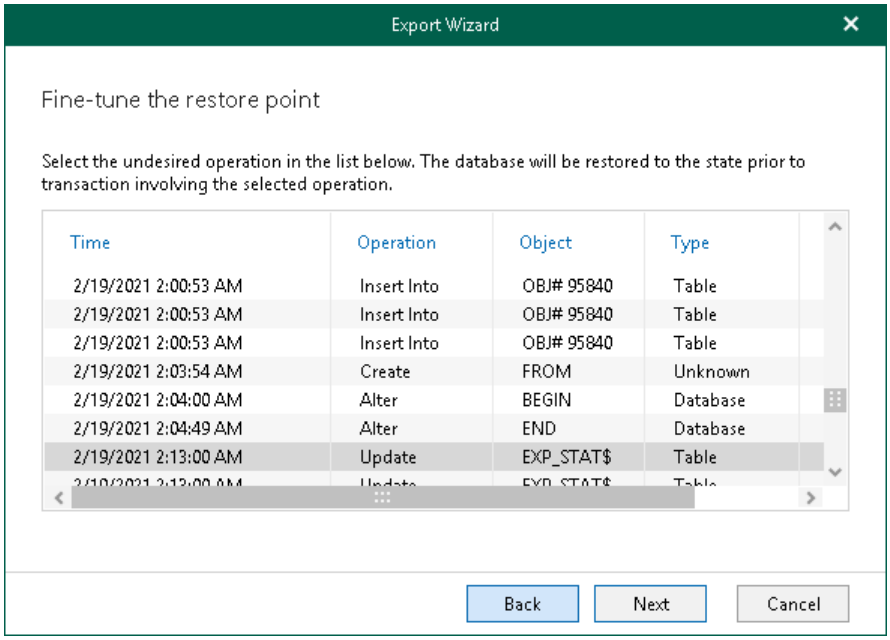
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target Location

At this step of the wizard, do the following:

1. In the **Export path** field, specify the location to which you want to export database files.

   If the folder you are specifying does not exist, it will be created.

2. In the **File name format** field, specify the format according to which your files will be named after the export.

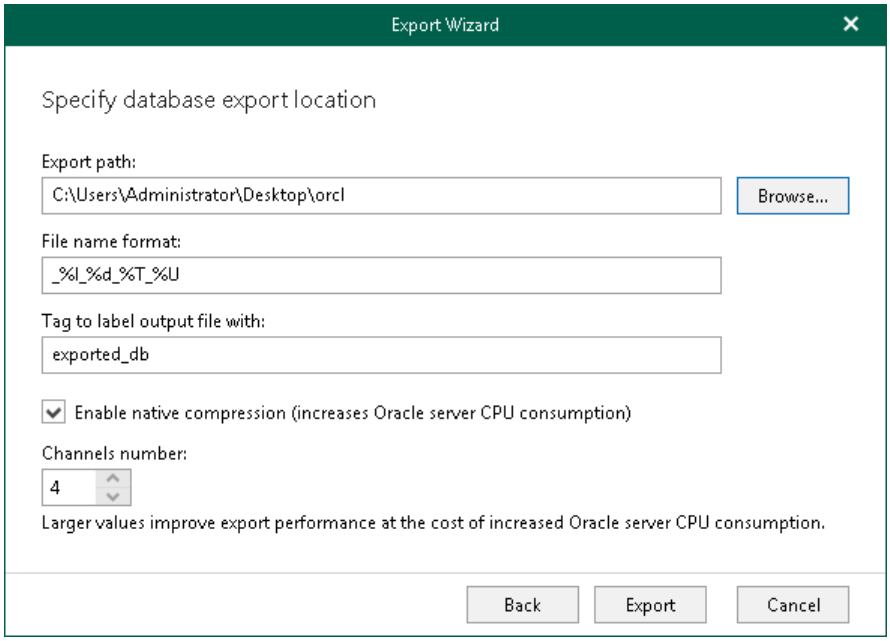
   For more information, see this Oracle article.

3. In the **Tag to label output file with** field, specify a new tag name.

4. To compress files using native Oracle compression, select the **Enable native compression** check box.

5. In the **Channels number** numeric field, specify the number of channels to be used when retrieving Oracle databases from the backup.

6. Click **Export**.



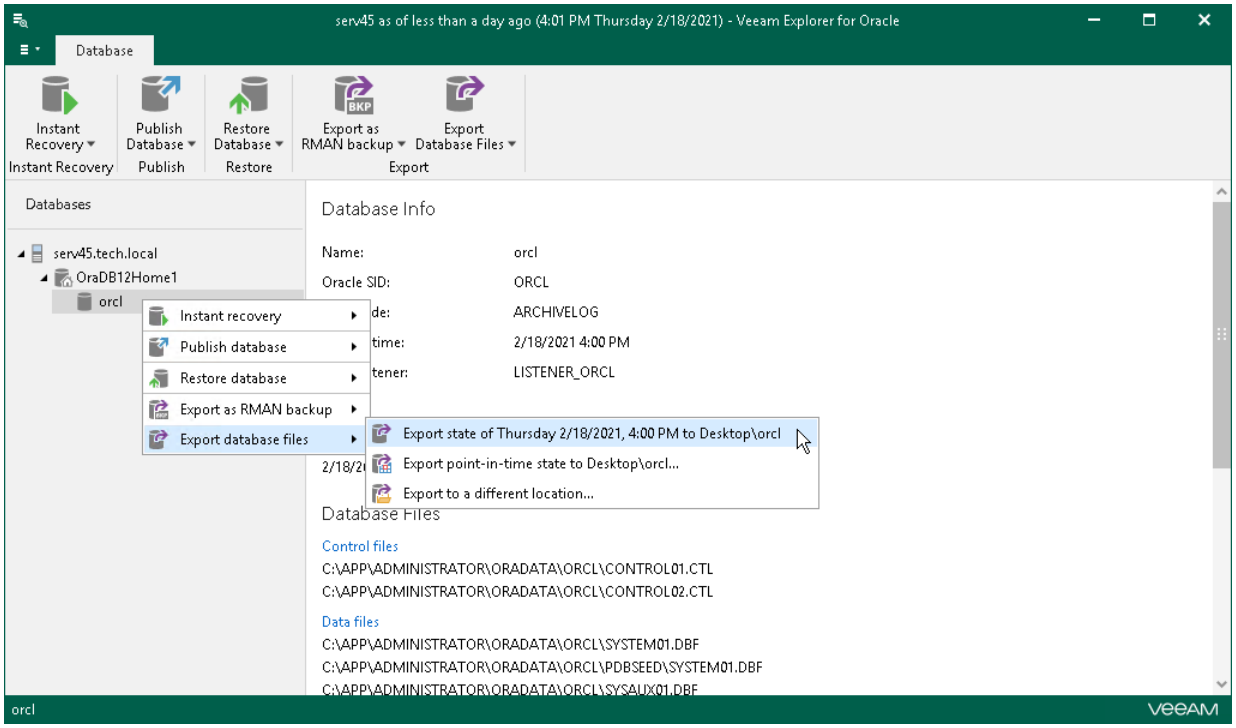
Export Database Files

Continue with this section to learn more about exporting Oracle databases.

Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export state of <point_in_time> to Desktop\<db_name>** or right-click a database and select **Export database files** > **Export state of <point_in_time> to Desktop\<db_name>**.
3. Wait until the export operation is complete.



Exporting Point-in-Time State

This section explains how to export data as of a point-in-time state.

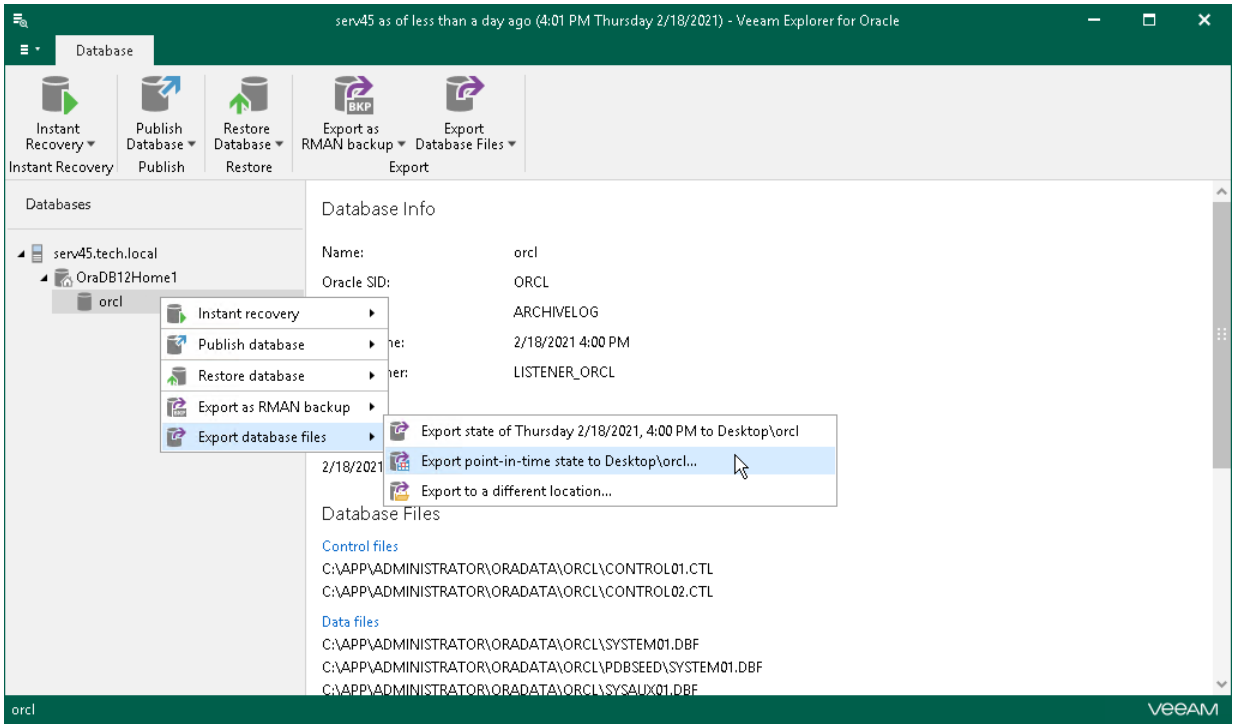
To export data as of a point-in-time state, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export point-in-time state to Desktop\<db_name>** or right-click a database and select **Export database files** > **Export point-in-time state to Desktop\<db_name>**.



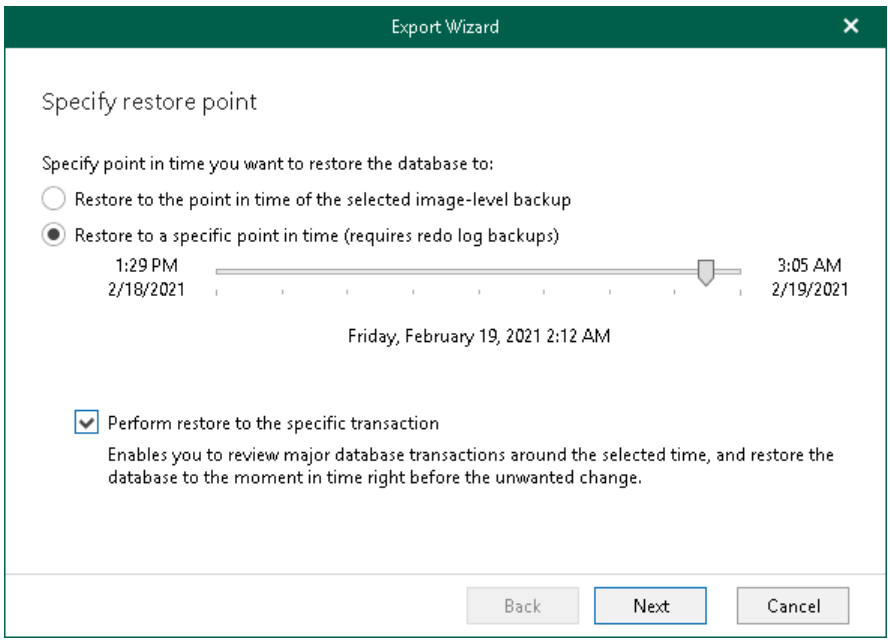
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

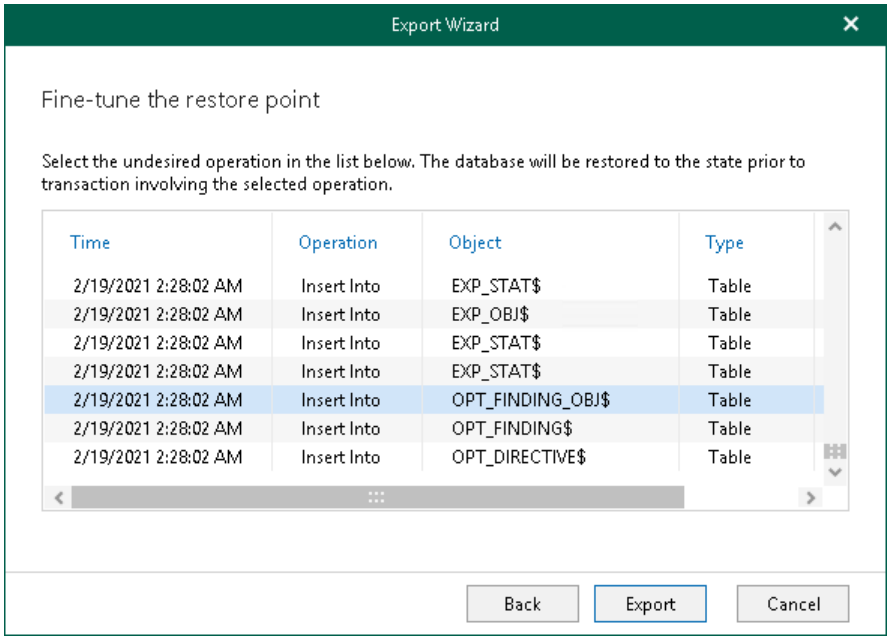
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Exporting to Custom Location

This section explains how to export a database to a custom location.

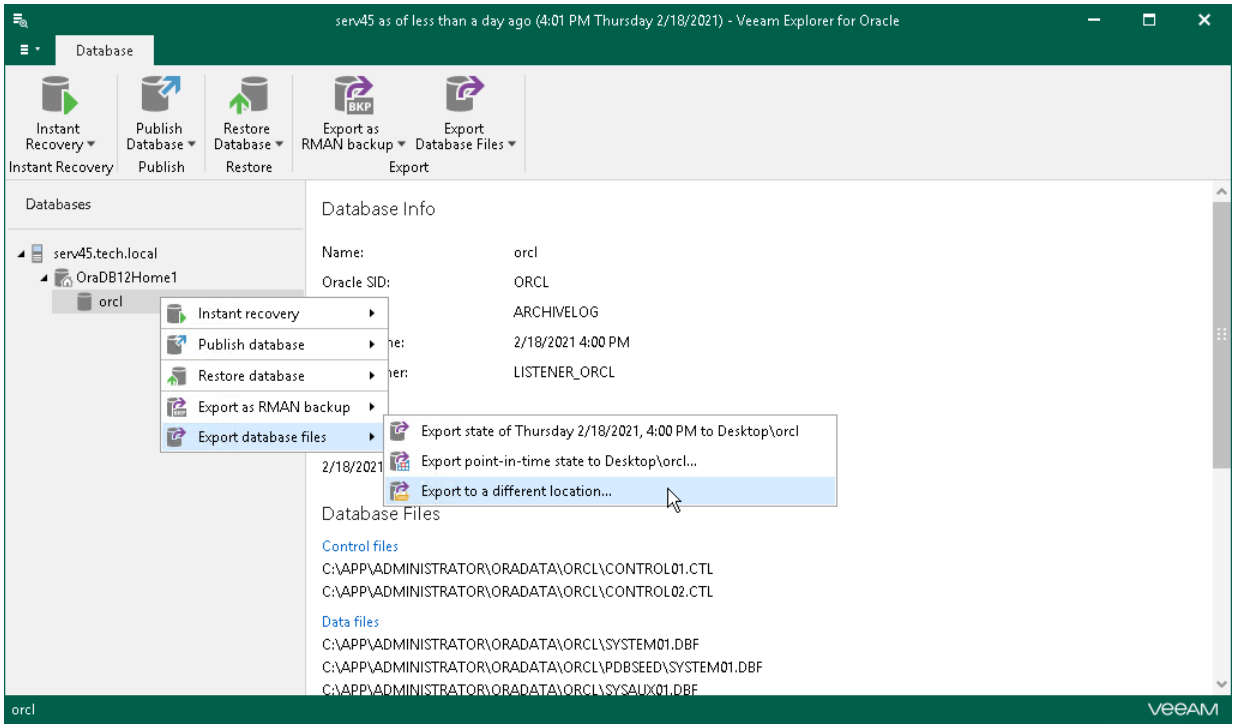
To export a database to a custom location, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export to a different location** or right-click a database and select **Export database files** > **Export to a different location**.



