



Veeam Backup Enterprise Manager

Version 12

User Guide

March, 2023

© 2023 Veeam Software.

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

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

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE	9
ABOUT THIS GUIDE	10
ABOUT VEEAM BACKUP ENTERPRISE MANAGER	11
How Veeam Backup Enterprise Manager Works	12
Enterprise Manager Components	13
Veeam Backup Catalog	15
Veeam Backup Search Capabilities	16
File-Level Restore Capabilities	18
How Indexing Works	19
Indexing Data	20
Indexing Data Retention	25
SAML Authentication Support	27
PLANNING AND PREPARATION	29
System Requirements	30
Permissions	34
Ports	36
Kerberos Authentication	42
LICENSING	43
Installing License	44
Viewing License Details	45
Updating License	47
License Update Session Data	49
Revoking License	50
Removing License	51
Managing Monthly Usage Reports	52
Reviewing Monthly Usage Report	53
Adjusting Monthly Usage Report	54
Downloading Monthly Usage Report	55
Submitting Monthly Usage Report	56
DEPLOYMENT	58
Installing Veeam Backup Enterprise Manager	59
Before You Begin	60
Step 1. Start Setup Wizard	61
Step 2. Select Product	62
Step 3. Read and Accept License Agreements	63
Step 4. Provide License File	64

Step 5. Install Missing Software	65
Step 6. Review Default Installation Settings.....	66
Step 7. Specify Service Account Settings	68
Step 8. Specify Database Server	69
Step 9. Specify Data Locations	71
Step 10. Specify Service Ports	72
Step 11. Begin Installation	73
Maintaining Veeam Backup Enterprise Manager	74
Upgrading to Veeam Backup Enterprise Manager 12.....	75
Before You Begin	76
Step 1. Start Upgrade Wizard.....	77
Step 2. Select Product.....	78
Step 3. Read and Accept License Agreements.....	79
Step 4. Review Components.....	80
Step 5. Provide License File.....	81
Step 6. Specify Service Account Settings.....	82
Step 7. Specify Database Server	83
Step 8. Begin Upgrade	84
Step 9. Finalize Upgrade	85
Updating Veeam Backup Enterprise Manager	86
Uninstalling Veeam Backup Enterprise Manager	87
Migrating Veeam Backup Enterprise Manager	88
GETTING TO KNOW VEEAM BACKUP ENTERPRISE MANAGER.....	89
Accessing Enterprise Manager Website	90
Veeam Backup Enterprise Manager UI	92
CONFIGURING VEEAM BACKUP ENTERPRISE MANAGER.....	95
Initial Configuration	96
Managing Backup Servers.....	97
Adding Backup Server	98
Editing Backup Server	100
Removing Backup Server	101
Collecting Data from Backup Servers.....	102
Reports on Backup Servers	104
Audit Reports	106
Customizing Dashboard Chart	109
Viewing vCenter Servers.....	110
Configuring Accounts and Roles	111
Accounts and Roles Overview.....	112
Managing Accounts	114

Configuring SAML Authentication Settings.....	124
Configuring AD FS for SAML Authentication.....	128
Configuring Retention Settings for Index and History.....	130
Configuring Notification Settings.....	133
Mail Server Settings.....	134
Notifications on Job Results.....	140
Notifications on Lab Requests.....	142
Notifications on Restore Operations.....	143
Notifications on Licensing.....	144
Notifications on Key Management.....	146
Viewing Information About Enterprise Manager.....	147
TLS Certificates.....	149
Connecting to Backup Servers.....	150
Updating TLS Certificates.....	151
Managing Languages.....	152
Language Files Overview.....	153
Adding Languages.....	154
VIEWING OPERATION STATISTICS.....	158
MANAGING JOBS.....	161
Viewing Jobs.....	162
Starting, Stopping and Retrying Jobs.....	163
Enabling and Disabling Jobs.....	164
Editing Jobs.....	165
Step 1. Launch Wizard.....	166
Step 2. Edit Job Name and Retention Settings.....	167
Step 3. Edit List of VMs.....	169
Step 4. Change VM Processing Order.....	171
Step 5. Configure Guest Processing Settings.....	172
Step 6. Edit Job Schedule.....	191
Creating Active Full Backups.....	194
Cloning Jobs.....	195
Deleting Jobs.....	196
MANAGING CDP POLICIES.....	197
Viewing Policies.....	198
Enabling and Disabling Policies.....	200
Editing Policies.....	201
Step 1. Launch Edit Policy Wizard.....	202
Step 2. Edit Policy Name and Description.....	203
Step 3. Edit List of VMs.....	204

Step 4. Edit Policy Schedule	207
Step 5. Configure Guest Processing Settings	210
Deleting Policies	221
WORKING WITH FILE SHARES	222
Viewing File Share Backups	223
Browsing File Share Backups	225
File Share Data Recovery	227
Instant File Share Recovery	228
Restoring Specific Files and Folders	241
Deleting File Share Backups	247
WORKING WITH MACHINES	248
Viewing Machines.....	249
Deleting Machine from Backup.....	251
Quick Backup	252
VM Recovery	253
Instant Recovery	254
Entire VM Restore	287
Virtual Disk Restore.....	315
VM Failover	319
Failover Plans.....	324
GUEST OS FILE RESTORE	326
Preparing for File Browsing and Searching	327
Performing Catalog Replication and Indexing	328
Preparing for File Search and Restore (non-Windows machines).....	329
Browsing Machine Backups for Guest OS Files	331
Searching Guest OS Files in Machine Backups.....	333
Performing 1-Click File Restore	335
Restoring Files to Original Location.....	336
Downloading Files to Local Machine.....	338
Restoring Multiple Files	340
Using Self-Service File Restore Portal to Restore Machine Guest Files.....	342
APPLICATION ITEM RESTORE	345
Restoring Microsoft Exchange Items	346
Restoring Microsoft SQL Server Databases	348
Restore to Original Location.....	349
Restore with Custom Settings	351
Restoring Oracle Databases.....	357
Restore to Original Location.....	358
Restore with Custom Settings	360

Restoring PostgreSQL Instances	367
Restore to Original Location	368
Restore with Custom Settings	370
SUPPORT FOR VEEAM AGENTS	376
Guest File Browsing and 1-Click Restore	377
Preparing for File Browsing and Restore	378
Browsing and Restore Procedures	380
Application Item Restore	381
MANAGING ENCRYPTION KEYS	382
Generating Enterprise Manager Keyset	383
Activating Enterprise Manager Keyset	384
Specifying Retention Settings for Enterprise Manager Keyset	385
Exporting and Importing Enterprise Manager Keyset	386
Deleting Enterprise Manager Keyset	388
Handling Password Recovery Requests	389
WORKING WITH VIRTUAL LAB REQUESTS	391
Creating Virtual Lab Requests	392
Approving Virtual Lab Requests	395
WORKING WITH VMWARE CLOUD DIRECTOR	396
Managing Configurations for Cloud Director Organizations	399
Before You Begin	400
Viewing Organization Configurations	402
Adding Organization Configuration	403
Editing Organization Configuration	406
Removing Organization Configuration	407
Exporting Configuration Report	408
Veeam Self-Service Backup Portal	409
Permissions	410
Accessing Veeam Self-Service Backup Portal	411
Working with Veeam Self-Service Backup Portal	415
VEEAM PLUG-IN FOR VMWARE VSPHERE CLIENT	454
Deploying vSphere Client Plug-in	455
Installing vSphere Client Plug-in	456
Uninstalling vSphere Client Plug-in	457
Local vSphere Client Plug-in	458
Accessing vSphere Client Plug-in	459
Configuring Plug-in Settings	460
Examining Backup Infrastructure	462
Creating Restore Points with VeeamZIP and Quick Backup	464

Remote vSphere Client Plug-in.....	469
Accessing vSphere Client Plug-in	470
Examining Backup Infrastructure.....	471
Creating Restore Points with VeeamZIP and Quick Backup	472
VSPHERE SELF-SERVICE BACKUP PORTAL.....	476
Configuring Delegation Mode.....	478
Managing Tenant Accounts	480
Adding Tenant Account.....	481
Editing Tenant Account.....	485
Exporting List of Tenant Accounts.....	487
Removing Tenant Account	488
Using vSphere Self-Service Backup Portal	489
Viewing Self-Service Backup Portal Statistics	491
Managing Backup Jobs	493
Managing VMs.....	495
Restoring Guest OS Files	498
Restoring Application Items	499
VEEAM BACKUP ENTERPRISE MANAGER UTILITIES.....	500
Enterprise Manager Database Migration Utility	501
Configuration Database Connection Settings Utility	504
Step 1. Launch Utility	505
Step 2. Select Product	506
Step 3. Specify Connection Settings	507
Step 4. Apply Connection Settings	510
Step 5. Finish Working with Wizard	511

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 Guide

This guide provides information on how to install and use Veeam Backup Enterprise Manager 12 until it is replaced with a newer version of the product.

Intended Audience

The user guide is intended for IT administrators, consultants, analysts and other IT professionals using the product. 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.

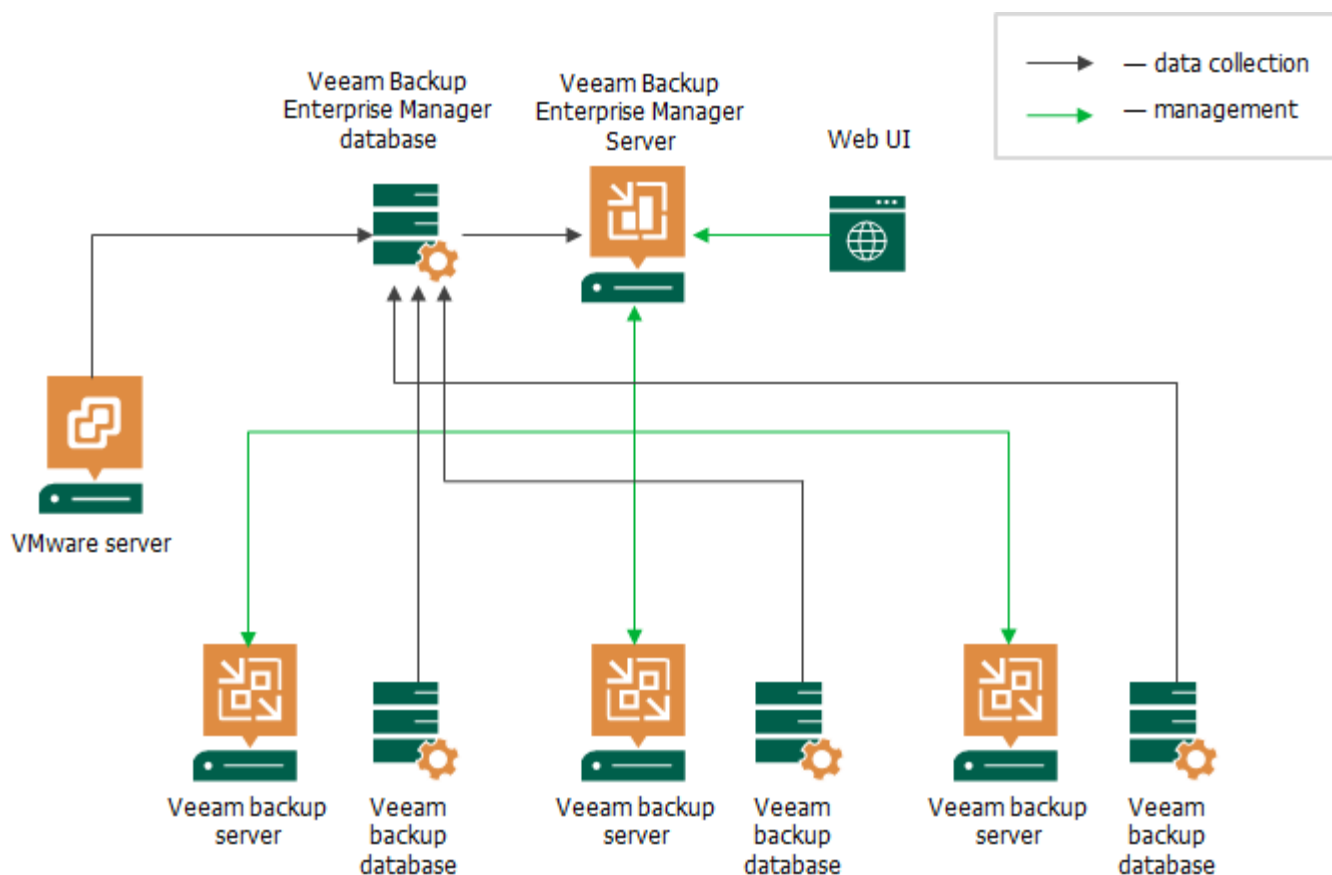
In particular, with Veeam Backup Enterprise Manager you can:

- 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 Cloud 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 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.

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 PostgreSQL or Microsoft 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 Cloud Director** that provide members of VMware Cloud 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 Cloud Director, and VMware vSphere Self-Service Backup Portal features are available in the Enterprise Plus edition of Veeam Backup & Replication.

- **Microsoft SQL Server database** or **PostgreSQL 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 backup servers. 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 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 Plug-in for VMware vSphere Client** allows vSphere administrators to manage backup infrastructure of the virtual environment. For more information, see [Veeam Plug-in for VMware vSphere Client](#).

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 a helper host or 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.

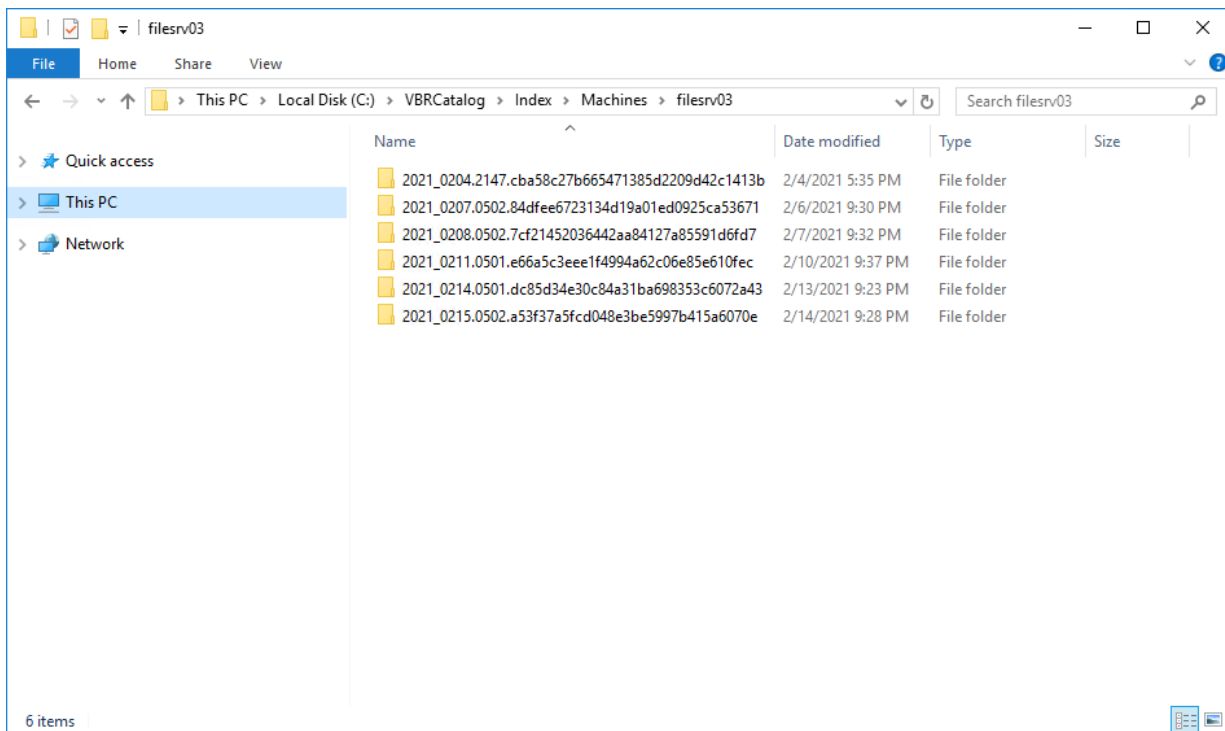
Veeam Backup Catalog comprises the following data:

- [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.