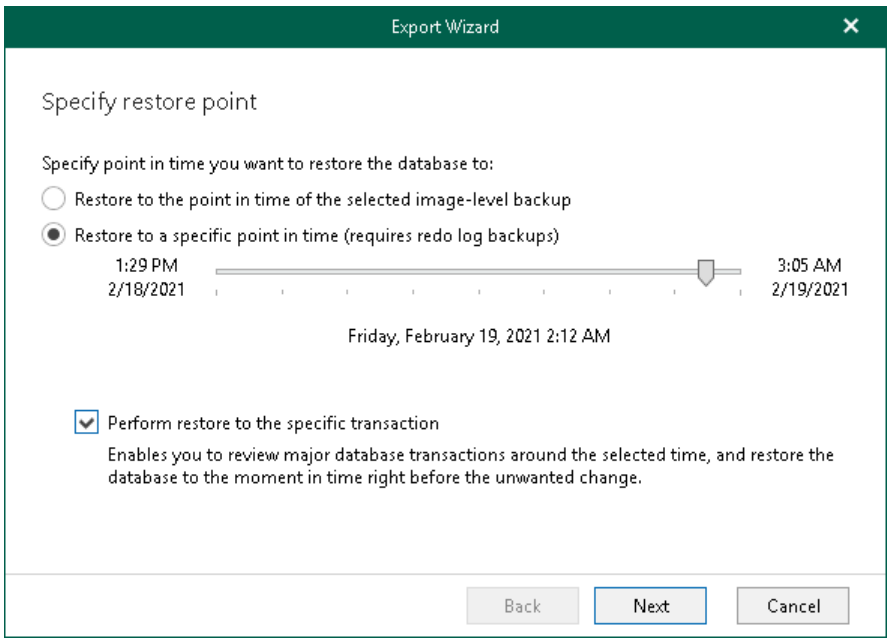
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

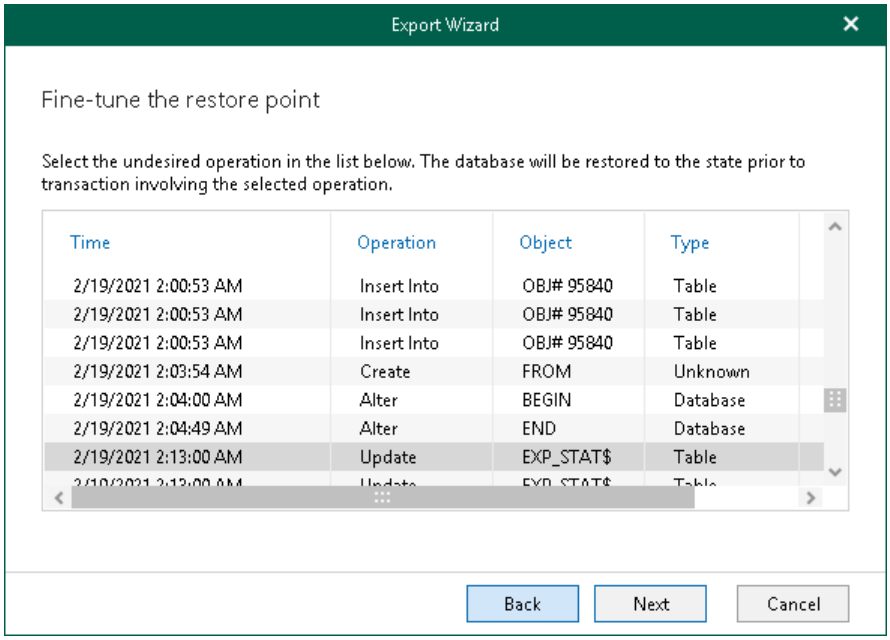
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

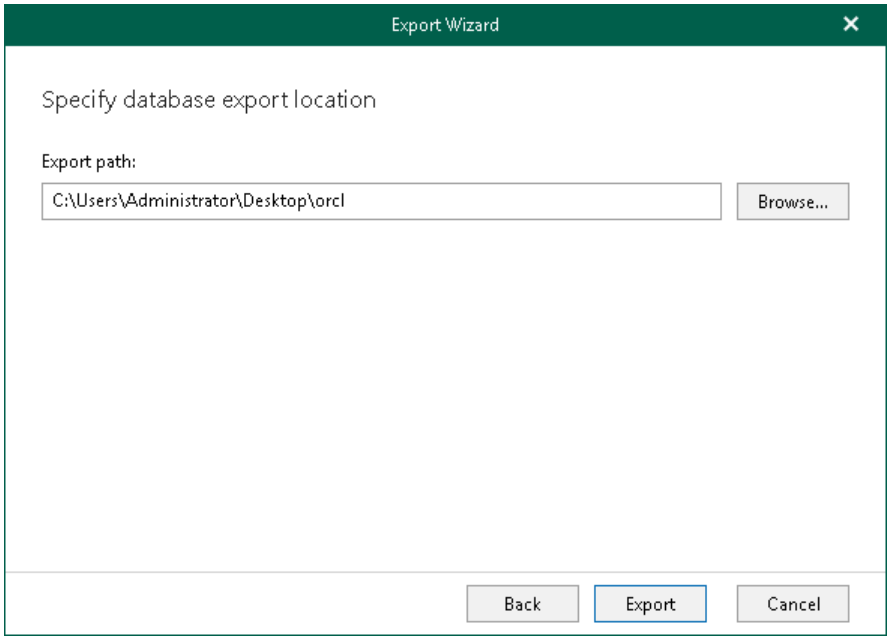
At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the previous step.



Step 4. Specify Target Location

At this step of the wizard, in the **Export path** field, specify the location to export data.



Veeam Explorer for Microsoft Exchange

Veeam Explorer for Microsoft Exchange allows you to restore and export Microsoft Exchange objects from backups created in Veeam Backup & Replication and Veeam Backup for Microsoft Office 365.

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft Exchange.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft Exchange.

Component	Requirement
Microsoft Exchange	For more information about supported versions of Microsoft Exchange, see: • The Supported Applications subsection of the Veeam Backup & Replication User Guide. • The System Requirements section of the Veeam Backup for Microsoft Office 365 User Guide.

Consider the following:

- To work with database files, Veeam Explorer for Microsoft Exchange requires a dynamic link library *ese.dll* supplied with Microsoft Exchange. The *ese.dll* file must be of the same version as that of Microsoft Exchange in which database files were created.
- To restore mailbox items from a server running Microsoft Windows ReFS, the Veeam backup server or a management console must be installed on the Microsoft Windows Server 2012 or higher.
- To restore mailbox items from a server running Microsoft Windows ReFS 3.x, Veeam backup server or a management console must be installed on the Microsoft Windows Server 2016.
- To restore data that was backed up by Veeam Backup for Microsoft Office 365 v1.5 via PowerShell, make sure to install Windows PowerShell 2.0 or higher.
- Restore of mailbox datastore from backups created by Veeam Agent for Microsoft Windows 2.0 (and higher) requires integration with Veeam Backup & Replication to be set up, as described in the Using with Veeam Backup & Replication section of the Veeam Agent for Microsoft Windows User Guide.

Used Ports

The following tables list network ports that must be opened to manage inbound/outbound traffic.

Backup

From	To	Protocol	Port	Notes
Veeam Backup Server / Guest Interaction Proxy (Enterprise and Enterprise Plus editions)	**Exchange Server VM Guest OS**	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on a VM guest OS.
Exchange Server VM Guest OS	**Veeam Backup Server / Guest Interaction Proxy (Enterprise and Enterprise Plus editions)**	TCP	6005 to 65535	The dynamic RPC range that is used by the runtime coordination process which is deployed on a VM guest OS for application-aware processing (when working over the network). Note that Exchange 2010 or higher (in particular, Client Access) expands standard Windows dynamic RPC port range to provide a better scalability. For more information, see this Microsoft article.

NOTE

Configuring dynamic RPC range is not required when using default Microsoft Windows firewall settings as Veeam Backup & Replication automatically creates an associated firewall rule for the runtime process during installation. When using custom firewall settings or if application-aware processing fails with the *RPC function call failed* error, make sure to configure dynamic RPC ports manually. For more information, see this Microsoft article.

Restore

From	To	Protocol	Port	Notes
Veeam Backup Server /	**Microsoft Exchange 2003/2007 CAS Server**	TCP	80, 443	Ports used for WebDAV connections.

From	To	Protocol	Port	Notes
Standalone Console	Microsoft Exchange 2010/2013/2016/2019 CAS Server	TCP	443	Port used for Microsoft Exchange web services connections.

Required Permissions

The following table lists required permissions for user accounts to back up and restore Microsoft Exchange data.

Operation	Required Roles and Permissions
Backup	For more information, see: • The Required Permissions section of the Veeam Backup & Replication User Guide. • The Required Permissions section of the Veeam Backup for Microsoft Office 365 User Guide.
Restore to Microsoft Office 365 and on-premises Microsoft Exchange from backups created in Veeam Backup & Replication and Veeam Backup for Microsoft Office 365	To restore data to Microsoft Office 365 and on-premises Microsoft Exchange, make sure to configure user accounts as follows: **Restore to a Public Folder** • The account being used must own a mailbox on a target Microsoft Exchange server. • The account must be assigned the *Organization Management* role on a target Microsoft Exchange server. See Assigning Organization Management Role. • [For restore of *In-Place Hold Items* to the original location] If the *In-Place Hold Items* folder already exists, make sure the account being used can create, modify and delete items. If the *In-Place Hold Items* folder does not exist, the account being used must be able to create folders under the *All Public Folders* root node. **Restore to a Mailbox** • If the account owns a mailbox, make sure it has *Full Access.* • If the account does not own a mailbox, then access must be granted through impersonation. See Granting Full Access. **Restore Using Modern App-Only Authentication Method** The account used to log in to Microsoft Office 365 must be assigned the following roles: • *ApplicationImpersonation* role. For more information, see this Microsoft article. • *Global Administrator* or *Exchange Administrator* role. Also make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Required Azure AD Application Settings section of the Veeam Backup for Microsoft Office 365 User Guide.

Examples

Assigning Organization Management Role

To assign the *Organization Management* role, use the following cmdlet.

```
Add-RoleGroupMember "Organization Management" -Member "<user_account>"
```

For more information about the *Add-RoleGroupMember* cmdlet, see this Microsoft article.

Granting Full Access

To grant *Full Access* to the account that owns a mailbox, use the following cmdlet.

```
Add-MailboxPermission -Identity "<target_mailbox>" -User "<user_account>" -Acce
ssRights FullAccess -InheritanceType All
```

For more information about the *Add-MailboxPermission* cmdlet, see this Microsoft article.

To grant *Full Access* to the account that do not own a mailbox (i.e. through impersonation), use the following cmdlet.

```
New-ManagementRoleAssignment -Name "<role_name>" -Role ApplicationImpersonation
-User "<user_account>"
```

For more information about the *New-ManagementRoleAssignment* cmdlet, see this Microsoft article.

Recalling Given Permissions

To recall given access level, run either of the following cmdlets.

```
Remove-ManagementRoleAssignment "<role_name>"
```

```
Remove-ManagementRoleAssignment -Identity <role_name>
```

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware image processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication user guide.

> **NOTE**
>
> By default, Exchange transaction logs will be truncated upon successful backup. To keep transaction logs for further processing by a third-party application, select the Exchange server VM from the list, click **Edit** and on the **General** tab select **Perform copy only**.

Support for Database Availability Groups (DAG)

Veeam Backup & Replication supports any configuration of DAGs. In particular, having all the databases active on a single node or with the active databases on each node. Transaction logs will be truncated on all DAG members.

For more information and recommendations, see the following articles:

- How to virtualize and protect Exchange 2016
- Veeam Knowledge Base article

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft Exchange.

General

- When Veeam Explorer for Microsoft Exchange is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft Exchange does not support restore via *PSDirect*, *VIX* or *Sphere API*.
- Sending objects that exceed 3 MB in size may fail. To fix this issue, install this Microsoft update.
- Multiple restore is not supported for public folders. Use per-object restore.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location, consider the following:
  - *In-Place Hold Items* restore is not supported for On-Premises Exchange Server 2013 due to EWS limitations.
  - To restore *In-Place Hold Items* of Exchange 2016 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with *DiscoveryHolds* system folder creation. Otherwise, restore will fail with the following error:

    "*Failed to restore In-Place Hold Items. Restore of In-Place Hold Items into Exchange 2013 is not supported*".

    For information on enabling *In-Place Hold* and *Litigation Hold*, see this Microsoft article.

> **NOTE**
>
> To use an internet proxy server to restore backups created in Veeam Backup for Microsoft Office 365, make sure to provide appropriate proxy server address and the port number. For that, go to the **Control Panel** > **Internet Options Connections** tab, click **LAN Settings**, select the **Use a proxy server for your LAN** check box and specify a proxy server you want to use. Credentials for such a proxy (if needed) will be taken from the **Control Panel** > **Credential Manager** > **Windows Credentials** console.
>
> Consider that this functionality is available only in Veeam Explorer for Microsoft Exchange that comes as part of the Veeam Backup for Microsoft Office 365 distribution package.

Export

- Export is available only if you have a 64-bit version of Microsoft Outlook 2019, Microsoft Outlook 2016, Microsoft Outlook 2013 or Microsoft Outlook 2010 installed on a computer with Veeam Explorer for Microsoft Exchange.
- To avoid conflicts during export, make sure to exclude .pst files from the indexing scope. Oftentimes conflicts may occur due to a file you are exporting is being indexed at the same time. When exporting to shared folders, exclude Outlook files or disable Windows search on the destination computer.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Exchange and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created in Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- The **Explore** option to load backups created in Veeam Backup for Microsoft Office 365.

  For more information, see the Data Restore section of the Veeam Backup for Microsoft Office 365 User Guide.

  When loading backups located in object storage repositories, Veeam Explorer for Microsoft Exchange will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To enable notifications, select the **Show pop-up notifications on startup** check box, as described in Configuring Advanced Settings.

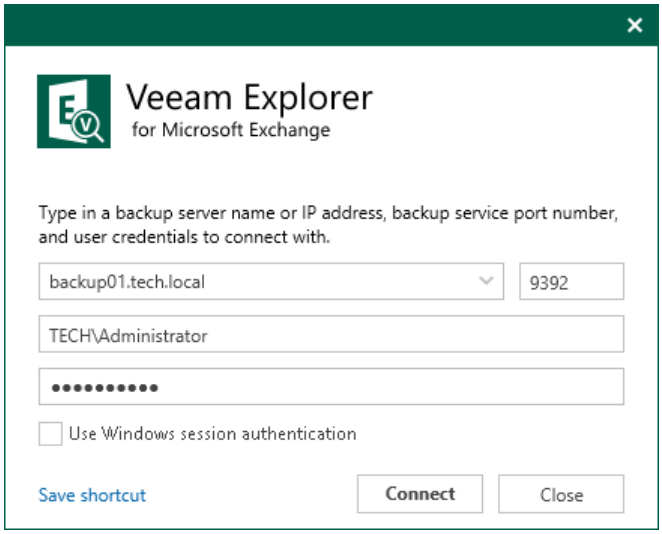
- Go to **Start**, click **Veeam Explorer for Microsoft Exchange** and manually open Microsoft Exchange databases, as described in Standalone Databases Management section.

If you open Veeam Explorer for Microsoft Exchange from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

- The domain name or IP address of a server to which you want to connect
- The port number
- User credentials

  The account must be a member of the *Local Administrator* group on a target server. To use your current account, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



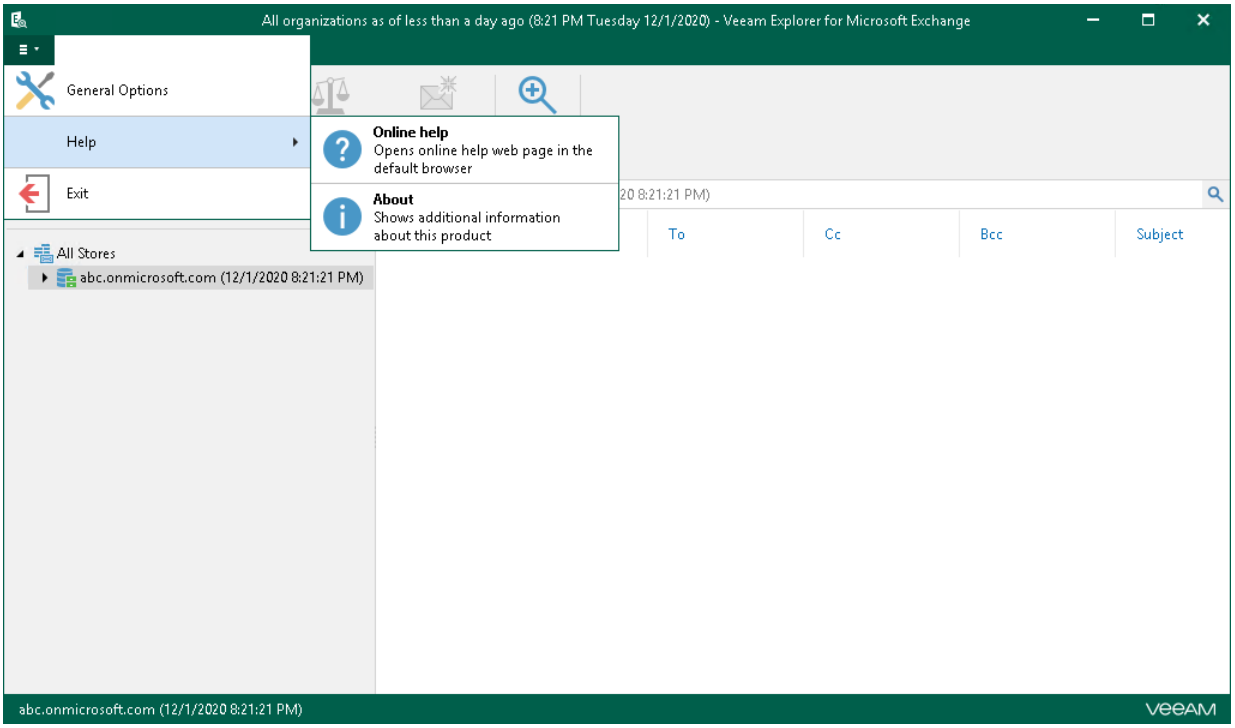
Understanding User Interface

Veeam Explorer for Microsoft Exchange provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

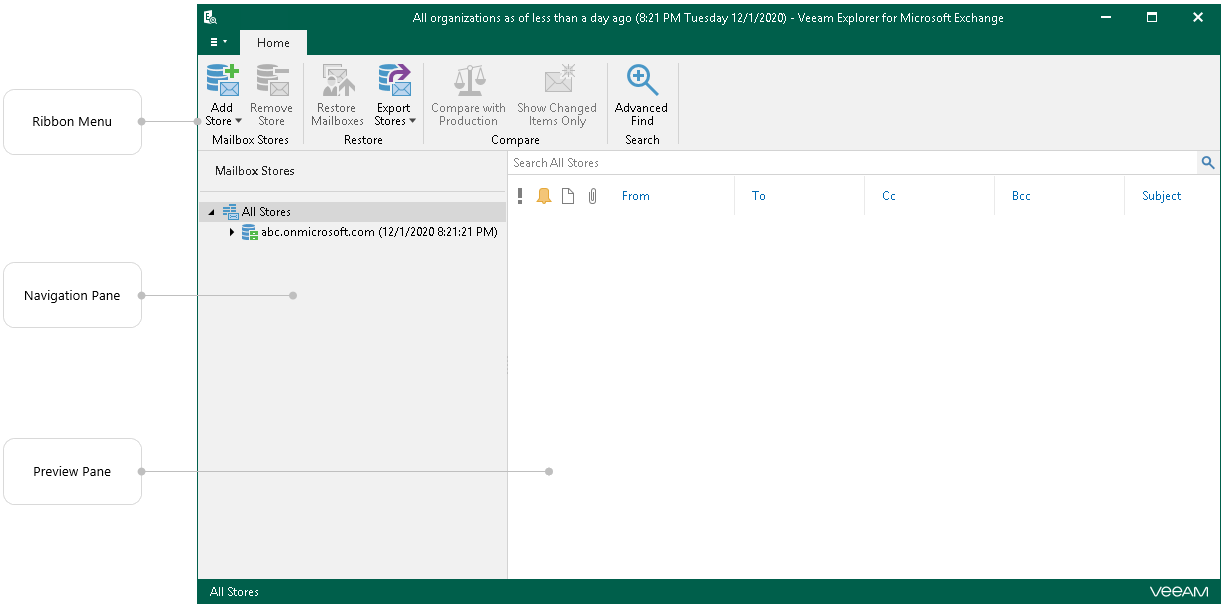
- **General Options**. Allows you to configure program options.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows information about the product.
- **Exit**. Closes the program.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

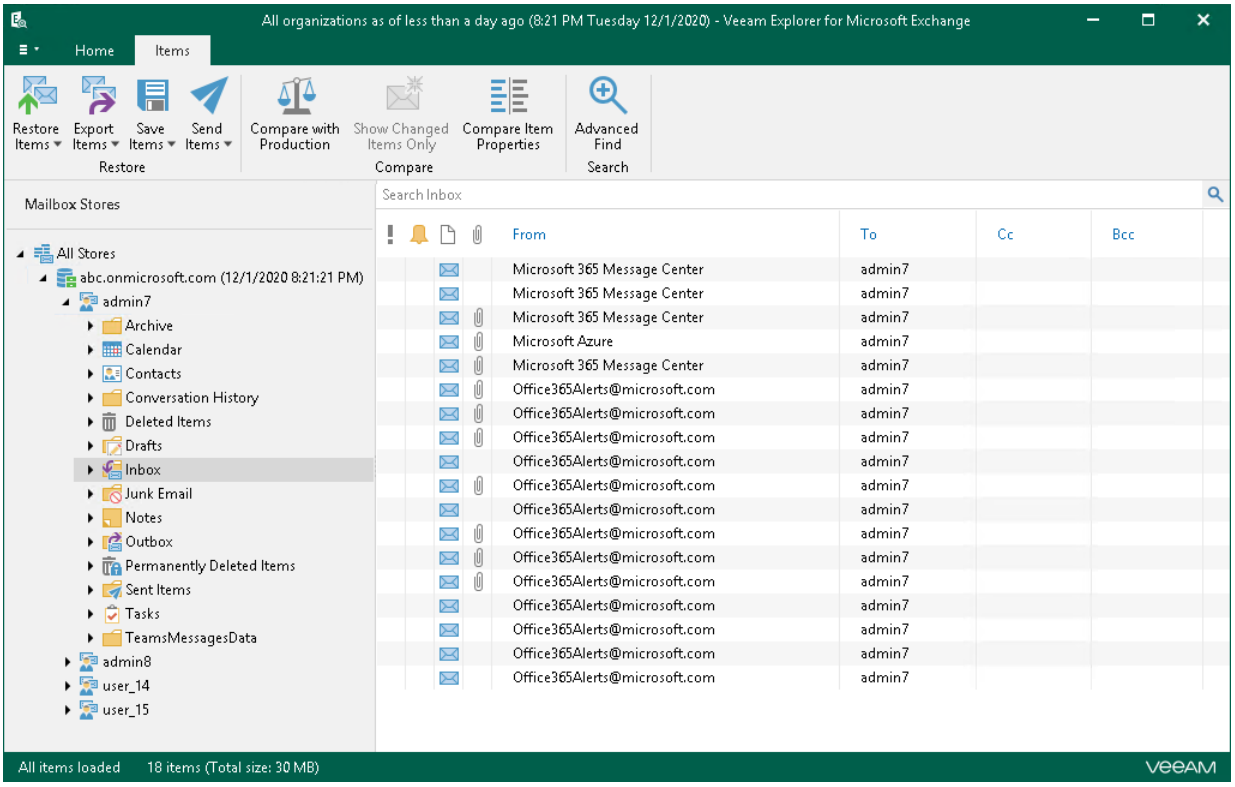
Continue with this section to learn about:

- Browsing backup content
- Opening Messages
- Searching for objects in a backup file
- Using advanced search

Browsing

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your Exchange objects.

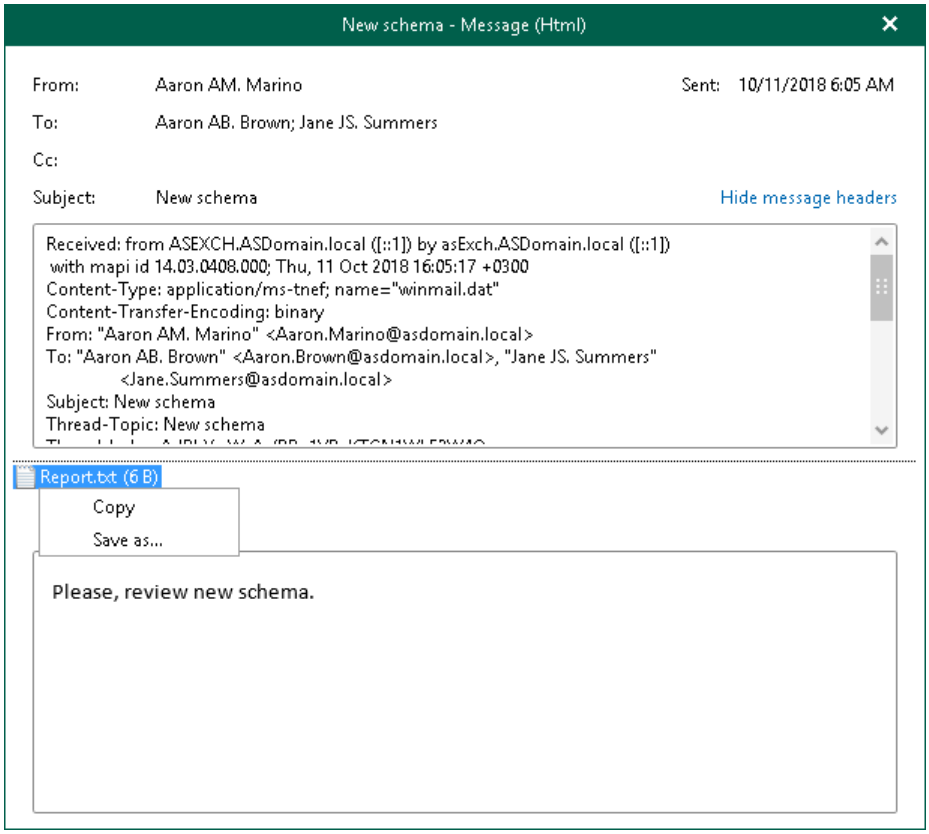
After you select an object in the navigation pane, you can see its content in the preview pane.



Opening Messages

To open a message, right-click a message in the preview pane and select **Open**. You can also double-click a message:

- To show message headers, click **Show message headers**.
- To open attachments, double-click an attachment or right-click an attachment and select **Open**.
- To save attachments, right-click an attachment and select **Save as**.



Searching

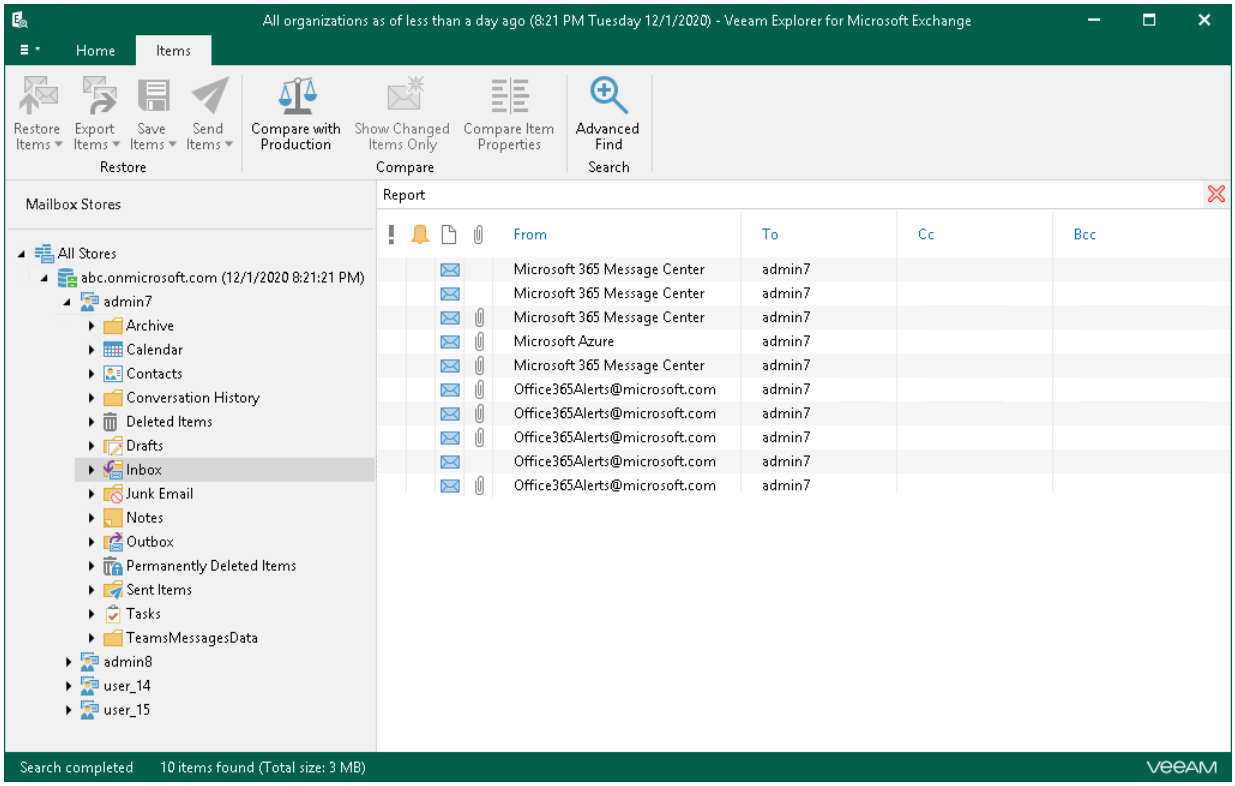
The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane. select an object in which you want to find data.
2. Enter a search query to the search field at the top of the preview pane.