- o Group 2 will list restore points that are required to restore the machine to the 3rd, the latest restore point.

```

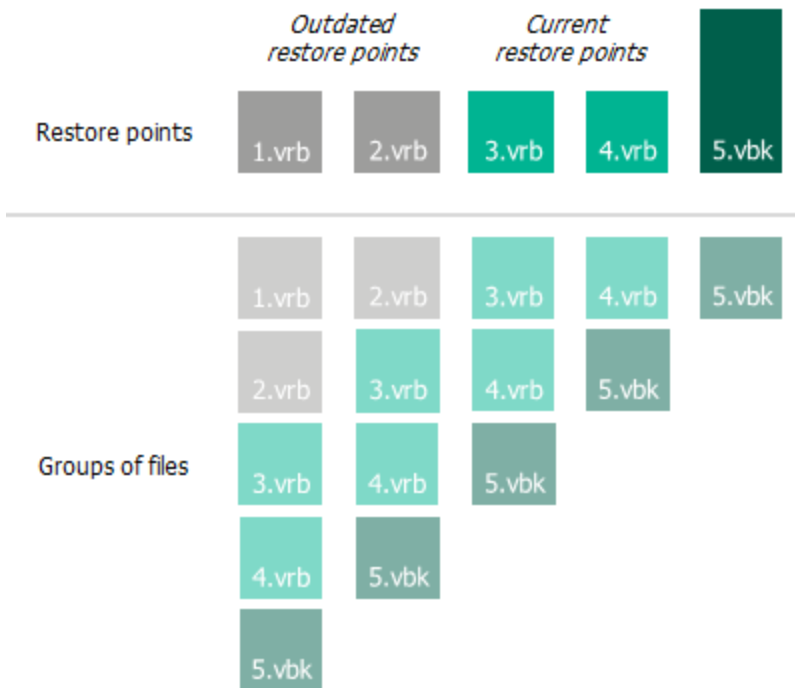
BackupServer=SRV02
JobName=srv01_reversed
SessionDateUtc=05/14/2014 11:20:18.952
#####
# OIBS
oib0.VmName=srv01
oib0.BackupTimeUtc=05/14/2014 10:56:55.993
oib0.OibUID=47c62e82-3066-478c-8272-1fb65a47d601
oib0.Platform=EVmware
oib0.Group=grp1
oib1.VmName=srv01
oib1.BackupTimeUtc=05/14/2014 11:02:20.15
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.



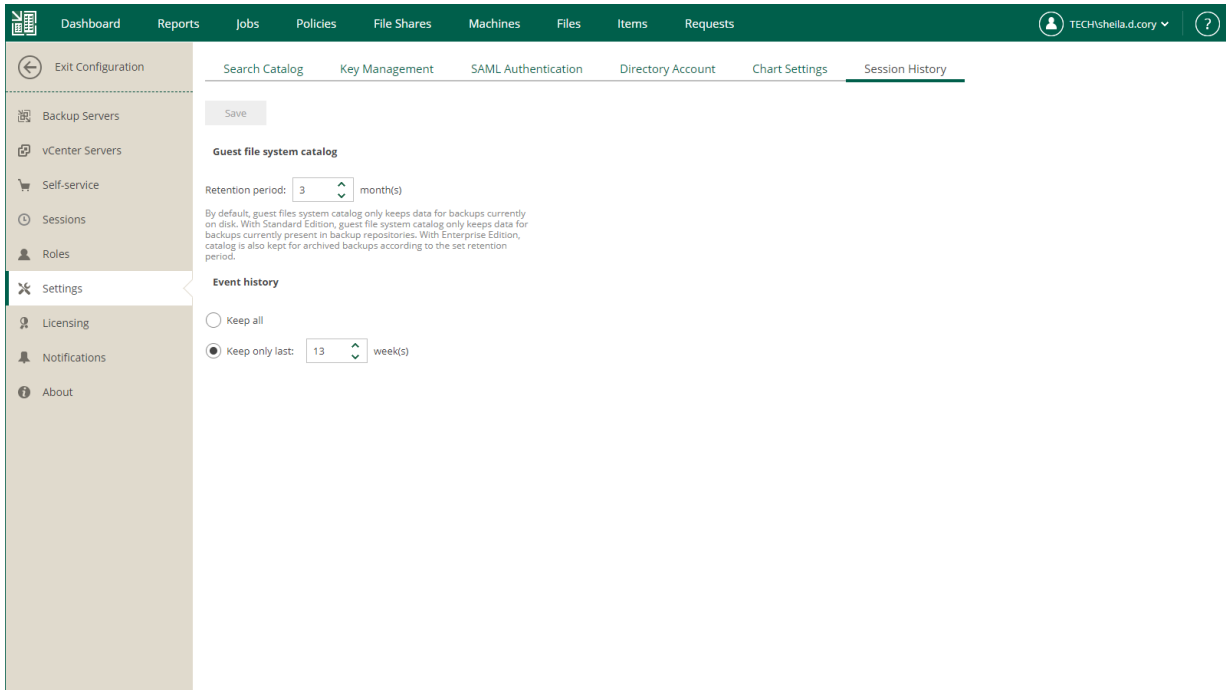
Current and Historical Indexing Data

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:

$$\text{Retention period} = \text{MAX}(\text{Catalog Retention}, X)$$

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.

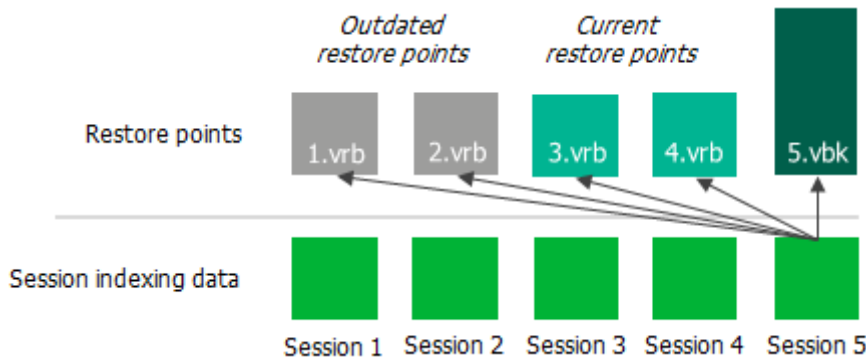
Retention for Reverse Incremental Backups

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:

$$\text{Retention period} = \text{MAX}(\text{Catalog Retention}, X) + X$$

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

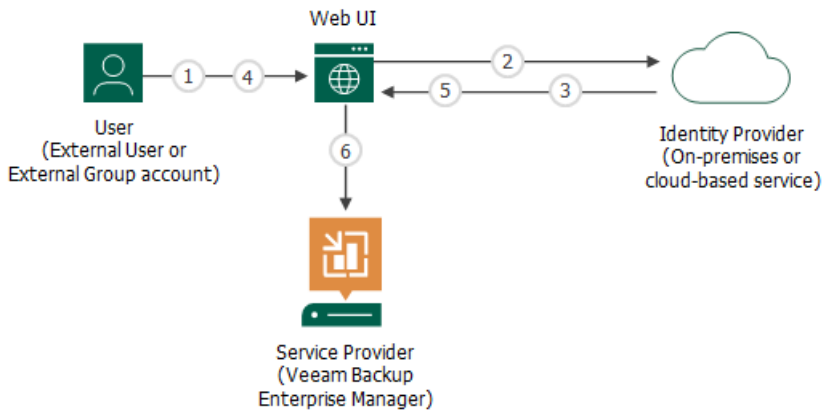
In Veeam Backup Enterprise Manager, SAML authentication is performed in the following way:

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*.

- 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 [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 the system requirements listed below.

All backup servers must be based on the same database engine as Veeam Backup Enterprise Manager (PostgreSQL or Microsoft SQL Server). For more considerations and limitations on adding backup servers, see [Adding Backup Server](#).

Veeam Backup Enterprise Manager

Server Side

Specification	Requirement
Hardware	<ul style="list-style-type: none">• CPU: x86-64 processor.• Memory: 4 GB RAM (minimum recommended).• Hard disk space: for product installation plus sufficient disk space to store guest file system catalog from connected backup servers (according to data retention policy).• Network: 1 Mbps or faster connection to Veeam Backup & Replication servers.
OS	64-bit versions of the following operating systems are supported: <ul style="list-style-type: none">• Microsoft Windows Server 2022• Microsoft Windows Server 2019• Microsoft Windows Server 2016• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows Server Semi-Annual Channel 20H2 (versions 1803 to 20H2)• Microsoft Windows 11 (versions 21H2, 22H2)• Microsoft Windows 10 (versions 1909 to 22H2)• Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)
PostgreSQL	Local or remote installation of the following versions of PostgreSQL: <ul style="list-style-type: none">• PostgreSQL 14• PostgreSQL 15 (PostgreSQL 15.1 is included in the Veeam Backup & Replication setup)

Specification	Requirement
<p>Microsoft SQL Server</p>	<p>Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported):</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 with Microsoft SQL Server 2014 Management Objects and Microsoft System CLR for Microsoft SQL Server 2014 • Microsoft SQL Server 2012 <p>Microsoft SQL Server 2012 databases and later with compatibility to Microsoft SQL Server 2005 are not supported.</p> <p>All editions of Microsoft SQL Server are supported. The usage of Microsoft SQL Server Express Edition is limited by the database size up to 10 GB. If you plan to have larger databases, use other editions of Microsoft SQL Server.</p> <p>Veeam Backup & Replication and Veeam Backup Enterprise Manager configuration databases can be deployed in Microsoft SQL AlwaysOn Availability Groups. For more information, see this Veeam KB article.</p>

Specification	Requirement
Software	<p>During installation and upgrade, the setup wizard system performs configuration check to determine if all prerequisite software is available on the machine where you plan to install Enterprise Manager. If some of the required software components are missing, the setup wizard tries to install missing software automatically. This refers to the following software:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2 • Microsoft Visual C++ 2015-2019 Redistributable • Microsoft SQL Server System CLR Types for SQL Server 2014 • IIS URL Rewrite Module 2 • Microsoft Universal C Runtime • Microsoft Report Viewer Redistributable 2015 • Microsoft Internet Information Services: <ul style="list-style-type: none"> ○ Default Document Component ○ Directory Browser Component ○ HTTP Errors Component ○ Static Content Component ○ Windows Authentication Component ○ WebSocket Protocol Component ○ ASP.NET 4.5 Component ○ .NET Extensibility 4.5 Component • Windows Installer 4.5 (included in the setup) <p>If you plan to install Veeam Backup Enterprise Manager in the unattended mode using the command line interface, manually install all prerequisite software before that. For more information, see the <i>Veeam Backup Enterprise Manager Server</i> subsection of the Installing Veeam Backup & Replication in Unattended Mode section of the Veeam Backup & Replication User Guide.</p>

IMPORTANT

To restore Microsoft Exchange items with Veeam Backup Enterprise Manager, Microsoft Exchange servers must be members of the same Microsoft Active Directory forest.

Client Side

Specification	Requirement
Browsers	<p>Mozilla Firefox, Google Chrome and Microsoft Edge. The browser must have JavaScript and WebSocket protocol enabled.</p> <p>Enterprise Manager User Interface may not work correctly in Mozilla Firefox running on Microsoft Windows 11 22H2.</p>
Microsoft Excel	Microsoft Excel (to view reports exported to Microsoft Excel format).

[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	<ul style="list-style-type: none">• For PC: Microsoft Edge, Mozilla Firefox and Google Chrome• For portable devices (tablets): Safari for iOS or Google Chrome for Android

[Optional] VMware Cloud Director

Specification	Requirement
VMware Cloud Director	VMware Cloud Director 10.1 to 10.4. Note that you can use VMware Cloud Director on a backup server that is based on Microsoft Windows Server 2016 or later.
Other software	If your Enterprise Manager deployment uses IIS 8.5, a URL rewrite module is required to work with Veeam Self-Service Backup Portal for VMware Cloud Director.

[Optional] vSphere Client Plug-in

Specification	Requirement
VMware vSphere	VMware vSphere version 6.0 or later.

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 <i>local Administrator</i> 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 Microsoft SQL Server level. After the database is created, this account automatically gets a <i>db_owner</i> role and can perform all operations with the database. Note: If a database is created in advance (by a database administrator or Microsoft SQL Server administrator), the setup account must have the <i>db_owner</i> role for the database.
	To upgrade an existing Microsoft SQL Server database, the account must have the <i>db_owner</i> role.
Veeam Backup Enterprise Manager service account	<p>It is recommended to use the <i>Local System</i> 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:</p> <ul style="list-style-type: none">• <i>Local Administrator</i> permissions on the Veeam Backup Enterprise Manager server.• <i>Log on as service</i> right (granted automatically to the Veeam Backup Enterprise Manager Service account).• <i>Db_datareader</i> and <i>db_datawriter</i> roles, as well as permissions to <i>execute stored procedures</i> for the Enterprise Manager database on the Microsoft SQL Server. Alternatively, you can assign this account the <i>db_owner</i> role for the Enterprise Manager database.• <i>Full Control</i> NTFS permissions for the <i>VBRCatalog</i> or another folder where index files are stored. <p>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 "<i>Cannot find user account DOMAIN\username</i>" error.</p>

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 Client Plug-in for Veeam Backup & Replication (optional)	<p>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.</p> <p>The account used to install the plug-in must be assigned the following vCenter Server permissions:</p> <ul style="list-style-type: none"> • 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.

Ports

This section covers typical Veeam Backup Enterprise Manager connections and default ports required for communication between Enterprise Manager components.

NOTE

For more information on ports specific for Veeam Backup & Replication infrastructure components, see the [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 server	Backup server	TCP	9405	Default certificate port used by Enterprise Manager for collecting data from backup servers that have Veeam Backup & Replication 12 or later installed. You can customize the port when you add a backup server. For more information, see Adding Backup Server .
			9392	Default port used by Enterprise Manager for collecting data from backup servers that have Veeam Backup & Replication 11a or earlier installed. You can customize the port when you add a backup server. For more information, see Adding Backup Server .
			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.

From	To	Protocol	Port	Notes
			49152 to 65535 (for Microsoft Windows Server 2012 and later)	Dynamic RPC port range. For more information, see this Microsoft KB article .
	PostgreSQL hosting the Enterprise Manager configuration database	TCP	5432	Default port used for communication with PostgreSQL hosting the Enterprise Manager configuration database.
	Microsoft SQL Server hosting the Enterprise Manager configuration database	TCP	1433	Default port used for communication with Microsoft SQL Server hosting the Enterprise Manager configuration database. 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.
	VMware vCenter Server	TCP	443	Default port used for connection to a vCenter Server and deploying the Veeam Plug-in for vSphere Client. Can be customized during 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.

From	To	Protocol	Port	Notes
		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 .
	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 native VMware Cloud Director 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 .

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager REST API client and VMware vSphere Client plug-in	Veeam Backup Enterprise Manager REST API	HTTP	9399	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 .
		HTTPS	9398	
Veeam ONE Server (optional)	Veeam Backup Enterprise Manager server	TCP	Dynamically assigned ports	If you add the Veeam Backup Enterprise Manager server to the 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:

- For communication between the Veeam Backup Enterprise Manager server and backup servers, Kerberos authentication is used by default.
- 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 server	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 server	Mount server (helper host or helper appliance)	TCP	2500 to 6000	Ports used for file download. For more information on the mount server, 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 [Ports](#) section of the Veeam Backup & Replication User Guide.

Microsoft SQL Server Database Restore

From	To	Protocol	Port	Notes
Target remote Microsoft 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	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](#).

Kerberos Authentication

Veeam Backup Enterprise Manager supports Kerberos authentication for communication with backup servers and file-level restore. Although Veeam Backup Enterprise Manager works in a Kerberos-only environment, NTLM authentication is still supported as a fallback.

For more information on Kerberos authentication and requirements for a Kerberos-only environment, see the [Kerberos Authentication](#) section of the Veeam Backup & Replication User Guide.

NOTE

Backup servers with Veeam Backup & Replication 11a or earlier require NTLM for communication.

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.

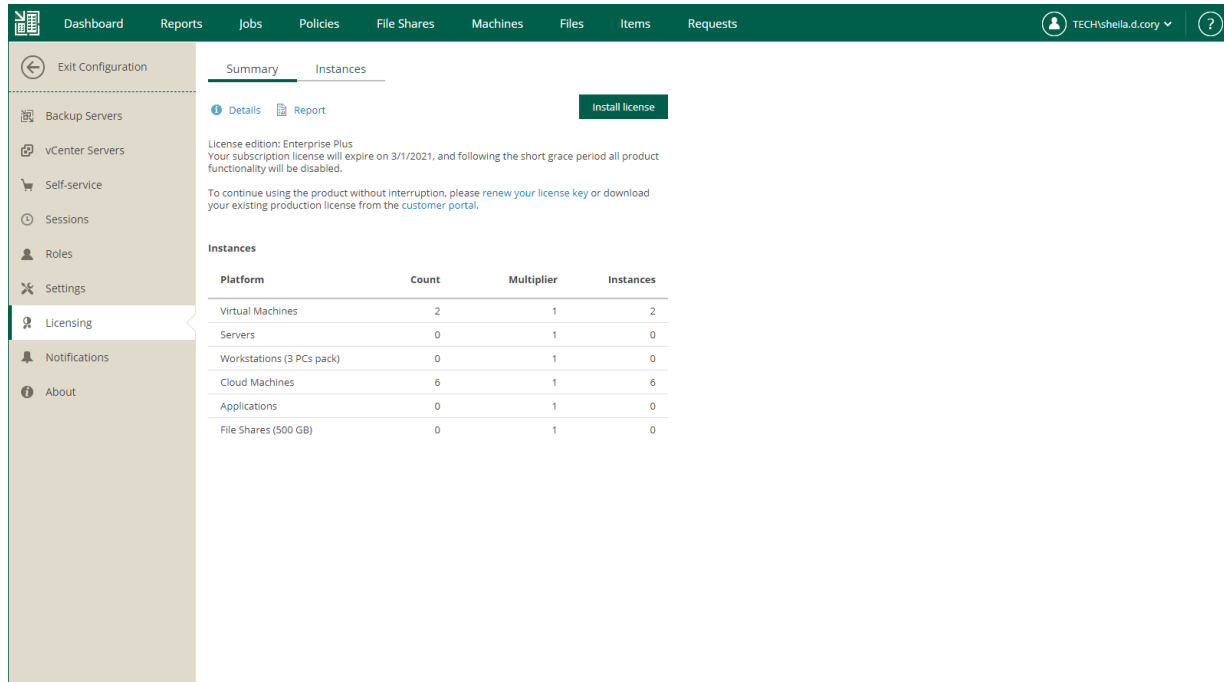
If you have a Perpetual Socket license installed, you can install an instance license over it. In this case, the licenses will be merged. For more information on licenses available for merging, see the [Merging Licenses](#) section of the Veeam Backup & Replication User Guide. After the merge, you can remove an unnecessary part of the merged license. For details, see [Removing License](#).

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**.



The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\shella.d.cory'. The left sidebar shows the 'Licensing' section selected. The main content area is titled 'Summary' and features an 'Install license' button. Below the button, a message states: 'License edition: Enterprise Plus. Your subscription license will expire on 3/1/2021, and following the short grace period all product functionality will be disabled. To continue using the product without interruption, please [renew your license key](#) or download your existing production license from the [customer portal](#).' Below this message is a table titled 'Instances' with the following data:

Platform	Count	Multiplier	Instances
Virtual Machines	2	1	2
Servers	0	1	0
Workstations (3 PCs pack)	0	1	0
Cloud Machines	6	1	6
Applications	0	1	0
File Shares (500 GB)	0	1	0

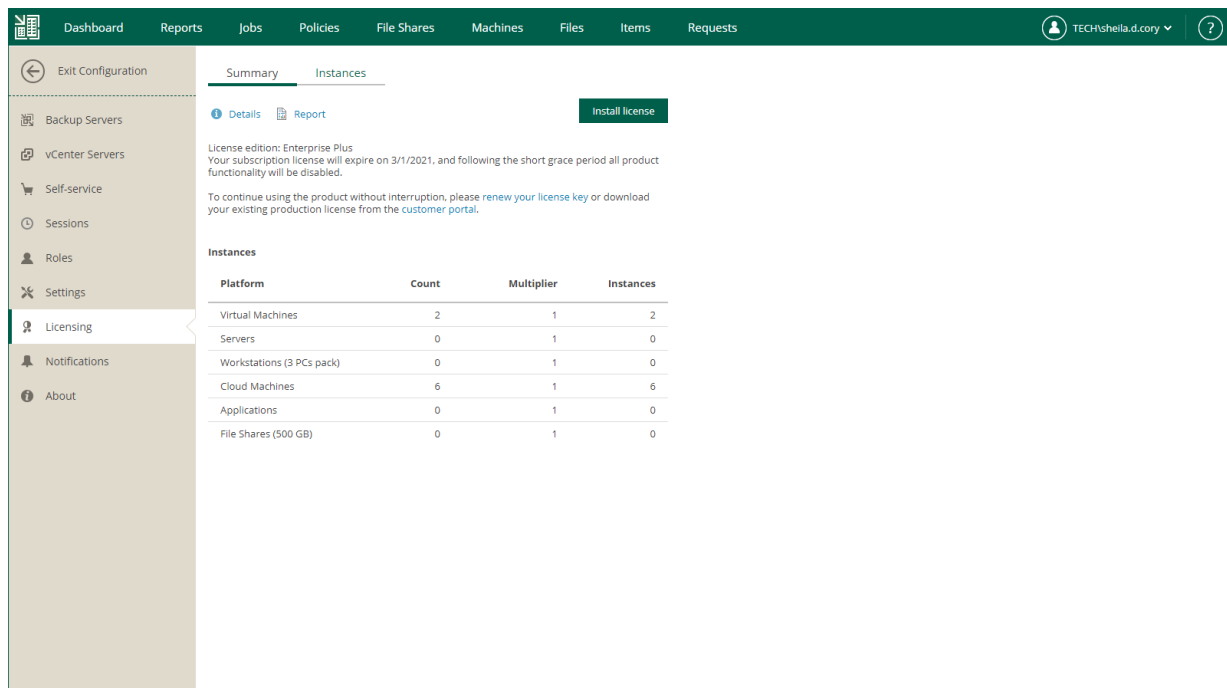
Viewing License Details

You can view 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](#).

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.



The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECHSheila.d.cory. The main content area is titled 'Licensing' and shows the license edition as 'Enterprise Plus' with an expiration date of 3/1/2021. Below this, there is a table of instances for various platforms.

Platform	Count	Multiplier	Instances
Virtual Machines	2	1	2
Servers	0	1	0
Workstations (3 PCs pack)	0	1	0
Cloud Machines	6	1	6
Applications	0	1	0
File Shares (500 GB)	0	1	0

TIP

You can configure Veeam Backup Enterprise Manager to send notifications about expiring license. 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.

You can display detailed information about the current license, including license type, expiration date and the number of instances. To do this, click the **Details** link. To view information about license usage, click the **Report** link.

License Details ✕

License Information

Status	Valid
Type	Subscription
Edition	Enterprise Plus
Support ID	02067762
Licensed to	Veeam Software Group GmbH
Package	Backup

Instances

Instances	1000
Expiration date	3/1/2021

Update license key automatically

[Update now](#)

Save Cancel

Updating License

To be able to use all data protection and disaster recovery features, you must update your license upon expiry.

You can use the following methods to update the license:

- [Updating license manually](#)
- [Updating license automatically](#)

NOTE

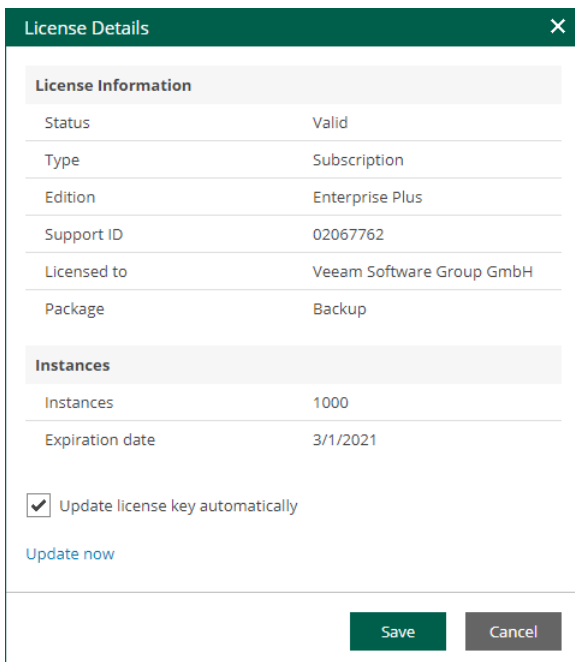
When updating the license, Veeam Backup Enterprise Manager requires internet access to connect to the Veeam License Update Server. If your network is not connected to the internet, you can download a new license file from my.veeam.com and install a new license. For more information on license installation, see [Installing 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.



The screenshot shows a dialog box titled "License Details" with a close button (X) in the top right corner. The dialog is divided into two main sections: "License Information" and "Instances".

License Information	
Status	Valid
Type	Subscription
Edition	Enterprise Plus
Support ID	02067762
Licensed to	Veeam Software Group GmbH
Package	Backup

Instances	
Instances	1000
Expiration date	3/1/2021

Below the instances table, there is a checkbox labeled "Update license key automatically" which is checked. At the bottom of the dialog, there is a blue link "Update now" and two buttons: "Save" (green) and "Cancel" (gray).

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 on the **Dashboard** tab and in the sessions information.

The screenshot shows the Veeam Backup Enterprise Manager Dashboard. At the top, a green navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', 'Requests', a user profile 'TECHSheila.d.cory', 'Configuration', and a help icon. A yellow warning banner at the top states: 'Warning: Your subscription license will expire on 3/1/2021, and following the short grace period all product functionality will be disabled. To continue using the product without interruption, please renew your license key or download your existing production license from the customer portal.' Below the banner, there are two tabs: 'Last 24 hours' (selected) and 'Last 7 days', with a 'Refresh' button. The dashboard is divided into five main sections: 1. Summary: Backup servers (2), Jobs (9), Machines (10), File shares (1). 2. Image Data: Processing speed (0 KB/s), Source size (134.5 GB), Full backups (64.2 GB), Restore points (11 GB). 3. File Data: Processing speed (0 KB/s), Source size (3.6 GB), Backup (3.4 GB), Archive (0 B). 4. Last 24 hours: Total job runs (0), Success (0), Warning (0), Error (0). 5. Status: Backups (OK), Backup servers (OK), Management server (OK), License (Warning).

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 [License Update Session Data](#) section. Similar messages are received as pop-ups after you force the immediate update.

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.

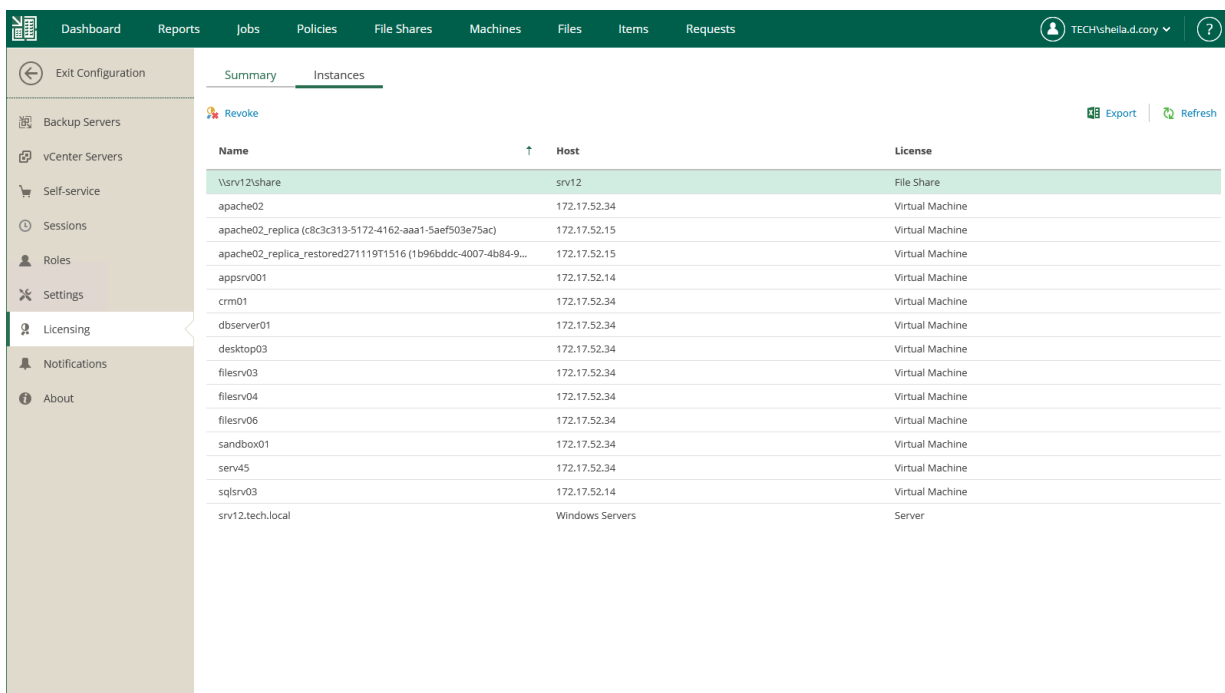
Message	Reason	Comment
<p>"New license key has been received"</p> <p>"New license key has been installed"</p> <p>"License key has been auto-updated"</p>	<p>This sequence of messages means automatic license key update procedure has completed successfully.</p>	<p>You can open the License Information dialog in Veeam backup console or the Licensing section in Enterprise Manager to examine the details.</p>
<p>"License key type is not supported at the moment"</p>	<p>License key generation failed due to currently unsupported license type.</p>	<p>Currently, automatic update is supported only for licenses associated with <i>Hosting Rental</i> contract type.</p>
<p>"License key is invalid"</p>	<p>License signature (identifier) is invalid.</p>	<p>Contact your Veeam sales representative.</p>
<p>"Your existing license key is up to date"</p>	<p>License expiration date is more than 7 days from now.</p>	<p>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.</p>
<p>"Your contract has expired, so the license key cannot be updated automatically. Please contact your Veeam sales representative to renew your contract."</p>	<p>Your contract has expired and needs to be renewed.</p>	<p>Contact your Veeam sales representative for contract renewal.</p>
<p>"General license key generation error has occurred"</p>	<p>Web licensing server did not return a new key upon request due to some other reason.</p>	<p>Wait for 24 hours (Veeam will re-try to update the key). Retries will take place for 1 month after key expiration date.</p>

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**.



The screenshot shows the Veeam Backup Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECHSheila.d.cory. The left sidebar shows the Configuration view with the Licensing section selected. The main area displays the Instances tab with a table of instances.

Name	Host	License
vsrv12\share	srv12	File Share
apache02	172.17.52.34	Virtual Machine
apache02_replica (c8c3c313-5172-4162-aaa1-5aef503e75ac)	172.17.52.15	Virtual Machine
apache02_replica_restored271119T1516 (1b96bddc-4007-4b84-9...	172.17.52.15	Virtual Machine
appsrv001	172.17.52.14	Virtual Machine
crm01	172.17.52.34	Virtual Machine
dbserver01	172.17.52.34	Virtual Machine
desktop03	172.17.52.34	Virtual Machine
filesrv03	172.17.52.34	Virtual Machine
filesrv04	172.17.52.34	Virtual Machine
filesrv06	172.17.52.34	Virtual Machine
sandbox01	172.17.52.34	Virtual Machine
serv45	172.17.52.34	Virtual Machine
sqlsrv03	172.17.52.14	Virtual Machine
srv12.tech.local	Windows Servers	Server

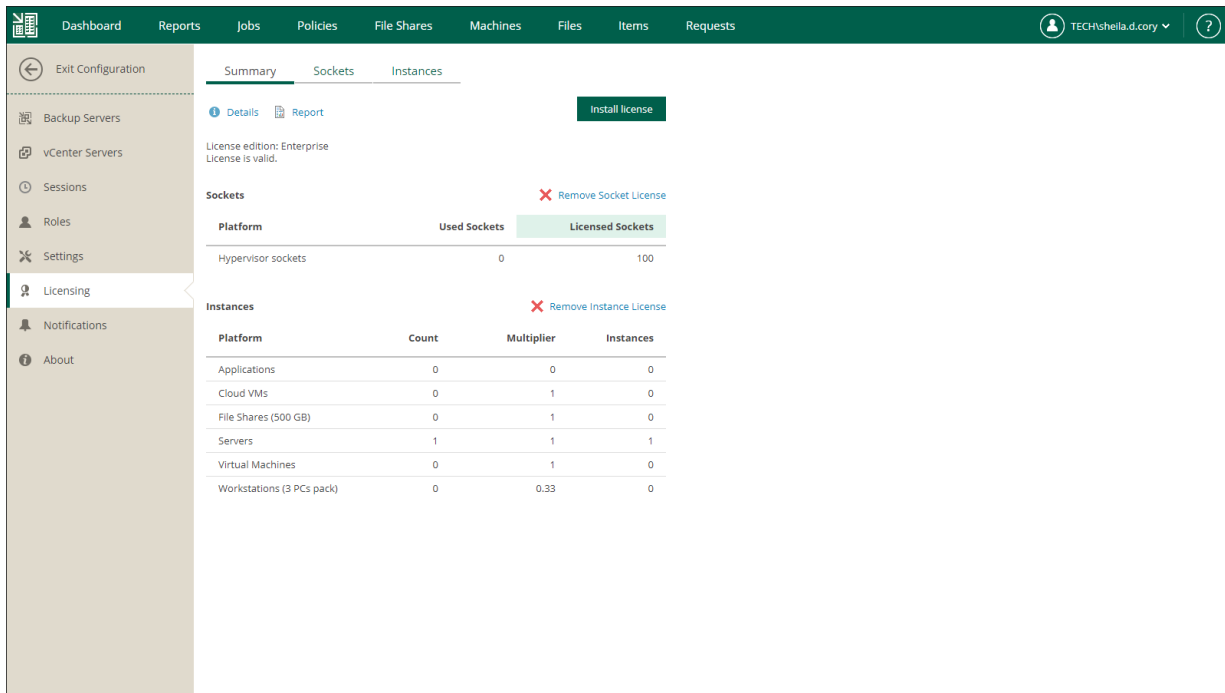
Removing License

Since Veeam Backup Enterprise Manager does not work without a license, you are not able to remove an installed license completely. You can replace already installed license by installing a new license.

If you have a merged license installed, you can remove a part of it: a socket license or an instance license. After you remove a part of the merged license, Veeam Backup Enterprise Manager and connected backup servers will operate under the other part of the merged license.

To remove a part of a merged license, do the following:

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 **Remove Socket License** or **Remove Instance License**.
5. To confirm the removal, click **Yes**.



Managing Monthly Usage Reports

Veeam Cloud & Service Providers (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](#)

April 2021
License information

Edition	Enterprise Plus
Expiration Date	6/1/2021
Company	Veeam Software Group GmbH
Support ID	02067762
Installation ID	1050A970-9493-449A-900C-5842B4DE7CF0

Summary

Type	Count	Multiplier	Instances
VMs	2	11	22 22 (rounded)

enterprise06.tech.local (22 instances)

VMs (22 instances)

Name	Instances	Type	Job name	Last processed	Note
dbserver01	11	vSphere	Backup Job 1	04/07/2021	
winsrv100	11	vSphere	Backup Job 1	04/07/2021	

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:

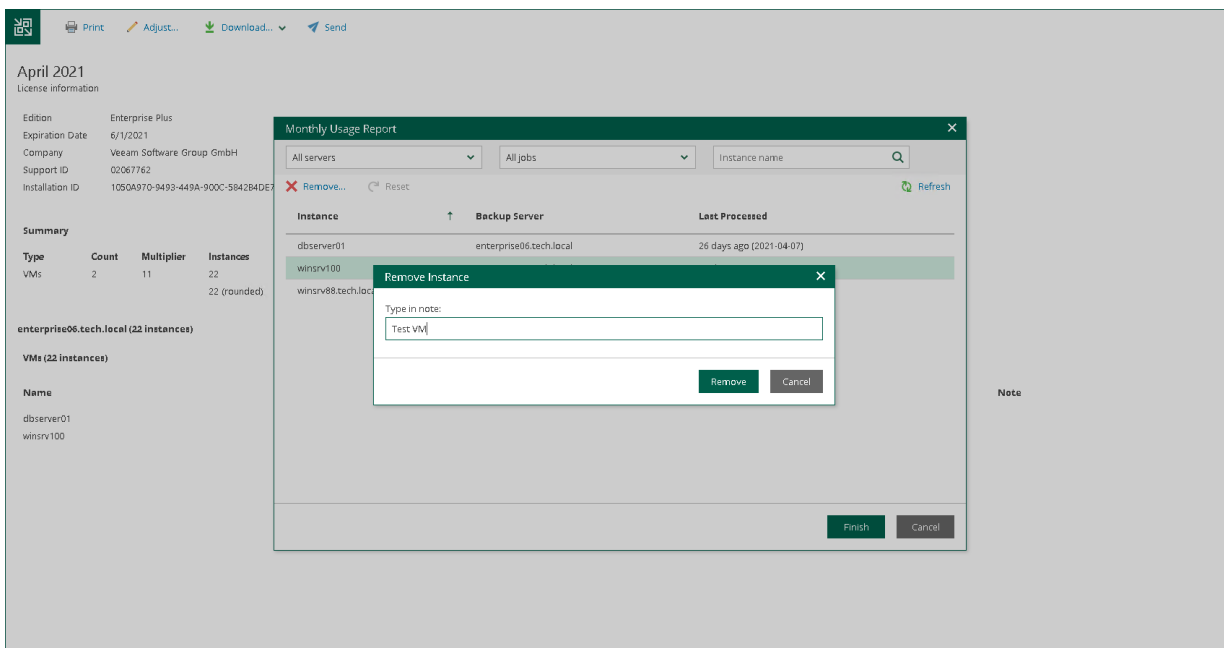
1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, click **Review**.
3. On the report page, click **Adjust**.
4. In the list of VMs, select the VM that you want to remove from the report and click **Remove**.

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.

The screenshot displays the Veeam Backup Enterprise Manager dashboard. At the top, a navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. A user profile 'TECH\shella.d.cory' and 'Configuration' settings are visible. A warning banner states: 'Warning: Please submit a monthly usage report (7 days left)'. Below this, there are tabs for 'Last 24 hours' and 'Last 7 days'. The main dashboard area is divided into several panels: 'Summary' (Backup servers: 1, Jobs: 2, Machines: 2, File shares: 1), 'Image Data' (Processing speed: 18 MB/s, Source size: 32 GB, Full backups: 8 GB, Restore points: 5.3 GB), 'File Data' (Processing speed: 0 KB/s, Source size: 4.5 MB, Backup: 4.2 MB, Archive: 0 B), 'Last 24 hours' (Total job runs: 2, Success: 2, Warning: 0, Error: 0), and 'Status' (Backups: OK, Backup servers: OK, Management server: OK, License: OK). A 'Backup Servers' chart shows throughput over time. A 'Monthly Usage Report' notification window is open, displaying a message: 'Monthly usage report has been generated. Number of managed instances for the previous month: 3. Please review and submit the report within the next 7 days.' The notification includes a 'Review' button, a 'Download' dropdown menu (with 'PDF' and 'JSON' options), and a 'Postpone' button. The 'Download' menu is currently open, showing the 'PDF' and 'JSON' options.

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.

The screenshot shows the Veeam Backup Enterprise Manager interface. At the top, there is a navigation bar with tabs for Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. A warning banner at the top left states: "Warning: Please submit a monthly usage report (6 days left)". Below the navigation bar, there are several data panels: Summary, Image Data, File Data, Last 24 hours, and Status. A "Monthly Usage Report" dialog box is open in the center, displaying a question mark icon and the text: "Monthly usage report has been generated. Number of managed instances for the previous month: 3. Please review and submit the report within the next 6 days." The dialog box has three buttons: "Review", "Send", and "Postpone". Below the dialog box, there is a "Backup Servers" section with a line graph showing throughput over time. The graph has a y-axis labeled "Throughput (GB/s)" ranging from 1.00 to 10 000.00 and an x-axis showing time from 06:00 pm to 04:00 pm. To the right of the graph, there is a "Name" section with a single entry: "enterprise06.tech.local".

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. [Select Enterprise Manager as a product to install](#).
3. [Read and accept the license agreements](#).
4. [Provide a license file](#).
5. [Install missing software](#).
6. [Review the default installation settings](#).
7. [Specify service account settings](#).
8. [Specify a database server](#).
9. [Specify data locations](#).
10. [Specify service ports](#).
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 [Permissions](#).
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see [Ports](#).
- Local antivirus or antimalware software can interfere with Veeam Backup Enterprise Manager installation. 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 completes. For more information, see [this Veeam KB article](#).
- .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.
- Make sure there is no Microsoft Search Server installed on the machine. If you have Microsoft Search Server, uninstall it prior to the Veeam Backup Enterprise Manager installation.
- Check the *Known Issues* section of the [Veeam Backup & Replication 12 Release Notes](#).

Step 1. Start Setup Wizard

To start the setup wizard, take the following steps:

1. Download the latest version of the Veeam Backup & Replication installation image from the [Veeam Product Downloads](#) page.
2. Mount the installation image to the machine where you plan to install Veeam Backup Enterprise Manager or burn the image file to a flash drive or other removable storage device. 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 ISO files of large size and can properly work with long file paths.

3. After you mount the image or insert the disk, Autorun opens a splash screen. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. Click **Install**.

IMPORTANT

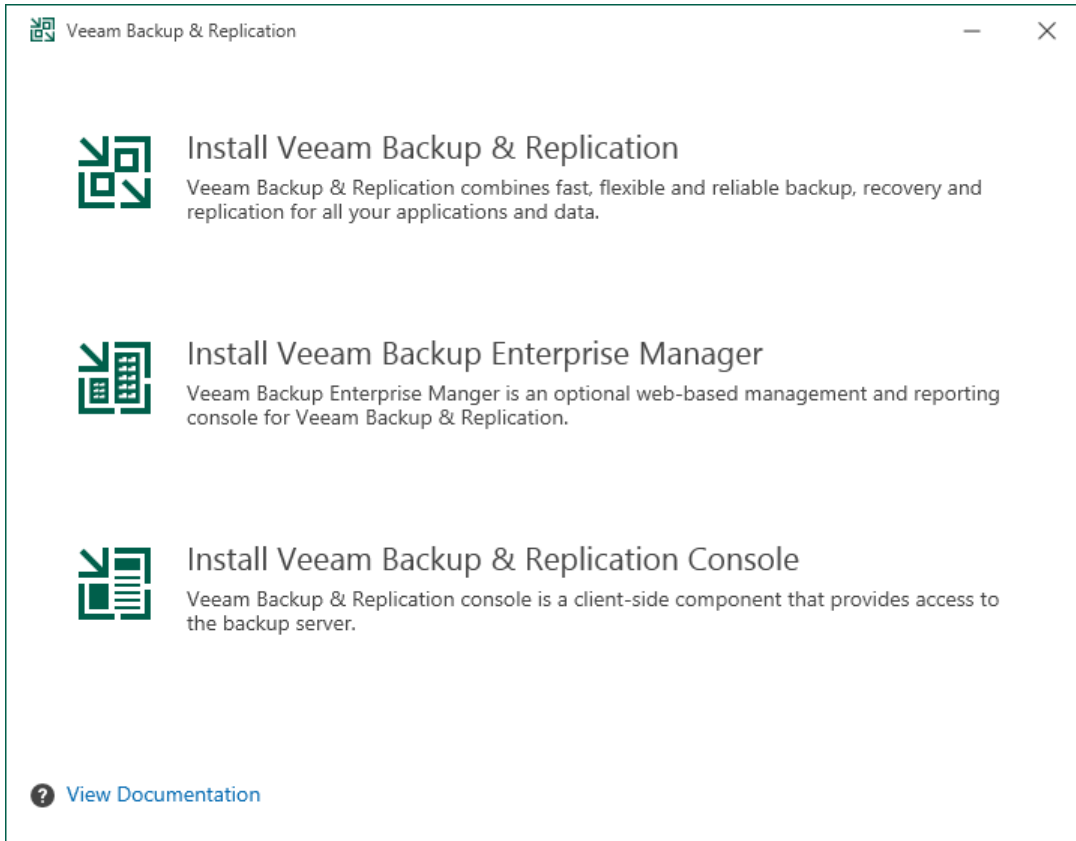
It is strongly recommended that you install Veeam Backup Enterprise Manager using Autorun or the `Setup.exe` file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup Enterprise Manager may not work as expected.



Step 2. Select Product

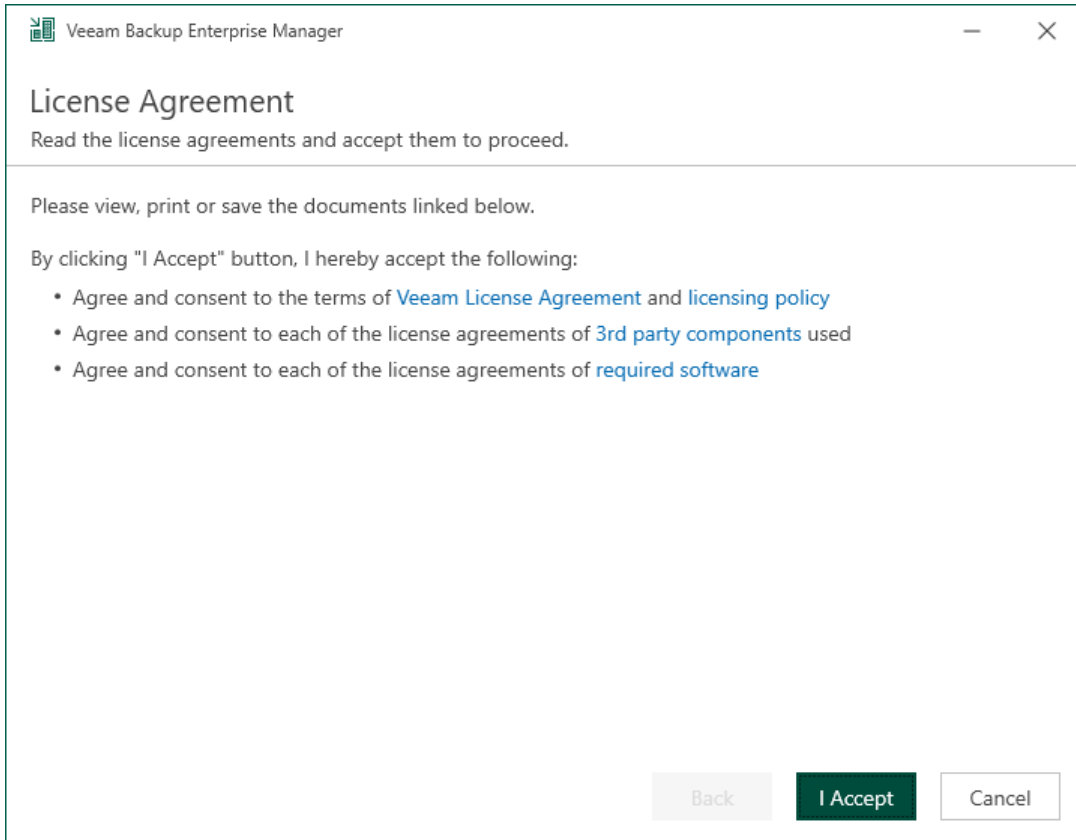
At this step of the wizard, select **Install Veeam Backup Enterprise Manager**.

To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Read and Accept License Agreements

At the **License Agreement** step of the wizard, read Veeam License Agreement and licensing policy as well as license agreements of 3rd party components that Veeam incorporates and license agreements of required software. To accept the license agreements and continue installing Veeam Backup Enterprise Manager, click **I Accept**.



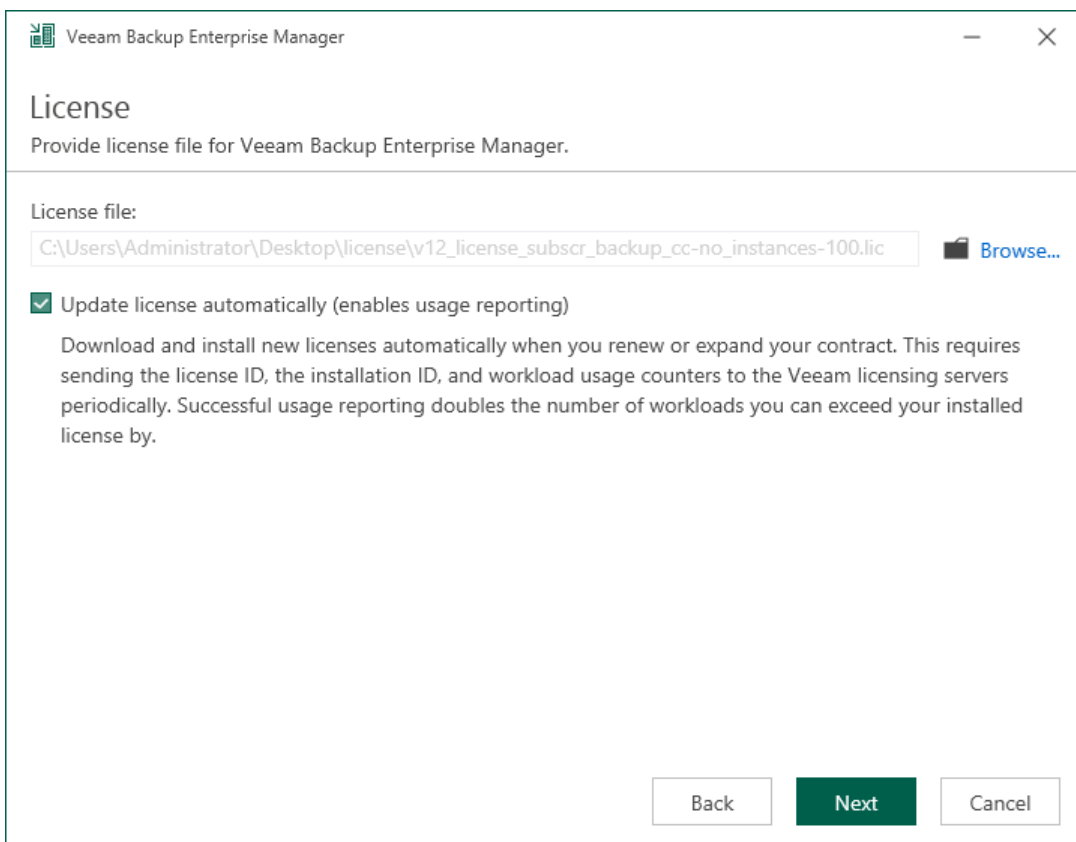
Step 4. Provide License File

At the **License** step of the wizard, specify what license you want to install for Veeam Backup Enterprise Manager. You can install the following types of licenses:

- Trial license that was sent to you after you downloaded the product.
- Purchased full license.

To provide a license, do the following:

1. Next to the **License file** field, click **Browse**.
2. Choose a valid license file for Veeam Backup Enterprise Manager.
3. To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. For more information on license update, see [Updating License](#).



The screenshot shows the 'License' dialog box in Veeam Backup Enterprise Manager. The title bar reads 'Veeam Backup Enterprise Manager'. The main heading is 'License' with the instruction 'Provide license file for Veeam Backup Enterprise Manager.' Below this, there is a 'License file:' label followed by a text input field containing the path 'C:\Users\Administrator\Desktop\license\v12_license_subscr_backup_cc-no_instances-100.lic'. To the right of the input field is a 'Browse...' button with a folder icon. Below the input field, there is a checked checkbox labeled 'Update license automatically (enables usage reporting)'. Underneath the checkbox, there is a paragraph of text: 'Download and install new licenses automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to the Veeam licensing servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.' At the bottom of the dialog, there are three buttons: 'Back', 'Next' (which is highlighted in green), and 'Cancel'.

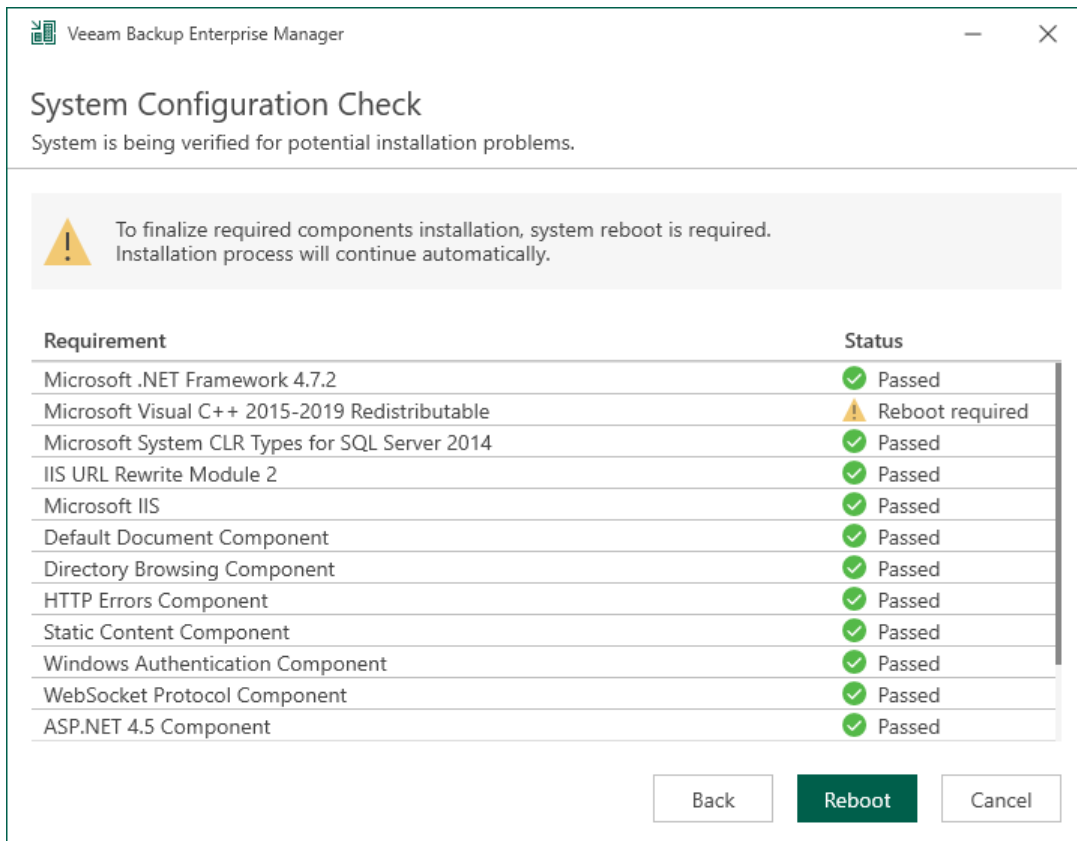
Step 5. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup checks whether required software is installed on the machine. If some of the required components are missing, the setup will try to install them automatically. After the components are installed successfully, reboot is required. When you are ready to reboot the machine, click **Reboot**.

If the setup is not able to install some of the required software automatically, install it manually and click **Retry**.

NOTE


If all required software is already installed on the machine, the **System Configuration Check** step will be skipped. For more information on the necessary software, see [System Requirements](#).



Veeam Backup Enterprise Manager

System Configuration Check

System is being verified for potential installation problems.

 To finalize required components installation, system reboot is required. Installation process will continue automatically.

Requirement	Status
Microsoft .NET Framework 4.7.2	Passed
Microsoft Visual C++ 2015-2019 Redistributable	Reboot required
Microsoft System CLR Types for SQL Server 2014	Passed
IIS URL Rewrite Module 2	Passed
Microsoft IIS	Passed
Default Document Component	Passed
Directory Browsing Component	Passed
HTTP Errors Component	Passed
Static Content Component	Passed
Windows Authentication Component	Passed
WebSocket Protocol Component	Passed
ASP.NET 4.5 Component	Passed

Back Reboot Cancel

Step 6. Review Default Installation Settings

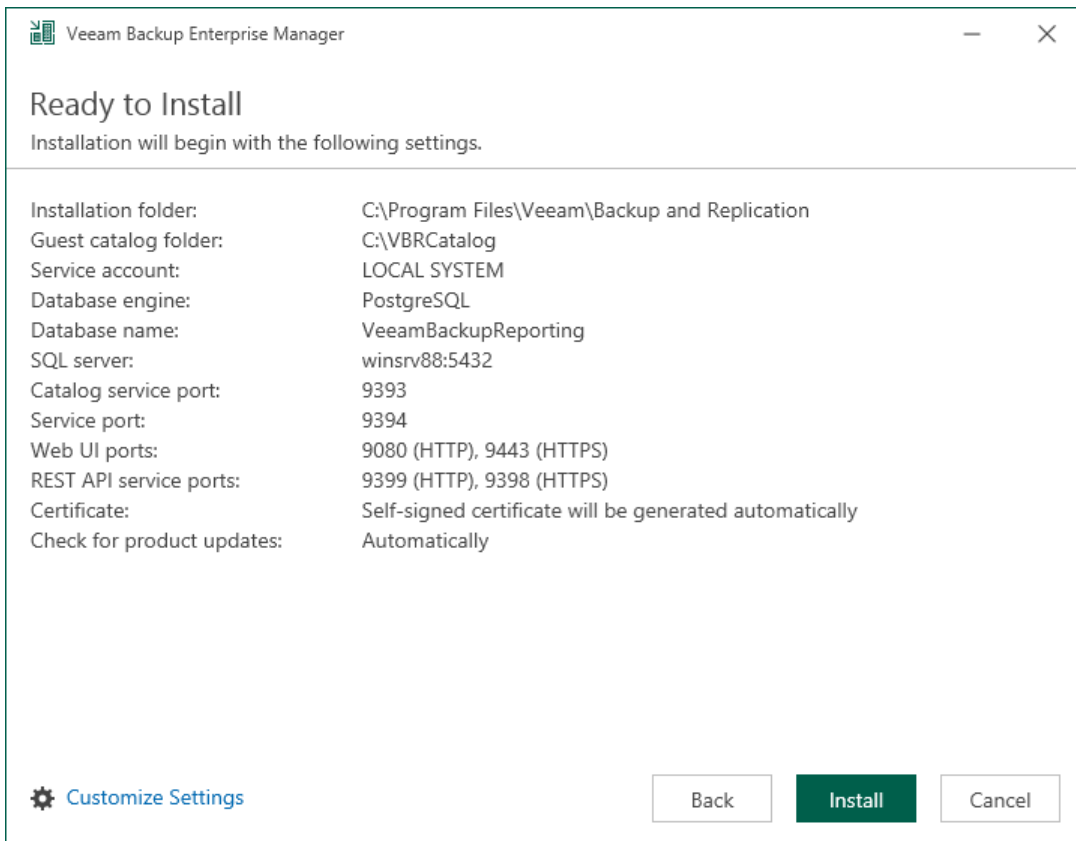
At the **Ready to Install** step of the wizard, you can select to install Veeam Backup Enterprise Manager with default installation settings or specify custom installation settings.

- To use the default installation settings, click **Install**.
- To use custom installation settings, click **Customize Settings**. The setup wizard will include additional steps that will let you configure installation settings.

The table below lists the default installation settings.

Setting	Default Value	Description
Installation folder	<i>%ProgramFiles% Veeam Backup and Replication</i>	Folder where Veeam Backup Enterprise Manager is installed.
Guest catalog folder	<i>C: VBRCatalog</i>	The <code>VBRCatalog</code> folder on a volume with the maximum amount of free space. 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.
Service account	<i>LOCAL SYSTEM</i>	Account under which the Veeam Backup Enterprise Manager runs.
Database engine	<i>PostgreSQL</i>	The setup installs PostgreSQL 15.1 locally on the Veeam Backup Enterprise Manager server.
Database name	<i>VeeamBackupReporting</i>	The setup deploys the Veeam Backup Enterprise Manager configuration database on the locally installed instance of PostgreSQL.
Catalog service port	<i>9393</i>	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 port	<i>9394</i>	The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers.
Web UI ports	For HTTP protocol: <i>9080</i> For HTTPS protocol: <i>9443</i>	These ports are used for accessing Veeam Backup Enterprise Manager web interface.

Setting	Default Value	Description
REST API service ports	For HTTP protocol: <i>9399</i> For HTTPS protocol: <i>9398</i>	These ports are used for accessing Veeam Backup Enterprise Manager REST API.
Certificate	<i>Self-signed certificate will be generated automatically</i>	During installation a self-signed certificate is generated that will be used for all Enterprise Manager connections. You can update the certificate upon installation. For more information, see TLS Certificates .
Check for updates	<i>Automatically</i>	Veeam Backup Enterprise Manager will check for product updates weekly. When a new product build is published on the Veeam update server, a notification is displayed in the Windows Action Center.



Step 7. Specify Service Account Settings

The **Service Account** step of the wizard is available if you have selected to configure installation settings manually.

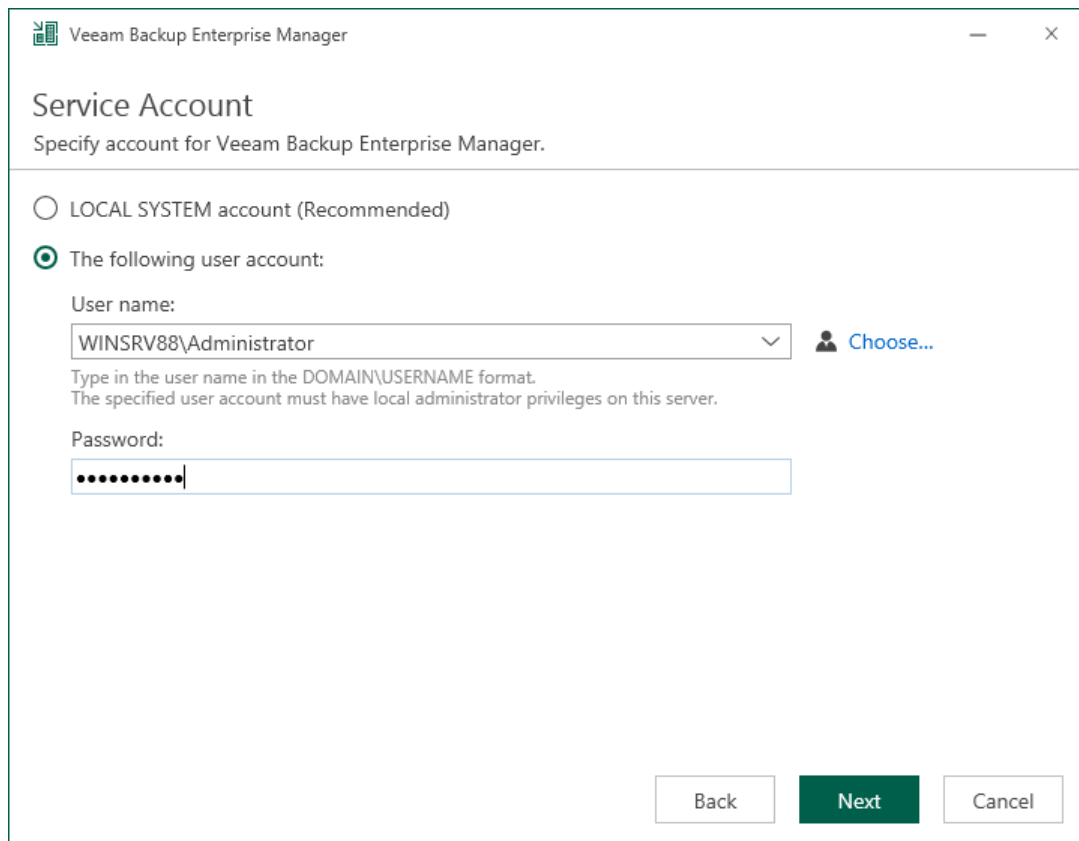
You can select an account under which you want to run the Veeam Backup Enterprise Manager Service:

- 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 [Permissions](#).



The screenshot shows a window titled "Veeam Backup Enterprise Manager" with the subtitle "Service Account". Below the subtitle is the instruction "Specify account for Veeam Backup Enterprise Manager." There are two radio button options: "LOCAL SYSTEM account (Recommended)" which is unselected, and "The following user account:" which is selected. Under the selected option, there is a "User name:" label followed by a text box containing "WINSRV88\Administrator" and a dropdown arrow. To the right of the text box is a "Choose..." button with a person icon. Below the text box is a note: "Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server." There is also a "Password:" label followed by a password field with masked characters. At the bottom right, there are three buttons: "Back", "Next" (highlighted in green), and "Cancel".

Step 8. Specify Database Server

The **Database** step of the wizard is available if you have selected to configure installation settings manually.

At this step of the wizard, you can choose a database engine (Microsoft SQL Server or PostgreSQL) for the Enterprise Manager configuration database, specify a new or existing instance where you want to deploy the configuration database, and specify the authentication mode.

NOTE

Note that configuration databases of the Enterprise Manager server and backup servers added to the Enterprise Manager infrastructure must use the same database engine.

1. Select one of the following database engines that you want to use for the configuration database:
 - PostgreSQL
 - Microsoft SQL Server
2. Specify instance settings:
 - [For PostgreSQL] You can use an already installed PostgreSQL instance or install a new one.
 - To install a new PostgreSQL instance, select the **Install a new instance** option. The setup will install PostgreSQL 15.1 on the Veeam Backup Enterprise Manager server and create a database with the *VeeamBackupReporting* name.
 - To use an already installed PostgreSQL instance, select the **Use the existing instance** option. Enter the instance name in the *HOSTNAME:PORT* format. In the **Database name** field, specify a name for the Veeam Backup Enterprise Manager configuration database.

Veeam Backup Enterprise Manager

Database

Choose database engine and instance for Veeam Backup Enterprise Manager.

Use following database engine: PostgreSQL Server

Install new instance

Use existing instance (HOSTNAME:PORT)

winsrv88:5432

Database name: VeeamBackupReporting

Connect to PostgreSQL Server using:

Windows authentication credentials of service account

Native authentication using the following credentials:

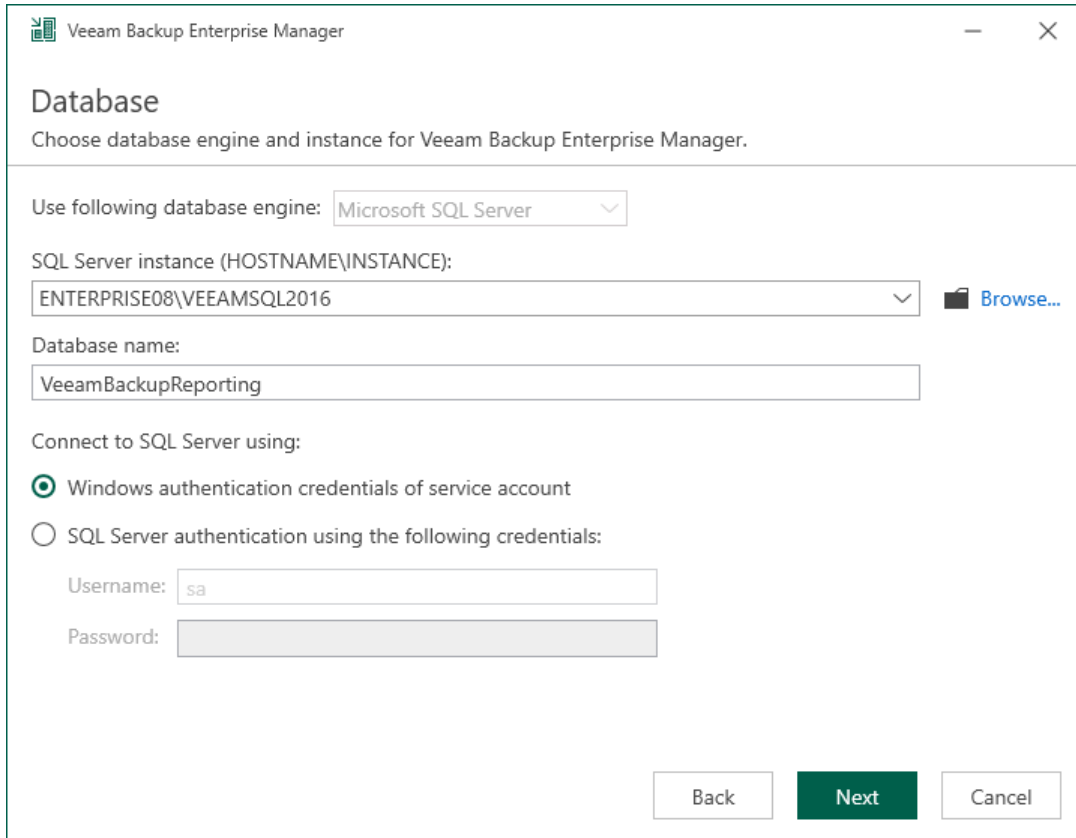
Login: postgres

Password:

Back Next Cancel

- [For Microsoft SQL Server] You can use an already installed Microsoft SQL Server database only.

- i. In the **SQL Server instance** field, enter the instance name in the *HOSTNAME\INSTANCE* format or select an instance from the drop-down list. You can also click **Browse** to choose a Microsoft SQL Server on a remote machine.
- ii. In the **Database name** field, specify a name for the Veeam Backup Enterprise Manager configuration database.



The screenshot shows the 'Database' configuration window in Veeam Backup Enterprise Manager. The window title is 'Veeam Backup Enterprise Manager'. The main heading is 'Database' with the instruction 'Choose database engine and instance for Veeam Backup Enterprise Manager.' The configuration options are as follows:

- Use following database engine:** A dropdown menu set to 'Microsoft SQL Server'.
- SQL Server instance (HOSTNAME\INSTANCE):** A dropdown menu set to 'ENTERPRISE08\VEEAMSQL2016' with a 'Browse...' button to its right.
- Database name:** A text input field containing 'VeeamBackupReporting'.
- Connect to SQL Server using:** Two radio button options:
 - Windows authentication credentials of service account
 - SQL Server authentication using the following credentials:
- SQL Server authentication fields:** A 'Username:' field containing 'sa' and a 'Password:' field which is currently empty.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

3. Select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the database account.

If a configuration database with the specified name already exists (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.

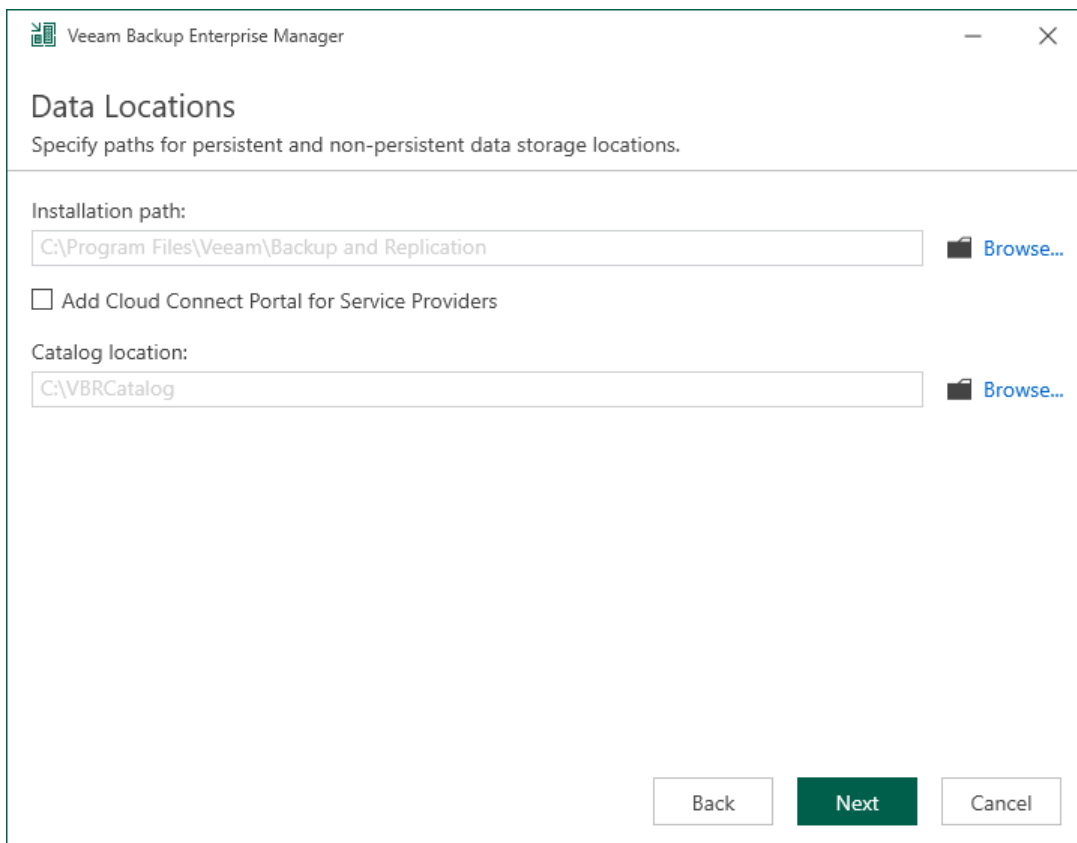
Step 9. Specify Data Locations

The **Data Locations** step is available if you have selected to configure installation settings manually and to install a new instance of the database server.

At this step of the wizard, you can specify an installation folder and a folder for the guest file system catalog. Service providers that use Veeam Backup & Replication to offer disaster recovery as a service to their tenants can also choose to install Veeam Cloud Connect Portal. For more information on the portal, see the [Veeam Cloud Connect Portal](#) section of the Veeam Cloud Connect Guide.

1. To change the default installation folder, click **Browse** next to the **Installation path** field.
The default installation folder is %ProgramFiles%\Veeam\Backup and Replication.
2. To install Veeam Cloud Connect Portal, select the **Add Cloud Connect Portal for Service Providers** check box.
3. To change a path to the folder where index files must be stored, click **Browse** next to the **Catalog location** field.

By default, the setup wizard creates the `VBRCatalog` folder on a volume with the maximum amount of free space, for example: `C:\VBRCatalog`.



The screenshot shows the 'Data Locations' step of the Veeam Backup Enterprise Manager installation wizard. The window title is 'Veeam Backup Enterprise Manager'. The main heading is 'Data Locations' with the instruction 'Specify paths for persistent and non-persistent data storage locations.' Below this, there are three main sections: 1. 'Installation path:' with a text box containing 'C:\Program Files\Veeam\Backup and Replication' and a 'Browse...' button. 2. A checkbox labeled 'Add Cloud Connect Portal for Service Providers' which is currently unchecked. 3. 'Catalog location:' with a text box containing 'C:\VBRCatalog' and a 'Browse...' button. At the bottom of the window, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

Step 10. Specify Service Ports

The **Port Configuration** step of the wizard is available if you have selected to configure installation settings manually.

At this step of the wizard, you can customize ports that will be used for communication between backup infrastructure components. For more information about Veeam Backup Enterprise Manager used ports, see [Ports](#).

1. Provide HTTP and HTTPS port numbers.

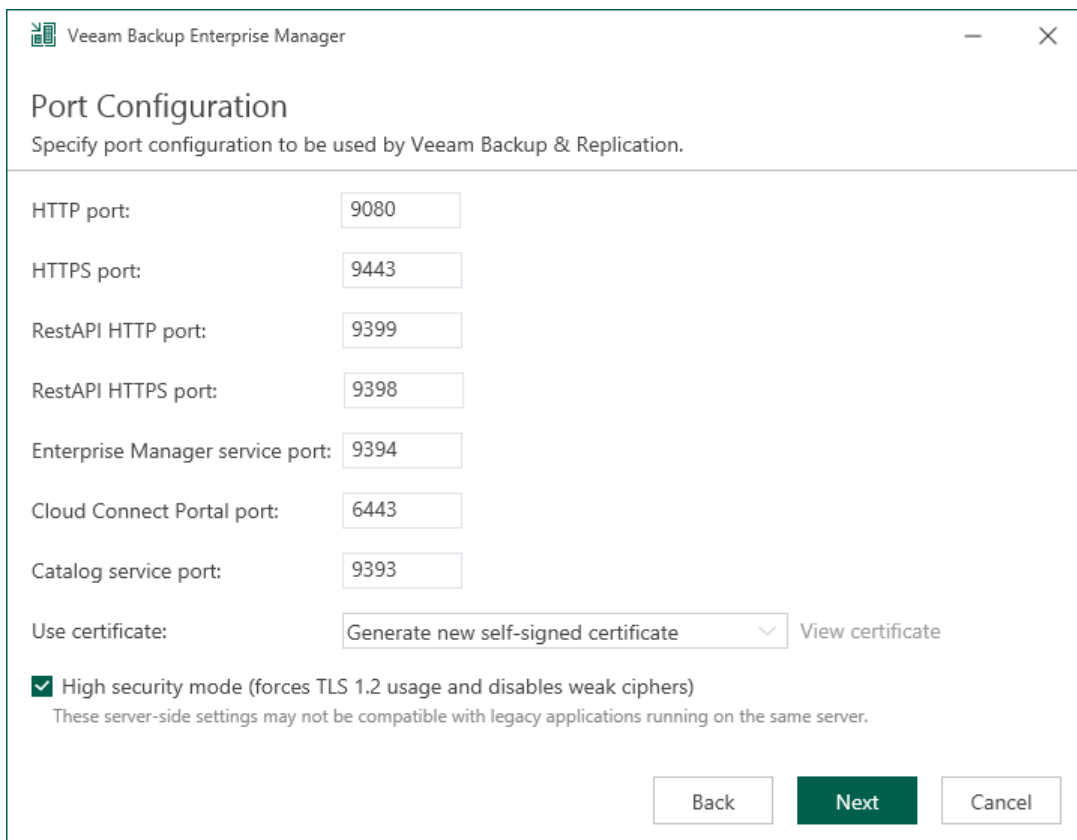
If you are installing Veeam Cloud Connect Portal, you can also specify a port number that will be used by browser to access its website (the default port is *6443*).

2. Specify 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; Veeam plug-in for vSphere Client and REST API client also will use this certificate to receive data using HTTPS protocol. If the setup wizard does not find an appropriate certificate, it will generate a self-signed certificate.

Click **View certificate** to review the details of the selected certificate.

3. To enforce TLS 1.2 encryption protocol for network connections, select the **High security mode** check box.

This 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.



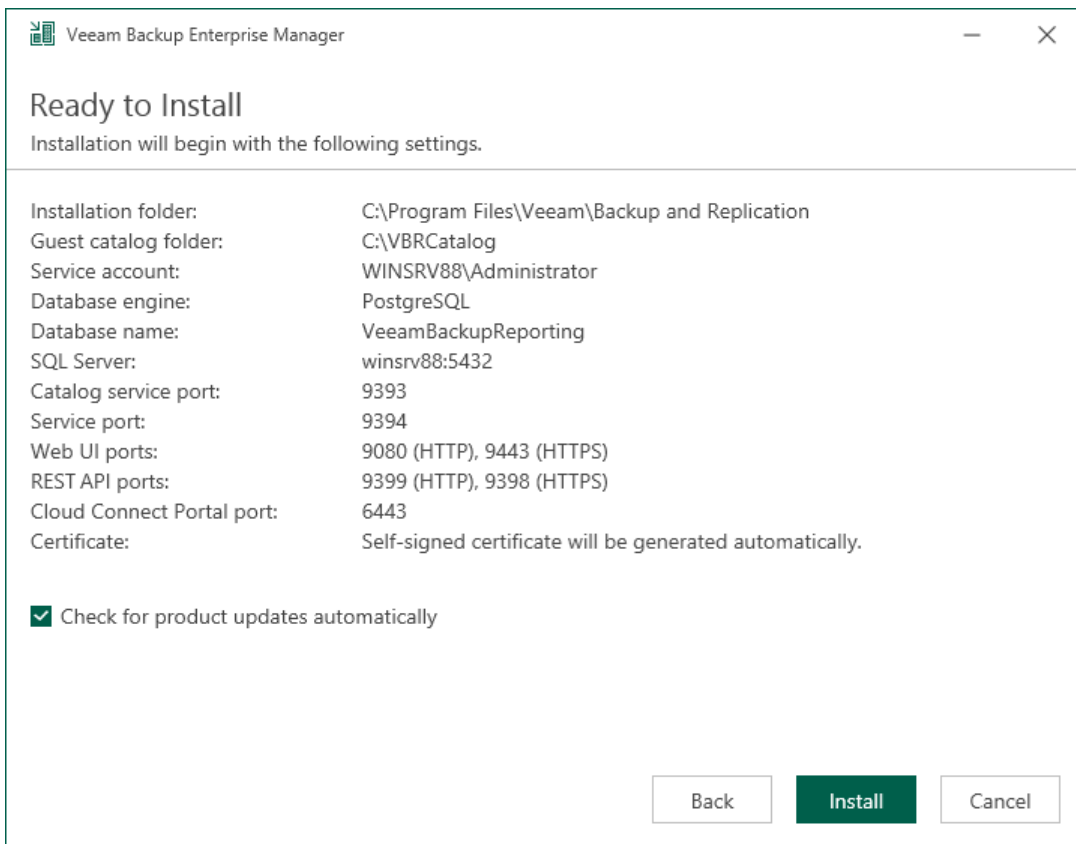
The screenshot shows the 'Port Configuration' window of the Veeam Backup Enterprise Manager wizard. The window title is 'Veeam Backup Enterprise Manager' and the subtitle is 'Port Configuration'. Below the subtitle, it says 'Specify port configuration to be used by Veeam Backup & Replication.' The window contains several input fields for port numbers: HTTP port (9080), HTTPS port (9443), RestAPI HTTP port (9399), RestAPI HTTPS port (9398), Enterprise Manager service port (9394), Cloud Connect Portal port (6443), and Catalog service port (9393). There is a dropdown menu for 'Use certificate:' set to 'Generate new self-signed certificate' with a 'View certificate' link next to it. A checked checkbox for 'High security mode (forces TLS 1.2 usage and disables weak ciphers)' is present, with a note below it: 'These server-side settings may not be compatible with legacy applications running on the same server.' At the bottom, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

Step 11. Begin Installation

The **Ready to Install** step of the wizard is available if you have selected to configure installation settings manually.

At this step of the wizard, you can review the Veeam Backup Enterprise Manager installation settings and start the installation process:

1. If you want Veeam Backup Enterprise Manager to check for product updates weekly, select the **Check for product updates automatically** check box. When a new product build is published on the Veeam update server, a notification will be displayed in the Windows Action Center.
2. Click **Install** to begin the installation.
3. 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 to Veeam Backup Enterprise Manager 12

Before you upgrade Veeam Backup Enterprise Manager to version 12, [check prerequisites](#).

To upgrade Veeam Backup Enterprise Manager, take the following steps:

1. [Start the upgrade wizard](#).
2. [Select Enterprise Manager as a product to upgrade](#).
3. [Read and accept the license agreements](#).
4. [Review Enterprise Manager components to upgrade](#).
5. [Provide a license file](#).
6. [Specify service account settings](#).
7. [Specify a database server](#).
8. [Begin upgrade](#).
9. [Finalize upgrade](#).

Before You Begin

Before starting the upgrade procedure, read and follow the recommendations below:

- To upgrade Veeam Backup Enterprise Manager to version 12, you must be running version 10a (build 10.0.1.4854) or later. To upgrade from earlier versions, contact [Veeam Customer Support](#).
- 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 upgrade must have sufficient permissions. For more information, see [Permissions](#).
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see [Ports](#).
- Local antivirus or antimalware software can interfere with Veeam Backup Enterprise Manager upgrade. If you receive the *Failed to create website 0x80070020* message, disable your local antivirus or antimalware software and start the upgrade process again. You can re-enable your antivirus software once the upgrade completes. For more information, see [this Veeam KB article](#).
- .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.
- Check the *Known Issues* section of the [Veeam Backup & Replication 12 Release Notes](#).
- 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 a backup server installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server.

Step 1. Start Upgrade Wizard

To start the upgrade wizard, take the following steps:

1. Download the latest version of the Veeam Backup & Replication installation image from the [Veeam Product Downloads](#) page.
2. Mount the installation image to the machine where Veeam Backup Enterprise Manager is installed, or burn the image file to a flash drive or other removable storage device. If you plan to upgrade Veeam Backup Enterprise Manager on a VM, use built-in tools of the virtualization management software to mount the 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 ISO files of large size and can properly work with long file paths.

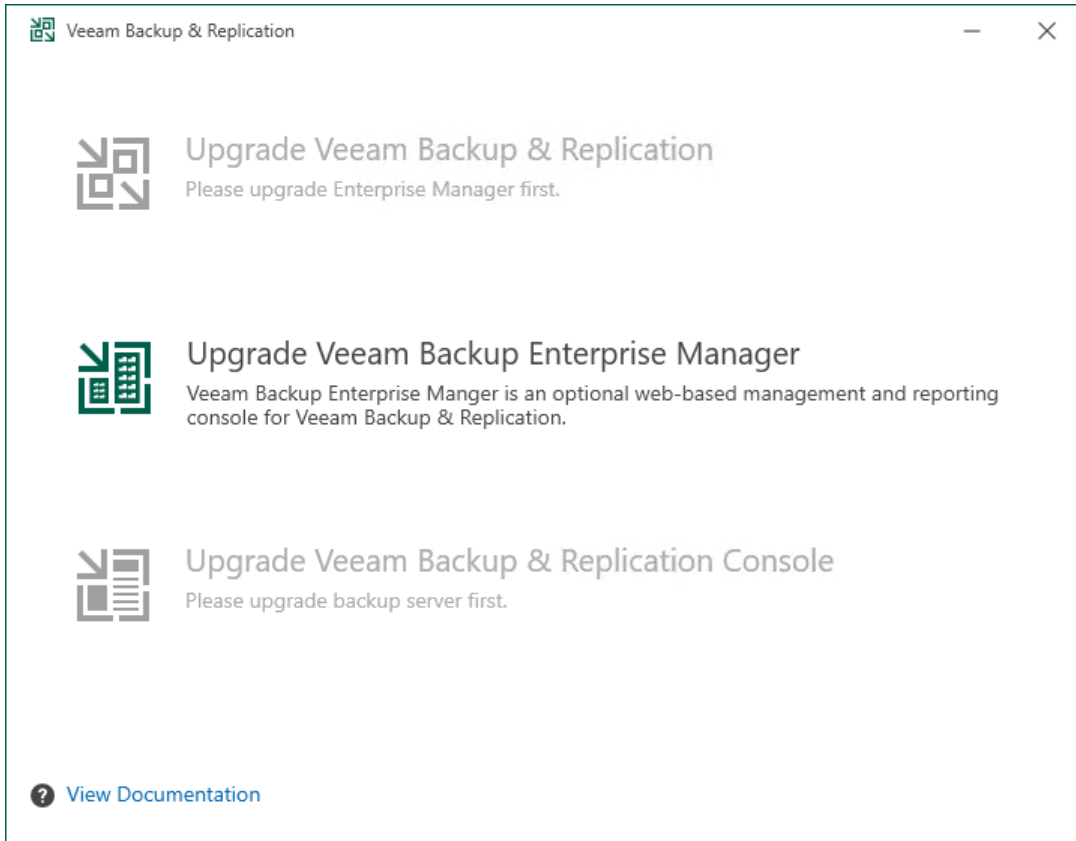
3. After you mount the image or insert the disk, Autorun opens a splash screen. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. Click **Upgrade**.



Step 2. Select Product

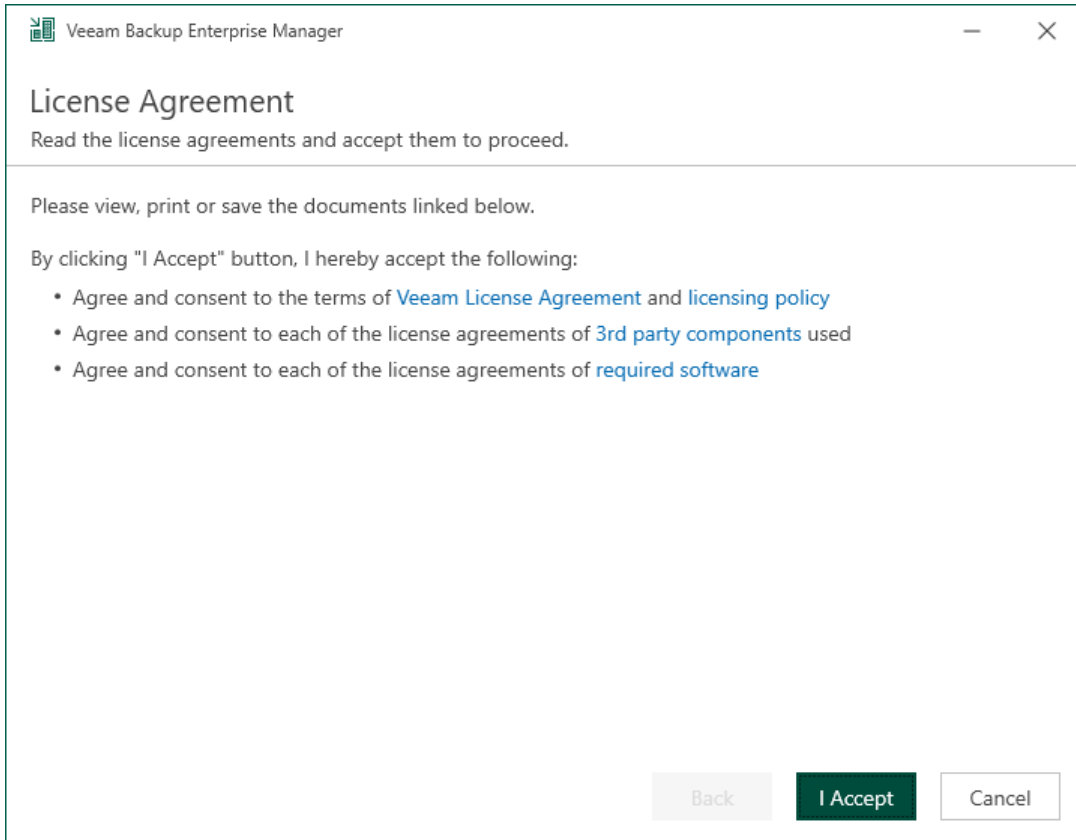
At this step of the wizard, select **Upgrade Veeam Backup Enterprise Manager**.

To open Veeam Help Center from the upgrade wizard, click **View Documentation**.



Step 3. Read and Accept License Agreements

At the **License Agreement** step of the wizard, read Veeam License Agreement and licensing policy as well as license agreements of 3rd party components that Veeam incorporates and license agreements of required software. To accept the license agreements and continue installing Veeam Backup Enterprise Manager, click **I Accept**.



Step 4. Review Components

At the **Upgrade** step of the wizard, you can review the components that will be upgraded.

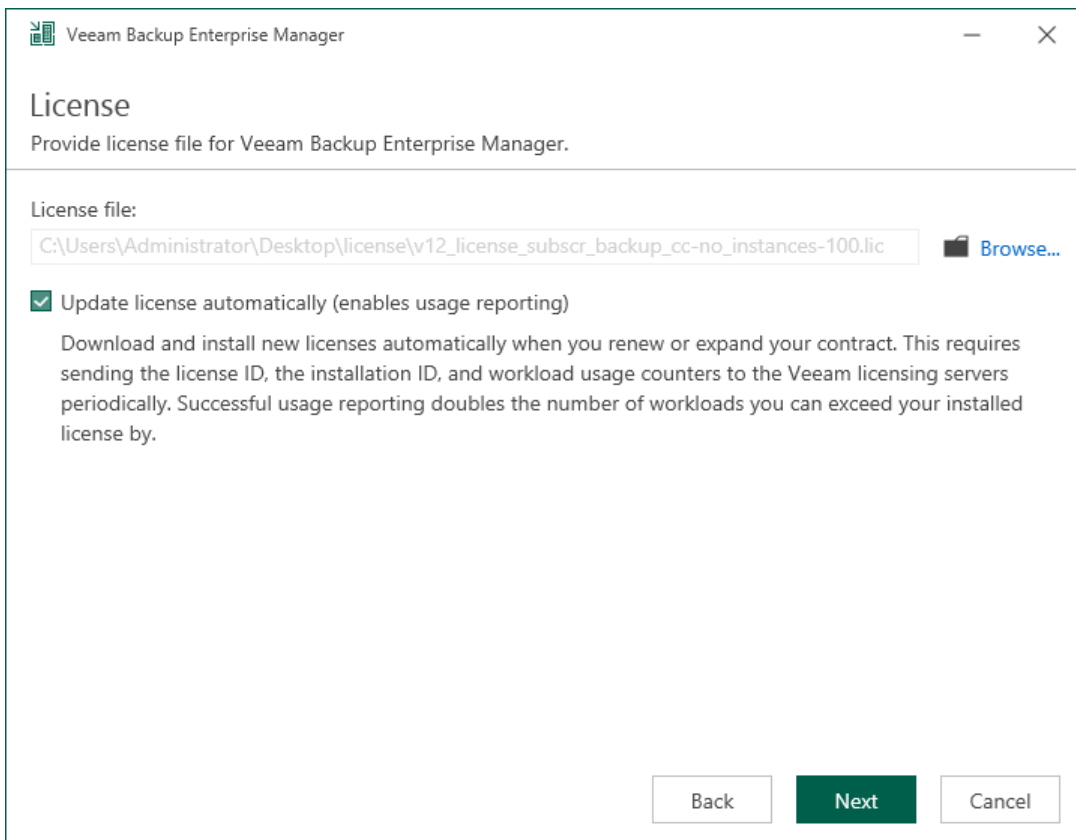
Product	Version
Veeam Backup Catalog	11.0.1.1261 → 12.0.0.1326
Veeam Backup Enterprise Manager	11.0.1.1261 → 12.0.0.1326

Step 5. Provide License File

At the **License** step of the wizard, specify what license you want to install for Veeam Backup Enterprise Manager. You can leave the license file used in the previous version of Veeam Backup Enterprise Manager or install a new one.

To provide a license, do the following:

1. Next to the **License file** field, click **Browse**.
2. Choose a valid license file for Veeam Backup Enterprise Manager.
3. To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. For more information on license update, see [Updating License](#).



The screenshot shows the 'License' dialog box in Veeam Backup Enterprise Manager. The title bar reads 'Veeam Backup Enterprise Manager'. The main heading is 'License' with the subtitle 'Provide license file for Veeam Backup Enterprise Manager.' Below this, there is a 'License file:' label followed by a text input field containing the path 'C:\Users\Administrator\Desktop\license\v12_license_subscr_backup_cc-no_instances-100.lic'. To the right of the input field is a 'Browse...' button with a folder icon. Below the input field is a checked checkbox labeled 'Update license automatically (enables usage reporting)'. Underneath the checkbox is a paragraph of text: 'Download and install new licenses automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to the Veeam licensing servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.' At the bottom of the dialog are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

Step 6. Specify Service Account Settings

The **Service Account** step of the wizard is available if you have selected to configure installation settings manually.

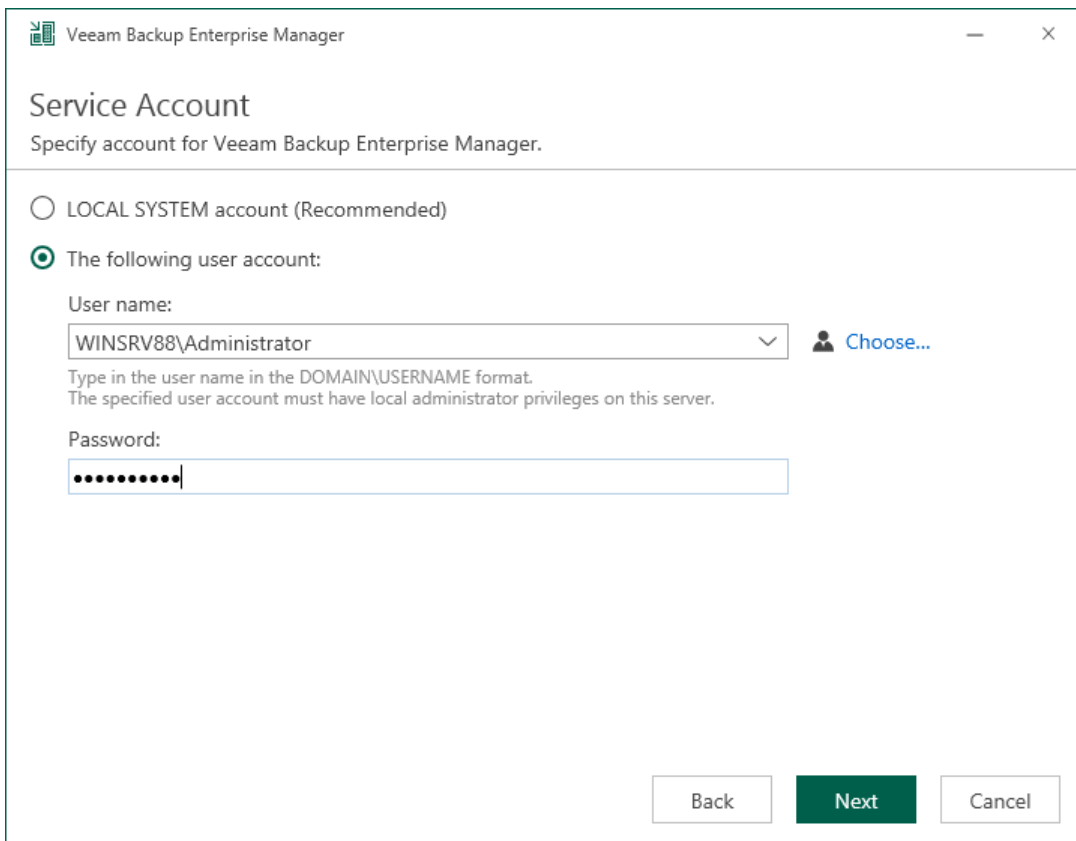
You can select an account under which you want to run the Veeam Backup Enterprise Manager Service:

- 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 [Permissions](#).



The screenshot shows a window titled "Veeam Backup Enterprise Manager" with a subtitle "Service Account". Below the subtitle is the instruction "Specify account for Veeam Backup Enterprise Manager." There are two radio button options: "LOCAL SYSTEM account (Recommended)" and "The following user account:". The second option is selected. Under "The following user account:", there is a "User name:" label, a text box containing "WINSRV88\Administrator", and a "Choose..." button with a user icon. Below the text box is the instruction "Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server." There is also a "Password:" label and a password text box with masked characters. At the bottom right, there are three buttons: "Back", "Next" (highlighted in green), and "Cancel".

Step 7. Specify Database Server

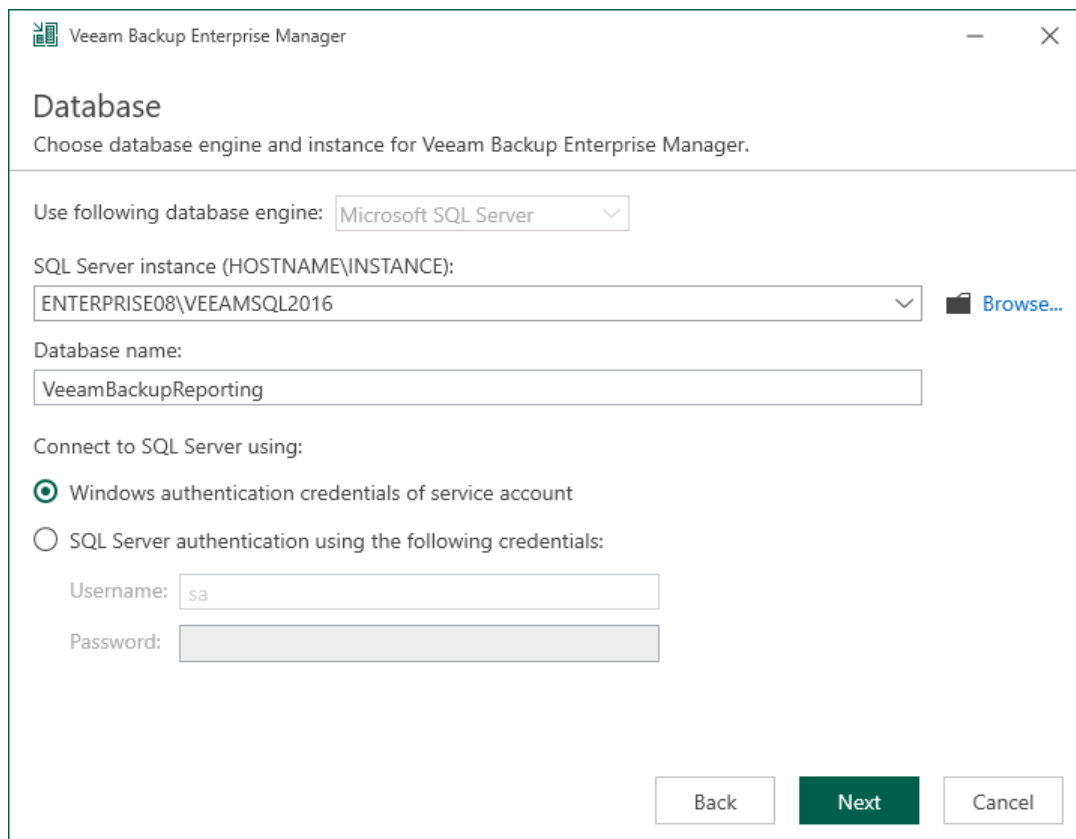
At the **Database** step of the wizard, select the Microsoft SQL server instance and database that were used by the previous version of Veeam Backup Enterprise Manager, and specify the authentication mode.

NOTE

After you upgrade Veeam Backup Enterprise Manager, you can migrate its configuration database to PostgreSQL using the Enterprise Manager Database Migration and Configuration Database Connection Settings utilities. For more information, see [Veeam Backup Enterprise Manager Utilities](#).

1. Specify instance settings:
 - a. In the **SQL Server instance** field, enter the instance name in the *HOSTNAME\INSTANCE* format or select an instance from the drop-down list. You can also click **Browse** to choose a Microsoft SQL Server on a remote machine.
 - b. In the **Database name** field, specify a name for the configuration database.
2. Select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the database account.
3. If the configuration database is in use by another Enterprise Manager server, the wizard will notify about it. To continue the installation, click **Yes**.
4. If the wizard detects a configuration database with the specified name (for example, it was created by a previous installation of Enterprise Manager), the wizard will notify about it. To connect to the detected database, click **Yes**.

Veeam Backup Enterprise Manager will automatically upgrade the database to the latest version.



The screenshot shows the 'Database' configuration window in Veeam Backup Enterprise Manager. The window title is 'Veeam Backup Enterprise Manager' and the subtitle is 'Database'. Below the subtitle, it says 'Choose database engine and instance for Veeam Backup Enterprise Manager.' The configuration options are as follows:

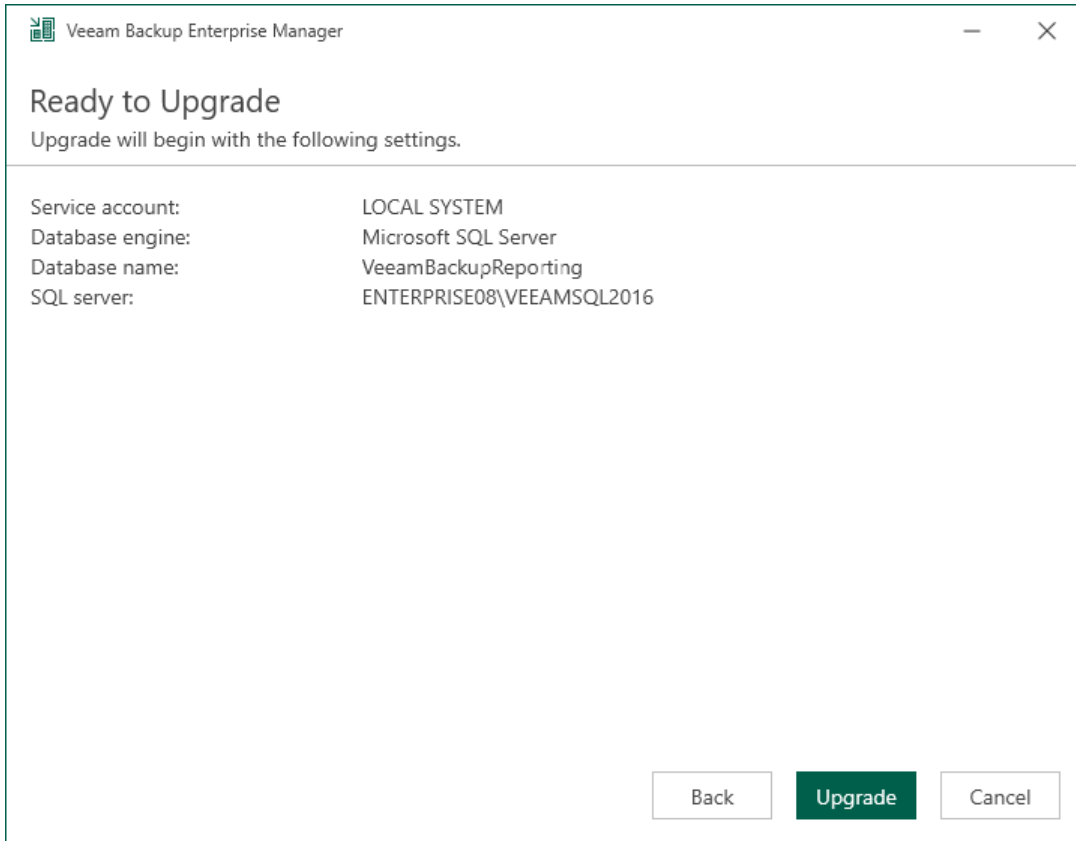
- Use following database engine:** A dropdown menu set to 'Microsoft SQL Server'.
- SQL Server instance (HOSTNAME\INSTANCE):** A text box containing 'ENTERPRISE08\VEEAMSQL2016' and a 'Browse...' button.
- Database name:** A text box containing 'VeeamBackupReporting'.
- Connect to SQL Server using:** Two radio button options:
 - Windows authentication credentials of service account
 - SQL Server authentication using the following credentials:
 - Username:** A text box containing 'sa'.
 - Password:** A password field.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

Step 8. Begin Upgrade

At the **Ready to Upgrade** step of the wizard, you can review the upgrade configuration and start the upgrade.

Wait for the upgrade process to complete and click **Finish** to exit the wizard.



Step 9. Finalize Upgrade

After you successfully upgraded Veeam Backup Enterprise Manager, consider the following recommendations:

1. If you have Veeam Backup & Replication installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server.
2. Proceed with upgrade of remote backup servers.

After you upgrade backup servers, Veeam Backup Enterprise Manager starts a maintenance job to optimize the state of its database. The initial maintenance job 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.

3. New features of Veeam Backup Enterprise Manager version 12 will be available after all connected backup servers are upgraded, and initial collection of data from these servers in Veeam Backup Enterprise Manager completes successfully.
4. Download and install the latest available update (if any). For more information, see [Updating Veeam Backup Enterprise Manager](#).

Updating Veeam Backup Enterprise Manager

Over the life cycle of a Veeam Backup Enterprise Manager version, Veeam Software releases updates – cumulative patches containing bug fixes, performance enhancements, and new features. When you update Veeam Backup Enterprise Manager, you apply a cumulative patch to it (as opposed to product upgrade, which is moving between major release versions).

Before You Begin

Before you install a cumulative patch for Veeam Backup Enterprise Manager 12, check the following prerequisites:

- Make sure you have Veeam Backup Enterprise Manager 12 (build 12.0.0.1420) installed.
For information on how to upgrade from product version 10a or later, see [Upgrading to Veeam Backup Enterprise Manager 12](#).
- With Veeam Backup Enterprise Manager and connected backup servers, remember to begin the update process with Veeam Backup Enterprise Manager. Backup servers should be updated after that. If you have Veeam Backup & Replication and Veeam Backup Enterprise Manager deployed on the same machine, the update wizard will update both products at once.
For more information on the backup server update procedure and prerequisites, see the [Updating Veeam Backup & Replication 12](#) section of the Veeam Backup & Replication User Guide.

Performing Update

To install the latest update for Veeam Backup & Replication, perform the following steps:

1. Review [this Veeam KB article](#) to check if a cumulative patch is available for the version of Veeam Backup & Replication that is installed.
2. If a cumulative patch is listed as available, click the Veeam KB article link for that cumulative patch.
3. In the **Download Information** section of the Veeam KB article, click **DOWNLOAD PATCH**.
4. To launch the update wizard, unzip the downloaded file and run the cumulative patch installer.
5. In the update wizard, click **Next**, then click **Install**.

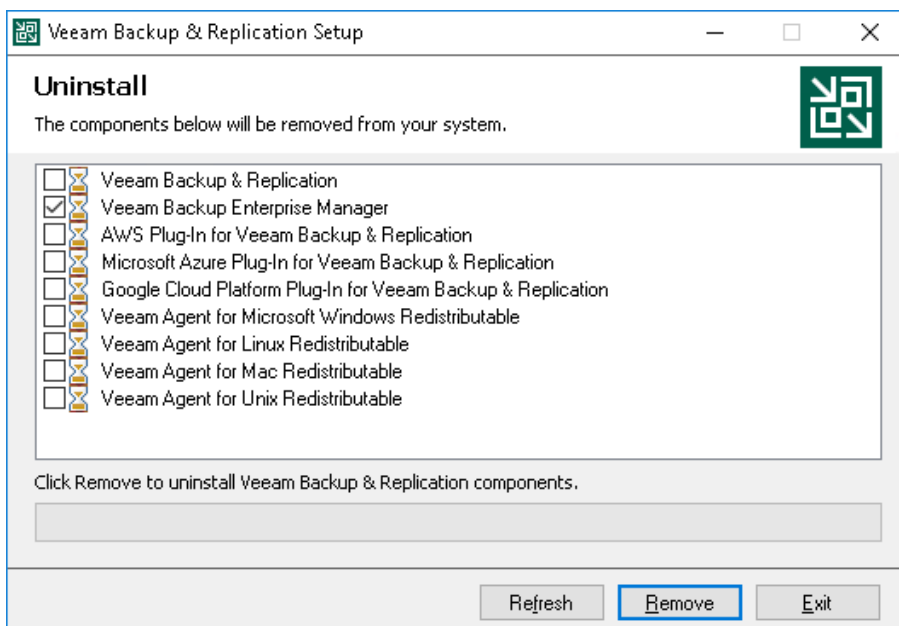
Uninstalling Veeam Backup Enterprise Manager

When you uninstall Veeam Backup Enterprise Manager, only the application itself is removed. The Enterprise Manager configuration database (the default name is *VeeamBackupReporting*) and all configuration data that is stored in the database remain. This lets you install Enterprise Manager again and use the preconfigured settings. If you are not going to reuse the Enterprise Manager configuration, you can delete the database manually.

The Enterprise Manager server is also recorded in configuration databases of added backup servers, which binds the backup servers to the Enterprise Manager server. If you are not going to use Enterprise Manager on this or another machine, it is recommended that you unbind the backup servers by removing them from Enterprise Manager before you uninstall the application. For more information, see [Removing Backup Server](#).

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.



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 language 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 KB article](#).

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

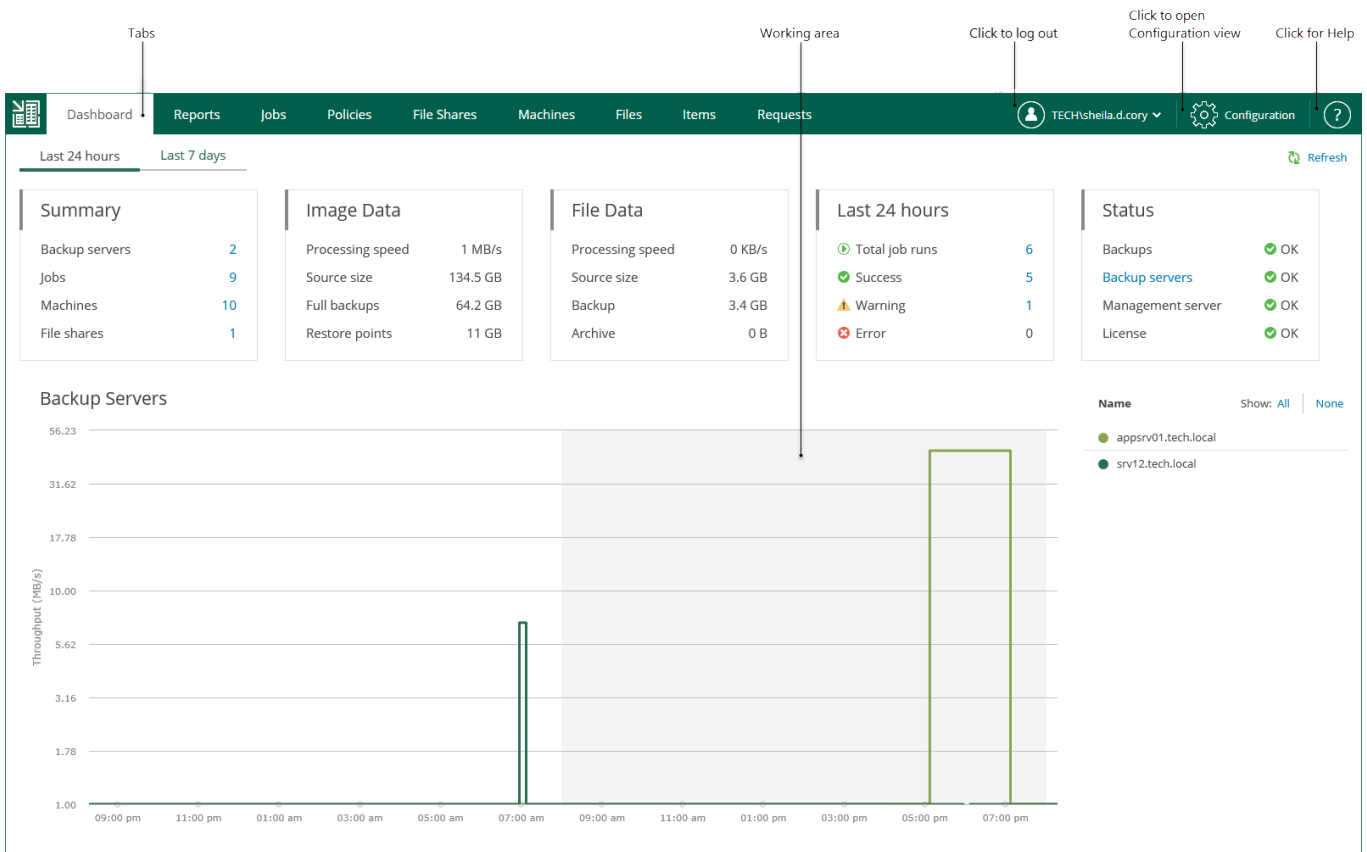
Home View

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 [Guest OS File Restore](#).
- Perform item-level recovery from application-aware backups created by Veeam Backup & Replication using the **Items** tab. For more information, see [Application Item Restore](#).

- 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

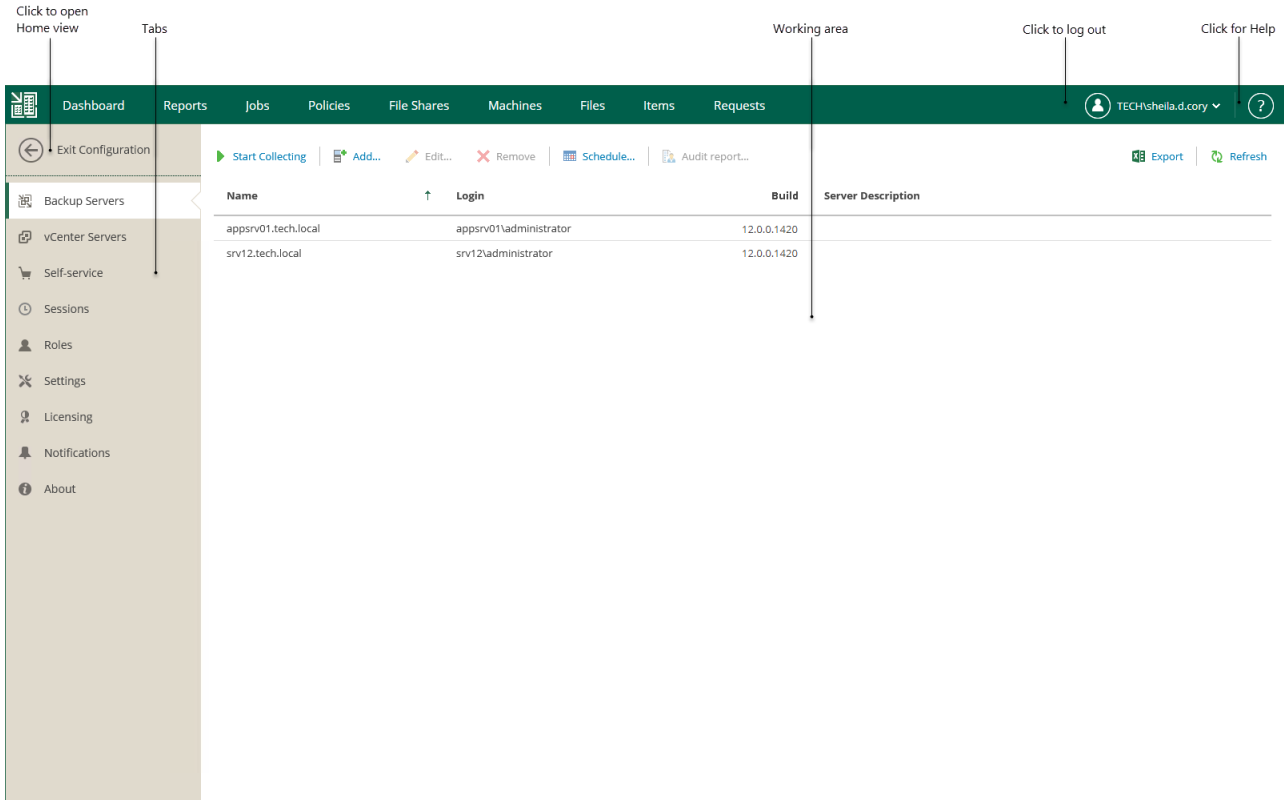
If you logged in with an administrative account, on the **Home** view you can click **Configuration** to open the **Configuration** view.

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 VMware Cloud Director organizations and vSphere tenant accounts using the **Self-Service** tab. For more information, see [Working with VMware Cloud 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](#).



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 Client on necessary servers](#)
- [Configure retention settings for index and history](#)
- [Configure Enterprise Manager accounts and roles](#)
- [Configure SAML authentication settings](#)
- [Configure notification settings](#)
- [Update TLS certificates](#)
- [Manage display languages](#)

To start working with Veeam Backup Enterprise Manager, you must perform initial configuration. For more information, see [Initial Configuration](#).

NOTE

Configuration backup and restore is not supported for Veeam Backup Enterprise Manager.

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, job 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

Veeam Backup Enterprise Manager allows you to manage jobs across multiple Veeam Backup & Replication servers and perform recovery operations from backups and replicas using the information from these backup servers.

In This Section

- [Adding Backup Server](#)
- [Editing Backup Server](#)
- [Removing Backup Server](#)
- [Collecting Data from Backup Servers](#)
- [Reports on Backup Servers](#)
- [Audit Reports](#)

Adding Backup Server

Veeam Backup Enterprise Manager lets you manage jobs across multiple backup servers and perform recovery operations in a single application.

You can add backup servers by specifying its DNS name, IPv4 or IPv6 address. For more information on IPv6 support, see the [IPv6 Support](#) section of the Veeam Backup & Replication User Guide.

Before you add backup servers to the Veeam Backup Enterprise Manager infrastructure, consider the following limitations:

- 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 already added backup server.
- All backup servers must be based on the same database engine as Veeam Backup Enterprise Manager (PostgreSQL or Microsoft SQL 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](#).
- Install the same product version on the Veeam Backup Enterprise Manager server and 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.

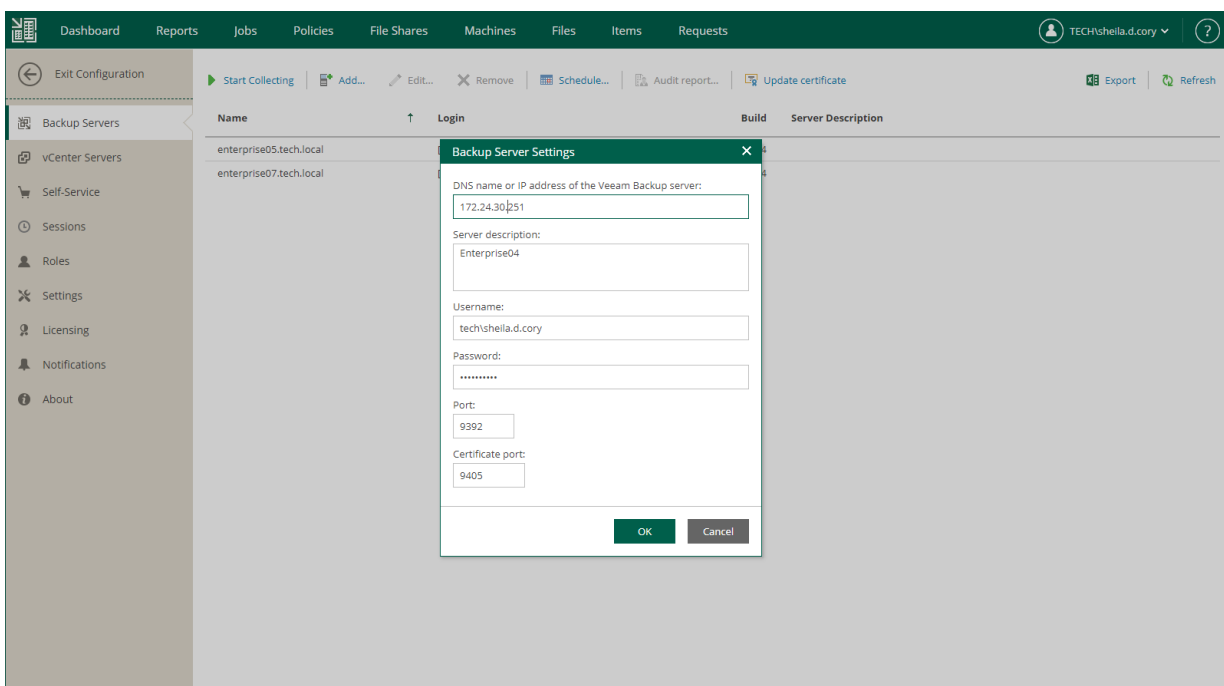
Veeam Backup Enterprise Manager supports adding backup servers with Veeam Backup & Replication 10a or later.

- When communicating with backup servers that have Veeam Backup & Replication 12 installed, Veeam Backup Enterprise Manager uses a TLS certificate for authentication, so that Veeam Backup Enterprise Manager does not store backup server account credentials. For connections with backup servers with earlier versions of Veeam Backup & Replication, Veeam Backup Enterprise Manager uses backup server account credentials. For more information, see [Connecting to Backup Servers](#).

To add a backup server to the Enterprise Manager infrastructure, take the following steps:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. Go to the **Backup Servers** section on the left.
4. Click **Add** at the top of the **Backup Servers** section.
5. In the **DNS name or IP address of the Veeam backup server** field, enter a full DNS name or IP address of the server you want to add.
6. In the **Server description** field, specify a backup server description.
7. Provide a name and password of the backup server account. The account must be assigned the Veeam Backup Administrator role. For more information, see [Configuring Backup Server Roles](#).

8. Specify ports used by Veeam Backup Service on the backup server:
 - On backup servers with Veeam Backup & Replication 11a or earlier, the port specified in the **Port** field will be used. The default port is 9392.
 - On backup servers with Veeam Backup & Replication 12, the port specified in the **Certificate port** field will be used. The default port is 9405.
9. Click **OK** to add the server.
10. [For backup servers with Veeam Backup & Replication 12] In the open window that shows a certificate thumbprint of the backup server, validate the thumbprint:
 - Click **Yes** if you trust the server.
 - Click **No** if you do not trust the server. Veeam Backup Enterprise Manager will display an error message, and you will not be able to connect to the server.



Configuring Backup Server Roles

Veeam Backup Enterprise Manager communicates with backup servers using accounts or TLS certificates 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 Enterprise Manager has rights to accomplish the necessary actions. The account used by Enterprise Manager must have the Veeam Backup Administrator role assigned in Veeam Backup & Replication.

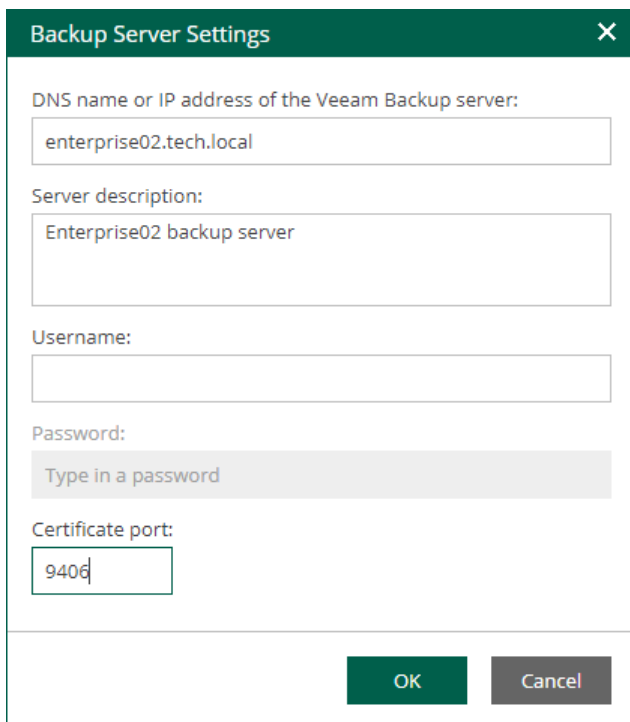
By default, when you install Veeam Backup & Replication on a backup server, the Veeam Backup Administrator role is assigned to the Windows Server Administrators group, so you can choose a user from the Administrators group as an account that will be used to communicate with the backup server. As soon 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.

Editing Backup Server

After a backup server was added to the Enterprise Manager infrastructure, you can edit connection settings. After you specify new connection settings, Enterprise Manager will try to connect to the backup server using these settings. If you specify credentials, Veeam Backup Enterprise Manager Service will send them to the backup server for the initial authentication. Otherwise, the Enterprise Manager certificate will be used.

To edit connection settings of a backup server, do the following:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. Go to the **Backup Servers** section on the left.
4. Select a backup sever from the list and click **Edit** on the toolbar.
Alternatively, you can right-click the selected backup server and select **Edit**.
5. Specify new connection settings and click **OK**.



The image shows a dialog box titled "Backup Server Settings" with a close button (X) in the top right corner. The dialog contains several input fields and buttons:

- DNS name or IP address of the Veeam Backup server:** A text box containing "enterprise02.tech.local".
- Server description:** A text box containing "Enterprise02 backup server".
- Username:** An empty text box.
- Password:** A password field with a grey background and the placeholder text "Type in a password".
- Certificate port:** A text box containing "9406".
- At the bottom, there are two buttons: "OK" (green) and "Cancel" (grey).

Removing Backup Server

You can remove an added Veeam backup server added to the Veeam Backup Enterprise Manager infrastructure.

After you remove a backup server, Enterprise Manager stops collecting data from the backup server and showing information about the backup server such as jobs, backed up machines and so on.

On the backup server side, a record about the Enterprise Manager instance is deleted from the configuration database. The backup server continues using the license that Enterprise Manager pushed to the backup server until you remove the license or install a new one.

To remove a backup server, do the following:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the top right corner.
3. Go to the **Backup Servers** section on the left.
4. Select a backup sever from the list and click **Remove** on the toolbar.
Alternatively, you can right-click the selected backup server and select **Remove**.
5. In the open window, click **Yes** to confirm the removal.

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

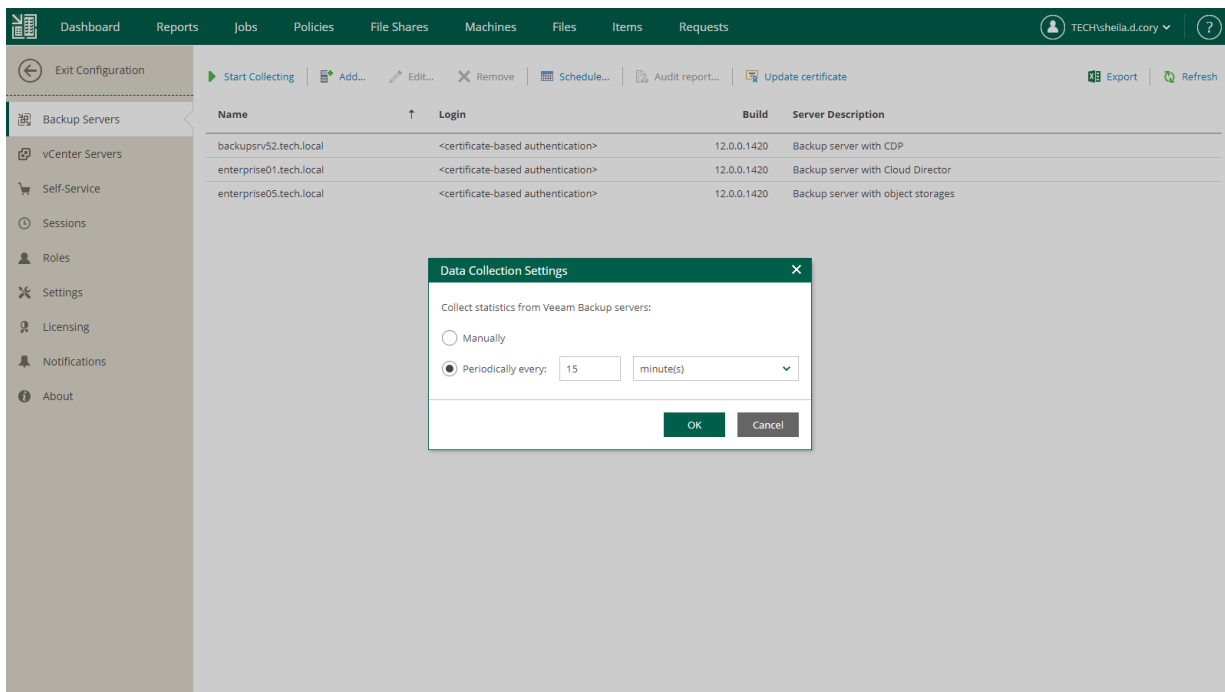
- Data collection job collects data from all added backup servers at once.
- To ensure periodic update of the information available to Veeam Backup Enterprise Manager users, use periodic data collection.

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.

The screenshot displays the Veeam Backup Enterprise Manager interface. The main window shows a list of sessions with columns for Type, Start Time, Status, and Initiated by. A 'Log' window is open, showing a detailed list of events for a selected session. The log events include:

Time	Status	Information
2/13/2023 09:05:29...	Success	Starting data collection job...
2/13/2023 09:05:30...	Success	Job successfully started.
2/13/2023 09:05:30...	Success	Checking deleted backup servers removal
2/13/2023 09:05:31...	Success	Preparing to collect data from enterprise01.tech.local
2/13/2023 09:05:31...	Success	Retrieving data from enterprise01.tech.local...
2/13/2023 09:05:47...	Success	Data collection from enterprise01.tech.local completed successfully.
2/13/2023 09:05:47...	Success	Preparing to collect data from backupsvr52.tech.local
2/13/2023 09:05:47...	Success	Retrieving data from backupsvr52.tech.local...
2/13/2023 09:06:03...	Success	Data collection from backupsvr52.tech.local completed successfully.
2/13/2023 09:06:04...	Success	Preparing to collect data from enterprise05.tech.local
2/13/2023 09:06:04...	Success	Retrieving data from enterprise05.tech.local...
2/13/2023 09:06:21...	Success	Data collection from enterprise05.tech.local completed successfully.
2/13/2023 09:06:21...	Success	Data collection job finished.

The interface also shows a sidebar with navigation options like Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, Requests, Sessions, Roles, Settings, Licensing, Notifications, and About. The bottom of the window displays 'Records per Page: 25', 'Page 1 of 67', and 'Displaying 1 - 25 of 1674'.

Reports on Backup Servers

On the **Reports** tab, you can view statistical information about backup servers added to the Enterprise Manager infrastructure.

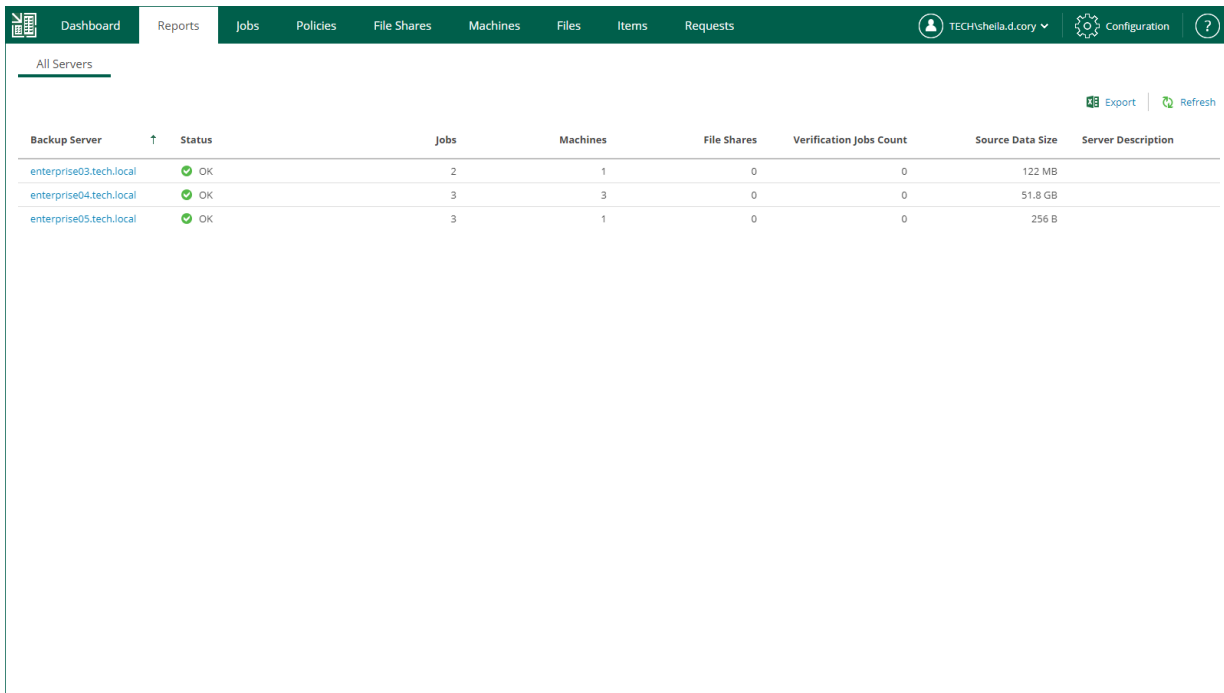
For each backup server, the report contains the following data.

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: <ul style="list-style-type: none">• <i>Never processed</i> – data collection has never been started for the backup server• <i>Processing</i> – data collection is in progress• <i>OK</i> – data was collected successfully• <i>Warning</i> – data collection completed with a warning• <i>Error</i> – 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.



The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\sheila.d.cory'. The main content area is titled 'All Servers' and features a table with the following data:

Backup Server	Status	Jobs	Machines	File Shares	Verification Jobs Count	Source Data Size	Server Description
enterprise03.tech.local	OK	2	1	0	0	122 MB	
enterprise04.tech.local	OK	3	3	0	0	51.8 GB	
enterprise05.tech.local	OK	3	1	0	0	256 B	

Toolbar actions include 'Export' and 'Refresh'.

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 Report Overview

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 initiated by the user

For more information on operations included in the report, see [Audited Operations](#).

- 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	sessionId='2c4ee74003764f1aaffd08c47e471fc0';vmName='virt03-vm01'
6	30.09.2020 09:29:30Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionId='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	sessionId='ce6199e4cc1e47abb0b1e947a4d2fc1c';vmName='virt03-vm01'
12	08.10.2020 10:46:22Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionId='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	sessionId='d0b1640995a2413086077923956f7f88';vmName='virt03-vm01'
15	13.10.2020 15:11:39Z	TECH\hue.spenser	S-1-5-21-4081262488-3246261347-3296280108-2040	StartFailover	Success	sessionId='fb47bdd80c01493cab2521d1359ef27e';vmName='virt03-vm01'

Generating Audit Report

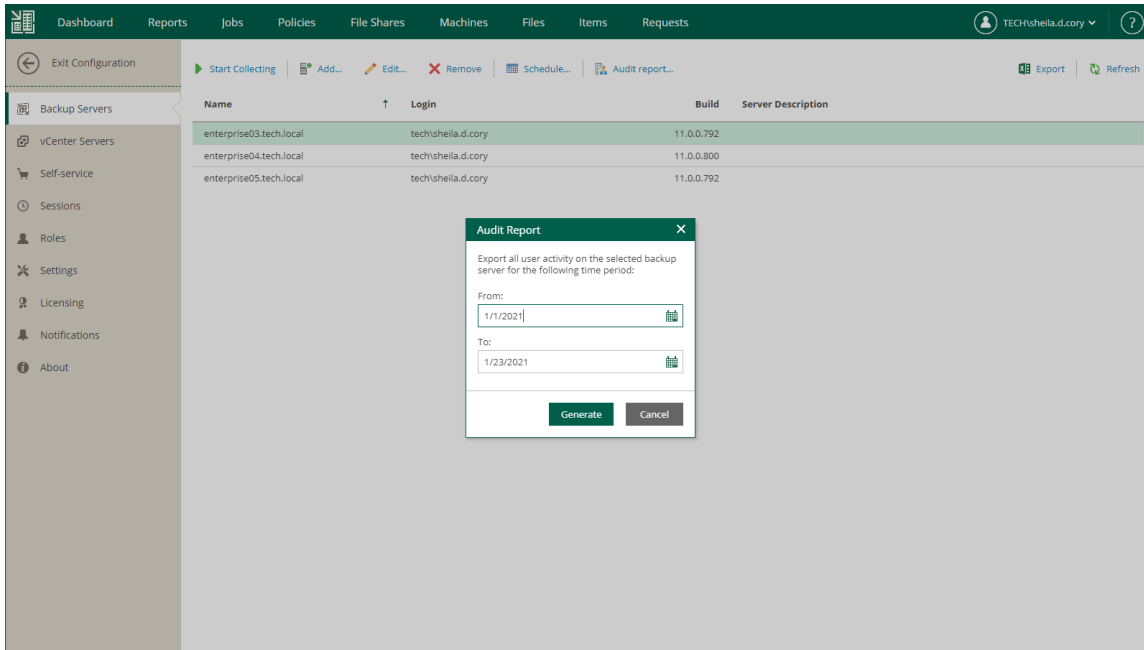
When you generate an audit report, it is downloaded in the CSV format to the local machine.

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**.

- 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. For details, see [Configuring Retention Settings for Index and History](#).



Audited Operations

Audit reports contain records about the following operations performed on a backup server:

Operation Type	Operation Name	Description
User Activity	Login	User login
Operations with Jobs	JobEnable	Enabling a job
	JobDisable	Disabling a job
	JobStart	Starting a job
	JobStop	Stopping a job
	JobRetry	Retrying a job
	JobActiveFullStart	Starting active full backup
	JobClone	Cloning a job
	JobEdit	Editing a job

Operation Type	Operation Name	Description
	JobDelete	Deleting a job
	BackupDelete	Deleting a backup
	MoveCopyBackup	Moving or copying a backup to another backup job
Recovery Operations	VmRestore	Restoring entire VM
	AzureVmRestore	Restoring entire Azure VM
	InstantRestore	Performing Instant Recovery
	VappRestore	Restoring entire vApp
	VmDiskRestore	Performing virtual disk restore
	QuickMigration	Performing quick migration of VMs or disks
	StartFileLevelRestore	Starting file-level restore
	RestoreOperation	Restoring files to the original location
	FlrDownloadFromEm	Downloading files to the local machine
	CopyToOperation	Restoring files to a new location
	StartFailover	Performing failover to the VM replica
	NasRestore	Restoring entire file share,
	NasInstantRestore	Performing instant file share recovery
	FileShareMigration	Migrating a file share
	NasFileLevelRestore	Performing file-level restore
Mount	Mounting backup content to a mount server	

Customizing Dashboard Chart

You can customize the appearance of the **Backup Servers** chart that you can see on the Enterprise Manager dashboard.

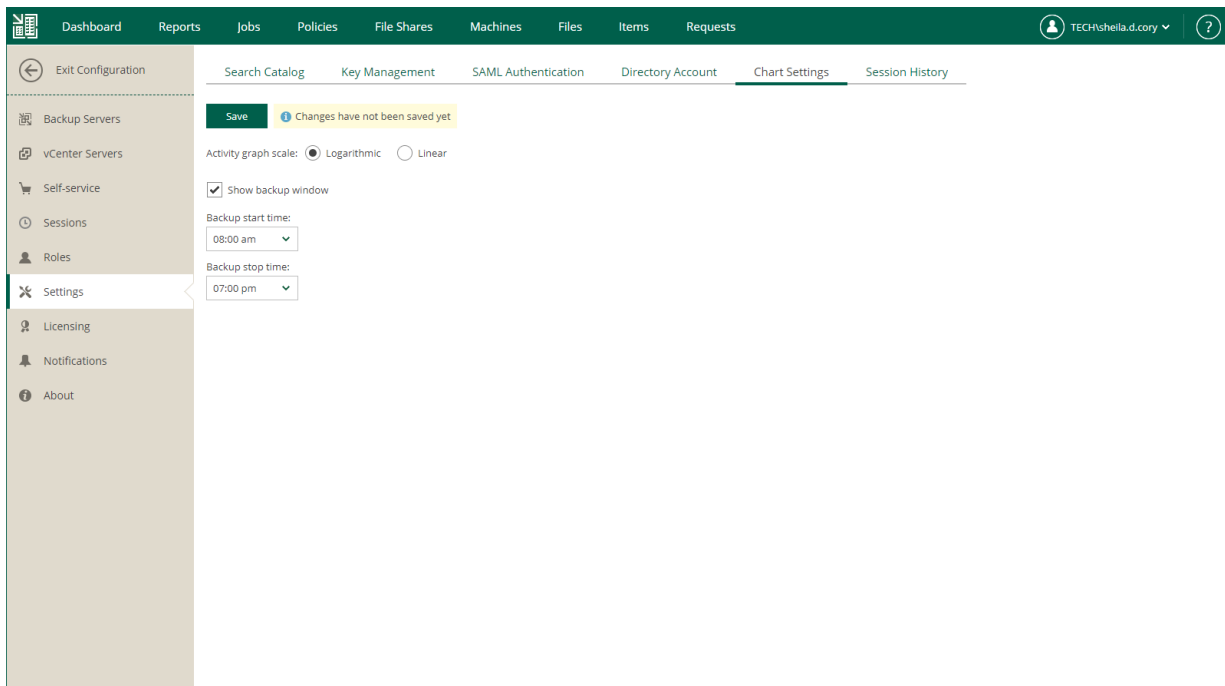
IMPORTANT

Backup window interval that you specify here, effects the job settings that you configure for tenants that use the following portals:

- [vSphere Self-Service Backup Portal](#)
- [Veeam Self-Service Backup Portal](#)

To customize the appearance of the chart, do the following:

1. Open the **Configuration** view.
2. Click the **Settings** section on the left of the **Configuration** view.
3. Select the **Chart Settings** tab.
4. Use the **Activity graph scale** options to switch between graph types: *Linear* and *Logarithmic*.
5. Select the **Show backup window** check box to highlight the backup window on the dashboard chart.
6. Specify time interval for the backup window. Default interval is from 8:00 PM to 8:00 AM. You can change the interval to correlate with your planned backup window by editing the start and stop time.
7. To save the changes, click **Save**.



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.

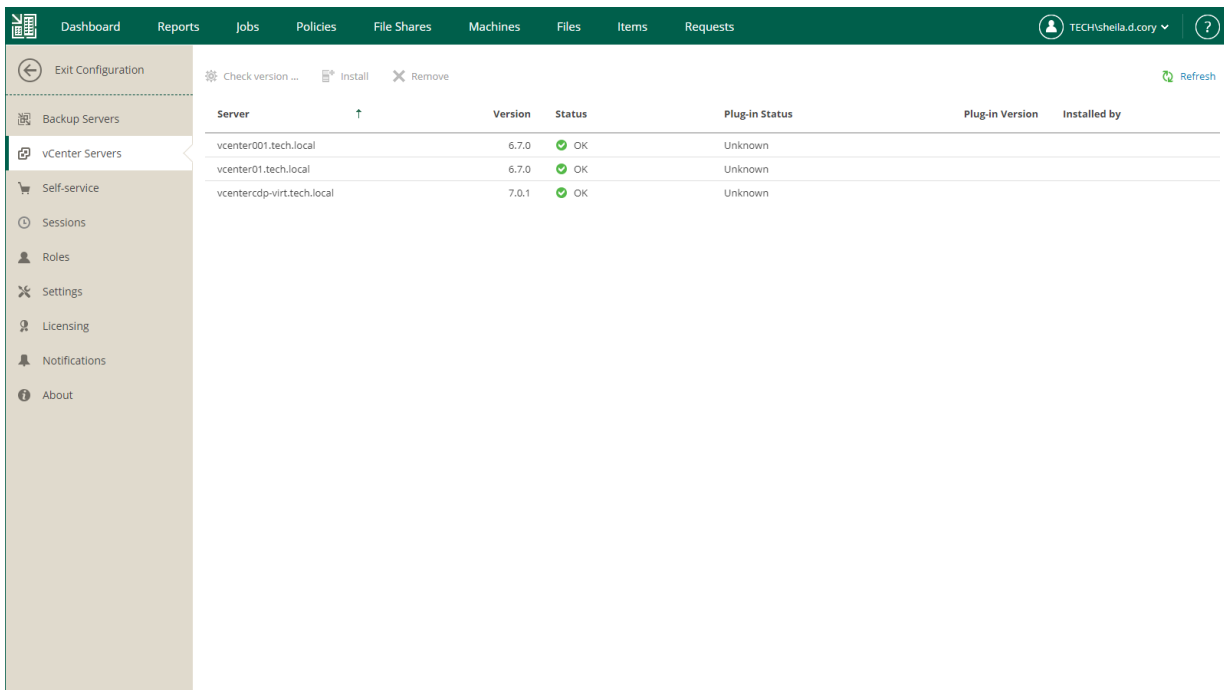
You can perform the following operations with vCenter Servers:

- **Check version** – use this command to request vCenter Server version and operation status. If Veeam Plug-in for VMware vSphere Client is deployed, its version, status and installation account will be also displayed.
- **Install** – use this command to install Veeam Plug-in for VMware vSphere Client on the selected server.
- **Remove** – use this command to uninstall Veeam Plug-in for VMware vSphere Client from selected server.

For more information on the plug-in, see [Veeam Plug-in for VMware vSphere Client](#).

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.



The screenshot shows the Veeam Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECH\sheila.d.cory. The left sidebar shows the navigation menu with 'vCenter Servers' selected. The main content area displays a table of vCenter Servers with columns for Server, Version, Status, Plug-in Status, Plug-in Version, and Installed by. The table contains three entries, all with a status of 'OK'.

Server	Version	Status	Plug-in Status	Plug-in Version	Installed by
vcenter001.tech.local	6.7.0	OK	Unknown		
vcenter01.tech.local	6.7.0	OK	Unknown		
vcentercdp-virt.tech.local	7.0.1	OK	Unknown		

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 provide permissions for guest OS file restore and application item 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	<i>DOMAIN Username</i> Domain is optional
Group	Local or AD group	By specifying a user name and password	<i>DOMAIN Groupname</i> Domain is optional
External User	IdP user	By using single sign-on*	<i>Username@Suffix</i>
External Group	IdP group	By using single sign-on*	Free-form string
vSphere Role	VMware vCenter Server role used to access the Remote vSphere Client plug-in	—	—

* 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	<ul style="list-style-type: none">Initially by default to the users listed in the local Administrators group and the user who installed Enterprise ManagerBy Portal Administrator in Configuration > Roles	Yes	Full access to all available operations on all tabs of the web UI

Role	How Is Assigned	Access to Configuration	Permissions
Portal User	By Portal Administrator in Configuration > Roles	No	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 (Microsoft 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 Permissions for File and Application Item Restore](#).

Managing Accounts

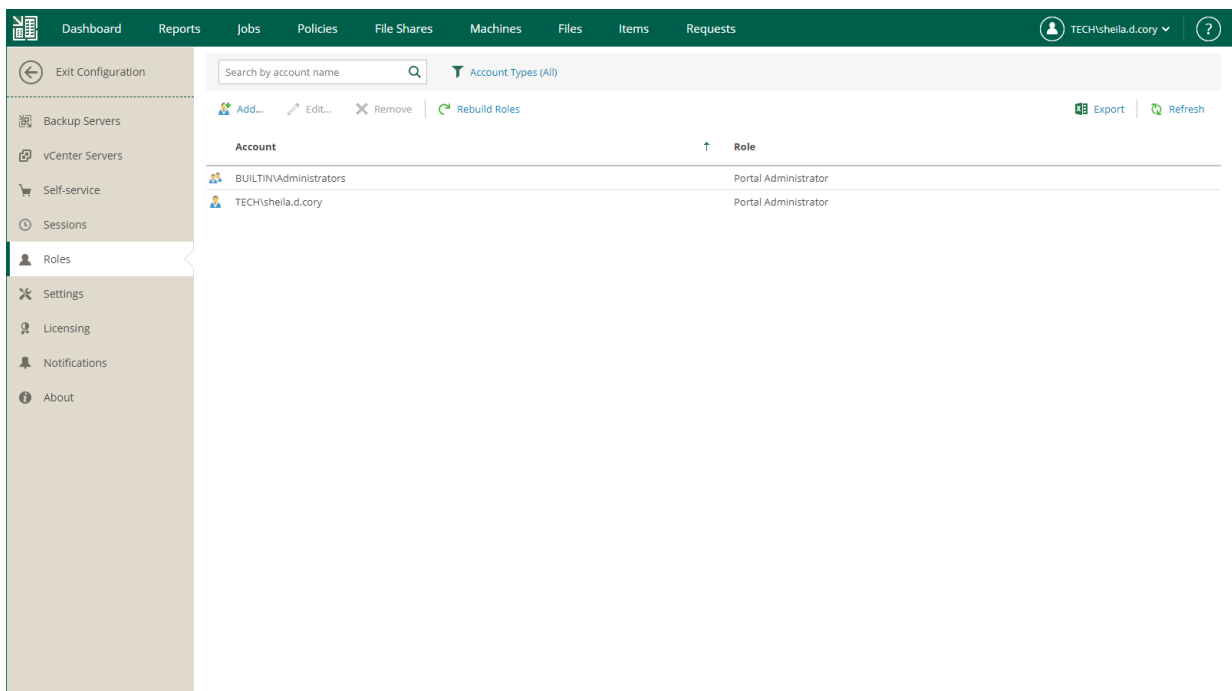
Users with the Portal Administrator role can perform the following actions with accounts:

- [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 Permissions for File and Application Item Restore](#).

Add Role [X]

Account type: User

Account: tech\william.fox

Role: Restore Operator

Restore scope:

All objects

Selected objects only Choose

Allow restore of:

Entire machines and disks

Files and folders

Allow in-place file restores only

Allow restore of files with these extensions only:

Microsoft Exchange items

Databases

Microsoft SQL Server databases

Oracle databases

PostgreSQL instances

Deny in-place database restores (safer)

OK Cancel

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.

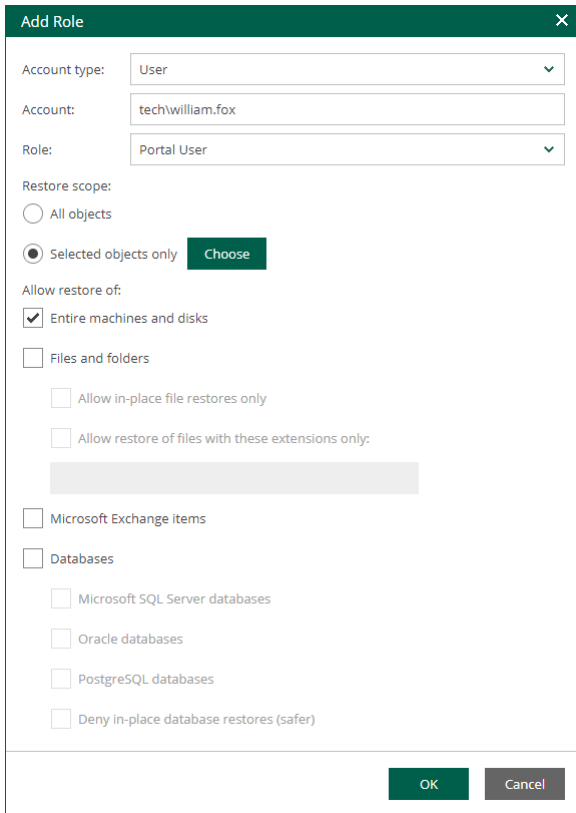
Configuring Restore Scope

Restore scope is a list of objects (machines and file shares) that can be recovered by appropriate users. By default, the restore scope for users with a non-administrative role (Portal User and Restore Operator) includes all objects from available backups. If you have the Enterprise Plus edition of Veeam Backup & Replication, you can customize the restore scope.

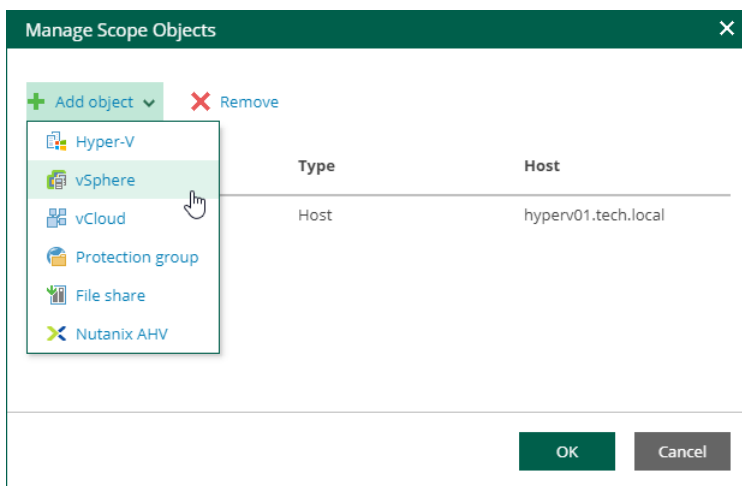
To customize the restore scope, perform the following steps when adding or editing a Portal User or Restore Operator account:

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.



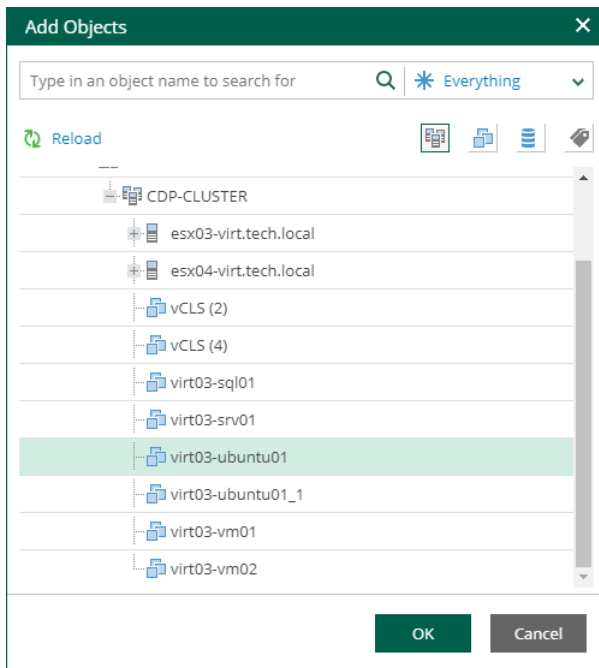
5. In the **Add Objects** window, select the objects you allow the user to restore.

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.

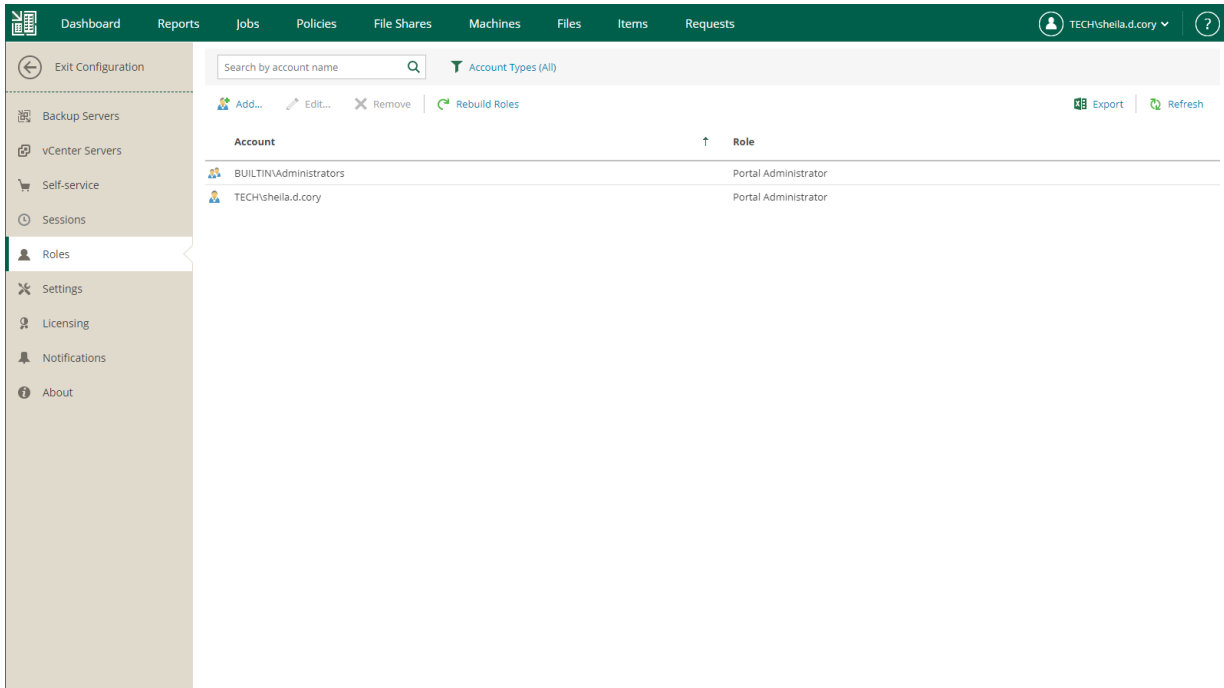
After the users log in to Enterprise Manager, they will be able to view objects and files included in their restore scope.

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.

Users with the Portal Administrator role can click **Rebuild Roles** to refresh all scopes of all accounts manually. Consider that this operation will affect all configured roles. You can watch the progress of the security scope rebuild in the **Sessions** section.



Configuring Permissions for File and Application Item Restore

Accounts that you want to use for guest OS file restore and application item restore must have sufficient permissions.

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 user or prohibit downloading of restored files at all.

To let users restore application items, you must assign a security role to the user account and allow the account to access and restore application items. For example, users responsible for Oracle database restore must be assigned an Enterprise Manager role and be able to restore Oracle databases.

To configure permissions for file and application item restore, take the following steps when adding or editing an 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:
 - Select **Microsoft SQL Server databases** to allow restore of Microsoft SQL databases on machines included in the user's restore scope.
 - Select **Oracle databases** to allow restore of Oracle databases on machines included in the user's restore scope.
 - Select **PostgreSQL instances** to allow restore of PostgreSQL instances on machines included in the user's restore scope.
 - Select **Deny in-place database restores** to restrict the user from overwriting the original databases during the database restore process.

7. Click **OK** to save the changes.

Add Role [X]

Account type: User

Account: tech\william.fox

Role: Restore Operator

Restore scope:

All objects

Selected objects only **Choose**

Allow restore of:

Entire machines and disks

Files and folders

Allow in-place file restores only

Allow restore of files with these extensions only:

Microsoft Exchange items

Databases

Microsoft SQL Server databases

Oracle databases

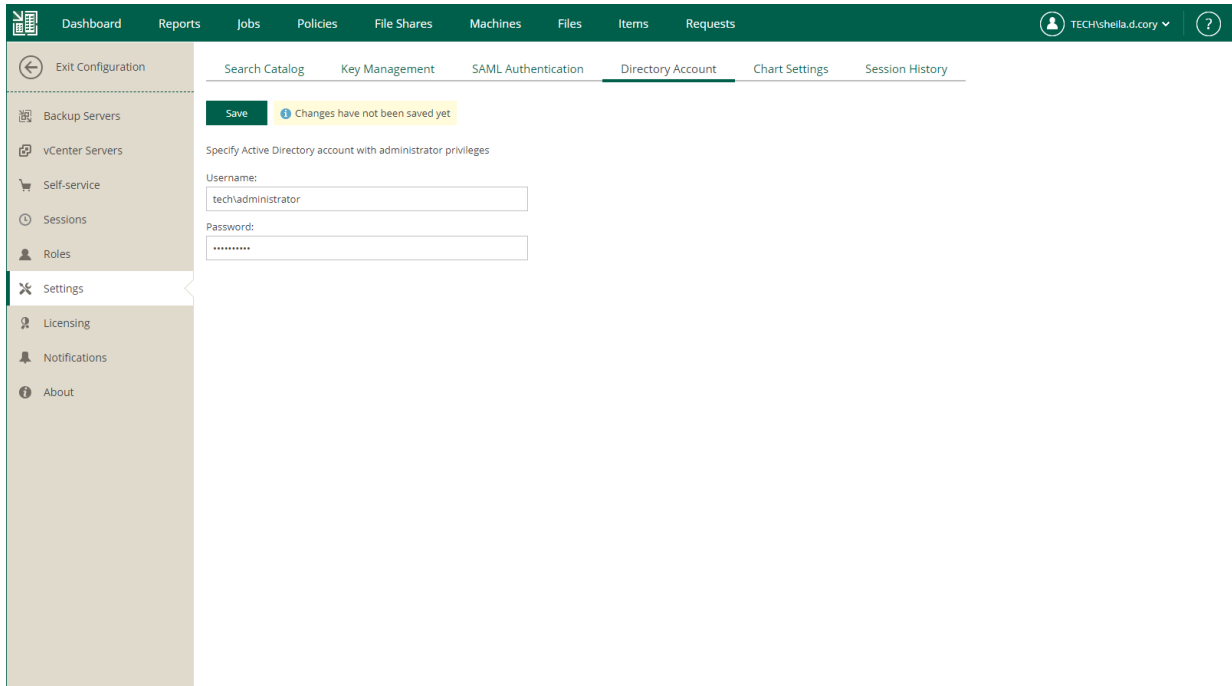
PostgreSQL instances

Deny in-place database restores (safer)

OK **Cancel**

8. [For Microsoft Exchange items restore] Specify an Active Directory account that will be used to restore Exchange items:
- Open the **Settings** section of the **Configuration** view.
 - 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.



Configuring VMware vSphere Roles

If you use a remotely installed [Veeam Plug-in for VMware vSphere Client](#), you need to map one of the Veeam Backup Enterprise Manager roles with a VMware vSphere role that you will use to log in to the remote vSphere Client plug-in.

To add a VMware vSphere role, take the following steps:

1. Open the **Roles** section of the **Configuration** view.
2. Click **Add** on the toolbar.
3. From the **Account type** list, select *vSphere Role*.
4. From the **vSphere role** list, select a vCenter Server role created in VMware vSphere.
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 Permissions for File and Application Item Restore](#).

Add Role [X]

Account type: vSphere Role [v]

vSphere role: Administrator [v]

Role: Portal User [v]

Restore scope:

All objects

Selected objects only **Choose**

Allow restore of:

Entire machines and disks

Files and folders

Allow in-place file restores only

Allow restore of files with these extensions only:

Microsoft Exchange items

Databases

Microsoft SQL Server databases

Oracle databases

PostgreSQL databases

Deny in-place database restores (safer)

OK **Cancel**

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 [Configuring 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.

The screenshot displays the SAML Authentication configuration interface. The 'Identity Provider Configuration' section includes the following fields:

- Entity ID:** `http://srv16.tech.local/adfs/services/trust`
- Login URL:** `https://srv16.tech.local/adfs/ls/`
- Binding:** `HttpRedirect`
- IdP certificate:** A long alphanumeric string representing the identity provider's certificate.

Below the main configuration, the 'Advanced Settings' section for 'Enterprise Manager Configuration' provides download links for metadata and manual configuration details:

- Veeam Backup Enterprise Manager: [Download](#)
- vSphere Self-Service Backup Portal: [Download](#)

Alternatively, you can configure your Identity Provider manually using the following details:

- SP Entity ID / Issuer: `https://srv12.tech.local:9443/Saml2` [Copy Link](#)
- Assertion consumer URL: `https://srv12.tech.local:9443/Saml2/Acs` [Copy Link](#)
- Certificate: `F74D4A5F65F34DFB36E499777FCCA70B145F976` [Select](#) [Download](#) [Remove](#)

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 and 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**.

SAML Advanced Settings

Service Provider Settings

- Include encryption certificate in metadata
- Include signing certificate in metadata
- Minimum accepted incoming signing algorithm: SHA256
- Outbound signing algorithm: SHA256
- Group claim type: http://schemas.xmlsoap.org/claims/Group

Identity Provider Settings

- Sign AuthnRequests to IdP
- Authentication context comparison: Exact
- Authentication context class: Password

Apply Cancel

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 and 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 and 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.

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*

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.

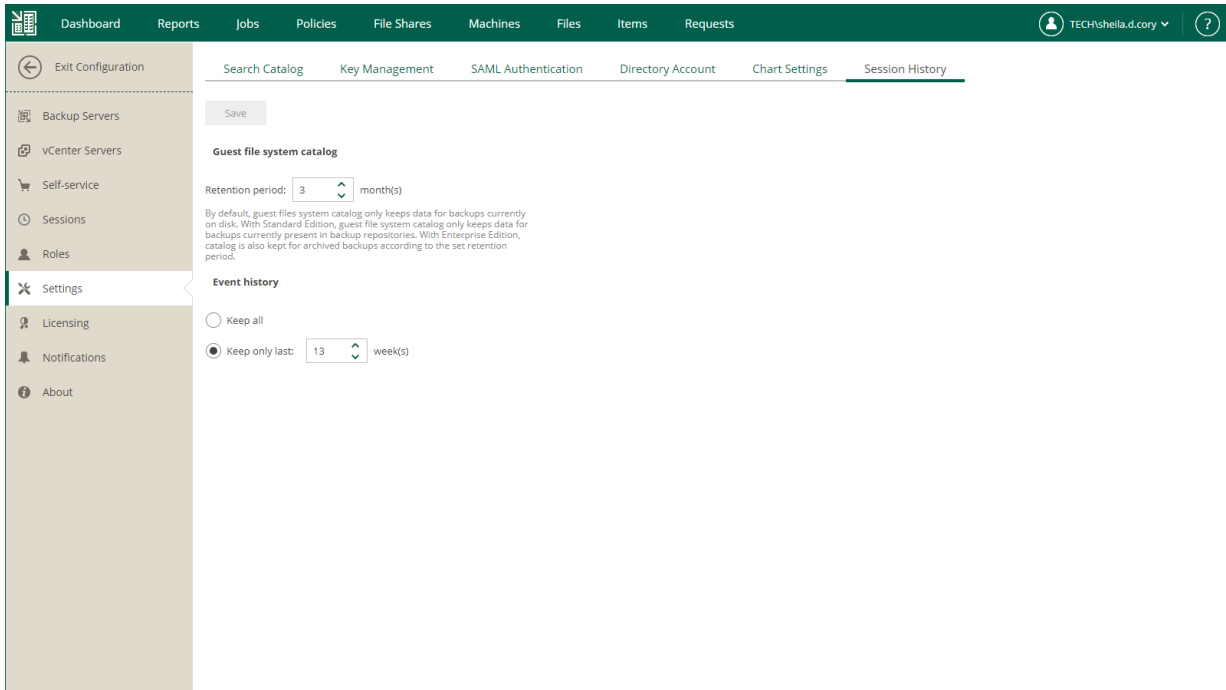
IMPORTANT

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.

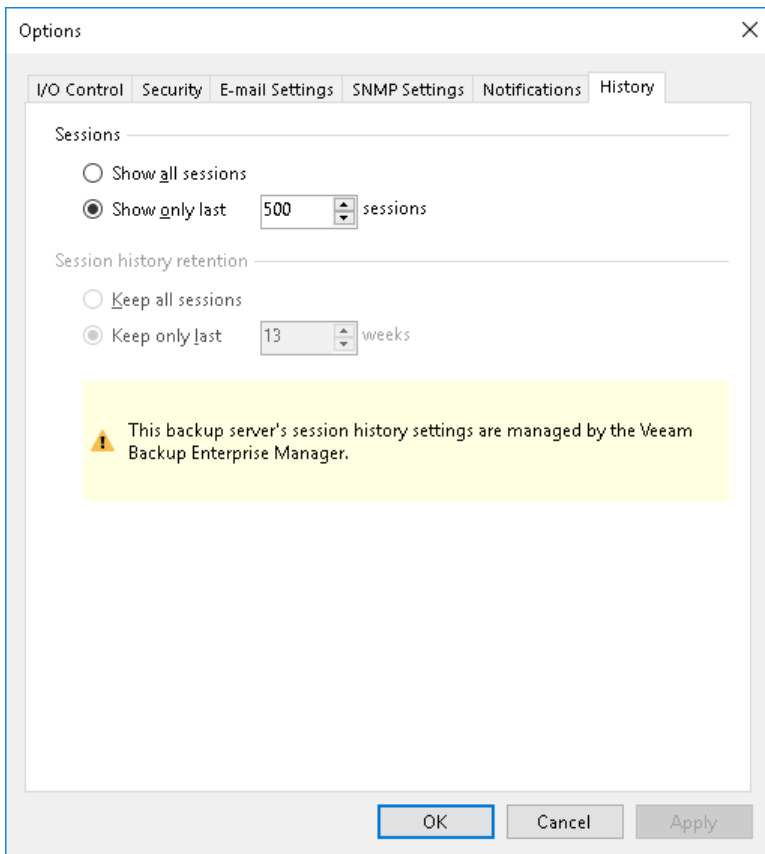
To configure retention settings:

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 Notification Settings

Veeam Backup Enterprise Manager allows you to receive email notifications on job results, restore operations and so on.

Before you configure notification settings, specify settings of the server that will send email notifications to necessary email addresses. For more information, see [Mail Server Settings](#).

After that, you can fine tune necessary notifications:

- [Notifications on job results](#)
- [Notifications on lab requests](#)
- [Notifications on restore operations](#)
- [Notifications on licensing](#)
- [Notifications on encryption keys operations](#)

Mail Server Settings

To receive notifications from Veeam Backup Enterprise Manager, you need to specify settings of the server that will send email notifications to necessary email addresses.

You can allow Veeam Backup Enterprise Manager to send email notifications on behalf of your Google or Microsoft 365 account using [OAuth 2.0](#) authentication, or you can specify connection settings of your SMTP server that use basic (with a password) authentication. You can select from the following options:

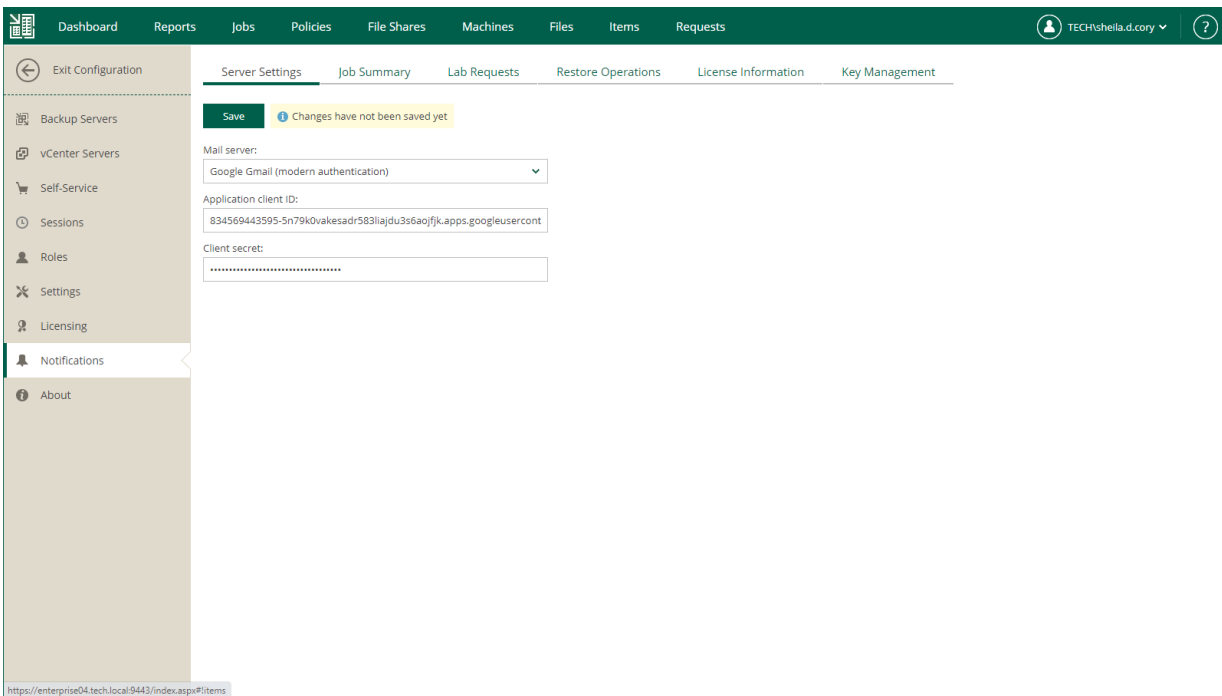
- [Connect Veeam Backup Enterprise Manager with a Google account](#)
- [Connect Veeam Backup Enterprise Manager with a Microsoft 365 account](#)
- [Use an SMTP server with basic authentication](#)

Google Account Settings

You can authorize Veeam Backup Enterprise Manager to send email notifications on behalf of your Google account. To send notifications, Enterprise Manager communicates with the Gmail API. For authentication, Enterprise Manager uses an access token issued by Google Authorization Server. To acquire an access token, you need to specify OAuth 2.0 client credentials of the application registered in the Google Cloud console. For more information on obtaining client credentials, see [Registering Application in Google Cloud Console](#).

To connect Veeam Backup Enterprise Manager with your Google account, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. On the **Server Settings** tab, select *Google Gmail* from the **Mail server** list.
3. In the **Application client ID** field, specify the obtained client ID.
4. In the **Client secret** field, specify the client secret.
5. To save the credentials, click **Save**.
6. Click **Sign in with Google**.
7. Allow Veeam Backup Enterprise Manager to have access to your Google account and send email notifications on your behalf.



Registering Application in Google Cloud Console

Before the Veeam Backup Enterprise Manager web application can obtain an access token, you need to register the application in the Google Cloud console. Upon registration you will have a client ID and client secret required for acquiring an access token.

You can register Veeam Backup Enterprise Manager in the Google Cloud console.

1. Log in to the Google Cloud console under a Google account that you want to use for sending email notifications.

2. Create a new project and enable *Gmail API* for the project.

You can do this with [the Google setup tool](#).

3. Create the *OAuth client ID* credentials – a client ID and client secret for the Veeam Backup Enterprise Manager application.

As an authorized redirect URI, specify the following:

```
https://<EnterpriseManagerServer>:9443/api/Notifications/GrantPermissions
```

where `<EnterpriseManagerServer>` is a host name or IP address of the host where the Enterprise Manager server resides.

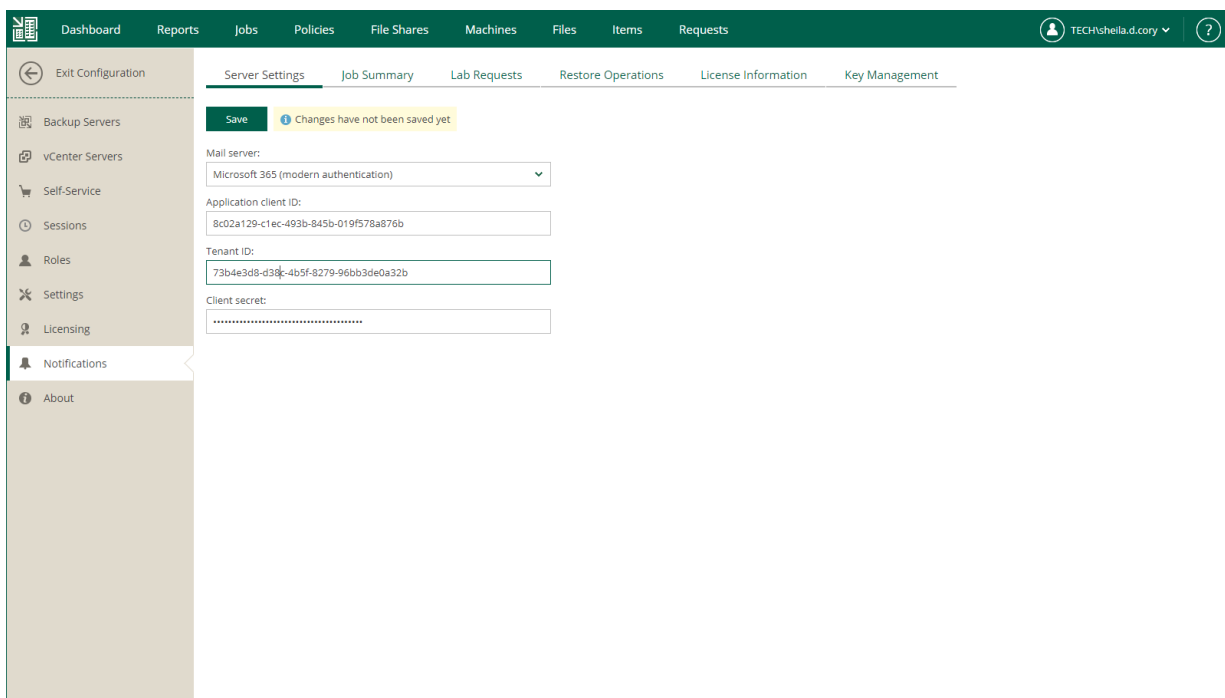
4. Record the following data required for acquiring an access token:
 - Client ID
 - Client secret

Microsoft 365 Account Settings

You can authorize Veeam Backup Enterprise Manager to send email notifications on behalf of your Microsoft 365 account. To send notifications, Enterprise Manager communicates with the Microsoft Graph API. For authentication, Enterprise Manager uses an access token issued by Microsoft identity platform. To acquire an access token, you need to specify details of an application registered with the Microsoft identity platform. For more information on obtaining application details, see [Registering Application in Azure Portal](#).

To connect Veeam Backup Enterprise Manager with your Microsoft 365 account, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. On the **Server Settings** tab, select *Microsoft 365* from the **Mail server** list.
3. In the **Application client ID** field, specify the client ID assigned to your Azure Active Directory application.
4. In the **Tenant ID** field, specify your Azure Active Directory tenant ID.
5. In the **Client secret** field, specify the client secret assigned to your Azure Active Directory application.
6. To save the settings, click **Save**.
7. Click **Authorize now**.
8. Allow Veeam Backup Enterprise Manager to access your Microsoft 365 account and send email notifications on your behalf.



Registering Application in Azure Portal

Before the Veeam Backup Enterprise Manager web application can obtain an access token, you need to register the application with the Microsoft identity platform. Upon registration you will have application essentials required for acquiring an access token.

You can register Veeam Backup Enterprise Manager in the Azure portal. For more information on registering applications, see [Microsoft Docs](#).

1. Log in to the Azure portal under an account that you want to use for sending email notifications. The account must have an active subscription.
2. Register Veeam Backup Enterprise Manager as an application.

As a redirect URI, specify the following:

```
https://<EnterpriseManagerServer>:9443/api/Notifications/GrantPermissions
```

where <EnterpriseManagerServer> is a host name or IP address of the host where the Enterprise Manager server resides.

3. Grant the application the *Mail.Send* permission of Microsoft Graph. This will allow Veeam Backup Enterprise Manager to call the Microsoft Graph API for sending email notifications.
4. Add a new client secret. It is used to prove the application identity to the Microsoft identity platform.
5. Record the following data required for acquiring an access token:
 - Directory (tenant) ID
 - Application (client) ID
 - Client secret value

SMTP Server with Basic Authentication

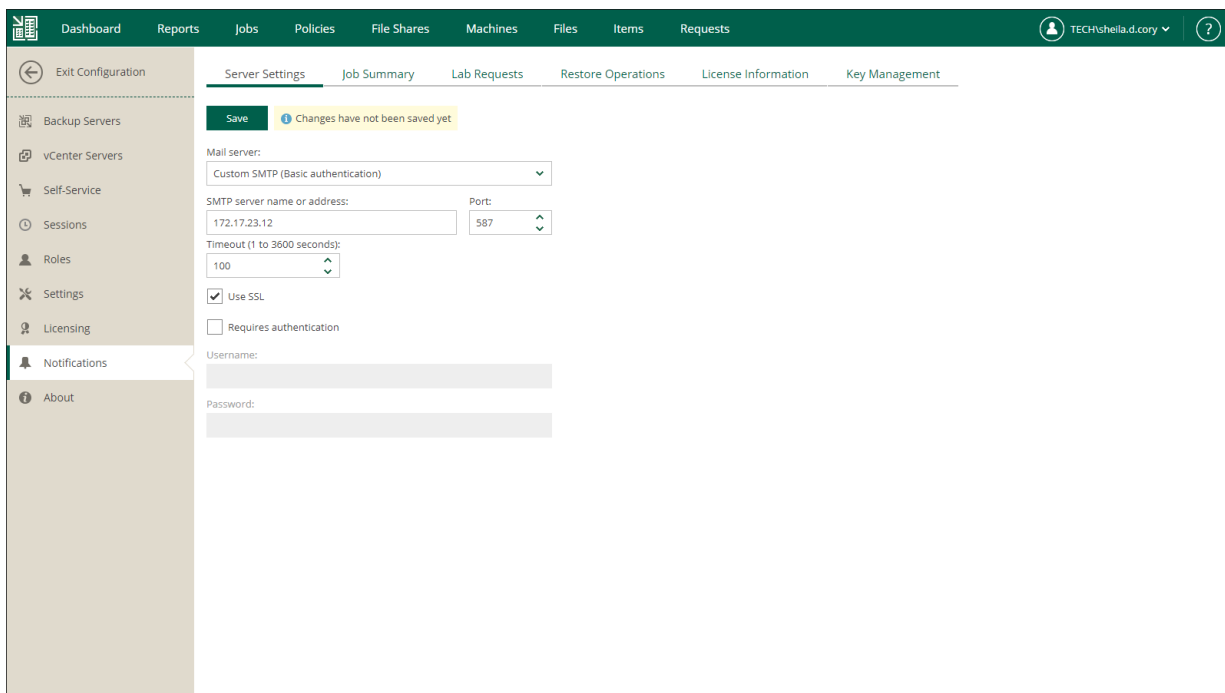
For sending email notifications, you can use a custom SMTP server with basic authentication.

NOTE

When you add an SMTP server, Veeam Backup Enterprise Manager saves its TLS certificate thumbprint. If the SMTP server certificate is changed and the certificate is not trusted, Enterprise Manager stops sending email notifications until you validate the new certificate.

To specify SMTP server settings, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. On the **Server Settings** tab, select *Custom SMTP* from the **Mail server** list.
3. 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**.
4. In the **Timeout** field, specify a timeout for email server – this should be a value from 1 to 3600 seconds. Default is **100** seconds.
5. If the SMTP server requires SSL connection, select the **Use SSL** check box.
6. If the SMTP server requires authentication, select the **Requires authentication** check box and specify authentication credentials.
7. Click **Save**.



Notifications on Job Results

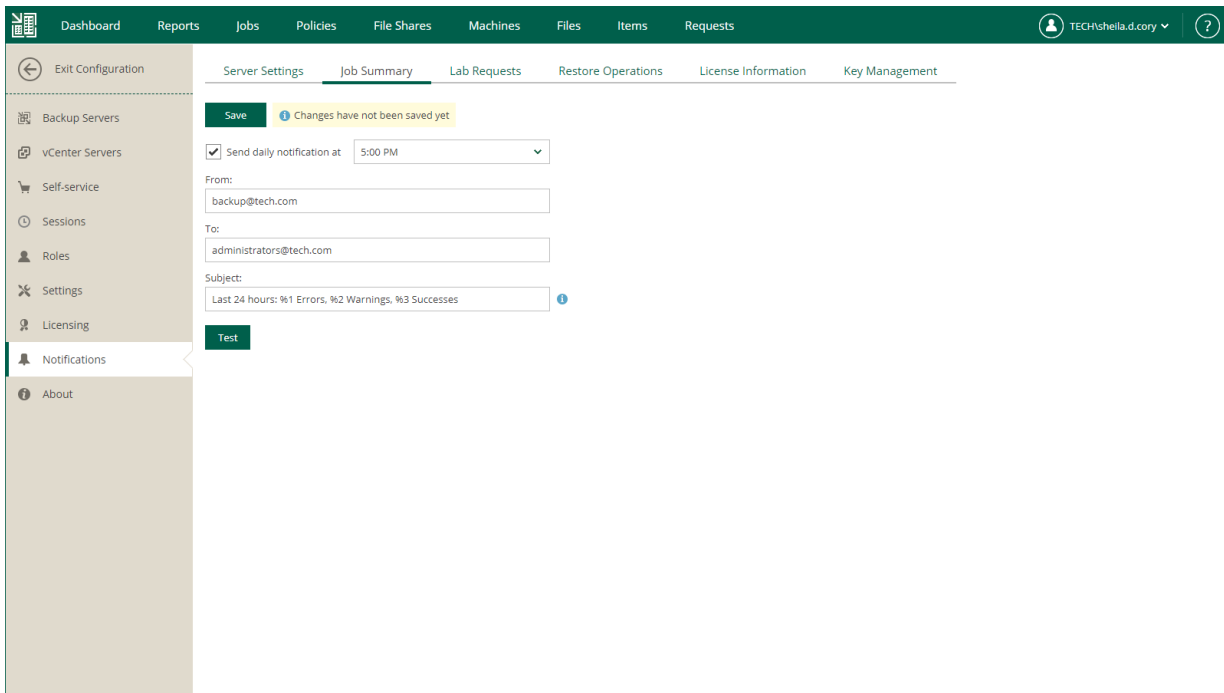
You can configure Veeam Backup Enterprise Manager to send daily notification emails with the results of finished jobs. The notification email contains a report about the number of jobs performed with the *Error*, *Warning* and *Success* statuses, and provides a link to the Veeam Backup Enterprise Manager 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 hoursJob 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.

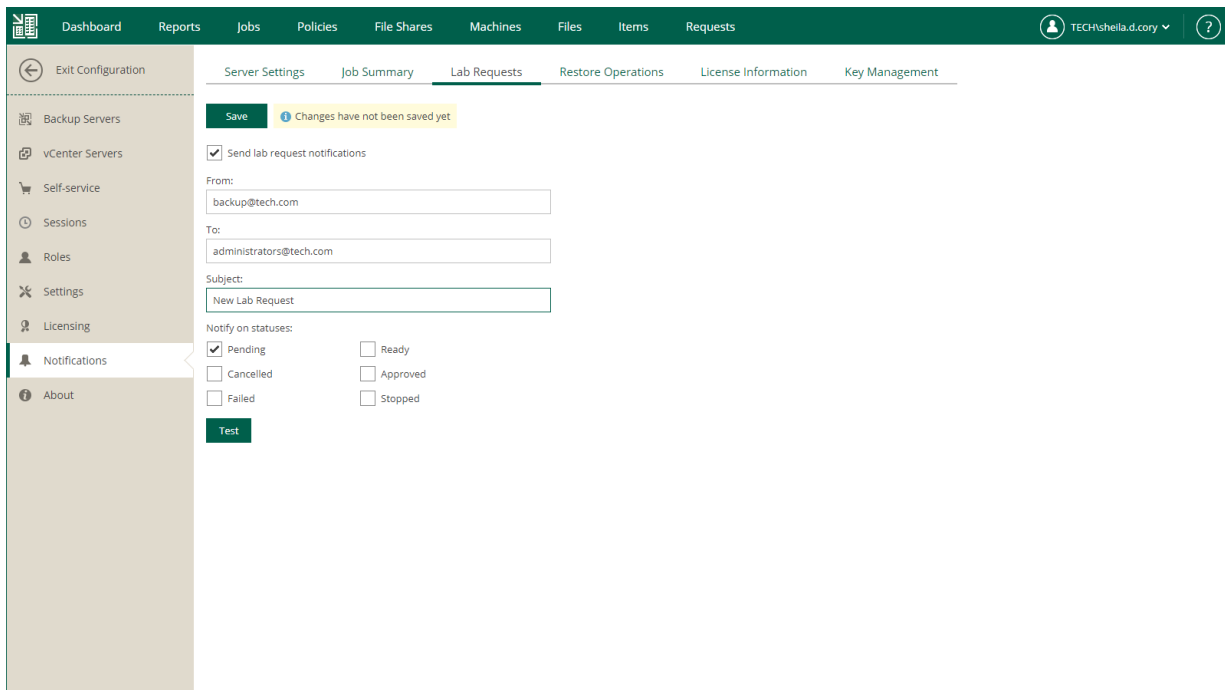
To receive notifications about lab requests, do the following:

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 email notifications about the following recovery operations:

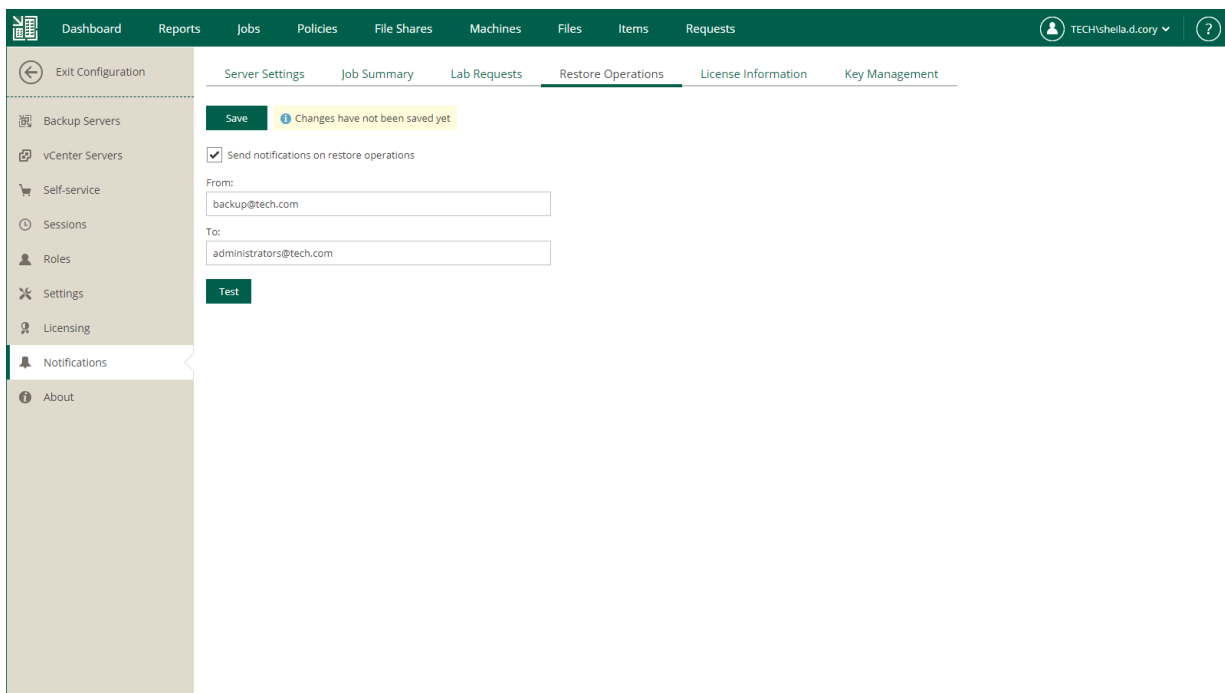
- [Instant VM Recovery](#)
- [Entire VM Restore](#)
- [Guest OS file restore](#)
- [Instant File Share Recovery](#)
- [Application Item Restore](#)

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.

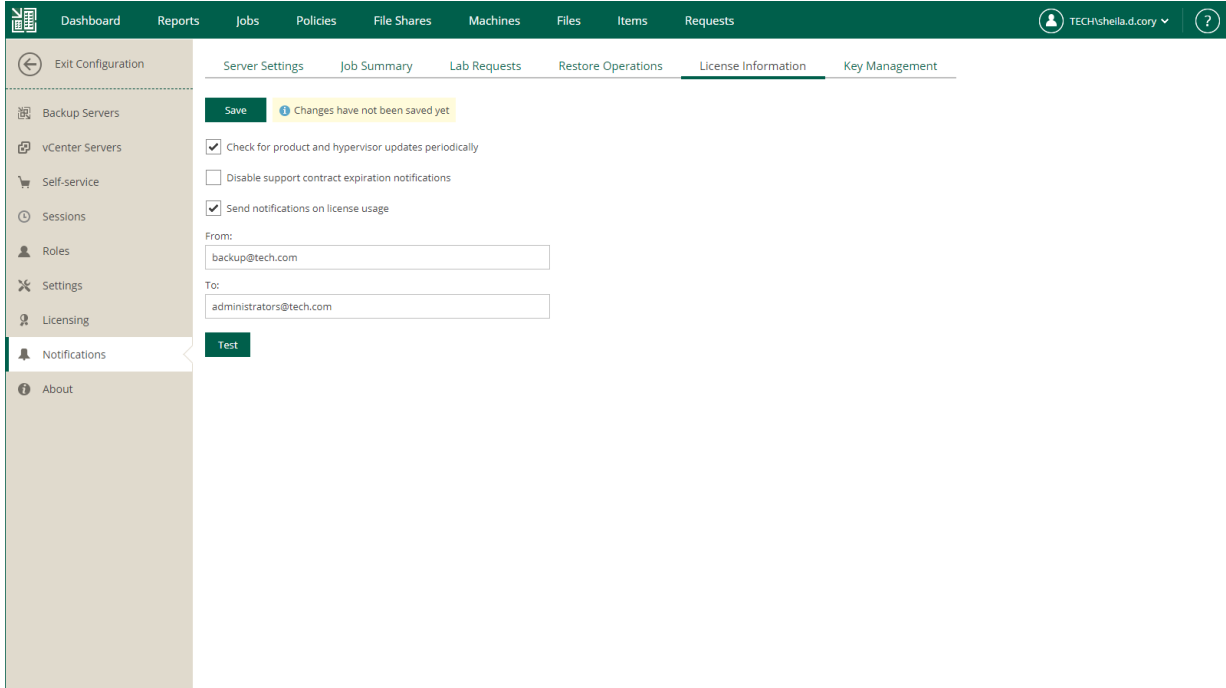
To enable email notifications on license usage:

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](#).

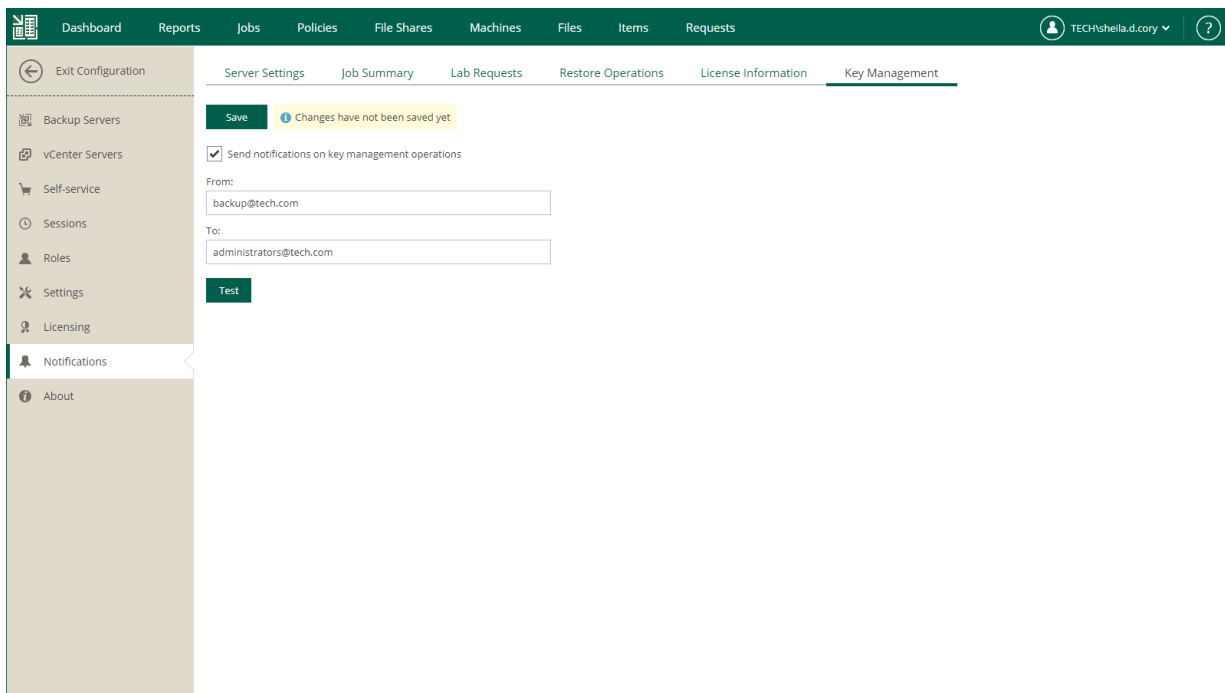
You can configure Enterprise Manager to send notifications about the following key management operations: key expiration, key deletion, key modification.

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.

Enterprise Manager Logs

You can use Veeam Backup Enterprise Manager logs to submit a support ticket. To ensure that overall and comprehensive information is provided to Veeam Customer Support, send all log files when submitting a support ticket.

To download Enterprise Manager logs, in the **About** section of the **Configuration** view, click **Download support logs**.

Alternatively, you can find the Enterprise Manager log files on the Enterprise Manager server at the following paths:

- Veeam Backup Enterprise Manager Service logs

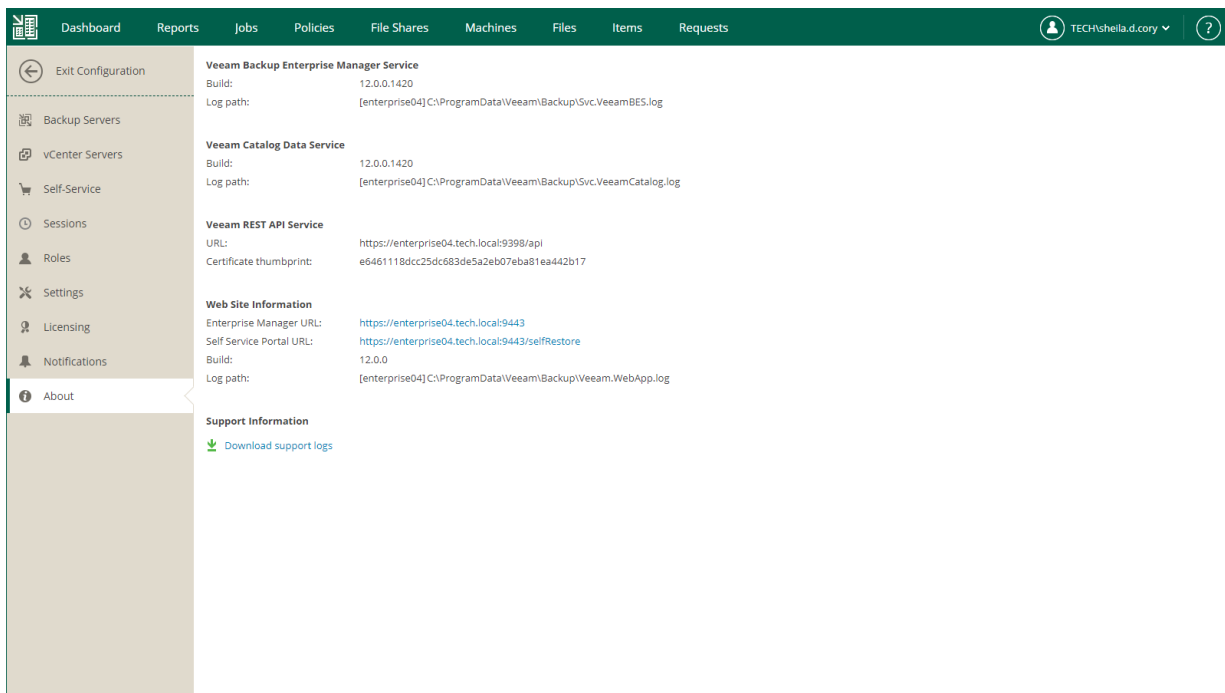
```
C:\ProgramData\Veeam\Backup\Svc.VeeamBES.log
```

- Veeam Guest Catalog Service logs

```
C:\ProgramData\Veeam\Backup\Svc.VeeamCatalog.log
```

- Enterprise Manager web app logs