> **NOTE**
>
> To find the exact phrase, use double quotes. For example: *"Office 365"*.

You can narrow search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



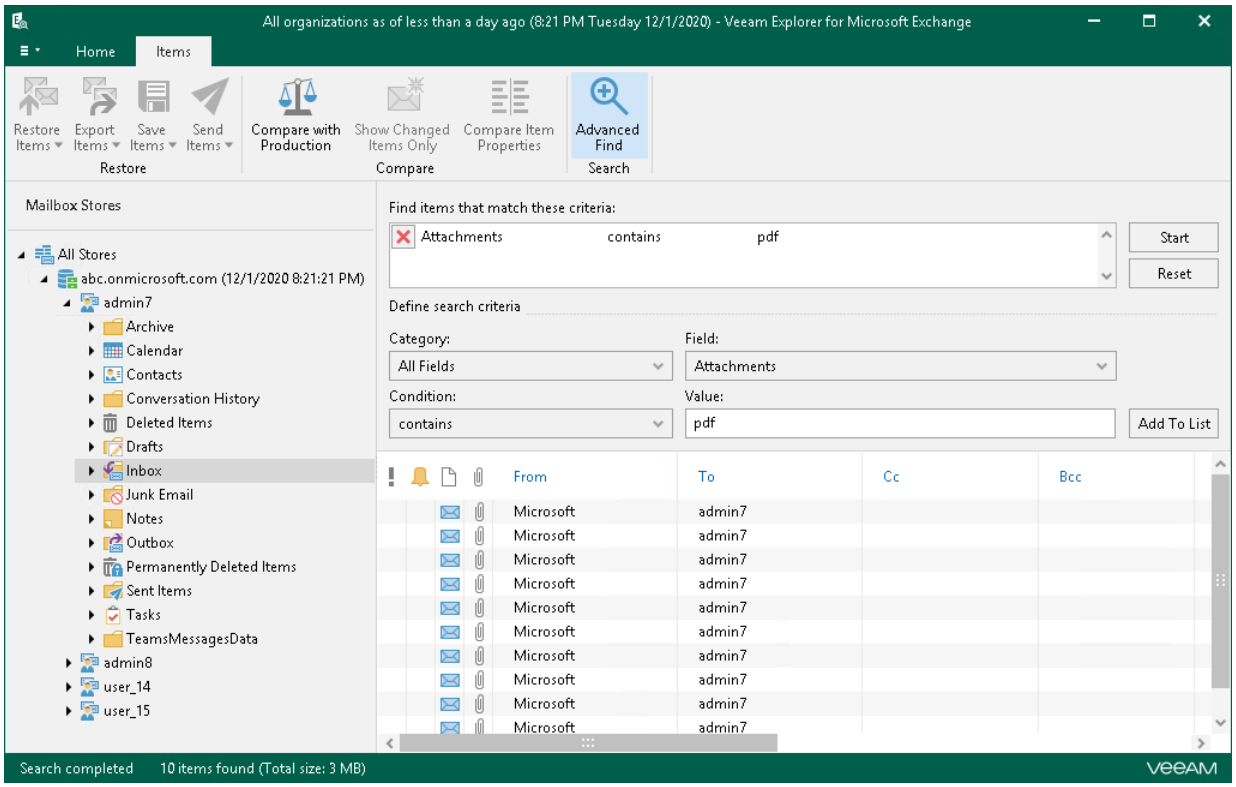
Using Advanced Find Capabilities

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find messages with the subject *Report*, do the following:

1. In the preview pane, select a node and click **Advanced Find**.
2. In the **Define search criteria** section, select **Category** > **All fields**.
3. In the **Field** list, select **Subject**.
4. In the **Condition** list, select **Contains**.
5. In the **Value** field, specify a substring to look for.
6. Click **Start**.

To remove a filter, click the cross mark on the left. To remove all configured filters, click **Reset**.



General Application Settings

Continue with this section to learn more about configuring required application settings and components.

Configuring Extensible Storage Engine

To work with database files, Veeam Explorer for Microsoft Exchange requires a special dynamic link library `ese.dll`, which is shipped with Microsoft Exchange.

The `ese.dll` file must be of the same version as the Microsoft Exchange application with which your database files were created. When restoring a VM that was backed up with application-aware image processing, the `ese.dll` file will be located automatically.

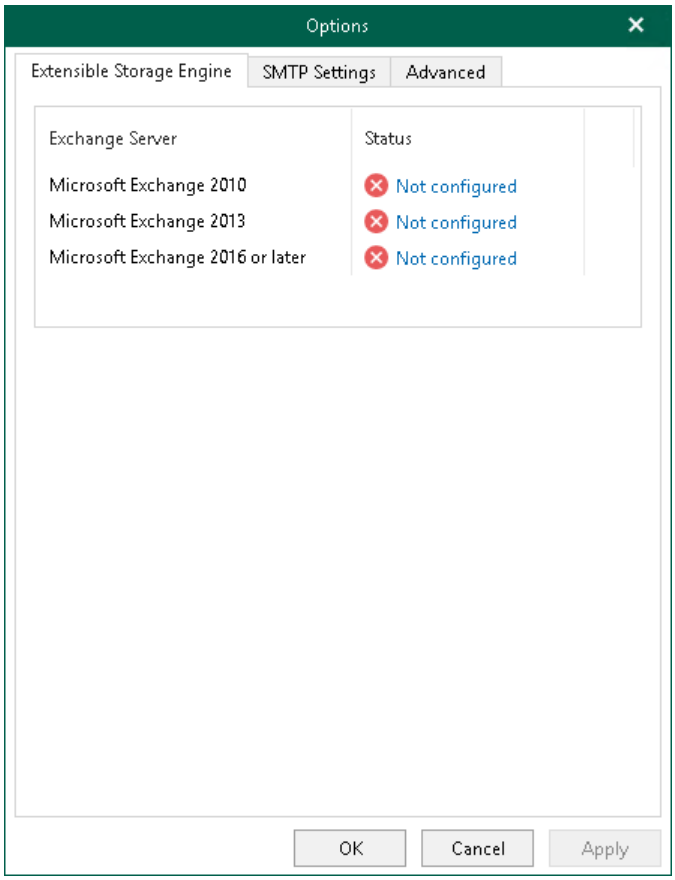
The following versions of Microsoft Exchange are supported:

- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013
- Microsoft Exchange 2010 SP1, SP2 and SP3

To specify the path to the `ese.dll` file, do the following:

1. Go to the main menu and click **General Options**.
2. Got to the **Extensible Storage Engine** tab.
3. Click the link next to the Microsoft Exchange version and specify the path to the `ese.dll` file.

   This file can be found on the Microsoft Exchange Server distribution CD in the *X:|Setup|ServerRoles|Common|ese.dll* directory or in the installation directory of the Microsoft Exchange server.

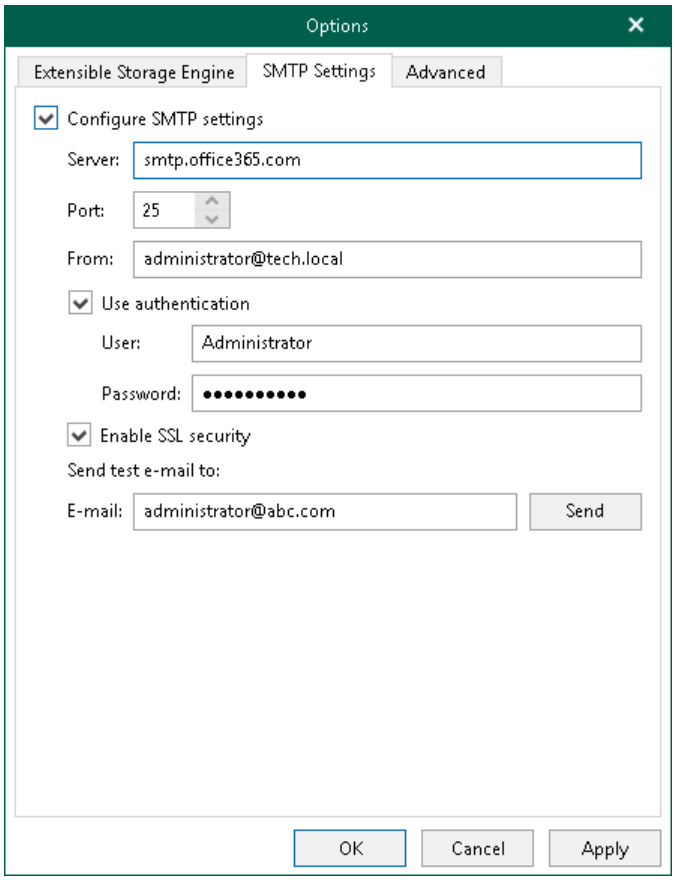


Configuring SMTP Settings

To send Microsoft Exchange items, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **SMTP Settings** tab, select the **Configure SMTP settings** check box and do the following:
   - In the **Server** field, specify a DNS name or IP address of the mail server.
   - In the **Port** field, specify the SMTP port of the specified mail server.
   - In the **From** field, specify the address that will be shown as the sender of an email.
   - Select the **Use authentication** check box if the specified SMTP server requires SMTP authentication for outgoing traffic, and provide valid credentials.
   - Select the **Enable SSL security** check box to enable SSL data encryption.
3. Click **Send** to send a test email message.
4. Click **Apply**.



Configuring Advanced Settings

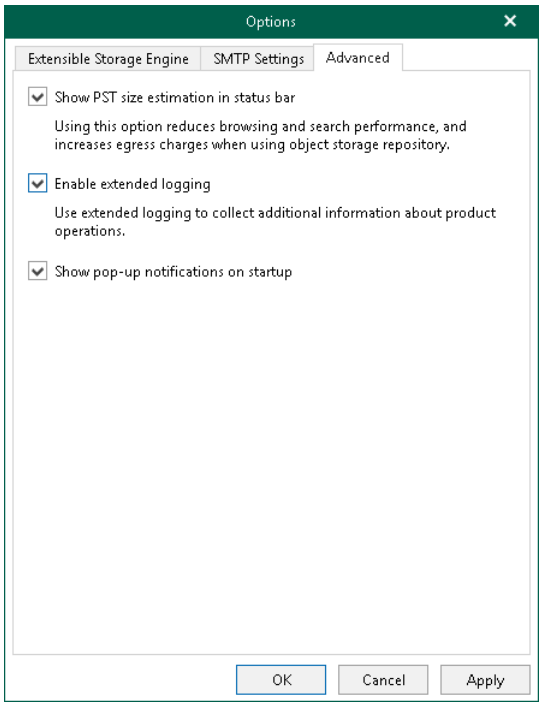
This section explains how to configure advanced settings of the application.

To configure advanced settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Advanced** tab.
3. If you want to see the estimated size of the Outlook database file in the status bar, select the **Show PST size estimation in status bar** check box.
4. If you want to enable extended logging mode to collect logs that contain more details on specific operations, select the **Enable extended logging** check box.

   After enabling extended logging mode, you can go back to the application and perform actions for which you want to collect additional information. Then you can collect logs.
5. By default, Veeam Explorer for Microsoft Exchange displays notifications when loading backups from object storage repositories. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.

   Applicable to backups created in Veeam Backup for Microsoft Office 365.



Standalone Databases Management

Continue with this section to learn more about adding and removing Microsoft Exchange databases.

Veeam Explorer for Microsoft Exchange supports adding databases created with the following Microsoft Exchange versions:

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2010 SP1, SP2 or SP3

If you back up Microsoft Exchange data with Veeam Backup for Microsoft Office 365, you can also add backups created with the product to Veeam Explorer for Microsoft Exchange in the similar way as standalone Microsoft Exchange databases. For more information, see Adding Microsoft Exchange Stores.

Adding Microsoft Exchange Stores

This section explains how to add Microsoft Exchange databases manually.

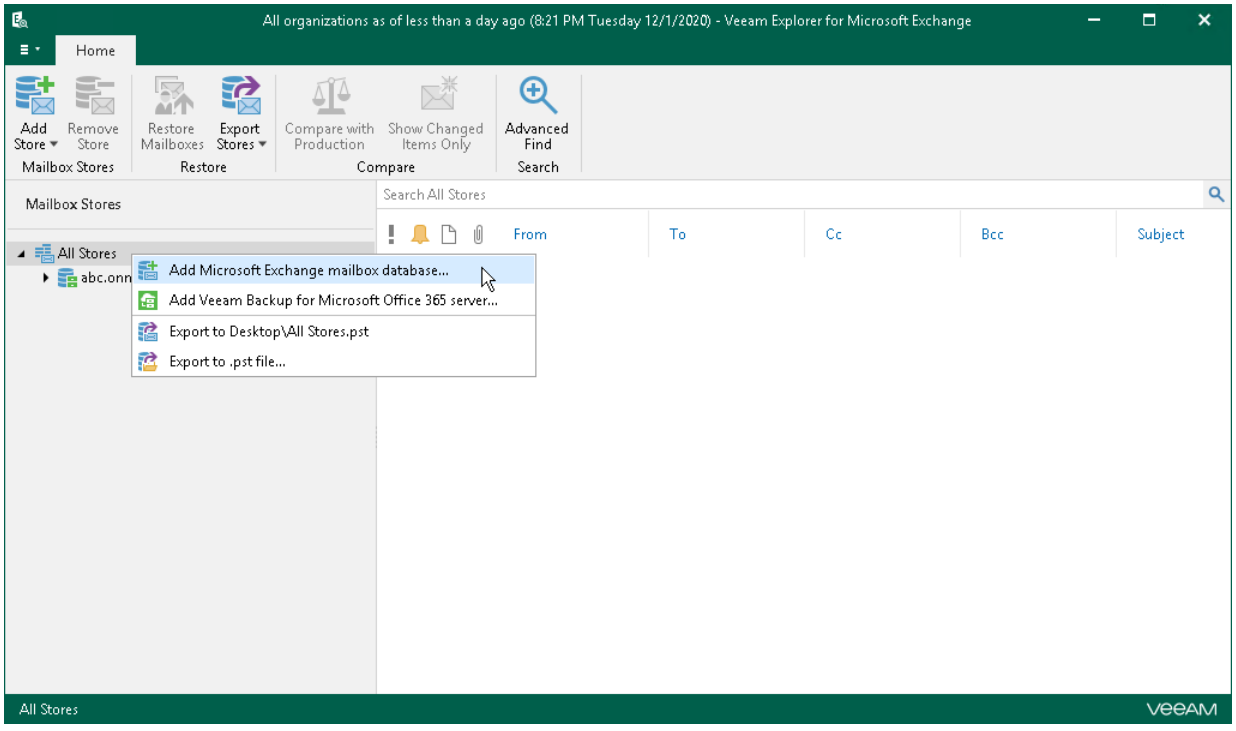
Consider the following:

- Before you add databases, make sure that Veeam Explorer for Microsoft Exchange has access to the `ese.dll` file. For more information, see Configuring Extensible Storage Engine.
- If a database is in *Dirty State*, you will have to recover it by applying log files. Click **Recover** and wait until log files are applied, then re-add the database. Make sure that the **Write** permission is granted to the account that you use to connect to the database.

To manually add a Microsoft Exchange database file (`.edb`) to the application scope, do the following:

1. On the **Home** tab, click **Add Store** > **Microsoft Exchange mailbox database** or right-click the **All Stores** node and select **Add Microsoft Exchange mailbox database**.
2. Click **Browse** to specify the path to the `.edb` and Exchange logs folder.

If you use Veeam Backup for Microsoft Office 365, you can also add Microsoft Exchange data backed-up with the product to the application scope. To do this, specify a path to the `repository.adb` backup file.