```
C:\ProgramData\Veeam\Backup\Veeam.WebApp.log
```



TLS Certificates

TLS certificates ensure secure connection with Veeam Backup Enterprise Manager over HTTPS. During the Enterprise Manager installation, you can select an existing certificate or generate a new self-signed certificate. The certificate is bound to Enterprise Manager, the REST API and their ports.

Initially, Veeam Backup Enterprise Manager uses the same TLS certificate for all connections. If you want to use different certificates, you can update your current certificate. For more information, see [Updating TLS Certificates](#).

TLS certificates are used for the following purposes:

- Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service communicate with backup servers added to the Enterprise Manager infrastructure.

For more information, see [Connecting to Backup Servers](#).

- Veeam Backup Enterprise Manager web app and Veeam vSphere Client plug-in communicate with a browser.
- Veeam Backup Enterprise Manager REST API service communicates with a REST API client.

Connecting to Backup Servers

When communicating with backup servers that have Veeam Backup & Replication 12 installed, Veeam Backup Enterprise Manager uses a TLS certificate for authentication so that Veeam Backup Enterprise Manager does not store backup server account credentials. For connections with backup servers with earlier versions of Veeam Backup & Replication, Veeam Backup Enterprise Manager uses backup server account credentials for authentication.

Certificate-based connection works in the following way:

1. When adding a backup server, you specify connection settings including an account with Veeam Backup Administrator role assigned on the backup server.

For more information, see [Adding, Editing and Removing Backup Servers](#).

2. Veeam Backup Enterprise Manager sends the credentials as well as the certificate thumbprint that will be used by Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service for authentication.
3. Veeam Backup & Replication validates the credentials and saves Enterprise Manager data including the certificate thumbprint.
4. Veeam Backup & Replication sends its certificate thumbprint to Enterprise Manager.

For more information on managing backup server certificates, see the [Backup Server Certificate](#) section of the Veeam Backup & Replication User Guide.

5. You validate the certificate. If you trust the certificate, Enterprise Manager adds the backup server to the infrastructure and saves the thumbprint to the database.

If a backup server is not available at the moment, Enterprise Manager stores the backup server account credentials until the connection is established. Then the credentials are deleted from the Enterprise Manager database.

6. The next time Enterprise Manager connects to Veeam Backup & Replication, the Enterprise Manager certificate is used for authentication.
7. If a backup server certificate is updated, you will have to validate it from Enterprise Manager. Until you validate the certificate, Enterprise Manager cannot collect data from the backup server.
8. Thirty days before the Enterprise Manager certificate is expired, you are prompted to update it.

For more information, see [Updating TLS Certificates](#).

Updating TLS Certificates

If an existing TLS certificate expires, or if you want to use another certificate, for example, the one obtained from a Certificate Authority, you can update the current certificate.

- To update the certificate used by Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service, go to **Configuration > Backup Servers** and click **Update certificate**.
- To update the certificate used by Veeam Backup Enterprise Manager web app and Veeam vSphere Client plug-in, you can use Internet Information Services (IIS) Manager. For more information, see [this Microsoft Docs article](#).

If you want to use a certificate obtained from a Certificate Authority, make sure that the fully qualified domain name of the Enterprise Manager server is specified in the certificate subject or subject alternative name.

- To update the Veeam Backup 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.

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 file 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:

- o `messages.pot`
- o `vcloud_messages.pot`
- o `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:

- o `messages.<code>.po`
- o `vcloud_messages.<code>.po`
- o `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 <i>1.0</i> .
Content-Type	Content type and character encoding used for the translation language. Set the type value to <i>text/plain</i> . You can use the UTF-8 encoding for any language.
Content-Transfer-Encoding:	Content transfer encoding. Set the value to <i>8bit</i> .
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\resources\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.

Viewing Operation Statistics

On the **Dashboard** tab of the home page, you can see on-going statistics on backup servers and a chart that shows date and time when backup jobs were performed, and the network throughput rate during the backup jobs.

Backup Servers Statistics

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.

You can view statistics for one of the following time ranges:

- Last 24 hours
- Last 7 days

To switch between the ranges, select the necessary tab in the top left corner.

The **Summary** widget contains the following information:

- *Backup servers* – number of backup servers added to the Enterprise Manager infrastructure.
- *Jobs* – number of jobs configured on the added backup servers (including backup, backup copy, replication, sure backup, backup to tape and file to tape jobs).
- *Machines* – number of machines processed by the backup servers (including VMware VMs, Microsoft Hyper-V VMs, and Veeam Agent machines managed by backup servers). If a machine is processed by multiple jobs, it is counted as a single machine.
- *File shares* – number of file shares processed by the backup servers.

The **Image Data** widget contains information about backups of VMware VMs, Microsoft Hyper-V VMs, and Veeam Agent machines managed by backup servers. Note that the data covers all Veeam Agent backup modes: image-level, volume-level and file-level.

- *Processing speed* – average processing speed.
- *Source size* – total size of processed machines. If a machine is processed by multiple jobs (including backup copy jobs), it is counted as a single machine.
- *Full backups* – total size of full backups. This number does not include backups created by backup copy jobs.
- *Restore points* – total size of incremental backups. This number does not include backups created by backup copy jobs.

The **File Data** widget contains the following information about file share backups:

- *Processing speed* – average speed of file share processing.
- *Source size* – total size of processed source files.
- *Backup* – total size of backup files.
- *Archive* – total size backup files moved to the archive repository.

The **Last 24 hours / Last 7 days** widget reports on the job session results for the selected period.

- *Total job runs* – total number of job runs.

- *Success* – number of jobs completed successfully.
- *Warning* – number of jobs completed with a warning.
- *Error* – number of failed jobs.

The **Status** widget contains the following information:

- *Backups* – status of backups that are verified by SureBackup jobs.
- *Backup servers* – status of the last collection job session.
- *Management server* – status of the Veeam Backup Enterprise Manager management server.
- *License* – status of 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

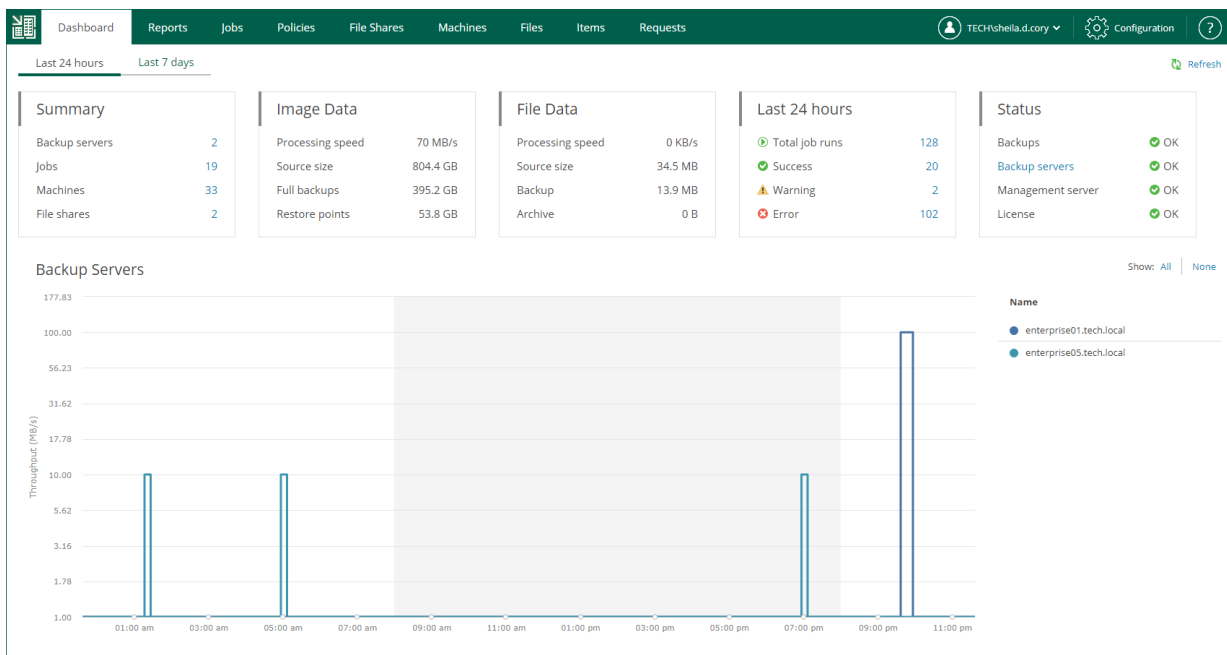
The **Backup Servers** chart shows date and time when backup jobs were performed, and the network throughput rate during the backup jobs. Jobs related to each backup server have their own color on the chart. The legend on the right interprets the color scheme used for all backup servers added to the Enterprise Manager infrastructure.

You can view the chart for one of the time following ranges:

- Last 24 hours
- Last 7 days

To switch between the ranges, select the 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 Dashboard Chart](#).



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:

- Enterprise Manager does not display backup policies created with the following Veeam solutions for cloud environments:
 - Veeam Backup for AWS
 - Veeam Backup for Google Cloud
 - Veeam Backup for Microsoft Azure
- 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.

Name	Type	Platform	Backup Server	Status	Latest Run	Next Run	Description
Repository Backup Copy	Periodic Copy	Image-Level	enterprise05.tech.lo...	Never started	Not available	Disabled	Created by TECH\shella.d.cory
Windows Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	3 hours ago	3/7/2023 08:00:00 am	Created by ENTERPRISE01\Administrator
SMB Share Backup	File Share Backup	File Share	enterprise05.tech.lo...	Failed	4 hours ago	3/7/2023 07:00:00 am	Created by TECH\shella.d.cory
AD Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	4 hours ago	3/7/2023 07:00:00 am	Created by TECH\shella.d.cory
NFS Share Backup	File Share Backup	File Share	enterprise05.tech.lo...	Success	5 hours ago	3/7/2023 06:30:00 am	Created by TECH\shella.d.cory
MSSQL02 Backup to Default Repository	Backup	VMware vSphere	enterprise05.tech.lo...	Success	6 hours ago	3/7/2023 05:00:00 am	Created by TECH\shella.d.cory
HV Backup	Backup	Microsoft Hyper-V	enterprise01.tech.lo...	Success	12 hours ago	3/6/2023 11:15:00 pm	Created by ENTERPRISE01\Administrator at 2/2...
PostgreSQL Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	12 hours ago	3/6/2023 11:00:00 pm	Created by ENTERPRISE01\Administrator
Window Oracle Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	13 hours ago	3/6/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
File Copy	Copy	Not available	enterprise01.tech.lo...	Success	13 hours ago	3/6/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
Web Servers Backup Copy	Immediate Copy	Image-Level	enterprise05.tech.lo...	Failed	15 hours ago	As new restore points appear	Created by TECH\shella.d.cory
Web Servers Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	20 hours ago	3/6/2023 03:00:00 pm	Created by TECH\shella.d.cory
RHEL Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	1 day ago	3/8/2023 07:00:00 am	Created by ENTERPRISE05\Administrator
Cloud Director Backup	Backup	VMware Cloud Director	enterprise01.tech.lo...	Success	1 day ago	3/11/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
Backup Copy Job 1	Periodic Copy	Image-Level	enterprise05.tech.lo...	Failed	1 day ago	3/8/2023 02:00:00 pm	Created by ENTERPRISE03\Administrator
Templates Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	1 day ago	3/6/2023 03:00:00 pm	Created by TECH\shella.d.cory
Oracle Linux Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Failed	6 days ago	Disabled	Created by ENTERPRISE05\Administrator
Ubuntu Replication	Replica	VMware vSphere	enterprise05.tech.lo...	Warning	27 days ago	Not scheduled	Created by TECH\shella.d.cory
Backup Job	Backup	VMware Cloud Director	enterprise05.tech.lo...	Warning	38 days ago	Not scheduled	Created by TECH\hue.spenser at 1/27/2023 12:...
Cloud Director Backup Job	Backup	VMware Cloud Director	backupsrv52.tech.lo...	Success	38 days ago	Not scheduled	Not available
Daily Backup Job	Backup	VMware vSphere	backupsrv52.tech.lo...	Success	39 days ago	Not scheduled	Not available

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 Microsoft SQL Server, Oracle or PostgreSQL backup job with transaction log processing enabled, see the [Starting and Stopping Transaction Log Backup Jobs](#) section of the Veeam Backup & Replication User Guide.

The screenshot displays the 'Jobs' tab in the Veeam Backup & Replication portal. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The 'Jobs' tab is active, showing a list of backup jobs. The table has the following columns: Name, Type, Platform, Backup Server, Status, Latest Run, Next Run, and Description. The 'SMB Share Backup' job is highlighted, and a mouse cursor is clicking the 'Start' button. Other jobs include 'Repository Backup Copy', 'Windows Backup', 'AD Backup', 'NFS Share Backup', 'MSSQL02 Backup to Default Repository', 'HV Backup', 'PostgreSQL Backup', 'Window Oracle Backup', 'File Copy', 'Web Servers Backup Copy', 'Web Servers Backup', 'RHEL Backup', 'Cloud Director Backup', 'Backup Copy Job 1', 'Templates Backup', 'Oracle Linux Backup', 'Ubuntu Replication', 'Backup Job', 'Cloud Director Backup Job', and 'Daily Backup Job'. The status of jobs varies, including 'Never started', 'Success', 'Failed', and 'Warning'. The bottom of the interface shows 'Records per Page: 25', 'Page 1 of 1', and 'Displaying 1 - 21 of 21'.

Name	Type	Platform	Backup Server	Status	Latest Run	Next Run	Description
Repository Backup Copy	Periodic Copy	Image-Level	enterprise05.tech.lo...	Never started	Not available	Disabled	Created by TECH\shella.d.cory
Windows Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	3 hours ago	3/7/2023 08:00:00 am	Created by ENTERPRISE01\Administrator
SMB Share Backup	File Share Backup	File Share	enterprise05.tech.lo...	Failed	4 hours ago	3/7/2023 07:00:00 am	Created by TECH\shella.d.cory
AD Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	4 hours ago	3/7/2023 07:00:00 am	Created by TECH\shella.d.cory
NFS Share Backup	File Share Backup	File Share	enterprise05.tech.lo...	Success	5 hours ago	3/7/2023 06:30:00 am	Created by TECH\shella.d.cory
MSSQL02 Backup to Default Repository	Backup	VMware vSphere	enterprise05.tech.lo...	Success	6 hours ago	3/7/2023 05:00:00 am	Created by TECH\shella.d.cory
HV Backup	Backup	Microsoft Hyper-V	enterprise01.tech.lo...	Success	12 hours ago	3/6/2023 11:15:00 pm	Created by ENTERPRISE01\Administrator at 2/2...
PostgreSQL Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	12 hours ago	3/6/2023 11:00:00 pm	Created by ENTERPRISE01\Administrator
Window Oracle Backup	Backup	VMware vSphere	enterprise01.tech.lo...	Success	13 hours ago	3/6/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
File Copy	Copy	Not available	enterprise01.tech.lo...	Success	13 hours ago	3/6/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
Web Servers Backup Copy	Immediate Copy	Image-Level	enterprise05.tech.lo...	Failed	15 hours ago	As new restore points appear	Created by TECH\shella.d.cory
Web Servers Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	20 hours ago	3/6/2023 03:00:00 pm	Created by TECH\shella.d.cory
RHEL Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	1 day ago	3/8/2023 07:00:00 am	Created by ENTERPRISE05\Administrator
Cloud Director Backup	Backup	VMware Cloud Director	enterprise01.tech.lo...	Success	1 day ago	3/11/2023 10:00:00 pm	Created by ENTERPRISE01\Administrator
Backup Copy Job 1	Periodic Copy	Image-Level	enterprise05.tech.lo...	Failed	1 day ago	3/8/2023 02:00:00 pm	Created by ENTERPRISE03\Administrator
Templates Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Success	1 day ago	3/6/2023 03:00:00 pm	Created by TECH\shella.d.cory
Oracle Linux Backup	Backup	VMware vSphere	enterprise05.tech.lo...	Failed	6 days ago	Disabled	Created by ENTERPRISE05\Administrator
Ubuntu Replication	Replica	VMware vSphere	enterprise05.tech.lo...	Warning	27 days ago	Not scheduled	Created by TECH\shella.d.cory
Backup Job	Backup	VMware Cloud Director	enterprise05.tech.lo...	Warning	38 days ago	Not scheduled	Created by TECH\hue.spenser at 1/27/2023 12:...
Cloud Director Backup Job	Backup	VMware Cloud Director	backupsrv52.tech.lo...	Success	38 days ago	Not scheduled	Not available
Daily Backup Job	Backup	VMware vSphere	backupsrv52.tech.lo...	Success	39 days ago	Not scheduled	Not available

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, Oracle or PostgreSQL machines, transaction log processing (if enabled for that job) will be also disabled.

- Scheduled replication jobs

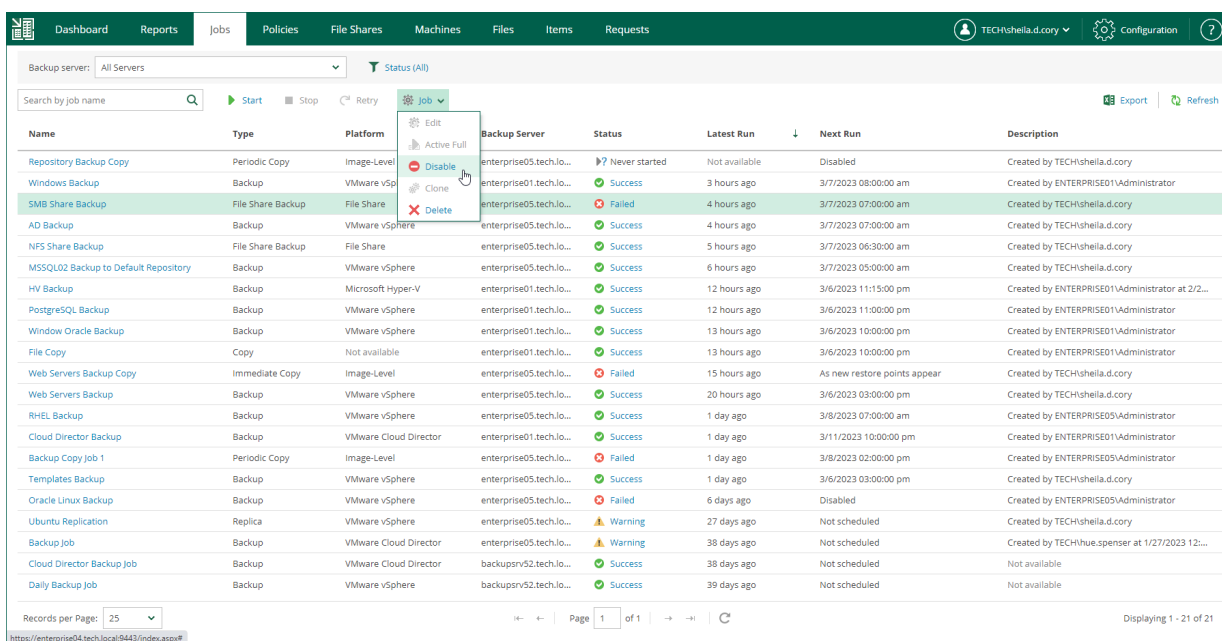
Disabled replication jobs are not started by the specified schedule.

- 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.

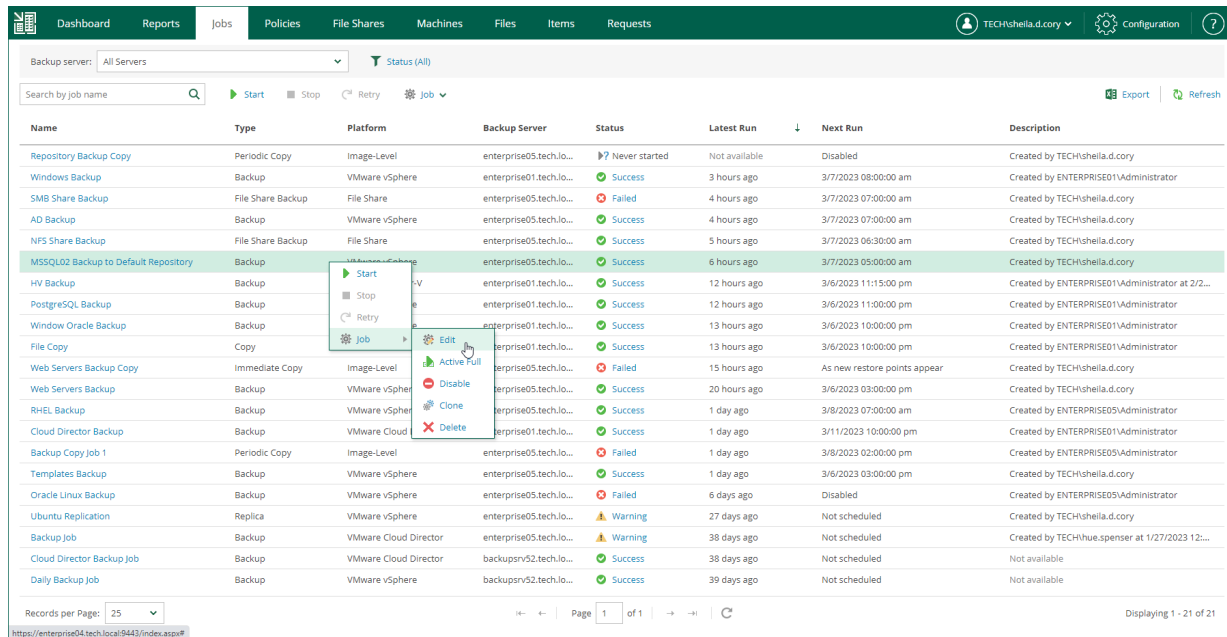
1. [Launch the wizard for job editing.](#)
2. [Edit job name and retention settings.](#)
3. [Edit the list of VMs.](#)
4. [Change the VM processing order.](#)
5. [Configure guest processing settings.](#)
6. [Edit job scheduling settings.](#)

Step 1. Launch Wizard

To launch the wizard for job editing:

1. On **Jobs** tab, select the necessary job from the list.
2. On the toolbar, click **Job** to expand the list of available actions.
3. Select **Edit**.

Alternatively, you can right-click a job and select **Job > 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.

5. 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. For more information on job priorities, see the [Job Priorities](#) section of the Veeam Backup & Replication User Guide.

Edit Backup Job [X]

Job Settings | Specify the job name, description and retention policy

VMs

Guest Processing

Job Schedule

Job name: Backup to Default Repository

Description: Created by TECH\sheila.d.cory

Retention policy

Retention policy: 6 Days

Keep certain full backups longer for archival purposes [Configure](#)
1 weekly, 1 monthly, 1 yearly

High priority [i](#)

Next Finish Cancel

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.

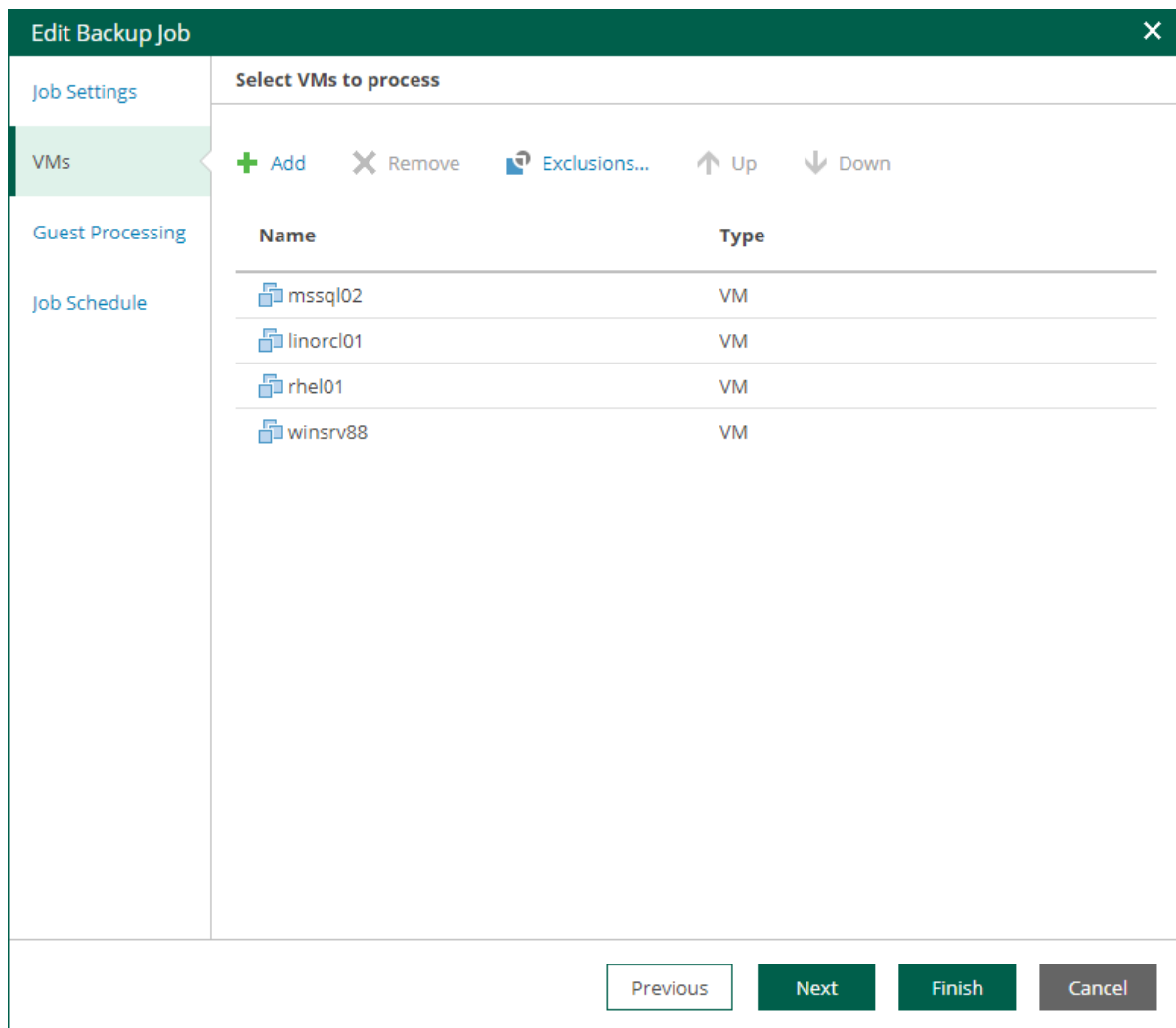
NOTE

- For VMware Cloud Director backup jobs, you can add and remove the following Cloud Director objects: VMs, vApps, organization VDCs, organizations and the Cloud Director instance. The scope depends on your Cloud Director access rights.
- For VMware Cloud Director replication jobs, you cannot add or remove single VMs. You can manage only vApps and other Cloud Director containers.

Adding VMs and VM containers

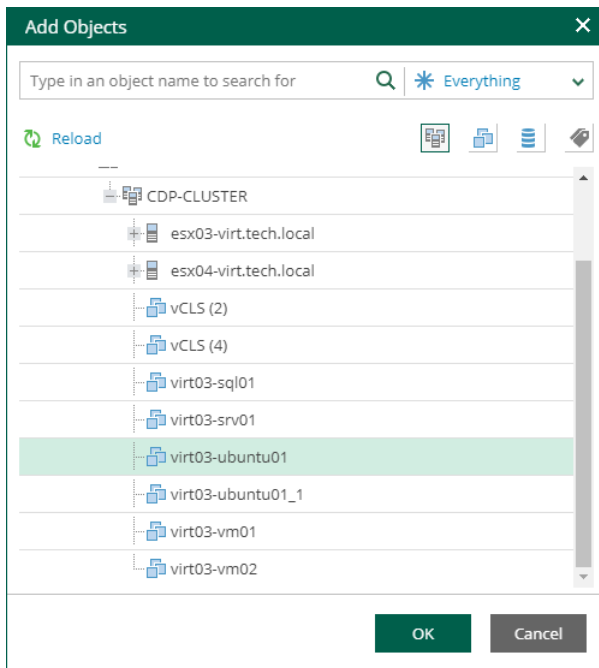
To add a VM or a VM container:

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 VMware Cloud Director backup jobs, you can change the order of the following Cloud Director objects: VMs, vApps, organization VDCs, organizations and the Cloud Director instance. The scope depends on your Cloud Director access rights.
- For VMware Cloud Director replication jobs, you cannot change the VM processing order. You can manage only vApps and other Cloud Director containers.

Edit Backup Job

Job Settings

VMs

Guest Processing

Job Schedule

Select VMs to process

+ Add X Remove Exclusions... Up Down

Name	Type
rhel01	VM
mssql02	VM
linorcl01	VM
winsrv88	VM

Previous Next Finish Cancel

Step 5. Configure Guest Processing Settings

At the **Guest Processing** step of the wizard, you can configure the following settings for VM guest OS processing:

- [Application-Aware Processing](#)
- [Guest OS File Indexing](#)
- [Guest OS Credentials](#)

Edit Backup Job

Job Settings

VMs

Guest Processing

Job Schedule

Choose guest OS processing options available for running machines

Enable application-aware processing ⓘ

[Customize Application](#)

Customize application handling options for individual machines and applications

Enable guest file system indexing ⓘ

[Customize Indexing](#)

Customize advanced guest file system indexing options for individual machines

Guest OS credentials

Credentials: [+ Add](#)

[Customize Credentials](#)

Customize guest OS credentials for individual machines and operating systems

[Previous](#) [Next](#) [Finish](#) [Cancel](#)

Application-Aware Processing

At the **Guest Processing** step of the wizard, you can enable application-aware processing. Application-aware processing is a Veeam technology based on Microsoft VSS and used to create transactionally consistent backups or replicas of VMs that run Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, Oracle or PostgreSQL. For more information, see the [Application-Aware Processing](#) section of the Veeam Backup & Replication User Guide.

To configure application-aware processing, take the following steps:

1. Select the **Enable application-aware processing** check box.
2. Click the **Customize Application** link.

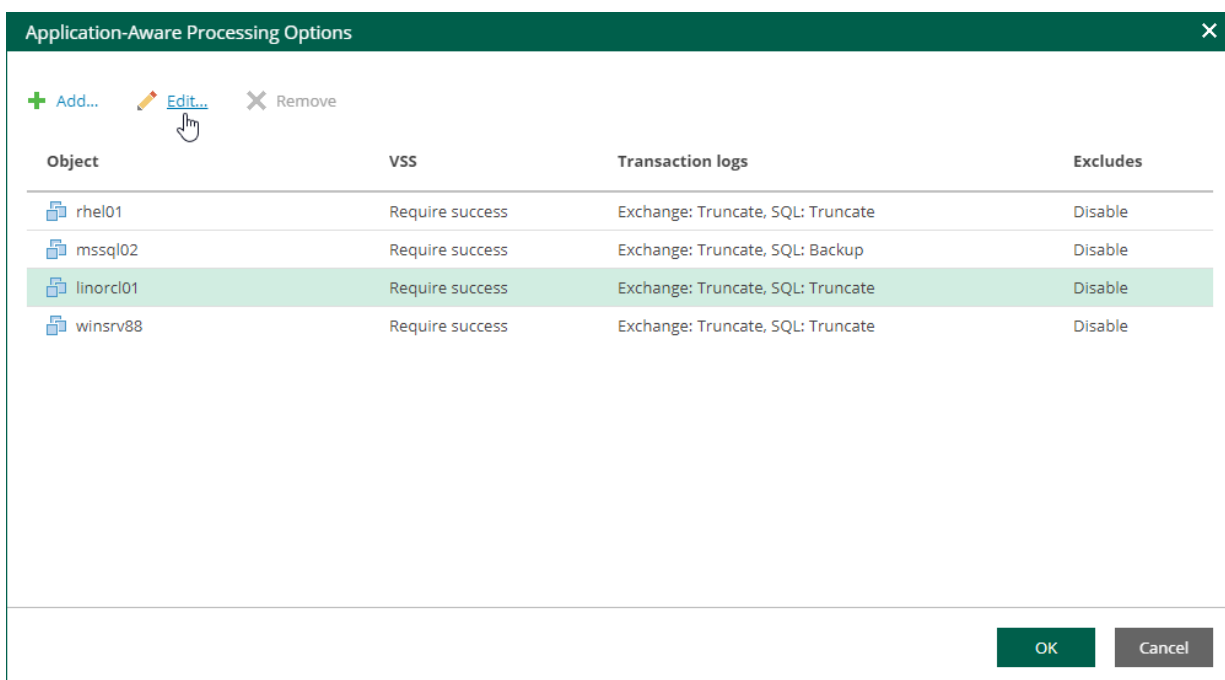
3. To define custom settings for a machine, select it and click **Edit**.

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](#)
- [Microsoft SQL Server Transaction Log Settings](#)
- [Oracle Archived Redo Log Settings](#)
- [PostgreSQL Archive Log Settings](#)
- [VM Guest OS File Exclusion](#)



General Settings

On the **General** tab, you can specify general application-aware processing settings.

1. In the **Applications** section, select the option that corresponds to your transactionally-consistent backup creation scenario.
 - 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.

2. If you want Veeam Backup & Replication to process application logs or create copy-only backups, do one of the following:

- [For Microsoft Exchange and Microsoft SQL VMs] If you want Veeam Backup & Replication to process application logs, select **Process transaction logs with this job** and specify settings on the **SQL** tab. For more information, see [Microsoft SQL Server Transaction Log Settings](#).

NOTE

[For Microsoft Exchange VMs] If you select this option, Veeam Backup & Replication will back up the Exchange database and its logs. The non-persistent runtime components or persistent components that run on the VM guest OS will wait for a backup job to complete successfully. After that, they will trigger truncation of transaction logs on a Microsoft Exchange server. If the backup job fails, the logs on this server will remain untouched.

- [For Microsoft Exchange and Microsoft SQL VMs] If you use a third-party backup tool to perform VM guest level backup, and this tool maintains consistency of the database state, select **Perform copy only**. Veeam Backup & Replication will create a copy-only backup for the selected VM. The copy-only backup preserves the chain of full or differential backup files and transaction logs on the VM. For more information, see [Microsoft Docs](#).

Note that if you select this option, the **SQL** tab will not be available in the **VM Processing Settings** window.

- [For Oracle VMs and PostgreSQL VMs] You must specify settings for application log handling on the **Oracle** and **PostgreSQL** tabs of the **VM Processing Settings** window. For more information, see [Oracle Archived Redo Log Settings](#) and [PostgreSQL Archive Log Settings](#).

3. In the **Persistent guest agent** section, specify if Veeam Backup & Replication must use persistent guest agents on each protected VM for application-aware processing.

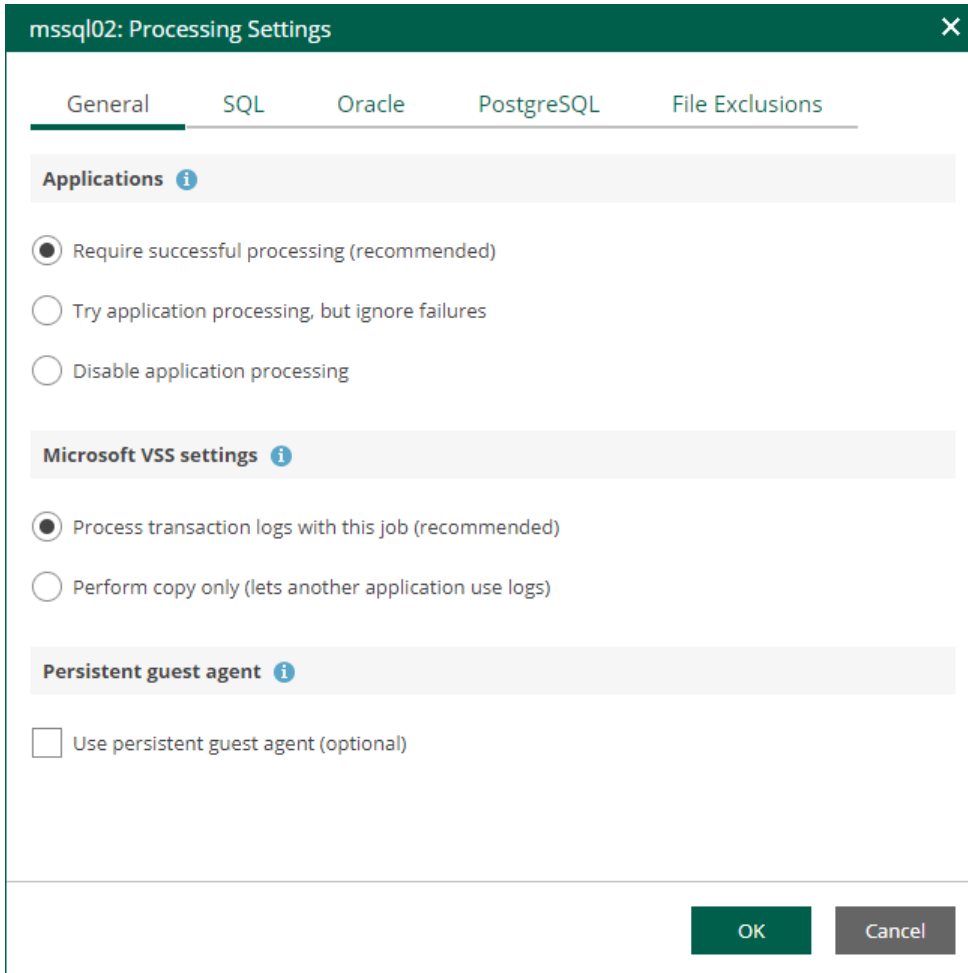
By default, Veeam Backup & Replication uses non-persistent runtime components.

Veeam Backup & Replication deploys runtime components on each protected VM when the backup job starts, and removes the runtime components as soon as the backup job finishes.

Select the **Use persistent guest agent check** box to enable persistent agent components for guest processing. For more information, see the [Non-Persistent Runtime Components and Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.

IMPORTANT

If both Microsoft SQL Server and Oracle Server are installed on the same VM, and this VM 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.

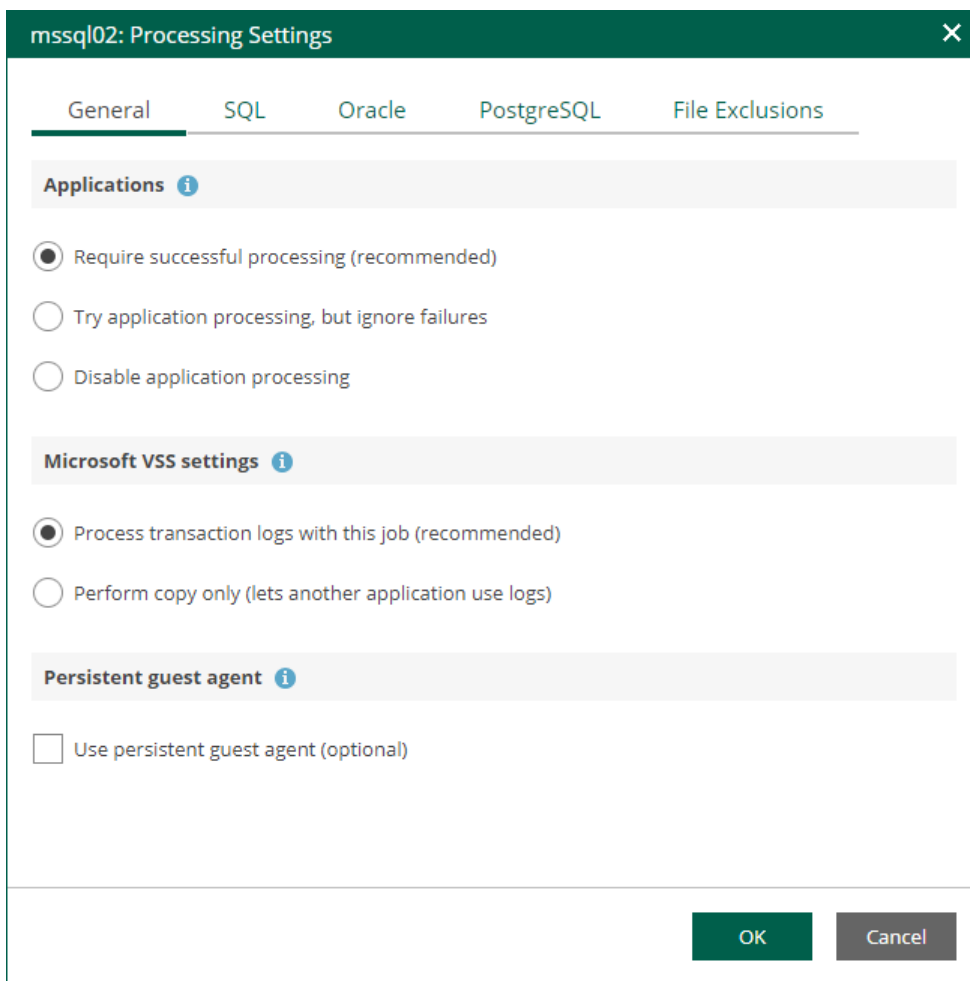


Microsoft SQL Server Transaction Log Settings

If you back up a Microsoft SQL VM, you can specify how Veeam Backup & Replication must process transaction logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Microsoft SQL Server VM from the list and click **Edit**.
4. On the **General** tab of the **VM Processing Settings** window, make sure the following options are selected:
 - In the **Applications** section, either the **Require successful processing** or **Try application processing, but ignore failures** option must be selected.

- In the **Microsoft VSS settings** section, the **Process transaction logs with this job** option must be selected.



5. Open the **SQL** tab of the **VM Processing Settings** window.
6. Specify how Veeam Backup & Replication will process SQL transaction logs.
 - Select **Truncate logs** to truncate transaction logs after successful backup. The non-persistent runtime components or persistent components running on the VM guest OS will wait for the backup to complete successfully and then truncate transaction logs. If the job does not manage to back up the Microsoft SQL Server VM, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

NOTE

If the account specified at the [Guest Processing](#) step does not have enough rights, Veeam Backup & Replication tries to truncate logs using the `NT AUTHORITY\SYSTEM` account. Make sure that the account has permissions listed in the [Permissions](#) section of the Veeam Explorers User Guide.

- Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Backup & Replication will not truncate transaction logs on the Microsoft SQL Server VM.
Select 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 on the VM guest OS may grow large and consume all disk space. In this case, the database administrators must take care of transaction logs themselves.

- Select **Backup logs periodically** to back up transaction logs with Veeam Backup & Replication. Veeam Backup & Replication will periodically copy transaction logs to the backup repository and store them together with the image-level backup of the Microsoft SQL Server VM. During the backup job session, transaction logs on the VM guest OS will be truncated.

For more information, see the [Microsoft SQL Server Transaction Log Settings](#) sections of the Veeam Backup & Replication User Guide.

7. If you have selected the **Backup logs periodically** option, specify settings for transaction log backup:
 - a. In the **Backup logs every <N> minutes** field, specify the frequency for transaction log backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
 - b. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup repository.
 - 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** 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 backups. For more information, see [Retention for Transaction Log Backups](#) section of the Veeam Backup & Replication User Guide.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport transaction logs. For more information, see the [Microsoft SQL Server Transaction Log Settings](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows a dialog box titled "dbserver01: Processing Settings" with a close button (X) in the top right corner. It has four tabs: "General", "SQL", "Oracle", and "File Exclusions". The "SQL" tab is selected. Below the tabs, there is a section titled "Choose how this job should process Microsoft SQL Server transaction logs". There are three radio button options:

- Truncate logs (prevents logs from growing forever)
- Do not truncate logs (requires simple recovery model)
- Backup logs periodically (backed up logs are truncated)

 Below the third option, there is a label "Backup logs every" followed by a spinner box containing the number "15" and the word "minutes". Underneath, there is a section titled "Retain log backups:" with two radio button options:

- Until the corresponding image-level backup is deleted
- Keep only last

 The second option has a spinner box containing the number "15" and the word "days". At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

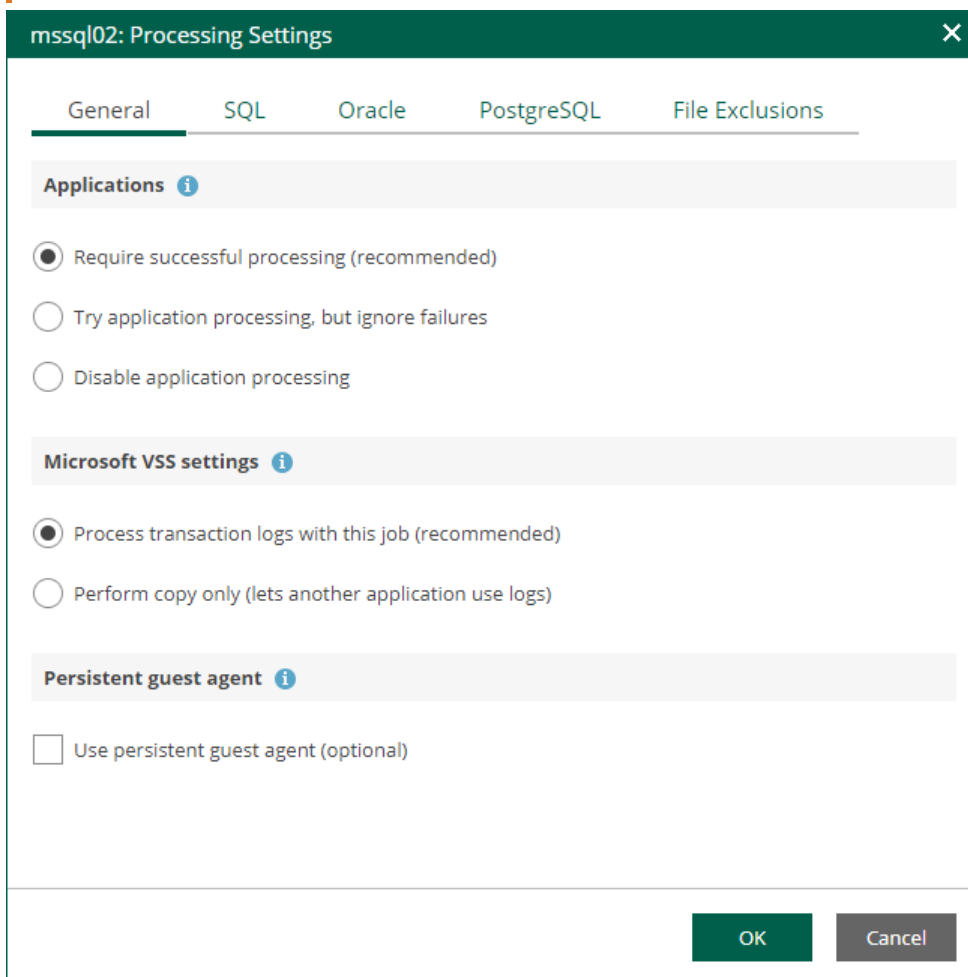
Oracle Archived Redo Log Settings

If you back up a VM where Oracle Database is deployed, you can specify how Veeam Backup & Replication must process archived redo logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Oracle VM from the list and click **Edit**.
4. On the **General** tab of the **VM Processing Settings** window, make sure that either the **Require successful processing** or **Try application processing, but ignore failures** option is selected.

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.



5. On the **Oracle** tab of the **VM Processing Settings** window, specify log processing settings.
 - a. Specify a user account that will connect to the Oracle database and perform Oracle archived logs backup and deletion.
 - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.

- Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

Make sure the specified account has sufficient rights. For details, see the [Permissions](#) section of the Veeam Explorers User Guide.

b. Specify how Veeam Backup & Replication must process archived redo logs on the Oracle VM.

- Select **Do not delete archived logs** to preserve archived redo logs on the original Oracle server.

Select this option for databases in the NOARCHIVELOG mode. If the database is in the ARCHIVELOG mode, archived logs on the VM guest OS may grow large and consume all disk space. In this case, database administrators must take care of archived logs themselves.

- Select **Delete logs older than <N> hours / Delete logs over <N> GB** to delete archived logs that are older than <N> hours or larger than <N> GB. The log size threshold refers not to the total size of all logs for all databases, but to the log size of each database on the selected Oracle VM.

When the parent backup job (job creating an image-level backup) runs, Veeam Backup & Replication will wait for the backup to complete successfully, and then trigger archived logs deletion on the Oracle VM over Oracle Call Interface (OCI). If the primary job does not manage to back up the Oracle VM, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

TIP

Veeam Backup & Replication removes redo logs only after the parent backup job session. To remove redo logs more often, you can schedule the job to run more often.

c. To back up Oracle archived logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archived log backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

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. Thus, you need to set up backup schedule and log removal conditions appropriately.

d. If you have selected the **Backup logs every <N> minutes** option, specify retention policy for the archived logs stored in the backup repository. For the **Retain log backups** setting, select one of the following:

- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level 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 image-level backups. For more information, see the [Retention for Archived Log Backups](#) section of the Veeam Backup & Replication User Guide.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport archived logs. For more information, see the [Oracle Archived Log Settings](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows the 'linorcl01: Processing Settings' dialog box with the 'Oracle' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with 'General', 'SQL', 'Oracle', 'PostgreSQL', and 'File Exclusions'. The 'Oracle' tab is active, displaying the following settings:

- Choose how this job should process Oracle archived logs**
- Specify Oracle account with SYSDBA privileges:
 - admin (admin) [dropdown arrow] + Add
- Do not delete archived logs
- Delete logs older than: 48 [spinners] hours
- Delete logs over: 10 [spinners] GB
- Backup logs every: 15 [spinners] minutes
- Retain log backups:**
 - Until the corresponding image-level backup is deleted
 - Keep only last: 15 [spinners] days

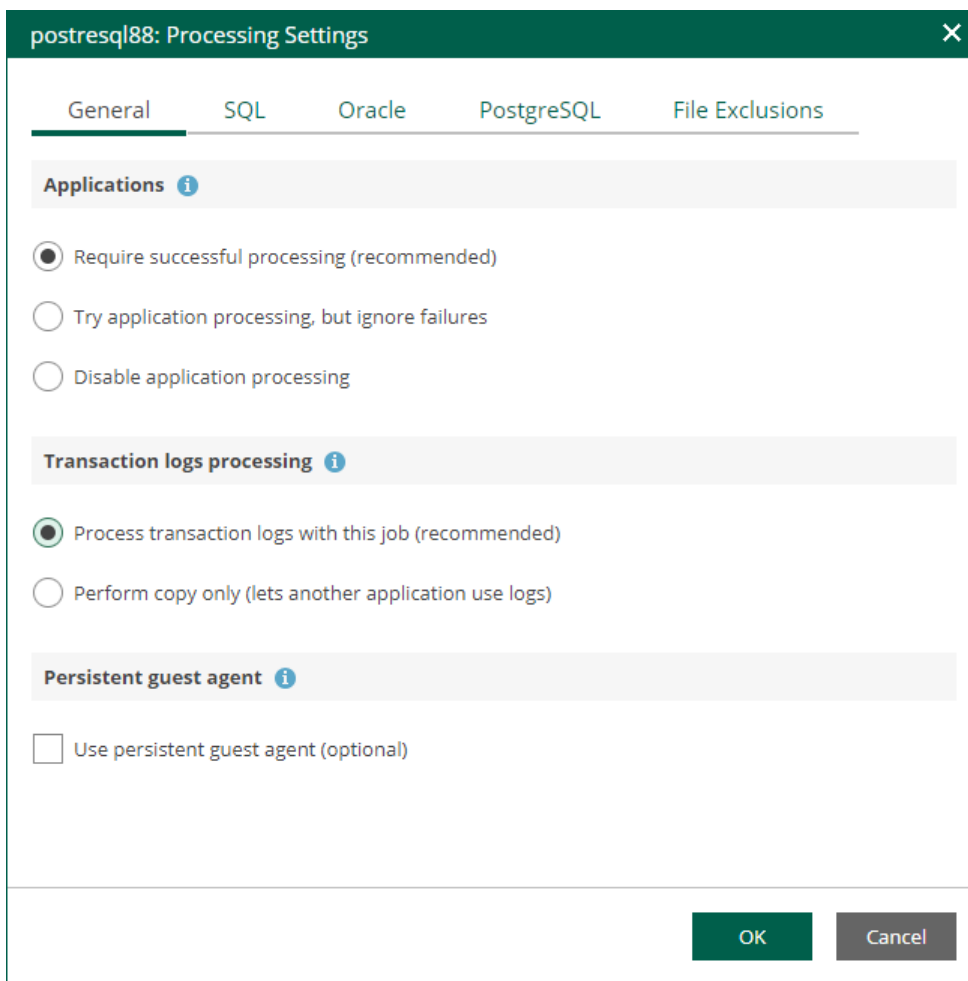
At the bottom right, there are 'OK' and 'Cancel' buttons.

PostgreSQL Archive Log Settings

If you back up a VM where PostgreSQL is deployed, you can specify how Veeam Backup & Replication must process PostgreSQL archive logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the PostgreSQL VM from the list and click **Edit**.

4. On the **General** tab of the **VM Processing Settings** window, make sure that either the **Require successful processing** or **Try application processing, but ignore failures** option is selected.



5. On the **PostgreSQL** tab of the **VM Processing Settings** window, specify settings for PostgreSQL logs processing.
- Specify an account that will connect to the PostgreSQL instance and perform PostgreSQL archive logs backup and deletion. The `pg_hba.conf` configuration file of the PostgreSQL instance must contain a record with the account.
 - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the PostgreSQL instance.
 - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

Make sure the specified account has sufficient rights. For details, see the [Permissions](#) section of the Veeam Explorers User Guide.
 - Specify an authentication method for the selected user account.
 - Select **Database user with password** if you have specified an account with password-based authentication. In this case, you must provide Veeam Backup & Replication with the account password that will be stored in the Veeam Backup & Replication database.
 - Select **Database user with password file (.pgpass)** if you have specified an account with password-based authentication. In this case, you do not have to specify the account password when adding the account in Veeam Backup & Replication. Instead, the account password must be specified in the PGPASS password file stored in the user's home directory.

- Select **System user without password (peer)** if you have specified a local system account with peer authentication.
- c. To back up PostgreSQL archive logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archive log backup. By default, archive logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
- d. If you have selected the **Backup logs every <N> minutes** option, specify retention policy for the archive logs stored in the backup repository. For the **Retain log backups** setting, select one of the following:
- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
 - Select **Keep only last <N> days** to keep archive logs for a specific number of days. By default, archive logs are kept for 15 days. If you select this option, you must make sure that retention for archive logs is not greater than retention for the image-level backups. For more information, see the [Retention for PostgreSQL WAL Files](#) section of the Veeam Backup & Replication User Guide.
- e. In the **PostgreSQL archive logs local temporary storage** field, specify a path on the PostgreSQL machine that Veeam Backup & Replication will use to temporarily store PostgreSQL archive logs until they are backed up. Veeam Backup & Replication does not create the temporary storage folder so the folder must exist on the machine. Make sure the temporary location has enough free space for storing the log files.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport archive logs. For more information, see the [Retention for PostgreSQL WAL Files](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows the 'rhel02: Processing Settings' dialog box with the 'PostgreSQL' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with 'General', 'SQL', 'Oracle', 'PostgreSQL', and 'File Exclusions'. The 'PostgreSQL' tab is active, showing the following settings:

- Choose how this job should process PostgreSQL transaction logs**
- Specify PostgreSQL account with superuser privileges:
 - Use guest credentials (selected in dropdown) + Add
- The specified user is:
 - Database user with password
 - Database user with password file (.pgpass)
 - System user without password (peer)
 - Backup logs every 15 minutes
- Retain log backups:
 - Until the corresponding image-level backup is deleted
 - Keep only last 15 days
- PostgreSQL archive logs local temporary storage:
 - /tmp

At the bottom right, there are 'OK' and 'Cancel' buttons.

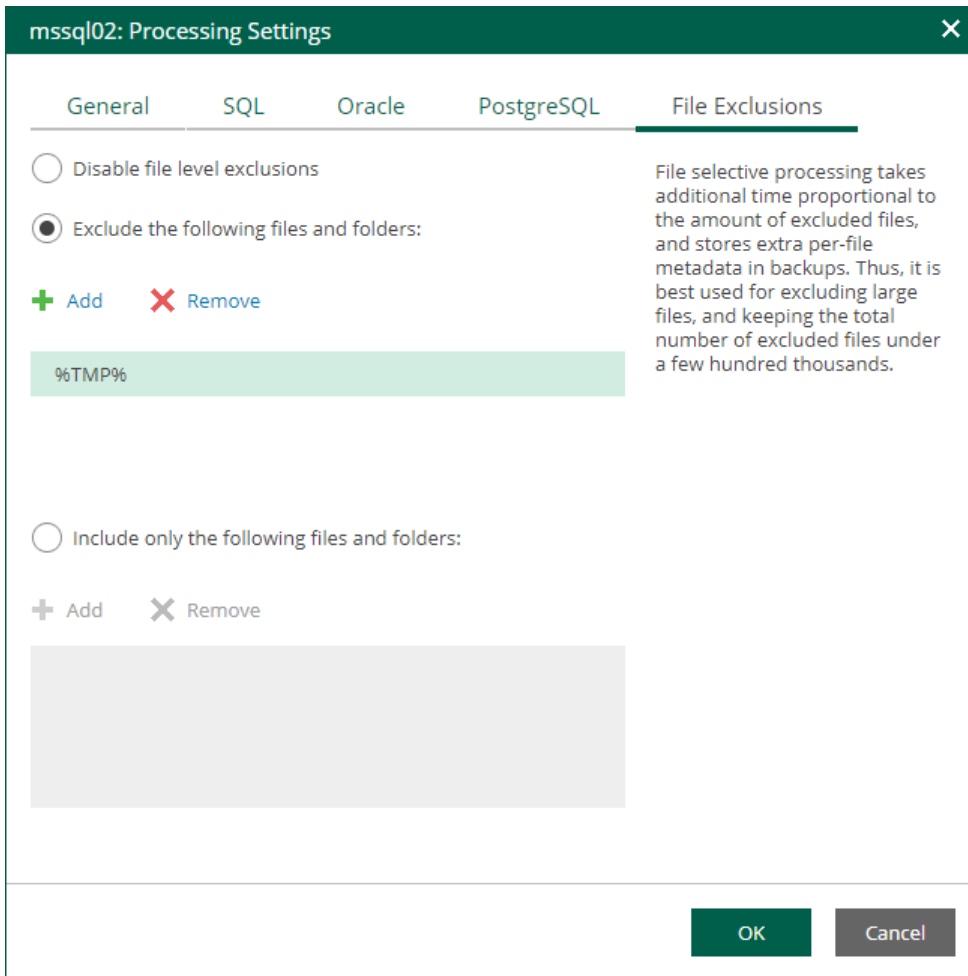
VM Guest OS File Exclusion

If you do not want to back up specific files and folders on the VM guest OS, you can exclude them from the backup. Exclusions can help decrease the backup file size. However, selective processing takes additional time that depends on the number of excluded files. It also 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.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select a VM from the list and click **Edit**.
4. On the **File Exclusions** tab, specify the files that must be excluded from the backup.
 - Select **Exclude the following files and folders** to remove individual files and folders from the backup.
 - Select **Include only the following files and folders** to leave only the specified files and folders in the backup.

5. 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

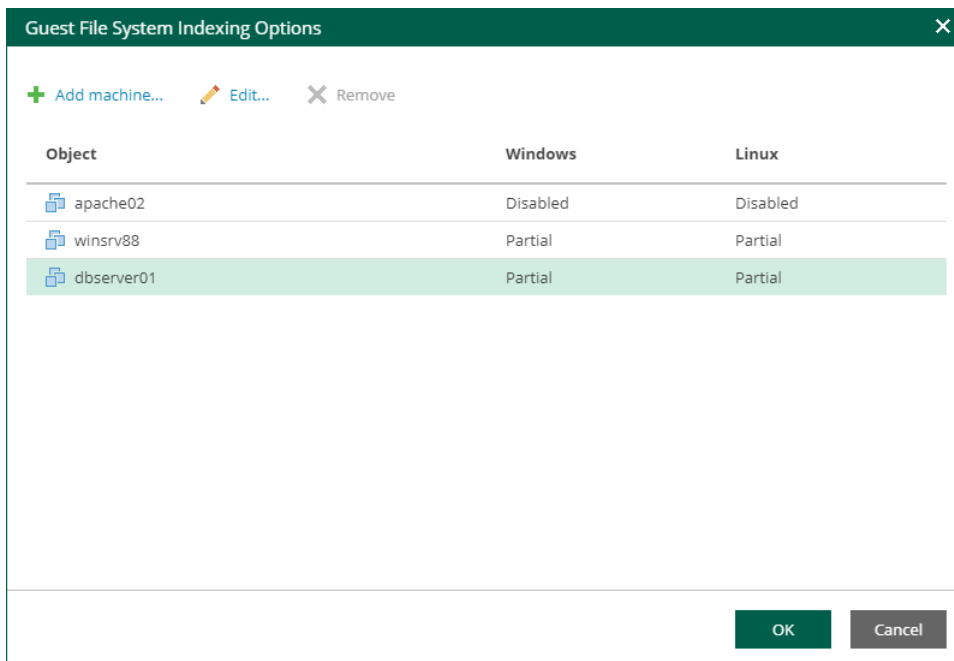
For proper file indexing of Linux machines, Veeam Backup & Replication requires several utilities to be installed on the machines: `mlocate`, `gzip`, and `tar`. If these utilities are not found, you are prompted to deploy them to support index creation.

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**.

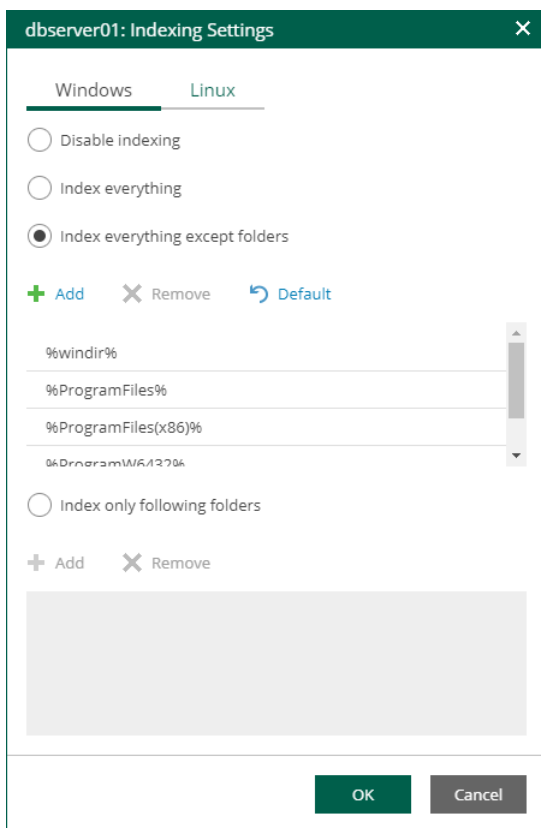
Consider the following:

- 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.

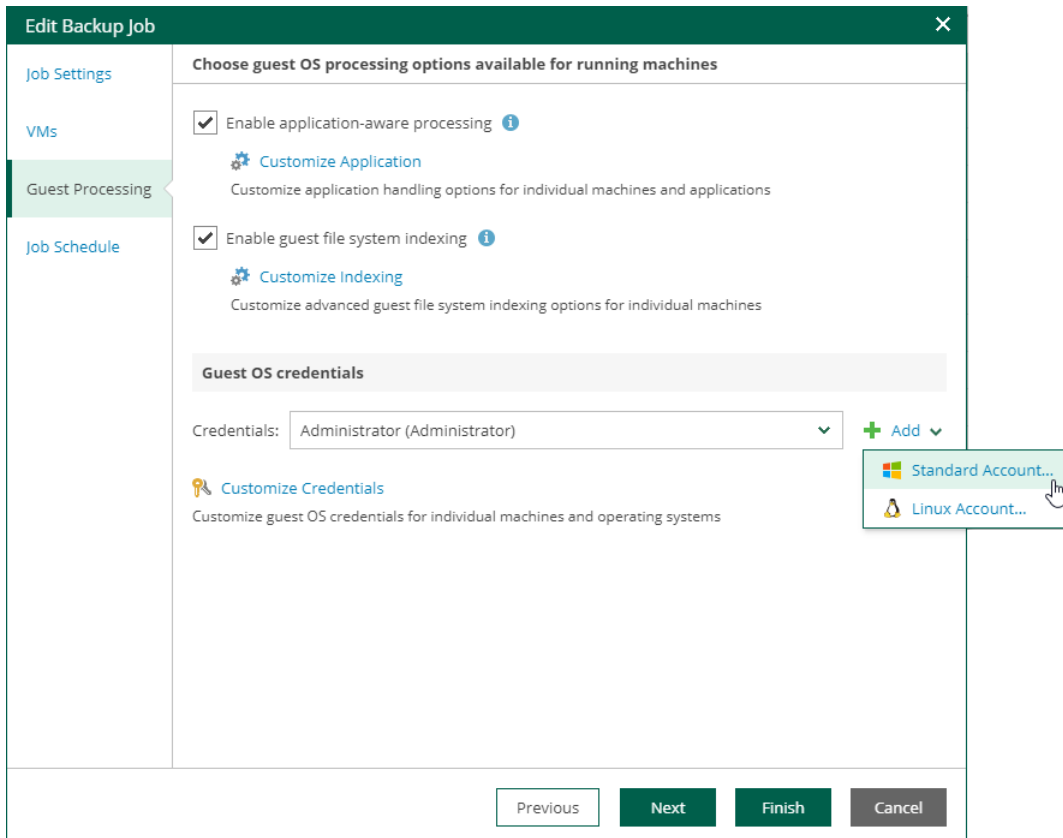


4. Click **OK** to save the settings and close the window.

Guest OS Credentials

If you specify guest OS credentials, Veeam Backup & Replication deploys a runtime process on the VM guest OS to coordinate guest processing activities. The process runs only during guest processing and is stopped immediately after the processing is finished.

If you have Management Agent installed on a Linux VM, you have an option to use it for coordinating guest processing activities. In this case, guest OS credentials are not stored in the configuration database, which makes using Management Agent a more secure option. For more information, see the [Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.



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, you can choose one of the following options:
 - If Management Agent is installed on the VM, you can select the **Use management agent** option.
 - If Management Agent is not installed on the VM, 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.

- i. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

- ii. 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.

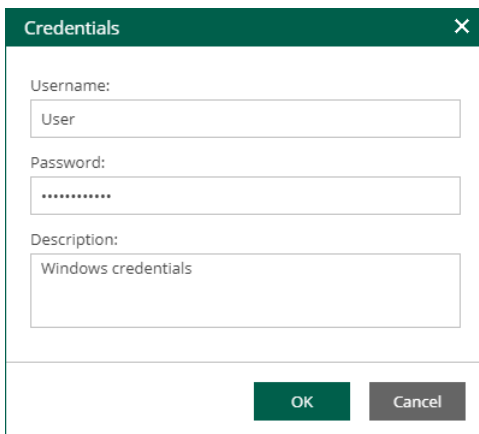
- iii. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password 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.



The screenshot shows a 'Credentials' dialog box with the following fields and values:

- Username: User
- Password:
- Description: Windows credentials

Buttons: OK, Cancel

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

The screenshot shows a dialog box titled "Linux Credentials" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Username:** A text box containing "Administrator".
- Password:** A password field with masked characters (dots).
- Private key is required for this connection
- Private Key:** A text box containing "key01.ppk" and a "Browse..." button to the right.
- Passphrase:** A password field with masked characters (dots).
- SSH port:** A dropdown menu showing "22".
- Non-root account** section (shaded background):
 - Elevate specified account to root
 - Add account to the sudoers file automatically
 - Use "su" if "sudo" fails
 - Root password:** A password field with masked characters (dots).
- Description:** A text area containing "Linux account for srv12".

At the bottom right, there are two buttons: "OK" (green) and "Cancel" (grey).

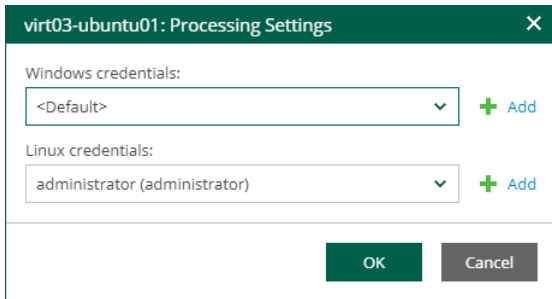
Special Credentials for Machine

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 [Schedule 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.

Edit Backup Job

Job Settings

VMs

Guest Processing

Job Schedule

Specify the job scheduling options

Run the job automatically:

Daily at this time:
08:00 pm Everyday Days...

Monthly at:
08:00 am Fourth Saturday Months...

Periodically every:
12 Hours Schedule...

After this job:
Backup Job 2

Automatic retry

Retry failed machine processing: 3 times
Wait before each attempt for: 10 minutes

Backup window

Terminate job if it gets out of allowed backup window Window...

Previous Next Finish Cancel

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.

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.

Select Period

AM 12 1 2 3 4 5 6 7 8 9 10 11 12 PM 1 2 3 4 5 6 7 8 9 10 11 12

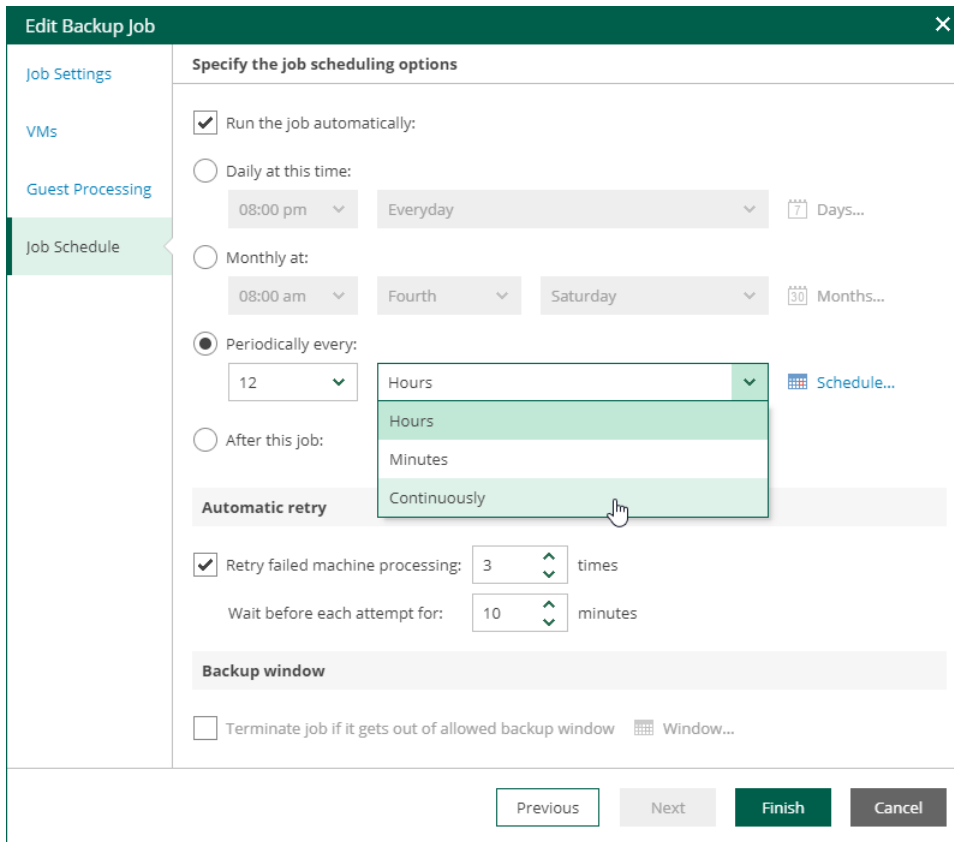
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Select: Denied Permitted [Deny All](#) [Permit All](#)

Start time within an hour: 0 min

OK Cancel

- 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

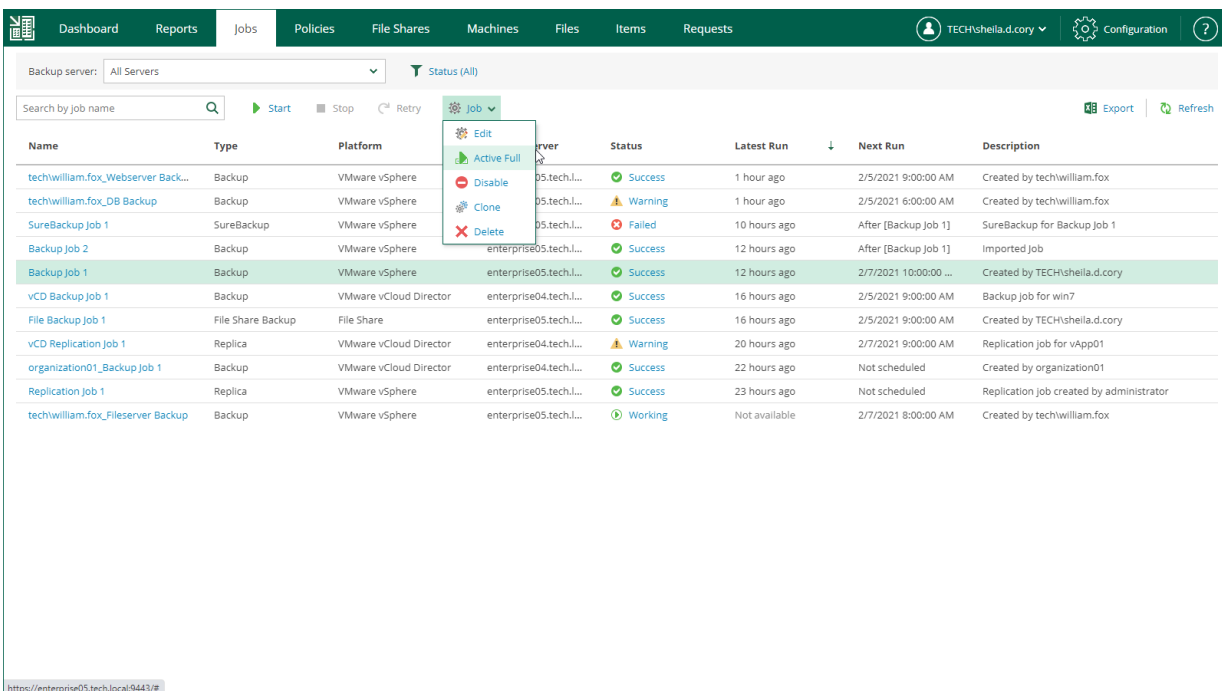
You can create an ad-hoc full backup – active full backup, and add it to the backup chain in the backup repository. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain in the backup 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**.



The screenshot shows the Veeam Backup Enterprise Manager interface. The 'Jobs' tab is active, displaying a table of backup jobs. A context menu is open over the 'Backup Job 1' row, with the 'Active Full' option selected. The table columns include Name, Type, Platform, Server, Status, Latest Run, Next Run, and Description.

Name	Type	Platform	Server	Status	Latest Run	Next Run	Description
techwilliam.fox_Webserver Back...	Backup	VMware vSphere	05.tech.l...	Success	1 hour ago	2/5/2021 9:00:00 AM	Created by techwilliam.fox
techwilliam.fox_DB Backup	Backup	VMware vSphere	05.tech.l...	Warning	1 hour ago	2/5/2021 6:00:00 AM	Created by techwilliam.fox
SureBackup Job 1	SureBackup	VMware vSphere	05.tech.l...	Failed	10 hours ago	After [Backup Job 1]	SureBackup for Backup Job 1
Backup Job 2	Backup	VMware vSphere	enterprise05.tech.l...	Success	12 hours ago	After [Backup Job 1]	Imported job
Backup Job 1	Backup	VMware vSphere	enterprise05.tech.l...	Success	12 hours ago	2/7/2021 10:00:00 ...	Created by TECHHsheila.d.cory
vCD Backup Job 1	Backup	VMware vCloud Director	enterprise04.tech.l...	Success	16 hours ago	2/5/2021 9:00:00 AM	Backup job for win7
File Backup Job 1	File Share Backup	File Share	enterprise05.tech.l...	Success	16 hours ago	2/5/2021 9:00:00 AM	Created by TECHHsheila.d.cory
vCD Replication Job 1	Replica	VMware vCloud Director	enterprise04.tech.l...	Warning	20 hours ago	2/7/2021 9:00:00 AM	Replication job for vApp01
organization01_Backup Job 1	Backup	VMware vCloud Director	enterprise04.tech.l...	Success	22 hours ago	Not scheduled	Created by organization01
Replication Job 1	Replica	VMware vSphere	enterprise05.tech.l...	Success	23 hours ago	Not scheduled	Replication job created by administrator
techwilliam.fox_Fileserver Backup	Backup	VMware vSphere	enterprise05.tech.l...	Working	Not available	2/7/2021 8:00:00 AM	Created by techwilliam.fox

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 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.

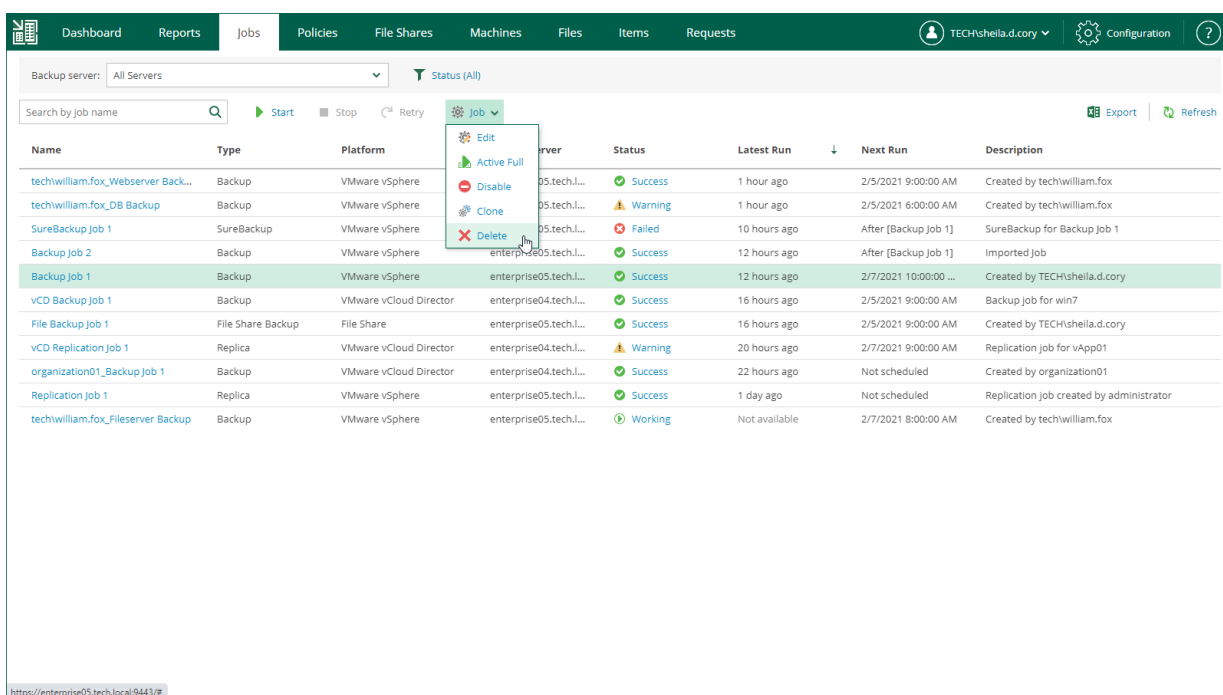
Deleting Jobs

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.

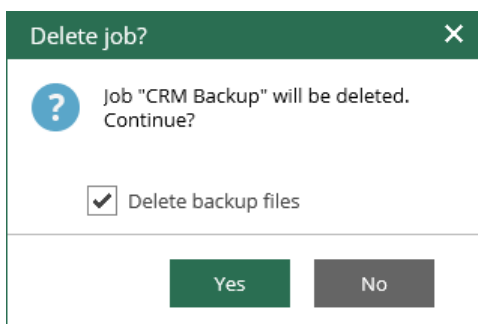
If you have Veeam backup servers of earlier versions added to Enterprise Manager, jobs managed by these servers cannot be deleted using Enterprise Manager.

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** checkbox 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. Veeam Backup Enterprise Manager displays CDP policies that process VMware vSphere or VMware Cloud Director objects.

Users with the Portal Administrator role can view, disable and enable, edit and delete CDP policies. Users with the Portal User role can only view 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 CDP policies, open the **Policies** tab.

Each policy in the list is described with the following data:

- **Name** – policy name
- **Status** – current policy status
- **SLA** – percentage of sessions completed within the specified RPO
- **RPO** – recovery point objective, that is, how often to create short-term restore points
- **Max delay** – difference between the configured RPO and time required to transfer and save data
- **Target** – target host
- **Platform** – VMware vSphere or VMware Cloud Director
- **Description** – 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.

The screenshot displays the 'Policies' section of the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\sheila.d.cory'. The 'Backup server' is set to 'All Servers' and the status is 'Status (All)'. A search bar is available for job names. The main content area shows a table of policies:

Name	Status	SLA	RPO	Max delay	Target	Platform	Description
Cloud Director CDP Policy	Syncing	100%	00:30	0 seconds	Repl-Org.VDC	Cloud Director	Not available
CDP Policy for Servers	Syncing	100%	00:30	0 seconds	prgtwex02-virt.tech...	VMWare	Not available

At the bottom left, the URL is <https://enterprise04.tech.local:9443/index.aspx#policies>.

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**.

Name	Status	SLA	RPO	Max delay	Target	Platform	Description
Cloud Director CDP Policy	Disabled	100%	00:30	0 seconds	Repl-Org;VDC	Cloud Director	Not available
CDP Policy for Servers	Syncing	100%	00:30	0 seconds	prgtwex02-virt.tech...	VMWare	Not available

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 added 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

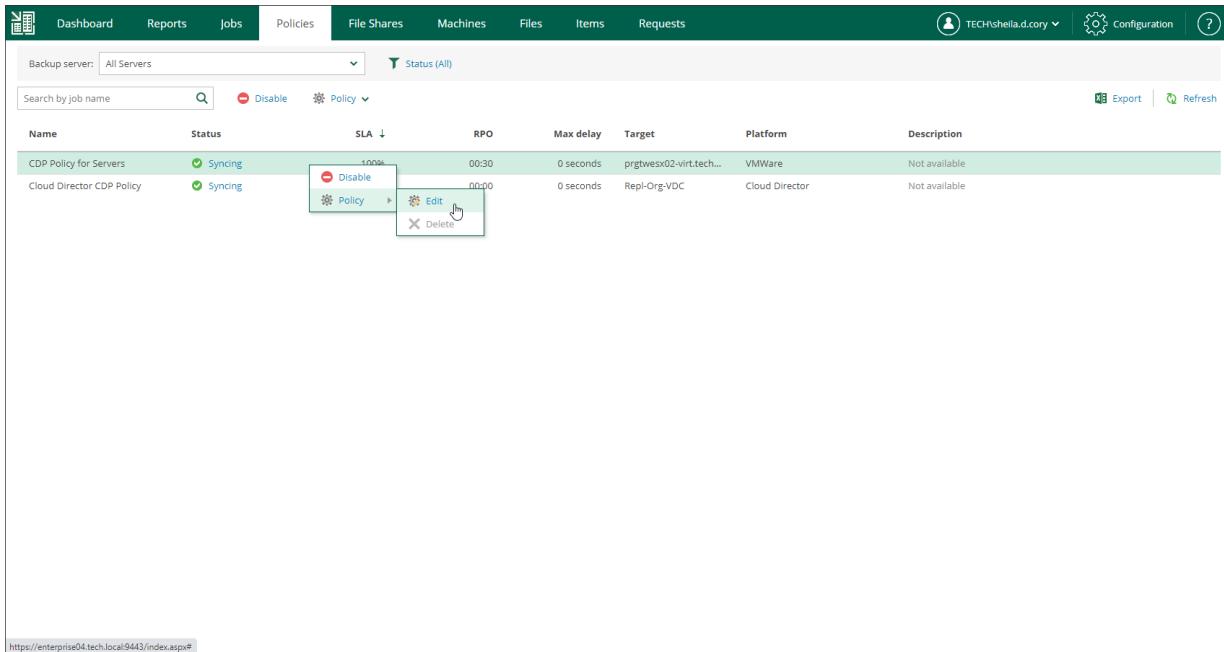
To edit a CDP policy, use the **Edit Policy** wizard.

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:

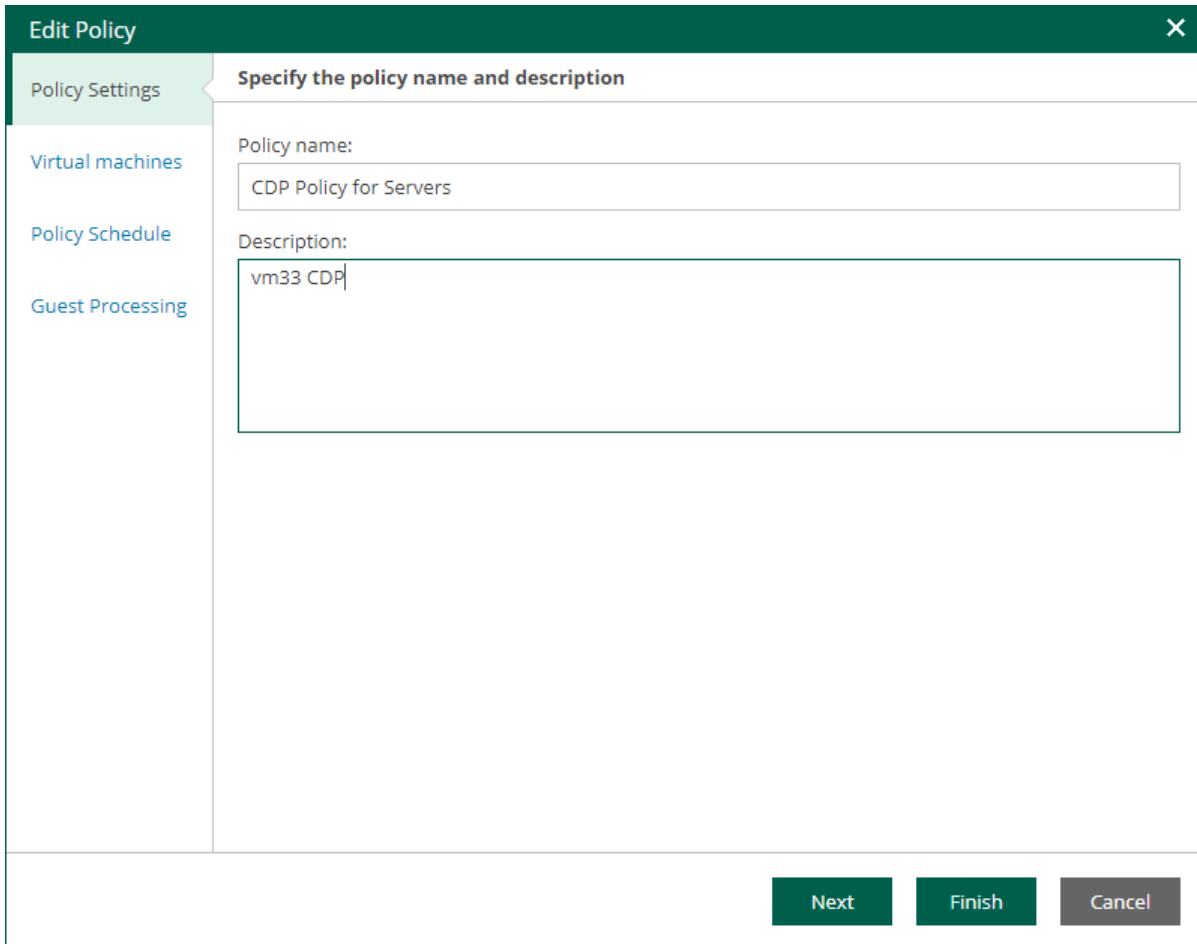
1. Open the **Policies** tab and select the necessary policy from the list.
2. On the toolbar, click **Policy** and select **Edit**.



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.



The screenshot shows a dialog box titled "Edit Policy" with a close button (X) in the top right corner. The dialog is divided into a left sidebar and a main content area. The sidebar contains four menu items: "Policy Settings" (highlighted in green), "Virtual machines", "Policy Schedule", and "Guest Processing". The main content area is titled "Specify the policy name and description" and contains two text input fields. The first field is labeled "Policy name:" and contains the text "CDP Policy for Servers". The second field is labeled "Description:" and contains the text "vm33 CDP". At the bottom right of the dialog, there are three buttons: "Next" (green), "Finish" (green), and "Cancel" (grey).

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.

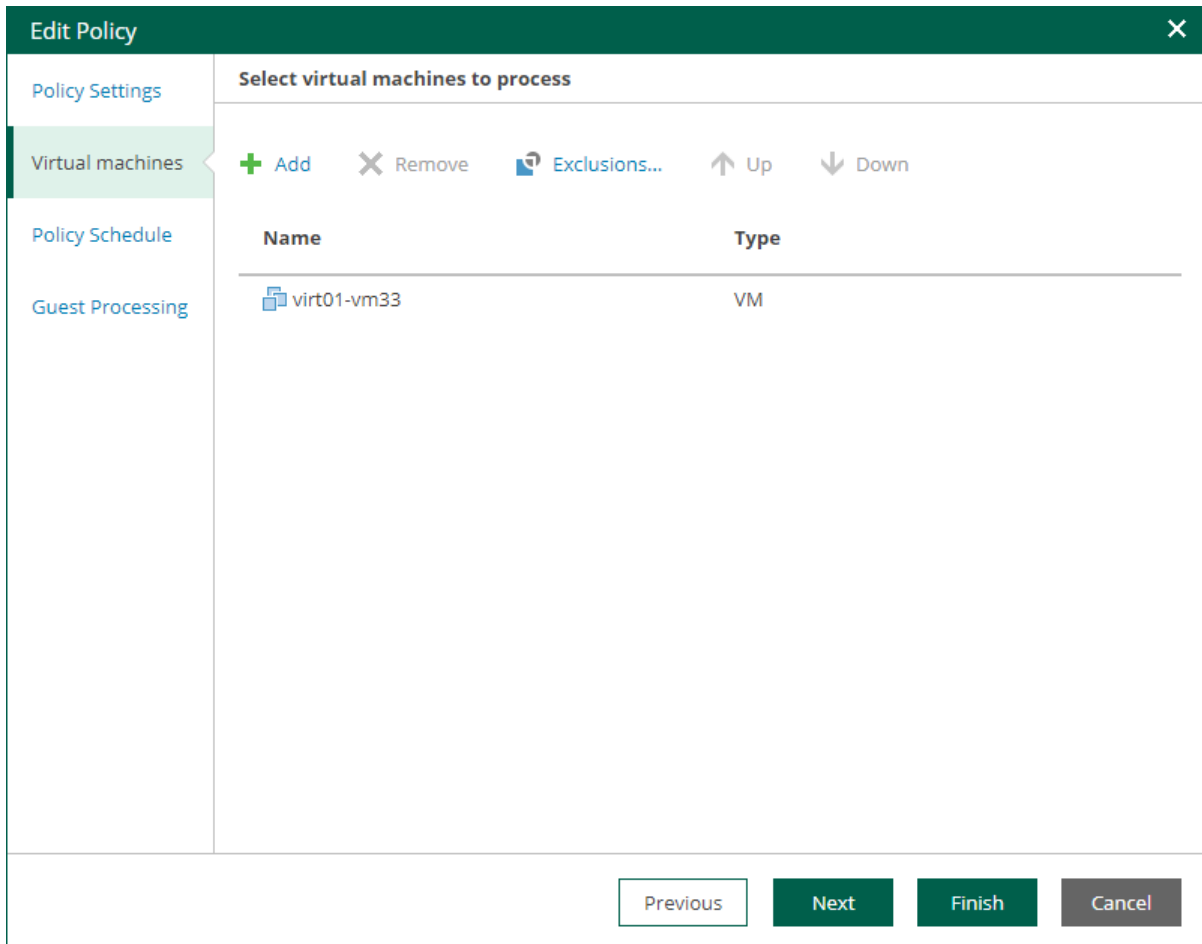
NOTE

For VMware Cloud Director CDP policies, you cannot add single VMs. You can manage only vApps and other Cloud Director containers. The scope depends on your Cloud Director access rights.

Adding VMs and VM containers

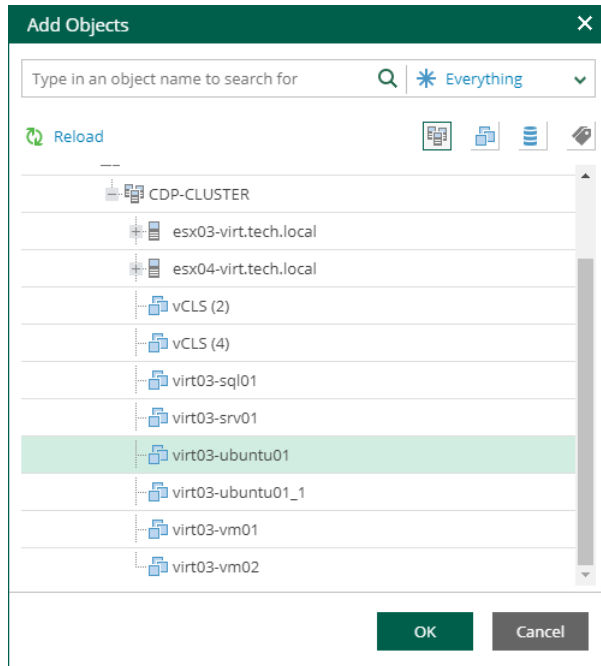
To add a VM or VM container:

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.

Edit Policy [Close]

Policy Settings

Virtual machines

Policy Schedule

Guest Processing

Specify the policy scheduling options

Recovery point objective:
30 [Up/Down] Seconds [Down] [Schedule...] [Reporting...]

RPO defines maximum acceptable data loss in case of the protected VM failure

Short-term retention

Enable point-in-time recovery within:
4 [Up/Down] Hours [Down]

Defines how far back you can go from the latest state for a point-in-time recovery

Long-term retention

Create additional restore points every:
8 [Up/Down] hours [Schedule...]

Keep these restore points for:
7 [Up/Down] days

Previous Next Finish Cancel

- b. To specify permitted and denied hours for the policy run, click **Schedule** on the right and use the timetable.

The screenshot shows a 'Time periods' dialog box with a 7-day grid. The grid has columns for hours 1-12 AM and 1-12 PM. The 'Denied' status is selected by default. The grid shows that hours 8-11 AM and 1-7 PM are denied on Monday through Friday, while all other hours are permitted. The 'Permitted' status is selected for all other hours. The dialog includes 'Deny All' and 'Permit All' buttons, and 'OK' and 'Cancel' buttons at the bottom.

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.

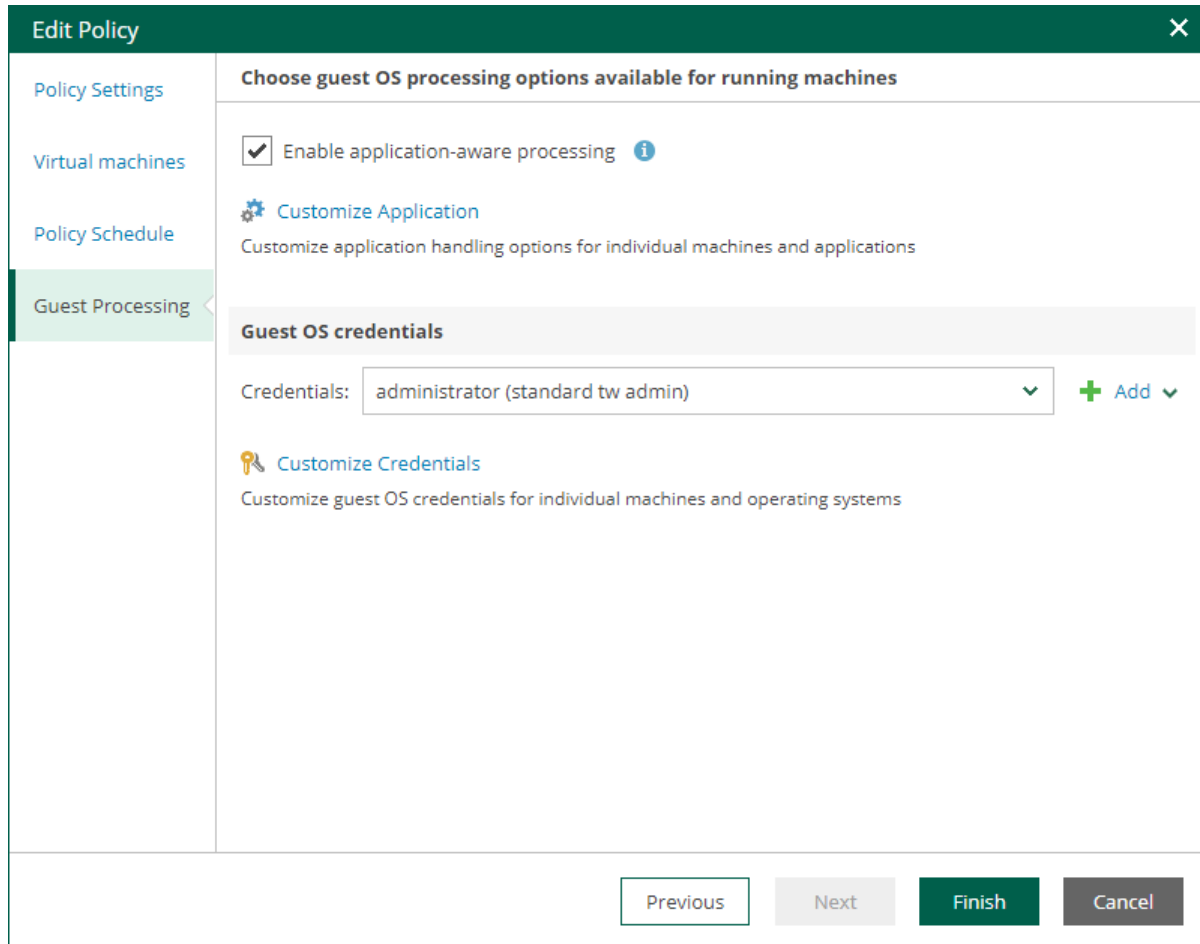
- c. To specify time periods when Veeam Backup & Replication must create application-consistent and crash-consistent long-term restore points, click **VSS**. In the **Time periods** window, select the necessary time area and click **Crash-consistent** or **Application-consistent**. By default, Veeam 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.

The screenshot shows the 'Time periods' dialog box. At the top, there is a title bar with 'Time periods' and a close button. Below the title bar, there is a grid representing the days of the week (Sunday to Saturday) and the hours of the day (12 to 12). The grid is divided into AM and PM sections. The 'Application-consistent' radio button is selected. Below the grid, there is a 'Start time within an hour' field with a dropdown menu set to '15' and a 'min' label. At the bottom right, there are 'OK' and 'Cancel' buttons.

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:

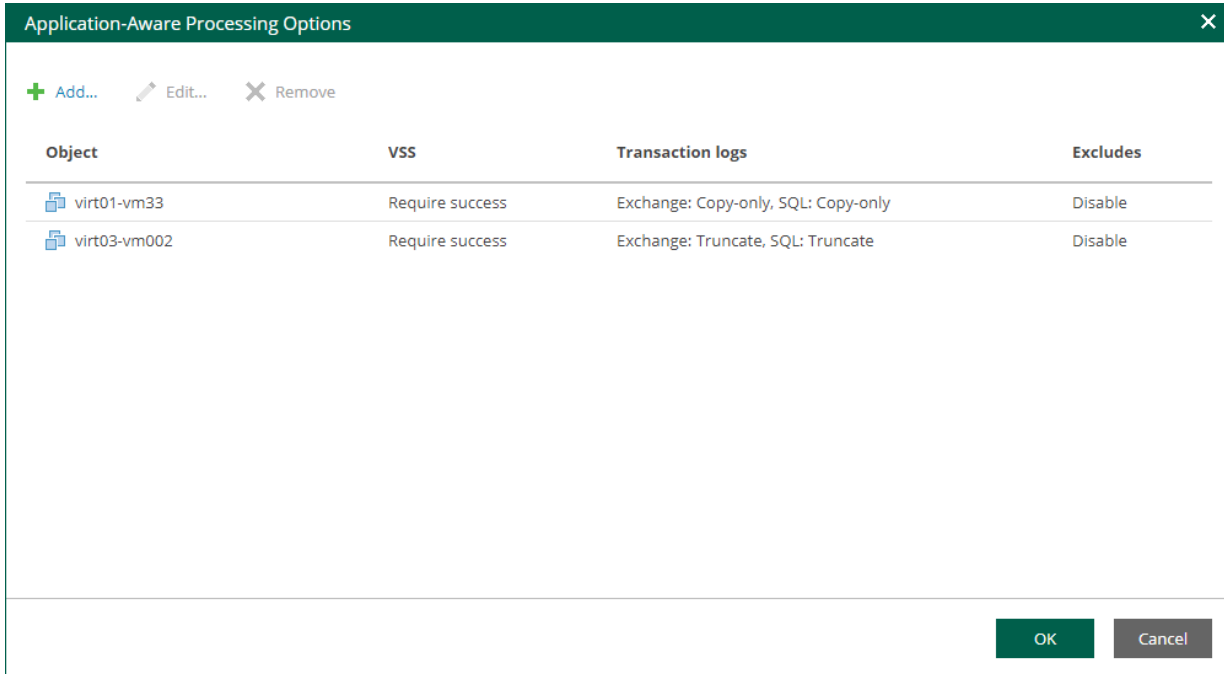
1. Select the **Enable application-aware processing** check box.
2. Click the **Customize Application** link.
3. To define custom settings for a machine in the list, select it and click **Edit**.

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](#)
- [Microsoft SQL Server Transaction Log Settings](#)
- [Oracle Archived Log Settings](#)



General Settings

On the **General** tab, you can specify general application-aware processing settings.

1. In the **Applications** section, select the option that corresponds to your transactionally-consistent backup creation scenario.
 - Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the CDP replication if an error occurs.
 - Select **Try application processing, but ignore failures** if you want to continue the CDP replication 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.
2. [For Microsoft Exchange, Microsoft SQL Server, and Oracle] In the **Microsoft VSS** section, specify whether this 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 process transaction logs.

[For Microsoft Exchange] Transaction logs will be truncated after the CDP policy creates a long-term restore point. If the creation fails, the logs will remain untouched until the next start of the long-term restore point creation.

[For Microsoft SQL Server, Oracle] Specify settings for transaction log handling:

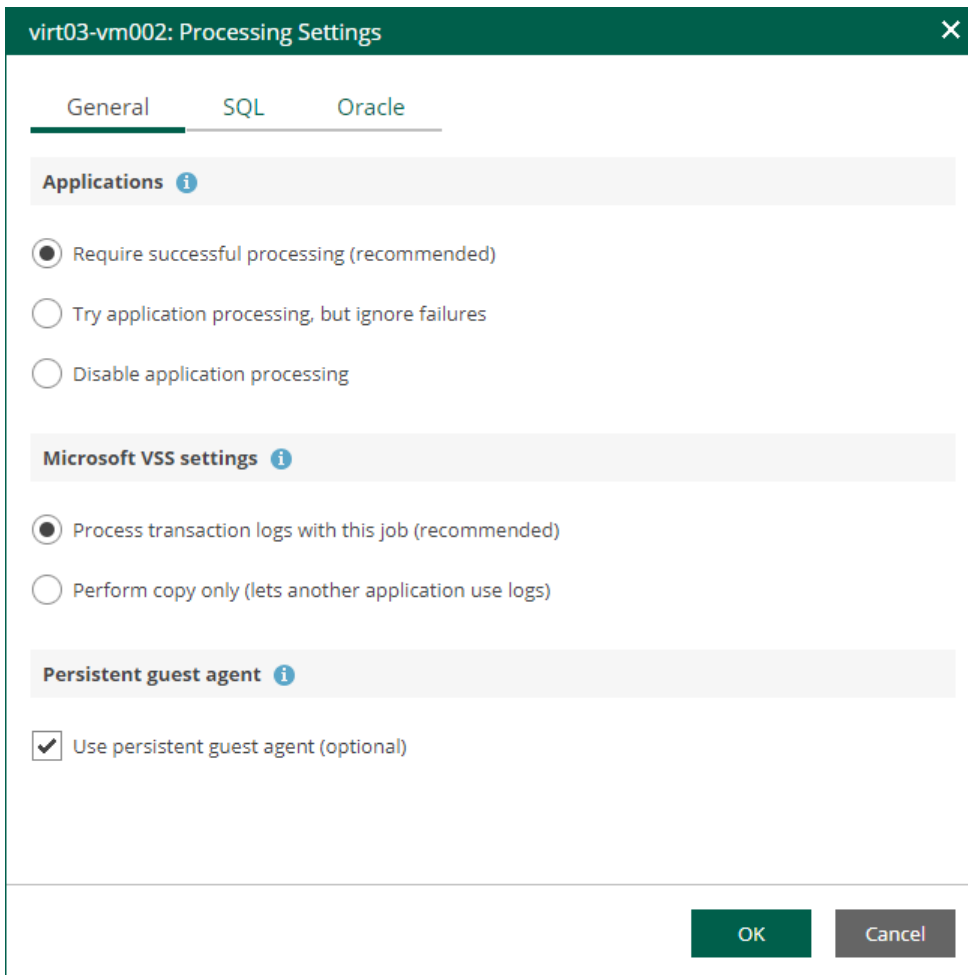
- For Microsoft SQL Server transaction log processing – on the **SQL** tab. For more information, see [Microsoft SQL Server Transaction Log Settings](#).
- For Oracle database archived logs processing – on the **Oracle** tab. For more information, see [Oracle Archived Log Settings](#).
- Select **Perform 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](#).

With this option selected, the **SQL**, **Oracle** and **PostgreSQL** tabs are not available.

3. In the **Persistent guest agent** section, specify if Veeam Backup & Replication must use persistent guest agents on the VM for application-aware processing.

By default, Veeam Backup & Replication uses non-persistent runtime components. Veeam Backup & Replication deploys runtime components on each protected VM when the backup job starts, and removes the runtime components as soon as the backup job finishes.

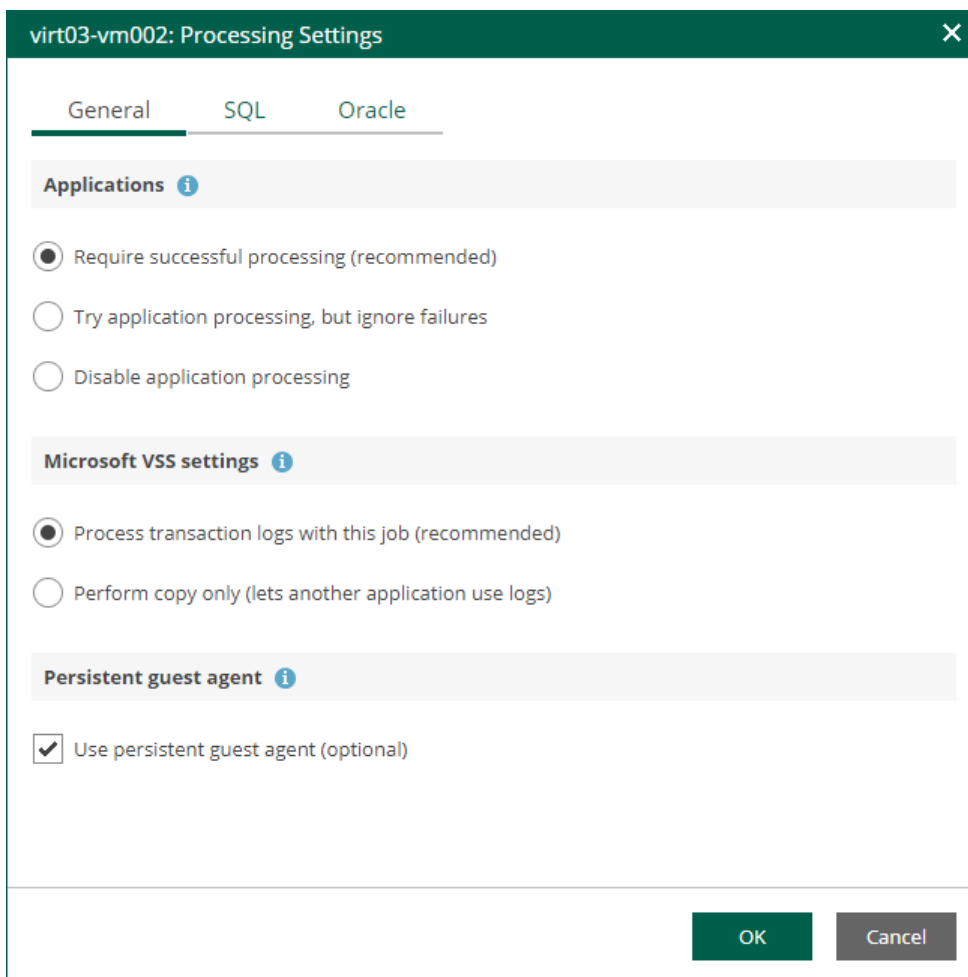
Select **Use persistent guest agent** to enable persistent agent components for guest processing. For more information, see the [Non-Persistent Runtime Components and Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.



Microsoft SQL Server Transaction Log Settings

If you replicate a Microsoft SQL Server VM, you can specify how Veeam Backup & Replication must process transaction logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Microsoft SQL Server VM from the list and click **Edit**.
4. On the **General** tab of the **VM Processing Settings** window, make sure the following options are selected:
 - In the **Applications** section, either the **Require successful processing** or **Try application processing, but ignore failures** option must be selected.
 - In the **Transaction logs processing** section, the **Process transaction logs with this job** option must be selected.



5. Open the **SQL** tab of the **VM Processing Settings** window.

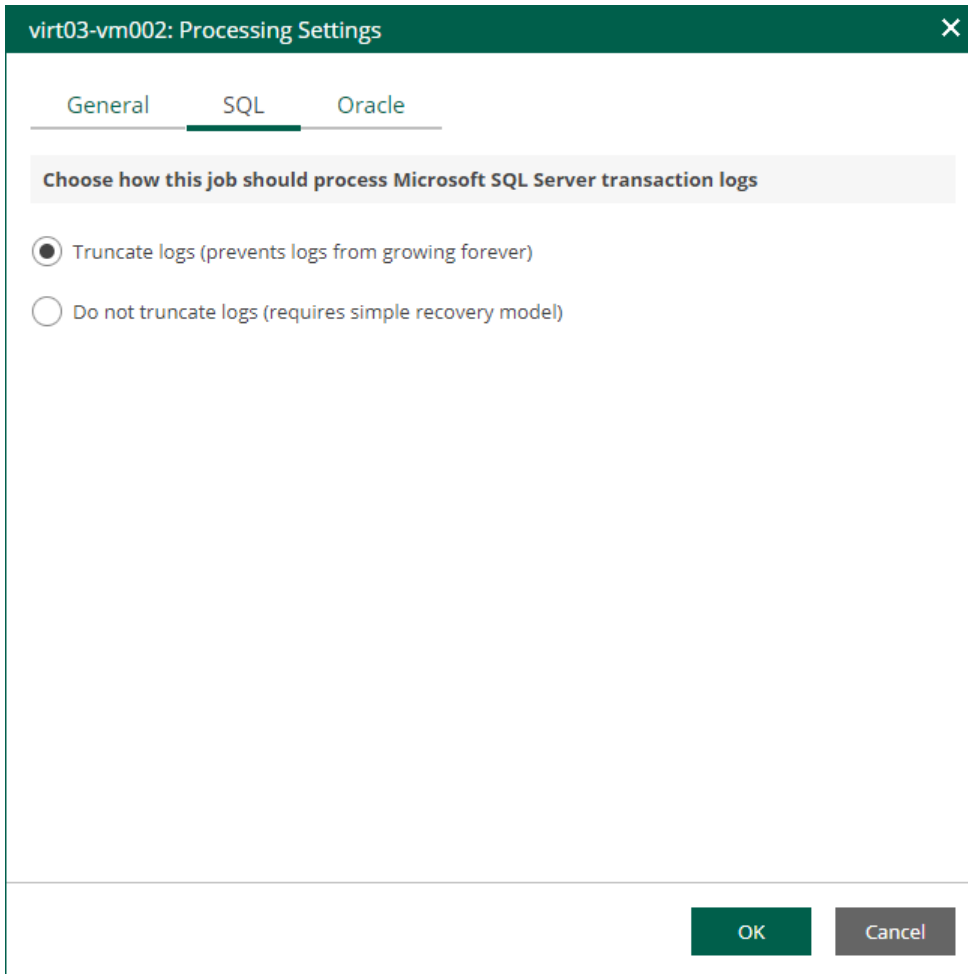
6. Specify how Veeam Backup & Replication will process Microsoft SQL Server transaction logs.

- Select **Truncate logs** to truncate transaction logs after the CDP policy creates a long-term restore point.

In this case, transaction logs will be truncated after the CDP policy creates a long-term restore point. If the creation fails, the logs will remain untouched until the next start of the long-term restore point creation.

- Select **Do not truncate logs** to preserve transaction logs.

This option is recommended if you use another tool to perform VM guest-level replication, and this tool maintains consistency of the database state.

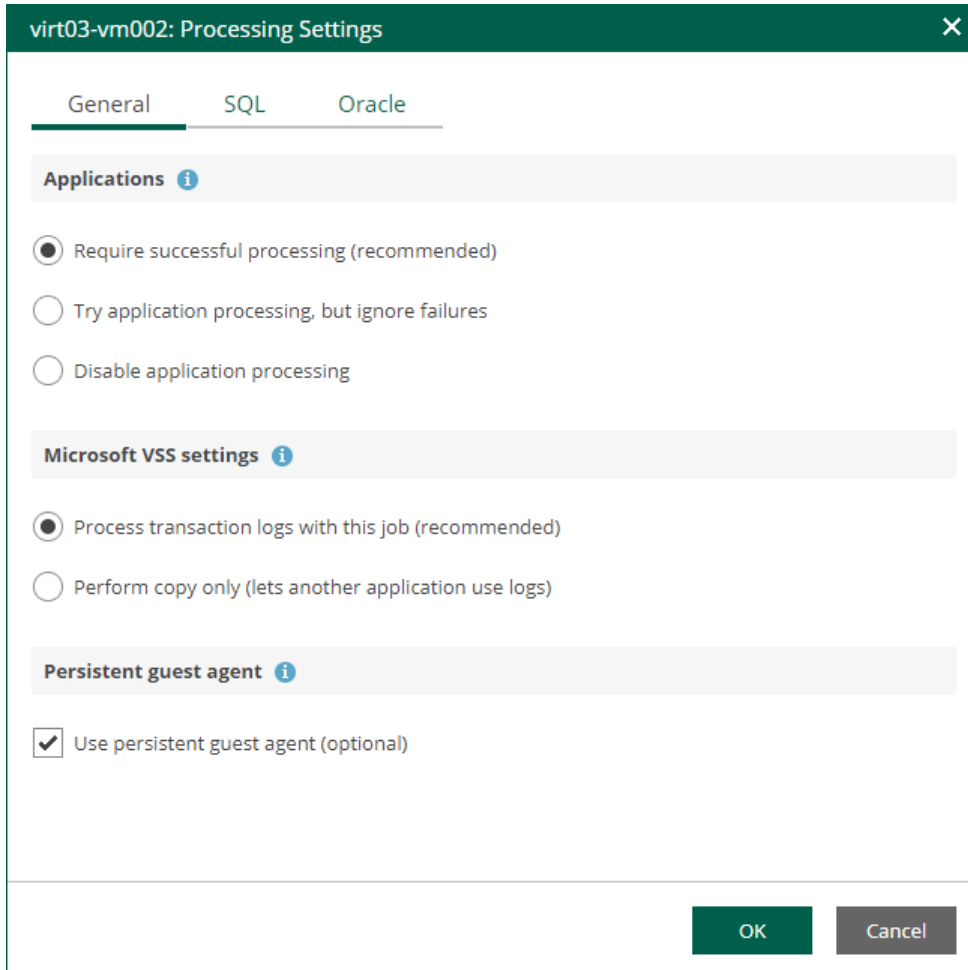


Oracle Archived Log Settings

If you replicate a VM where Oracle Database is deployed, you can specify how Veeam Backup & Replication must process archived redo logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Oracle VM from the list and click **Edit**.

4. On the **General** tab of the **VM Processing Settings** window, make sure the following options are selected:
 - In the **Applications** section, either the **Require successful processing** or **Try application processing, but ignore failures** option must be selected.
 - In the **Transaction logs processing** section, the **Process transaction logs with this job** option must be selected.



5. On the **Oracle** tab of the **VM Processing Settings** window, specify log processing settings.
 - a. Specify a user account that will connect to the Oracle database.
 - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.
 - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

Make sure the specified account has sufficient rights. For details, see the [Permissions](#) section of the Veeam Explorers User Guide.
 - b. Specify how Veeam Backup & Replication must process archived redo logs on the Oracle VM.
 - Select **Do not delete archived logs** to preserve archived redo logs on the original Oracle server.

Select this option for databases in the NOARCHIVELOG mode. If the database is in the ARCHIVELOG mode, archived logs on the VM guest OS may grow large and consume all disk space. In this case, database administrators must take care of archived logs themselves.

- Select **Delete logs older than <N> hours / Delete logs over <N> GB** to delete archived logs that are older than <N> hours or larger than <N> GB. The log size threshold refers not to the total size of all logs for all databases, but to the log size of each database on the selected Oracle VM.

Transaction logs will be deleted using Oracle Call Interface after the CDP policy creates a long-term restore point. If the creation fails, the logs will remain untouched until the next start of the long-term restore point creation.

virt03-vm002: Processing Settings

General SQL Oracle

Choose how this job should process Oracle archived logs

Specify Oracle account with SYSDBA privileges:

Use guest credentials + Add

Do not delete archived logs

Delete logs older than: 24 hours

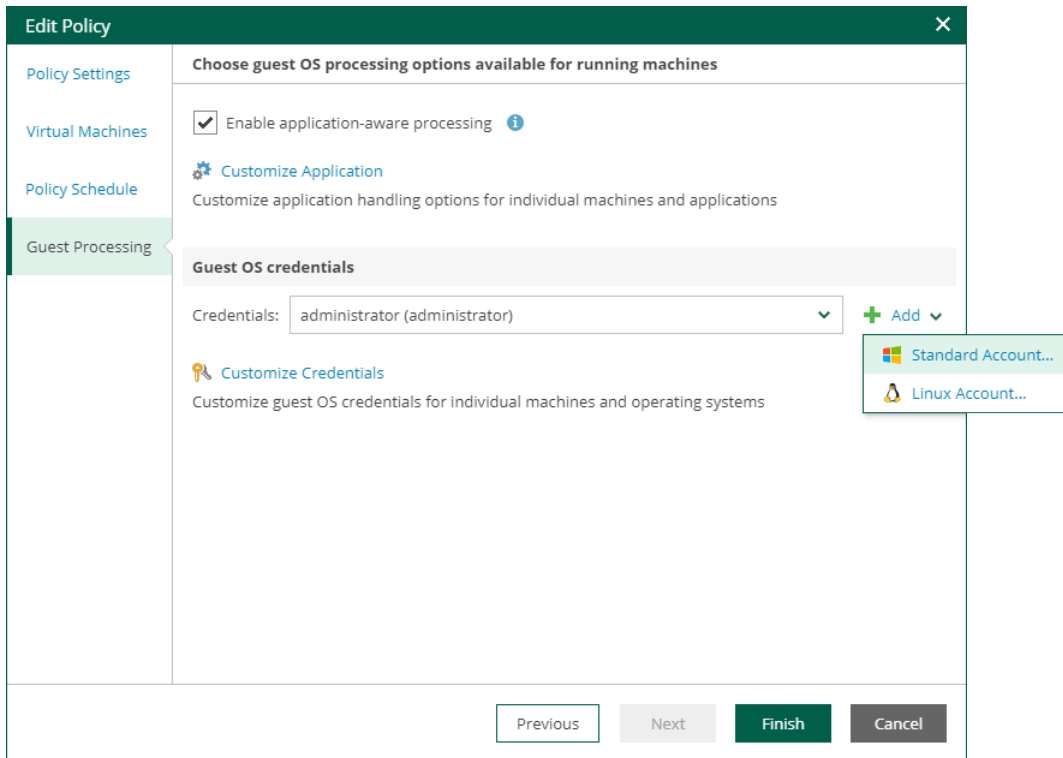
Delete logs over: 10 GB

OK Cancel

Guest OS Credentials

If you specify guest OS credentials, Veeam Backup & Replication deploys a runtime process on the VM guest OS to coordinate guest processing activities. The process runs only during guest processing and is stopped immediately after the processing is finished.

If you have Management Agent installed on a Linux VM, you have an option to use it for coordinating guest processing activities. In this case, guest OS credentials are not stored in the configuration database, which makes using Management Agent a more secure option. For more information, see the [Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.



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, you can choose one of the following options:
 - If Management Agent is installed on the VM, you can select the **Use management agent** option.
 - If Management Agent is not installed on the VM, 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.

- i. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

- ii. 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.

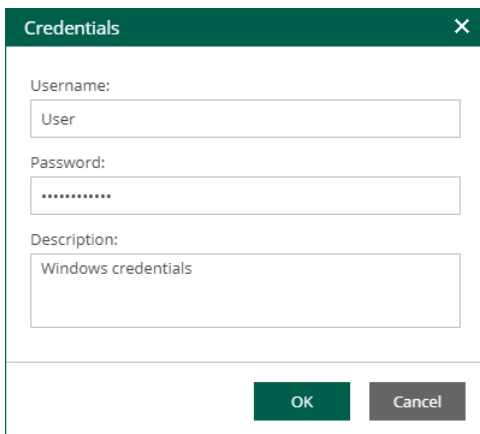
- iii. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password 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.



The screenshot shows a 'Credentials' dialog box with the following fields and values:

- Username: User
- Password:
- Description: Windows credentials

Buttons: OK, Cancel

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

Linux Credentials

Username: Administrator

Password:

Private key is required for this connection

Private Key: key01.ppk [Browse...](#)

Passphrase:

SSH port: 22

Non-root account

Elevate specified account to root

Add account to the sudoers file automatically

Use "su" if "sudo" fails

Root password:

Description: Linux account for srv12

OK Cancel

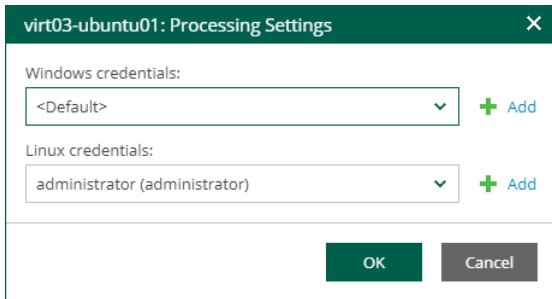
Special Credentials for Machine

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.

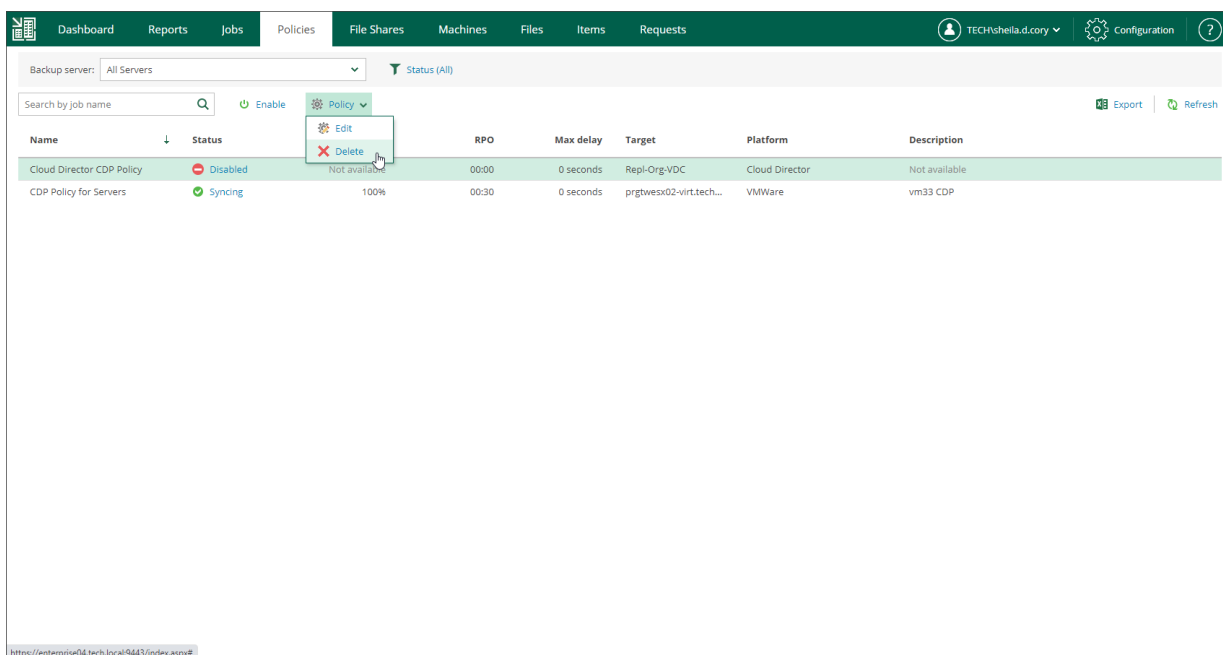
Deleting Policies

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.

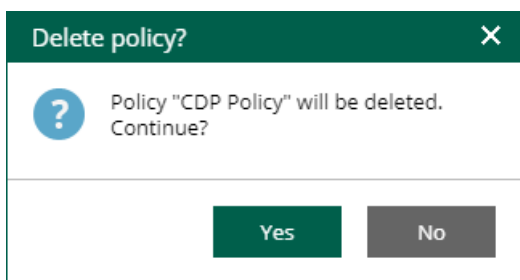
Before you delete a CDP policy, you must disable it.

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.



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

In the Enterprise Plus edition of Veeam Backup & Replication, users with the Portal Administrator role can customize a restore scope of other users (list of objects the user can recover). In other editions, the restore scope 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 Permissions for File and Application Item 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.

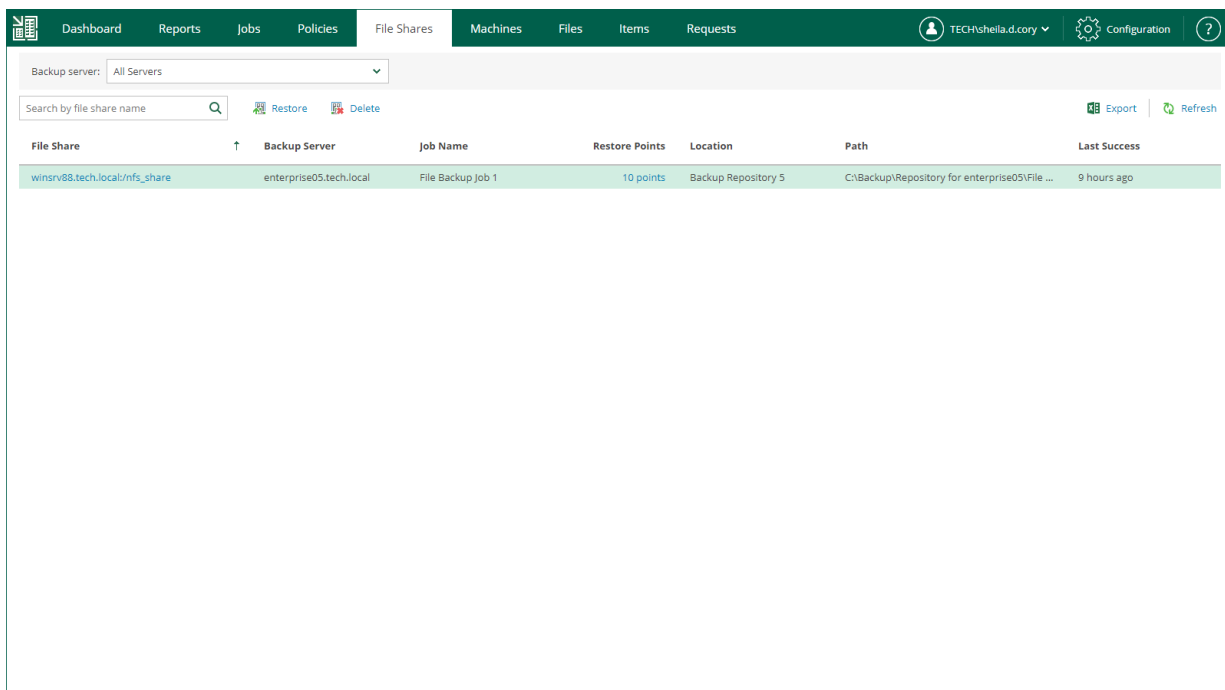
You can search for file shares in one of the following ways:

- 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.





File Share	Backup Server	Job Name	Restore Points	Location	Path	Last Success
winsrv88.tech.local/mfs_share	enterprise05.tech.local	File Backup Job 1	10 points	Backup Repository 5	C:\Backup\Repository for enterprise05\File ...	9 hours ago

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.

winsrv88.tech.local:/nfs_share: Restore Points ✕

 Export |  Refresh

Restore Point	Type	Status
2/9/2021 09:00:54 am	Backup	✓ Success
2/9/2021 02:41:17 am	Backup	✓ Success
2/8/2021 09:00:47 am	Backup	✓ Success
2/7/2021 09:00:38 am	Backup	✓ Success
2/6/2021 09:00:41 am	Backup	✓ Success
2/5/2021 09:00:42 am	Backup	✓ Success
2/5/2021 03:41:54 am	Backup	✓ Success
2/5/2021 03:31:28 am	Backup	✓ Success
2/5/2021 03:17:30 am	Backup	✓ Success
2/4/2021 09:00:36 am	Backup	✓ Success

Close

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

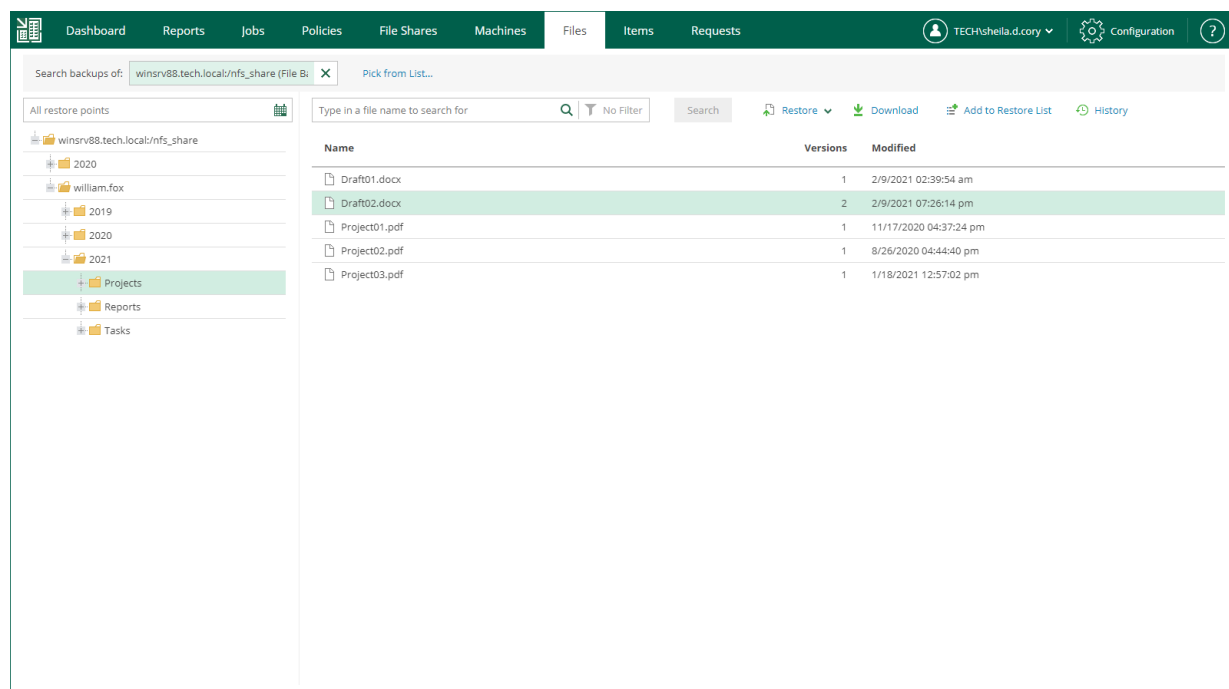
You can browse file share backups for backed-up files. Note that with the file browsing functionality, you can browse for files in the selected file share backup only.

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:

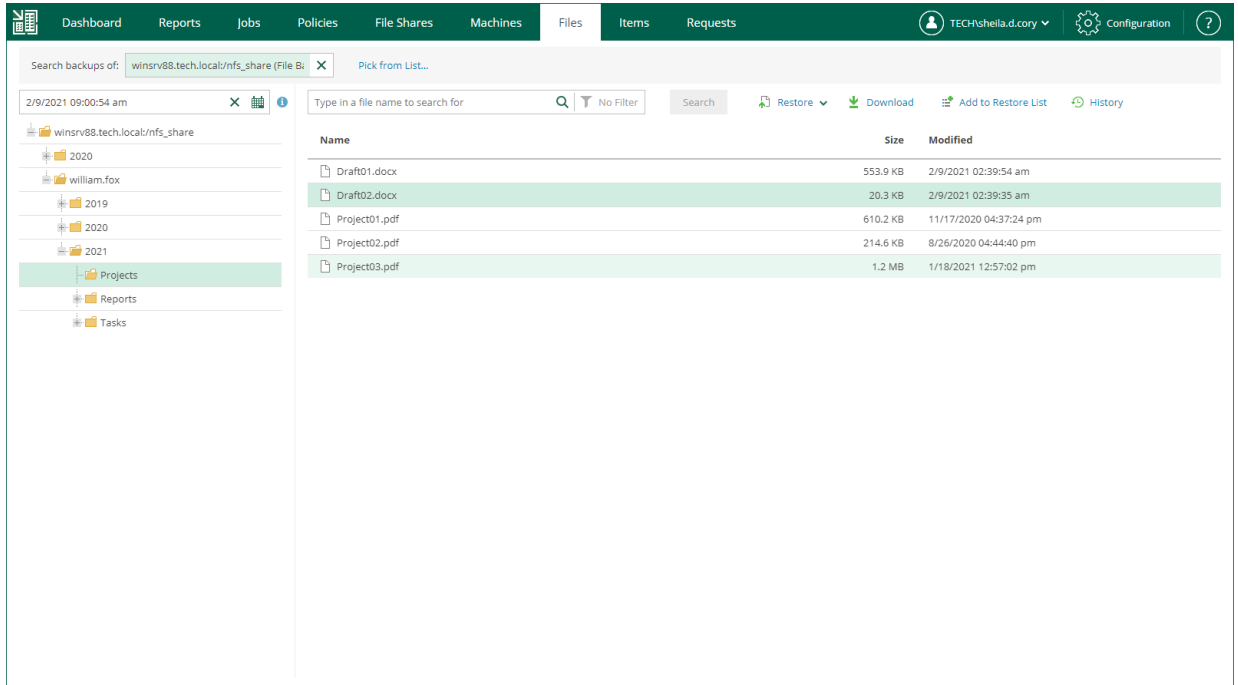
1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a file share whose files you want to browse or click the **Pick from List** link and select the necessary file share in the **Select Object** window.
3. Click **Mount**.
4. Wait while Veeam Backup & Replication mounts 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 [Restoring Specific Files and Folders](#).



- 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 [Restoring Specific Files and Folders](#).



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.

File Share Data Recovery

You can restore data previously backed up with file share backup jobs. You can restore the following data:

- SMB file share files and folders
- NFS file share files and folders
- Files and folders of a managed Microsoft Windows server
- Files and folders of a managed Linux server

Veeam Backup Enterprise Manager offers the following recovery options:

- [Instant file share recovery](#) allows you to recover a point-in-time file share state.
- [Restore of files and folders](#) allows you to select files and folders to restore to one of the restore points.

Instant File Share Recovery

Instant file share recovery allows you to recover data from backups of the following file shares:

- SMB file shares

For SMB file shares, you can mount a recovered file share, make changes to the file share (add, edit or remove files and folders), and migrate the file share to the production environment.

- NFS file shares

For NFS file shares, you can use the feature to publish a point-in-time file share state as a read-only SMB file share. This lets you instantly access all recovered files.

After you have performed instant file share recovery, you have to finalize it. For more information, see [Finalizing Instant File Share Recovery](#).

Performing Instant File Share Recovery

When you perform instant file share recovery using Veeam Backup Enterprise Manager, Veeam Backup & Replication publishes the recovered file share to the mount server associated with a backup repository that stores the file share backup. If you want to mount a recovered file share to another mount server, use the Veeam Backup & Replication console. For more information, see the [Performing Instant File Share Recovery](#) section of the Veeam Backup & Replication User Guide.

To perform instant file share recovery, use the **Instant File Share Recovery** wizard.

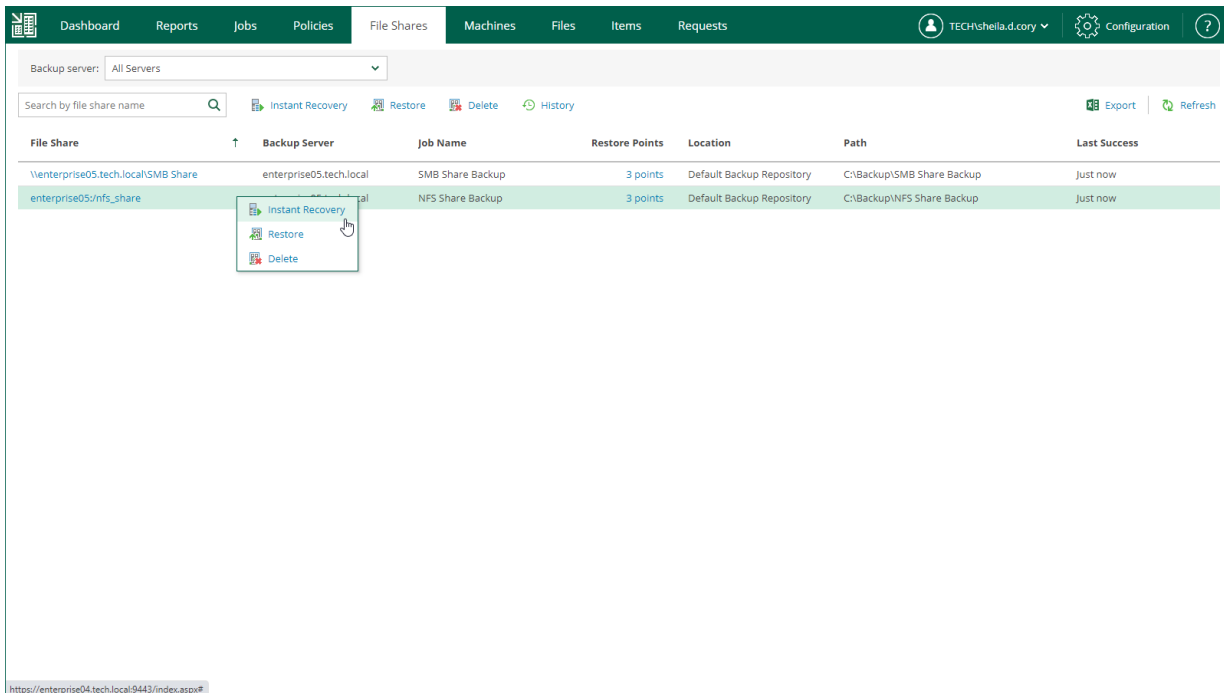
1. [Launch the Instant File Share Recovery wizard](#).
2. [Select a restore point](#).
3. [Specify access permissions](#).
4. [Review the recovery settings](#).

Step 1. Launch Instant File Share Recovery Wizard

To launch the **Instant File Share Recovery** wizard, do the following:

1. Open the **File Shares** tab and select a file share from the list.
2. On the toolbar, click **Instant Recovery**.

Alternatively, you can right-click a file share and select **Instant Recovery**.



Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a file share restore point from which you want to perform instant recovery.

Instant File Share Recovery [X]

Restore Point
Select the restore point for file share to be restored to.

Share name: enterprise05:/nfs_share

Backup Date	Type	Job Name
1/31/2023 09:36:14 pm		
1/31/2023 09:34:46 pm		
1/31/2023 09:24:36 pm		

Next Cancel

Step 3. Specify Access Permissions

At the **Access Permissions** step, you can specify the owner account and permissions for the file share.

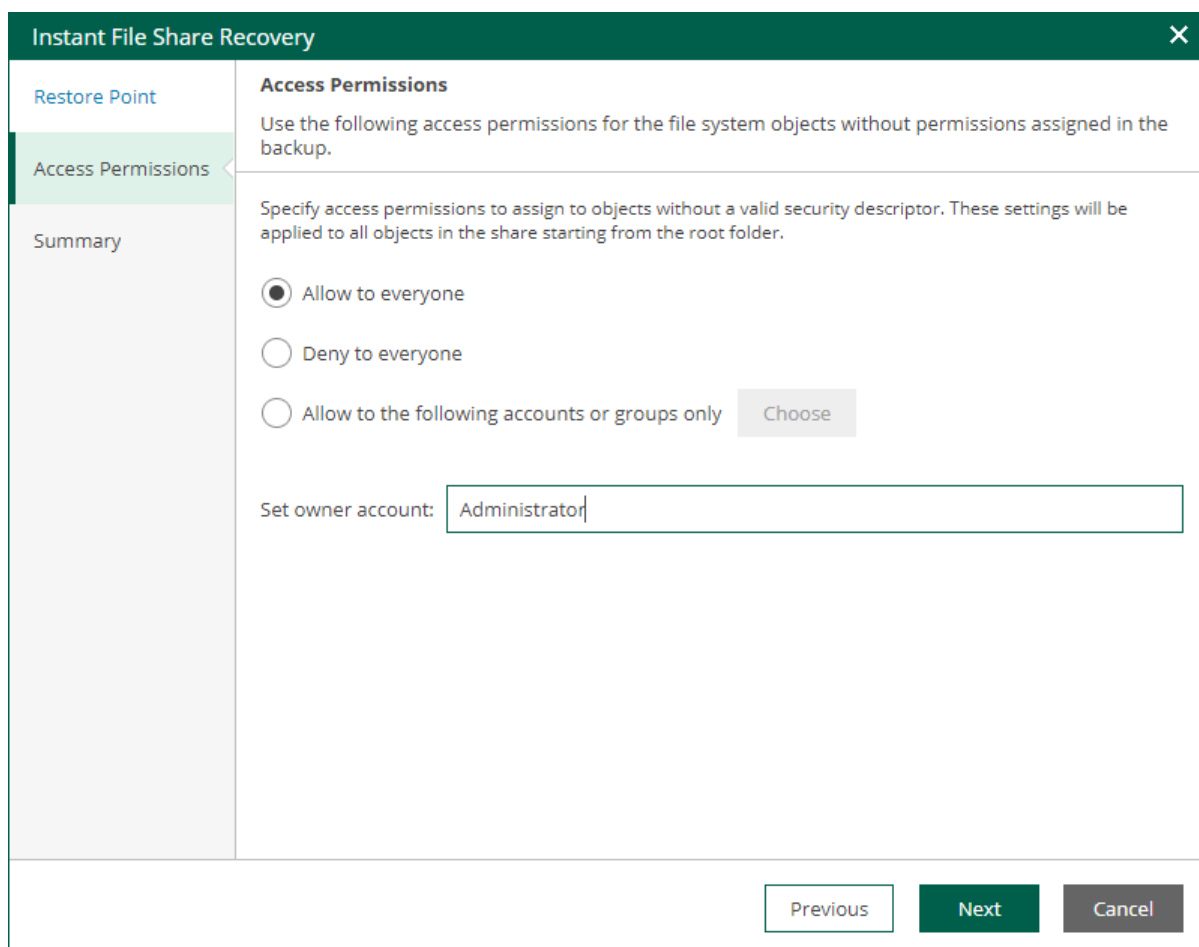
1. Configure access permissions for the file share. The following options are available:

- **Allow to everyone**
- **Deny to everyone**
- **Allow to the following accounts or groups only**

If you select this option, configure accounts and groups to which you want to grant permissions for accessing the file share:

- i. Next to the **Allow to the following accounts or groups only** option, click **Choose**.
- ii. In the **Accounts and Groups** window, click **Add** to add an account or group.
- iii. Specify a name of the account or group and click **OK**.
- iv. Add other accounts or groups if necessary. Use the **Remove** button to remove an account or group.

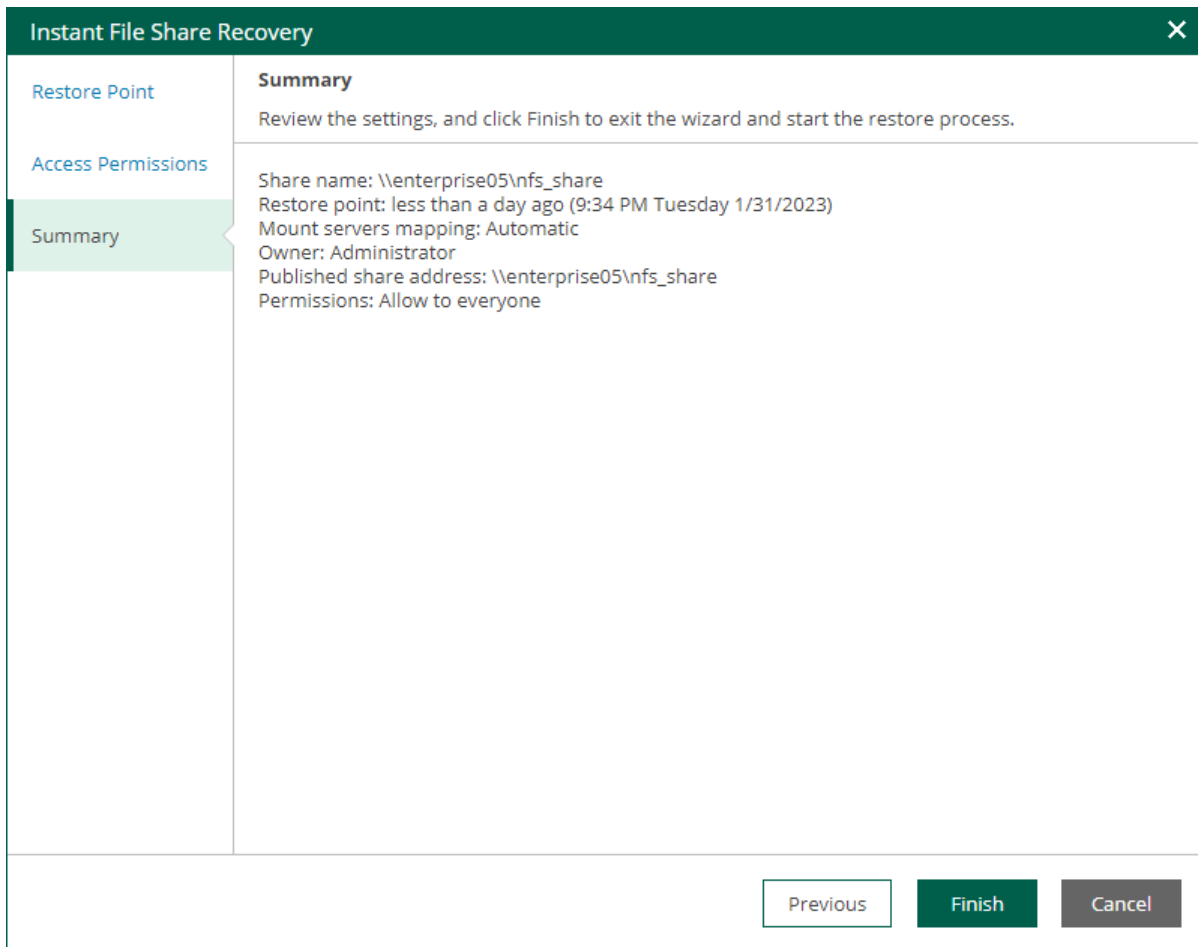
2. In the **Set owner account field**, specify the owner account for the file share.



The screenshot shows the 'Instant File Share Recovery' dialog box with the 'Access Permissions' tab selected. The dialog has a dark green header with a close button (X) in the top right corner. On the left, there is a sidebar with three tabs: 'Restore Point', 'Access Permissions' (which is highlighted in light green), and 'Summary'. The main content area is titled 'Access Permissions' and contains the following text: 'Use the following access permissions for the file system objects without permissions assigned in the backup.' Below this, there is a sub-section titled 'Specify access permissions to assign to objects without a valid security descriptor. These settings will be applied to all objects in the share starting from the root folder.' This section contains three radio button options: 'Allow to everyone' (which is selected), 'Deny to everyone', and 'Allow to the following accounts or groups only'. To the right of the third option is a grey 'Choose' button. Below the radio buttons is a text input field labeled 'Set owner account:' with the text 'Administrator' entered. At the bottom right of the dialog, there are three buttons: 'Previous' (light green), 'Next' (dark green), and 'Cancel' (grey).

Step 4. Review Recovery Settings

At the **Summary** step of the wizard, review the instant file share recovery settings and click **Finish**. Veeam Backup & Replication will publish the recovered file share to the mount server associated with a backup repository that stores the file share backup.



What You Do Next

After you have performed instant file share recovery, you have to finalize it. For more information, see [Finalizing Instant File Share Recovery](#).

Finalizing Instant File Share Recovery

After you have performed instant file share recovery, you have to finalize the process. You can migrate recovered file shares to the production environment or stop publishing.

- [For NFS file shares] When you perform instant recovery of an NFS file share, the file share is published as a read-only SMB file share that lets you instantly access all recovered files. After you finish working with the files, you must stop publishing the recovered file share.
- [For SMB file shares] When you perform instant recovery of an SMB file share, the published file share is available for reading and writing. After you finish working with the files, you must stop publishing the recovered file share or migrate it to the production environment.

Until you finalize instant recovery of all recovered file shares, a notification about running instant recovery sessions is displayed on the **Dashboard** tab.

Migrating Recovered File Shares

You can migrate recovered SMB file shares to the production environment.

To migrate a recovered file share, use the **Migrate to Production** wizard.

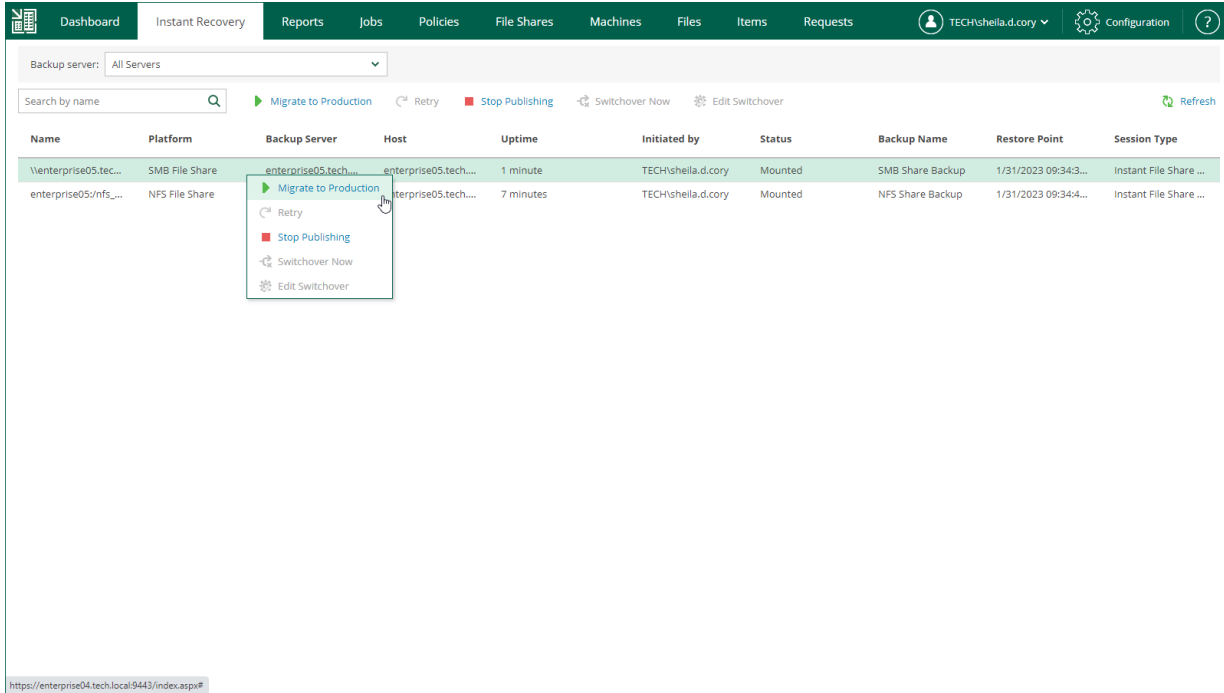
1. [Launch the Migrate to Production wizard.](#)
2. [Specify file share destination.](#)
3. [Specify restore options.](#)
4. [Configure switchover.](#)
5. [Review the migration settings.](#)

Step 1. Launch Migrate to Production Wizard

To launch the **Migrate to Production** wizard, do the following:

1. Open the **Instant Recovery** tab and select a file share from the list.
2. On the toolbar, click **Migrate to production**.

Alternatively, you can right-click a file share and select **Migrate to Production**.



The screenshot shows the Veeam Backup Enterprise Manager interface. The top navigation bar includes tabs for Dashboard, Instant Recovery, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECH\shella.d.cory. The main area displays a table of file shares under the Instant Recovery tab. A context menu is open over the first row, with 'Migrate to Production' highlighted.

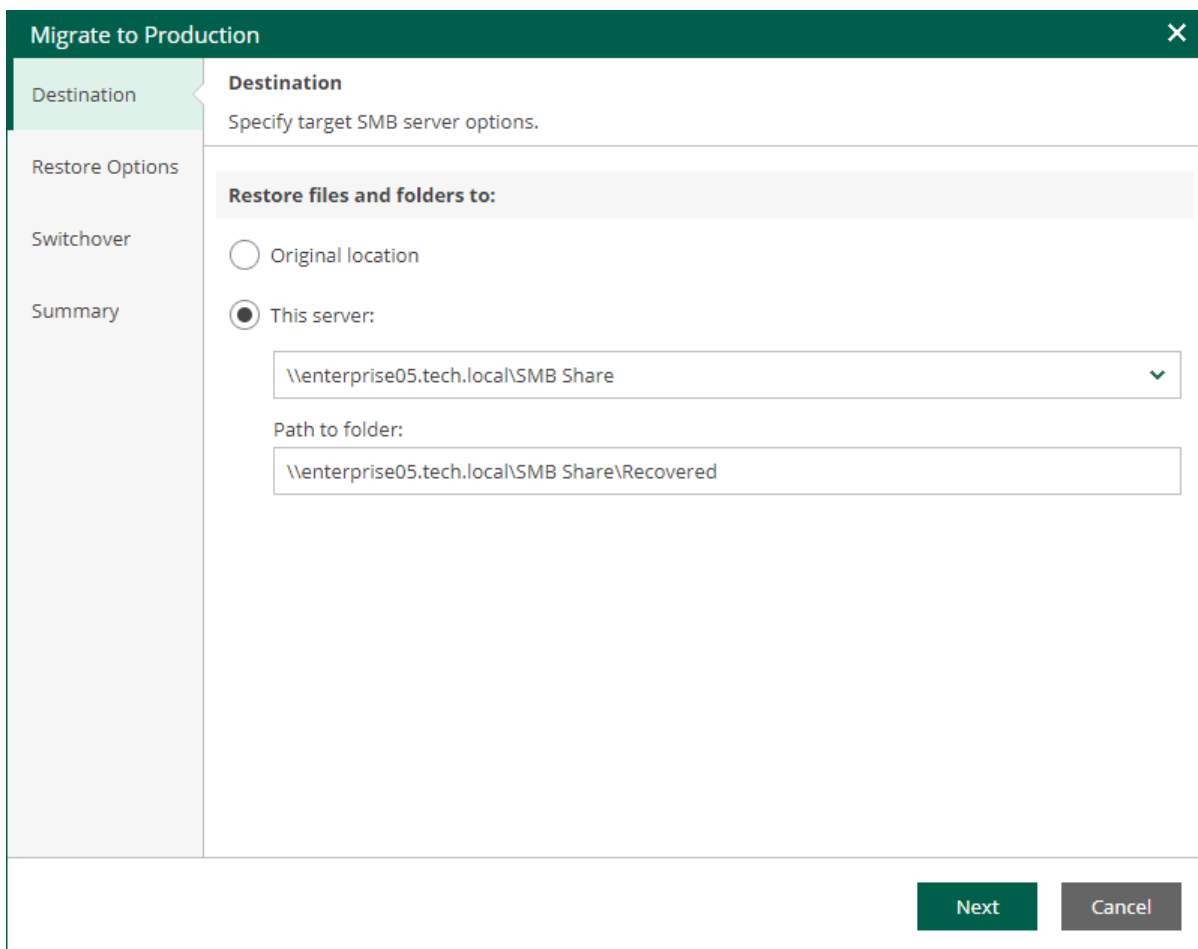
Name	Platform	Backup Server	Host	Uptime	Initiated by	Status	Backup Name	Restore Point	Session Type
\\enterprise05.tec...	SMB File Share	enterprise05.tech...	enterprise05.tech...	1 minute	TECH\shella.d.cory	Mounted	SMB Share Backup	1/31/2023 09:34:3...	Instant File Share ...
enterprise05\dfs_...	NFS File Share	enterprise05.tech...	enterprise05.tech...	7 minutes	TECH\shella.d.cory	Mounted	NFS Share Backup	1/31/2023 09:34:4...	Instant File Share ...

Step 2. Specify Destination

At the **Destination** step of the wizard, specify the location to which you want to restore the file share.

- Select **Original location** to restore data to the location where the file share resided originally. This type of restore is only possible if the original device is connected to Veeam Backup & Replication and powered on.
- Select **This server** to restore data to another location:
 - a. From the **This server** drop-down list, select a file share to which the data must be restored.

You can select any file share added to the backup inventory. If the required file share is missing in the drop-down list, add a new file share to the backup server infrastructure. For more information on how to add a new file share, see the [Adding File Share](#) section of the Veeam Backup & Replication User Guide.
 - b. In the **Path to file** field, specify a path to the folder on the selected file share where the files must be restored.



The screenshot shows the 'Migrate to Production' wizard window. The 'Destination' step is active, with a sidebar on the left containing 'Destination', 'Restore Options', 'Switchover', and 'Summary'. The main area is titled 'Destination' and contains the instruction 'Specify target SMB server options.' Below this, there is a section 'Restore files and folders to:' with two radio button options: 'Original location' (unselected) and 'This server:' (selected). Under 'This server:', there is a dropdown menu showing '\\enterprise05.tech.local\SMB Share' and a 'Path to folder:' text box containing '\\enterprise05.tech.local\SMB Share\Recovered'. At the bottom right, there are 'Next' and 'Cancel' buttons.

Step 3. Specify Restore Options

At the **Restore Options** step of the wizard, specify overwrite options in case the file with the same name already exists in the target folder.

- **Replace older files only**

Select this option if you want to overwrite the existing file only if it is older than the restored file.

- **Restore anyway**

Select this option if you want to overwrite the existing file with the restored file in all cases.

The screenshot shows a wizard window titled "Migrate to Production" with a close button (X) in the top right corner. On the left is a vertical navigation pane with four items: "Destination" (highlighted in blue), "Restore Options" (highlighted in green), "Switchover", and "Summary". The main content area is titled "Restore Options" and contains the instruction "Specify additional restore options." Below this is a section header "If a restored file already exists in the destination:" followed by two radio button options: "Replace older files only" (unselected) and "Restore anyway (overwrites the existing file)" (selected). At the bottom right of the window are three buttons: "Previous" (disabled), "Next" (active), and "Cancel" (disabled).

Step 4. Configure Switchover

At the **Switchover** step of the wizard, select a type of the switchover from the mounted file share to the migrated file share.

- **Automatic** – select this option if you want Veeam Backup & Replication to perform the switch automatically right after the entire file share will be restored.
- **Manual** – select this option if you want to perform the switch manually.
- **Scheduled** – select this option if you want Veeam Backup & Replication to perform the switchover at a specified date and time.

The screenshot shows a window titled "Migrate to Production" with a close button (X) in the top right corner. On the left is a navigation pane with four items: "Destination", "Restore Options", "Switchover" (which is highlighted with a green bar), and "Summary". The main area is titled "Switchover" and contains the instruction "Specify file share switchover options." Below this is a section labeled "Switchover type:" with three radio button options: "Automatic" (unselected), "Manual" (selected), and "Scheduled" (unselected). The "Scheduled" option has a date field set to "1/31/2023" and a time field set to "10:45 pm". At the bottom right of the window are three buttons: "Previous", "Next" (highlighted in green), and "Cancel".

Step 5. Review Migration Settings

At the **Summary** step of the wizard, review the migration settings and click **Finish**. Veeam Backup & Replication will migrate the recovered file share to the specified location.

Migrate to Production	
Destination	Summary Please review the migration settings, and click Finish to start the migration.
Restore Options	Source file share: \\enterprise05.tech.local\SMB Share Restore point: less than a day ago (9:34 PM Tuesday 1/31/2023)
Switchover	Mount host: enterprise05.tech.local Access path: \\enterprise05\SMB Share Migrate to:
Summary	Share: \\enterprise05.tech.local\SMB Share Path: \\enterprise05.tech.local\SMB Share\Recovered Restore option: Restore anyway (overwrites the existing file) Switchover type: Manual

Previous Finish Cancel

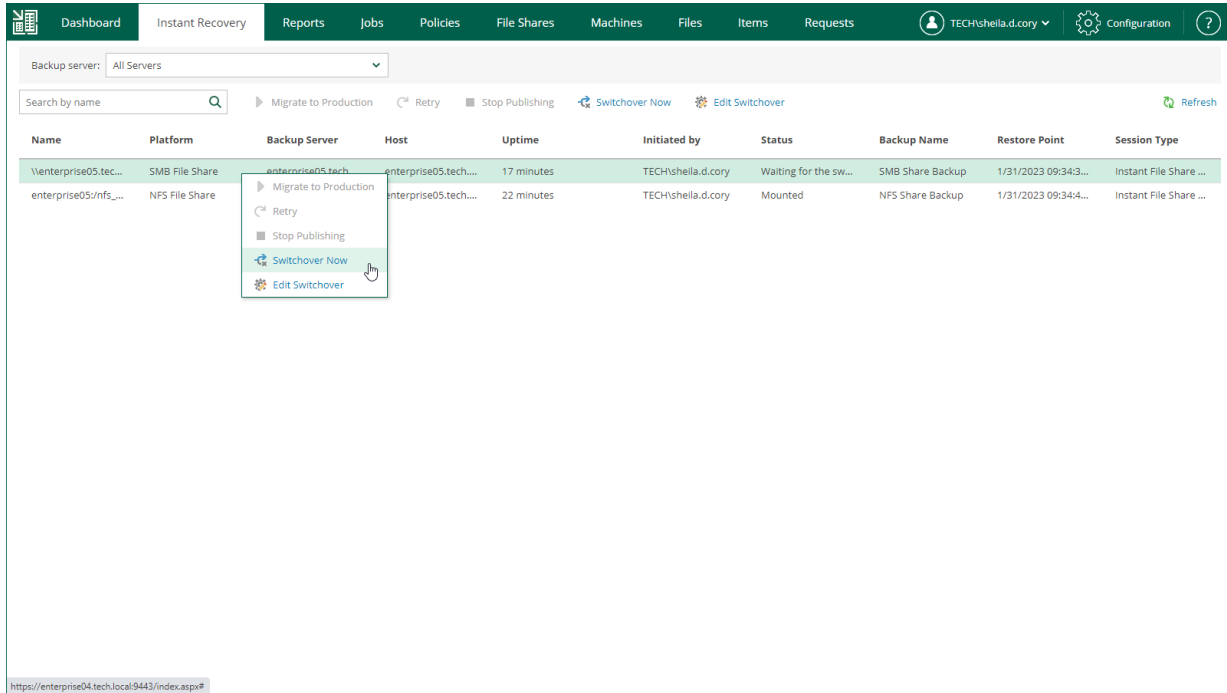
Switching to Production File Share Manually

The following instructions apply if you have selected to switch from the mounted file share to the production file share manually or at the scheduled time at the **Switchover** step of the **Migrate to Production** wizard.

To switch to a production file share, do the following:

1. Open the **Instant Recovery** tab and select a file share from the list.
2. On the toolbar, click **Switchover Now**.

Alternatively, you can right-click a file share and select **Switchover Now**.



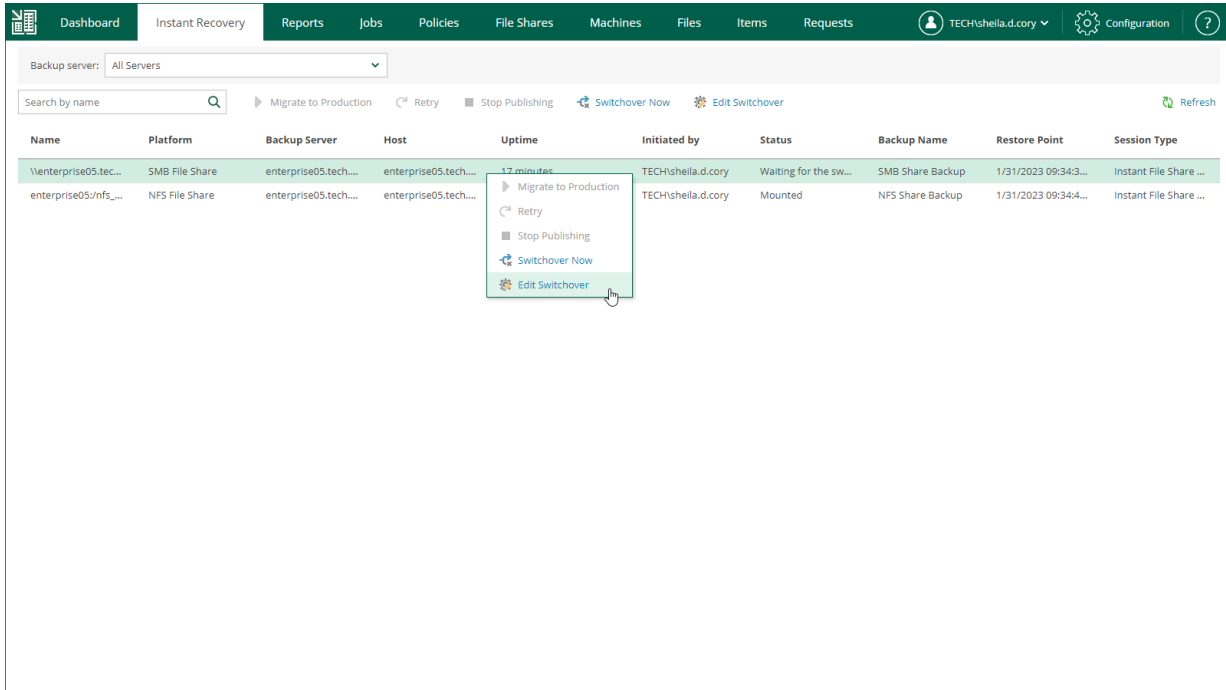
Changing Switchover Time

The following instructions apply if you have selected to switch from the mounted file share to the production file share manually or at the scheduled time at the **Switchover** step of the **Migrate to Production** wizard.

To change the time when Veeam Backup & Replication will switch from the mounted file share to the production file share, do the following:

1. Open the **Instant Recovery** tab and select the necessary file share from the list.
2. On the toolbar, click **Edit Switchover**.
3. At the **Switchover** step of the **Edit Switchover** wizard, select a type of the switchover from the mounted to the migrated file share.
 - **Automatic** – select this option if you want Veeam Backup & Replication to perform the switch automatically right after the entire file share will be restored.
 - **Manual** – select this option if you want to perform the switch manually.
 - **Scheduled** – select this option if you want Veeam Backup & Replication to perform the switchover at a specified date and time.

4. At the **Summary** step of the **Edit Switchover** wizard, review the migration settings and click **Finish**.



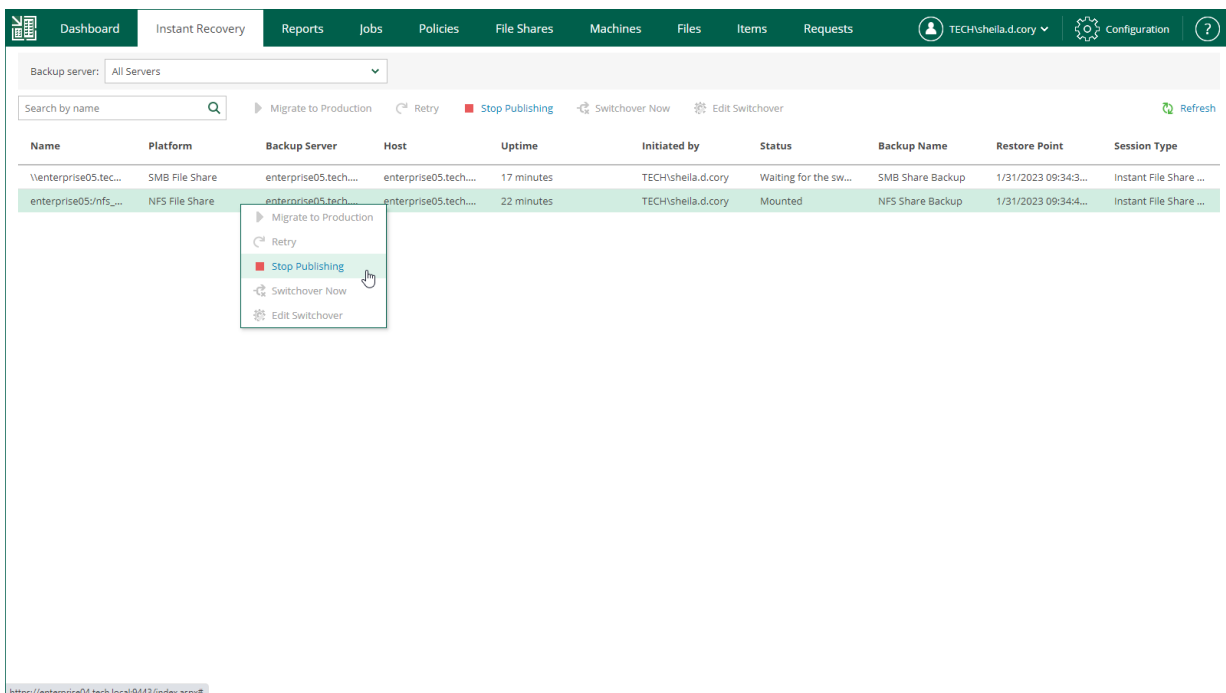
Unpublishing Recovered File Shares

When you finish reviewing the recovered file shares, you can stop publishing them. This will unmount the recovered file shares from the mount server. Note that all changes made in the recovered file shares will be lost.

To stop publishing a recovered file share, do the following:

1. Open the **Instant Recovery** tab and select a file share from the list.
2. On the toolbar, click **Stop Publishing**.

Alternatively, you can right-click a file share and select **Stop Publishing**.



Restoring Specific Files and Folders

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.

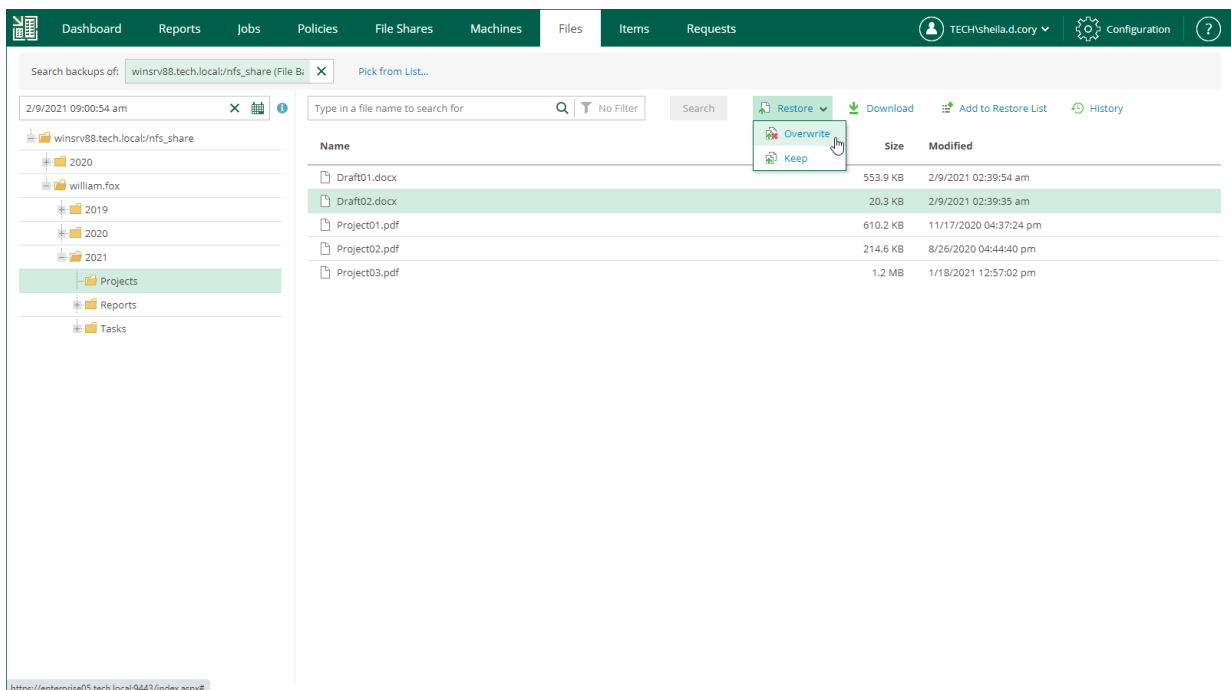
For users with the non-administrative roles, you can configure additional restriction settings. For example, you can prohibit restore operators to download files to the local machine so that they will be able to restore files to the original location only. Additionally, you can specify the types of files that can be restored by operators (this can be helpful if you want to limit operators' access to sensitive data). For details, see [Configuring Permissions for File and Application Item Restore](#).

Restoring Files to Original Location

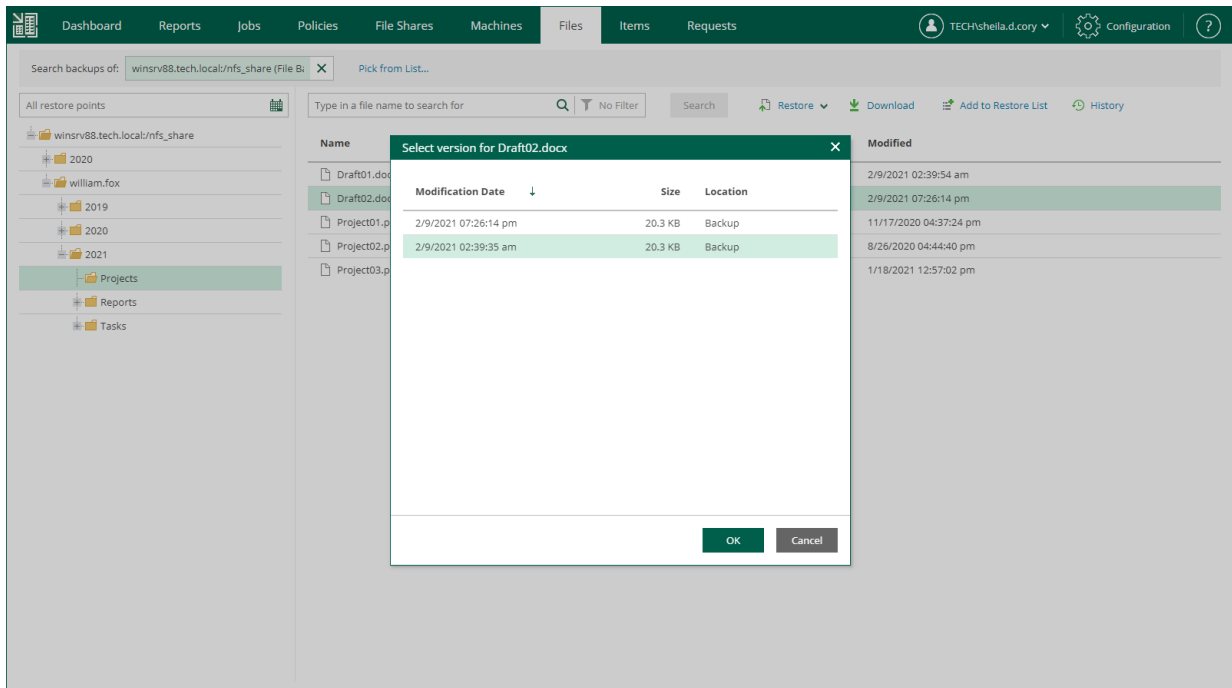
In this restore scenario, Veeam Backup Enterprise Manager will extract the file from the backup and restore it to the original location in the file share. Restoring files to the original location is the most secure file recovery method, as the user who initiates the file restore operation in the Enterprise 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.

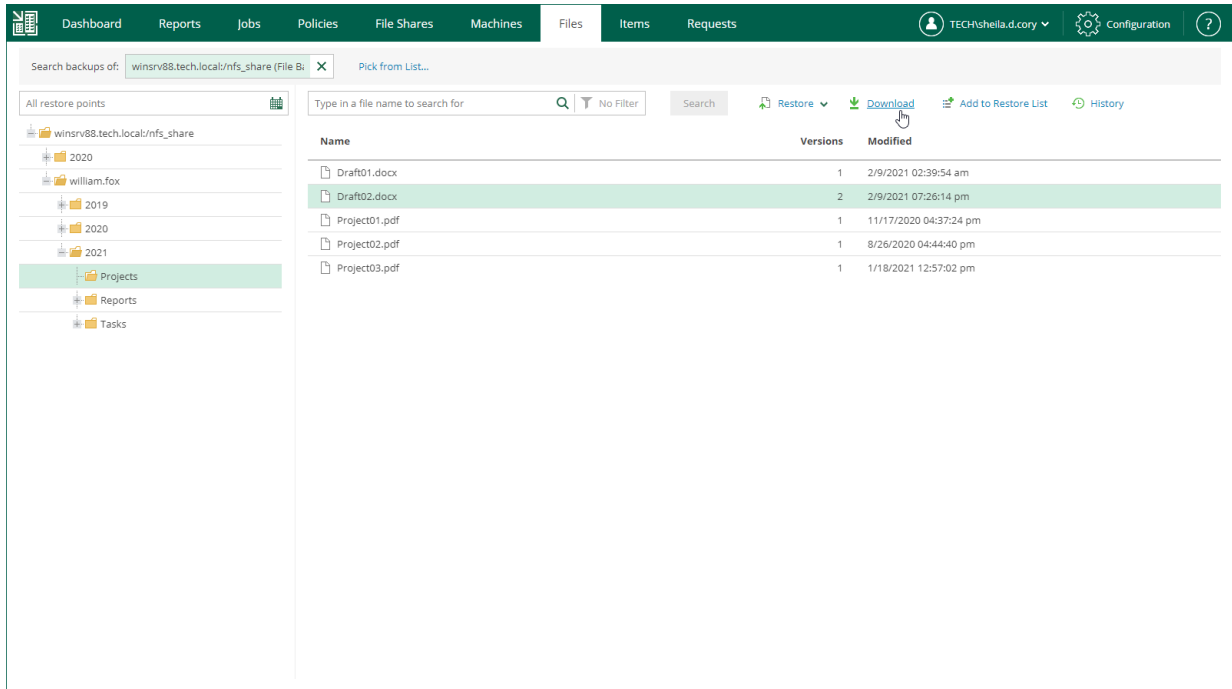
Downloading Files

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.

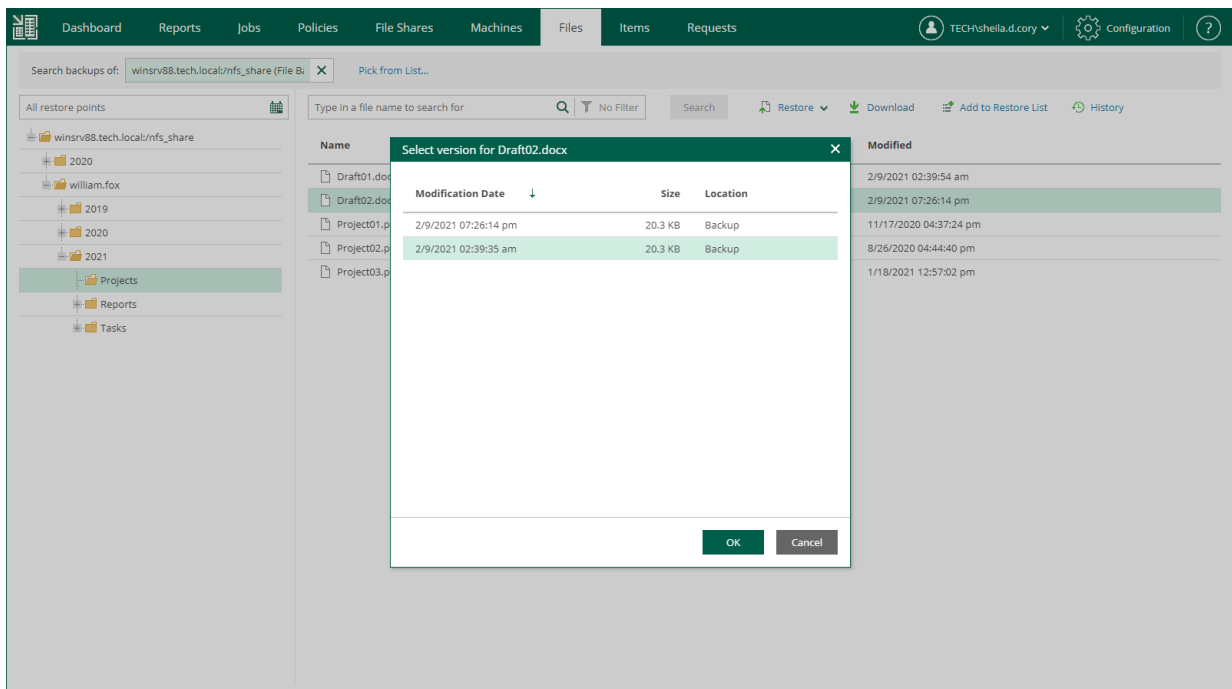
To download a file:

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.

- 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](#).

Initiated by	Started at	Status	Ended at	Total Objects	Progress	Target
TECHshella.d.cory	2/9/2021 09:45:14 pm	Success	2/9/2021 09:45:42 pm	1	100%	Download
TECHshella.d.cory	2/9/2021 02:12:27 am	Success	2/9/2021 02:12:39 am	1	100%	Download

Log

- Starting data transfer agent on server 'enterprise05.tech.local'.
- Starting FLR job for Object winsrv88.tech.local/nfs_share
- winsrv88.tech.local/nfs_share: Processing File restore
- Successfully restored [William.Fox\2021\Projects\Draft02.docx] to server winsrv88.tech.local/nfs_share
- File restore job has completed successfully
- Updating FLR session history
- Packing restored files
- Restored files are available for download

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.

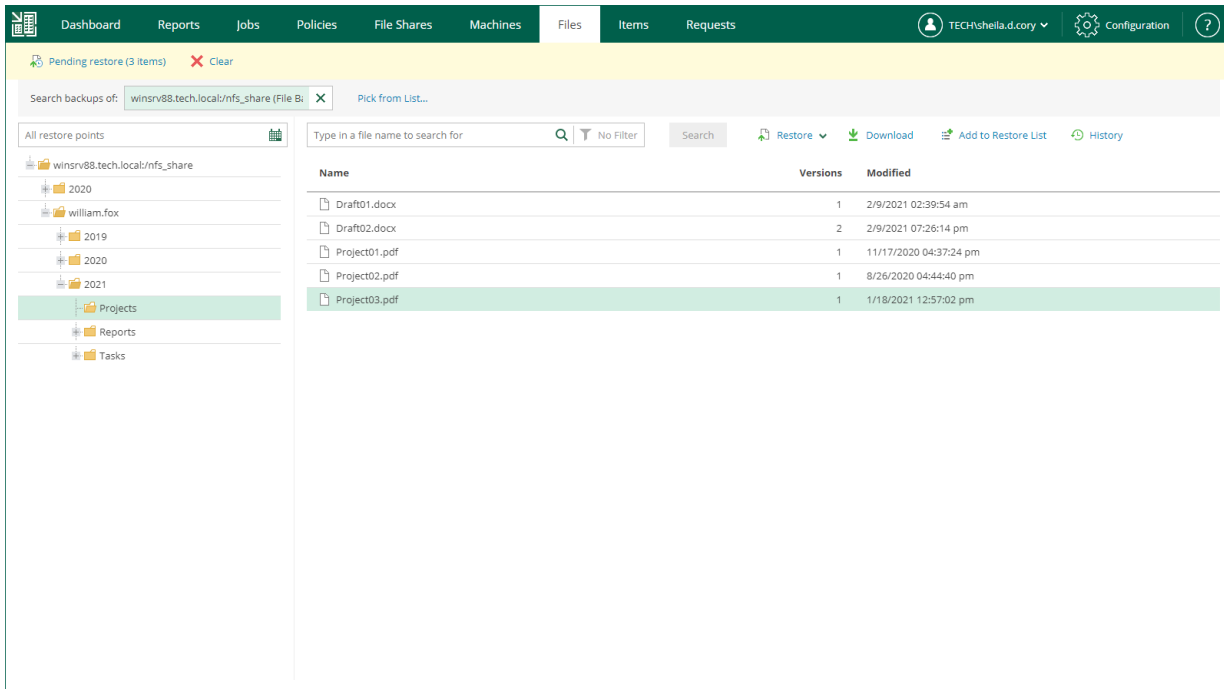
To add a file to the restore list:

- 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](#).
- Click **Add to Restore List**.
- 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.

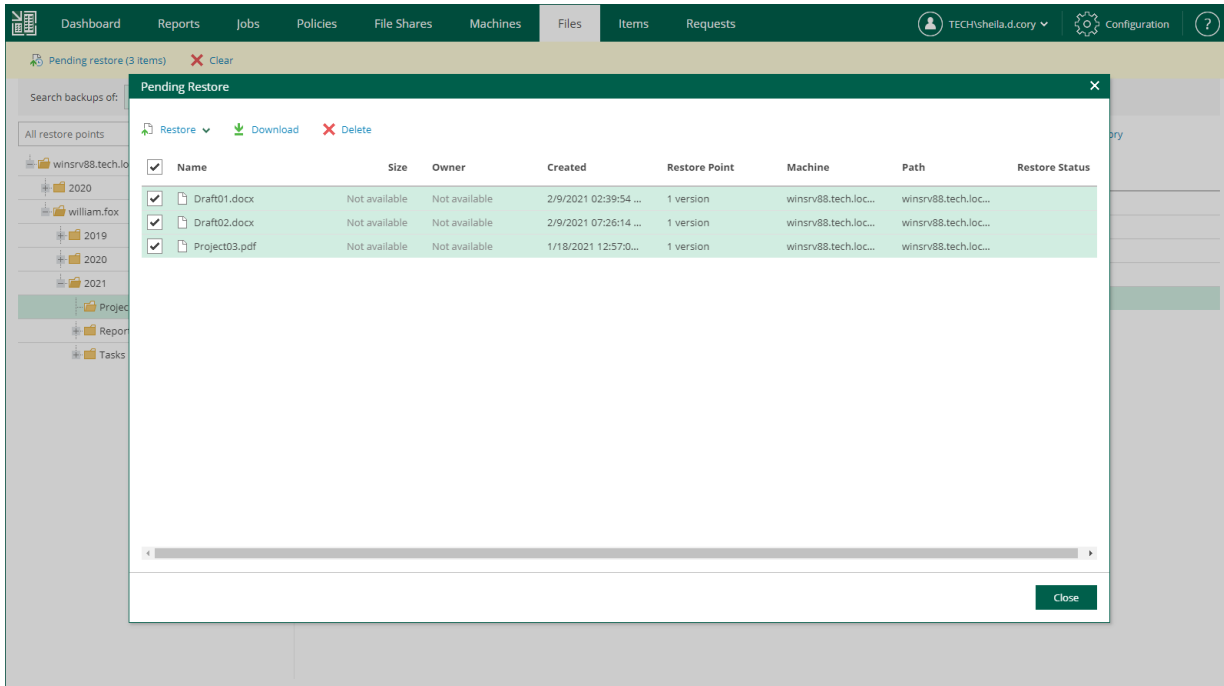
The files are saved to the default download folder on your local machine.

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:

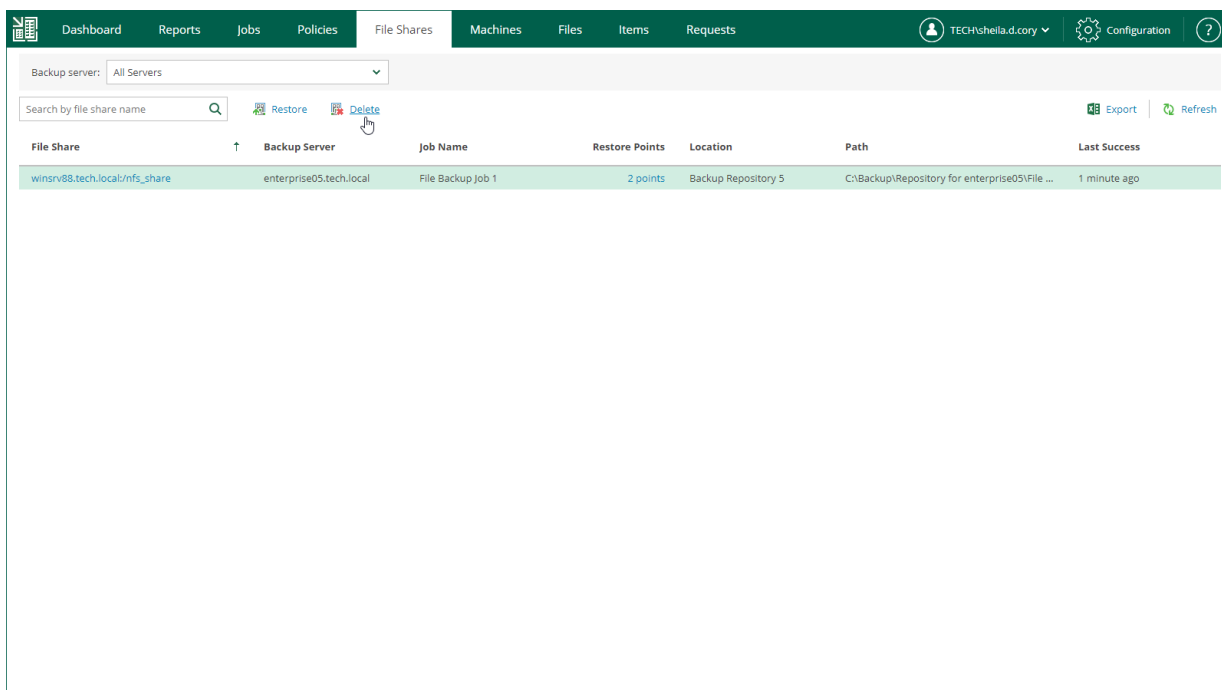
1. In Veeam Backup Enterprise Manager, open the **File Shares** tab.
2. In the list of file share backups, select the necessary backup and click **Delete**.

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

Authorized users can restore VMs included in their restore scope. Users with the Portal Administrator role have no scope limitations. The restore scope 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.

With Veeam Backup Enterprise Manager, you 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 VMware Cloud Director vApps
- Run failover plans for VMware vSphere and Microsoft Hyper-V VMs

Veeam Backup Enterprise Manager does not display Nutanix AHV VMs, and recovery of Nutanix AHV VMs is not available. However, you can browse and restore guest OS files of Nutanix AHV VMs from the backups created by backup copy jobs. For more information, see [Restoring Guest OS Files](#).

Viewing Machines

On the **Machines** tab, you can view information about all machines engaged in performed jobs configured on backup servers.

Entries in the list contain the following data:

- Machine name
- vApp name (for VMware Cloud Director VMs)
- Backup server that processes the machine
- Job name
- Number of restore points
- Path to backup files
- Last time when a restore point was successfully created

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.

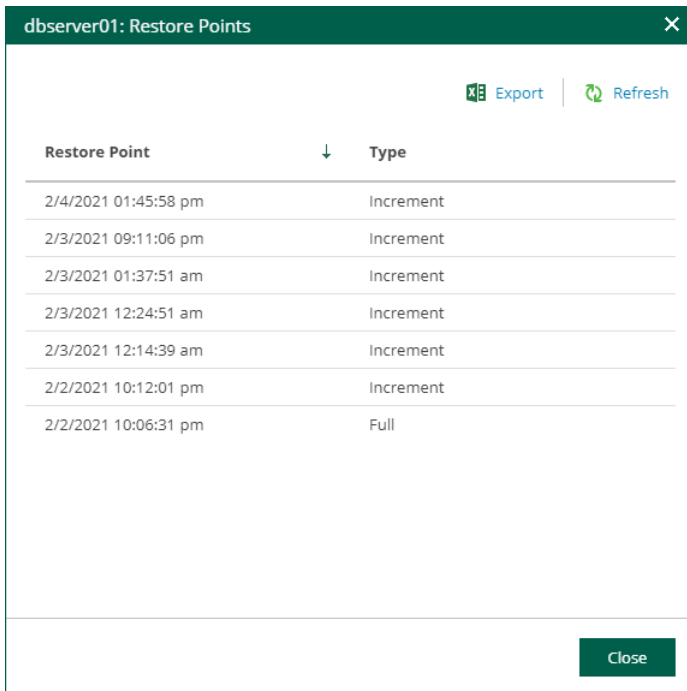
Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
ts-vm01	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	18 points	vcenter01.tech.local/pr...	ts-vm01-xbds	5 hours ago
ts-vm022	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	18 points	vcenter01.tech.local/pr...	ts-vm022-IVN	5 hours ago
mssql02	Not available	enterprise05.tech.local	MSSQL02 Backup to Default Repos...	8 points	Default Backup Reposit...	C:\Backup\MSSQL02 Backup to Default Repository	9 hours ago
win10_pro	Not available	enterprise05.tech.local	Templates Backup	1 point	Default Backup Reposit...	C:\Backup\Templates Backup	13 hours ago
ubuntu88	Not available	enterprise05.tech.local	Ubuntu Replication	2 points	vcenter01.tech.local/pr...	ubuntu88_replica	19 hours ago
linux03	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	12 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	20 hours ago
linux02	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	12 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	20 hours ago
apache05	Not available	enterprise05.tech.local	Web Servers Backup	12 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	23 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	12 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	23 hours ago
rhei01	Not available	enterprise05.tech.local	RHEL Backup	5 points	Default Backup Reposit...	C:\Backup\RHEL Backup	1 day ago
op-win10	op-win10-0dfe29a8-1fa7...	enterprise05.tech.local	Backup Job	1 point	Default Backup Reposit...	C:\Backup\Backup Job	6 days ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	129 points	Backup Repository 1	C:\Backup\Repository\AD Backup	12 days ago
disq01	Not available	enterprise05.tech.local	MS SQL Backup	4 points	Backup Repository 1	C:\Backup\Repository\MS SQL Backup_1	14 days ago
disq01	Not available	enterprise05.tech.local	disq01_2023-01-20 (Exported)	1 point	Backup Repository 1	C:\Backup\Repository\disq01_2023-01-20	14 days ago
linorc01	Not available	enterprise05.tech.local	Oracle Linux Backup	3 points	Backup Repository 1	C:\Backup\Repository\Oracle Linux Backup	14 days ago

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.



The screenshot shows a window titled "dbserver01: Restore Points" with a close button in the top right corner. Below the title bar is a toolbar containing an "Export" button (with a file icon) and a "Refresh" button (with a circular arrow icon). The main area of the window displays a table with two columns: "Restore Point" and "Type". The table contains seven rows of data, with the last row having a "Full" type and the others having an "Increment" type. A "Close" button is located in the bottom right corner of the window.

Restore Point	Type
2/4/2021 01:45:58 pm	Increment
2/3/2021 09:11:06 pm	Increment
2/3/2021 01:37:51 am	Increment
2/3/2021 12:24:51 am	Increment
2/3/2021 12:14:39 am	Increment
2/2/2021 10:12:01 pm	Increment
2/2/2021 10:06:31 pm	Full

Deleting Machine from Backup

When you delete a machine, it is not removed from the list of machines immediately. The machine will be removed after the records about the machine are removed from the configuration database on the backup server. Once this operation completes, a notification appears at the top of the Enterprise Manager UI window.

NOTE

Consider the following:

- If multiple 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.

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.

Quick Backup

Quick backup is an ad-hoc incremental backup for one or more machines. To create a new incremental restore point, Veeam Backup & Replication triggers an existing backup job that processes the selected machine. This restore point 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. For more information on quick backup, see the [Quick Backup](#) section of the Veeam Backup & Replication User Guide.

You can perform quick backup for machines that meet the following requirements:

- Physical or virtual machine is processed by a regular backup job or Veeam Agent backup job managed by the backup server.
- Backup job processing the machine exists on the backup server.
- Full backup file for the machine exists in the backup repository.

NOTE

Quick backup is not available for VMware Cloud Director VMs processed with VMware Cloud Director jobs.

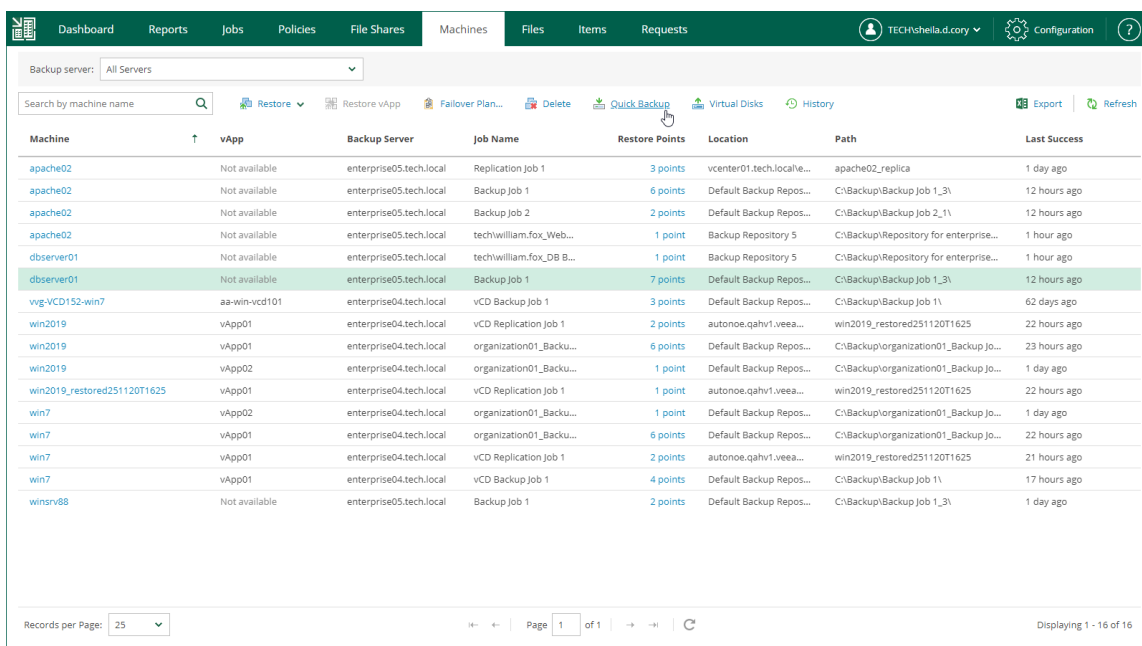
To perform quick backup, do the following:

1. On the **Machines** tab, select the necessary machine.
2. On the toolbar, click **Quick Backup**.

Alternatively, you can right-click the machine and select Quick Backup.

To view the details of the quick backup, open the backup job session that processes the selected machine.

1. On **Jobs** tab, select the backup job that processes the machine.
2. Click the job status link in the **Status** column.
3. To view the session log, on the opened Reports tab, select the machine.



Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
apache02	Not available	enterprise05.tech.local	Replication Job 1	3 points	vcenter01.tech.local/e...	apache02_replica	1 day ago
apache02	Not available	enterprise05.tech.local	Backup Job 1	6 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	12 hours ago
apache02	Not available	enterprise05.tech.local	Backup Job 2	2 points	Default Backup Repos...	C:\Backup\Backup Job 2_1\	12 hours ago
apache02	Not available	enterprise05.tech.local	tech\william.fox_Web...	1 point	Backup Repository 5	C:\Backup\Repository for enterprise...	1 hour ago
dbserver01	Not available	enterprise05.tech.local	tech\william.fox_DB B...	1 point	Backup Repository 5	C:\Backup\Repository for enterprise...	1 hour ago
dbserver01	Not available	enterprise05.tech.local	Backup Job 1	7 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	12 hours ago
wvg-VCD152-win7	aa-win-vcfd101	enterprise04.tech.local	vCD Backup Job 1	3 points	Default Backup Repos...	C:\Backup\Backup Job 1\	62 days ago
win2019	vApp01	enterprise04.tech.local	vCD Replication Job 1	2 points	autonoe.qahv1.veea...	win2019_restored251120T1625	22 hours ago
win2019	vApp01	enterprise04.tech.local	organization01_Backu...	6 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	23 hours ago
win2019	vApp02	enterprise04.tech.local	organization01_Backu...	1 point	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	1 day ago
win2019_restored251120T1625	vApp01	enterprise04.tech.local	vCD Replication Job 1	1 point	autonoe.qahv1.veea...	win2019_restored251120T1625	22 hours ago
win7	vApp02	enterprise04.tech.local	organization01_Backu...	1 point	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	1 day ago
win7	vApp01	enterprise04.tech.local	organization01_Backu...	6 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	22 hours ago
win7	vApp01	enterprise04.tech.local	vCD Replication Job 1	2 points	autonoe.qahv1.veea...	win2019_restored251120T1625	21 hours ago
win7	vApp01	enterprise04.tech.local	vCD Backup Job 1	4 points	Default Backup Repos...	C:\Backup\Backup Job 1\	17 hours ago
winsrv88	Not available	enterprise05.tech.local	Backup Job 1	2 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	1 day ago

VM Recovery

Authorized users can recover VMs from backups to the original location or a new location included in their restore scope. Users with the Portal Administrator role have no scope limitations. For more information on restore scope, see [Configuring Restore Scope](#).

With Veeam Backup Enterprise Manager, you can perform the following types of recovery:

- [Instant Recovery](#)
- [Entire VM Restore](#)
- [Virtual Disk Restore](#)
- [VM Failover](#)
- [Failover Plans](#)

Instant Recovery

Authorized users can instantly recover VMs from backups to the original location or a new location included in their restore scope. Users with the Portal Administrator role have no scope limitations. For more information on restore scope, see [Configuring Restore Scope](#).

Veeam Backup Enterprise Manager supports the following scenarios of Instant Recovery:

- [Instant recovery of VMware vSphere VMs to VMware vSphere](#)
- [Instant recovery of VMware Cloud Director VMs to VMware Cloud Director](#)
- [Instant recovery of Microsoft Hyper-V VMs to Microsoft Hyper-V](#)

Using the Veeam Backup & Replication console, you can instantly recover VMware vSphere VMs to Microsoft Hyper-V and instantly recover Microsoft Hyper-V VMs to VMware vSphere. For more information, see the [VM Recovery](#) section of the Veeam Backup & Replication User Guide.

IMPORTANT

Instant Recovery is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Supported Backup Types

You can recover workloads from the following types of backups:

- Backups of VMware vSphere virtual machines created by Veeam Backup & Replication
- Backups of VMware Cloud Director virtual machines created by Veeam Backup & Replication
- Backups of Microsoft Hyper-V virtual machines created by Veeam Backup & Replication

Instant Recovery to VMware vSphere

Veeam Backup Enterprise Manager allows you to instantly recover VMware vSphere VMs to VMware vSphere. You can recover VMs from backups to the original location or a new location included in your restore scope. After you have performed Instant Recovery, you have to finalize it. For more information, see [Finalizing Instant Recovery to VMware vSphere](#).

For more information on Instant Recovery, see the [Instant Recovery to VMware vSphere](#) section of the Veeam Backup & Replication User Guide.

Performing Instant Recovery to VMware vSphere

To instantly recover a VM, use the **Instant Recovery to VMware vSphere** wizard.

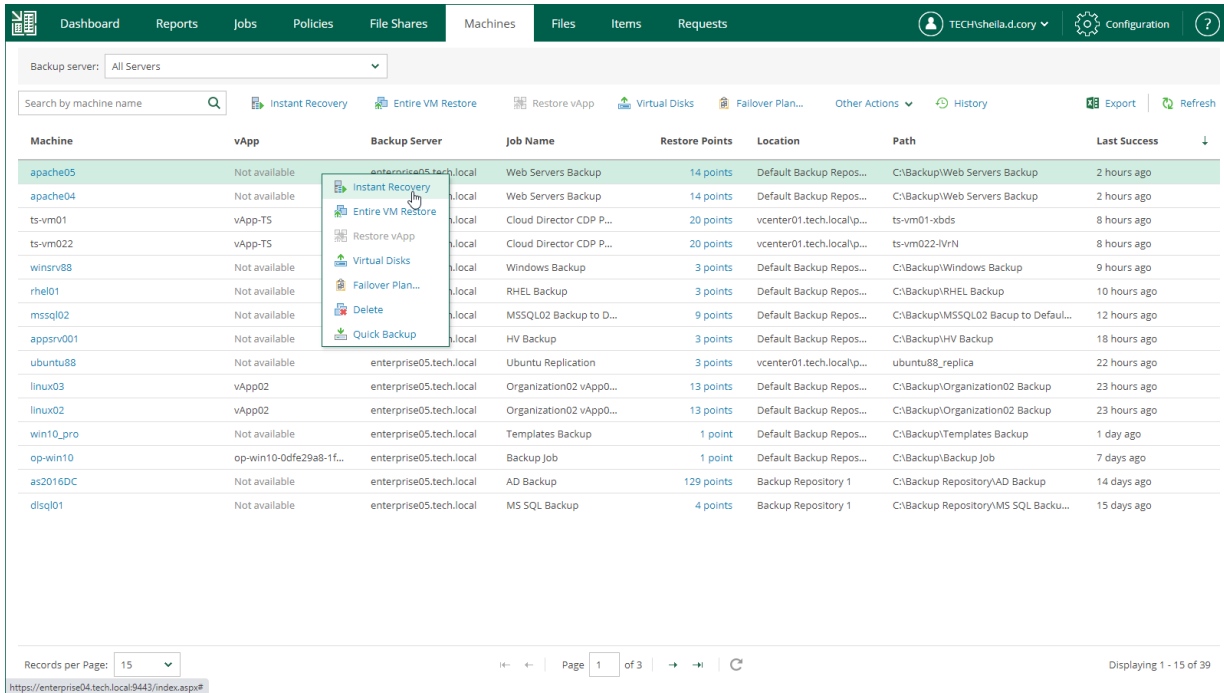
1. [Launch the Instant Recovery wizard](#).
2. [Select a restore point](#).
3. [Select a recovery mode](#).
4. [Specify destination settings for the recovered VM](#).
5. [Specify target datastore](#).
6. [Review the recovery settings](#).

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery to VMware vSphere** wizard, do the following:

1. On the **Machines** tab, select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Instant Recovery**.

Alternatively, you can right-click the VM and select **Instant Recovery**.



The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\shella.d.cory'. The 'Machines' tab is active, showing a list of machines. A context menu is open over the 'apache04' machine, with 'Instant Recovery' selected. The table below shows the details of the machines.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
apache05	Not available	enterprise05.tech.local	Web Servers Backup	14 points	Default Backup Repos...	C:\Backup\Web Servers Backup	2 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	14 points	Default Backup Repos...	C:\Backup\Web Servers Backup	2 hours ago
ts-vm01	vApp-T5	enterprise05.tech.local	Cloud Director CDP P...	20 points	vcenter01.tech.local/p...	ts-vm01-xbds	8 hours ago
ts-vm022	vApp-T5	enterprise05.tech.local	Cloud Director CDP P...	20 points	vcenter01.tech.local/p...	ts-vm022-lvN	8 hours ago
winsrv88	Not available	enterprise05.tech.local	Windows Backup	3 points	Default Backup Repos...	C:\Backup\Windows Backup	9 hours ago
rhel01	Not available	enterprise05.tech.local	RHEL Backup	3 points	Default Backup Repos...	C:\Backup\RHEL Backup	10 hours ago
mssql02	Not available	enterprise05.tech.local	MSSQL02 Backup to D...	9 points	Default Backup Repos...	C:\Backup\MSSQL02 Backup to Defaul...	12 hours ago
appsrv001	Not available	enterprise05.tech.local	HV Backup	3 points	Default Backup Repos...	C:\Backup\HV Backup	18 hours ago
ubuntu88	Not available	enterprise05.tech.local	Ubuntu Replication	3 points	vcenter01.tech.local/p...	ubuntu88_replica	22 hours ago
linux03	vApp02	enterprise05.tech.local	Organization02 vApp0...	13 points	Default Backup Repos...	C:\Backup\Organization02 Backup	23 hours ago
linux02	vApp02	enterprise05.tech.local	Organization02 vApp0...	13 points	Default Backup Repos...	C:\Backup\Organization02 Backup	23 hours ago
win10_pro	Not available	enterprise05.tech.local	Templates Backup	1 point	Default Backup Repos...	C:\Backup\Templates Backup	1 day ago
op-win10	op-win10-0dfe29a8-1f...	enterprise05.tech.local	Backup Job	1 point	Default Backup Repos...	C:\Backup\Backup Job	7 days ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	129 points	Backup Repository 1	C:\Backup Repository\AD Backup	14 days ago
dlsq01	Not available	enterprise05.tech.local	MS SQL Backup	4 points	Backup Repository 1	C:\Backup Repository\MMS SQL Backu...	15 days ago

Records per Page: 15 | Page 1 of 3 | Displaying 1 - 15 of 39

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point from which you want to perform instant recovery.

Instant Recovery to VMware vSphere [Close]

Restore Point
Select the restore point to restore VM from.

Restore Mode
VM name: apache05

Summary

Backup Date	Type
2/3/2023 03:01:09 pm	Increment
2/2/2023 03:01:00 pm	Increment
2/1/2023 03:01:13 pm	Increment
1/31/2023 03:06:51 pm	Increment
1/30/2023 03:00:40 pm	Increment
1/29/2023 03:01:33 pm	Increment
1/28/2023 03:00:40 pm	Full
1/27/2023 03:00:49 pm	Increment
1/26/2023 03:00:46 pm	Increment
1/25/2023 03:00:56 pm	Increment
1/24/2023 03:00:55 pm	Increment
1/23/2023 03:00:47 pm	Increment

Next **Cancel**

Step 3. Select Recovery Mode

At the **Restore mode** step, select a recovery mode for the VM and choose whether you want to recover VM tags.

1. Select a destination for recovery:

- Select **Restore to the original location** to recover the VM with initial settings to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

IMPORTANT

If you recover a VM with initial settings, and the original VM still exists in the virtual infrastructure, the original VM will be removed.

- Select **Restore to a new location or with different settings** to recover the VM to a new location, or to any location but with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.

2. If you want to recover tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will recover the VM with original tags if the following conditions are met:

- You recover a VM to the original location.
- The original VM tags are available on the source vCenter Server.

The screenshot shows a wizard window titled "Instant Recovery to VMware vSphere" with a close button (X) in the top right corner. On the left is a navigation pane with the following items: "Restore Point", "Restore Mode" (highlighted in green), "Destination", "Datastore", and "Summary". The main content area is titled "Restore Mode" and contains the following text: "Specify whether selected VM should be restored back to the original location, or to a new location or with different settings." Below this text are two radio button options: "Restore to the original location" (unselected) and "Restore to a new location, or with different settings" (selected). The "Restore to the original location" option has a sub-description: "Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error." The "Restore to a new location, or with different settings" option has a sub-description: "Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults." At the bottom of the main content area is a checked checkbox labeled "Restore VM tags". At the bottom right of the wizard are three buttons: "Previous" (disabled), "Next" (active), and "Cancel" (disabled).

Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you recover a VM to a new location or with different settings.

At this step of the wizard, you configure destination settings such as the recovered VM name, target host, VM folder and so on.

1. In the **Restored VM name** field, specify a name under which the workload will be recovered.
2. In the **Host** field, specify a host on which the VM will run.
3. In the **VM folder** field, specify a folder to which the recovered VM files will be placed.
4. In the **Resource pool** field, specify a resource pool to which the VM will be placed.
5. Choose whether to preserve the BIOS UUID or generate a new BIOS UUID.

If the original workload still resides in the production environment, select the **Generate new BIOS UUID** option to prevent conflicts. The BIOS UUID change is not required if the original VM no longer exists, for example, if it was deleted.

The screenshot shows a wizard window titled "Instant Recovery to VMware vSphere" with a close button (X) in the top right corner. The left sidebar contains navigation options: "Restore Point", "Restore Mode", "Destination" (highlighted), "Datastore", and "Summary". The main content area is titled "Destination" and includes the following instructions and fields:

Choose ESXi server to run the recovered virtual machine on. You can choose to power on VM automatically, unless you need to adjust VM settings first (such as change VM network).

Restored VM name:

Host: prgtwesx01.tech.local [Choose...](#)

VM folder: Enterprise [Choose...](#)

Resource pool: Enterprise [Choose...](#)

Preserve BIOS UUID
Preserving system UUID for the restored VM prevents issues with applications that match system by UUID.

Generate new BIOS UUID
Generating new UUID prevents possible conflicts between the restored clone and the original machine.

At the bottom right, there are three buttons: "Previous" (disabled), "Next" (active), and "Cancel" (disabled).

Step 5. Specify Datastore

The **Datastore** step of the wizard is available if you recover a VM to a new location or with different settings.

At this step of the wizard, you can select where to store redo logs when a VM is running from the backup. Redo logs are auxiliary files used to keep changes that take place while the recovered VM runs.

By default, redo logs are stored in vPower NFS datastore. You can store redo logs in any datastore in the virtual environment if necessary. Redirecting redo logs improves recovery performance but makes Storage vMotion not possible for ESXi 5.5. As soon as a recovery verification job completes, Veeam Backup & Replication deletes redo logs. For more information on vPower NFS datastore, see the [vPower NFS Servise](#) section of the Veeam Backup & Replication User Guide.

To redirect redo logs, do the following:

1. Select the **Redirect write cache** check box.
2. Click **Choose** and select a datastore.

IMPORTANT

If the size of recovered VM disks is greater than 2 TB, you must not place redo logs on a VSAN datastore. Otherwise, Veeam Backup & Replication will fail to create a snapshot for the recovered VMs. For more information, see [VMware Docs](#).

Instant Recovery to VMware vSphere [X]

Restore Point

Restore Mode

Destination

Datastore

Summary

Datastore

By default, changed virtual disk blocks are stored in the vPower NFS cache folder on the backup repository's mount server. If desired for performance or capacity reasons, you can redirect this write cache to a different datastore.

Redirect write cache

Datastore: prgtwesx01-ds02 [Choose...](#)

1.2 TB free of 7.3 TB

[Previous](#) [Next](#) [Cancel](#)

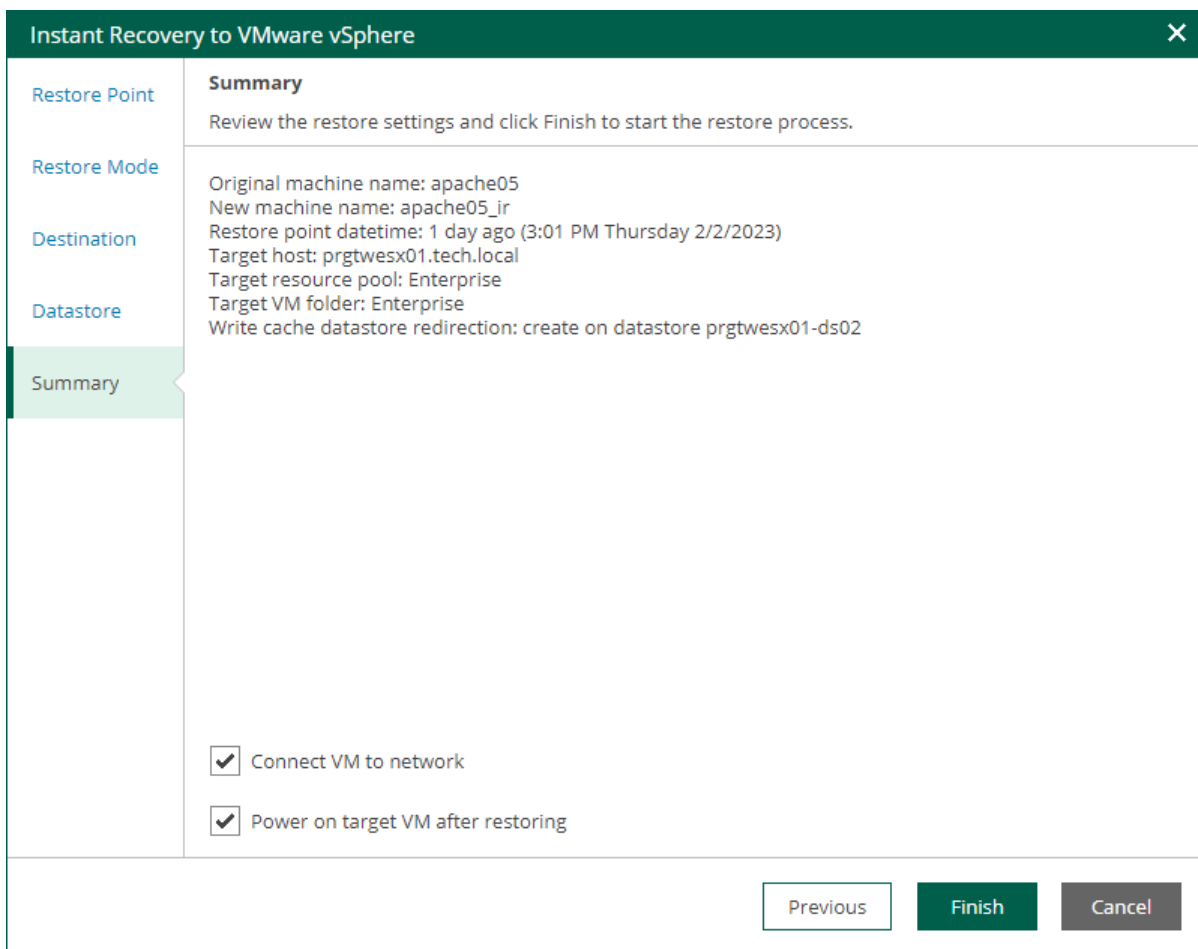
Step 6. Review Recovery Settings

At the **Summary** step of the wizard, specify additional settings for Instant Recovery:

1. If you recover a VM that have failed and want to recover them with initial network settings, select the **Connect VM to network** check box.

If you recover a VM for testing disaster recovery while the original VM is still running, leave this check box unselected. Before you power on the recovered VM, you must disconnect it from the production network and connect to a non-production network to avoid conflicts.
2. To start the VM right after recovery, select the **Power on target VM after restoring** check box. If you recover the workloads to the production network, make sure that the original VM is powered off.
3. Review the settings that you have specified for Instant Recovery and click **Finish**.

To view the Instant Recovery progress, on the **Machines** tab, click **History**.



The screenshot shows a dialog box titled "Instant Recovery to VMware vSphere" with a close button (X) in the top right corner. The dialog is divided into a left sidebar and a main content area. The sidebar contains the following items: "Restore Point", "Restore Mode", "Destination", "Datastore", and "Summary" (which is highlighted with a green background). The main content area is titled "Summary" and contains the following text: "Review the restore settings and click Finish to start the restore process." Below this, there is a list of settings: "Original machine name: apache05", "New machine name: apache05_ir", "Restore point datetime: 1 day ago (3:01 PM Thursday 2/2/2023)", "Target host: prgtwesx01.tech.local", "Target resource pool: Enterprise", "Target VM folder: Enterprise", and "Write cache datastore redirection: create on datastore prgtwesx01-ds02". At the bottom of the main content area, there are two checked checkboxes: "Connect VM to network" and "Power on target VM after restoring". At the bottom right of the dialog, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

What You Do Next

After you have performed instant file share recovery, you must finalize it. For more information, see [Finalizing Instant Recovery to VMware vSphere](#).

Finalizing Instant Recovery to VMware vSphere

After you have performed instant recovery, you have to finalize the process. For this, test the recovered VMs and decide whether to migrate them to production environment or stop publishing.

Until you finalize instant recovery of all recovered VMs, a notification about running instant recovery sessions is displayed on the **Dashboard** tab.

Testing Recovered VM

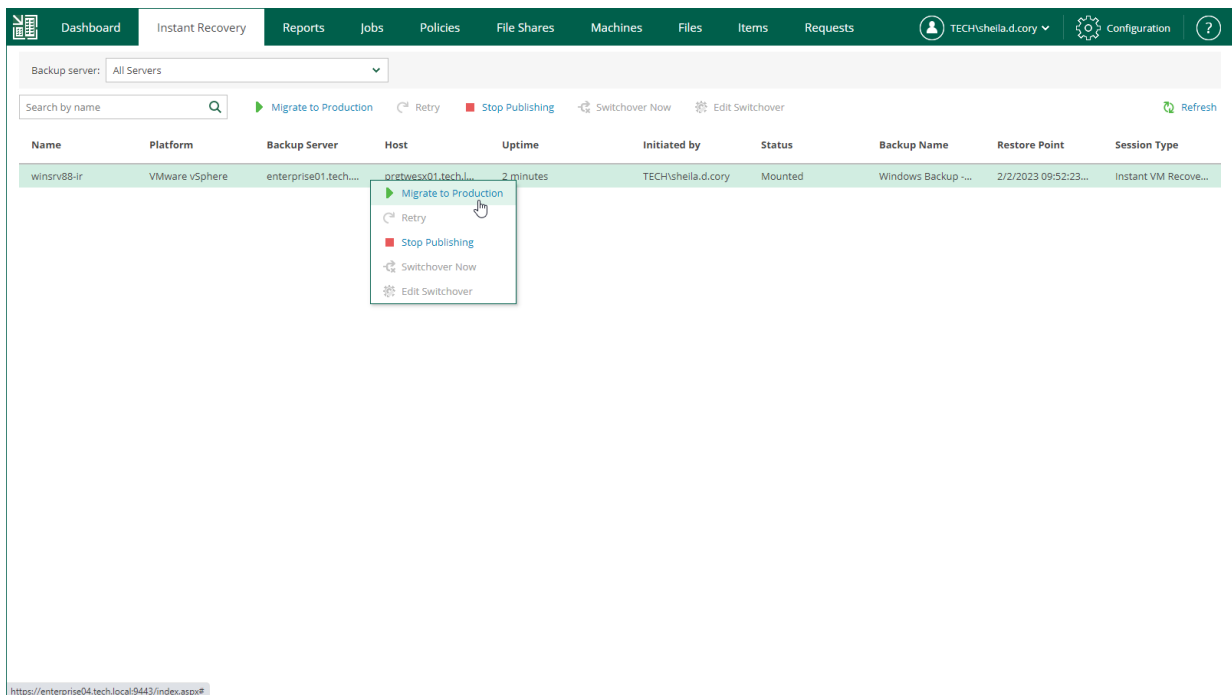
To test a recovered VM before you migrate it to production, you can launch the VMware Remote Console software from the Veeam Backup & Replication console. For more information, see the [Finalizing Instant Recovery to VMware vSphere](#) section of the Veeam Backup & Replication User Guide.

Migrating Recovered VM

If a VM is recovered successfully, you can migrate it to the production environment.

To migrate a recovered VM to production, do the following:

1. Open the **Instant Recovery** tab and select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Migrate to production**.



3. At the **Destination** step of the **VMware Cloud Director Quick Migration** wizard, specify destination where you want to migrate the VM to.
 - a. Click **Choose** next to the **Host** field and select an ESXi host or cluster where the relocated VM must be registered.
 - b. Click **Choose** next to the **VM folder** field and select the target VM folder.
 - c. Click **Choose** next to the **Resource pool** field and select the target resource pool.

d. Click **Choose** next to the **Datastore** field and select the target datastore.

If you want to change the target datastore for the VM configuration files or disk files, do the following:

- i. Select the **Pick datastore for selected virtual disks** check box.
- ii. Select the configuration files or one of the hard disks and click **Change datastore**.
- iii. In the **Add objects** window, choose the necessary datastore and click **OK**.

The screenshot shows the 'Quick Migration' dialog box with a dark green header and a close button (X) in the top right corner. On the left, there is a sidebar with 'Destination' selected and 'Ready' below it. The main area is titled 'Destination' and contains the following information:

Choose destination host, resource pool, VM folder and datastore.

Host: prgtwesx01.tech.local [Choose...](#)

VM folder: Enterprise [Choose...](#)

Resource pool: Enterprise [Choose...](#)

Datastore: prgtwesx01-ds02 [1.2 TB free] [Choose...](#)

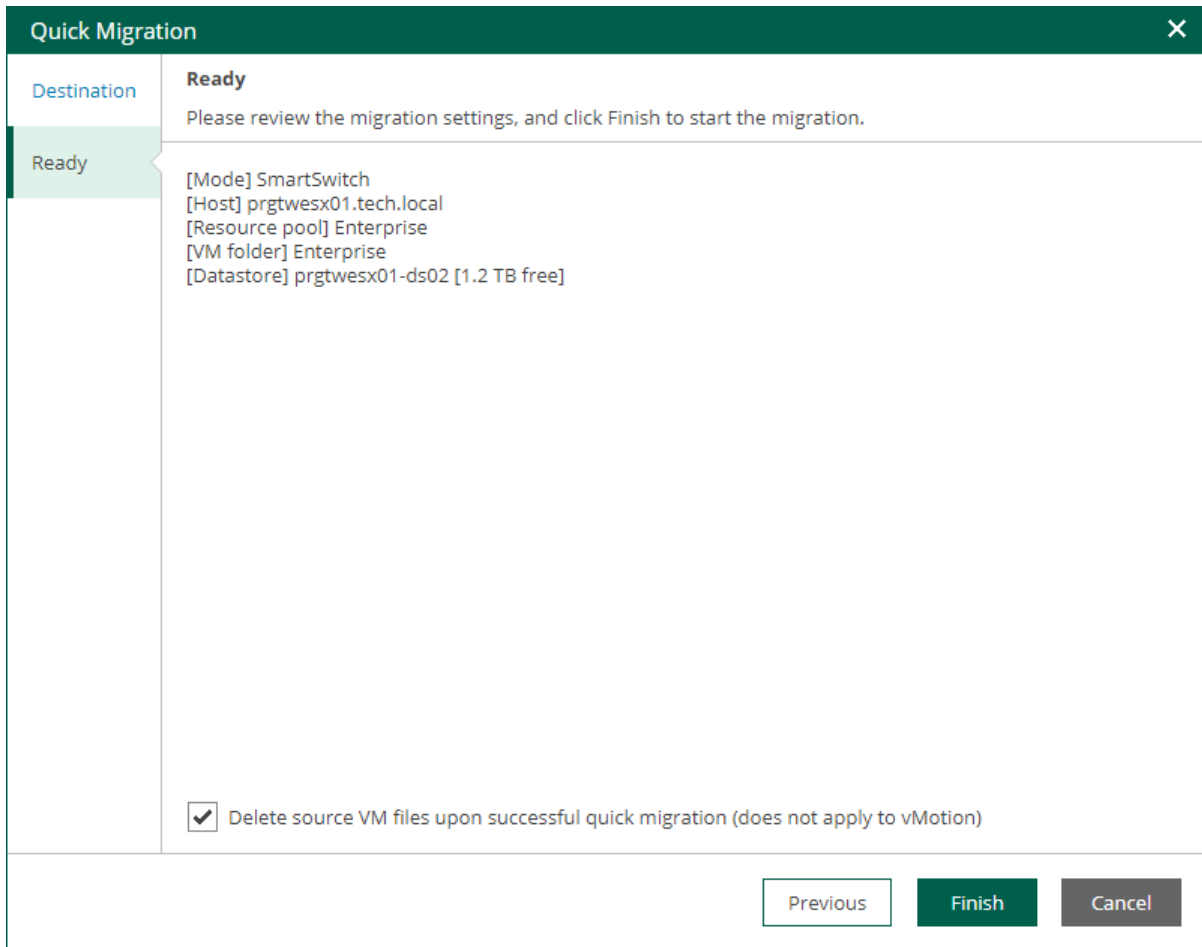
VM files location

Pick datastore for selected virtual disks [Change datastore...](#)

File	Size	Datastore	Disk Type
Configuration files		prgtwesx01-ds02 [1.2 TB free]	
Hard disk 1 (winsrv88-0000...	100 GB	prgtwesx01-ds02 [1.2 TB free]	Thick (lazy zeroed)
Hard disk 2 (winsrv88_1-000...	40 GB	prgtwesx01-ds02 [1.2 TB free]	Thick (lazy zeroed)

At the bottom right, there are two buttons: 'Next' (dark green) and 'Cancel' (grey).

4. At the **Ready** step of the wizard, review migration settings click **Finish**.



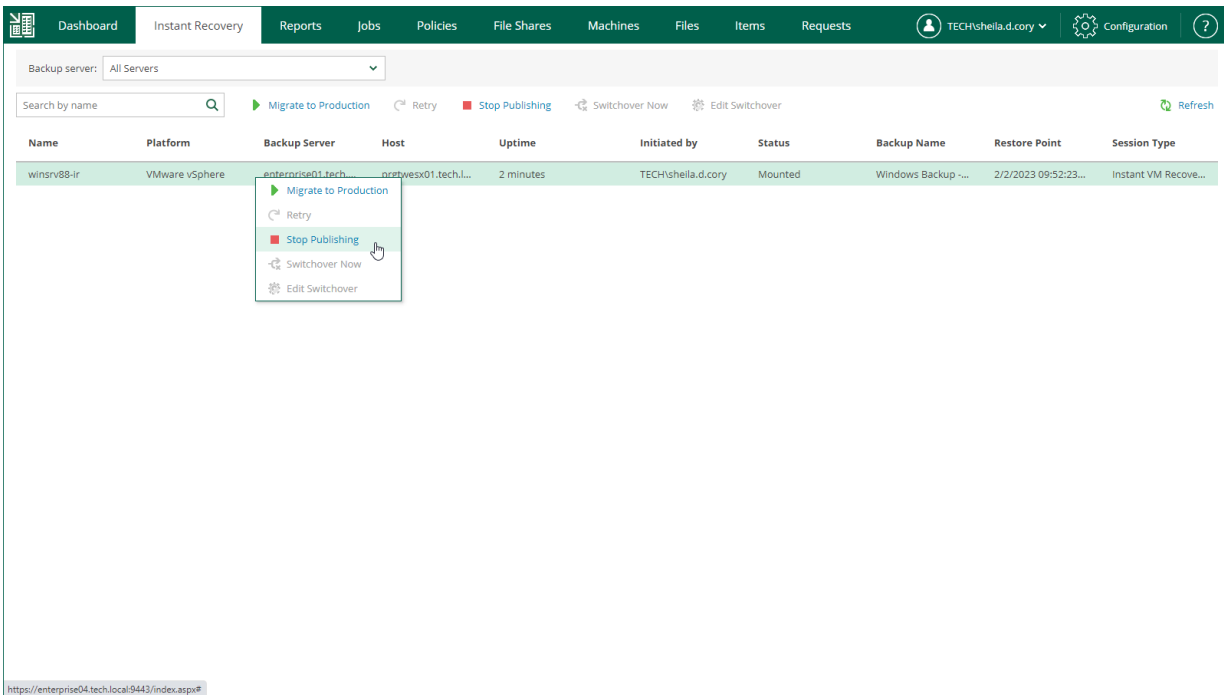
To view the migration progress, on the **Machines** tab, click **History**.

Unpublishing Recovered VM

If your tests have failed, you can stop publishing the recovered VM. This will remove the recovered VM from the host that you selected as the destination for recovery. Note that all changes made in the recovered VMs will be lost.

To remove a recovered VM, do the following:

1. Open the **Instant Recovery** tab and select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Stop Publishing**.



Instant Recovery to VMware Cloud Director

Veeam Backup Enterprise Manager allows you to instantly recover VMware Cloud Director VMs to a vApp in VMware Cloud Director. You can recover VMs from backups to the original vApp or another vApp included in your restore scope. After you have performed Instant Recovery, you have to finalize it. For more information, see [Finalizing Instant Recovery to VMware Cloud Director](#).

For more information on Instant Recovery, see the [Performing Instant Recovery for VMs](#) section of the Veeam Backup & Replication User Guide.

Performing Instant Recovery to VMware Cloud Director

To instantly recover a VM, use the **Instant Recovery to VMware Cloud Director** wizard.

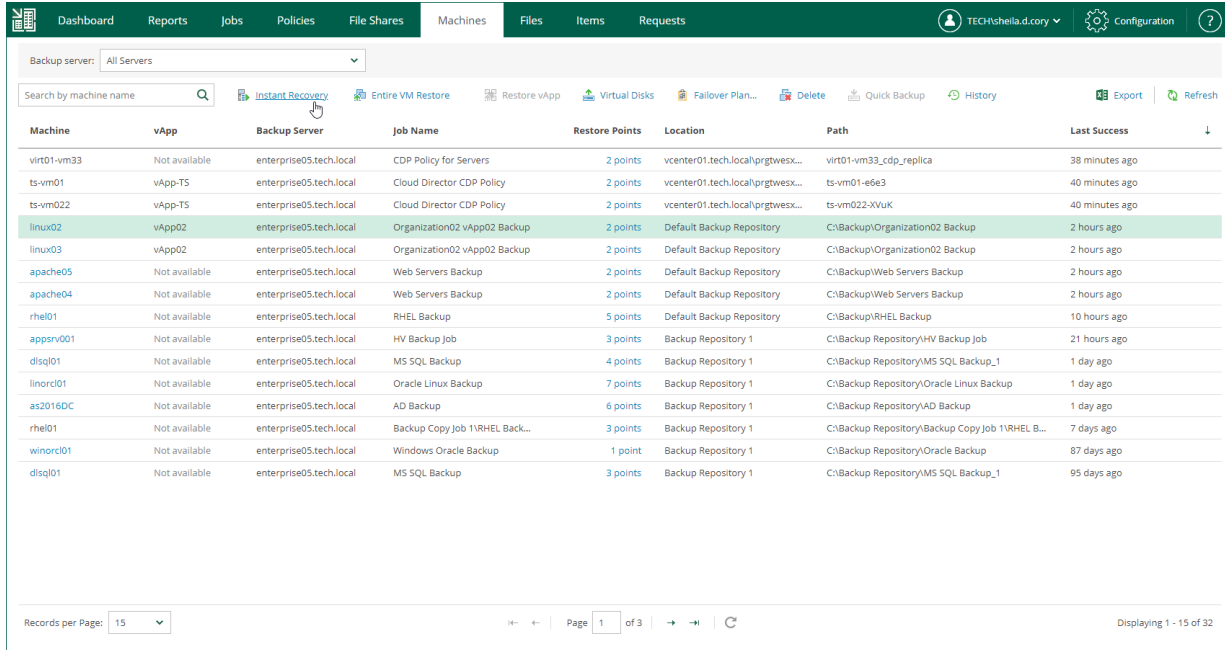
1. [Launch the Instant Recovery to VMware Cloud Director wizard.](#)
2. [Select a restore point.](#)
3. [Select a recovery mode.](#)
4. [Specify destination settings for the recovered VM.](#)
5. [Specify target datastore.](#)
6. [Configure network mapping.](#)
7. [Review the recovery settings.](#)

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery to VMware Cloud Director** wizard, do the following:

1. On the **Machines** tab, select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Instant Recovery**.

Alternatively, you can right-click the VM and select **Instant Recovery**.



The screenshot shows the Veeam Backup Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines (selected), Files, Items, and Requests. The user is logged in as TECH\shells.d.cory. The main area displays a list of machines under the 'Machines' tab. The 'Instant Recovery' button is highlighted in the toolbar. The table below lists the machines and their backup details.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
virt01-vm33	Not available	enterprise05.tech.local	CDP Policy for Servers	2 points	vcenter01.tech.local/prgtwex...	virt01-vm33_cdp_replica	38 minutes ago
ts-vm01	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	2 points	vcenter01.tech.local/prgtwex...	ts-vm01-e6e3	40 minutes ago
ts-vm022	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	2 points	vcenter01.tech.local/prgtwex...	ts-vm022-XVuK	40 minutes ago
linux02	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	2 points	Default Backup Repository	C:\Backup\Organization02 Backup	2 hours ago
linux03	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	2 points	Default Backup Repository	C:\Backup\Organization02 Backup	2 hours ago
apache05	Not available	enterprise05.tech.local	Web Servers Backup	2 points	Default Backup Repository	C:\Backup\Web Servers Backup	2 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	2 points	Default Backup Repository	C:\Backup\Web Servers Backup	2 hours ago
rhel01	Not available	enterprise05.tech.local	RHEL Backup	5 points	Default Backup Repository	C:\Backup\RHEL Backup	10 hours ago
appsrv001	Not available	enterprise05.tech.local	HV Backup Job	3 points	Backup Repository 1	C:\Backup Repository\HV Backup Job	21 hours ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	4 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	1 day ago
linorc01	Not available	enterprise05.tech.local	Oracle Linux Backup	7 points	Backup Repository 1	C:\Backup Repository\Oracle Linux Backup	1 day ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	6 points	Backup Repository 1	C:\Backup Repository\AD Backup	1 day ago
rhel01	Not available	enterprise05.tech.local	Backup Copy Job 1\RHEL Back...	3 points	Backup Repository 1	C:\Backup Repository\Backup Copy Job 1\RHEL B...	7 days ago
winorc01	Not available	enterprise05.tech.local	Windows Oracle Backup	1 point	Backup Repository 1	C:\Backup Repository\Oracle Backup	87 days ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	3 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	95 days ago

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point from which you want to perform instant recovery.

Instant Recovery to VMware Cloud Director [Close]

Restore Point
Select the restore point to restore VM from.

Restore Mode
VM name: linux02

Summary

Backup Date	Type
12/28/2022 06:02:50 pm	Increment
12/27/2022 06:01:47 pm	Increment
12/26/2022 06:01:45 pm	Increment
12/25/2022 06:02:16 pm	Increment
12/24/2022 06:01:39 pm	Full
12/23/2022 06:01:53 pm	Increment
12/23/2022 03:31:40 pm	Increment
12/23/2022 03:25:21 pm	Full

Next **Cancel**

Step 3. Select Recovery Mode

At the **Restore mode** step, select a recovery mode for the VM and choose whether you want to recover VM tags.

1. Select a destination for recovery:

- Select **Restore to the original location** to recover the VM with initial settings and to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

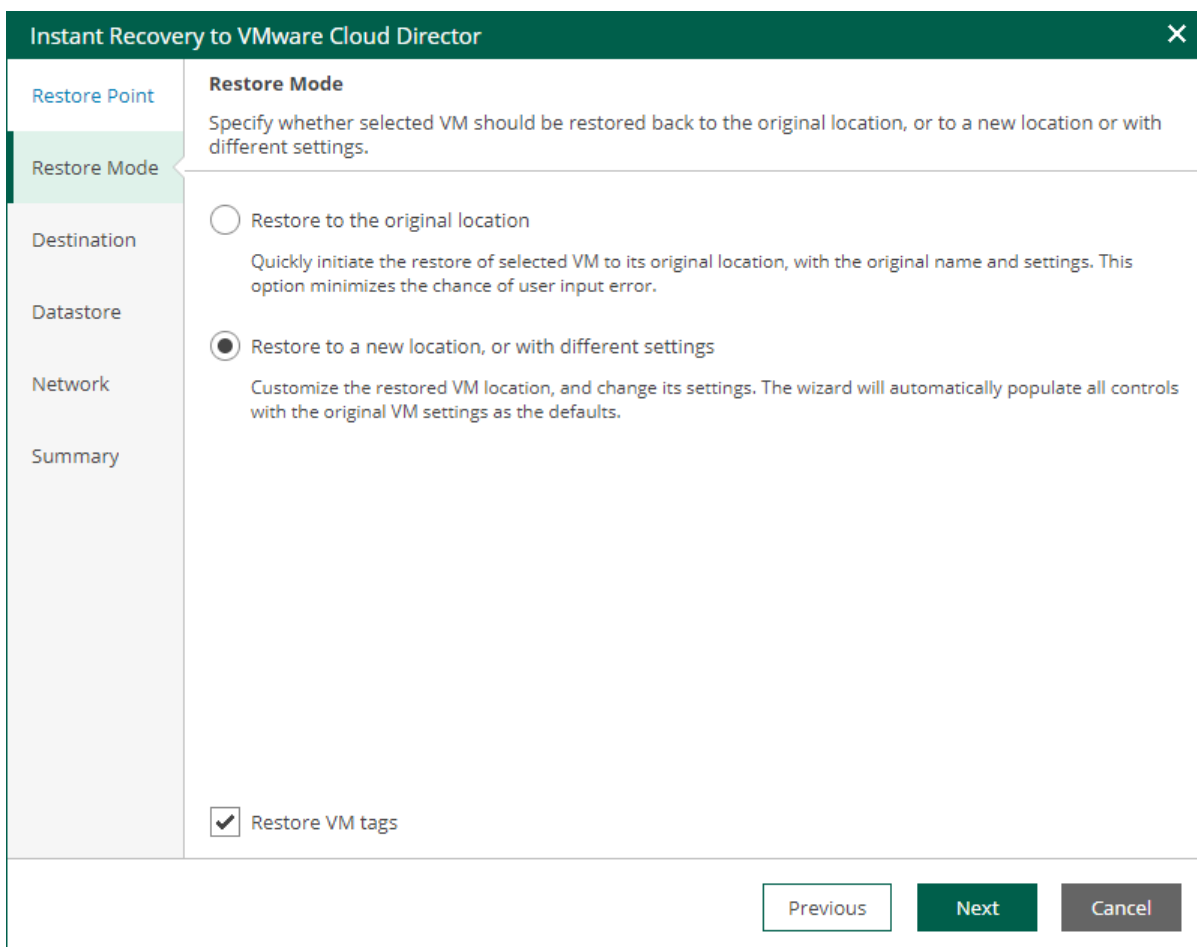
IMPORTANT

If you recover a VM with initial settings, and the original VM still exists in the virtual infrastructure, the original VM will be removed.

- Select **Restore to a new location or with different settings** to recover the VM to a new location, or to any location but with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.

2. If you want to recover tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will recover the VM with original tags if the following conditions are met:

- You recover a VM to the original location.
- The original VM tags are available on the source vCenter Server.



Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you recover a VM to a new location or with different settings.

At this step of the wizard, you configure destination settings such as the recovered VM name and target vApp.

1. In the **vApp** field, specify a vApp to which the VM must be recovered. By default, the original vApp is specified.
2. In the **Restored VM name** field, specify a name under which the VM will be recovered. By default, the original name of the VM is used. If you are restoring the VM to the same vApp where the original VM is registered and the original VM still resides there, change the VM name to avoid conflicts.

Instant Recovery to VMware Cloud Director [X]

Restore Point

Restore Mode

Destination

Datastore

Network

Summary

Destination

Specify vApp to restore the virtual machine to, and type in the restored VM's name.

vApp: vApp01 [Choose...](#)

Restored VM name:

linux04

Previous Next Cancel

Step 5. Specify Datastore

The **Datastore** step of the wizard is available if you recover a VM to a new location or with different settings.

At this step of the wizard, you can select where to store redo logs when a VM is running from the backup. Redo logs are auxiliary files used to keep changes that take place while the recovered VM runs.

By default, redo logs are stored in vPower NFS datastore. You can store redo logs in any datastore in the virtual environment if necessary. For more information on vPower NFS datastore, see the [vPower NFS Servise](#) section of the Veeam Backup & Replication User Guide.

To redirect redo logs, do the following:

1. Select the **Redirect write cache** check box.
2. Click **Choose** and select a datastore. You can select only a datastore that is available in the organization VDC hosting the vApp to which the VM is restored.

Instant Recovery to VMware Cloud Director

Restore Point

Restore Mode

Destination

Datastore

Network

Summary

Datastore

By default, virtual disk changes of recovered VM are stored on vPower NFS server. You can optionally redirect them to VMFS datastore for better performance.

Redirect write cache

Datastore: prgtwesx01-virt-ds1 [Choose...](#)

[Previous](#) [Next](#) [Cancel](#)

Step 6. Configure Network Mapping

The **Network** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can map a network in the original site to the network in the target site. During the restore process, Veeam Backup & Replication will update VM configuration files to replace the original networks with the specified networks in the target site. As a result, you will not have to re-configure network settings manually.

To change networks to which the restored VM will be connected:

1. From the **Network connections** list, select the necessary network.
2. Configure VM network mapping:
 - o To connect the restored VM to another network, do the following:
 - i. Click **Network**.
 - ii. In the **Select Network** window, select a necessary network and click **OK**.
 - o To disconnect the recovered VM from the network, click **Disconnect**.

The screenshot shows the 'Instant Recovery to VMware Cloud Director' wizard in the 'Network' step. The left sidebar contains navigation options: Restore Point, Restore Mode, Destination, Datastore, Network (selected), and Summary. The main area is titled 'Network' and includes the instruction: 'Specify the networks to connect restored virtual machine's vNICs to.' Below this, the VM name is 'linux02'. A 'Network connections' section has 'Network' and 'Disconnect' buttons. A table below shows the mapping:

Source	Target
Disconnected	Organization02 Network

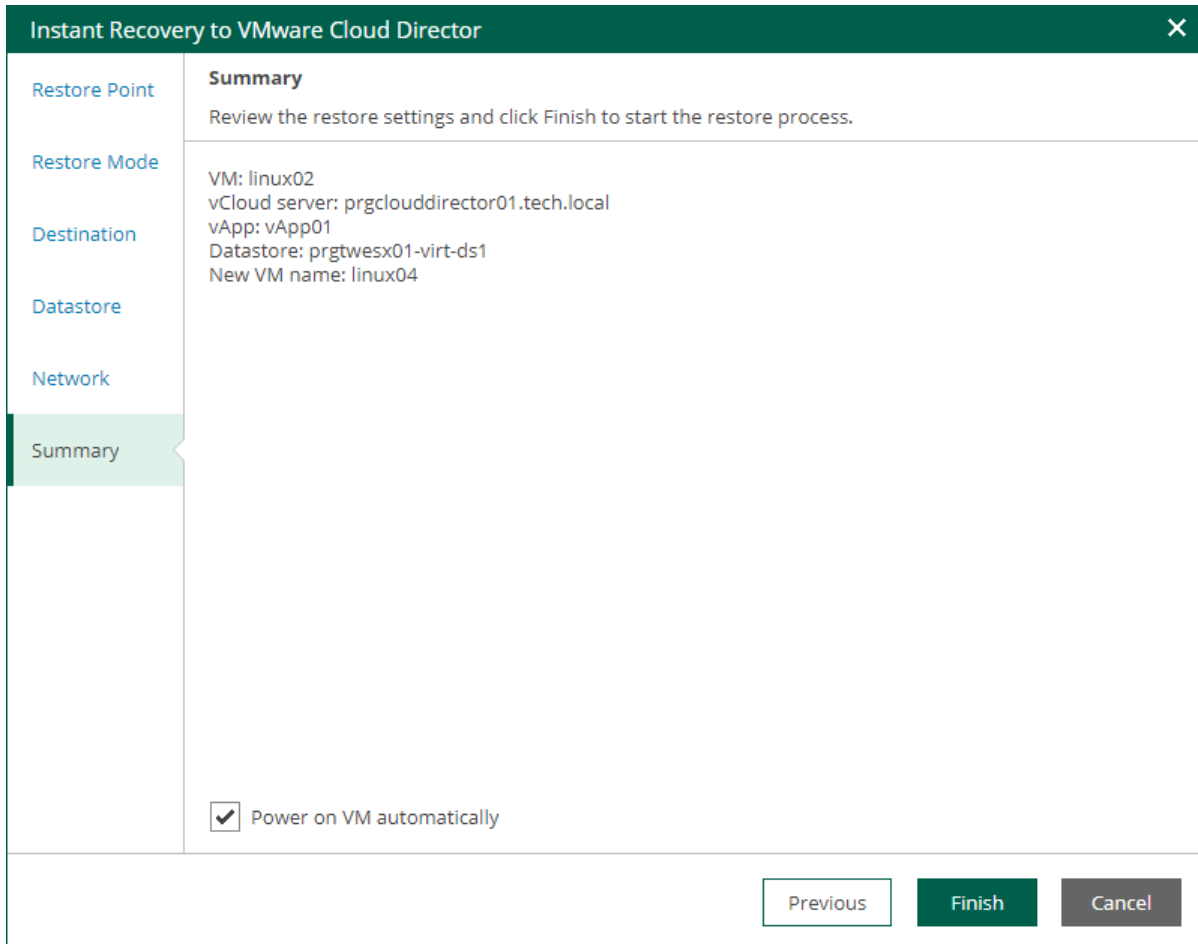
At the bottom right, there are three buttons: 'Previous' (disabled), 'Next' (active), and 'Cancel' (disabled).

Step 7. Review Recovery Settings

At the **Summary** step of the wizard, specify additional settings for Instant Recovery:

1. To start the VM right after recovery, select the **Power on target VM after restoring** check box. If you recover the workloads to the production network, make sure that the original VM is powered off.
2. Review settings that you have specified for Instant Recovery and click **Finish**.

To view the Instant Recovery progress, on the **Machines** tab, click **History**.



The screenshot shows a wizard window titled "Instant Recovery to VMware Cloud Director" with a close button (X) in the top right corner. The window is divided into a left sidebar and a main content area. The sidebar contains the following items: "Restore Point", "Restore Mode", "Destination", "Datastore", "Network", and "Summary". The "Summary" item is highlighted with a green bar. The main content area is titled "Summary" and contains the following text: "Review the restore settings and click Finish to start the restore process." Below this, the following settings are listed: "VM: linux02", "vCloud server: prgclouddirector01.tech.local", "vApp: vApp01", "Datastore: prgtwesx01-virt-ds1", and "New VM name: linux04". At the bottom of the main content area, there is a checked checkbox labeled "Power on VM automatically". At the bottom of the wizard window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

What You Do Next

After you have performed instant file share recovery, you have to finalize it. For more information, see [Finalizing Instant Recovery to VMware Cloud Director](#).

Finalizing Instant Recovery to VMware Cloud Director

After you have performed instant recovery, you have to finalize the process. For this, test the recovered VMs and decide whether to migrate them to production environment or stop publishing.

Until you finalize instant recovery of all recovered VMs, a notification about running instant recovery sessions is displayed on the **Dashboard** tab.

Testing Recovered VM

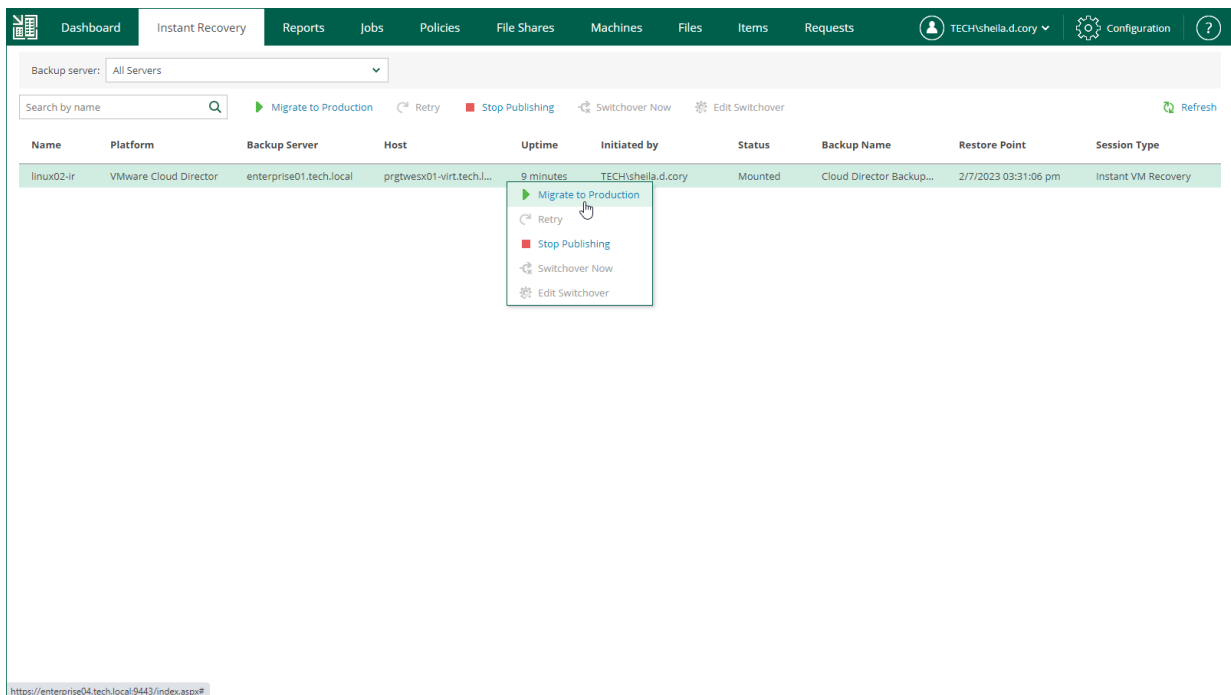
To test a recovered VM before you migrate it to production, you can launch the VMware Remote Console software from the Veeam Backup & Replication console. For more information, see the [Finalizing Instant Recovery to VMware vSphere](#) section of the Veeam Backup & Replication User Guide.

Migrating Recovered VM

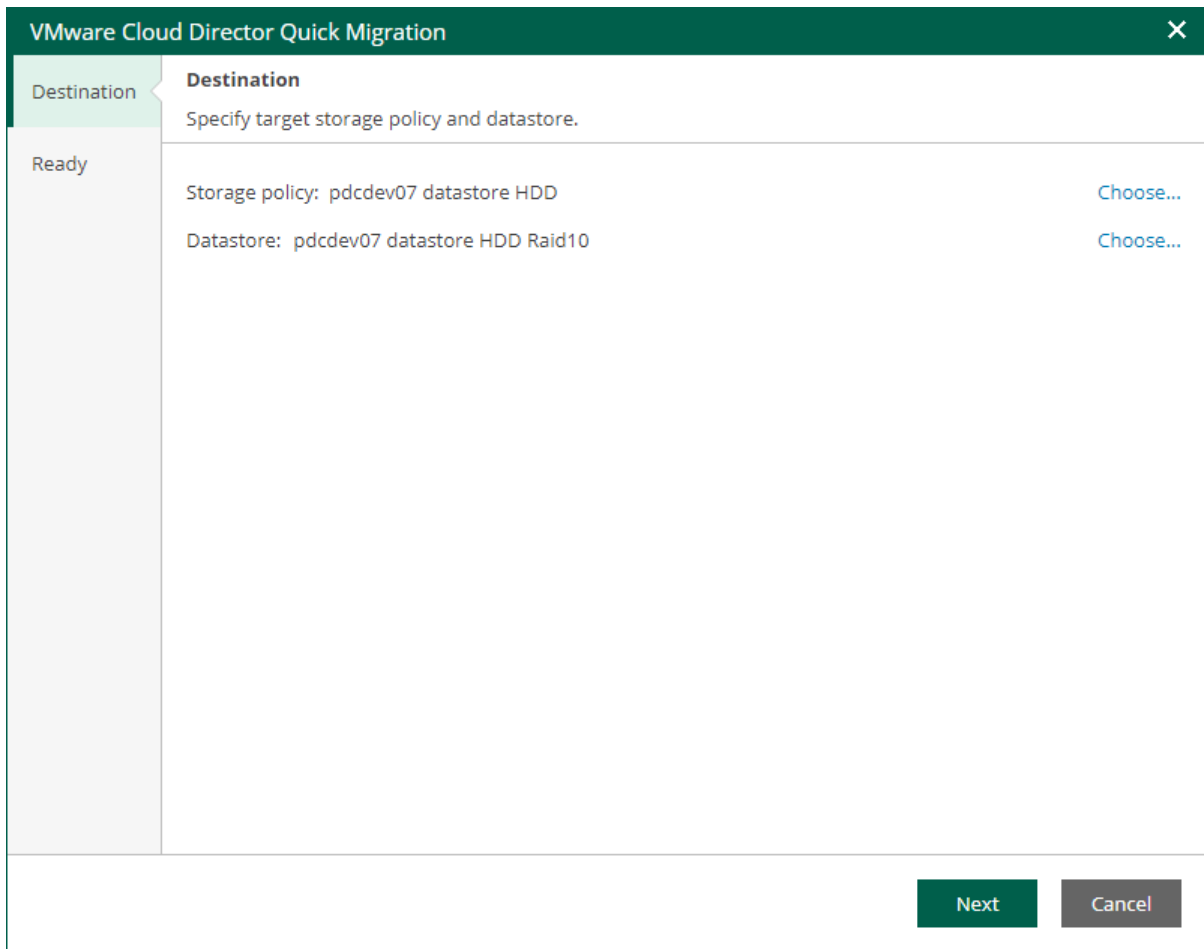
If a VM is recovered successfully, you can migrate it to the production environment.

To migrate a recovered VM to production, do the following:

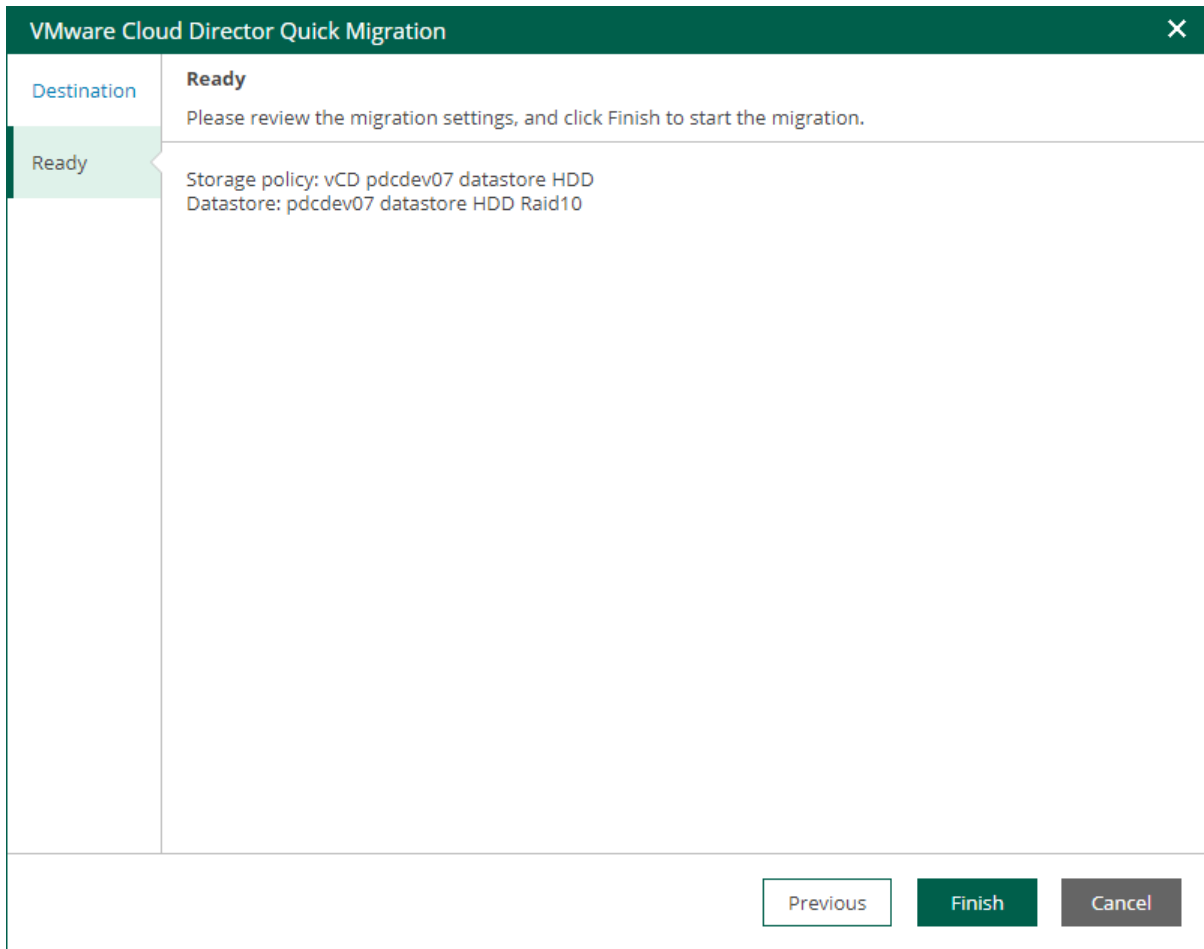
1. Open the **Instant Recovery** tab and select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Migrate to production**.



3. At the **Destination** step of the **VMware Cloud Director Quick Migration** wizard, specify a VM storage policy and a datastore. You can choose from the storage policies and datastores that are available in the organization VDC hosting the vApp to which the VM is recovered.



4. At the **Ready** step of the wizard, review migration settings and click **Finish**.



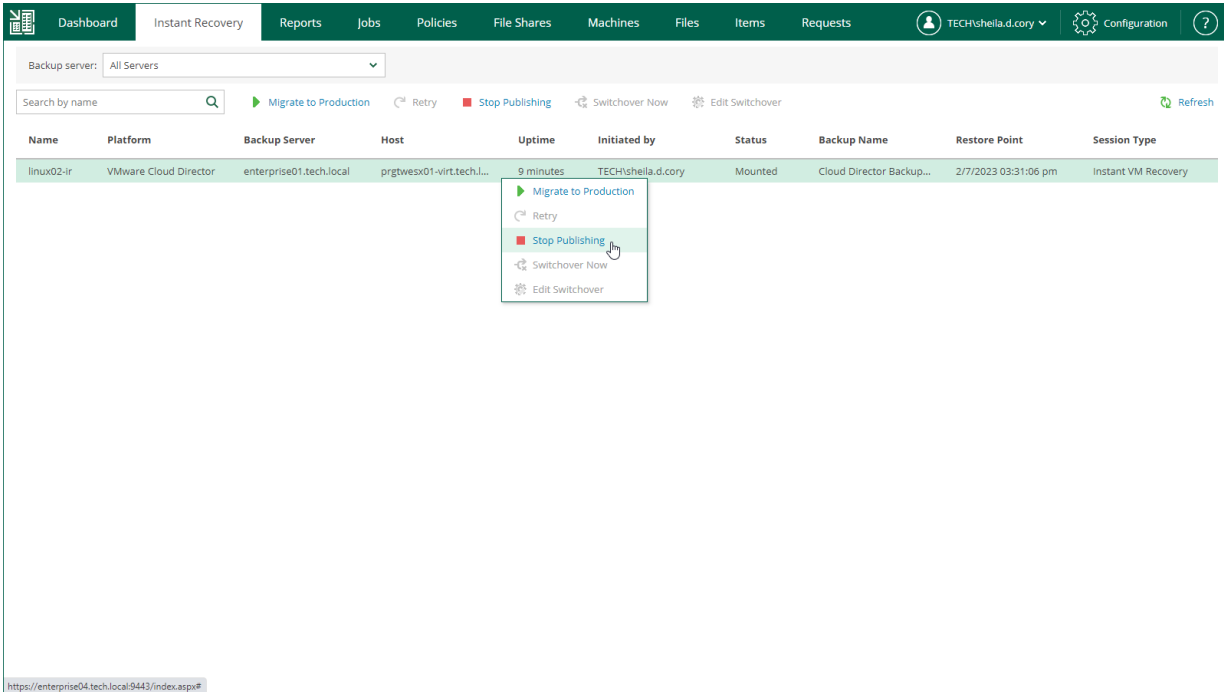
To view the migration progress, on the **Machines** tab, click **History**.

Unpublishing Recovered VM

If your tests have failed, you can stop publishing the recovered VM. This will remove the recovered VM from the host that you selected as the destination for recovery. Note that all changes made in the recovered VMs will be lost.

To remove a recovered VM, do the following:

1. Open the **Instant Recovery** tab and select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Stop Publishing**.



Instant Recovery to Microsoft Hyper-V

Veeam Backup Enterprise Manager allows you to instantly recover Microsoft Hyper-V VMs to Microsoft Hyper-V. You can recover VMs from backups to the original location or a new location included in your restore scope. After you have performed Instant Recovery, you must finalize it. For more information, see [Finalizing Instant Recovery to Microsoft Hyper-V](#).

For more information on Instant Recovery, see the [Instant Recovery to Microsoft Hyper-V](#) of the Veeam Backup & Replication User Guide.

Performing Instant Recovery to Microsoft Hyper-V

To instantly recover a VM, use the **Instant Recovery to Microsoft Hyper-V** wizard.

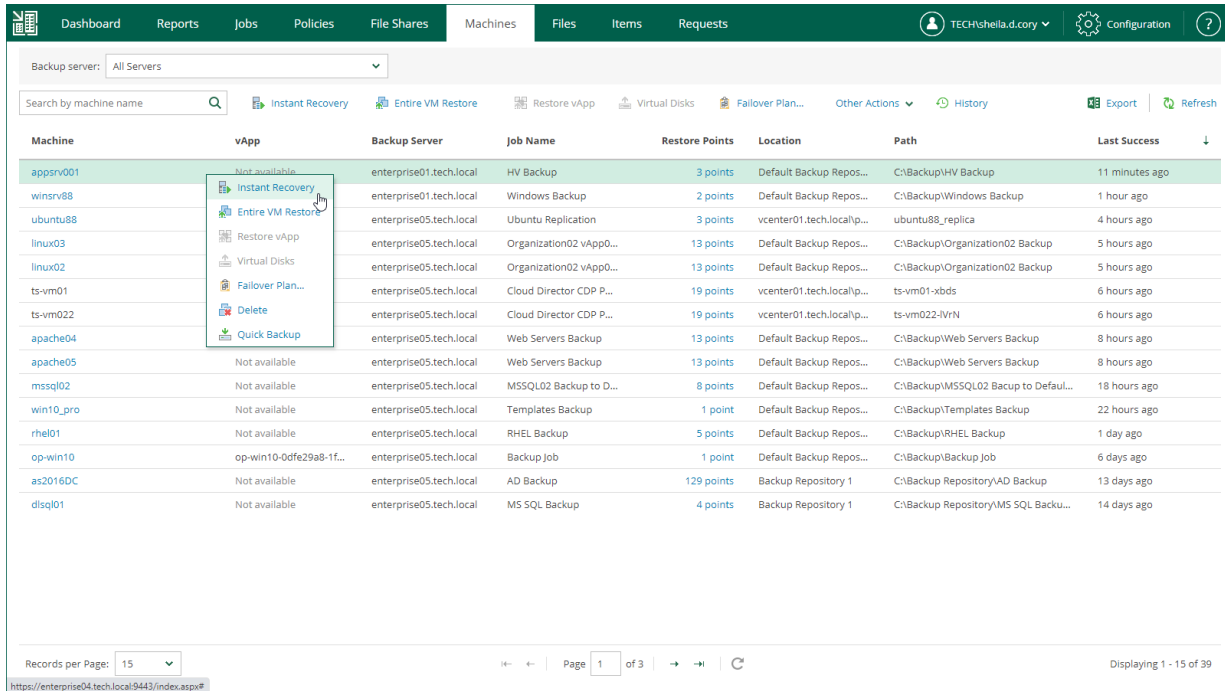
1. [Launch the Instant Recovery wizard](#).
2. [Select a restore point](#).
3. [Select a recovery mode](#).
4. [Specify destination settings for the recovered VM](#).
5. [Specify a target datastore](#).
6. [Configure network mapping](#).
7. [Review the recovery settings](#).

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery to Microsoft Hyper-V** wizard, do the following:

1. On the **Machines** tab, select the necessary Hyper-V VM from the list.
2. On the toolbar, click **Instant Recovery**.

Alternatively, you can right-click the VM and select **Instant Recovery**.



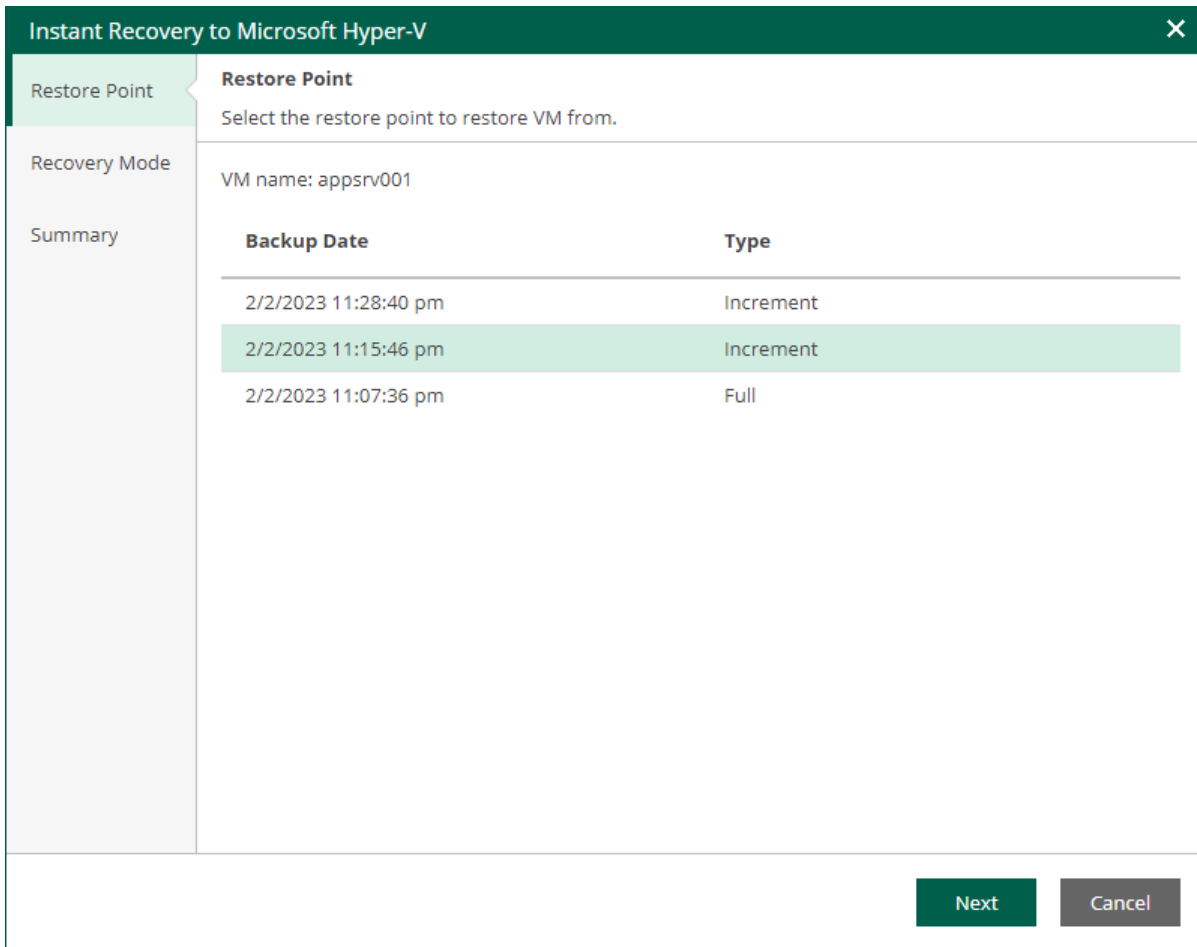
The screenshot shows the Veeam Backup Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECH\shella.d.cory. The main area displays a table of machines with a context menu open over the 'appsrv001' machine. The context menu options are: Instant Recovery, Entire VM Restore, Restore vApp, Virtual Disks, Failover Plan..., Delete, and Quick Backup. The table below shows the following data:

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
appsrv001	Not available	enterprise01.tech.local	HV Backup	3 points	Default Backup Repos...	C:\Backup\HV Backup	11 minutes ago
winsrv88	enterprise01.tech.local	enterprise01.tech.local	Windows Backup	2 points	Default Backup Repos...	C:\Backup\Windows Backup	1 hour ago
ubuntu88	enterprise05.tech.local	enterprise05.tech.local	Ubuntu Replication	3 points	vcenter01.tech.local/p...	ubuntu88_replica	4 hours ago
linux03	enterprise05.tech.local	enterprise05.tech.local	Organization02 vApp0...	13 points	Default Backup Repos...	C:\Backup\Organization02 Backup	5 hours ago
linux02	enterprise05.tech.local	enterprise05.tech.local	Organization02 vApp0...	13 points	Default Backup Repos...	C:\Backup\Organization02 Backup	5 hours ago
ts-vm01	enterprise05.tech.local	enterprise05.tech.local	Cloud Director CDP P...	19 points	vcenter01.tech.local/p...	ts-vm01-xbds	6 hours ago
ts-vm022	enterprise05.tech.local	enterprise05.tech.local	Cloud Director CDP P...	19 points	vcenter01.tech.local/p...	ts-vm022-IVN	6 hours ago
apache04	enterprise05.tech.local	enterprise05.tech.local	Web Servers Backup	13 points	Default Backup Repos...	C:\Backup\Web Servers Backup	8 hours ago
apache05	Not available	enterprise05.tech.local	Web Servers Backup	13 points	Default Backup Repos...	C:\Backup\Web Servers Backup	8 hours ago
mssql02	enterprise05.tech.local	enterprise05.tech.local	MSSQL02 Backup to D...	8 points	Default Backup Repos...	C:\Backup\MSSQL02 Backup to Defaul...	18 hours ago
win10_pro	enterprise05.tech.local	enterprise05.tech.local	Templates Backup	1 point	Default Backup Repos...	C:\Backup\Templates Backup	22 hours ago
rhel01	enterprise05.tech.local	enterprise05.tech.local	RHEL Backup	5 points	Default Backup Repos...	C:\Backup\RHEL Backup	1 day ago
op-win10	op-win10-0dfe29a8-1f...	enterprise05.tech.local	Backup Job	1 point	Default Backup Repos...	C:\Backup\Backup Job	6 days ago
as2016DC	enterprise05.tech.local	enterprise05.tech.local	AD Backup	129 points	Backup Repository 1	C:\Backup\Repository\AD Backup	13 days ago
dlsq01	enterprise05.tech.local	enterprise05.tech.local	MS SQL Backup	4 points	Backup Repository 1	C:\Backup\Repository\MSS SQL Backu...	14 days ago

Records per Page: 15 | Page 1 of 3 | Displaying 1 - 15 of 39

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point from which you want to perform instant recovery.



Instant Recovery to Microsoft Hyper-V [Close]

Restore Point
Select the restore point to restore VM from.

Recovery Mode
VM name: appsrv001

Summary

Backup Date	Type
2/2/2023 11:28:40 pm	Increment
2/2/2023 11:15:46 pm	Increment
2/2/2023 11:07:36 pm	Full

Next Cancel

Step 3. Select Recovery Mode

At the **Restore mode** step, select a recovery mode for the VM.

- Select **Restore to the original location** to recover the VM with initial settings to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

IMPORTANT

If you recover a VM with the original settings, and the original VM still exists in the virtual infrastructure, the original VM will be removed.

- Select **Restore to a new location or with different settings** to recover the VM to a new location, or to any location but with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.

The screenshot shows a wizard window titled "Instant Recovery to Microsoft Hyper-V" with a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: "Restore Point", "Recovery Mode" (highlighted in green), "Destination", "Datastore", "Network", and "Summary". The main content area is titled "Recovery Mode" and contains the following text: "Specify whether selected objects should be restored back to the original location, or to a new location or with different settings." Below this text are two radio button options: 1. "Restore to the original location" with a description: "Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error." 2. "Restore to a new location, or with different settings" (selected with a black dot) with a description: "Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults." At the bottom right of the window are three buttons: "Previous" (disabled), "Next" (active), and "Cancel" (disabled).

Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you recover a VM to a new location or with different settings.

To configure destination settings, do the following:

1. In the **Restored VM name** field, specify a name under which the workload will be recovered.
2. In the **Host** field, specify a host on which the VM will run.
3. If the specified host is a node of a Hyper-V failover cluster, you can register the recovered VM as a cluster resource by selecting the **Register VM as a cluster resource** check box. If the target host is brought offline or fails for any reason, the VM will fail over to another node in the cluster.

The check box is not displayed if the host is not a cluster node.

4. Choose whether to preserve the virtual machine ID or generate a new one.
 - Select **Preserve virtual machine ID** if the original VM no longer exists, for example, if it was deleted. In this case, it is not required to change the ID.
 - Select **Generate new virtual machine ID** if the original workload still resides in the production environment. This will prevent conflicts.

The screenshot shows the 'Instant Recovery to Microsoft Hyper-V' wizard window. The 'Destination' step is selected in the left-hand navigation pane. The main area contains the following fields and options:

- Destination** (Section Header): Select the host to recover machine to, specify the new virtual machine name, and whether you would like unique identifier to be preserved.
- Restored VM name:** Text input field containing 'appsrv001_ir'.
- Host:** Text input field containing 'pdctwhv02' with a 'Choose...' button to its right.
- Register VM as a cluster resource**
- Preserve virtual machine ID (recommended)**
Keep ID when restoring the existing virtual machine to avoid reconfiguring applications that match VM by ID.
- Generate new virtual machine ID**
Use this option if you are using restore to clone the virtual machine to prevent conflicts with the existing VM.

At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Step 5. Specify Datastore

The **Datastore** step of the wizard is available if you recover a VM to a new location or with different settings.

At this step of the wizard, you can change default paths where VM configuration files and disk files will be stored.

To change a default path, do the following:

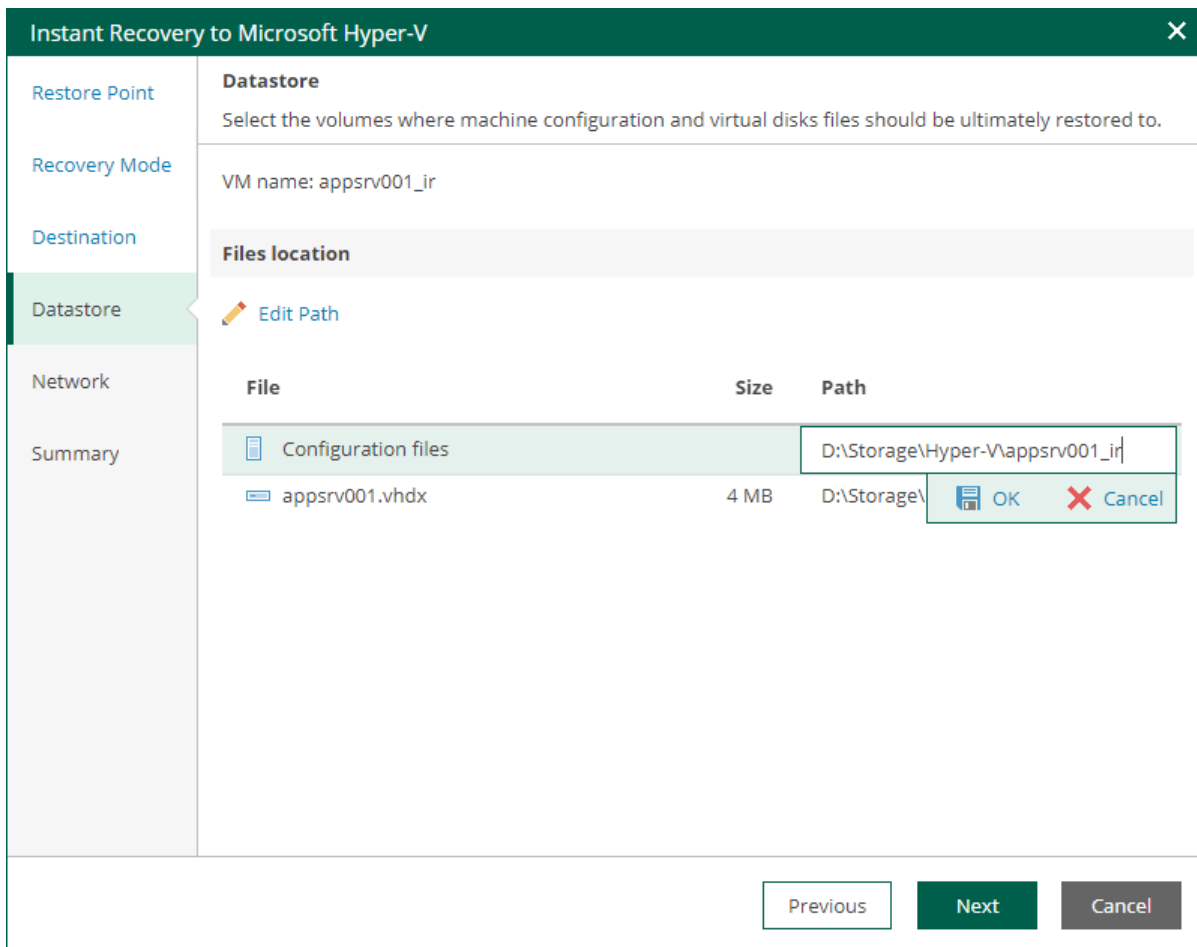
1. Select the configuration files or one of the disk files and click **Edit Path**.

Alternatively, you can double-click a file to edit its path.

2. Type in a path to the folder where the files will be stored. You can specify an existing folder, a new folder or an SMB3 shared folder. SMB3 shared folder path must be in the UNC format, for example: `||172.16.11.38|Share01`.

The host or cluster on which you register VMs must have access to the specified SMB3 shared folder. If you are using SCVMM 2012 or later, the server hosting the Microsoft SMB3 shared folder must be registered in SCVMM as a storage device. For more information, see [Microsoft Docs](#).

3. Click **OK** to apply the changes.



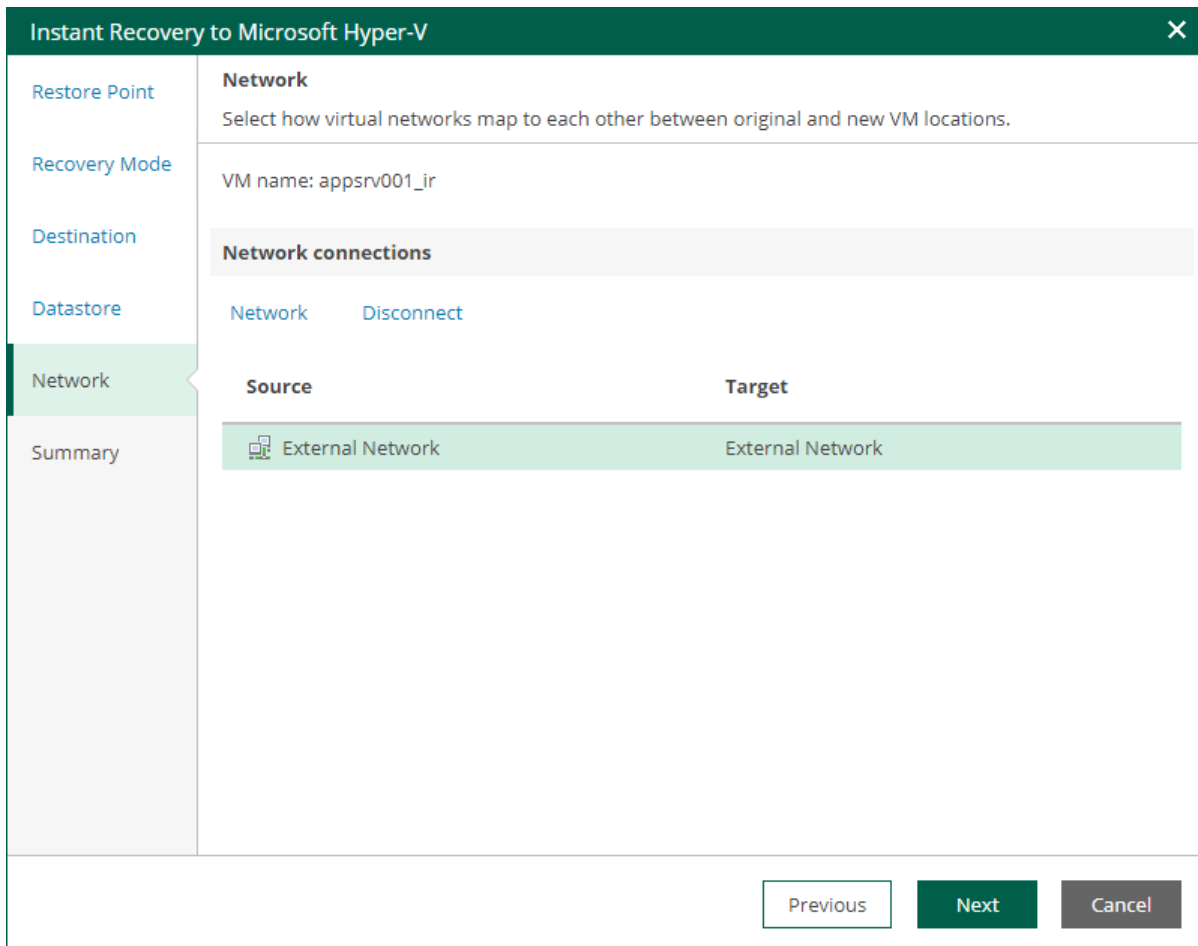
Step 6. Configure Network Mapping

The **Network** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can map a network in the original site to the network in the target site. During the restore process, Veeam Backup & Replication will update VM configuration files to replace the original networks with the specified networks in the target site. As a result, you will not have to re-configure network settings manually.

To change networks to which the restored VM will be connected:

1. From the **Network connections** list, select the necessary network.
2. Configure VM network mapping:
 - o To connect the restored VM to another network, do the following:
 - i. Click **Network**.
 - ii. In the **Select Network** window, select a necessary network and click **OK**.
 - o To disconnect the recovered VM from the network, click **Disconnect**.

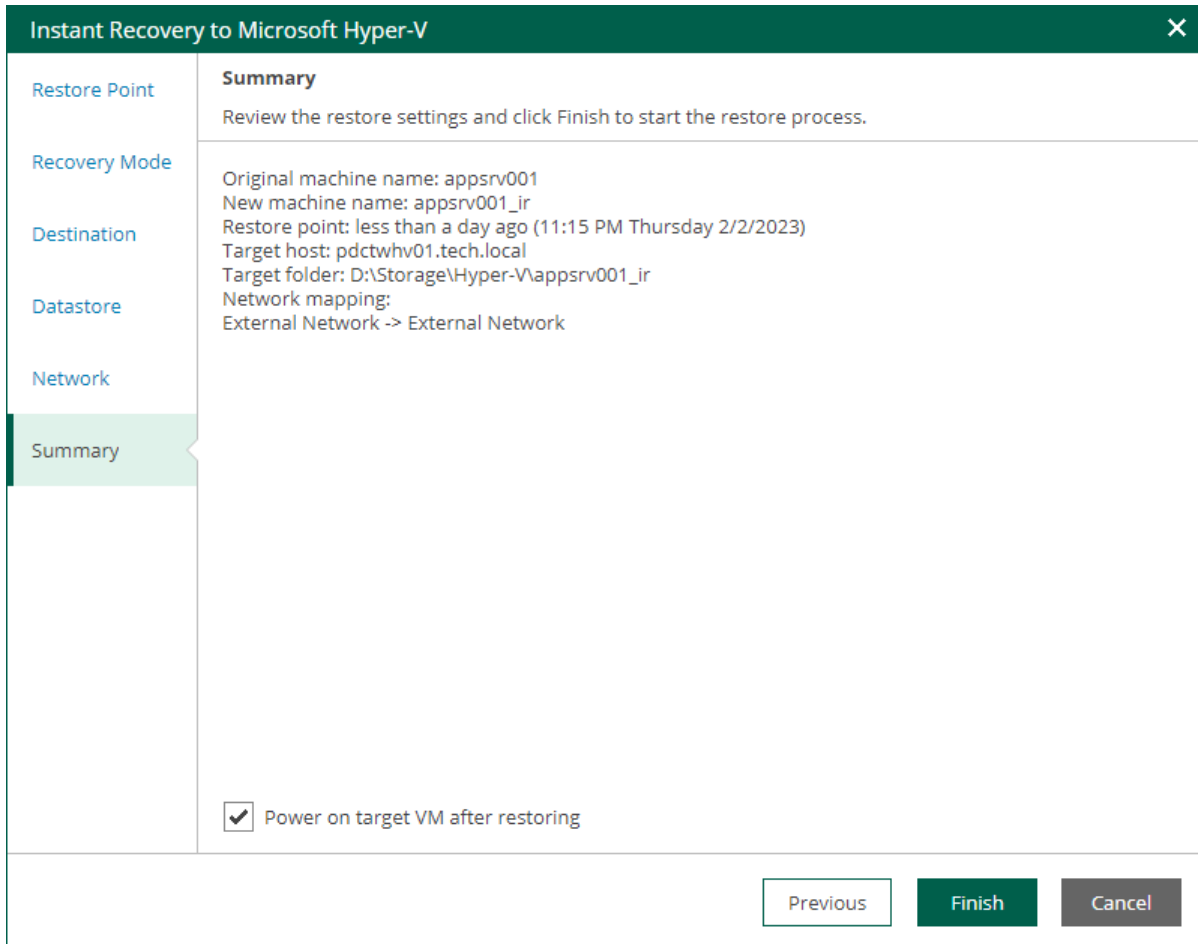


Step 7. Review Recovery Settings

At the **Summary** step of the wizard, do the following:

1. To start the VM right after recovery, select the **Power on target VM after restoring** check box. If you recover the workloads to the production network, make sure that the original VM is powered off.
2. Review settings that you have specified for instant recovery and click **Finish**.

To view the Instant Recovery progress, on the **Machines** tab, click **History**.



The screenshot shows a wizard window titled "Instant Recovery to Microsoft Hyper-V" with a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: "Restore Point", "Recovery Mode", "Destination", "Datastore", "Network", and "Summary". The "Summary" item is highlighted with a green background. The main content area is titled "Summary" and contains the following text: "Review the restore settings and click Finish to start the restore process." Below this, the following details are listed: "Original machine name: appsrv001", "New machine name: appsrv001_ir", "Restore point: less than a day ago (11:15 PM Thursday 2/2/2023)", "Target host: pdctwhv01.tech.local", "Target folder: D:\Storage\Hyper-V\appsrv001_ir", and "Network mapping: External Network -> External Network". At the bottom of the main area, there is a checked checkbox labeled "Power on target VM after restoring". At the bottom right of the window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

What You Do Next

After you have performed instant recovery, you have to finalize it. For more information, see [Finalizing Instant Recovery to Microsoft Hyper-V](#).

Finalizing Instant Recovery to Microsoft Hyper-V

After you have performed instant recovery, you have to finalize the process. For this, test the recovered VMs and decide whether to migrate them to production environment or stop publishing.

Until you finalize instant recovery of all recovered VMs, a notification about running instant recovery sessions is displayed on the **Dashboard** tab.

Testing Recovered VM

To test a recovered VM before you migrate it to production, you can launch the VM console from Veeam Backup & Replication or open the console from the Hyper-V client. For more information, see the [Finalizing Instant Recovery to Microsoft Hyper-V](#) section of the Veeam Backup & Replication User Guide.

Migrating Recovered VM

When Veeam Backup & Replication migrates VMs, it transfers VM disks data to the production storage that you have selected as a destination for the recovered VMs.

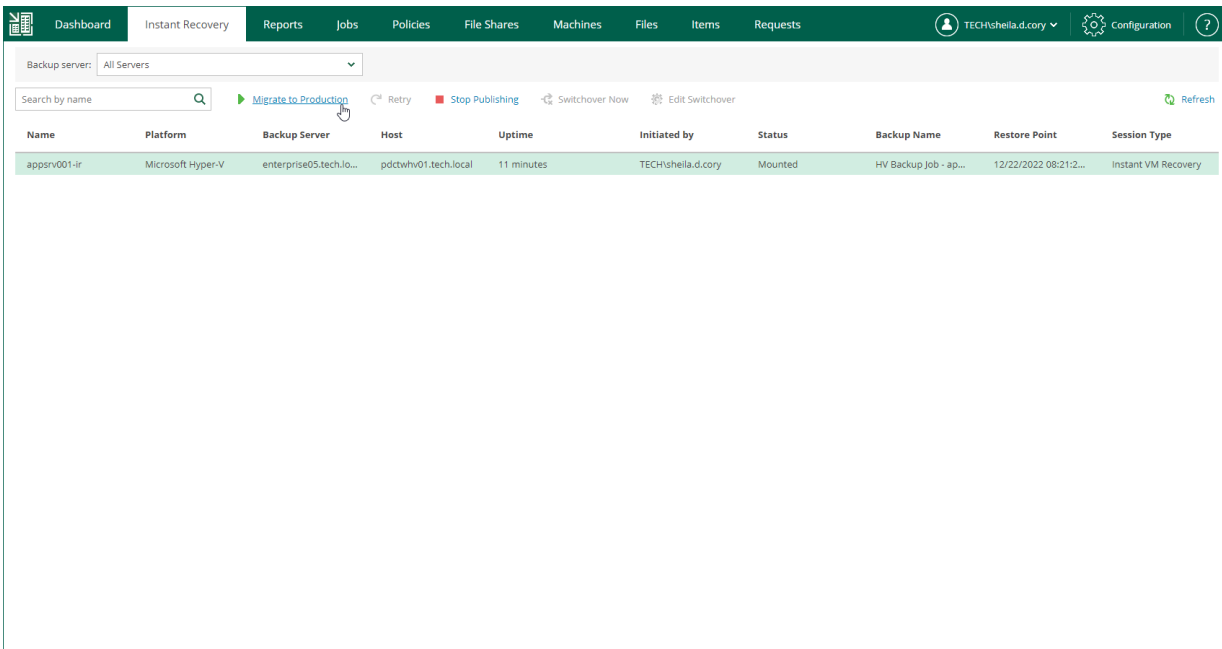
NOTE

After the migration is finished, the original VM still remains if the destination differs from the original location. If you do not need the VM, you have to manually remove it using the Hyper-V client.

To migrate a recovered VM to production, do the following:

1. Open the **Instant Recovery** tab and select the necessary Hyper-V VM from the list.
2. On the toolbar, click **Migrate to production**.

To view the migration progress, on the **Machines** tab, click **History**.



The screenshot shows the Veeam Backup & Replication interface. The top navigation bar includes 'Dashboard', 'Instant Recovery', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The 'Instant Recovery' tab is active. Below the navigation bar, there is a search bar and a toolbar with buttons: 'Migrate to Production', 'Retry', 'Stop Publishing', 'Switchover Now', 'Edit Switchover', and 'Refresh'. A table lists the recovered VMs with the following columns: Name, Platform, Backup Server, Host, Uptime, Initiated by, Status, Backup Name, Restore Point, and Session Type. The table contains one entry: 'appsrv001-ir' on a 'Microsoft Hyper-V' platform, backed up by 'enterprise05.tech.lo...', hosted on 'pdctwhv01.tech.local', with an uptime of '11 minutes', initiated by 'TECH\sheila.d.cory', with a status of 'Mounted', backup name 'HV Backup Job - ap...', restore point '12/22/2022 08:21:2...', and session type 'Instant VM Recovery'.

Name	Platform	Backup Server	Host	Uptime	Initiated by	Status	Backup Name	Restore Point	Session Type
appsrv001-ir	Microsoft Hyper-V	enterprise05.tech.lo...	pdctwhv01.tech.local	11 minutes	TECH\sheila.d.cory	Mounted	HV Backup Job - ap...	12/22/2022 08:21:2...	Instant VM Recovery

Unpublishing Recovered VM

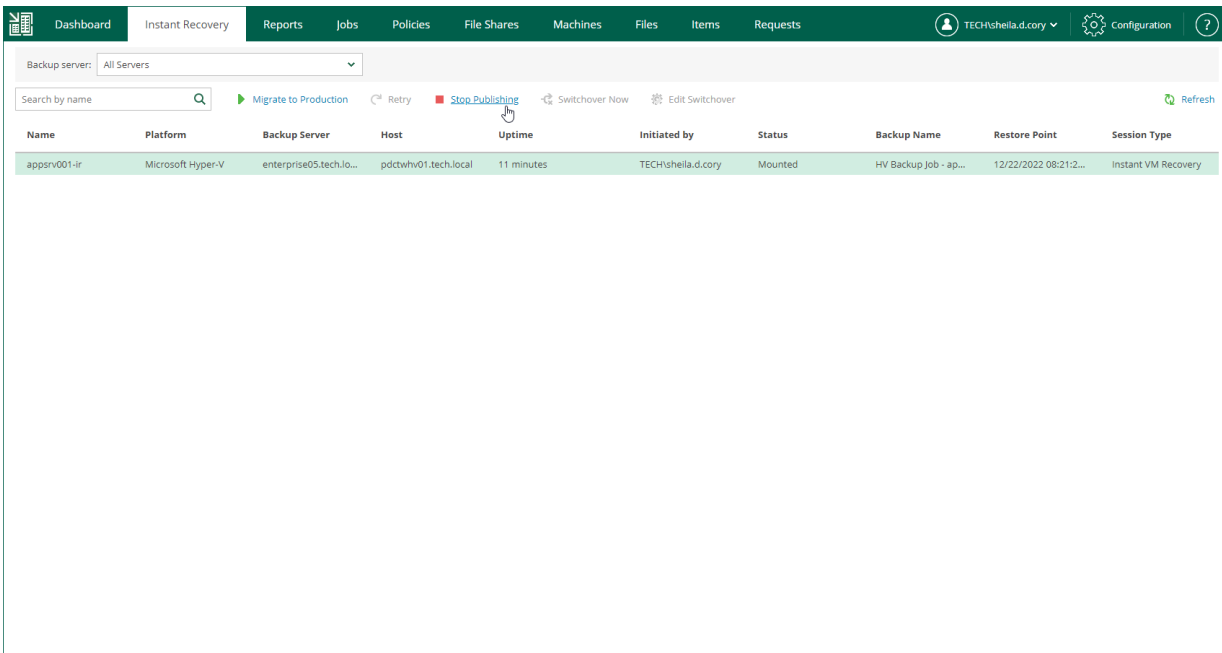
If you have ensured that the VM is working and you do not need it anymore, or your tests have failed, you can stop publishing the recovered VM. This will remove the recovered VM from the storage that you selected as the destination for recovery. Note that all changes made in the recovered VM will be lost.

IMPORTANT

If the destination is the original location, both the original and recovered VMs are removed.

To remove a recovered VM, do the following:

1. Open the **Instant Recovery** tab and select the necessary Hyper-V VM from the list.
2. On the toolbar, click **Stop Publishing**.



Entire VM Restore

Authorized users can restore entire VMs from backups to the original location or a new location included in their restore scope. Users with the Portal Administrator role have no scope limitations. For more information on restore scope, see [Configuring Restore Scope](#).

Veeam Backup Enterprise Manager supports the following scenarios of entire VM restore:

- [Restoring a VMware vSphere VM to VMware vSphere](#)
- [Restoring a VMware Cloud Director VM to VMware Cloud Director](#)
- [Restoring a Microsoft Hyper-V VM to Microsoft Hyper-V](#)

Before You Begin

Before you perform entire VM restore, consider the following:

- Entire VM Restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Veeam Backup Enterprise Manager does not support entire VM Restore from storage snapshots, Veeam Agent backups and backups created with Veeam Plug-ins for Enterprise Applications.

Restoring Entire VM to VMware vSphere

Veeam Backup Enterprise Manager allows you to restore VMware vSphere VMs to VMware vSphere. You can restore VMs from backups to the original location or a new location included in your restore scope.

For more information on entire VM restore of VMware vSphere VMs, see the [Entire VM Restore](#) section of the Veeam Backup & Replication User Guide.

To restore an entire VM, use the **Entire VM Restore** wizard.

1. [Launch the Entire VM Restore wizard.](#)
2. [Select a restore point.](#)
3. [Select a restore mode.](#)
4. [Specify destination settings for the recovered VM.](#)
5. [Specify a target datastore.](#)
6. [Configure network mapping.](#)
7. [Review the recovery settings.](#)

Step 1. Launch Entire VM Restore Wizard

To launch the **Entire VM Restore** wizard, do the following:

1. Open the **Machines** tab and select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Restore**.

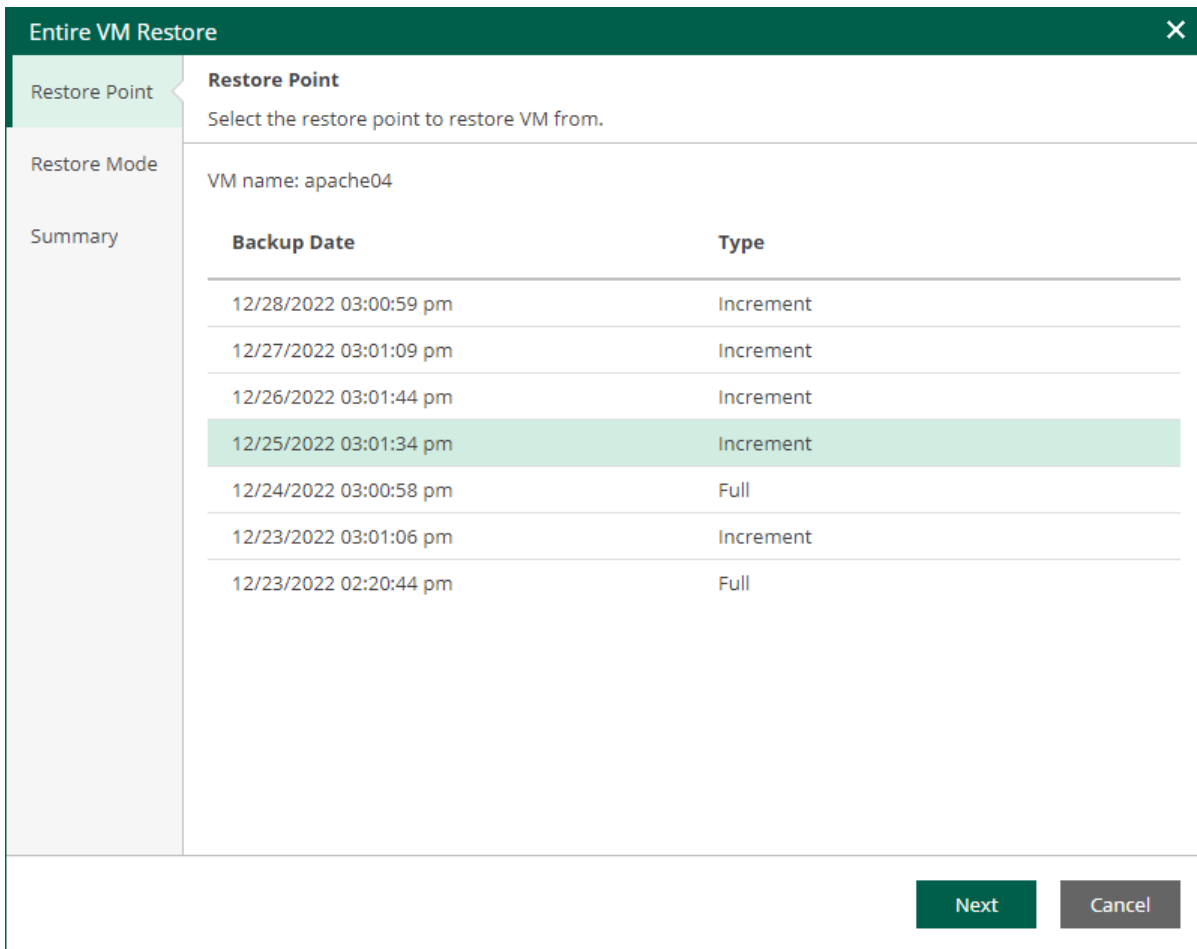
Alternatively, you can right-click the VM and select **Entire VM Restore**.

The screenshot shows the Veeam Backup Enterprise Manager interface. The 'Machines' tab is active, displaying a table of machines. A context menu is open over the 'apache04' machine, with 'Entire VM Restore' selected. The table columns are: Machine, vApp, Backup Server, Job Name, Restore Points, Location, Path, and Last Success. The table contains 20 rows of machine data. At the bottom, there is a pagination bar showing 'Page 1 of 3' and 'Displaying 1 - 15 of 32'.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
apache05	Not available	enterprise05.tech.local	Web Servers Backup	7 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	2 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	7 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	2 hours ago
rhel01	Not available	tech.local	Backup Copy Job 11RHE...	3 points	Backup Repository 1	C:\Backup\Repository\Backup Copy Job ...	10 hours ago
rhel01	Not available	tech.local	RHEL Backup	4 points	Default Backup Reposit...	C:\Backup\RHEL Backup	10 hours ago
linux03	vApp02	tech.local	Organization02 vApp02 ...	7 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	23 hours ago
linux02	vApp02	tech.local	Organization02 vApp02 ...	7 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	23 hours ago
disql01	Not available	tech.local	MS SQL Backup	7 points	Backup Repository 1	C:\Backup\Repository\MS SQL Backup_1	1 day ago
virt01-vm33	Not available	tech.local	CDP Policy for Servers	13 points	vcenter01.tech.local/prg...	virt01-vm33_cdp_replica	1 day ago
ts-vm022	vApp-TS	tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local/prg...	ts-vm022-XXvUK	1 day ago
ts-vm01	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local/prg...	ts-vm01-e6e3	1 day ago
linorcl01	Not available	enterprise05.tech.local	Oracle Linux Backup	6 points	Backup Repository 1	C:\Backup\Repository\Oracle Linux Back...	1 day ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	5 points	Backup Repository 1	C:\Backup\Repository\AD Backup	1 day ago
appsvr001	Not available	enterprise05.tech.local	HV Backup Job	3 points	Backup Repository 1	C:\Backup\Repository\HV Backup Job	3 days ago
winorcl01	Not available	enterprise05.tech.local	Windows Oracle Backup	1 point	Backup Repository 1	C:\Backup\Repository\Oracle Backup	92 days ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	3 points	Backup Repository 1	C:\Backup\Repository\MS SQL Backup_1	100 days ago

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point for which you want to perform entire VM restore.



The screenshot shows a window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left side, there is a vertical navigation pane with three items: "Restore Point" (highlighted in light green), "Restore Mode", and "Summary". The main content area is divided into sections:

- Restore Point:** Contains the instruction "Select the restore point to restore VM from."
- Restore Mode:** Displays "VM name: apache04".
- Summary:** Contains a table of backup points.

Backup Date	Type
12/28/2022 03:00:59 pm	Increment
12/27/2022 03:01:09 pm	Increment
12/26/2022 03:01:44 pm	Increment
12/25/2022 03:01:34 pm	Increment
12/24/2022 03:00:58 pm	Full
12/23/2022 03:01:06 pm	Increment
12/23/2022 02:20:44 pm	Full

At the bottom right of the window, there are two buttons: "Next" (green) and "Cancel" (grey).

Step 3. Select Restore Mode

At the **Restore mode** step, specify a destination for VM recovery and select whether you want to recover VM tags.

When you perform entire VM restore using Veeam Backup Enterprise Manager, Veeam Backup & Replication automatically selects a backup proxy over which VM data must be transported to the source datastore. You can select a backup proxy manually from the **Entire VM Restore** wizard in the Veeam Backup & Replication console. For more information, see the [Select Restore Mode](#) section of the Veeam Backup & Replication User Guide.

1. Select a restore mode:
 - **Restore to the original location** – select this option to restore the VM with initial settings and to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

During restore to the original location, Veeam Backup & Replication restores only those disks that are included in the backup file. This means that after the restore finishes, you do not have to update existing jobs which process the original VMs.
 - **Restore to a new location, or with different settings** – select this option to restore the VM to a new location, or to any location but with different settings. If this option is selected, the **Entire VM Restore** wizard will include additional steps for customizing VM settings.

During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication deletes the original VMs. In this case, you must edit existing jobs to exclude original VMs from them.

NOTE

If you need to run an executable script for the VM before restoring it to the production environment, you can use the Veeam Backup & Replication console to perform entire VM restore in the Staged restore mode. For more information, see the [Select Restore Mode](#) section of the Veeam Backup & Replication User Guide.

2. If you want to restore tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
 - You restore a VM to the original location.
 - The original VM tags are available on the source vCenter Server.
3. [For VM restore to the original location] Select the **Quick rollback** check box to perform incremental restore for the VM. Veeam Backup & Replication will query Changed Block Tracking to get data blocks that are required to revert the VM to the restore point, and will restore only these data blocks. Quick rollback significantly reduces the restore time and has little impact on the production environment.

Enable this option if you restore a VM after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.

For more information on quick rollback, its requirements and limitations, see the [Quick Rollback](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows the 'Entire VM Restore' wizard window. The title bar is dark green with a close button (X) on the right. On the left is a vertical navigation pane with the following items: 'Restore Point', 'Restore Mode' (highlighted in light green), 'Destination', 'Datastore', 'Network', and 'Summary'. The main content area is titled 'Restore Mode' and contains the following text: 'Specify whether selected VM should be restored back to the original location, or to a new location or with different settings.' Below this are two radio button options: 'Restore to the original location' (unselected) and 'Restore to a new location, or with different settings' (selected). The 'Restore to a new location...' option has a descriptive paragraph: 'Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.' Below the radio buttons are two checkboxes: 'Restore VM tags' (checked) and 'Quick rollback (restore changed blocks only)' (unchecked). The 'Quick rollback' option has a descriptive paragraph: 'Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.' At the bottom right of the window are three buttons: 'Previous' (white), 'Next' (dark green), and 'Cancel' (grey).

Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you configure destination settings such as a name of the restored VM, target host, VM folder and resource pool.

1. In the **Restored VM name** field, specify a name under which the workload will be restored.
2. In the **Host** field, specify a host on which the VM will run.
3. In the **VM folder** field, specify a folder to which the recovered VM files will be placed.
4. In the **Resource pool** field, specify a resource pool to which the VM will be placed.

Entire VM Restore [X]

Restore Point

Restore Mode

Destination

Restored VM name:

Datastore Host: prgtwesx01.tech.local [Choose...](#)

Network VM folder: Enterprise [Choose...](#)

Summary Resource pool: Recovered VMs [Choose...](#)

[Previous](#) [Next](#) [Cancel](#)

Step 5. Specify Datastore and Disk Type

The **Datastore** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can specify target datastore for VM configuration files and VM disk files, as well as change the disk type (provisioning policy) for the recovered VM. By default, Veeam Backup & Replication uses the datastore and disk type settings of the original VM. You can place an entire VM to a particular datastore or choose to store configuration files and disk files of the restored VM in different locations.

To specify a datastore and disk type, take the following steps:

1. To change the target datastore for VM configuration files or disk files, do the following:
 - a. Select the configuration files or one of the hard disks and click **Datastore**.
 - b. In the **Select Datastore** window, choose the necessary datastore and click **OK**.
2. By default, hard disks of the restored VM have the same type as disks of the original VM. To change the disk type, do the following:
 - a. Select a hard disk and click **Disk Type**.
 - b. In the **Restored VM Disk Type** window, select a disk type and click **OK**.

For more information about disk types, see [VMware Docs](#).

NOTE

Disk type change is supported only for VMs with Virtual Hardware version 7 or later.

Entire VM Restore

Datastore

By default, original datastore and disk type are selected for each VM file. You can change them by selecting desired VM file, and clicking Datastore or Disk Type.

VM name: apache04

Files location

Datastore... Disk Type...

File	Datastore	Disk Type
Configuration files	prgtwesx01-ds02	
Hard disk 1	prgtwesx01-ds02	Same as source

Previous Next Cancel

Step 6. Configure Network Mapping

The **Network** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can map a network in the original site to the network in the target site. During the restore process, Veeam Backup & Replication will update VM configuration files to replace the original networks with the specified networks in the target site. As a result, you will not have to re-configure network settings manually.

To change networks to which the restored VM will be connected:

1. From the **Network connections** list, select the necessary network.
2. Configure VM network mapping:
 - o To connect the restored VM to another network, do the following:
 - i. Click **Network**.
 - ii. In the **Select Network** window, select a necessary network and click **OK**.
 - o To disconnect the recovered VM from the network, click **Disconnect**.

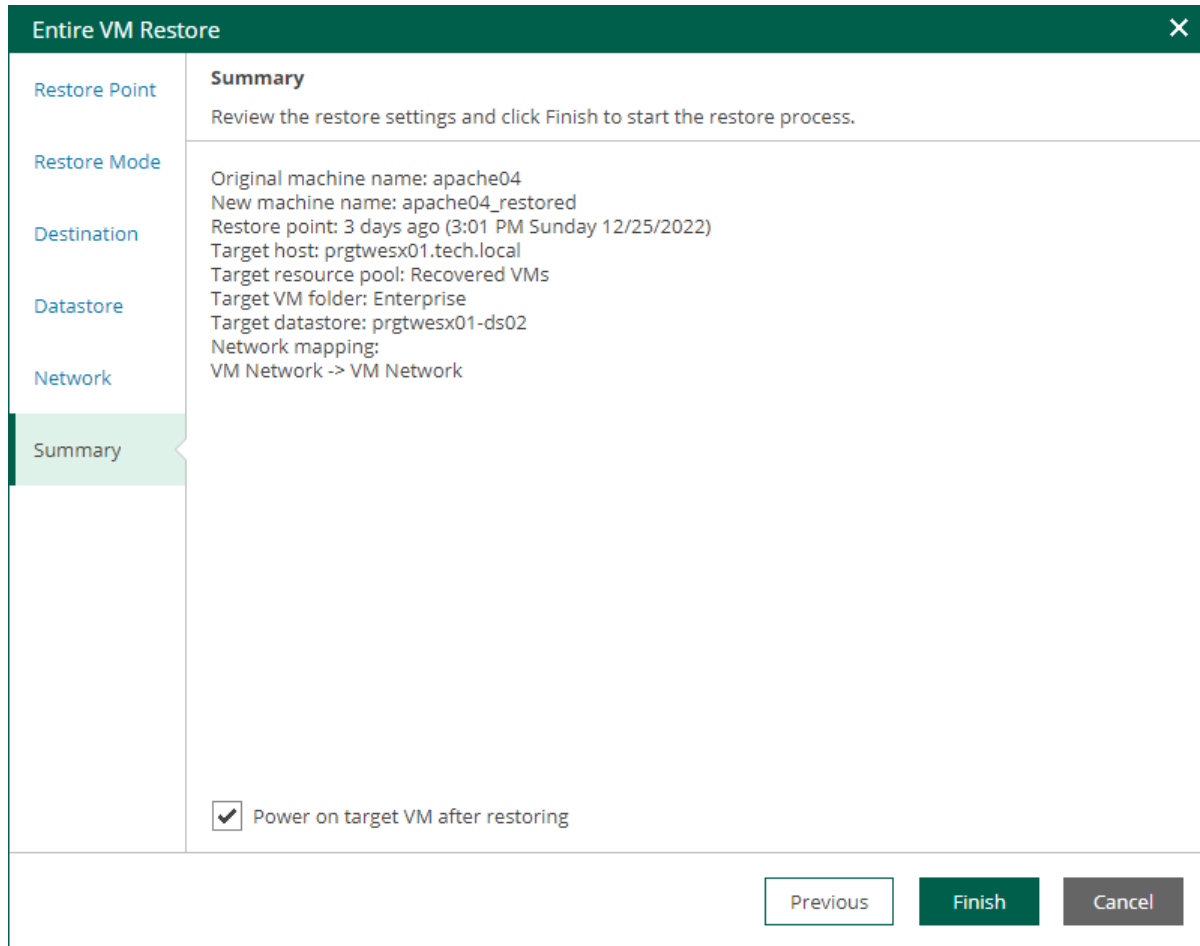
The screenshot shows the 'Entire VM Restore' wizard window. The title bar is green with a close button. On the left is a sidebar with options: Restore Point, Restore Mode, Destination, Datastore, Network (highlighted), and Summary. The main content area is titled 'Network' and contains the following text: 'By default, restored VM will be connected to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.' Below this, it says 'VM name: apache04'. There is a section titled 'Network connections' with two buttons: 'Network' and 'Disconnect'. Below that is a table with two columns: 'Source' and 'Target'. The table has one row with 'VM Network' in both columns. At the bottom right of the window are three buttons: 'Previous', 'Next', and 'Cancel'.

Source	Target
VM Network	VM Network

Step 7. Review Restore Settings

At the **Summary** step of the wizard, check restore settings and click **Finish**. If you want to start the restored VM on the target host, select the **Power on target VM after restoring** check box.

To view the restore progress, on the **Machines** tab, click **History**.



The screenshot shows the 'Entire VM Restore' wizard window. The title bar is dark green with a close button (X) on the right. The main area is divided into a left sidebar and a main content area. The sidebar has a green header 'Entire VM Restore' and a list of steps: 'Restore Point', 'Restore Mode', 'Destination', 'Datastore', 'Network', and 'Summary'. The 'Summary' step is highlighted with a green background. The main content area has a green header 'Summary' and a close button (X) on the right. Below the header, there is a text box with the instruction: 'Review the restore settings and click Finish to start the restore process.' Below this, there is a list of settings: 'Original machine name: apache04', 'New machine name: apache04_restored', 'Restore point: 3 days ago (3:01 PM Sunday 12/25/2022)', 'Target host: prgtwesx01.tech.local', 'Target resource pool: Recovered VMs', 'Target VM folder: Enterprise', 'Target datastore: prgtwesx01-ds02', 'Network mapping: VM Network -> VM Network'. At the bottom of the main content area, there is a checkbox labeled 'Power on target VM after restoring' which is checked. At the bottom of the window, there are three buttons: 'Previous' (white), 'Finish' (green), and 'Cancel' (grey).

Step	Summary
Restore Point	
Restore Mode	
Destination	
Datastore	
Network	
Summary	<p>Review the restore settings and click Finish to start the restore process.</p> <p>Original machine name: apache04 New machine name: apache04_restored Restore point: 3 days ago (3:01 PM Sunday 12/25/2022) Target host: prgtwesx01.tech.local Target resource pool: Recovered VMs Target VM folder: Enterprise Target datastore: prgtwesx01-ds02 Network mapping: VM Network -> VM Network</p> <p><input checked="" type="checkbox"/> Power on target VM after restoring</p>

Restoring Entire VM to VMware Cloud Director

Veeam Backup Enterprise Manager allows you to restore VMware Cloud Director VMs to a vApp in VMware Cloud Director. You can restore VMs from backups to the original location or a new location included in your restore scope.

For more information on entire VM restore of VMware Cloud Director VMs, see the [Restoring VMs into vCloud vApp](#) section of the Veeam Backup & Replication User Guide.

To restore an entire VM, use the **Entire VM Restore** wizard.

1. [Launch the Entire VM Restore wizard.](#)
2. [Select a restore point.](#)
3. [Select a restore mode.](#)
4. [Specify destination settings for the recovered VM.](#)
5. [Specify a target datastore.](#)
6. [Configure network mapping.](#)
7. [Configure fast provisioning.](#)
8. [Review the recovery settings.](#)

Step 1. Launch Entire VM Restore Wizard

To launch the **Entire VM Restore** wizard, do the following:

1. Open the **Machines** tab and select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Entire VM Restore**.

Alternatively, you can right-click the VM and select **Entire VM Restore**.

The screenshot shows the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The 'Machines' tab is active. Below the navigation bar, there is a search bar for machine names and a toolbar with various actions: 'Instant Recovery', 'Entire VM Restore', 'Restore vApp', 'Virtual Disks', 'Failover Plan...', 'Delete', 'Quick Backup', 'History', 'Export', and 'Refresh'. The 'Entire VM Restore' button is highlighted with a mouse cursor. Below the toolbar is a table with the following columns: Machine, vApp, Backup Server, Job Name, Restore Points, Location, Path, and Last Success. The table contains 15 rows of VM data. At the bottom, there is a 'Records per Page' dropdown set to 15, a pagination control showing 'Page 1 of 3', and a 'Displaying 1 - 15 of 32' indicator.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
apache05	Not available	enterprise05.tech.local	Web Servers Backup	8 points	Default Backup Repository	C:\Backup\Web Servers Backup	2 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	8 points	Default Backup Repository	C:\Backup\Web Servers Backup	2 hours ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	8 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	7 hours ago
linorc01	Not available	enterprise05.tech.local	Oracle Linux Backup	7 points	Backup Repository 1	C:\Backup Repository\Oracle Linux Backup	8 hours ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	6 points	Backup Repository 1	C:\Backup Repository\AD Backup	14 hours ago
linux03	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	8 points	Default Backup Repository	C:\Backup\Organization02 Backup	23 hours ago
linux02	vApp02	enterprise05.tech.local	Organization02 vApp02 Backup	8 points	Default Backup Repository	C:\Backup\Organization02 Backup	23 hours ago
rhel01	Not available	enterprise05.tech.local	Backup Copy Job 1\RHEL Backup	3 points	Backup Repository 1	C:\Backup Repository\Backup Copy Job 1\RH...	1 day ago
rhel01	Not available	enterprise05.tech.local	RHEL Backup	4 points	Default Backup Repository	C:\Backup\RHEL Backup	1 day ago
virt01-vm33	Not available	enterprise05.tech.local	CDP Policy for Servers	13 points	vcenter01.tech.local\prgtw...	virt01-vm33_cdp_replica	2 days ago
ts-vm01	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local\prgtw...	ts-vm01-e6e3	2 days ago
ts-vm022	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local\prgtw...	ts-vm022-XVuK	2 days ago
appsvr001	Not available	enterprise05.tech.local	HV Backup Job	3 points	Backup Repository 1	C:\Backup Repository\HV Backup Job	4 days ago
winorc01	Not available	enterprise05.tech.local	Windows Oracle Backup	1 point	Backup Repository 1	C:\Backup Repository\Oracle Backup	93 days ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	3 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	101 days ago

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point for which you want to perform entire VM restore.

The screenshot shows the 'Entire VM Restore' wizard window. The title bar is dark green with a close button. The left sidebar has three tabs: 'Restore Point' (selected), 'Restore Mode', and 'Summary'. The main content area is titled 'Restore Point' and contains the instruction 'Select the restore point to restore VM from.' Below this, it shows 'VM name: linux03'. A table lists backup points with columns for 'Backup Date' and 'Type'. The row for '12/27/2022 06:02:19 pm' (Increment) is highlighted in light green. At the bottom right, there are 'Next' and 'Cancel' buttons.

Backup Date	Type
12/28/2022 06:03:29 pm	Increment
12/27/2022 06:02:19 pm	Increment
12/26/2022 06:02:35 pm	Increment
12/25/2022 06:02:46 pm	Increment
12/24/2022 06:02:08 pm	Full
12/23/2022 06:01:53 pm	Increment
12/23/2022 03:31:40 pm	Increment
12/23/2022 03:25:21 pm	Full

Step 3. Select Restore Mode

At the **Restore mode** step, specify a destination for VM recovery and select whether you want to recover VM tags.

When you perform entire VM restore using Veeam Backup Enterprise Manager, Veeam Backup & Replication automatically selects a backup proxy over which VM data must be transported to the source datastore. You can select a backup proxy manually from the **Entire VM Restore** wizard in the Veeam Backup & Replication console. For more information, see the [Select Restore Mode](#) section of the Veeam Backup & Replication User Guide.

1. Select a restore mode:
 - **Restore to the original location** – select this option to restore the VM with initial settings and to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

During restore to the original location, Veeam Backup & Replication restores only those disks that are included in the backup file. This means that after the restore finishes, you do not have to update existing jobs which process the original VMs.
 - **Restore to a new location or with different settings** – select this option to restore the VM to a new location, or to any location but with different settings. If this option is selected, the **Entire VM Restore** wizard will include additional steps for customizing VM settings.