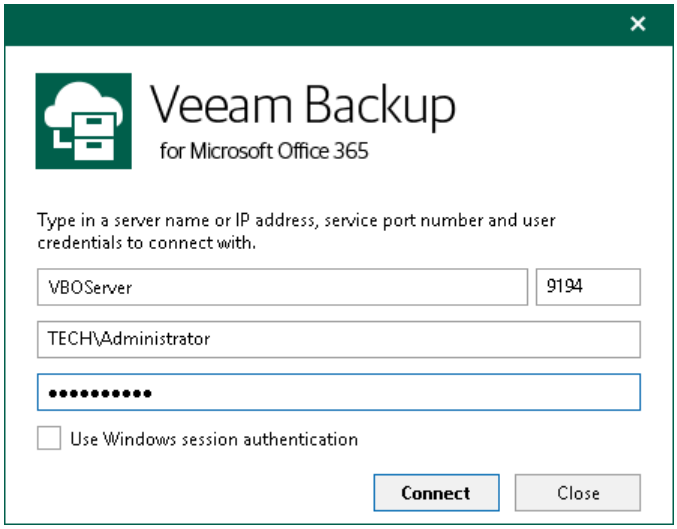


Adding Veeam Backup for Microsoft Office 365 Server

You can use the Veeam Explorer for Microsoft Exchange abilities to connect to another Veeam Backup for Microsoft Office 365 server and add its databases to the Veeam Explorer for Microsoft Exchange scope.

To add Veeam Backup for Microsoft Office 365 server that stores Microsoft Office 365 organization data, do the following:

1. On the **Home** tab, click **Add Store** > **Veeam Backup for Microsoft Office 365 server** or right-click the **All Stores** node in the navigation pane and select **Add Veeam Backup for Microsoft Office 365 server**.
2. Specify connection settings under which to connect to the Veeam Backup for Microsoft Office 365 server and click **Connect**.



Adding Veeam Backup for Microsoft Office 365 Service Provider

You can use Veeam Explorer for Microsoft Exchange to connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.

Consider the following:

- Both Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication must be installed on the same server.
- At least one service provider must be added to Veeam Backup & Replication, as described in the Connecting to Service Providers section of the Veeam Cloud Connect Guide.

To connect to a Veeam Backup for Microsoft Office 365 service provider, do the following:

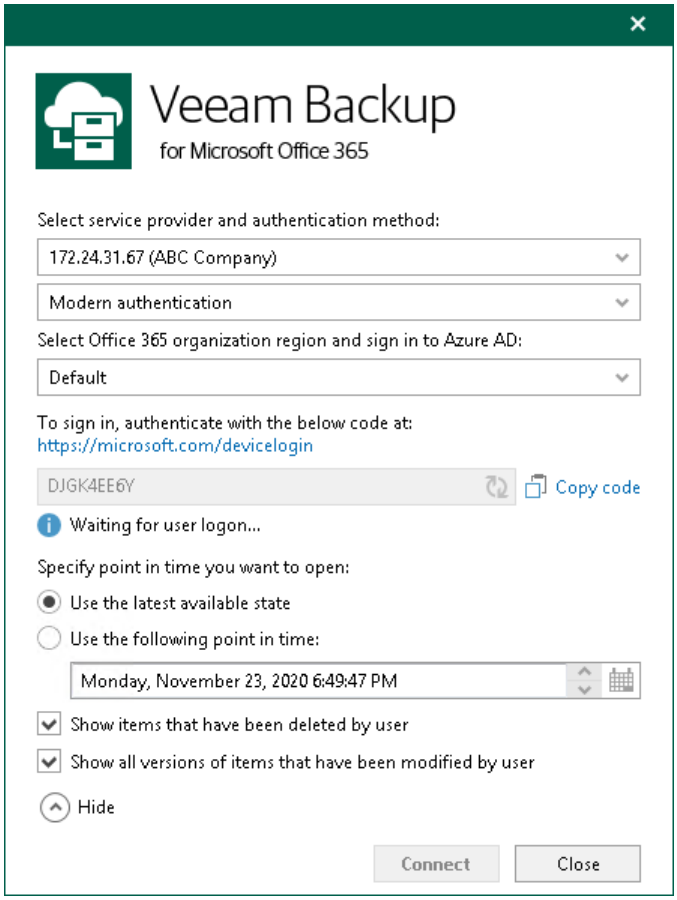
1. From the **Start** menu, launch Veeam Explorer for Microsoft Exchange.
2. On the ribbon, click **Add Store** > **Veeam Backup for Microsoft Office 365 service provider**.

   Alternatively, in the preview pane, right-click **All Stores** and select **Add Veeam Backup for Microsoft Office 365 service provider**.
3. In the **Select service provider and authentication method** section, select from the drop-down lists a service provider to which you want to connect and an authentication method: *Modern authentication* or *Basic authentication*.
4. [For *Modern authentication*] Select a region to which an Office 365 organization of the selected service provider belongs.
5. [For *Modern authentication*] Copy the device code and use it to sign in to Microsoft Azure Active Directory.

   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. If you want to select a point-in-time state as of which you want to load Office 365 backups, click **Specify point in time** and select the necessary option:
   - **Use the latest available state**. To load data as of the latest backup state.
   - **Use the following point in time**. To load data as of the selected point in time.

     To select a point in time, use the calendar control.

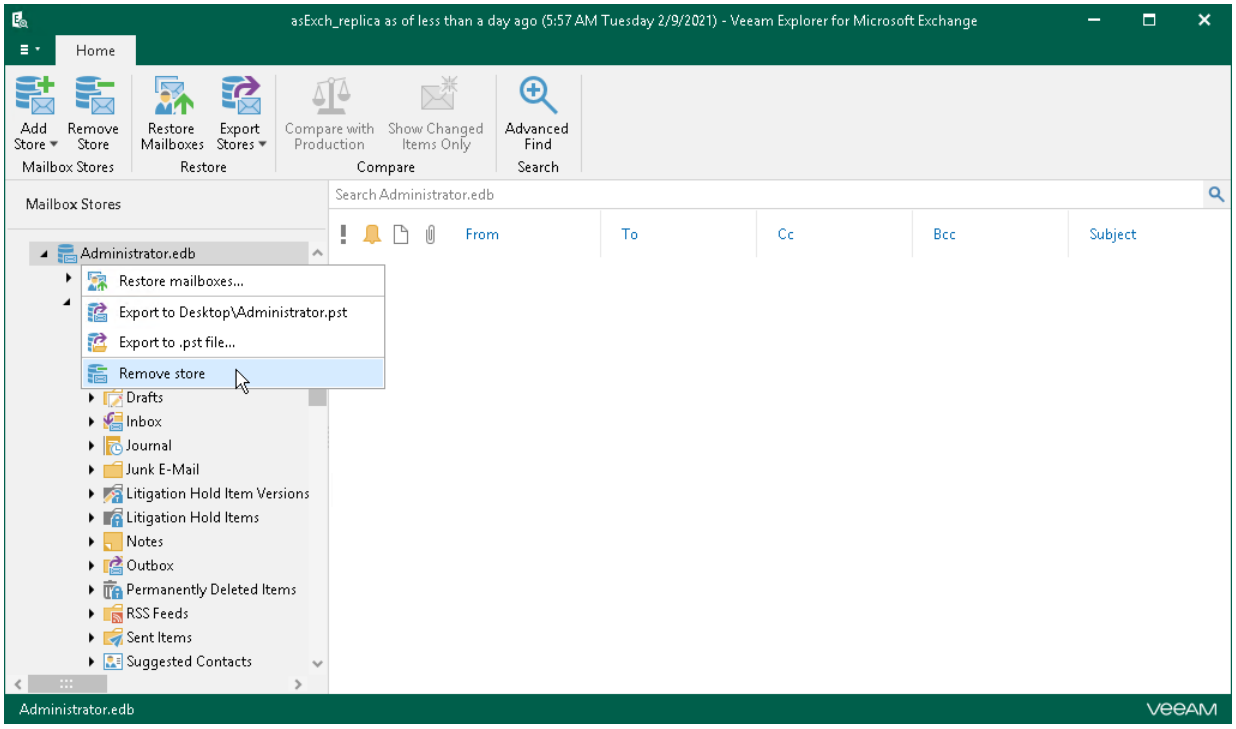
7. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
8. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.
9. Click **Connect**.



Removing Standalone Databases

Veeam Explorer for Microsoft Exchange allows you to remove an Exchange store from the application scope when you no longer need it.

To remove a store from the application scope, right-click a store in the navigation pane and select **Remove store**.



Data Restore

Continue with this section to learn more about restoring Microsoft Exchange data.

> **TIP**
>
> Before restoring data, make sure to read Considerations and Limitations.

Restore to Office 365 Organizations

This section explains how to restore data to Microsoft Office 365 organizations with enabled multi-factor authentication (MFA) and/or security defaults.

For more information, see the Microsoft Office 365 Organizations section of the Veeam Backup for Microsoft Office 365 User Guide.

When you perform a restore, you can specify a target mailbox, choose an authentication method that you want to use for a restore, specify a target folder to which you want to restore data and configure restore options.

You can also use 1-Click Restore if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folders and Items

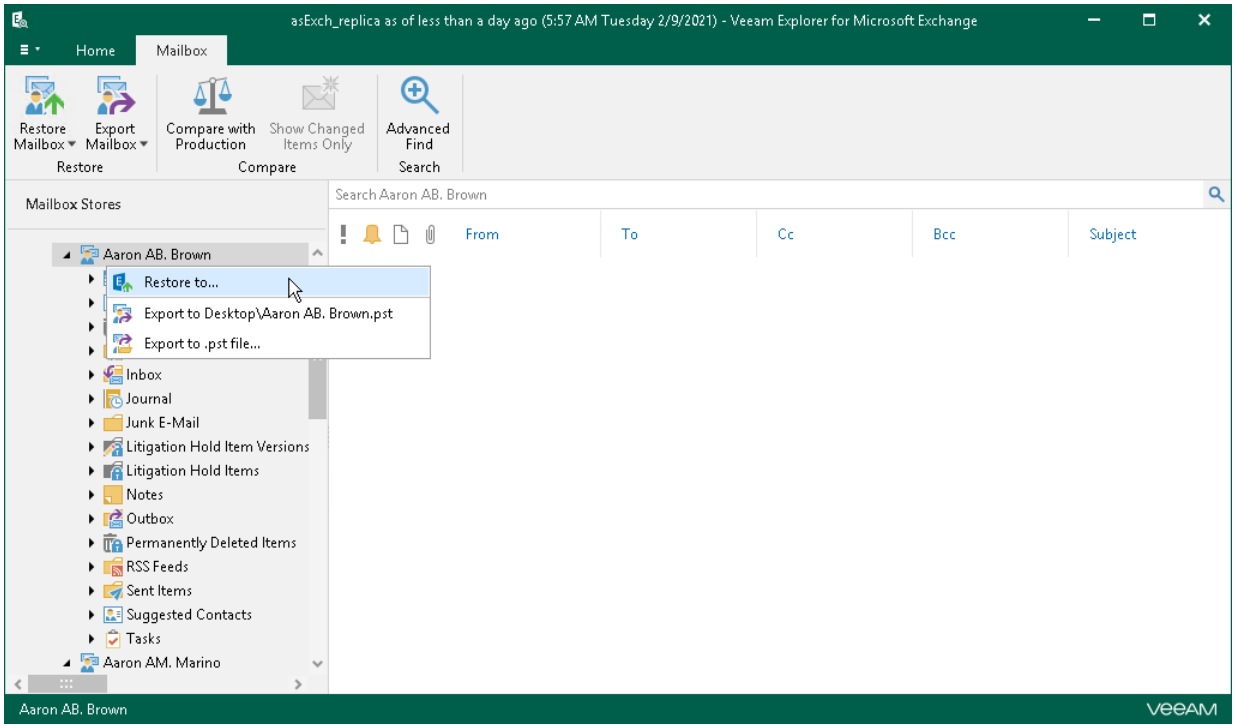
To restore the selected Exchange mailbox, do the following:

1. Launch the Restore wizard.
2. Specify a target mailbox.
3. Select an authentication method.
4. Log in to Office 365.
5. Specify a CAS server.
6. Specify a target folder.
7. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item** > **Restore to** or right-click a mailbox, folder or an item and select **Restore to**.



Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

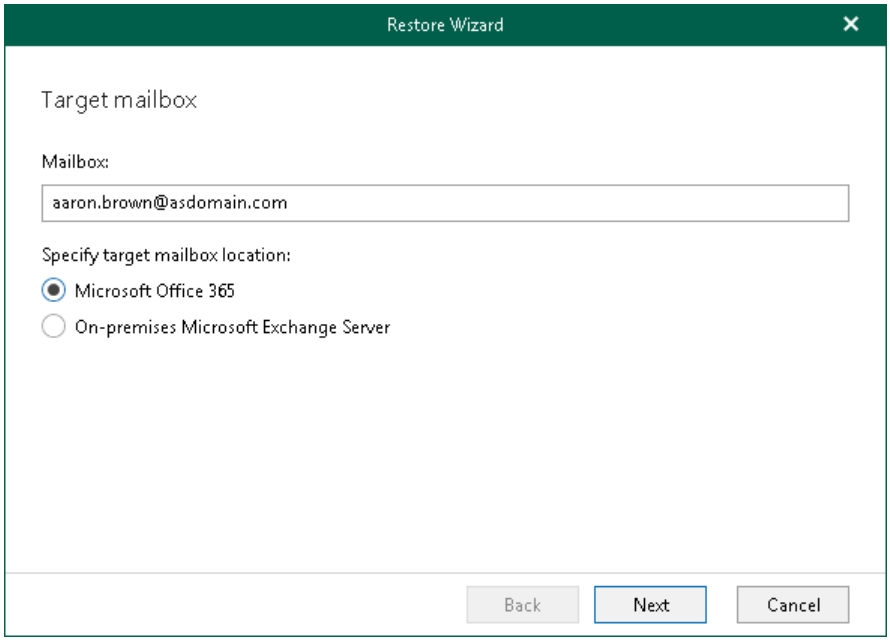
To specify mailbox settings, do the following:

1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.

   You can specify any name that you want. You can also restore a mailbox to a different organization. For example, you have backed up a mailbox *administrator@abc.onmicrosoft.com*. To restore such a mailbox to a different organization, you can specify, for example, *administrator@xyz.onmicrosoft.com* to restore a mailbox to the *xyz.onmicrosoft.com* organization.

2. Select **Microsoft Office 365** to restore the specified mailbox to an Exchange Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft Office 365 Organizations section of the Veeam Backup for Microsoft Office 365 User Guide.

   You can also perform a restore of backups created for Exchange Online organizations to on-premises Microsoft Exchange servers and vice versa, as described in Restore to On-Premises Microsoft Servers.



Step 3. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication metho**d drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

   For more information, see the Microsoft Office 365 Organizations section of the Veeam Backup for Microsoft Office 365 User Guide.

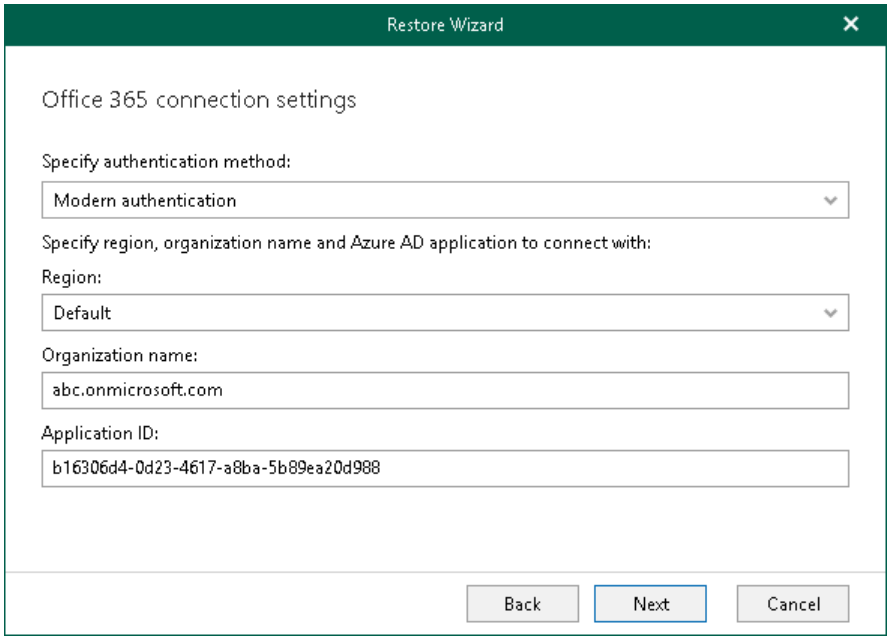
2. From the **Region** drop-down list, select a region to which your Exchange Online organization belongs.