During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication deletes the original VMs. In this case, you must edit existing jobs to exclude original VMs from them.
2. If you want to restore tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
 - You restore a VM to the original location.

- The original VM tags are available on the source vCenter Server.

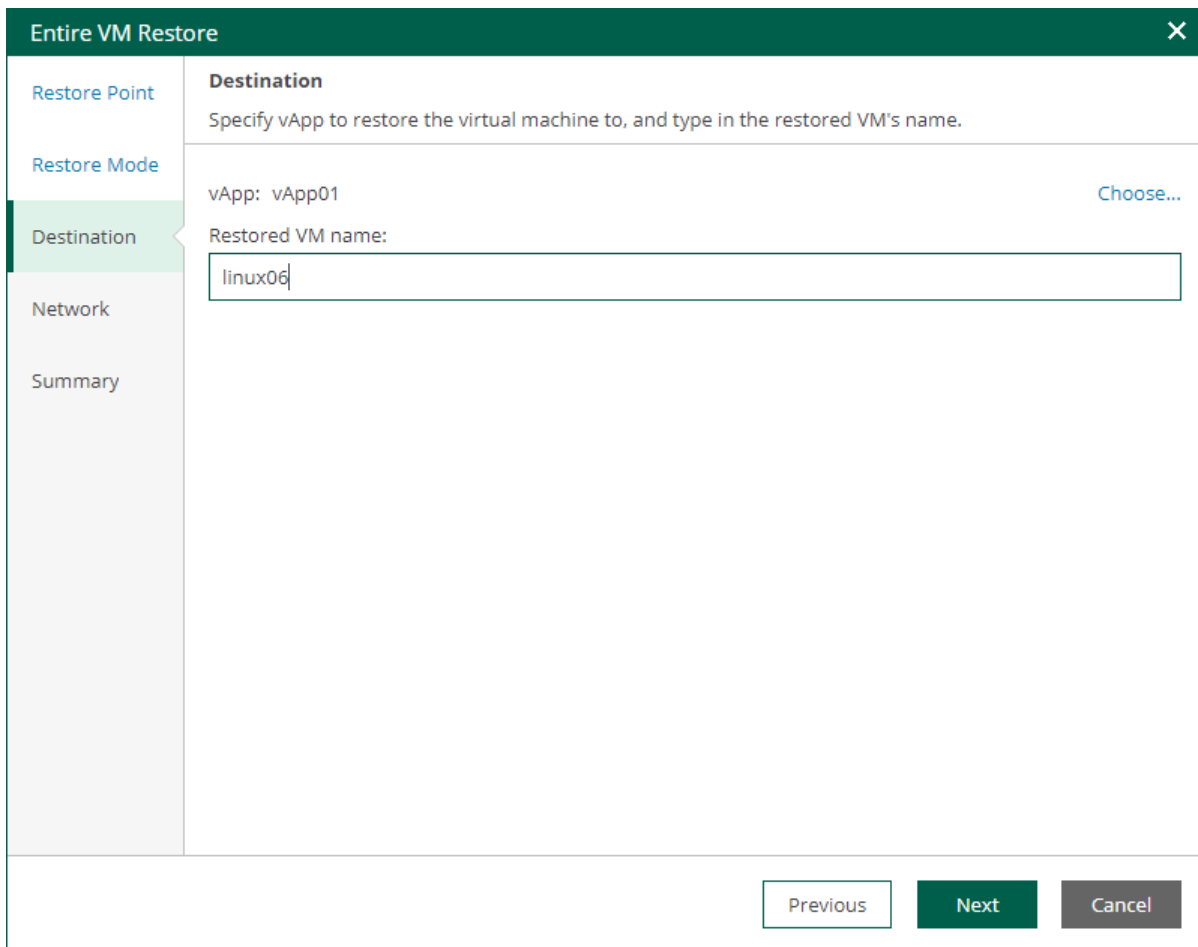
The screenshot shows a wizard window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left is a vertical sidebar with five items: "Restore Point", "Restore Mode" (highlighted in green), "Destination", "Network", and "Summary". The main area is titled "Restore Mode" and contains the following text: "Specify whether you want to restore VM back to the original location, or to a new location or with different settings." Below this are two radio button options: "Restore to the original location" (unselected) and "Restore to a new location, or with different settings" (selected). The second option has a descriptive paragraph: "Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults." At the bottom left of the main area is a checked checkbox labeled "Restore VM tags". At the bottom right are three buttons: "Previous" (disabled), "Next" (active), and "Cancel" (disabled).

Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you configure destination settings such as a name of the restored VM, target host, VM folder and resource pool.

1. In the **vApp** field, specify a vApp to which the VM must be restored. By default, the original vApp is specified. To change the vApp, click **Choose**.
2. In the **Restored VM name** field, specify a name under which the VM will be recovered. By default, the original name of the VM is used. If you are restoring the VM to the same vApp where the original VM is registered and the original VM still resides there, change the VM name to avoid conflicts.



The screenshot shows the 'Entire VM Restore' wizard window. The title bar is dark green with a close button (X) on the right. On the left is a vertical navigation pane with five items: 'Restore Point', 'Restore Mode', 'Destination' (highlighted in light green), 'Network', and 'Summary'. The main area is titled 'Destination' and contains the following text: 'Specify vApp to restore the virtual machine to, and type in the restored VM's name.' Below this, there are two fields: 'vApp: vApp01' with a 'Choose...' link to its right, and 'Restored VM name:' followed by a text input box containing 'linux06'. At the bottom right of the window are three buttons: 'Previous' (light gray), 'Next' (dark green), and 'Cancel' (dark gray).

Step 5. Configure Network Mapping

The **Network** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can map a network in the original site to the network in the target site. During the restore process, Veeam Backup & Replication will update VM configuration files to replace the original networks with the specified networks in the target site. As a result, you will not have to re-configure network settings manually.

To change networks to which the restored VM will be connected:

1. From the **Network connections** list, select the necessary network.
2. Configure VM network mapping:
 - o To connect the restored VM to another network, do the following:
 - i. Click **Network**.
 - ii. In the **Select Network** window, select a necessary network and click **OK**.
 - o To disconnect the recovered VM from the network, click **Disconnect**.

Entire VM Restore [X]

Network

Specify the networks to connect restored virtual machine's vNICs to.

VM name: linux06

Network connections

Network Disconnect

Source	Target
Disconnected	Organization02 Network

Previous Next Cancel

Step 6. Configure Fast Provisioning

The **Fast Provisioning** step of the wizard is available if you restore a VM to a new location or with different settings, and if fast provisioning is enabled on the target organization VDC.

At this step of the wizard, you can configure fast provisioning for the restored VM.

- To specify a fast provisioning template for the VM, select the VM in the list, click **Templates**, and choose a template to which the restored VM must be linked.
- To disable fast provisioning for the VM and restore it as a regular VM, select the VM in the list and click **Disable**.

Entire VM Restore ✕

Restore Point

Restore Mode

Destination

Network

Fast Provisioning

Datastore

Summary

Fast Provisioning

Specify restore settings for virtual machines that use Fast Provisioning feature.

Fast Provisioning Templates

Templates... Disable

VM Name	Template
linux03	Disabled

Previous **Next** Cancel

Step 7. Specify Storage Policy and Datastore

The **Datastore** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can specify a storage policy and datastore for the restored VM.

1. To change the target storage policy, do the following:
 - a. Select a VM and click **Policy**.
 - b. In the **Select Storage Policy** window, select a storage policy and click **OK**.
2. To change the target datastore, do the following:
 - c. Select a VM and click **Datastore**.
 - d. In the **Select Datastore** window, select a datastore and click **OK**.

The screenshot shows the 'Entire VM Restore' wizard window. The 'Datastore' step is active, indicated by a green highlight in the left sidebar. The main area displays 'VM storage settings' with a table of VMs and their storage configurations.

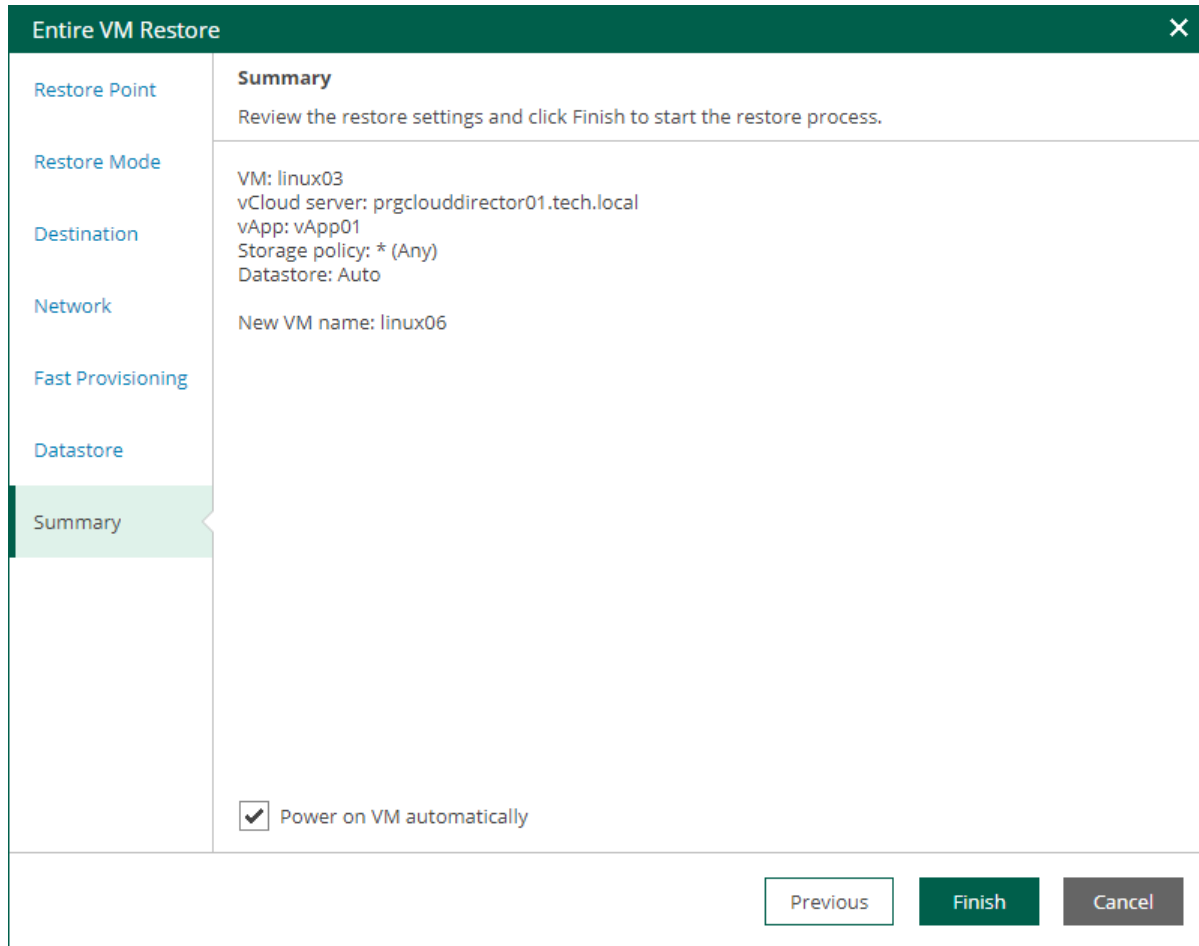
VM Name	Storage Policy	Datastore
linux03	* (Any)	docopsubuntuunfs01

At the bottom of the window, there are three buttons: 'Previous' (disabled), 'Next' (active), and 'Cancel' (disabled).

Step 8. Review Restore Settings

At the **Summary** step of the wizard, check restore settings and click **Finish**. If you want to start the restored VM on the target host, select the **Power on target VM after restoring** check box.

To view the restore progress, on the **Machines** tab, click **History**.



The screenshot shows a window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: "Restore Point", "Restore Mode", "Destination", "Network", "Fast Provisioning", "Datastore", and "Summary". The "Summary" item is highlighted with a green bar. The main content area is titled "Summary" and contains the following text: "Review the restore settings and click Finish to start the restore process." Below this, the settings are listed: "VM: linux03", "vCloud server: prgclouddirector01.tech.local", "vApp: vApp01", "Storage policy: * (Any)", "Datastore: Auto", and "New VM name: linux06". At the bottom of the main area, there is a checkbox labeled "Power on VM automatically" which is checked. At the bottom right of the window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

Restoring Entire VM to Microsoft Hyper-V

Veeam Backup Enterprise Manager allows you to restore Microsoft Hyper-V VMs to Microsoft Hyper-V. You can restore VMs from backups to the original location or a new location included in your restore scope.

For more information on entire VM restore of Microsoft Hyper-V VMs, see the [Entire VM Restore](#) section of the Veeam Backup & Replication User Guide.

To restore an entire VM, use the **Entire VM Restore** wizard.

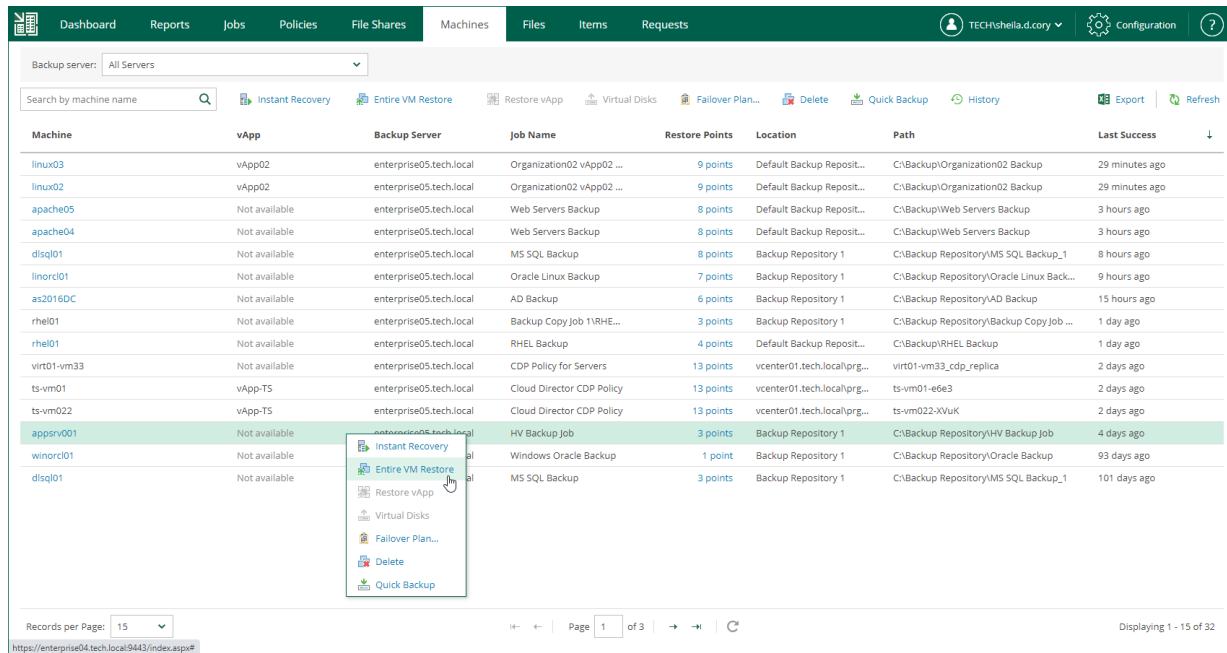
1. [Launch the Entire VM Restore wizard.](#)
2. [Select a restore point.](#)
3. [Select a recovery mode.](#)
4. [Specify destination settings for the recovered VM.](#)
5. [Specify a target datastore.](#)
6. [Configure network mapping.](#)
7. [Review the recovery settings.](#)

Step 1. Launch Entire VM Restore Wizard

To launch the **Entire VM Restore** wizard, do the following:

1. Open the **Machines** tab and select the necessary Microsoft Hyper-V VM from the list.
2. On the toolbar, click **Restore**.

Alternatively, you can right-click the VM and select **Entire VM Restore**.

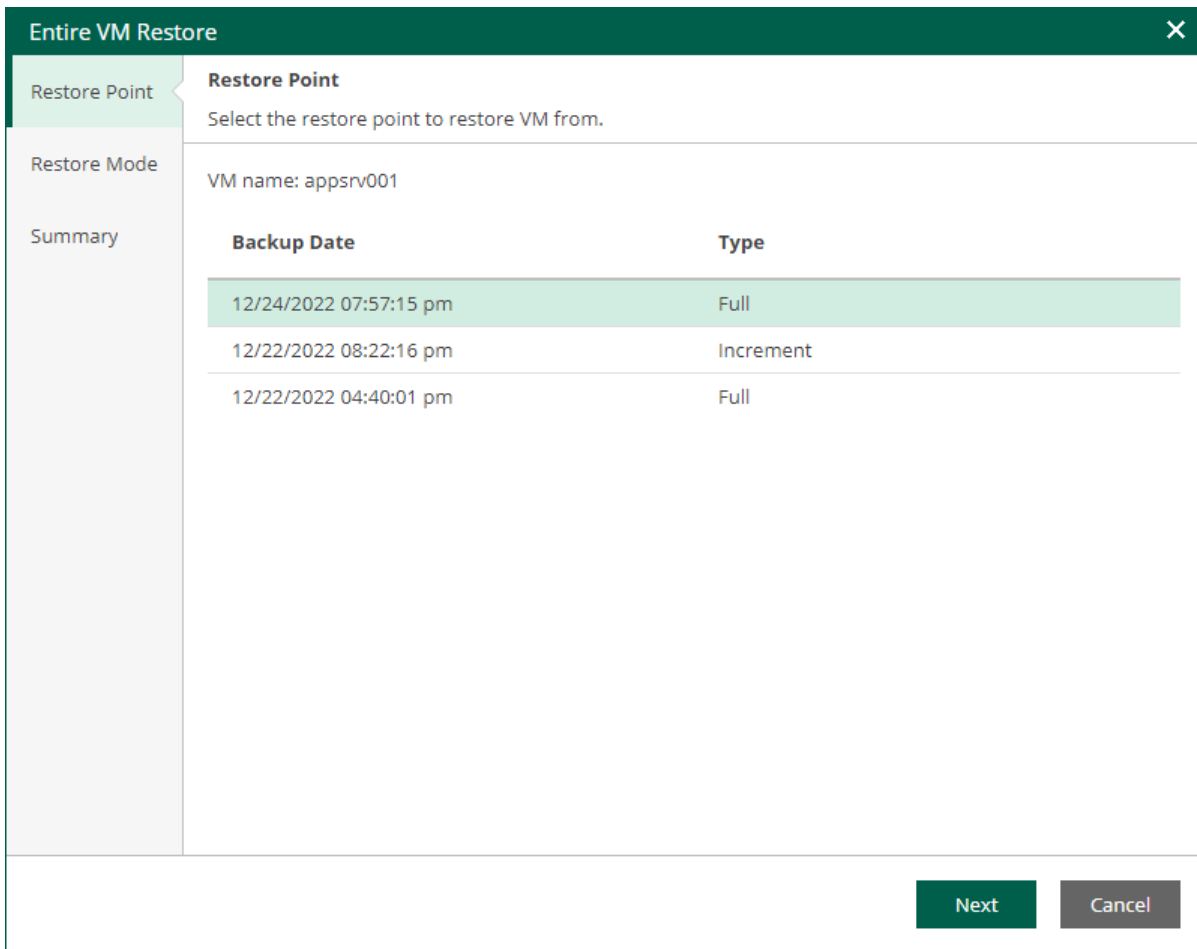


The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The 'Machines' tab is active, showing a list of virtual machines. A context menu is open over the 'winorcl01' VM, with the 'Entire VM Restore' option highlighted. The table below shows the details of the VMs.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
linux03	vApp02	enterprise05.tech.local	Organization02 vApp02 ...	9 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	29 minutes ago
linux02	vApp02	enterprise05.tech.local	Organization02 vApp02 ...	9 points	Default Backup Reposit...	C:\Backup\Organization02 Backup	29 minutes ago
apache05	Not available	enterprise05.tech.local	Web Servers Backup	8 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	3 hours ago
apache04	Not available	enterprise05.tech.local	Web Servers Backup	8 points	Default Backup Reposit...	C:\Backup\Web Servers Backup	3 hours ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	8 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	8 hours ago
linorc101	Not available	enterprise05.tech.local	Oracle Linux Backup	7 points	Backup Repository 1	C:\Backup Repository\Oracle Linux Back...	9 hours ago
as2016DC	Not available	enterprise05.tech.local	AD Backup	6 points	Backup Repository 1	C:\Backup Repository\AD Backup	15 hours ago
rhel01	Not available	enterprise05.tech.local	Backup Copy Job 1\RHE...	3 points	Backup Repository 1	C:\Backup Repository\Backup Copy Job ...	1 day ago
rhel01	Not available	enterprise05.tech.local	RHEL Backup	4 points	Default Backup Reposit...	C:\Backup\RHEL Backup	1 day ago
virt01-vm33	Not available	enterprise05.tech.local	CDP Policy for Servers	13 points	vcenter01.tech.local/prg...	virt01-vm33_cdp_replica	2 days ago
ts-vm01	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local/prg...	ts-vm01-e6e3	2 days ago
ts-vm022	vApp-TS	enterprise05.tech.local	Cloud Director CDP Policy	13 points	vcenter01.tech.local/prg...	ts-vm022-XVuK	2 days ago
appsvr001	Not available	enterprise05.tech.local	HV Backup Job	3 points	Backup Repository 1	C:\Backup Repository\HV Backup Job	4 days ago
winorc101	Not available	enterprise05.tech.local	Windows Oracle Backup	1 point	Backup Repository 1	C:\Backup Repository\Oracle Backup	93 days ago
disql01	Not available	enterprise05.tech.local	MS SQL Backup	3 points	Backup Repository 1	C:\Backup Repository\MS SQL Backup_1	101 days ago

Step 2. Select Restore Point

At the **Restore Points** step of the wizard, select a VM restore point for which you want to perform entire VM restore.



The screenshot shows a window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left side, there is a vertical navigation pane with three items: "Restore Point" (highlighted in light green), "Restore Mode", and "Summary".

The main content area is titled "Restore Point" and contains the instruction "Select the restore point to restore VM from." Below this, it displays "VM name: appsrv001".

A table lists the available restore points:

Backup Date	Type
12/24/2022 07:57:15 pm	Full
12/22/2022 08:22:16 pm	Increment
12/22/2022 04:40:01 pm	Full

At the bottom right of the window, there are two buttons: "Next" (in a green box) and "Cancel" (in a grey box).

Step 3. Select Restore Mode

At the **Restore mode** step, specify a destination for VM recovery and select whether you want to recover VM tags.

When you perform entire VM restore using Veeam Backup Enterprise Manager, Veeam Backup & Replication automatically selects a backup proxy over which VM data must be transported to the source datastore. You can select a backup proxy manually from the **Entire VM Restore** wizard in the Veeam Backup & Replication console. For more information, see the [Select Restore Mode](#) section of the Veeam Backup & Replication User Guide.

1. Select a restore mode:

- **Restore to the original location** – select this option to restore the VM with initial settings and to the original location. If this option is selected, you will pass directly to the [Summary](#) step of the wizard.

During restore to the original location, Veeam Backup & Replication restores only those disks that are included in the backup file. This means that after the restore finishes, you do not have to update existing jobs which process the original VMs.
- **Restore to a new location or with different settings** – select this option to restore the VM to a new location, or to any location but with different settings. If this option is selected, the **Entire VM Restore** wizard will include additional steps for customizing VM settings.

During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication deletes the original VMs. In this case, you must edit existing jobs to exclude original VMs from them.

NOTE

If you need to run an executable script for the VM before restoring it to the production environment, you can use the Veeam Backup & Replication console to perform entire VM restore in the Staged restore mode. For more information, see the [Select Restore Mode](#) section of the Veeam Backup & Replication User Guide.

- ### 2. [For VM restore to the original location] Select the **Quick rollback** check box to perform incremental restore for the VM. Veeam Backup & Replication will query Changed Block Tracking to get data blocks that are required to revert the VM to the restore point, and will restore only these data blocks. Quick rollback significantly reduces the restore time and has little impact on the production environment.

Enable this option if you restore a VM after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.

For more information on quick rollback, its requirements and limitations, see the [Quick Rollback](#) section of the Veem Backup & Replication User Guide.

The screenshot shows a wizard window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: "Restore Point", "Restore Mode" (highlighted in green), "Destination", "Datastore", "Network", and "Summary". The main content area is titled "Restore Mode" and contains the following text: "Specify whether selected objects should be restored back to the original location, or to a new location or with different settings." Below this are three radio button options: 1. "Restore to the original location" with a description: "Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error." 2. "Restore to a new location, or with different settings" (selected with a filled radio button) with a description: "Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults." 3. "Quick rollback (restore changed blocks only)" (unchecked) with a description: "Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss." At the bottom right of the window are three buttons: "Previous" (white), "Next" (green), and "Cancel" (grey).

Step 4. Specify Destination Settings

The **Destination** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can specify a name of the restored VM and target host, register the VM as a cluster resource, and generate a new BIOS UUID.

To configure destination settings, do the following:

1. In the **Restored VM name** field, specify a name under which the workload will be restored.
2. In the **Host** field, specify a target host.
3. If the specified host is a part of a Hyper-V failover cluster, you can register the restored VM as a cluster resource. In this case, if the target host is brought offline or fails for any reason, the VM will fail over to another node in the cluster. To do this, select the **Register VM as a cluster resource** check box.
4. Choose whether to preserve the BIOS UUID or generate a new BIOS UUID.

If the original VM still resides in the production environment, select the **Generate new BIOS UUID** option to prevent conflicts. The BIOS UUID change is not required if the original VM no longer exists, for example, if it was deleted.

The screenshot shows the 'Entire VM Restore' wizard window with a dark green header and a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: 'Restore Point', 'Restore Mode', 'Destination' (highlighted in light green), 'Datastore', 'Network', and 'Summary'. The main content area is titled 'Destination' and contains the following elements: a sub-header 'Destination' with a description: 'Select the host to recover machine to, specify the new virtual machine name, and whether you would like unique identifier to be preserved.'; a text input field for 'Restored VM name:' containing the text 'appsrv001-restored'; a 'Host:' label with the value 'pdctwhv02' and a 'Choose...' link to its right; a checked checkbox labeled 'Register VM as a cluster resource'; and two radio button options: 'Preserve virtual machine ID (recommended)' with the subtext 'Keep ID when restoring the existing virtual machine to avoid reconfiguring applications that match VM by ID.', and 'Generate new virtual machine ID' with the subtext 'Use this option if you are using restore to clone the virtual machine to prevent conflicts with the existing VM.' At the bottom right of the window are three buttons: 'Previous' (disabled), 'Next' (active), and 'Cancel' (disabled).

Step 5. Specify Datastore

The **Datastore** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can change default paths where VM configuration files and disk files will be stored.

To change a default path, do the following:

1. Select the configuration files or one of the disk files and click **Edit Path**.

Alternatively, you can double-click a file to edit its path.

2. Type in a path to the folder where the files will be stored. You can specify an existing folder, a new folder or an SMB3 shared folder. SMB3 shared folder path must be in the UNC format, for example:

`\\172.16.11.38\Share01`.

3. Click **OK**.

IMPORTANT

The host or cluster on which you register VMs must have access to the specified SMB3 shared folder. If you are using SCVMM 2012 or later, the server hosting the Microsoft SMB3 shared folder must be registered in SCVMM as a storage device. For more information, see [Microsoft Docs](#).

The screenshot shows the 'Entire VM Restore' wizard window. The 'Datastore' step is active, showing the VM name 'appsv001-restored'. Under 'Files location', there is an 'Edit Path' button and a table of files to be restored.

File	Size	Path
Configuration files		D:\Storage\Hyper-V
appsv001.vhdx	4 MB	D:\Storage\Hyper-V\appsv001-rest...

At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Step 6. Configure Network Mapping

The **Network** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can map a network in the original site to the network in the target site. During the restore process, Veeam Backup & Replication will update VM configuration files to replace the original networks with the specified networks in the target site. As a result, you will not have to re-configure network settings manually.

To change networks to which the restored VM will be connected:

1. From the **Network connections** list, select the necessary network.
2. Configure VM network mapping:
 - o To connect the restored VM to another network, do the following:
 - i. Click **Network**.
 - ii. In the **Select Network** window, select a necessary network and click **OK**.
 - o To disconnect the recovered VM from the network, click **Disconnect**.

The screenshot shows the 'Entire VM Restore' wizard window. The title bar is green with a close button. The left sidebar has a green highlight on the 'Network' step. The main content area is titled 'Network' and contains the following elements:

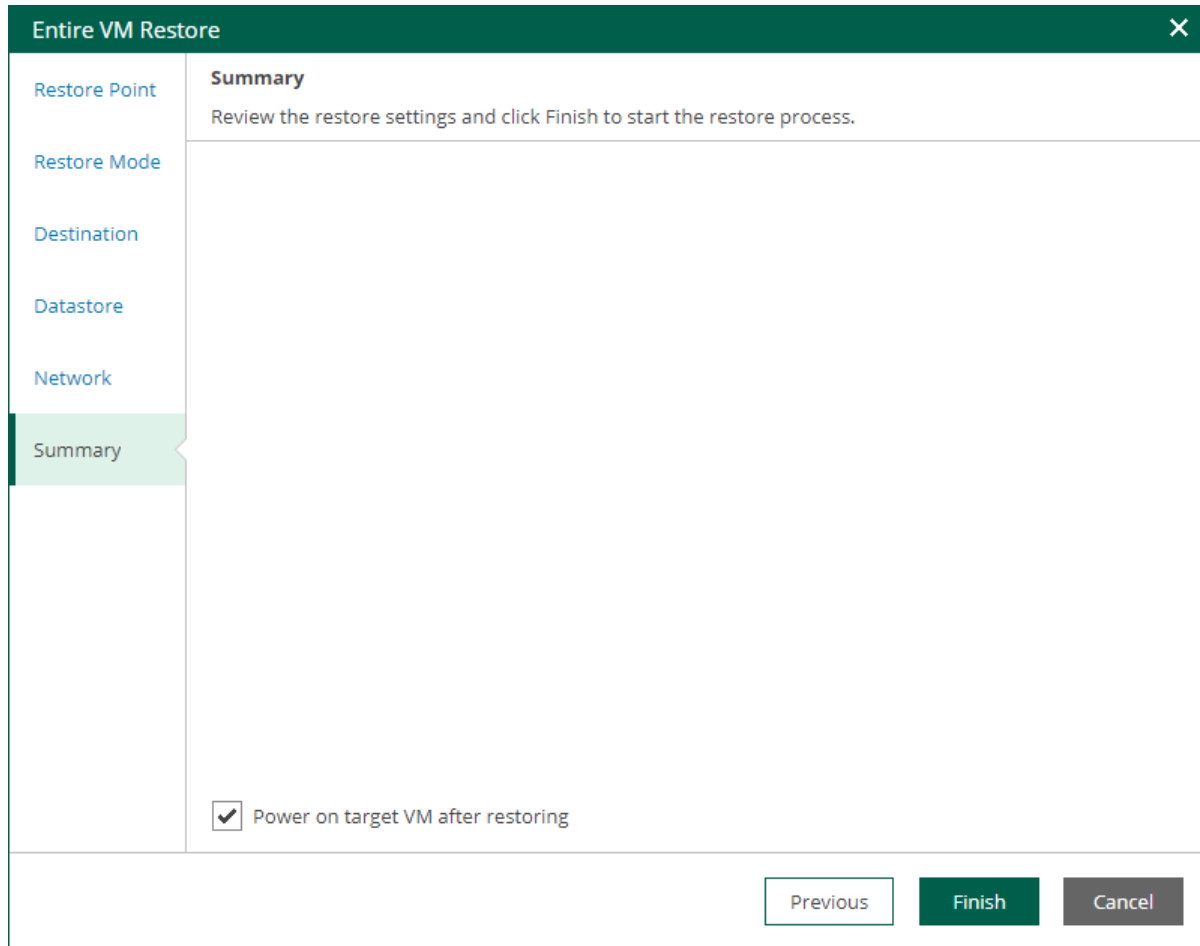
- Network**: Select how virtual networks map to each other between original and new VM locations.
- Restore Mode**: VM name: appsrv001-restored
- Network connections**: A section with two buttons: 'Network' (highlighted) and 'Disconnect'.
- Table**: A table with two columns, 'Source' and 'Target'. A single row is visible with 'Intel' in both columns, highlighted in light green.

At the bottom right, there are three buttons: 'Previous' (disabled), 'Next' (active), and 'Cancel' (disabled).

Step 7. Review Restore Settings

At the **Summary** step of the wizard, check restore settings and click **Finish**. If you want to start the restored VM on the target host, select the **Power on target VM after restoring** check box.

To view the restore progress, on the **Machines** tab, click **History**.



The screenshot shows a window titled "Entire VM Restore" with a close button (X) in the top right corner. On the left side, there is a vertical navigation pane with the following items: "Restore Point", "Restore Mode", "Destination", "Datastore", "Network", and "Summary". The "Summary" item is highlighted with a green bar. The main content area is titled "Summary" and contains the text: "Review the restore settings and click Finish to start the restore process." At the bottom of this area, there is a checked checkbox labeled "Power on target VM after restoring". At the bottom right of the window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

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 Disk Restore](#) section of the Veeam Backup & Replication User Guide.

IMPORTANT

Consider the following:

- Disk restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Disk restore 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.

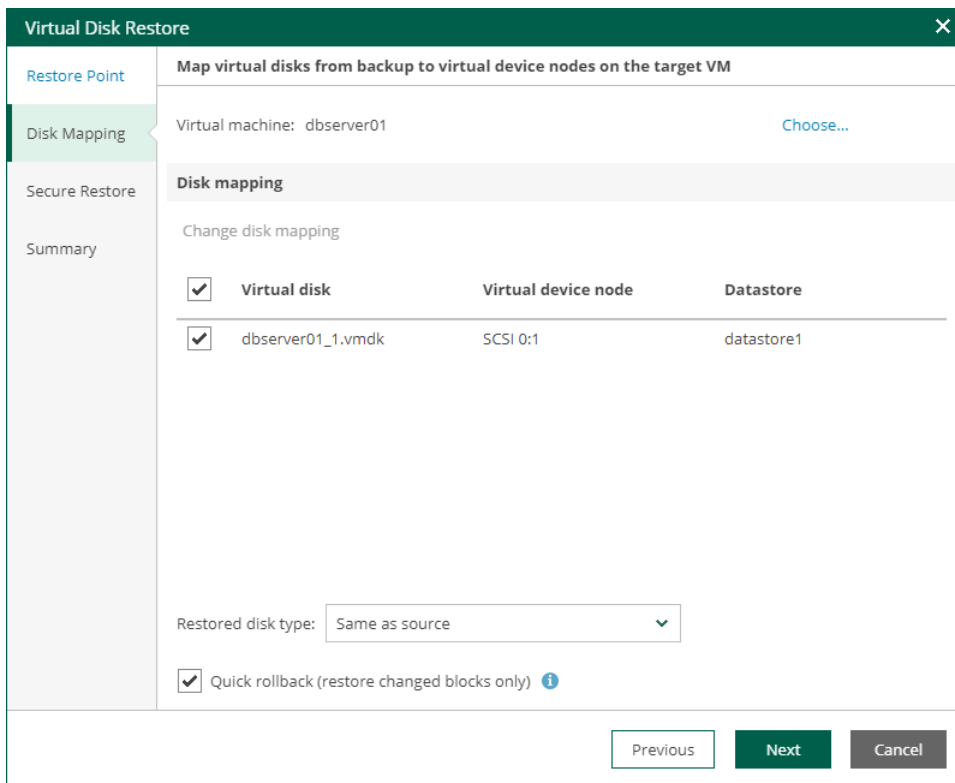
Backup Date	Type	Location
2/4/2021 01:45:58 pm	Increment	Default Backup Repository
2/3/2021 09:11:06 pm	Increment	Default Backup Repository
2/3/2021 01:37:51 am	Increment	Default Backup Repository
2/3/2021 12:24:51 am	Increment	Default Backup Repository
2/3/2021 12:14:39 am	Increment	Default Backup Repository
2/2/2021 10:12:01 pm	Increment	Default Backup Repository
2/2/2021 10:06:31 pm	Full	Default Backup Repository

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](#).

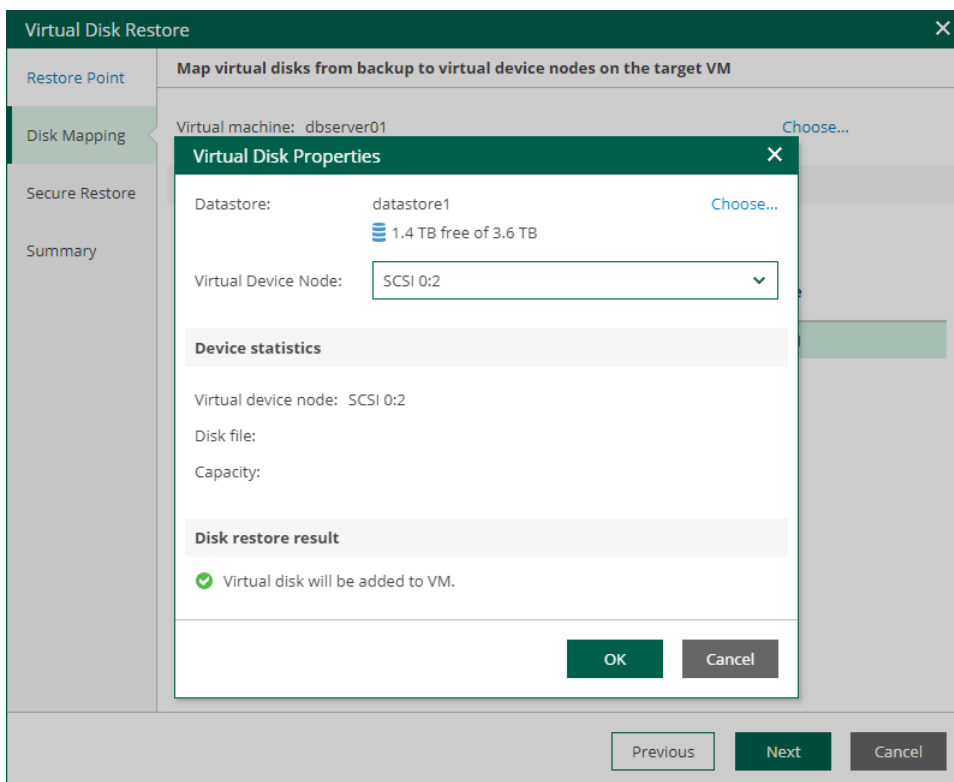
NOTE

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.

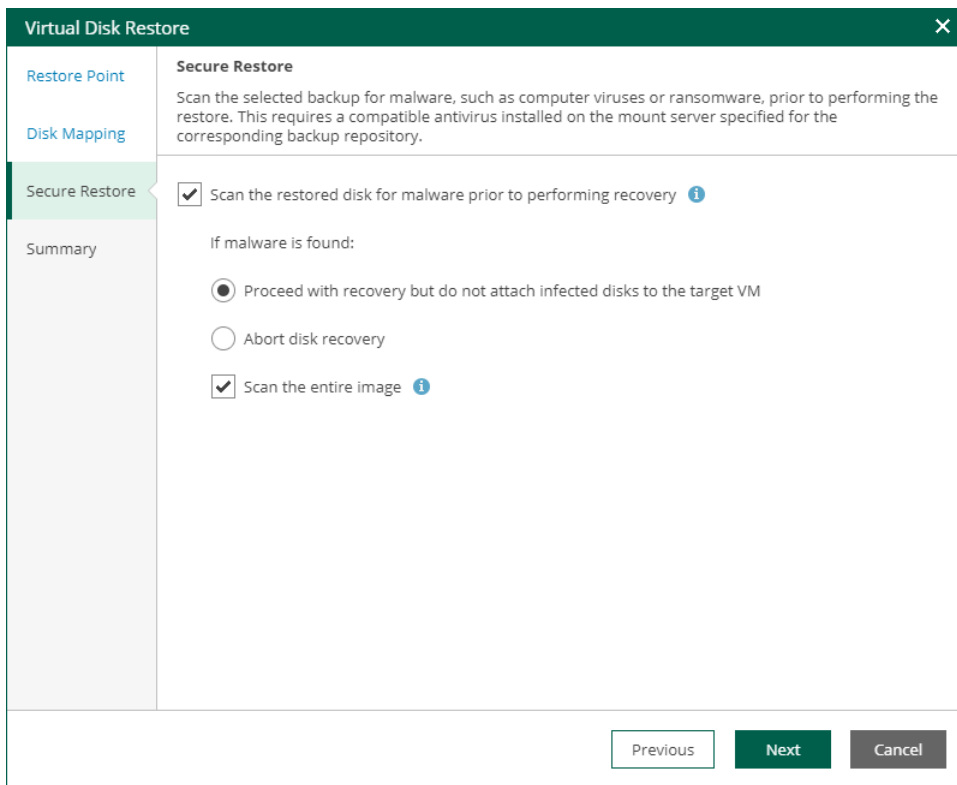


6. At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore – scan virtual disk data with antivirus software before restoring the disk. For more information on secure restore, see the [Secure Restore](#) section of the Veeam Backup & Replication User Guide.

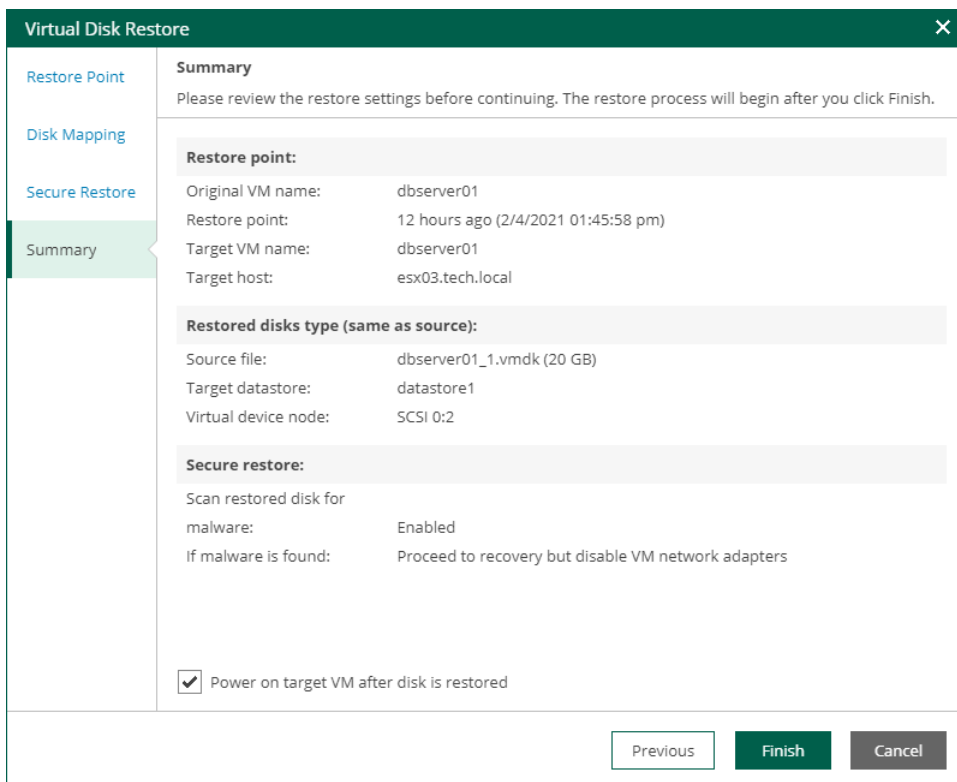
To specify secure restore settings:

- 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**.

VM Failover

Failover is a process of switching from the original VM in the production site to its VM replica in the disaster recovery site. 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 VMware Cloud Director replication job](#)
- [Failover of a vApp processed by a VMware Cloud Director CDP policy](#)

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](#).

NOTE

Consider the following:

- Failover is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- To perform permanent failover, failback, undo failover, or create a failover plan, use the Veeam Backup & Replication console.

Failover to VM Replica

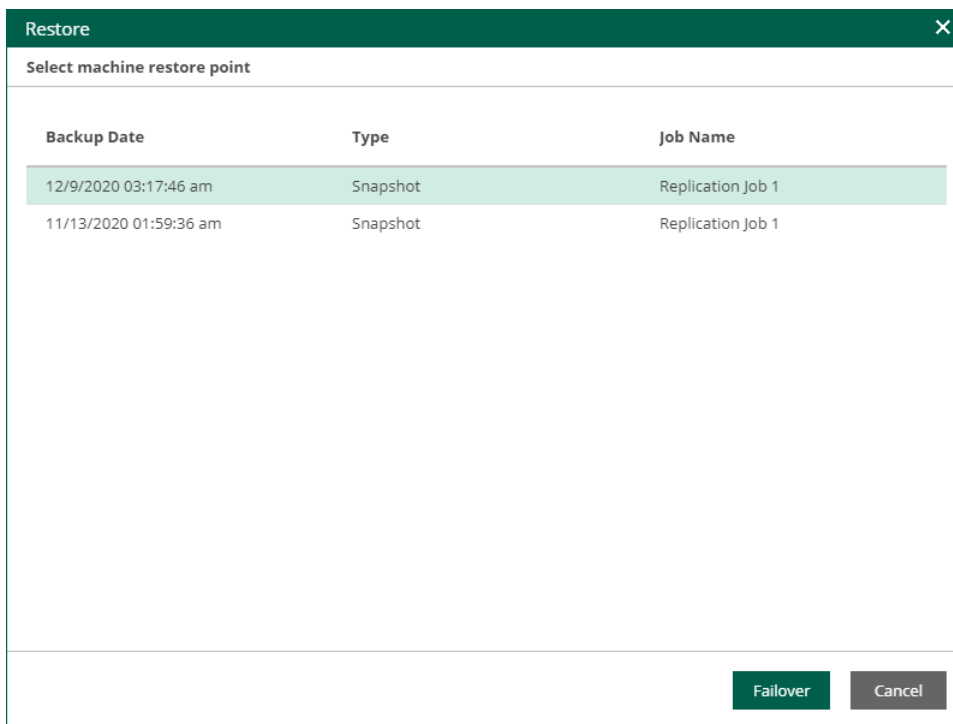
If a VM is processed by a regular replication job, you can fail over the VM to its replica. After the failover operation completes, the VM replica is powered on.

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**.



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:

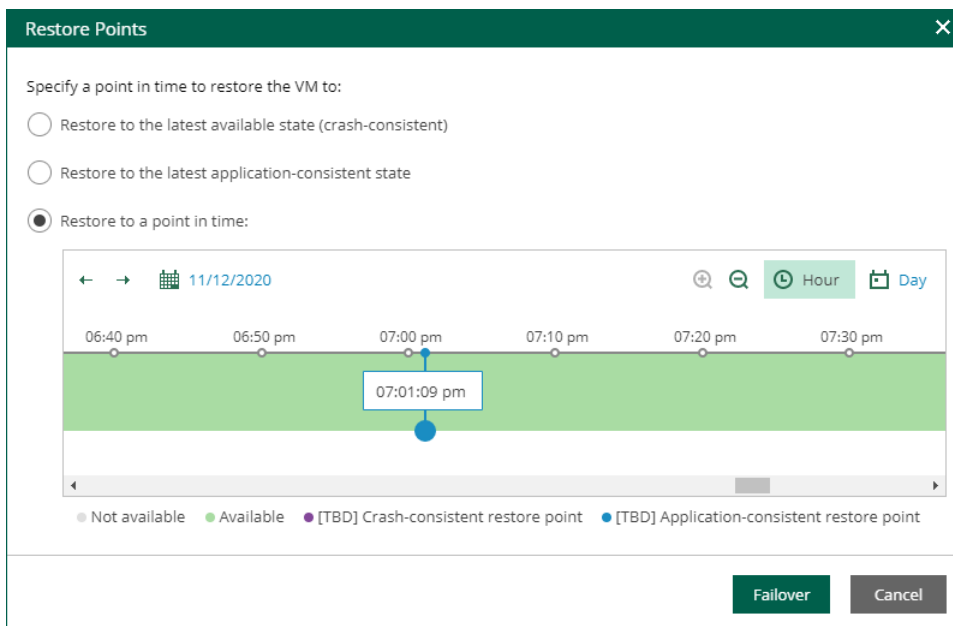
1. On the **Machines** tab, select a machine processed by a CDP policy.
2. Click **Restore**.
3. In the **Restore** window, select the restore point you need. You can fail over to the latest available crash-consistent state, to the latest application-consistent state or to a specific point in time.

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**.



Failover to Cloud Director Replica

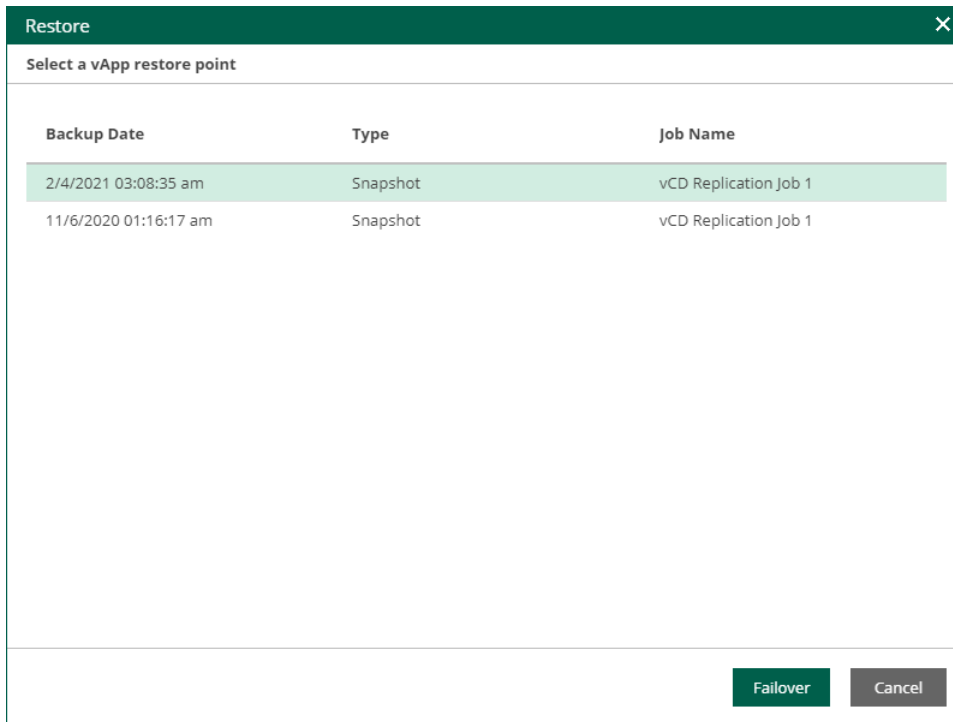
If a VM is processed by a VMware Cloud Director replication job, you can perform failover of the vApp that contains the VM.

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 Cloud Director 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**.



Failover to Cloud Director CDP Replica

If a VM is processed by a VMware Cloud Director CDP policy, 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 Cloud Director CDP policy.
2. Click **Restore vApp**.
3. In the **Restore Points** 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.

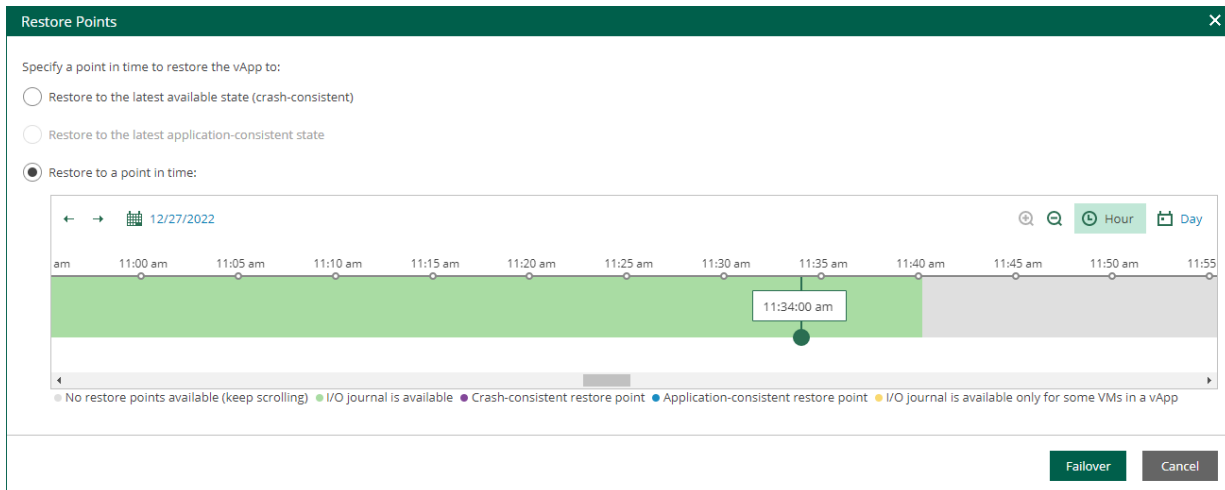
Application consistency is defined for the whole vApp. A vApp restore point is application-consistent if all VMs have application-consistent restore points. A vApp restore point is mixed if some VMs have crash-consistent restore points.

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**.



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.

Running Failover Plans

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.

To view the failover progress, on the **Machines** tab, click **History**.

The screenshot displays the Veeam Backup Enterprise Manager interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines (selected), Files, Items, and Requests. The user is logged in as TECH@sheila.d.cory. The main area shows a table of machines with the following columns: Machine, vApp, Backup Server, Job Name, Restore Points, Location, Path, and Last Success. A 'Failover Plan' dialog box is open in the center, showing a dropdown menu with 'Webserver Failover' selected. Below the dropdown are three radio button options: 'Start now', 'Start to most recent replica prior to:' (with a date and time selector set to 02/08/21 at 12:00 am), and 'Undo'. The 'OK' and 'Cancel' buttons are at the bottom of the dialog. The background table lists various machines, including apache02, dbserver01, filesrv03, vvg-VCD152-win7, win2019, win2019_restored251120T1625, win7, and winsrv88.

Machine	vApp	Backup Server	Job Name	Restore Points	Location	Path	Last Success
apache02	Not available	enterprise05.tech.local	Replication Job 1	3 points	vcenter01.tech.local/e...	apache02_replica	4 days ago
apache02	Not available	enterprise05.tech.local	Backup Job 1	8 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	3 hours ago
apache02	Not available	enterprise05.tech.local	Backup Job 2	8 points	Default Backup Repos...	C:\Backup\Backup Job 2_1\	3 hours ago
apache02	Not available	enterprise05.tech.local	Backup Job 3	8 points	Default Backup Repos...	C:\Backup\Repository for enterprise...	4 hours ago
dbserver01	Not available	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	C:\Backup\Repository for enterprise...	7 hours ago
dbserver01	Not available	enterprise05.tech.local	Backup Job 2	5 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	3 hours ago
filesrv03	Not available	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	C:\Backup\Repository for enterprise...	5 hours ago
vvg-VCD152-win7	aa-win-vcd101	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	C:\Backup\Backup Job 1\	65 days ago
win2019	vApp01	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	win2019_restored251120T1625-fjHY	1 day ago
win2019	vApp01	enterprise05.tech.local	Backup Job 2	5 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	4 days ago
win2019	vApp02	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	4 days ago
win2019_restored251120T1625	vApp01	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	win2019_restored251120T1625-fjHY	1 day ago
win7	vApp02	enterprise05.tech.local	Backup Job 1	5 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	4 days ago
win7	vApp01	enterprise04.tech.local	organization01_Backu...	6 points	Default Backup Repos...	C:\Backup\organization01_Backup Jo...	4 days ago
win7	vApp01	enterprise04.tech.local	vCD Replication Job 1	2 points	autonoe.qahv1.veea...	win2019_restored251120T1625-fjHY	1 day ago
win7	vApp01	enterprise04.tech.local	vCD Backup Job 1	7 points	Default Backup Repos...	C:\Backup\Backup Job 1\	1 day ago
winsrv88	Not available	enterprise05.tech.local	Backup Job 1	2 points	Default Backup Repos...	C:\Backup\Backup Job 1_3\	4 days ago

Guest OS File Restore

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.
- With 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 Backup & Replication 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 indexing capabilities to quickly find necessary 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. 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 a helper host or helper appliance.

Then you 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

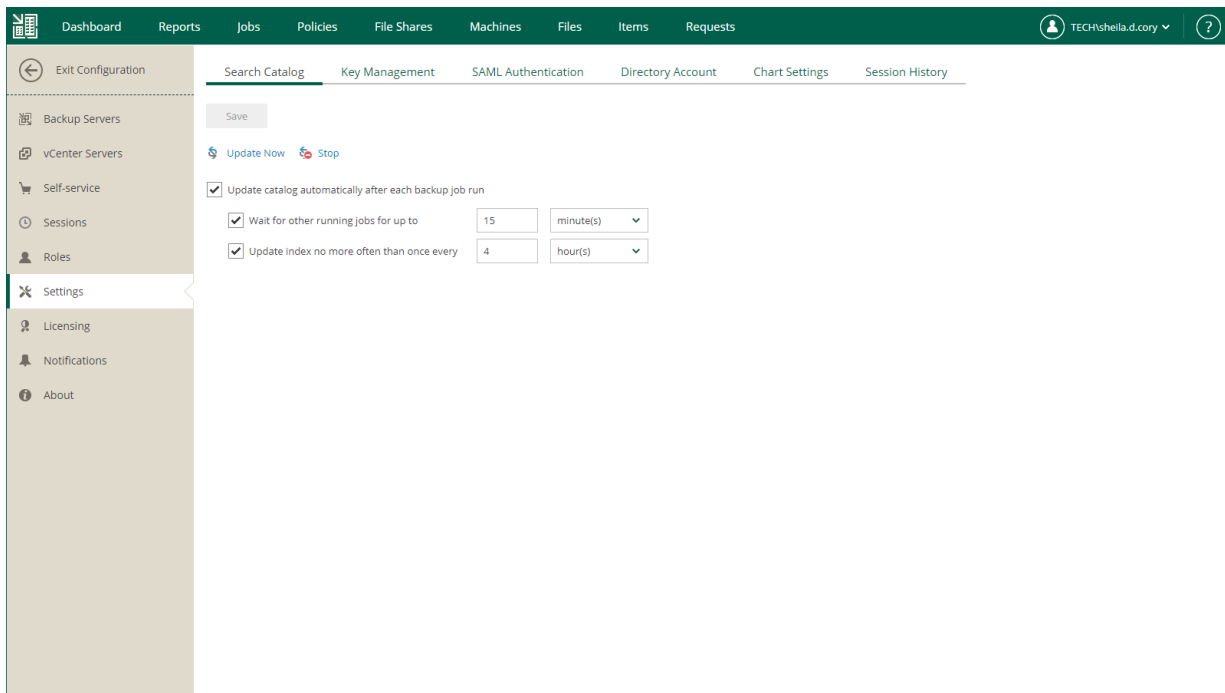
Once you have run backup jobs with guest OS file system indexing enabled, perform catalog replication to consolidate index files from multiple backup servers. During this operation, Veeam Backup Enterprise Manager aggregates index data from multiple backup servers and stores them on the Veeam Backup 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.

NOTE

Guest file indexing is optional. You can browse and restore 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](#).

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.

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 to specify another 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 Helper Host or Helper Appliance

When restoring guest OS files, Veeam Backup & Replication mounts machine disks from the backup or replica to a mount server (helper host or helper appliance). You specify mount server settings on the backup server when you configure a backup job for the machine. These settings are saved in the Veeam Backup & Replication database on per-user basis. The settings are applied each time the user starts file-level restore. For more information on the helper host and helper appliance, see the [Restore from Linux, Unix and Other File Systems](#) section of the Veeam Backup & Replication User Guide.

When you start guest OS file restore from Veeam Backup Enterprise Manager, the mount server settings are obtained from the configuration database of the backup server. If no helper host or helper appliance configuration is found for the user account, Veeam Backup & Replication uses the configuration set during the latest file-level restore performed on the backup server. Thus, before you start file-level restore from Enterprise Manager, make sure the mount server settings are configured on the backup server.

NOTE

If you configure a 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 helper appliances to restore machines backed up by different backup servers, their initial configuration must be performed on the backup servers. Centralized configuration from Veeam Backup Enterprise Manager is not supported.

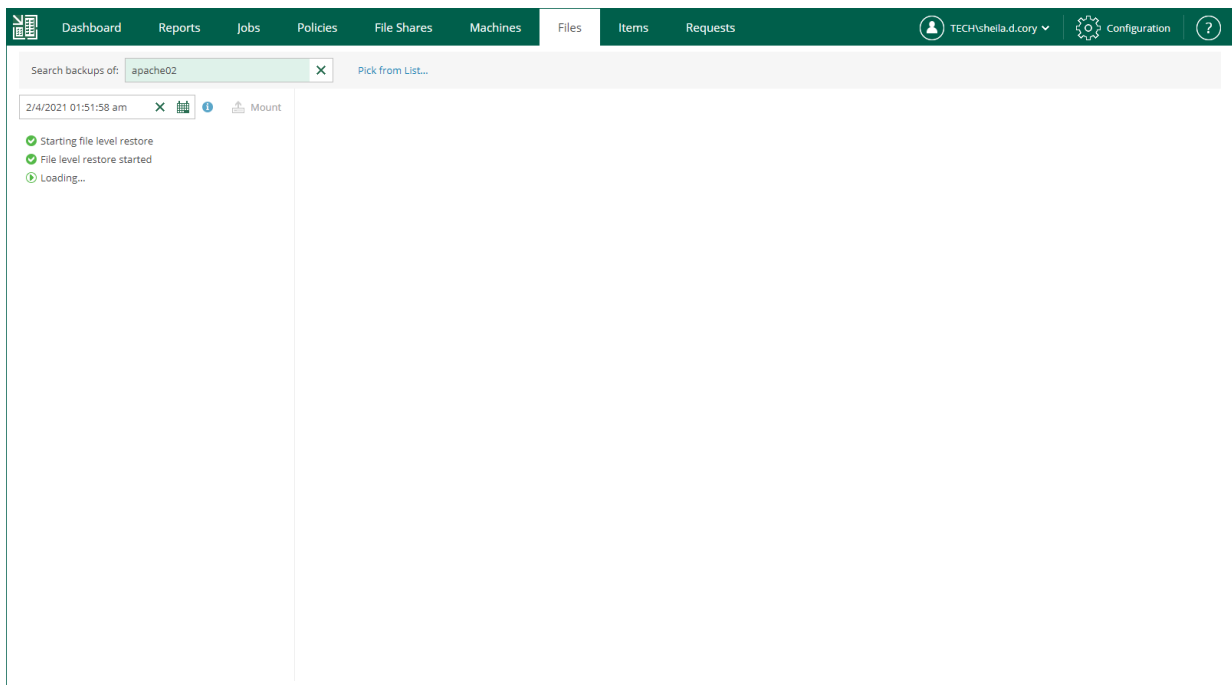
Browsing Machine Backups for Guest OS Files

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.

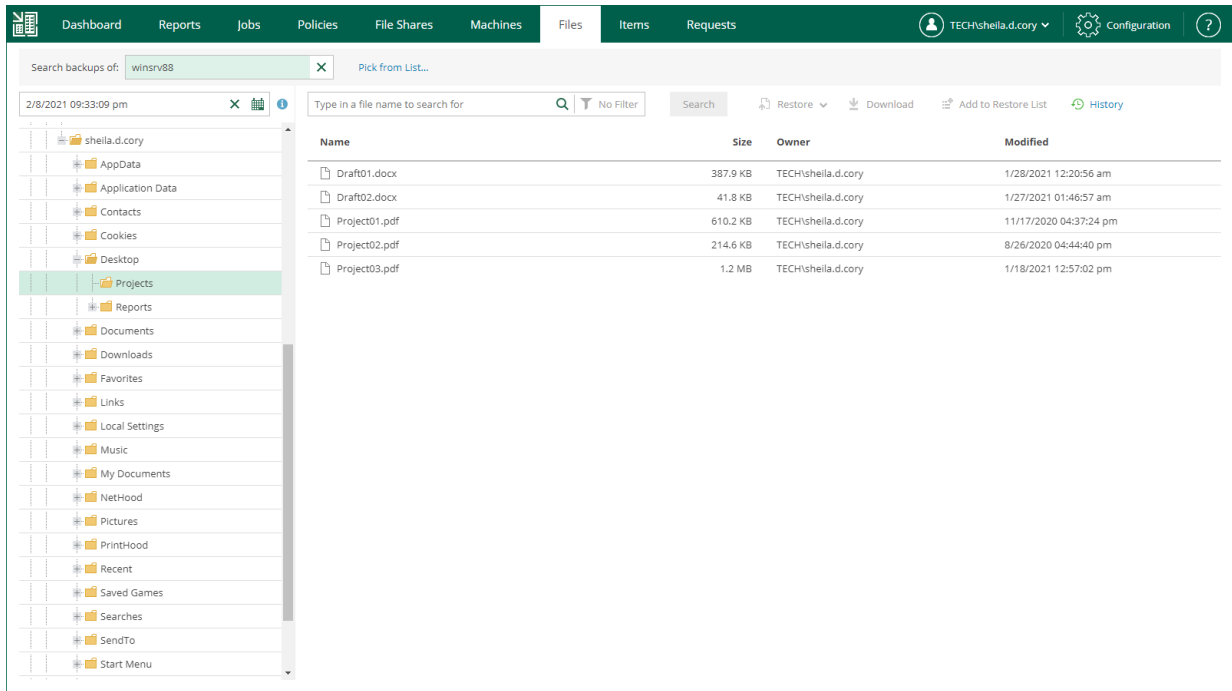
To browse guest OS files in a machine backup:

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.

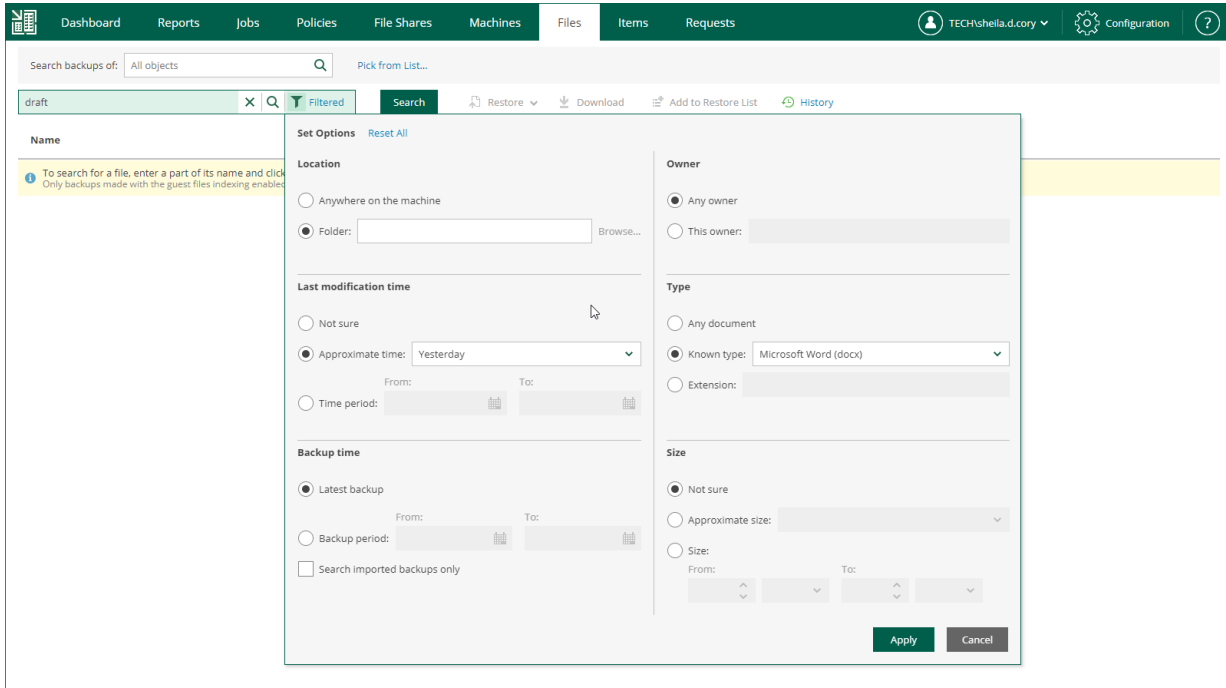
The simple search allows you to search for guest OS files in the latest restore point of the selected machine backup. To perform simple search:

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 Permissions for File and Application Item Restore](#).

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 extracts the object (file or folder) from the backup and restores 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.

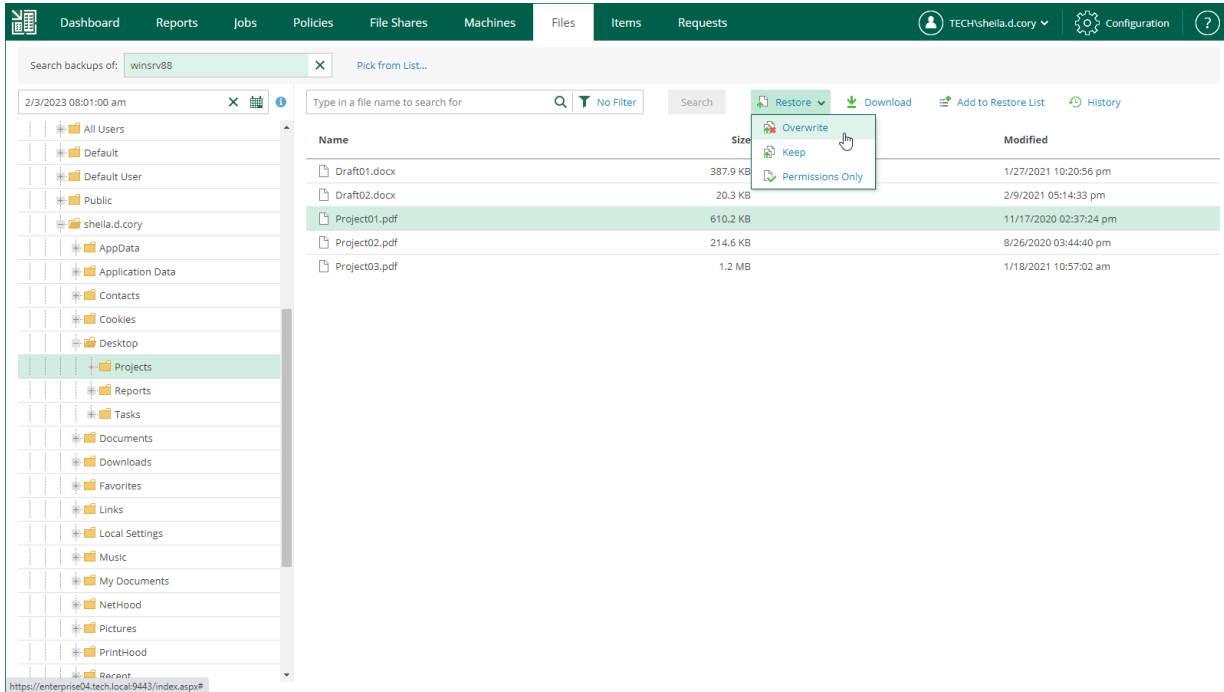
To restore a file or folder to the original location:

1. Locate the necessary object 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 object from the backup will replace the original object on the target machine.
 - If you select **Keep**, the object from the backup will be restored next to the original object on the target machine. The restored object will have the `_RESTORED_<DATE>_<TIME>` prefix in its name, where `<DATE>_<TIME>` is the restore date and time.
 - [For Microsoft Windows] If you select **Permissions Only**, you will restore file (or folder) permissions that were granted to users and groups to access the object. You can restore permissions only if the object exists on the target machine.
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](#).

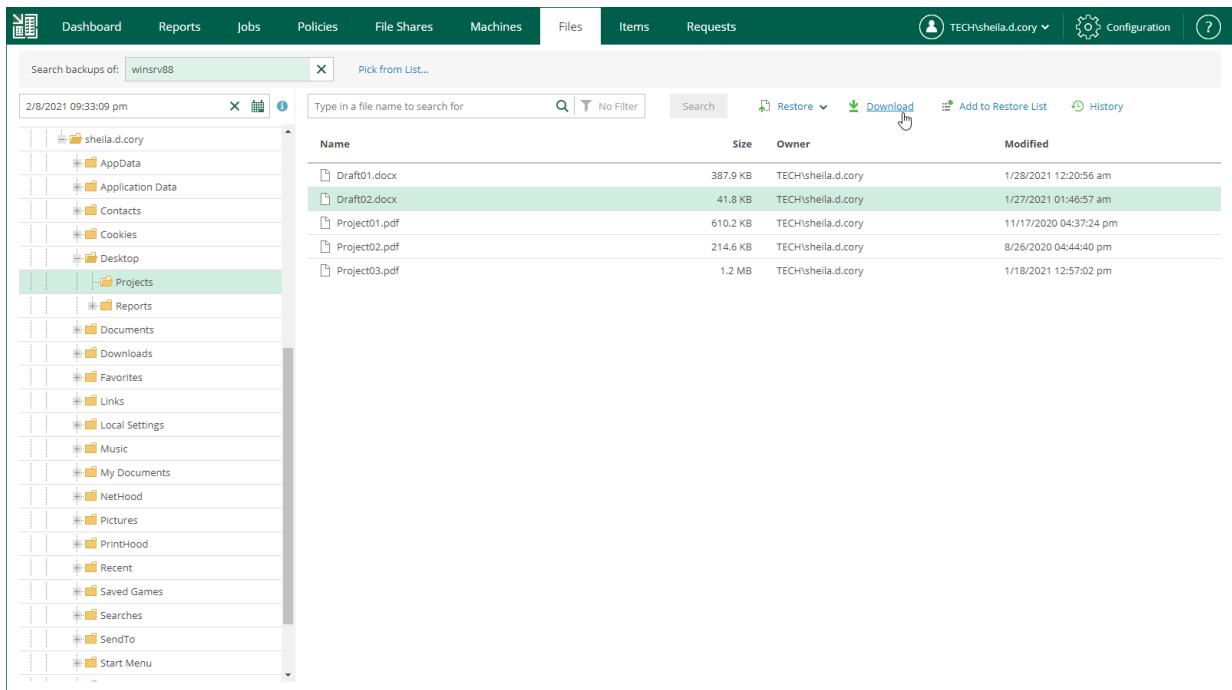


Downloading Files to Local Machine

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](#).

File Restore History

Initiated by	Started at	Status	Ended at	Total Objects	Progress	Target
TECH@shella.d.cory	2/9/2021 02:12:27 am	Success	2/9/2021 02:12:39 am	1	100%	Download

Log

- Starting data transfer agent on server 'enterprise04.tech.local'.
- Processing item 1 of 1: "Draft02.docx"
- Folders restored: 0
- Files restored: 1
- Total size: 41.8 KB
- Stopping data transfer agents on server 'enterprise04.tech.local'.
- Updating FLR session history
- Packing restored files
- Restored files are available for [download](#)

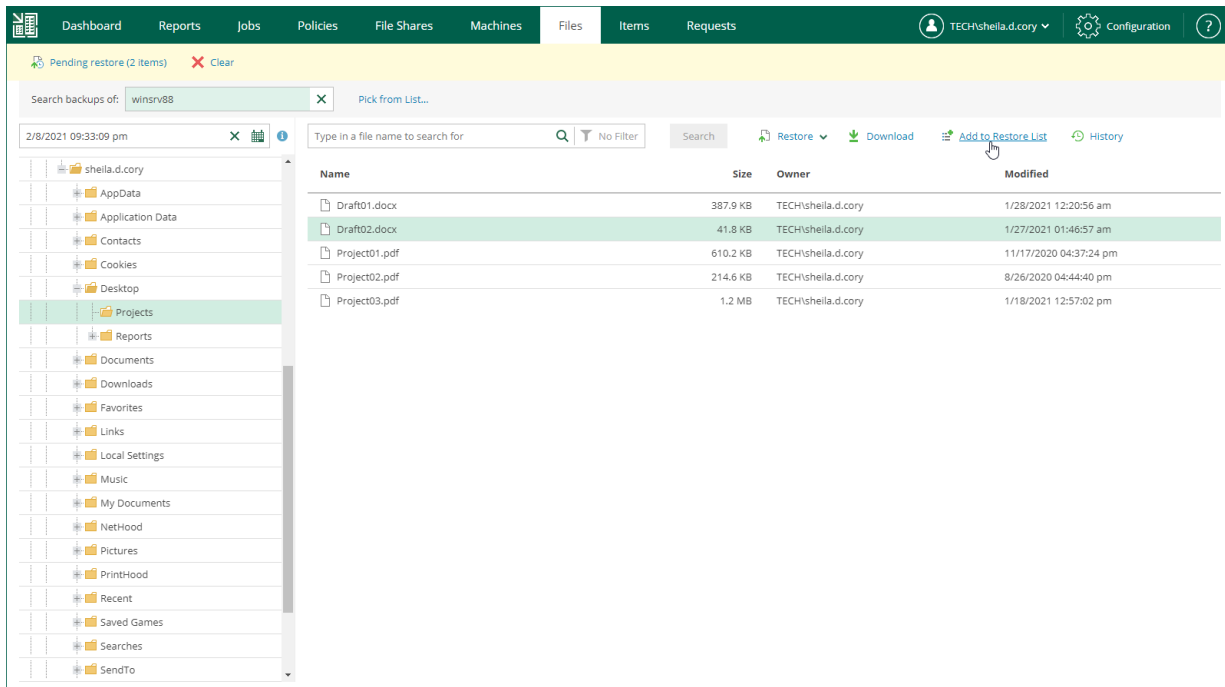
Restoring Multiple Files

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.

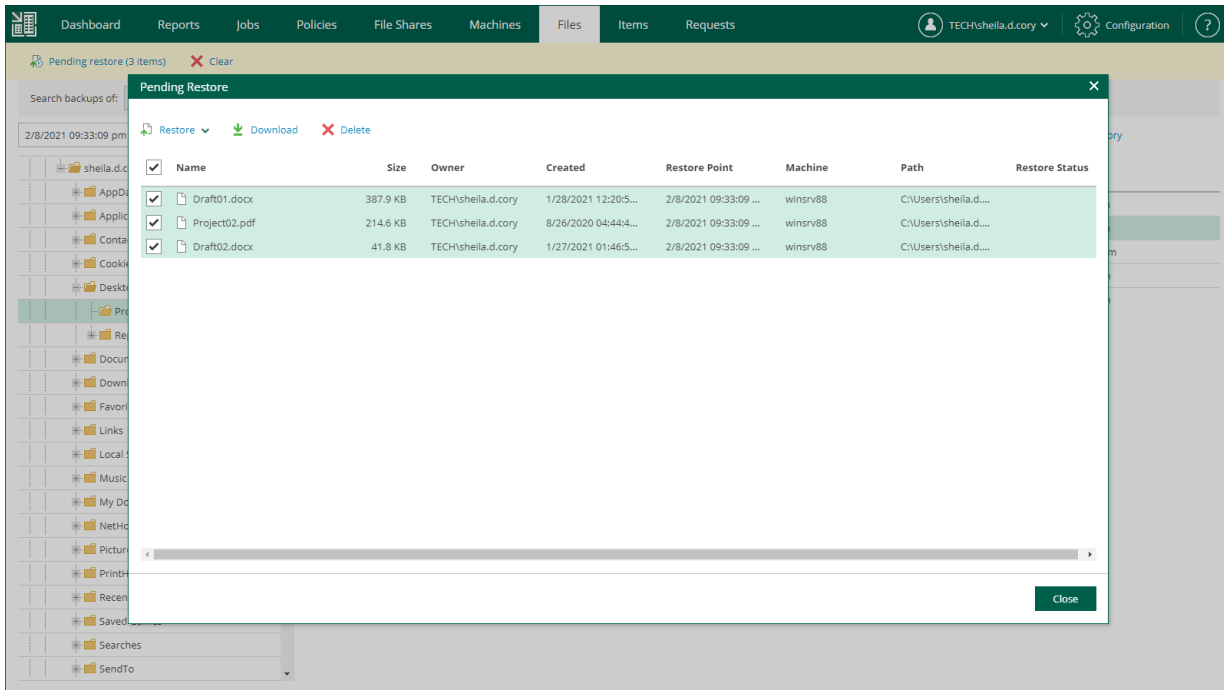
The files are saved to the default download folder on your local machine.

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 [Configuring 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).

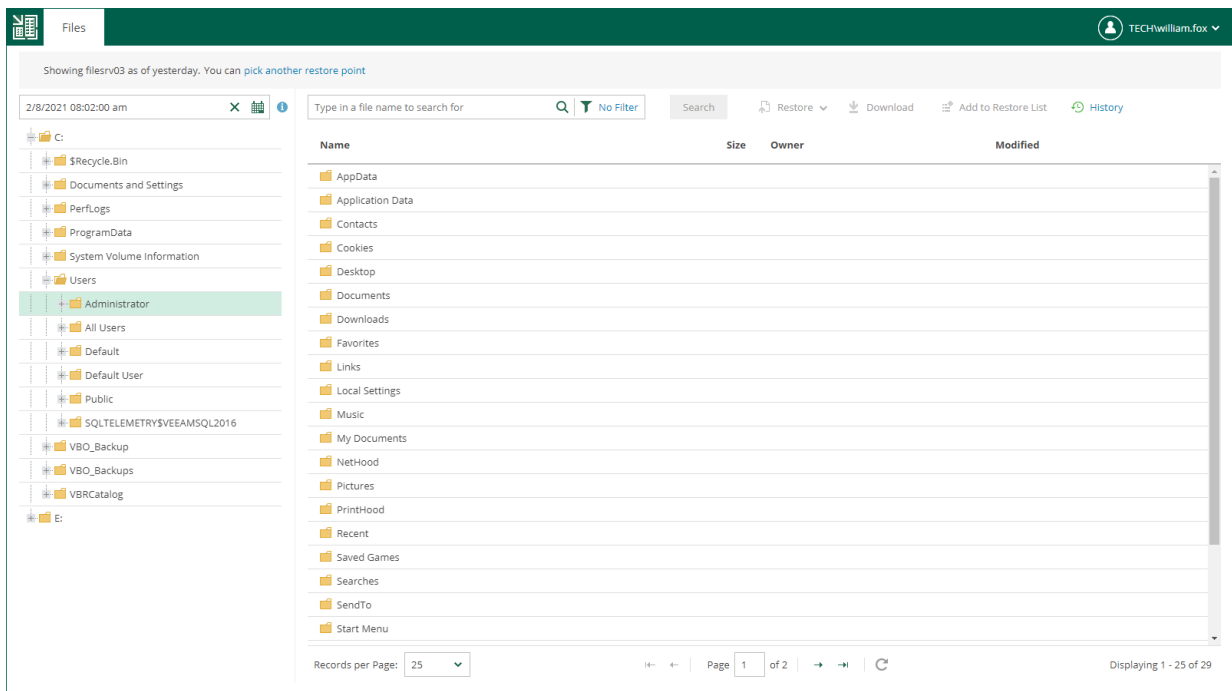
Browsing Guest OS Files Through Self-Service Portal

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](#).

Application Item Restore

Veeam Backup Enterprise Manager supports item-level recovery directly from backups or replicas. These backups and replicas must be created with enabled application-aware processing. If you restore a database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then the job processing the VM must handle database logs. For more information, see [Application-Aware Processing](#).

With Veeam Backup Enterprise Manager, you can restore the following application items:

- [Microsoft Exchange items](#)
- [Microsoft SQL Server databases](#)
- [Oracle databases](#)
- [PostgreSQL instances](#)

Restoring Microsoft Exchange Items

You can restore Microsoft Exchange items (emails, tasks, calendars) from backups of Microsoft Exchange Server machines.

Before You Begin

Before you restore application items, consider the following considerations and limitations:

- Application item restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Enterprise Manager does not support application item restore from storage snapshots.
- Enterprise Manager users can restore items to the original location or a new location within the restore scope. Users must also have sufficient permissions to restore application items. Users with the Portal Administrator role have no limitations. For more information, see [Configuring Accounts and Roles](#).
- To be able to restore Microsoft Exchange items, 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.
- You can restore deleted Microsoft Exchange items to the production mailbox only.
- When you restore application items with Enterprise Manager, restore limitations listed in the [Considerations and Limitations](#) section of the Veeam Explorers User Guide are also applied.

Performing Restore

To restore a Microsoft Exchange item to the production Exchange Server, take the following steps:

1. Open the **Items** tab and click **Mailbox Items**.
2. 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.
3. 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 and a restore point created on that date. By default, the latest valid restore point is selected.

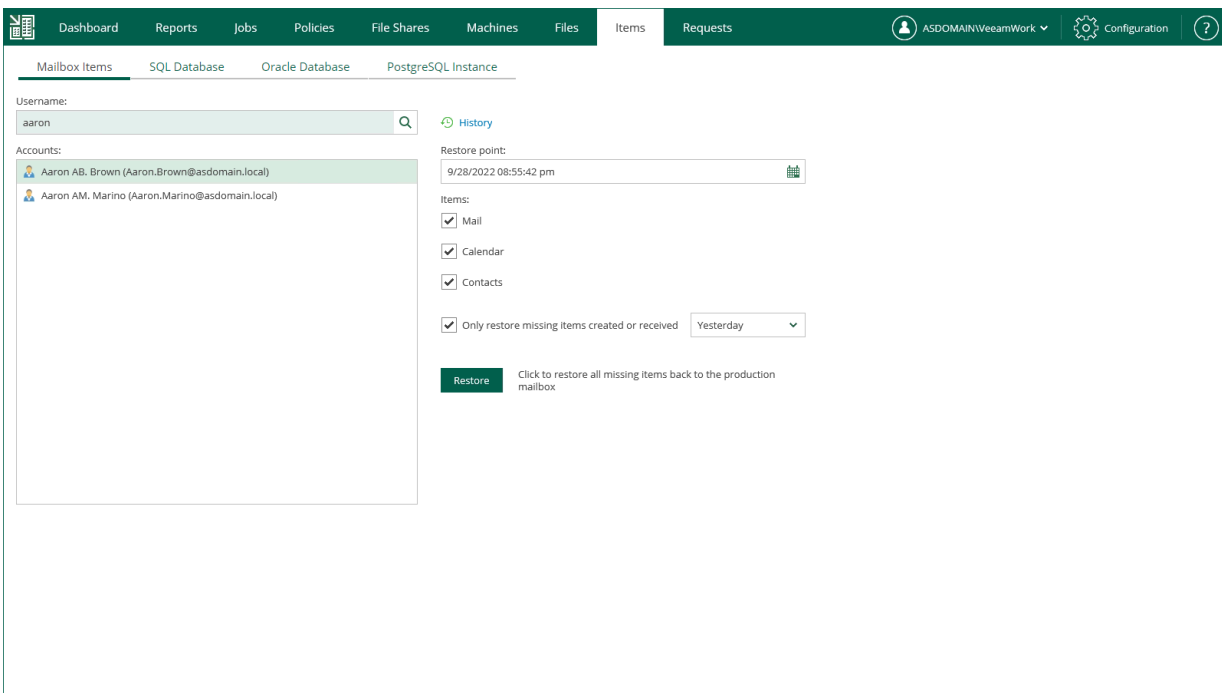
NOTE

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.
- If the specified user mailbox does not exist in the restore point, Veeam Backup Enterprise Manager will display an error message.

4. In the **Items** section, select the type of item you want to restore:
 - Mail
 - Calendar
 - Contacts
5. To restore only missing items created or received during a certain period, select the **Only restore missing items created or received <time period>** check box and select the period from the drop-down list.
6. Click **Restore**. Items that meet the specified conditions will be restored to the production Exchange Server.

To view a restore session log, click **History**.



Restoring Microsoft SQL Server Databases

You can restore a Microsoft SQL Server database by following one of the following scenarios:

- [Restore to the original location](#) – to restore a Microsoft SQL Server database to the original location with the same settings.
- [Restore with custom settings](#) – restore a Microsoft SQL Server database to a new location, or to any location but with different settings.

Before You Begin

Before you restore application items, consider the following prerequisites:

- Application item restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Enterprise Manager does not support application item restore from storage snapshots.
- Enterprise Manager users can restore items to the original location or a new location within the restore scope. Users must also have sufficient permissions to restore application items. Users with the Portal Administrator role have no limitations. For more information, see [Configuring Accounts and Roles](#).
- When you restore application items with Enterprise Manager, restore limitations listed in the [Considerations and Limitations](#) section of the Veeam Explorers User Guide are also applied.

Restore to Original Location

This scenario allows you to restore a Microsoft SQL Server database to the original location.

When performing database restore to the original location, a temporary iSCSI connection is established between the target Microsoft 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.

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the Microsoft SQL Server machine or the account you are currently logged in.
2. 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 provide the necessary credentials.

The security role specified for this account in Enterprise Manager must allow the user to restore Microsoft SQL Server databases. For more information, see [Configuring Permissions for File and Application Item Restore](#).

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.

To restore a Microsoft SQL Server database, take the following steps:

1. Open the **Items** tab and click **SQL Database**.
2. In the **SQL Server** field, enter a name of Microsoft SQL Server hosting the database you need to restore; use the *server_name|instance_name* format.

Alternatively, click the **Pick from List** link to choose a machine from the list of available Microsoft SQL Server backups.
3. From the **Database to restore** list, select the database you need.
4. 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. By default, the latest valid restore point is selected.
5. 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 restore point):
 - The beginning point refers to the previous restore point of the Microsoft SQL Server machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [Microsoft SQL Server Transaction Log Settings](#).

6. In the **Restore to** section, select the **Original location** option.

7. Click **Restore**.

To view a restore session log, click **History**.

The screenshot displays the Veeam Backup Enterprise Manager interface for configuring a restore operation. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECHSheila.d.cory'. The main content area is divided into tabs: 'Mailbox Items', 'SQL Database', 'Oracle Database', and 'PostgreSQL Instance'. The 'SQL Database' tab is active, showing the 'SQL server' as 'MSSQL021'. Below this, a list of databases to restore is shown, including 'db1', 'db2', 'HR', 'IT', and 'Sales'. The 'Restore point' is set to '3/6/2023 05:07:10 am'. A 'Point in time' slider is visible, with a selected point at '3/6/2023 05:06:30 am'. The 'Restore to' options are 'Original location' (selected) and 'Alternative location'. A 'Restore' button is present, with a tooltip that reads: 'Restore state as of 3/6/2023 05:06:30 am to original location'. A 'History' link is also visible next to the 'SQL server' field.

Restore with Custom Settings

You can use this scenario to restore a Microsoft SQL Server database to a new location, or to any location but with different settings.

To restore an Oracle database with custom settings, use the **SQL Restore** wizard.

1. [Launch the SQL Restore wizard.](#)
2. [Specify a target server.](#)
3. [Specify AlwaysOn restore settings.](#)
4. [Specify files location.](#)

Step 1. Launch SQL Restore Wizard

To launch the **SQL Restore** wizard, do the following:

1. Open the **Items** tab and click **SQL Database**.
2. In the **SQL Server** field, enter a name of Microsoft SQL Server hosting the database you need to restore; use the *server_name|instance_name* format.

Alternatively, click the **Pick from List** link to a machine from the list of available Microsoft SQL Server backups.

3. From the **Database to restore** list, 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 Microsoft 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.

The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see [Configuring Permissions for File and Application Item Restore](#).

4. 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. By default, the latest valid restore point is selected.
5. 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 restore point):
 - The beginning point refers to the previous restore point of the Microsoft SQL Server machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [Microsoft SQL Server Transaction Log Settings](#).

6. In the **Restore to** section, select the **Alternative location** option.

7. Click Restore.

The screenshot displays the Veeam Backup Enterprise Manager interface for configuring a restore. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\sheila.d.cory'. The 'SQL Database' tab is active, showing the 'MSSQL02' server. The 'Database to restore' list includes 'db1', 'db2', 'HR', 'IT', and 'Sales'. The 'Restore point' is set to '3/6/2023 05:07:10 am'. The 'Point in time' slider is set to '3/6/2023 05:06:30 am'. The 'Restore to' options are 'Original location' and 'Alternative location', with 'Alternative location' selected. A 'Restore' button is visible, with a tooltip that reads: 'Restore state as of 3/6/2023 05:06:30 am to alternative location'.

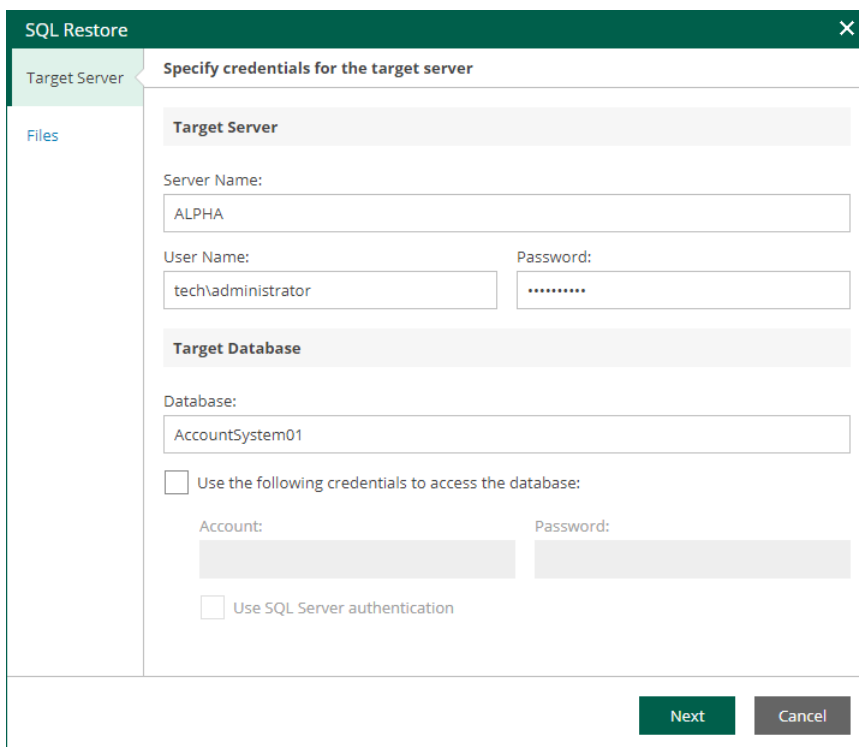
Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify settings to connect to the target server and the database.

1. In the **Target Server** section, enter the name of the Microsoft SQL Server or Microsoft SQL Server instance in the `<server IP or FQDN>|<instance name>` format, and credentials of the account that will be used to connect to the target server.

If the SQL Server instance is assigned a custom port, and Microsoft SQL Browser is not running on the machine, specify the instance port in the following format: `<server IP or FQDN>, <port>`.

2. In the **Target Database** section, specify the following database connection settings:
 - a. In the **Database** field, enter the name of the target database.
 - b. To use a separate account for connection to the target database, select the **Use the following credentials to access the database** check box and specify credentials of the necessary account.
 - c. To use Microsoft SQL Server authentication when connecting to the database, select the **Use SQL Server authentication** check box.



The screenshot shows the 'SQL Restore' wizard window, specifically the 'Specify credentials for the target server' step. The window has a dark green header with the title 'SQL Restore' and a close button. On the left, there is a sidebar with 'Target Server' selected and 'Files' below it. The main area is titled 'Specify credentials for the target server' and contains the following fields and options:

- Target Server** section:
 - Server Name: ALPHA
 - User Name: tech\administrator
 - Password: [masked]
- Target Database** section:
 - Database: AccountSystem01
 - Use the following credentials to access the database:
 - Account: [masked]
 - Password: [masked]
 - Use SQL Server authentication

At the bottom right, there are 'Next' and 'Cancel' buttons.

Step 3. Specify AlwaysOn Restore Settings

The **SQL Server Always On** step of the wizard is available if the specified target SQL Server supports AlwaysOn Availability Groups.

At this step of the wizard, you can add the restored database to an Availability Group.

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 Backup & Replication will restore the database to the primary server and then replicate it to secondary nodes.

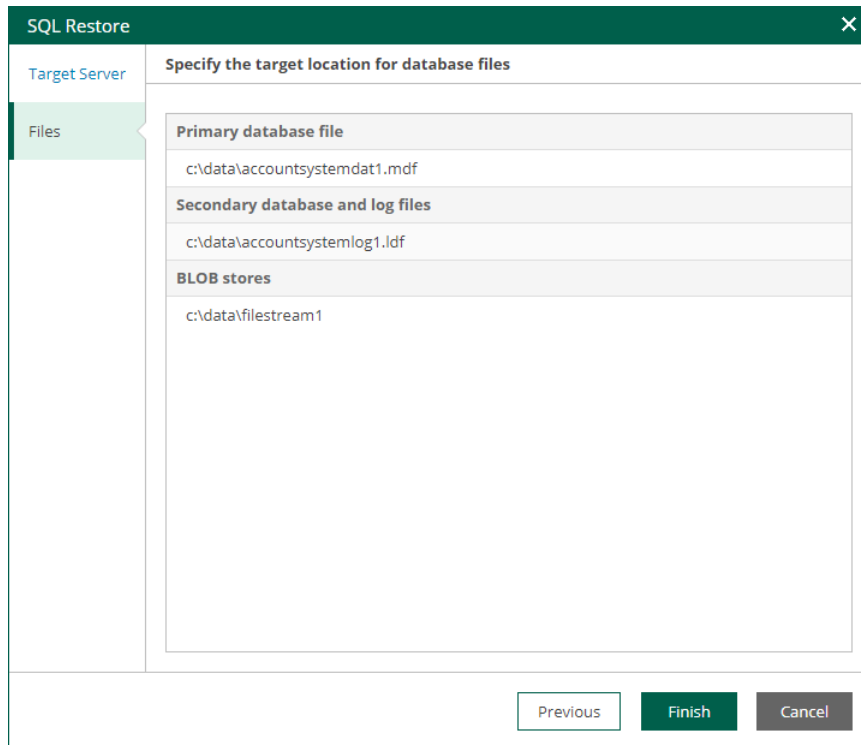
If you do not plan to use the AlwaysOn capabilities when restoring a database, clear the **Add the database to the following Availability Group** check box.

The screenshot shows the 'SQL Restore' wizard window. The left sidebar has three items: 'Target Server', 'SQL Server Always On' (which is selected and highlighted in green), and 'Files'. The main area is titled 'Specify Always On cluster restore parameters'. It contains a checked checkbox labeled 'Add database to the following Availability Group:'. Below this is a dropdown menu showing 'AON1'. Underneath, there is a section titled 'Database will be replicated to the following nodes:'. This section is divided into two expandable categories: 'Primary' and 'Secondary'. The 'Primary' category is expanded and shows 'ALPHA'. The 'Secondary' category is also expanded and shows 'ALPHA_2' and 'ALPHA_3'. At the bottom of the window, there are three buttons: 'Previous', 'Next' (highlighted in green), and 'Cancel'.

Step 4. Specify Files Location

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. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.



The screenshot shows the 'SQL Restore' wizard window. The title bar is dark green with the text 'SQL Restore' and a close button. The main area is divided into two panes. The left pane is titled 'Target Server' and has a 'Files' tab selected. The right pane is titled 'Specify the target location for database files' and contains three sections: 'Primary database file' with the path 'c:\data\accountsystemdat1.mdf', 'Secondary database and log files' with the path 'c:\data\accountsystemlog1.ldf', and 'BLOB stores' with the path 'c:\data\filestream1'. At the bottom of the window are three buttons: 'Previous', 'Finish', and 'Cancel'.

Section	Path
Primary database file	c:\data\accountsystemdat1.mdf
Secondary database and log files	c:\data\accountsystemlog1.ldf
BLOB stores	c:\data\filestream1

Restoring Oracle Databases

You can restore an Oracle database by following one of the following scenarios:

- [Restore to the original location](#) – to restore an Oracle instance to the original location with the same settings.
- [Restore with custom settings](#) – restore an Oracle instance to a new location, or to any location but with different settings.

Before You Begin

Before you restore application items, consider the following prerequisites:

- Application item restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Enterprise Manager does not support application item restore from storage snapshots.
- Enterprise Manager users can restore items to the original location or a new location within the restore scope. Users must also have sufficient permissions to restore application items. Users with the Portal Administrator role have no limitations. For more information, see [Configuring Accounts and Roles](#).
- When you restore application items with Enterprise Manager, restore limitations listed in the [Considerations and Limitations](#) section of the Veeam Explorers User Guide are also applied.

Restore to Original Location

This scenario allows you to restore an Oracle database to the original location.

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.

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Oracle server machine or the account you are currently logged in.
2. 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.

The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see [Configuring Permissions for File and Application Item Restore](#).

To restore an Oracle database, take the following steps:

1. Open the **Items** tab and click **Oracle Database**.
2. In the **Server** field, enter a name of the Oracle server hosting the database you need to restore.
Alternatively, click the **Pick from List** link to select a machine from the list of available Oracle backups.
3. From the **Database to restore** list, select Oracle home and the database you need.
4. 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. By default, the latest valid restore point is selected.
5. 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 restore point):
 - The beginning point refers to the previous restore point of the Oracle machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [Oracle Archived Redo Log Settings](#).

6. In the **Restore to** section, select the **Original location** option.
7. Click **Restore**.

To view a restore session log, click **History**.

The screenshot displays the Veeam Backup Enterprise Manager interface for configuring a restore session. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\sheila.d.cory'. The 'Oracle Database' tab is selected under the 'Mailbox Items' category.

Server: winorcl01.tech.local

Database to restore: winorcl01.tech.local (containing OraDB19Home1 and orcl)

Restore point: 3/5/2023 10:04:54 pm

Point in time: A timeline slider shows a range from 3/4/2023 10:33:04 pm to 3/6/2023 01:17:26 pm, with a selected point at 3/5/2023 10:05:09 pm.

Restore to: Original location, Alternative location

Restore: Restore state as of 3/5/2023 10:04:54 pm to original location

Restore with Custom Settings

You can use this scenario to restore a PostgreSQL instance to a new location, or to any location but with different settings.

To restore an Oracle database with custom settings, use the **Oracle Restore** wizard.

1. [Launch the Oracle Restore wizard.](#)
2. [Specify a target server.](#)
3. [Specify Oracle home settings.](#)
4. [Specify database files location.](#)

Step 1. Launch Oracle Restore Wizard

To launch the **Oracle Restore** wizard, do the following:

1. Open the **Items** tab and click **Oracle Database**.
2. In the **Server** field, enter a name of the Oracle server hosting the database you need to restore.
Alternatively, click the **Pick from List** link to select a machine from the list of available Oracle backups.
3. From the **Database to restore** list, 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.
4. 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. By default, the latest valid restore point is selected.
5. 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 restore point):
 - The beginning point refers to the previous restore point of the Oracle machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [Oracle Archived Redo Log Settings](#).

6. In the **Restore to** section, select the **Alternative location** option.

7. Click Restore.

The screenshot displays the Veeam Backup Enterprise Manager interface for configuring a restore request. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH\sheila.d.cory'. The 'Requests' tab is active, and the 'Oracle Database' sub-tab is selected.

Server: winorcl01.tech.local

Database to restore: winorcl01.tech.local, OraDB19Home1, orcl

Restore point: 3/5/2023 10:04:54 pm

Point in time: 3/4/2023 10:33:04 pm to 3/6/2023 01:17:26 pm (selected: 3/5/2023 10:05:09 pm)

Restore to: Original location, Alternative location

Restore Restore state as of 3/5/2023 10:04:54 pm to alternative location

URL: https://enterprise04.tech.local:9443/index.aspx#requests

Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify connection settings required to access the target Oracle server. The set of connection settings depends on the OS type of the target server: Windows or Linux.

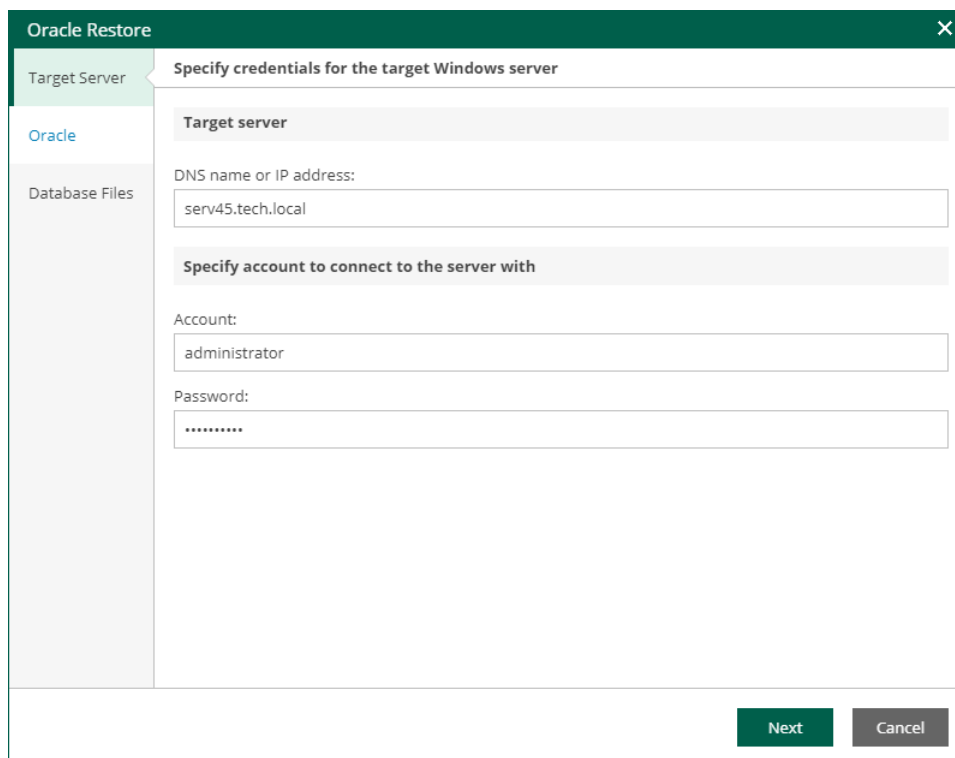
Windows-Based Oracle Server

For database restore to a Microsoft Windows server, specify the following connection settings:

1. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Microsoft Windows server.
2. In the **Account** and **Password** fields, specify credentials of the account that will be used for connection with the target Windows-based Oracle 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.



The screenshot shows the 'Oracle Restore' wizard window. The title bar is 'Oracle Restore' with a close button. The main area is titled 'Specify credentials for the target Windows server'. On the left, there is a sidebar with three options: 'Target Server' (selected), 'Oracle', and 'Database Files'. The main content area has three sections: 'Target server' with a text box containing 'serv45.tech.local'; 'Specify account to connect to the server with' with 'Account:' and 'Password:' labels and corresponding text boxes. The 'Account' box contains 'administrator' and the 'Password' box contains '.....'. At the bottom right, there are 'Next' and 'Cancel' buttons.

Linux-Based Oracle Server

For database restore to a Linux server, specify the following connection settings:

1. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Linux server.
2. In the **SSH port** field, specify a port number of the target Oracle server (by default, port 22 is used).

3. In the **Account** field, 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:
 - a. Select the **Private key is required for this connection** check box.
 - b. In the **Private key** field, specify a key.
To select a key, click **Browse** and select a key.
 - c. In the **Passphrase** field, enter the passphrase.
6. If you have specified a non-root account that does not have root permissions on the target server, do the following.
 - 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 the `sudo` command is not available or may fail on the target Linux server, 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, the `su` command will be used.

Consider that the user account must be a member of the **dba** group.

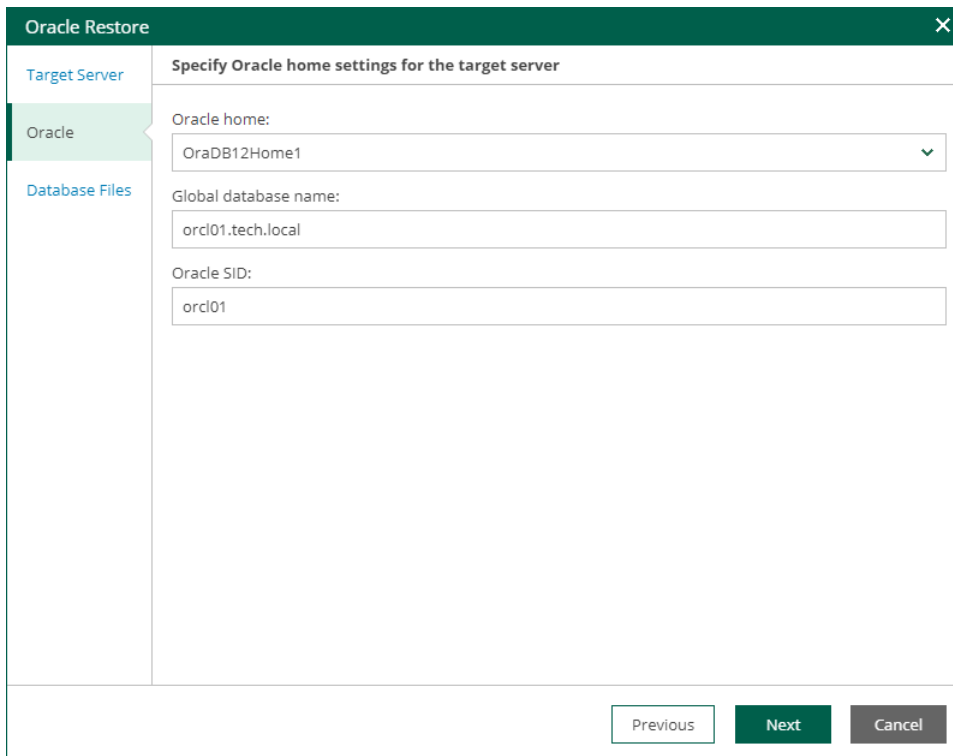
The screenshot shows the 'Oracle Restore' dialog box with the 'Specify credentials for the target Linux server' step selected. The 'Target Server' section contains a 'Target server' field with 'linorcl01' in the 'DNS name or IP address' field and '22' in the 'Port' field. The 'Specify account to connect to the server with' section has 'oracle' in the 'Account' field and a masked password in the 'Password' field. There are three checkboxes: 'Private key is required for this connection' (unchecked), 'Elevate specified account to root' (checked), and 'Add account to the sudoers file automatically' (unchecked). Below these are fields for 'Private Key' (with a 'Browse...' button) and 'Passphrase'. At the bottom, there is a 'Root password' field and 'Next' and 'Cancel' buttons.

Step 3. Specify Oracle Home Settings

At the **Oracle** step of the wizard, specify Oracle home settings.

1. In the **Oracle home** field, specify Oracle home.
2. In the **Global database name** field, specify a full name of the database including its network domain.
3. In the **Oracle SID** field, specify the database system identifier.

If a database with the specified SID exists on the target Oracle home, the restore process 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.

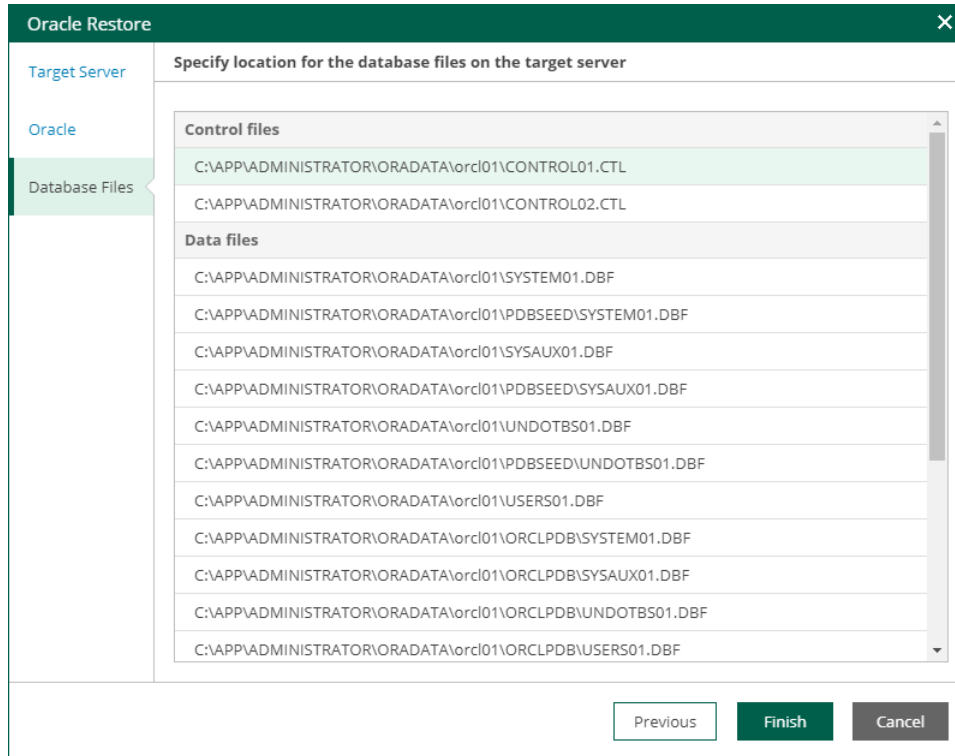


The screenshot shows the 'Oracle Restore' wizard window. The title bar is green with a close button. The main area is divided into a left sidebar and a main content area. The sidebar has three sections: 'Target Server' (blue), 'Oracle' (green, selected), and 'Database Files' (blue). The main content area is titled 'Specify Oracle home settings for the target server' and contains three input fields: 'Oracle home:' with a dropdown menu showing 'OraDB12Home1', 'Global database name:' with a text box containing 'orcl01.tech.local', and 'Oracle SID:' with a text box containing 'orcl01'. At the bottom right, there are three buttons: 'Previous' (white), 'Next' (green), and 'Cancel' (grey).

Step 4. Specify Database Files Location

At the **Database Files** step of the wizard, specify paths to database files on the target server. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.



Restoring PostgreSQL Instances

With Enterprise Manager you can restore PostgreSQL data at the instance level. To restore a PostgreSQL instance, follow one of the following scenarios:

- [Restore to the original location](#) – to restore a PostgreSQL instance to the original location with the same settings.
- [Restore with custom settings](#) – restore a PostgreSQL instance to a new location, or to any location but with different settings.

Before You Begin

Before you restore a PostgreSQL instance, consider the following prerequisites:

- Application item restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Enterprise Manager does not support application item restore from storage snapshots.
- Enterprise Manager users can restore items to the original location or a new location within the restore scope. Users must also have sufficient permissions to restore application items. Users with the Portal Administrator role have no restrictions. For more information, see [Configuring Accounts and Roles](#).
- When you restore application items with Enterprise Manager, restore limitations listed in the [Considerations and Limitations](#) section of the Veeam Explorers User Guide are also applied.

Restore to Original Location

This scenario allows you to restore a PostgreSQL instance to the original location.

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the PostgreSQL machine or the account you are currently logged in.
2. 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 provide the necessary credentials.

For more information on the account roles in Veeam Backup Enterprise Manager that allow a user to restore PostgreSQL, see [Configuring Permissions for File and Application Item Restore](#).

To restore a PostgreSQL instance to the original location, take the following steps:

1. Open the **Items** tab and click **PostgreSQL Instance**.
2. In the **Server** field, enter a VM name where the necessary PostgreSQL instance resides.
Alternatively, click the **Pick from List** link to select from the list of available PostgreSQL machine backups.
3. From the **Instance to restore** list, select a PostgreSQL instance you need.
4. To specify a restore point from which to restore the instance, 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. By default, the latest valid restore point is selected.
5. To view a list of databases included in the restore point, click **Show databases**.
6. For PostgreSQL instances 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 restore point):
 - The beginning point refers to the previous restore point of the PostgreSQL machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [PostgreSQL Archive Log Settings](#).

7. In the **Restore to** section, select the **Original location** option.
8. Click **Restore**.

To view a restore session log, click **History**.

The screenshot displays the Veeam Backup Enterprise Manager interface for configuring a restore session for a PostgreSQL Instance. The top navigation bar includes 'Dashboard', 'Reports', 'Jobs', 'Policies', 'File Shares', 'Machines', 'Files', 'Items', and 'Requests'. The user is logged in as 'TECH@sheila.d.cory'. The main content area is titled 'PostgreSQL Instance' and shows the following configuration options:

- Server:** rhel01 (with a search icon and 'Pick from List...' link)
- Instance to restore:** A list of instances including rhel01, rhel01:5433, rhel01:5434, and rhel01:5435. The instance rhel01:5435 is selected.
- Restore point:** 2/9/2023 04:39:36 pm (with a calendar icon)
- Show databases:** A button to view the list of databases.
- Point in time:** A timeline slider showing a range from 2/9/2023 04:40:32 pm to 2/9/2023 04:47:02 pm, with a selected point at 2/9/2023 04:44:44 pm.
- Restore to:** Radio buttons for 'Original location' (selected) and 'Alternative location'.
- Restore:** A green button with the text 'Restore state as of 2/9/2023 04:44:44 pm to original location'.

Restore with Custom Settings

You can use this scenario to restore a PostgreSQL instance to a new location, or to any location but with different settings.

To restore a PostgreSQL instance with custom settings, use the **PostgreSQL Restore** wizard.

1. [Launch the PostgreSQL Restore wizard.](#)
2. [Specify a target server.](#)
3. [Specify restore settings.](#)
4. [Specify location for database tablespaces.](#)

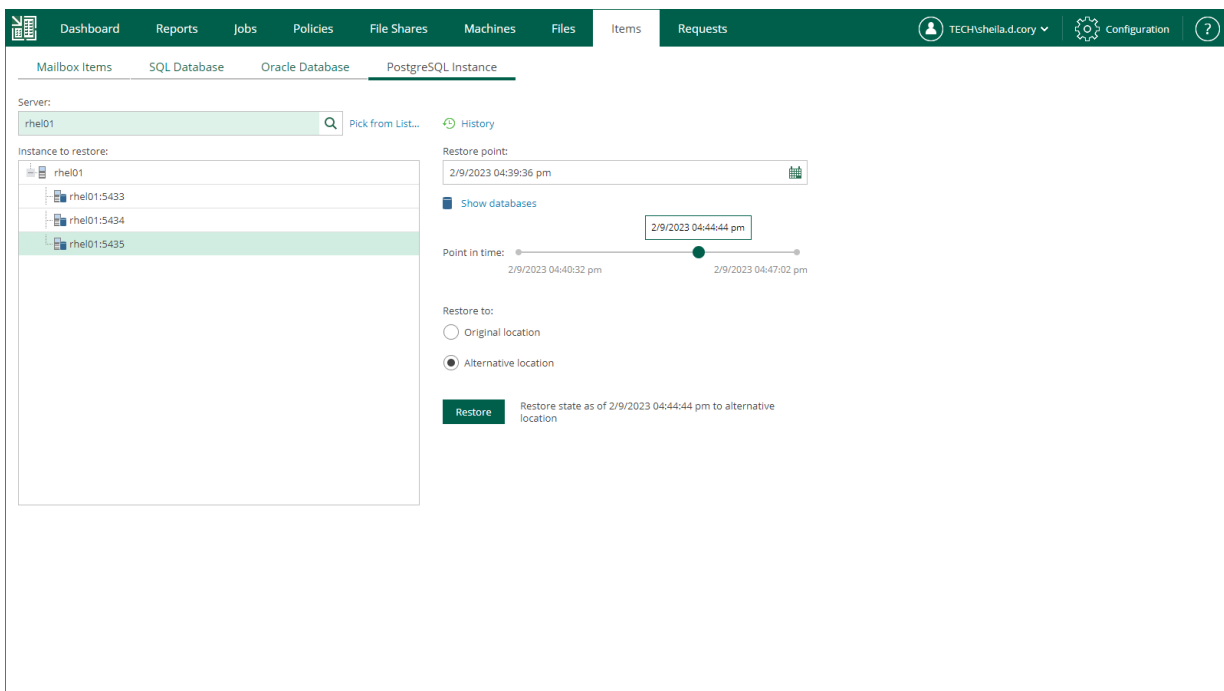
Step 1. Launch PostgreSQL Restore Wizard

To launch the **PostgreSQL Restore** wizard, do the following:

1. Open the **Items** tab and click **PostgreSQL Instance**.
2. In the **Server** field, enter a VM name where the necessary PostgreSQL instance resides.
Alternatively, click the **Pick from List** link to select from the list of available PostgreSQL machine backups.
3. From the **Instance to restore** list, select a PostgreSQL instance you need.
4. To specify a restore point from which to restore the instance, 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.
By default, the latest valid restore point is selected.
5. To view a list of databases included in the restore point, click **Show databases**.
6. For PostgreSQL instances 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 restore point):
 - The beginning point refers to the previous restore point of the PostgreSQL machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
 - The ending point refers to the next restore point that 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 the ending point 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 the ending point refers to the latest log backup time.

For more information on configuring transaction log backup, see [PostgreSQL Archive Log Settings](#).

7. In the **Restore to** section, select the **Alternative location** option.
8. Click **Restore**.



Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify settings for connection to the target PostgreSQL server.

1. In the **Target Server** section, enter a DNS name or IP address of the target server, as well as an SSH port (by default, port 22 is used).
2. Specify credentials of the account that will be used to connect to the target server:
 - a. In the **Account** field, specify the account name.
 - b. In the **Password** field, specify the account password.
 - c. If you want to use a Linux private key for this connection, select the **Private key is required for this connection** check box and specify the following private key settings:
 - i. In the **Private key** field, specify a file that contains a private key.
 - ii. In the **Passphrase** field, enter the passphrase used to decrypt the private key.
 - d. If you have specified a non-root account that does not have root permissions on the target server, select the **Elevate specified account to root** check box.

The account must have root privileges to mount the backed up file system to mount the backed up file system to the target server and to communicate with PostgreSQL.

- i. 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.

- ii. 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.

The screenshot shows the 'PostgreSQL Restore' dialog box with the 'Specify credentials for the target Linux server' section active. The 'Target Server' tab is selected in the left sidebar. The main area contains the following fields and options:

- Target server** section:
 - DNS name or IP address:
 - Port:
- Specify account to connect to the server with** section:
 - Account:
 - Password:
 - Private key is required for this connection
 - Private Key:
 - Passphrase:
 - Elevate specified account to root
 - Add account to the sudoers file automatically
 - Use "su" if "sudo" fails
 - Root password:

At the bottom right, there are two buttons: 'Next' (green) and 'Cancel' (grey).

Step 3. Specify Restore Settings

At the **Restore Settings** step of the wizard, specify instance folder and instance port.

1. In the **Data directory** field, specify a path to the directory where the restored instance data will be stored.
2. In the **Instance port** field, specify a TCP port that will be used to connect to the instance.
3. Select one of the following post-restore actions that the PostgreSQL server must take after the instance is restored. For more information, see the [Specify Post-Restore Action](#) section of the Veeam Explorers User Guide.
 - Select **Promote the instance to accept connections once the recovery is completed** to make the PostgreSQL instance available for connections.
 - Select **Pause the recovery process and keep the instance in a recovery mode** to make the PostgreSQL instance run but not accepting incoming remote TCP connections.
 - Select **Shut down the instance once recovery is completed** to make the PostgreSQL instance stop upon recovery.

The screenshot shows the 'PostgreSQL Restore' wizard window. The title bar is green with a close button. The main area is titled 'Specify PostgreSQL instance restore settings and the data directory path'. On the left, there is a sidebar with three options: 'Target Server' (blue), 'Restore Options' (green), and 'Tablespaces' (grey). The 'Restore Options' section is active and contains the following fields:

- Data directory:** A text input field containing the path `/var/lib/pgsql/13/data`.
- Instance port:** A spinner box showing the value `5436`.
- Post-restore actions:** Three radio button options:
 - Promote the instance to accept connections once the recovery is completed
 - Pause the recovery process at the end and keep the instance in a recovery mode
 - Shut down the instance once the recovery is completed

At the bottom right, there are three buttons: 'Previous' (white), 'Next' (green), and 'Cancel' (grey).

Step 4. Specify Tablespaces

At the **Tablespaces** step of the wizard, enter paths of directories where database tables will be stored. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.

The screenshot shows the 'PostgreSQL Restore' wizard window. The left sidebar has three tabs: 'Target Server', 'Restore Options', and 'Tablespaces', with 'Tablespaces' selected. The main area is titled 'Specify a location for tablespaces' and contains three rows of input fields. Each row has a label and a text input field:

Label	Path
backup	<input type="text" value="/var/lib/pgsql/tblspace6"/>
docs	<input type="text" value="/var/lib/pgsql/tblspace5"/>
sales	<input type="text" value="/var/lib/pgsql/tblspace4"/>

At the bottom right of the window, there are three buttons: 'Previous' (disabled), 'Finish' (active), and 'Cancel' (disabled).

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 [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 a helper host or helper appliance.

Preparing Helper Host or Helper Appliance

When restoring guest OS files, Veeam Backup & Replication mounts machine disks from the backup or replica to a mount server (helper host or helper appliance). For the mount server, you can use a machine running on VMware or Microsoft Hyper-V. You specify mount server settings on the backup server when you configure a backup job for the machine. These settings are saved in the Veeam Backup & Replication database on per-user basis. The settings are applied each time the user starts file-level restore. For more information on the helper host and helper appliance, see the [Restore from Linux, Unix and Other File Systems](#) section of the Veeam Backup & Replication User Guide.

When you start guest OS file restore from Veeam Backup Enterprise Manager, the mount server settings are obtained from the configuration database of the backup server. If no helper host or helper appliance configuration is found for the user account, Veeam Backup & Replication uses the configuration set during the latest file-level restore performed on the backup server. Thus, before you start file-level restore from Enterprise Manager, make sure the mount server settings are configured on the backup server with which Veeam Agent is integrated.

NOTE

If you plan to deploy multiple helper appliances to restore machines backed up by Veeam Agents integrated with different backup servers, their initial configuration must be performed on the backup servers. Centralized configuration from Veeam Backup Enterprise Manager is not supported.

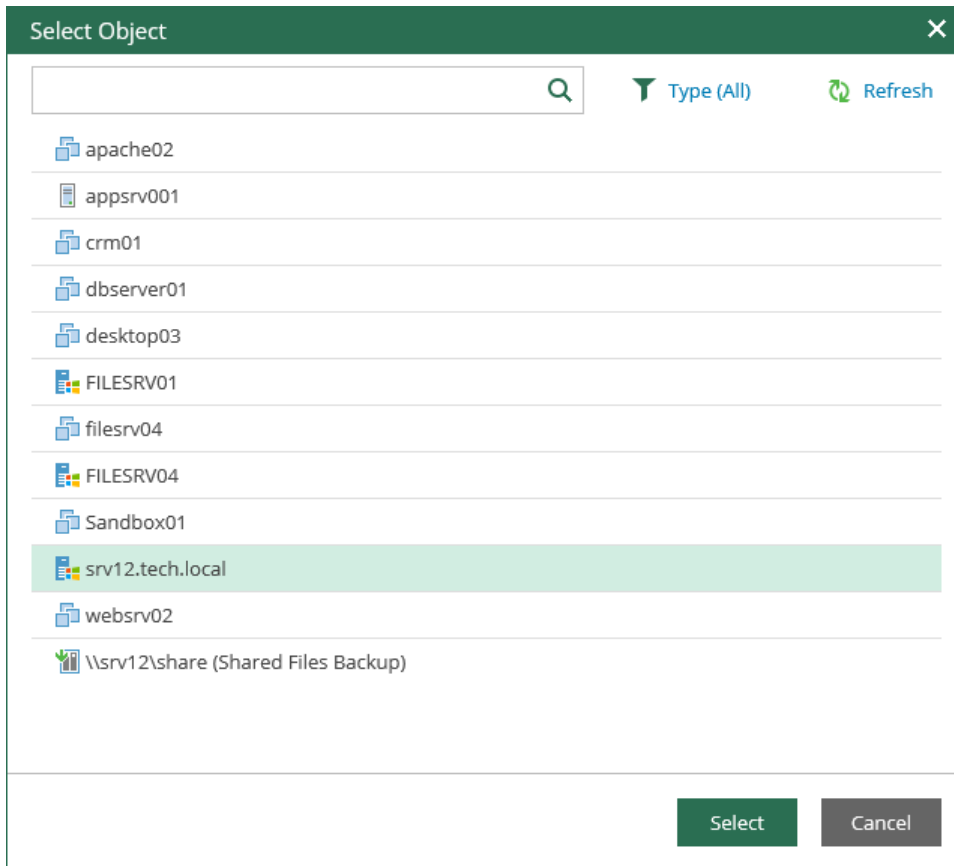
Other Prerequisites

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, take the steps described in the following sections:

- [Restoring Microsoft Exchange Items](#)
- [Restoring Microsoft SQL Server Databases](#)

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](#)

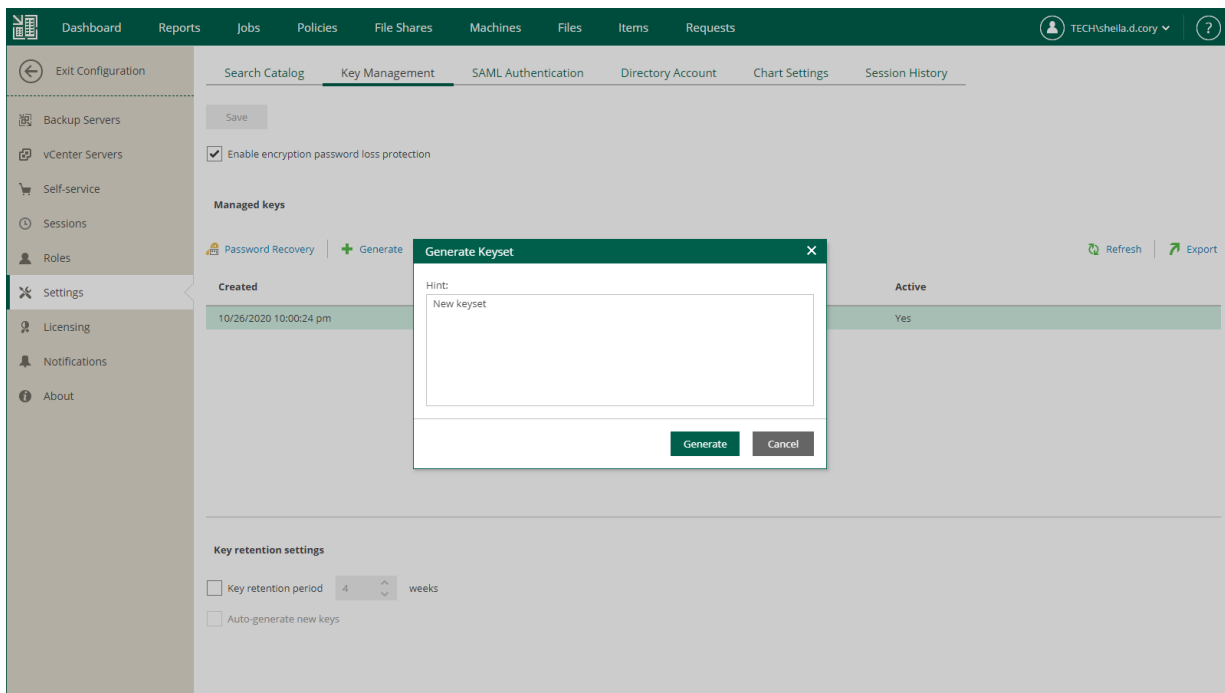
Generating Enterprise Manager Keyset

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.



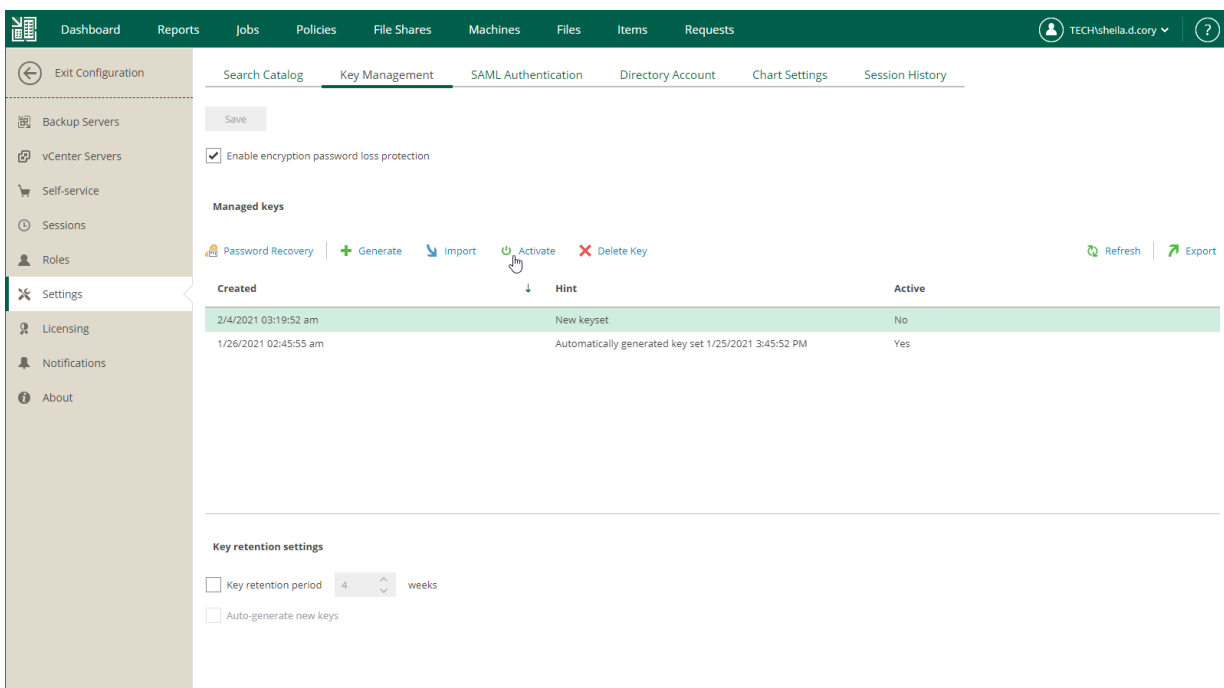
Activating Enterprise Manager Keyset

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.

The screenshot displays the Veeam Backup Enterprise Manager configuration interface. The top navigation bar includes Dashboard, Reports, Jobs, Policies, File Shares, Machines, Files, Items, and Requests. The user is logged in as TECHSheila.d.cory. The left sidebar shows the Settings menu. The main content area is titled 'Key Management' and includes a 'Save' button and a notification 'Changes have not been saved yet'. Below this, there is a checkbox for 'Enable encryption password loss protection'. The 'Managed keys' section features a table with columns for 'Created', 'Hint', and 'Active'. The table contains two rows of keyset data. Below the table, the 'Key retention settings' section includes a checked checkbox for 'Key retention period' set to 4 weeks, and a checked checkbox for 'Auto-generate new keys'.

Created	Hint	Active
2/4/2021 03:19:52 am	New keyset	No
1/26/2021 02:45:55 am	Automatically generated key set 1/25/2021 3:45:52 PM	Yes

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.

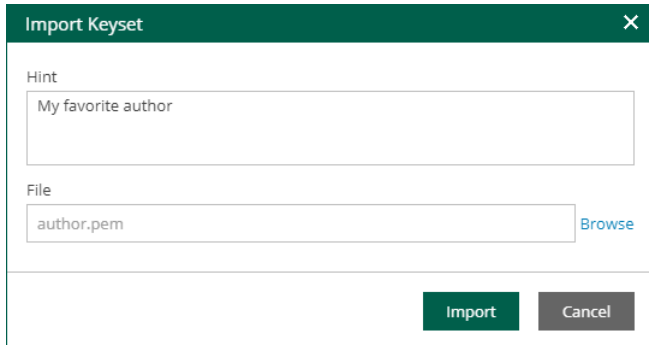
To import a previously exported keyset:

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](#).



The screenshot shows a dialog box titled "Import Keyset" with a close button (X) in the top right corner. The dialog contains the following elements:

- A "Hint" label above a text input field containing the text "My favorite author".
- A "File" label above a text input field containing the text "author.pem". To the right of this field is a "Browse" button.
- At the bottom of the dialog, there are two buttons: "Import" (highlighted in green) and "Cancel" (grey).

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**.

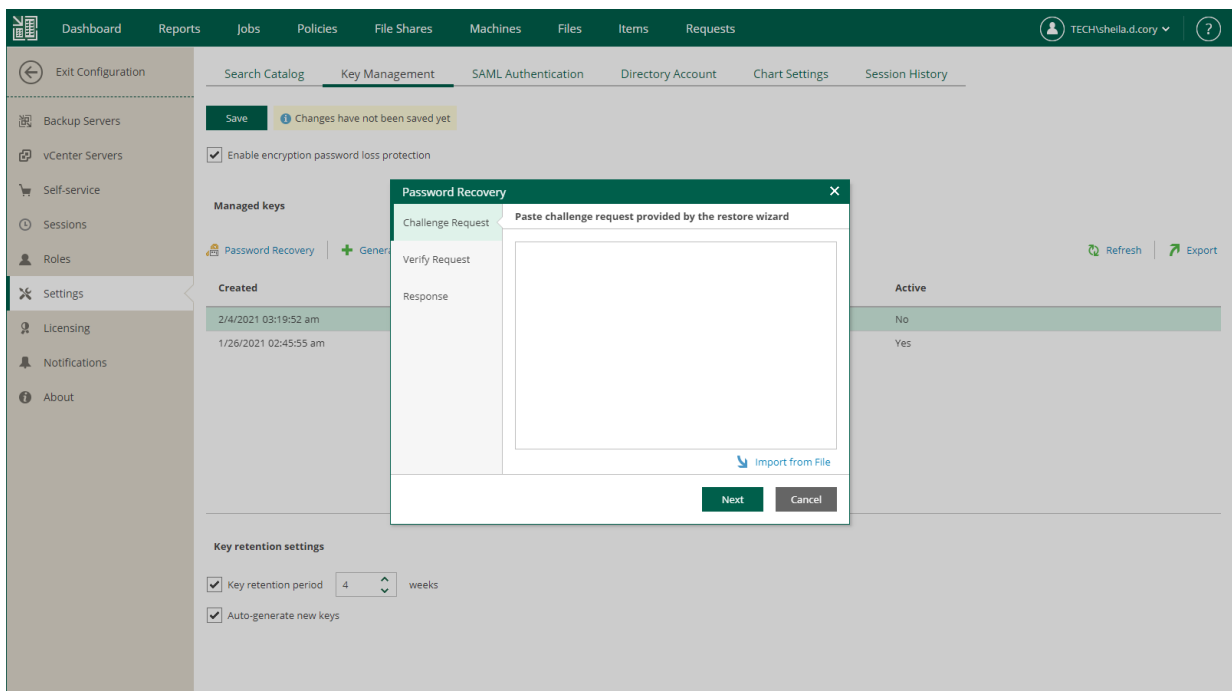
IMPORTANT

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 Veeam Universal Application-Item Recovery (or 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.

New Lab Request [X]

Lab Request | **Select machine to put in the virtual lab**

Machine: apache02

Issued by: TECH\sheila.d.cory

Date: 03:45 pm | 02/04/21

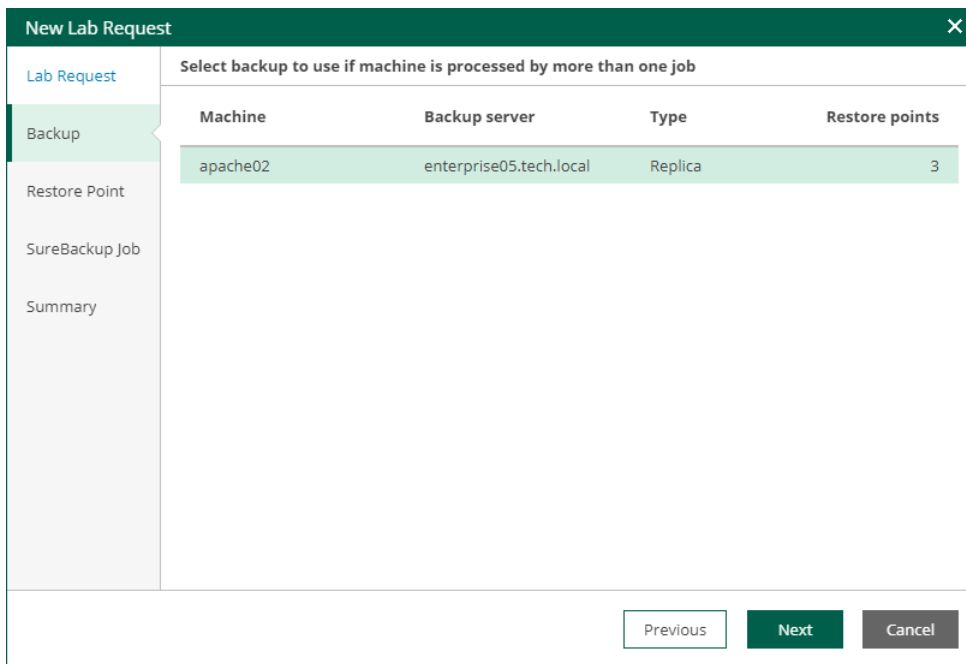
Required Duration: 30 min

Description:

[Cancel edits](#)

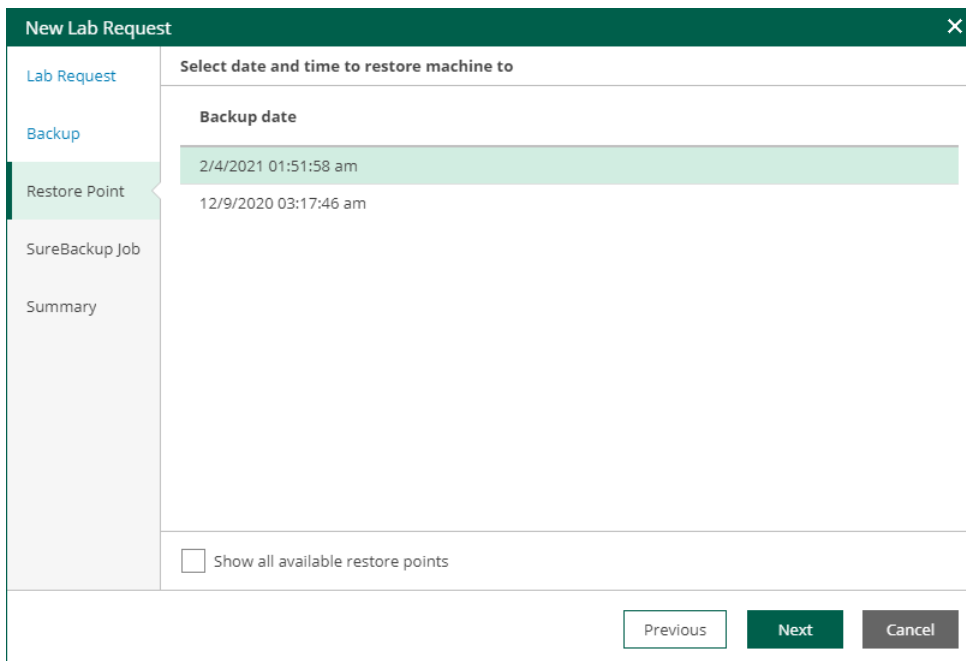
Next **Cancel**

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.



- 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.

The screenshot shows the 'New Lab Request' dialog box with the 'SureBackup Job' step selected. The main area displays a table of available jobs. Below the table, there is a 'Selected Job details' section showing 'Application group:' and 'Virtual Lab:'. At the bottom, there is a checkbox for 'Show all available SureBackup jobs' and three buttons: 'Previous', 'Next', and 'Cancel'.

Job name	Job state
SureBackup Job	Stopped

Selected Job details

Application group:
Virtual Lab:

Show all available SureBackup jobs

- 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.

The screenshot shows the 'New Lab Request' dialog box with the 'Summary' step selected. The main area displays a summary of the lab request settings. At the bottom, there are three buttons: 'Previous', 'Finish', and 'Cancel'.

Please review the lab request settings

Virtual machine: apache02
Point date: Thursday, February 4, 2021
SureBackup job: SureBackup Job 1
Verified status: Success

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 Cloud Director

Veeam Backup Enterprise Manager allows you to perform the following operations with VMware Cloud Director objects:

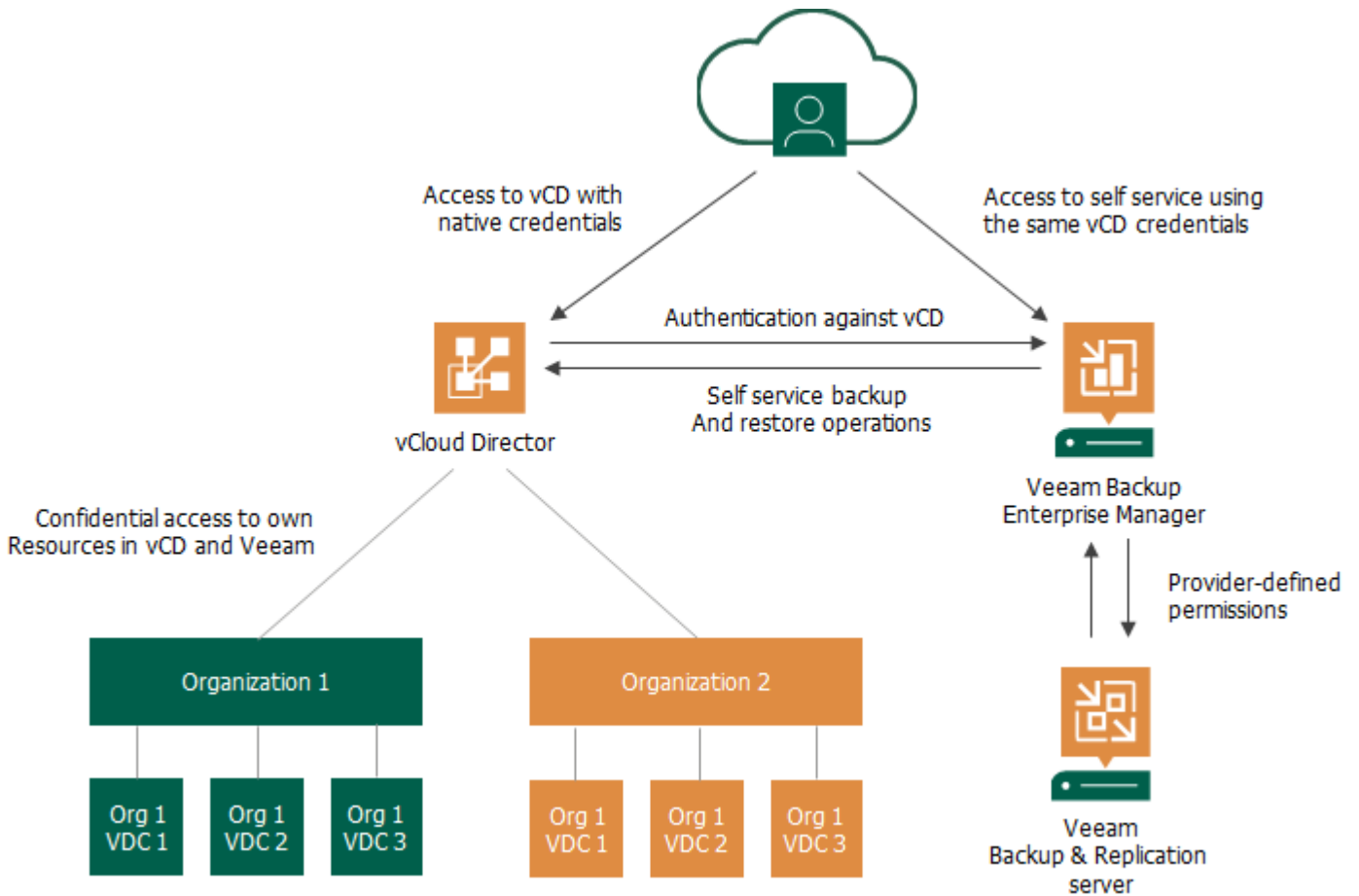
- Back up VMs, vApps and other containers
- Restore VMs and vApps
- Restore VM guest OS files
- Replicate vApps and other containers and fail over to their replicas

Cloud Director 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 Cloud Director organization configurations, including repository quota and backup job template. These administrators typically have access to Veeam Backup & Replication console that controls VMware Cloud Director as part of backup infrastructure on the provider side.
- Members of Cloud Director 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 Cloud Director jobs, as well as restore VMs, files and application items within their scope.

How It Works

Veeam Backup Enterprise Manager uses native VMware Cloud Director 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 VMware Cloud Director, 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 (Cloud Director 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 Cloud Director Organizations](#).

What Members of Cloud Director Organizations Can Do

Members of Cloud Director organizations can use their Cloud Director 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 Cloud Director objects when displaying them.

Members of Cloud Director 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 Cloud Director backups.
- Restore Cloud Director 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 Cloud Director Organizations

In Veeam Backup Enterprise Manager, users with the Portal Administrator role can manage configurations for VMware Cloud Director 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 Cloud Director organization configurations, [check prerequisites](#).

You can perform the following operations with Cloud Director organizations:

- [View the list of organization configurations](#)
- [Add a new configuration for a Cloud Director organization](#)
- [Edit a Cloud Director organization configuration](#)
- [Remove a Cloud Director organization configuration](#)
- [Export a configuration report](#)

Before You Begin

You can add configurations for VMware Cloud Director organizations created on multiple VMware Cloud Director servers that are added to the Veeam Backup Enterprise Manager infrastructure.

Before you manage Cloud Director organization configurations, check the following prerequisites:

1. The version of Cloud Director servers must be 10.1 or later.
For more information on system requirements, see [System Requirements](#).
2. All Cloud Director servers must be added to the backup infrastructure of backup servers.
For more information, see the [Adding VMware Cloud Director](#) section of the Veeam Backup & Replication User Guide.
3. Backup servers that contain the Cloud Director servers in their 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 [Adding 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 Cloud Director organization configurations must be assigned the Portal Administrator role.
For more information, see [Configuring Accounts and Roles](#).

Managing Multiple Cloud Director Servers

Starting from Veeam Backup Enterprise Manager 11a (build 11.0.1.1261), you can add Cloud Director organization configurations for multiple Cloud Director servers. In this case, organization members that work with Veeam Self-Service Backup Portal by the portal URL must specify the host of their Cloud Director server when accessing the portal. They can also open the portal from the native VMware Cloud Director environment. For more information, see [Accessing Veeam Self-Service Backup Portal](#).

Members of Cloud Director organizations can access Veeam Self-Service Backup Portal by the following portal URLs:

- Full URL that contains the host address where the necessary Cloud Director server resides:

```
https://<EnterpriseManagerServer>:9443/vcloud/<VCDServer>/<OrgName>
```

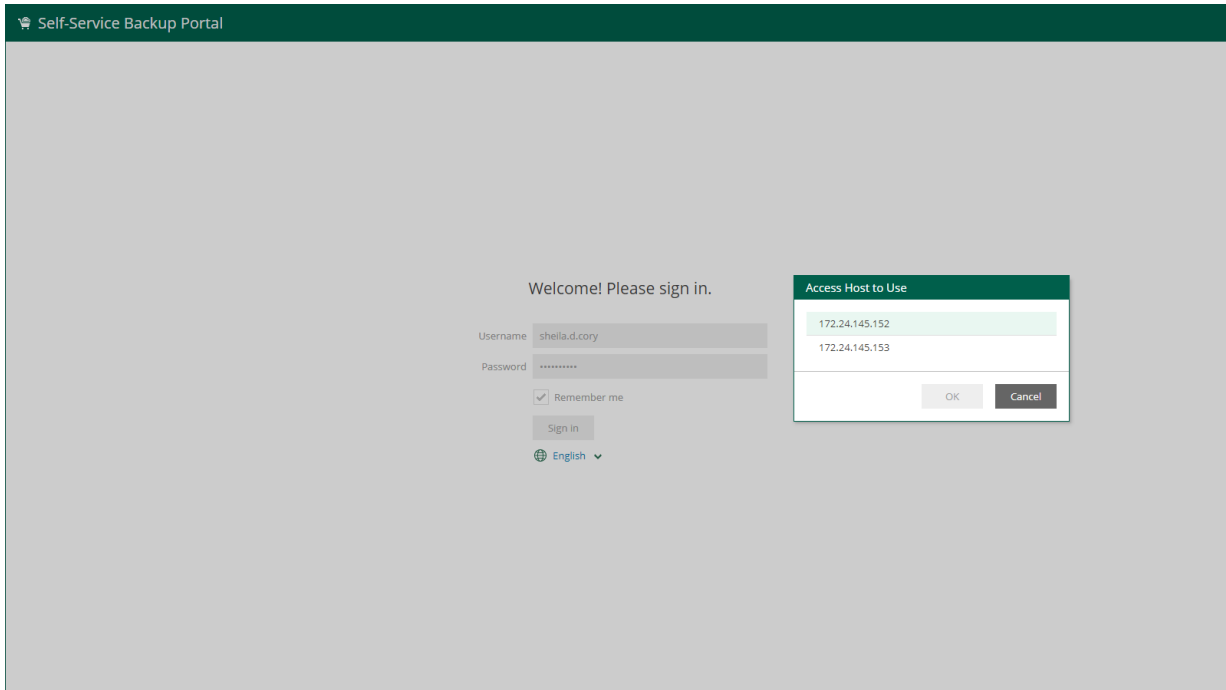
In this case, Veeam Self-Service Backup Portal will open right after clicking the **Sign in** button.

- Shorter URL that does not contain the host address where the necessary Cloud Director 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 Cloud Director host from the list of available Cloud Director hosts.

If you do not want Cloud Director organization members to see addresses of all Cloud Director hosts added to the Enterprise Manager infrastructure, add each Cloud Director 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 VMware Cloud Director 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 Cloud Director organizations. The configuration is applied to each 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](#).

The screenshot shows a configuration window titled "Edit" with a close button (X) in the top right corner. The window contains the following settings:

- Organization:** Other vCloud organizations (dropdown menu)
- Repository:** Disable self-service backup for other organizations (dropdown menu)
- Quota:** 1 (input field with up/down arrows) and TB (dropdown menu)
- Job scheduling:** Allow: Tenant has full access to all job scheduling options (dropdown menu)
- Job priority:** Normal (dropdown menu)

At the bottom of the window, there is a link "Show Advanced Job Settings" on the left, and "Save" and "Cancel" buttons on the right.

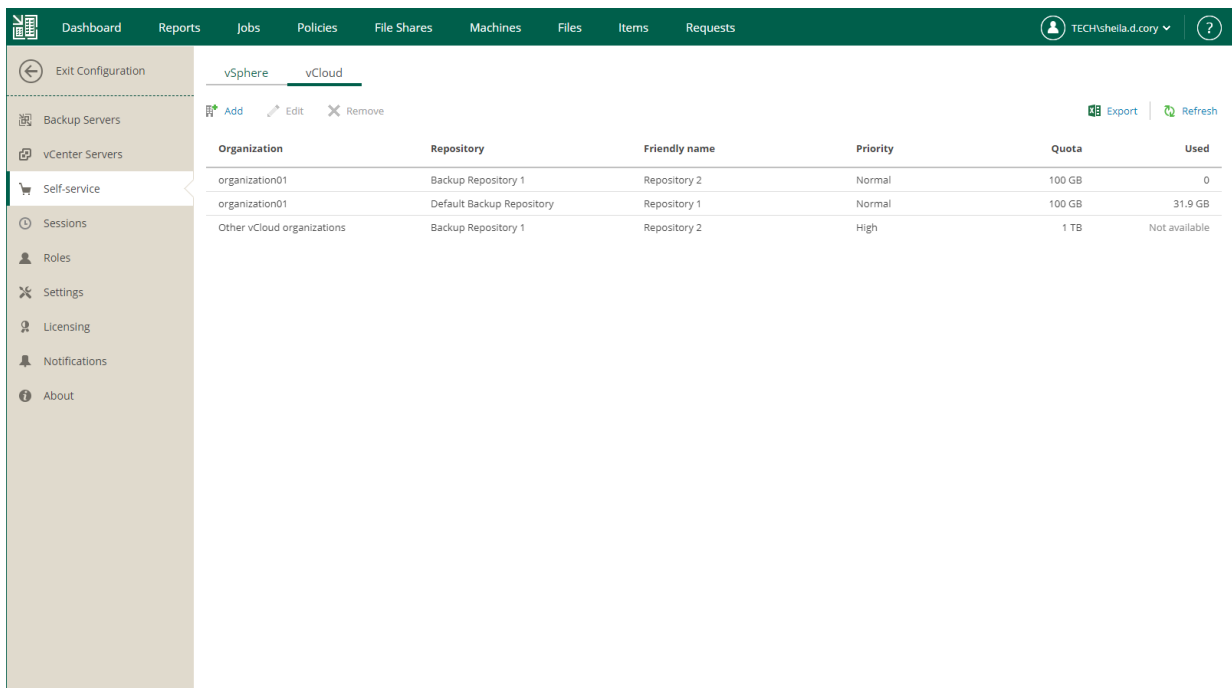
Adding Organization Configuration

Users with the Portal Administrator role can add a new configuration for a VMware Cloud Director 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 **VMware Cloud Director server** drop-down list, select a VMware Cloud Director server you need. The field is available if you have multiple Cloud Director 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 Cloud Director 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 backup servers that has a Cloud Director 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 Cloud Director 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 Cloud Director 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 Cloud Director backup job settings as they are shown in the Veeam backup console
 - *<Job Name>* – specific Cloud Director backup job configured in Veeam backup console

c. Click **Apply**.

Add [X]

vCloud Director server:
172.24.145.152

Organization:
organization01

Repository:
Default Backup Repository (enterprise04.tech.local)

Friendly name:
Repository 2

Quota:
100 GB

Job scheduling:
Allow: Tenant has full access to all job scheduling options

Job priority:
Normal

Advanced job settings:

Backup
Backup mode: Incremental
Create synthetic full backups periodically on: Saturday

Storage
Enable inline data deduplication: Yes
Exclude swap file blocks: Yes
Exclude deleted file blocks: Yes
Compression level: Optimal
Storage optimization: Local target

vSphere
Use changed block tracking data: Yes
Enable CBT for all protected VMs automatically: Yes
Reset CBT on each Active Full backup: Yes

Copy from:
vCD Backup Job 1

[Apply] [Save] [Cancel]

[Hide Advanced Job Settings](#)

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 Cloud Director 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 VMware Cloud Director organization configurations.

Before you edit a configuration, consider the following recommendations:

- When you change a job template for a Cloud Director 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 Cloud Director objects to the new repository.
 - b. Modify the backup job that is used as a template, and 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](#).

Edit

Organization: organization01

Repository: Default Backup Repository (enterprise04.tech.local)

Friendly name: Repository 1

Quota: 100 GB

Job scheduling: Allow: Tenant has full access to all job scheduling options

Job priority: Normal

Advanced job settings:

Backup

Backup mode: Incremental

Create synthetic full backups periodically on: Saturday

Storage

Enable inline data deduplication: Yes

Exclude swap file blocks: Yes

Exclude deleted file blocks: Yes

Compression level: Optimal

Storage optimization: Local target

vSphere

Use changed block tracking data: Yes

Copy from: Default job settings

Apply

Hide Advanced Job Settings

Save Cancel

Removing Organization Configuration

Users with the Portal Administrator role can remove VMware Cloud Director organization configurations. The removed configuration is still effective for the jobs created with this configuration. New Cloud Director 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.

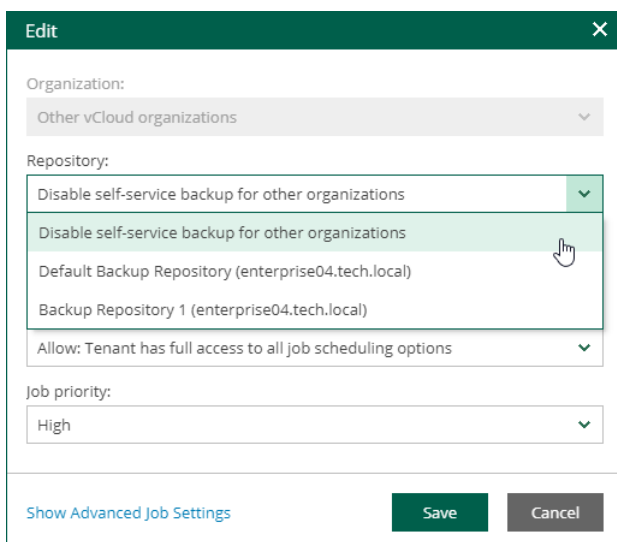
1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **vCloud** tab.
5. On the **vCloud** tab, select a configuration 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 VMware Cloud Director 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 VMware Cloud Director organizations with self-service operations for Cloud Director 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 Cloud Director credentials.

Permissions

Members of VMware Cloud Director organization can use Veeam Self-Service Backup Portal to backup and restore resources of their Cloud Director 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 Cloud Director UI using Veeam Plug-in for VMware Cloud Director. For more information, see [Accessing Veeam Self-Service Backup Portal](#).

The following organization members have access to Veeam Self-Service Backup Portal:

- Cloud Director organization administrators.
- Cloud Director organization members with the following rights granted in VMware Cloud Director:
 - *General: Administrator Control*
 - *General: Administrator View*
 - *Group / User: View*
- Any Cloud Director organization members whose roles (or associated LDAP user roles) are defined in registry keys and with the *Group / User: View* right granted in VMware Cloud Director. For more information, contact [Veeam Customer Support](#).

NOTE

Cloud Director system administrators cannot access Veeam Self-Service Backup Portal since they are not organization members.

Accessing Veeam Self-Service Backup Portal

Members of VMware Cloud Director organizations can access Veeam Self-Service Backup Portal in the following ways:

- [Access by URL](#)
- [Access from Cloud Director](#)

For more information on access rights, see [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/<OrgName>/<VCDServer>
```