3. In the **Organization name** field, enter a name of your Exchange Online organization.

   Make sure that the organization name matches the name specified at the previous step.

4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in the Azure AD Application Permissions section of the Veeam Backup for Microsoft Office 365 User Guide.

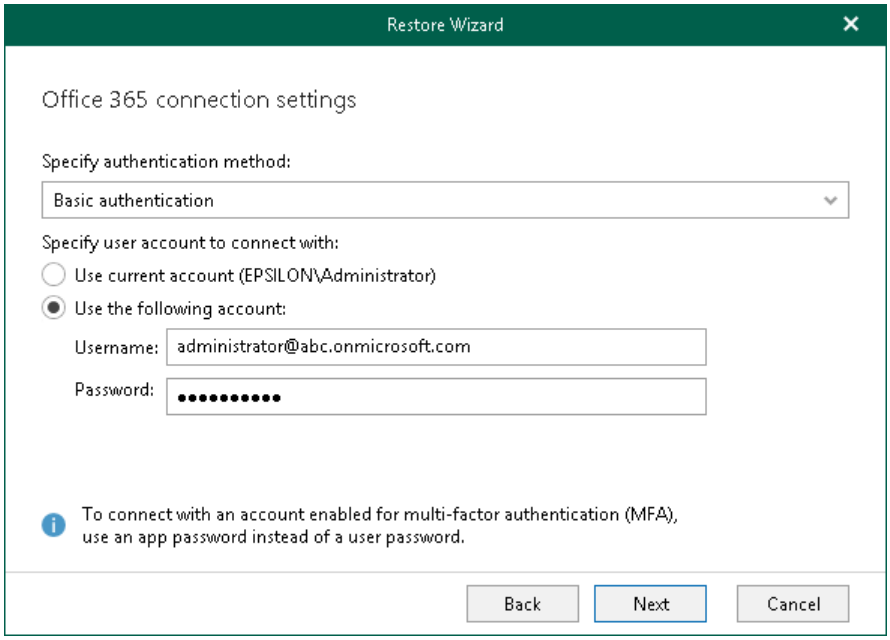


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the Exchange organization.

   When restoring to an on-premises Exchange server, make that the account that you use has both the *Exchange Admin* and the Global Admin roles.



Step 4. Log In to Office 365

[This step is available only if you have selected the *Modern Authentication* option at the previous step.]

At this step of the wizard, sign in to your Microsoft Office 365 organization.

To sign in to the Microsoft Office 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

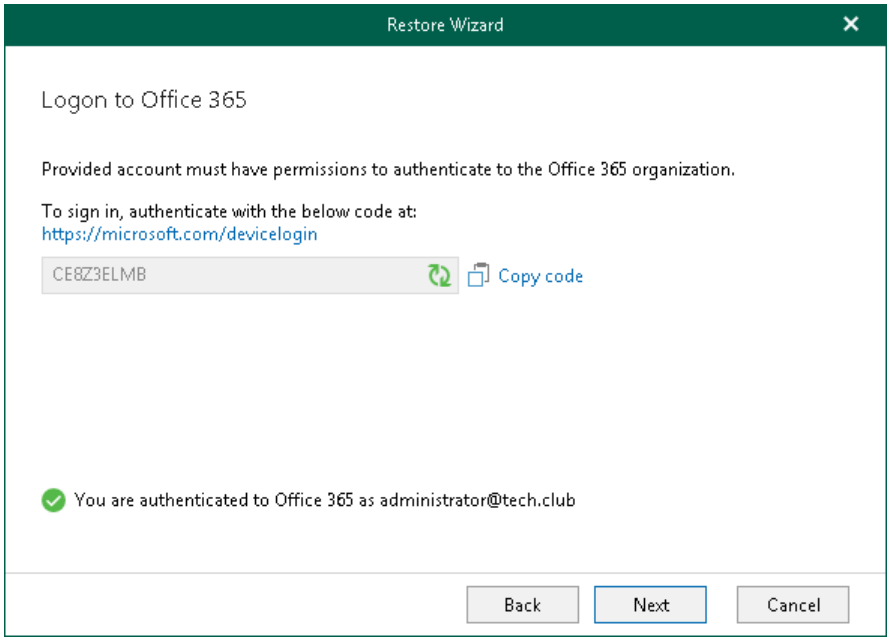
2. Click the link to the Microsoft portal.

3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Required Azure AD Application Settings section of the Veeam Backup for Microsoft Office 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



Step 5. Specify CAS Server and Folder

[This step is available only if you have selected the *Basic Authentication* option at the Select Authentication Method step.]

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

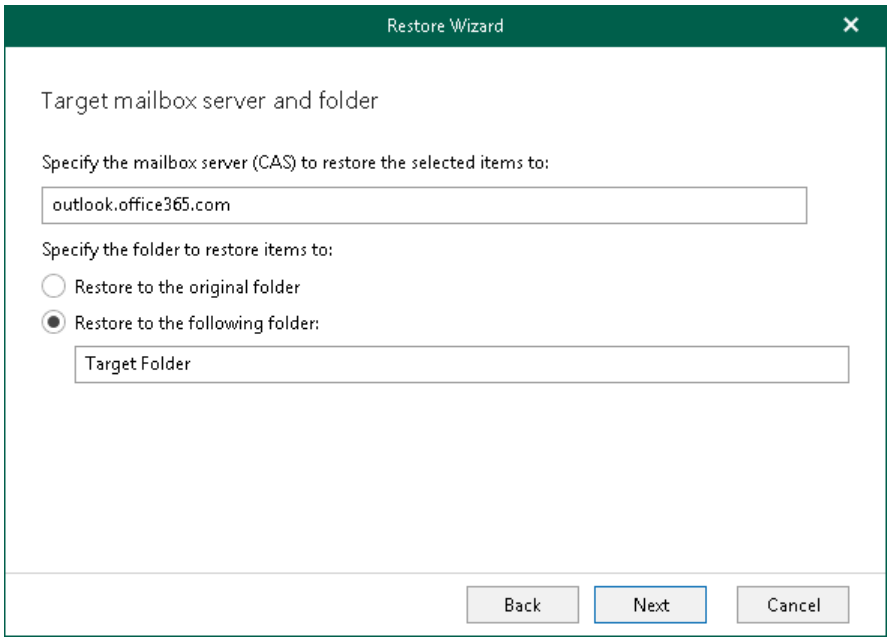
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or IP address.

   This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.

2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

   When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.

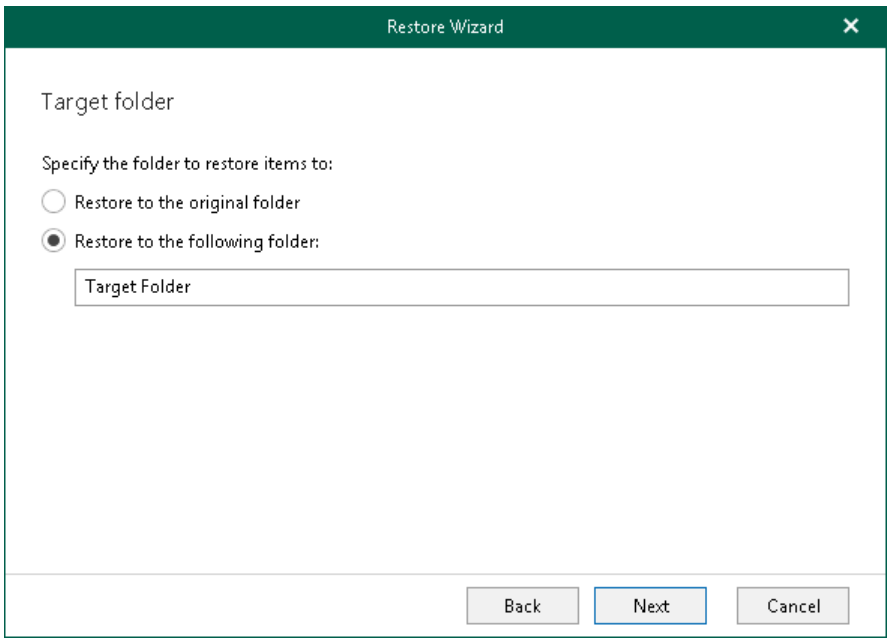


Step 6. Specify Target Folder

[This step is available only if you have selected the *Modern Authentication* option at the Select Authentication Method.]

At this step of the wizard, select a target folder to which you want to restore the specified mailbox. You can perform a restore to the original folder or specify a custom folder.

When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.



Step 7. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

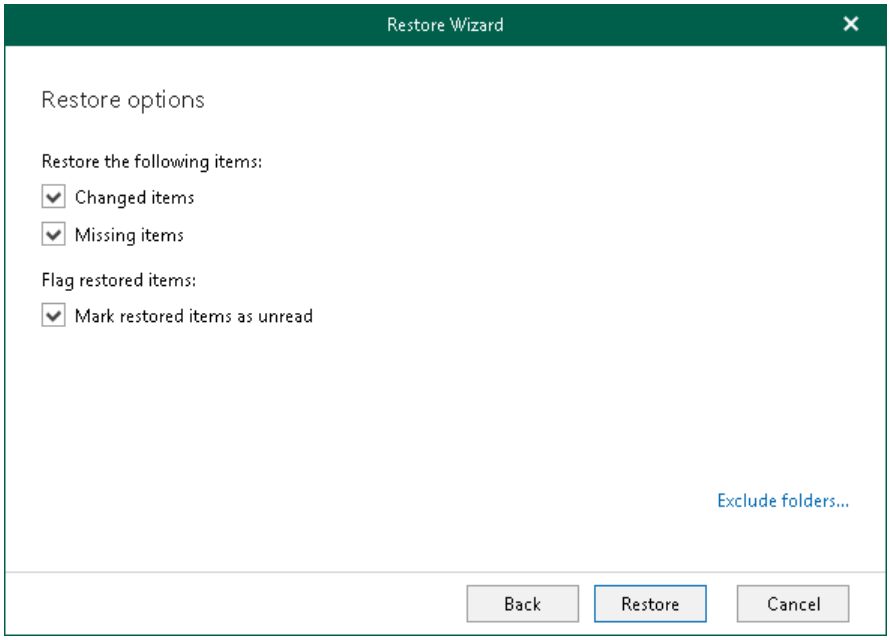
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

To prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.

> **NOTE**
>
> The **Exclude folders** link is not available when restoring folders and items.



Restoring Multiple Mailboxes

This scenario is available only for data restore from backups created in Veeam Backup for Microsoft Office 365.

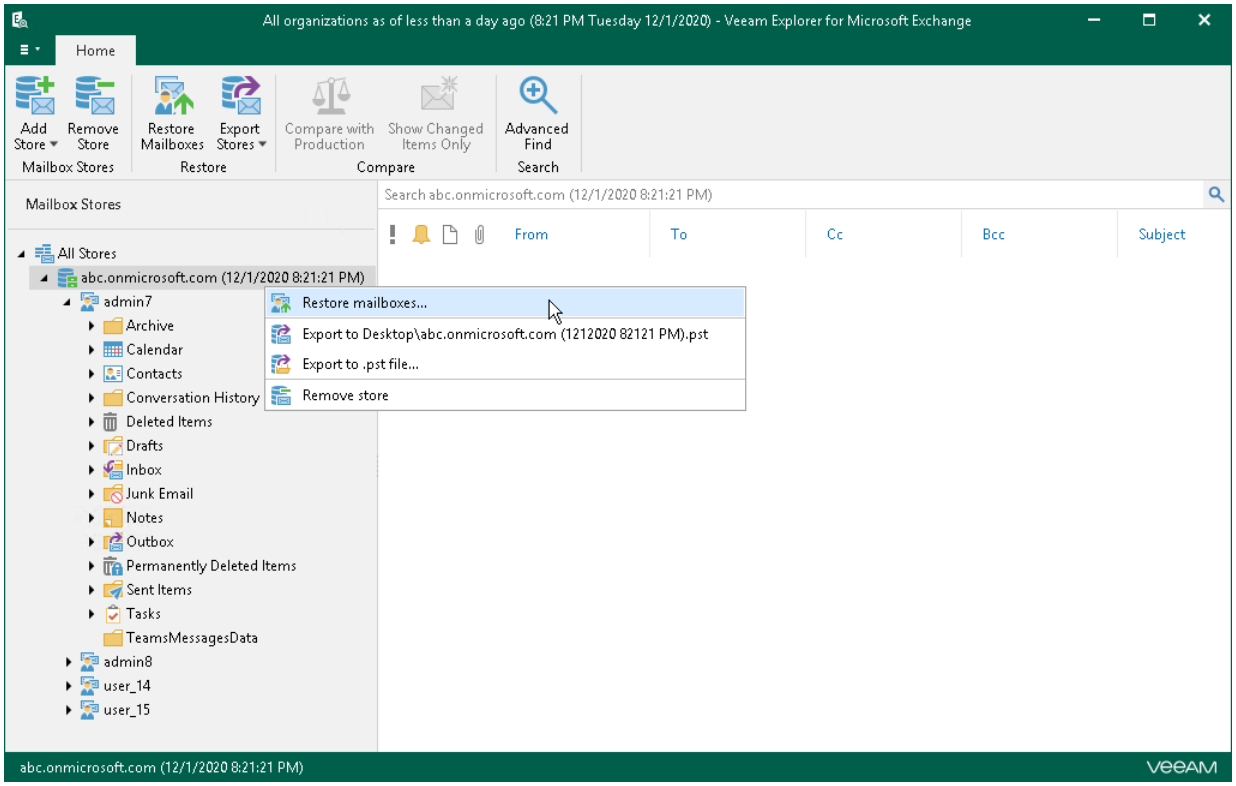
To restore multiple Exchange mailboxes to a Microsoft Office 365 organization, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Select mailboxes to restore.
5. Select restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox store.
2. On the **Home** tab, select **Restore Mailboxes** or right-click a container and select **Restore mailboxes**.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

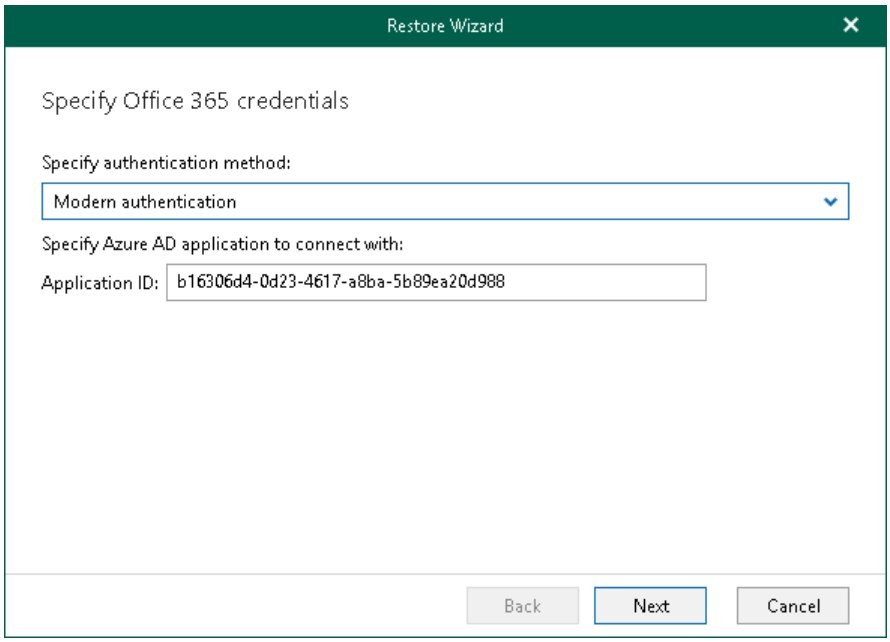
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

   For more information, see the Microsoft Office 365 Organizations section of the Veeam Backup for Microsoft Office 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in the Azure AD Application Permissions section of the Veeam Backup for Microsoft Office 365 User Guide.

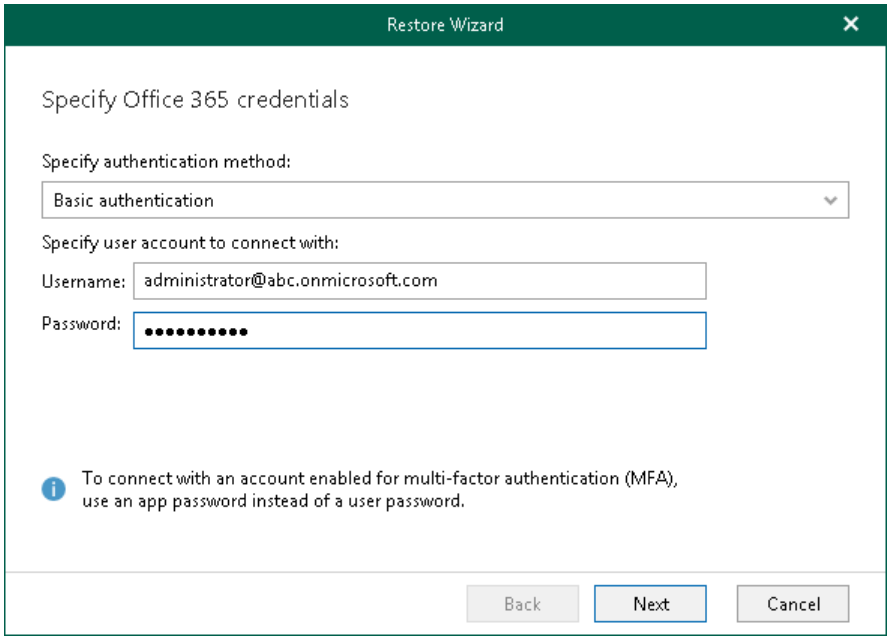


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the Exchange organization.

   When restoring to an on-premises Exchange server, make that the account that you use has both the *Exchange Admin* and the Global Admin roles.



Step 3. Log In to Office 365

[This step is available only if you have selected the *Modern Authentication* option at the previous step.]

At this step of the wizard, sign in to your Microsoft Office 365 organization.

To sign in to the Microsoft Office 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

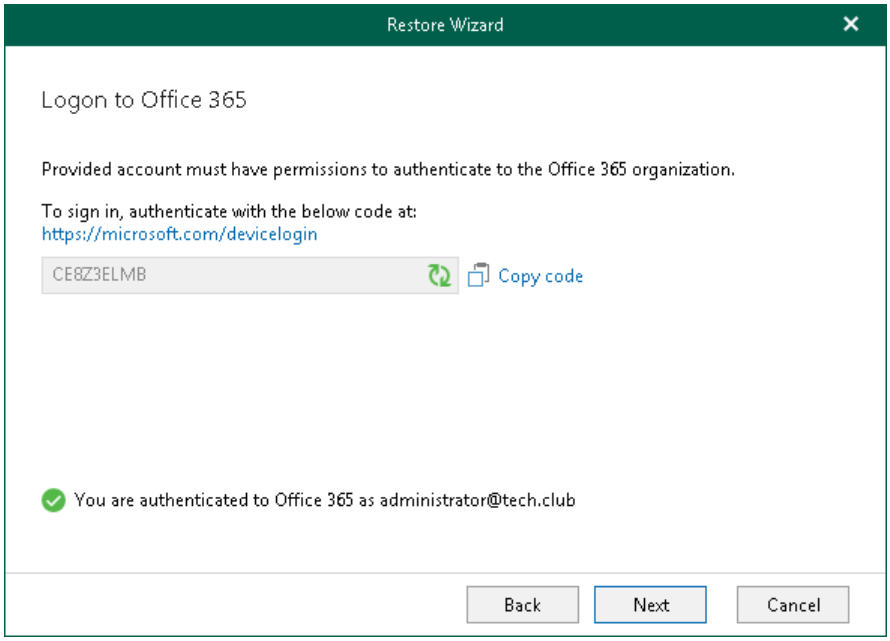
2. Click the link to the Microsoft portal.

3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Required Azure AD Application Settings section of the Veeam Backup for Microsoft Office 365 User Guide.

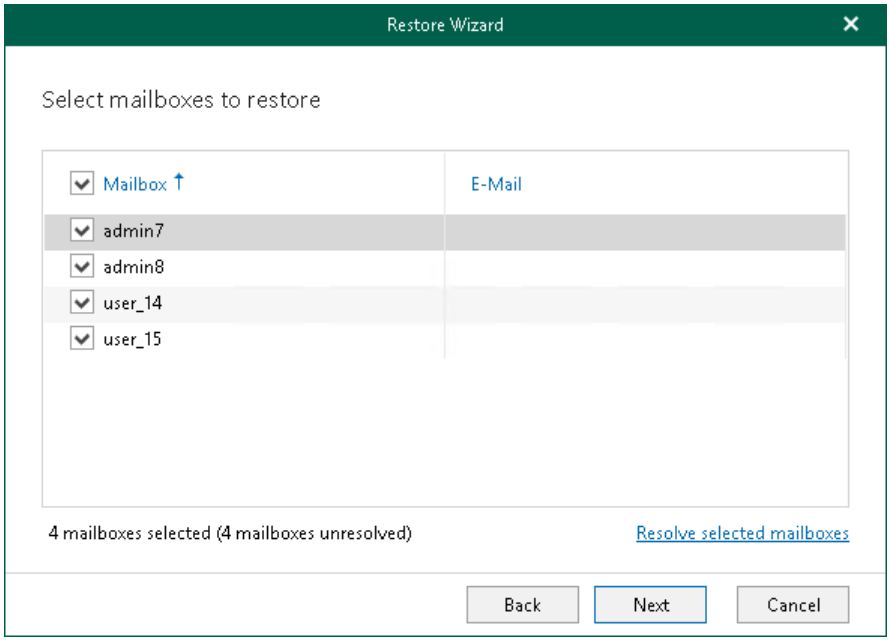
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Select Mailboxes to Restore

At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **E-Mail** column, click **Resolve selected mailboxes**.



Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

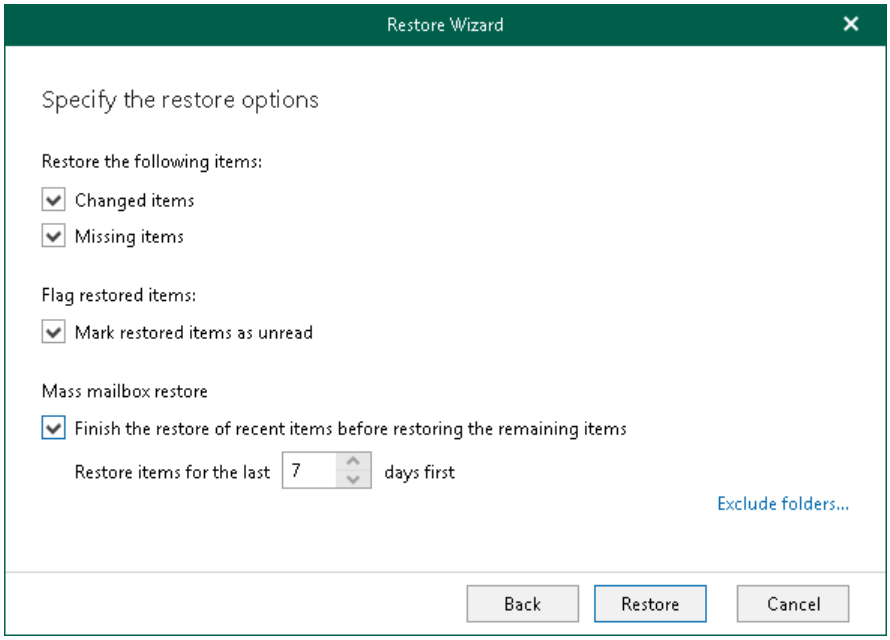
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being recovered, click the **Exclude folders** link and select folders to exclude.



Restore to On-Premises Microsoft Servers

This section explains how to restore data to on-premises Microsoft Exchange servers.

When you perform a restore, you can specify a target mailbox, choose an authentication method that you want to use for a restore, specify a target folder to which you want to restore data and configure restore options.

You can also use 1-Click Restore if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folders and Items

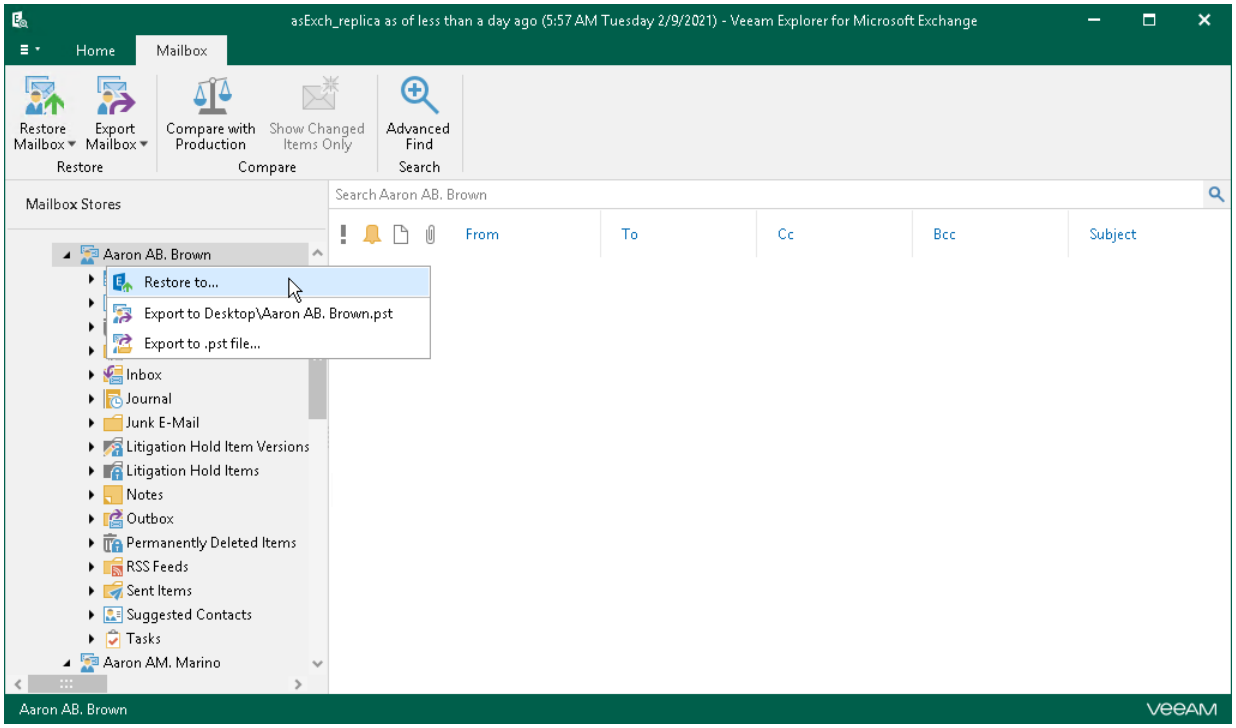
To restore mailboxes, folders and items, do the following:

1. Launch the Restore wizard.
2. Specify a target mailbox.
3. Specify a user account.
4. Specify a CAS server and target folder.
5. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item** > **Restore to** or right-click a mailbox, folder or an item and select **Restore to**.



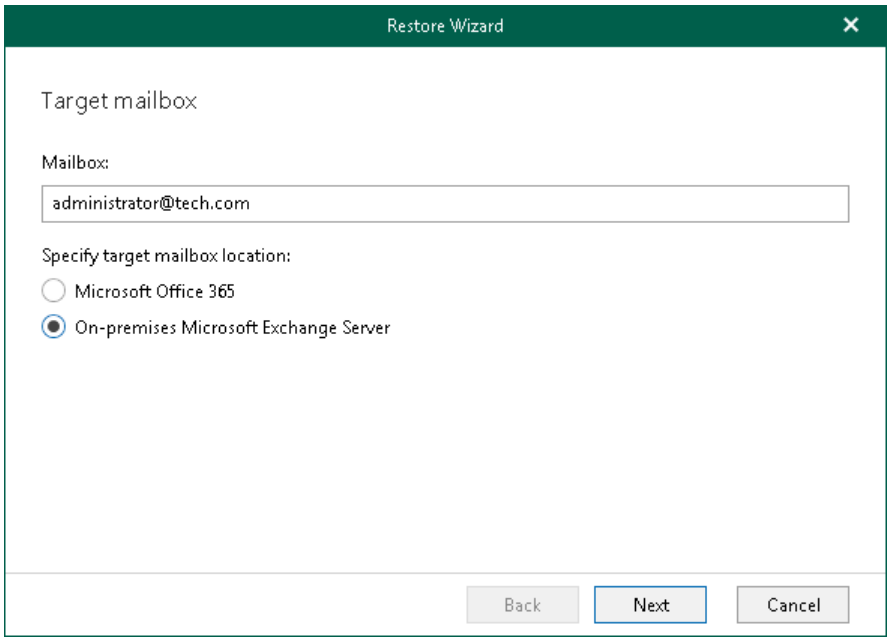
Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

To specify mailbox settings, do the following:

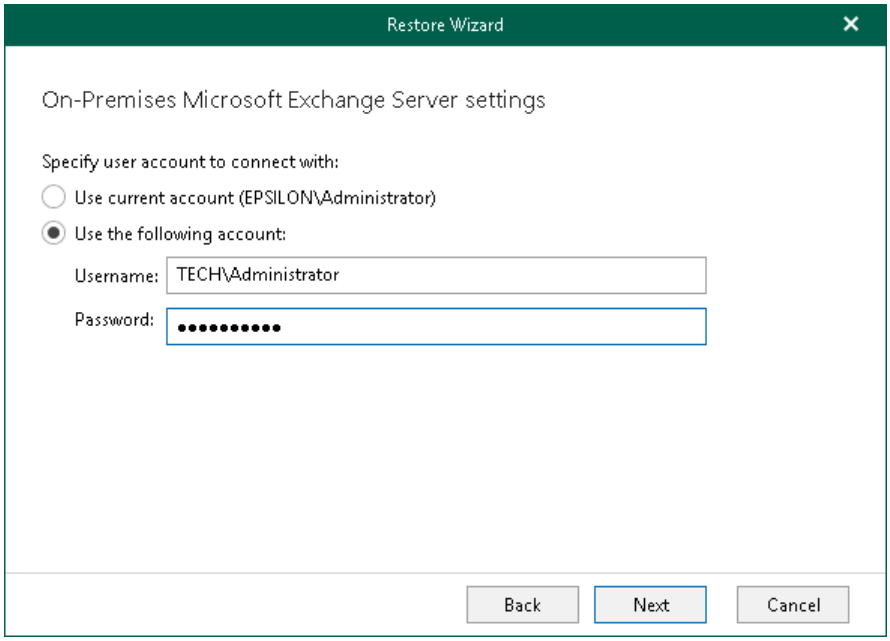
1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.
2. Select **On-premises Microsoft Exchange Server** to restore the specified mailbox to an on-premises Microsoft Exchange organization.

   You can also perform a restore of backups created for on-premises Microsoft Exchange organizations to Exchange Online organizations and vice versa, as described in Restore to Office 365 Organizations.



Step 3. Specify User Account

At this step of the wizard, specify an account that you want to use to connect to the Exchange server in your domain.



Step 4. Specify CAS Server and Target Folder

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

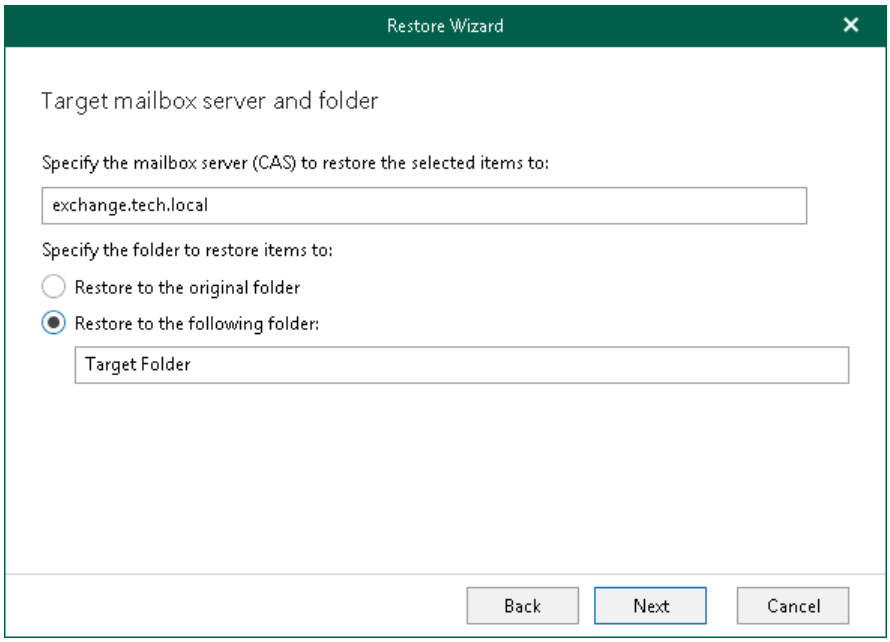
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or IP address.

   This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.

2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

   When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.



Step 5. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

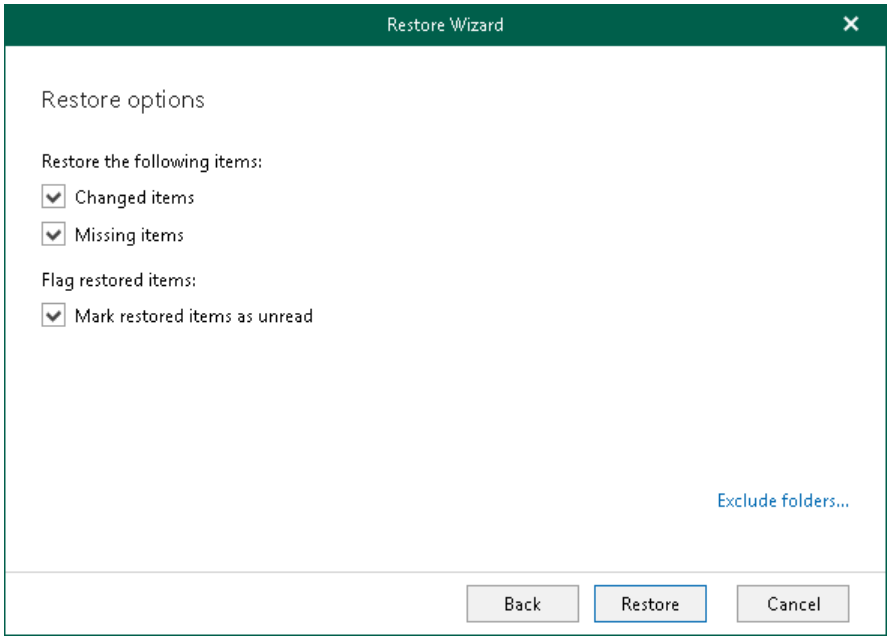
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

To prevent certain folders from being restored, click **Exclude folders** and select folders to exclude.

> **NOTE**
>
> The **Exclude folders** link is not available when restoring folders and items.



Restoring Multiple mailboxes

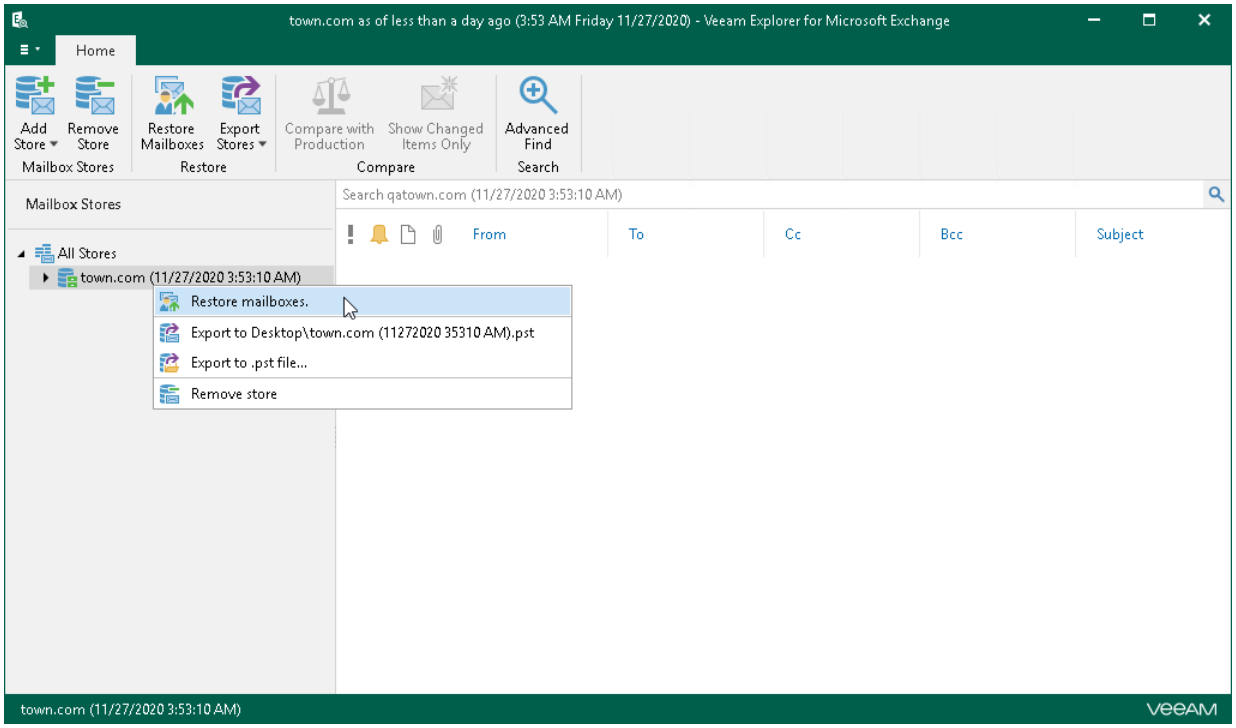
To restore multiple Exchange mailboxes, do the following:

1. Launch the Restore wizard.
2. Specify a domain and credentials.
3. Select mailboxes to restore.
4. Specify a target mailbox server.
5. Select restore options.

Step 1. Launch Restore Wizard

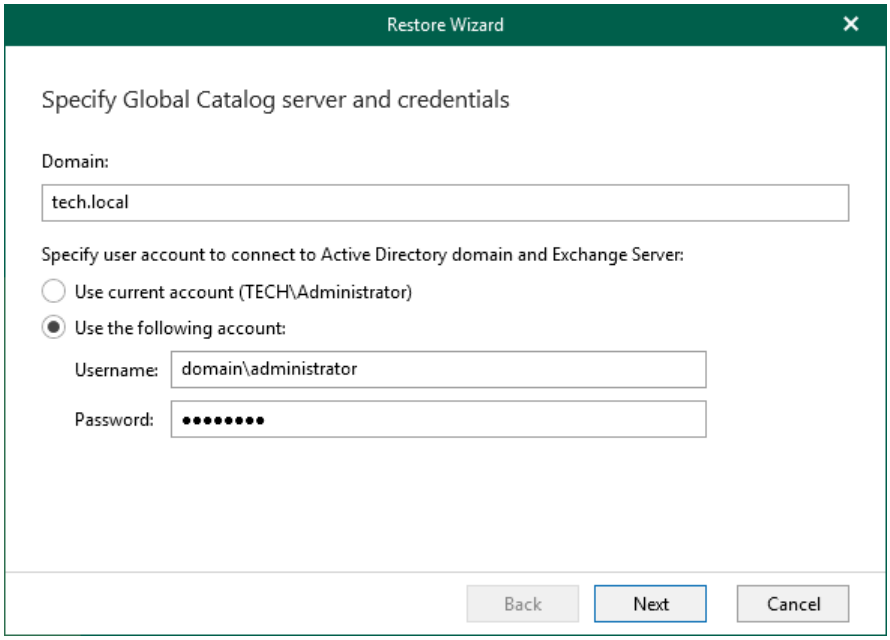
To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox store whose mailboxes you want to restore.
2. On the **Home** tab, select **Restore Mailboxes** or right-click a mailbox store and select **Restore mailboxes**.



Step 2. Specify Domain and Credentials

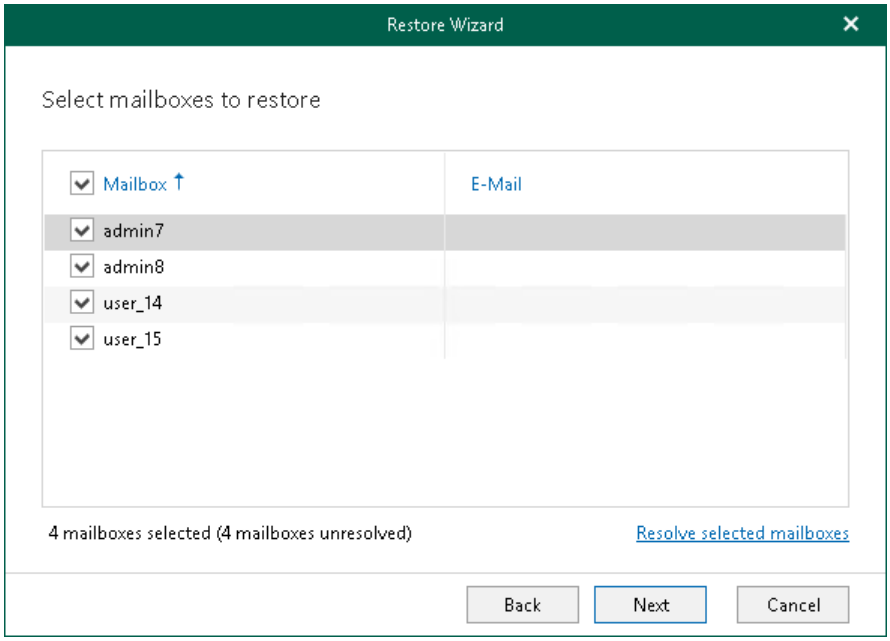
At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.



Step 3. Select Mailboxes to Restore

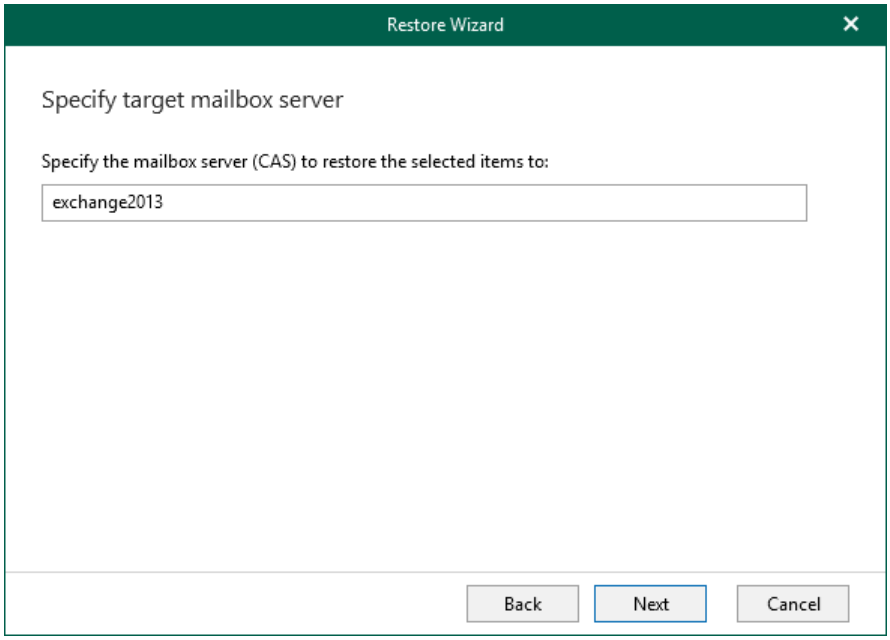
At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **E-Mail** column, click **Resolve selected mailboxes**.



Step 4. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes.



Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

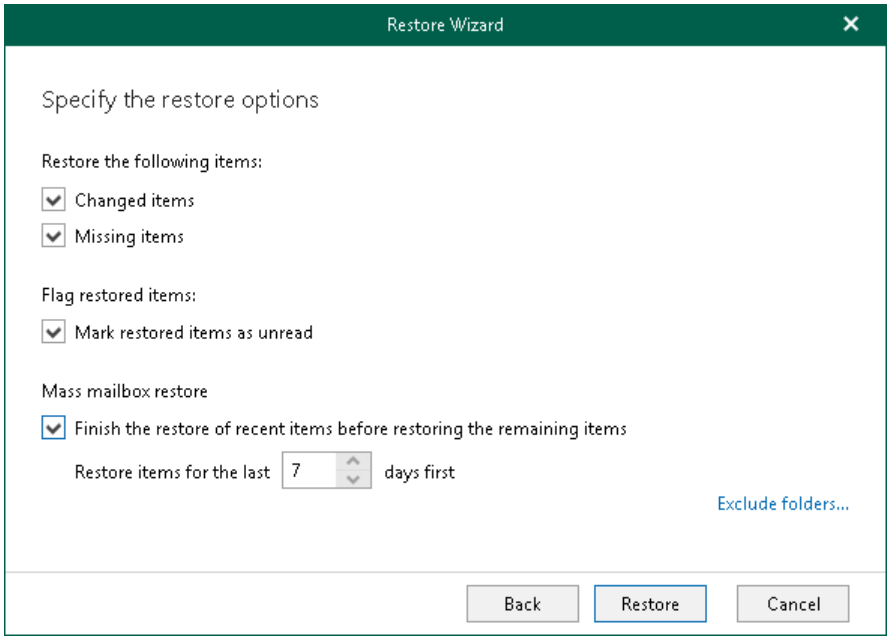
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being recovered, click the **Exclude folders** link and select folders to exclude.



1-Click Restore

The *1-Click Restore* feature allows you to quickly recover Exchange mailboxes, folders and items according to the following:

- The original Exchange server, original folder and the original mailbox name are restored.
- Both changed and missing items are restored.
- Restored items are marked as unread.
- No folders are excluded.

1-Click Restore is a convenient feature when you do not want to configure a restore session and prefer to restore data with the default settings.

Restoring to Office 365 Organizations

This scenario is available only for data restore from backups created in Veeam Backup for Microsoft Office 365.

To perform *1-Click Restore* to Office 365 organizations, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item** > **Restore to <mailbox_name>** or right-click a mailbox/folder/item and select **Restore to <mailbox_name>**.