where:

- <EnterpriseManagerServer> is a host name or IP address of the host where the Enterprise Manager server resides.
- <OrgName> is a name of the Cloud Director organization.
- <VCDServer> is a host name or IP address of the host where the Cloud Director server resides.

This URL part is optional. If you do not specify a Cloud Director host here, you may be asked to select the host when you log in to the portal.

For example:

```
https://enterprise01.tech.local:9443/vcloud/TechCompanyOrg/172.17.53.16
```

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 Cloud Director 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 Cloud Director servers, select the one where your organization has been created.

The list of hosts is displayed if multiple Cloud Director servers are added to the Enterprise Manager infrastructure.

Accessing Veeam Self-Service Backup Portal from VMware Cloud Director

In the VMware Cloud Director 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 VMware Cloud Director environment. For more information, see [Accessing Veeam Self-Service Backup Portal by URL](#).

Before members of Cloud Director organizations can access Veeam Self-Service Backup Portal from the Cloud Director UI, the Cloud Director system administrator must upload and configure Veeam Plug-in for VMware Cloud Director. For more information, see [Veeam Plug-in for VMware Cloud Director](#).

To access Veeam Self-Service Backup Portal from Cloud Director:

1. Log in to VMware Cloud Director Tenant Portal under a Cloud Director 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 Cloud Director, add the Veeam Backup Enterprise Manager certificate as trusted to your browser.

Veeam Plug-in for VMware Cloud Director

Veeam Plug-in for VMware Cloud Director lets members of VMware Cloud Director organizations access Veeam Self-Service Backup Portal from the native VMware Cloud Director environment.

You can upload and configure the plug-in in VMware Cloud Director Service Provider Admin Portal. When you upload the plug-in, you specify the scope – a set of Cloud Director organizations that can use the plug-in.

If you need to modify the scope of Cloud Director organizations after you configure the plug-in, update the plug-in configuration. For more information, see [Updating Plug-in Configuration](#).

IMPORTANT

In VMware Cloud Director Service Provider Admin Portal, you cannot upgrade plug-ins. To switch to a newer version of Veeam Plug-in for VMware Cloud Director, delete the current plug-in version and then upload a newer one. For more information on deleting the plug-in, see the [Delete a Plug-in](#) section of VMware Cloud Director documentation. For details on uploading the plug-in, see [Uploading and Configuring Plug-in](#).

Before you delete the plug-in, make a note of the Cloud Director organizations that are allowed to use the plug-in. For more information on how to view them, see the [Publish or Unpublish a Plug-in from an Organization](#) section of VMware Cloud Director documentation.

Before You Begin

Before you start uploading Veeam Plug-in for VMware Cloud Director, check the following prerequisites:

- Veeam Plug-in for VMware Cloud Director requires Veeam Backup & Replication 11 or later to be installed on the backup server that has the Cloud Director server in its infrastructure.
- Members of Cloud Director organizations using the plug-in must have network access to the Cloud Director server and Veeam Backup Enterprise Manager server.

You specify the Veeam Backup Enterprise Manager server URL in Cloud Director Service Provider Admin Portal when you configure the plug-in. For more information, see [Uploading and Configuring Plug-in](#).

- 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 TLS Certificates](#).

Uploading and Configuring Plug-in

To upload and configure Veeam Plug-in for VMware Cloud Director:

1. Log in to VMware Cloud Director Service Provider Admin Portal under a Cloud Director system administrator account.
2. Upload the `plugin.zip` file to the portal. You can find the file on the Veeam Backup & Replication installation disk in the `\Plugins\Cloud Director` folder.

For more information, see the [Upload a Plug-in](#) section of VMware Cloud 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 VMware Cloud 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 server, for example: `https://hostname:9443`.
5. Click **Save**.

NOTE

When you save the plug-in configuration, it is applied to all Cloud Director organizations. For that, a separate operation is performed for each organization. If you have operation limits that are set through the VMware Cloud Director API, the operations may fail with HTTP status 400.

In this case, use the VMware Cloud 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 Cloud Director API documentation.

6. 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

After you configure the plug-in, you can modify the scope of Cloud Director organizations. It may be useful, for example, if you create a new Cloud Director organization and you want members of this organization to use the plug-in. To include or exclude Cloud Director organizations, update the plug-in configuration.

To update the plug-in configuration:

1. Log in to VMware Cloud Director Service Provider Admin Portal under a Cloud Director system administrator account.
2. Modify the scope of Cloud Director organizations.

For more information, see the [Publish or Unpublish a Plug-in from an Organization](#) section of VMware Cloud 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 Cloud Director organizations.

Working with Veeam Self-Service Backup Portal

In Veeam Self-Service Backup Portal, members of VMware Cloud Director organizations can perform the following operations:

- On the [Dashboard tab](#) – view statistics on Cloud Director 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

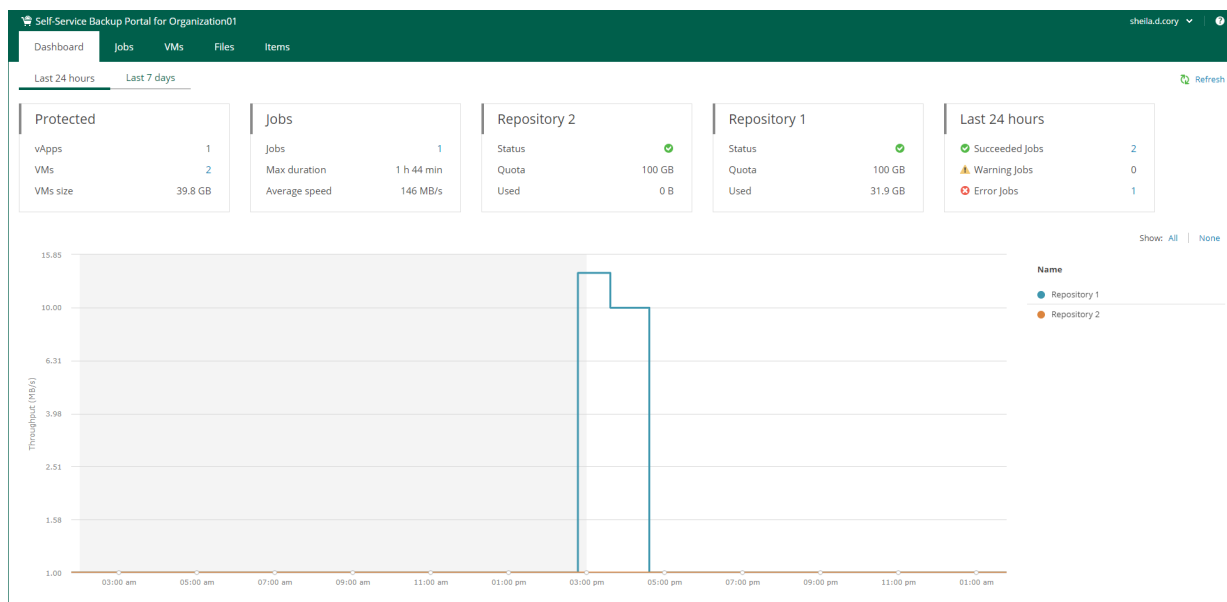
The **Dashboard** tab contains statistics on VMware Cloud Director backup jobs created by members of a Cloud Director organization, including information on the VMs, job runs and backup repositories.

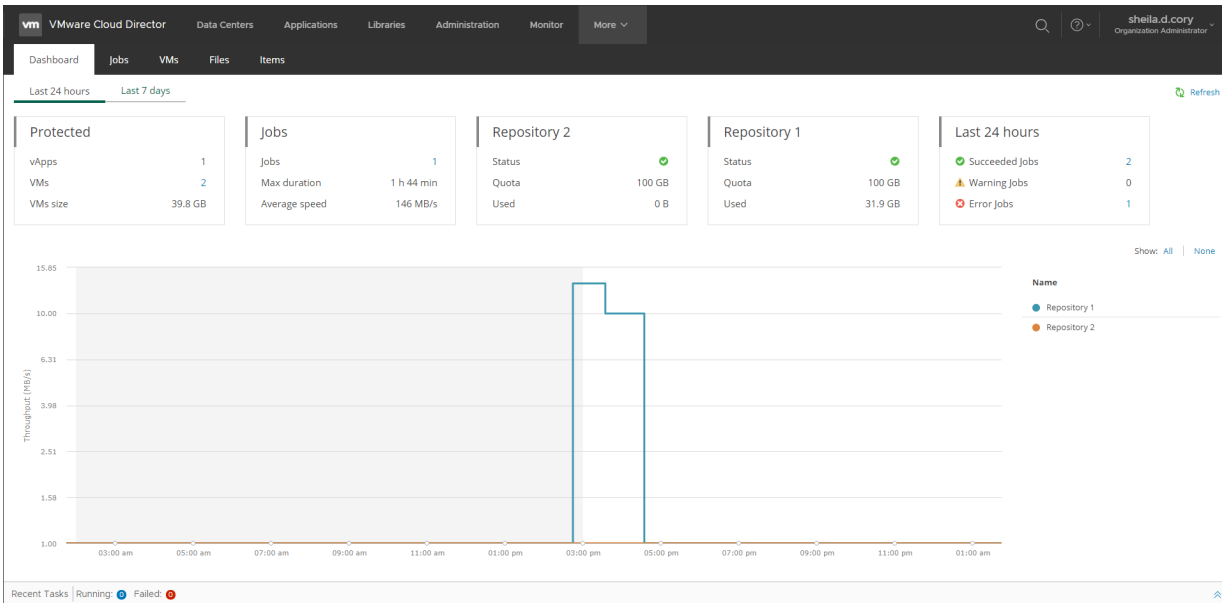
You can view the chart for one of the time ranges:

- 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





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 Cloud Director backup jobs of the current Cloud Director 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 Dashboard Chart](#).

Managing Cloud Director Jobs

On the **Jobs** tab, members of the VMware Cloud Director organization can perform the following operations with Cloud Director backup jobs:

- [Creating jobs](#)
- [Starting, stopping and retrying jobs](#)
- [Enabling and disabling jobs](#)
- [Editing job settings](#)
- [Deleting jobs](#)

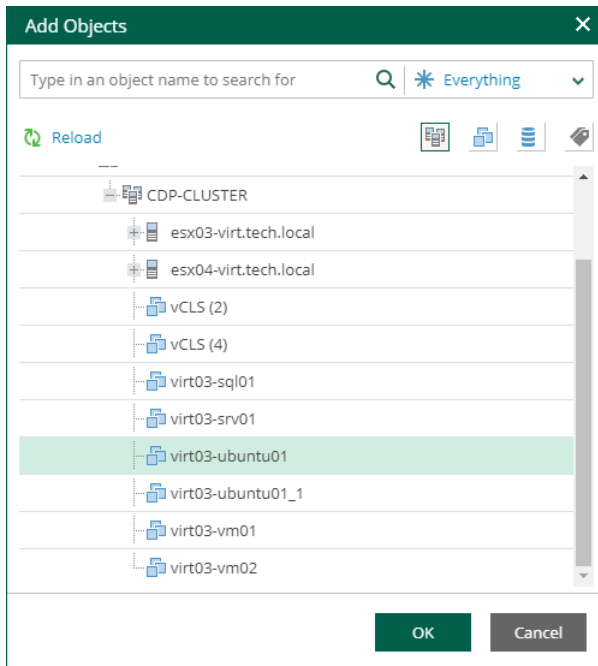
Before You Begin

Before you start working with jobs, consider the following:

- Organization members cannot see the jobs with VMs from their Cloud Director 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.
- 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 Cloud Director 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 Cloud Director 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.

Creating Jobs

With Veeam Self-Service Backup Portal, members of a VMware Cloud Director organization can create Cloud Director backup jobs. 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.

To create a Cloud Director backup job, use the **Create Backup Job** wizard:

1. [Launch the wizard.](#)
2. [Specify job name and retention settings.](#)
3. [Specify a list of VMs.](#)
4. [Configure VM processing order.](#)
5. [Configure guest OS processing settings.](#)
6. [Configure job schedule.](#)
7. [Configure email notifications.](#)

Step 1. Launch Wizard

To launch the **Create Backup Job** wizard, do the following:

1. Log in to the Veeam Self-Service Backup Portal under a Cloud Director account with proper rights.
For more information on user rights, see [Permissions](#).
2. On the **Jobs** tab, click **Create**.

Step 2. Specify Job Name and Retention Settings

At the **Job Settings** step of the wizard, specify a job name, repository, job description, retention policy and job priority.

1. In the **Job name** field, enter a name for the job.
2. From the **Repository** list, select a backup repository where the created backup files must be stored.
You can select a repository only if more than one configuration is added for the organization. For more information, see [Adding Organization Configuration](#).
3. 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.
4. 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](#).

5. 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.

The **Keep certain full backups longer for archival purposes** check box is available only if GFS retention policy can be applied to the job. For more information on GFS limitations, see the [Long-Term Retention Policy \(GFS\)](#) section of the Veeam Backup & Replication User Guide.

6. 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. For more information on job priorities, see the [Job Priorities](#) section of the Veeam Backup & Replication User Guide.

Create Backup Job ✕

- Job Settings
- Virtual Machines
- Guest Processing
- Job Schedule
- Email Notifications

Specify the job name, description and retention policy

Job name:

Repository:

Description:

Retention policy

Latest backups to keep:

Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Step 3. Specify List of VMs

At the **Virtual Machines** step of the wizard, you can add or remove VMs, vApps and VDCs of the organization. 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.

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.

3. Click **OK** to save the changes.

Removing VMs and VM containers

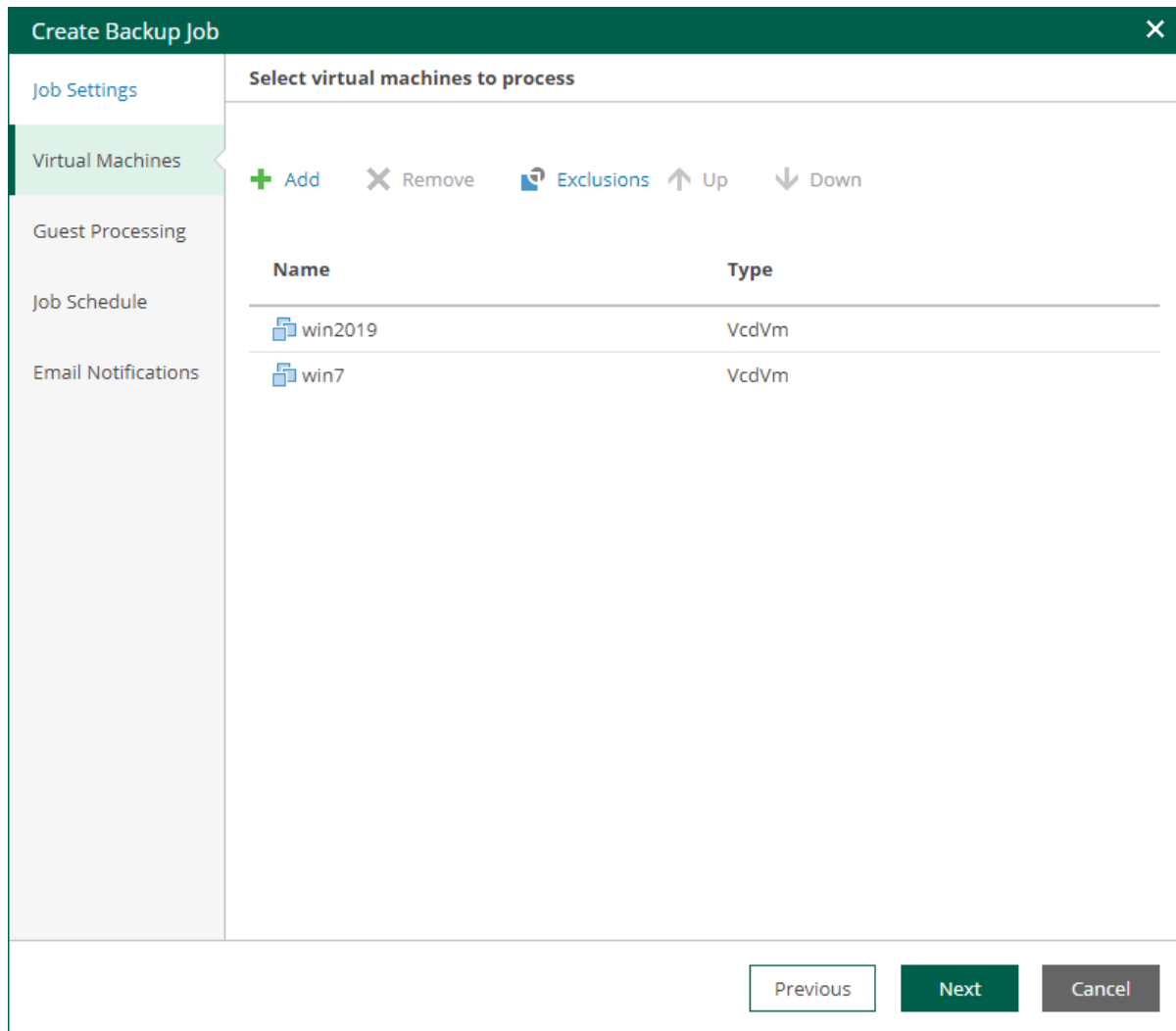
To remove a VM or VM container, select it in the list and click **Remove**.

Excluding VMs

You can also exclude individual VMs from VM containers.

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. Configure 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. You can change the order of the following VMware Cloud Director objects: VMs, vApps, organization VDCs, organizations and the Cloud Director instance. The scope depends on your Cloud Director access rights.

Create Backup Job [Close]

Job Settings

- Virtual Machines
- Guest Processing
- Job Schedule
- Email Notifications

Select virtual machines to process

+ Add ✕ Remove Exclusions ↑ Up ↓ Down

Name	Type
win2019	VcdVm
win7	VcdVm

Previous **Next** Cancel

Step 5. Configure Guest Processing Settings

At the **Guest Processing** step of the wizard, you can configure the following settings for VM guest OS processing:

- [Application-Aware Processing](#)
- [Guest OS File Indexing](#)
- [Guest OS Credentials](#)

NOTE

VMware Cloud Director system administrators can access guest OS credentials available for their organizations. They can also supply new credentials for guest OS processing.

The screenshot shows the 'Create Backup Job' wizard in the 'Guest Processing' step. The interface is divided into a left-hand navigation pane and a main content area. The navigation pane includes 'Job Settings', 'Virtual Machines', 'Guest Processing' (which is highlighted), 'Job Schedule', and 'Email Notifications'. The main content area is titled 'Choose guest OS processing options available for running VMs'. It contains three main sections: 1. 'Enable application-aware processing' (checked), with a 'Customize Application' link and a description: 'Customize application handling options for individual VMs and applications'. 2. 'Enable guest file system indexing' (checked), with a 'Customize Indexing' link and a description: 'Customize advanced guest file system indexing options for individual VMs'. 3. 'Guest OS credentials' section, which includes a 'Credentials:' dropdown menu currently showing 'william.fox (Guest OS credentials)', and buttons for '+ Add', 'Edit', and 'Delete'. Below this is a 'Customize Credentials' link with the description: 'Customize guest OS credentials for individual VMs and operating systems'. At the bottom of the wizard, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Application-Aware Processing

At the **Guest Processing** step of the wizard, you can enable application-aware processing. Application-aware processing is a Veeam technology based on Microsoft VSS and used to create transactionally consistent backups or replicas of VMs that run Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, Oracle or PostgreSQL. For more information, see the [Application-Aware Processing](#) section of the Veeam Backup & Replication User Guide.

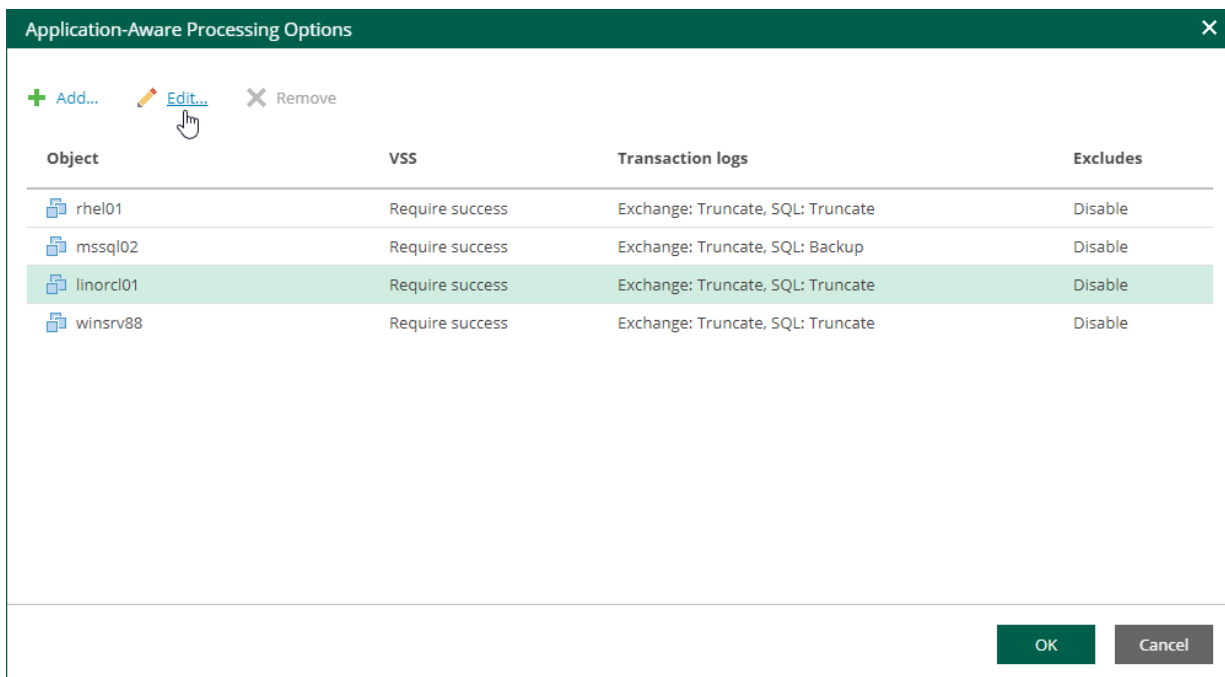
To configure application-aware processing, take the following steps:

1. Select the **Enable application-aware processing** check box.
2. Click the **Customize Application** link.
3. To define custom settings for a machine, select it and click **Edit**.

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](#)
 - [Microsoft SQL Server Transaction Log Settings](#)
 - [Oracle Archived Log Settings](#)
 - [PostgreSQL Archived Log Settings](#)
 - [VM Guest OS File Exclusion](#)



General Settings

On the **General** tab, you can specify general application-aware processing settings.

1. In the **Applications** section, select the option that corresponds to your transactionally-consistent backup creation scenario.
 - 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.

2. [For Microsoft Exchange, Microsoft SQL Server, Oracle and PostgreSQL] In the **Transaction Logs Processing** 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 process transaction logs.

[For Microsoft Exchange] With this option selected, the non-persistent runtime components or persistent components running on the VM guest OS will wait for backup to complete successfully and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

[For Microsoft SQL Server, Oracle and PostgreSQL] Specify settings for transaction log handling:

- For Microsoft SQL Server transaction log processing – on the **SQL** tab. For more information, see [Microsoft SQL Server Transaction Log Settings](#).
- For Oracle database archived logs processing – on the **Oracle** tab. For more information, see [Oracle Archived Log Settings](#).
- For PostgreSQL database archive logs processing – on the **PostgreSQL** tab. For more information, see [PostgreSQL Archive Log Settings](#).
- 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.

With this option selected, the **SQL**, **Oracle** and **PostgreSQL** tabs are not available.

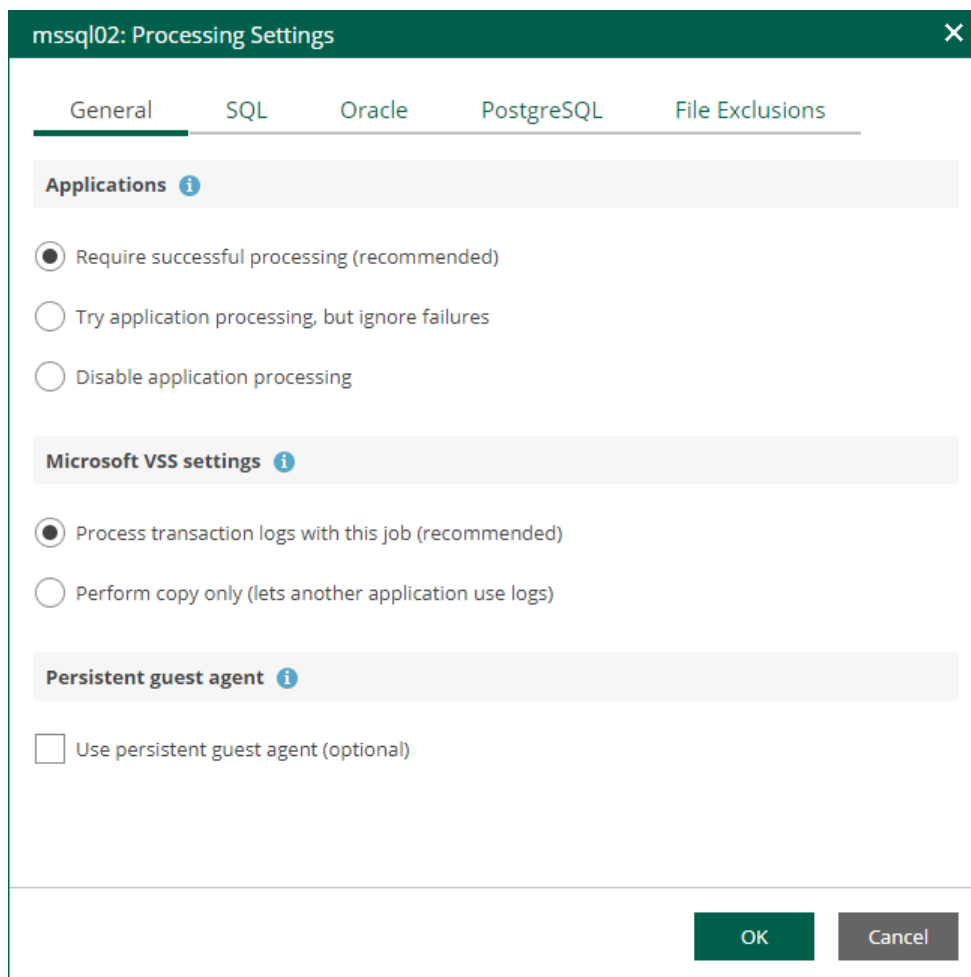
3. In the **Persistent guest agent** section, specify if Veeam Backup & Replication must use persistent guest agents on each protected VM for application-aware processing.

By default, Veeam Backup & Replication uses non-persistent runtime components. Veeam Backup & Replication deploys runtime components on each protected VM when the backup job starts, and removes the runtime components as soon as the backup job finishes.

Select the **Use persistent guest agent check** box to enable persistent agent components for guest processing. For more information, see the [Non-Persistent Runtime Components and Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.

IMPORTANT

If both Microsoft SQL Server and Oracle Server are installed on the same VM, and this VM 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.

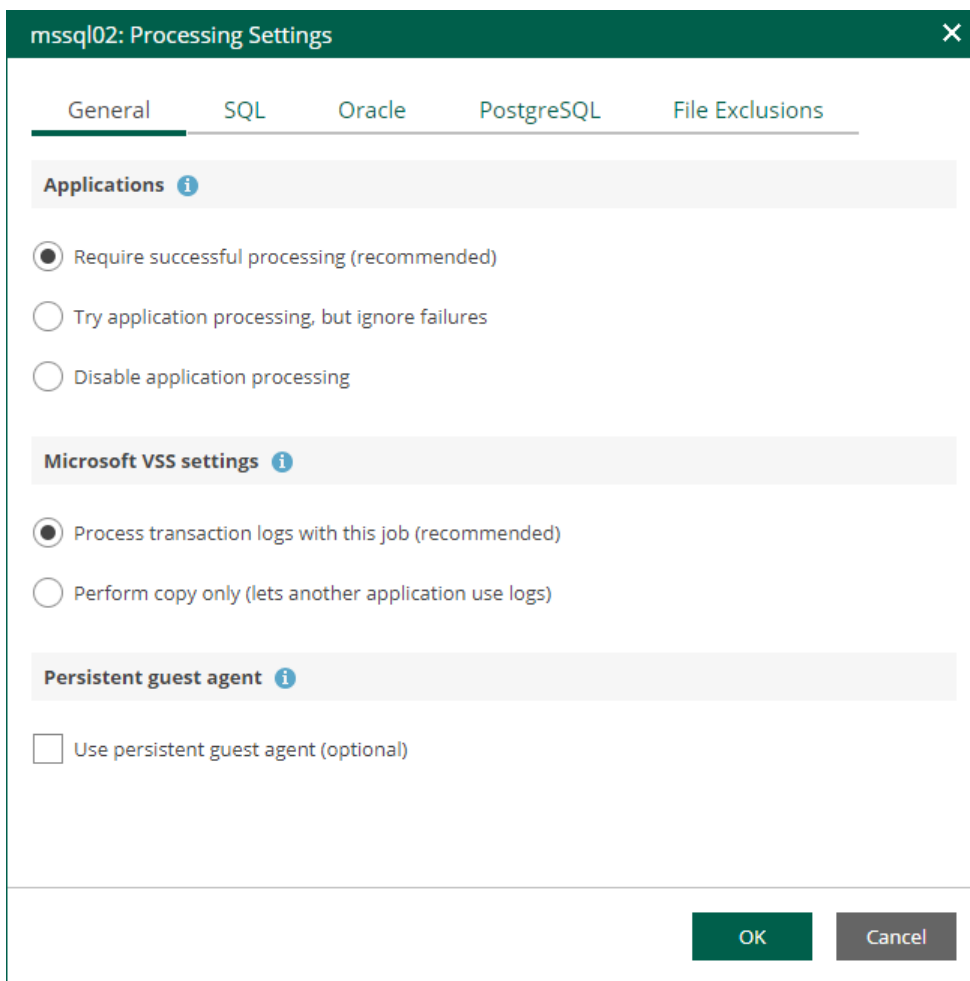


Microsoft SQL Server Transaction Log Settings

If you back up a Microsoft SQL VM, you can specify how Veeam Backup & Replication must process transaction logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Microsoft SQL Server VM from the list and click **Edit**.
4. On the **General** tab of the **VM Processing Settings** window, make sure the following options are selected:
 - o In the **Applications** section, either the **Require successful processing** or **Try application processing, but ignore failures** option must be selected.

- In the **Microsoft VSS settings** section, the **Process transaction logs with this job** option must be selected.



5. Open the **SQL** tab of the **VM Processing Settings** window.
6. Specify how Veeam Backup & Replication will process SQL transaction logs.
 - Select **Truncate logs** to truncate transaction logs after successful backup. The non-persistent runtime components or persistent components running on the VM guest OS will wait for the backup to complete successfully and then truncate transaction logs. If the job does not manage to back up the Microsoft SQL Server VM, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

NOTE

If the account specified at the [Guest Processing](#) step does not have enough rights, Veeam Backup & Replication tries to truncate logs using the *NT AUTHORITY\SYSTEM* account. Make sure that the account has permissions listed in the [Permissions](#) section of the Veeam Explorers User Guide.

- Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Backup & Replication will not truncate transaction logs on the Microsoft SQL Server VM.
Select 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 on the VM guest OS may grow large and consume all disk space. In this case, the database administrators must take care of transaction logs themselves.

- Select **Backup logs periodically** to back up transaction logs with Veeam Backup & Replication. Veeam Backup & Replication will periodically copy transaction logs to the backup repository and store them together with the image-level backup of the Microsoft SQL Server VM. During the backup job session, transaction logs on the VM guest OS will be truncated.

For more information, see the [Microsoft SQL Server Transaction Log Settings](#) sections of the Veeam Backup & Replication User Guide.

7. If you have selected the **Backup logs periodically** option, specify settings for transaction log backup:
 - a. In the **Backup logs every <N> minutes** field, specify the frequency for transaction log backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
 - b. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup repository.
 - 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** 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 backups. For more information, see [Retention for Transaction Log Backups](#) section of the Veeam Backup & Replication User Guide.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport transaction logs. For more information, see the [Microsoft SQL Server Transaction Log Settings](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows a dialog box titled "dbserver01: Processing Settings" with a close button (X) in the top right corner. It has four tabs: "General", "SQL", "Oracle", and "File Exclusions", with "SQL" currently selected. Below the tabs is a section titled "Choose how this job should process Microsoft SQL Server transaction logs". There are three radio button options: "Truncate logs (prevents logs from growing forever)", "Do not truncate logs (requires simple recovery model)", and "Backup logs periodically (backed up logs are truncated)". The "Backup logs periodically" option is selected. Below this, there is a field "Backup logs every" with a spinner box containing the number "15" and the unit "minutes". Underneath, there is a section titled "Retain log backups:" with two radio button options: "Until the corresponding image-level backup is deleted" (which is selected) and "Keep only last" with a spinner box containing "15" and the unit "days". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

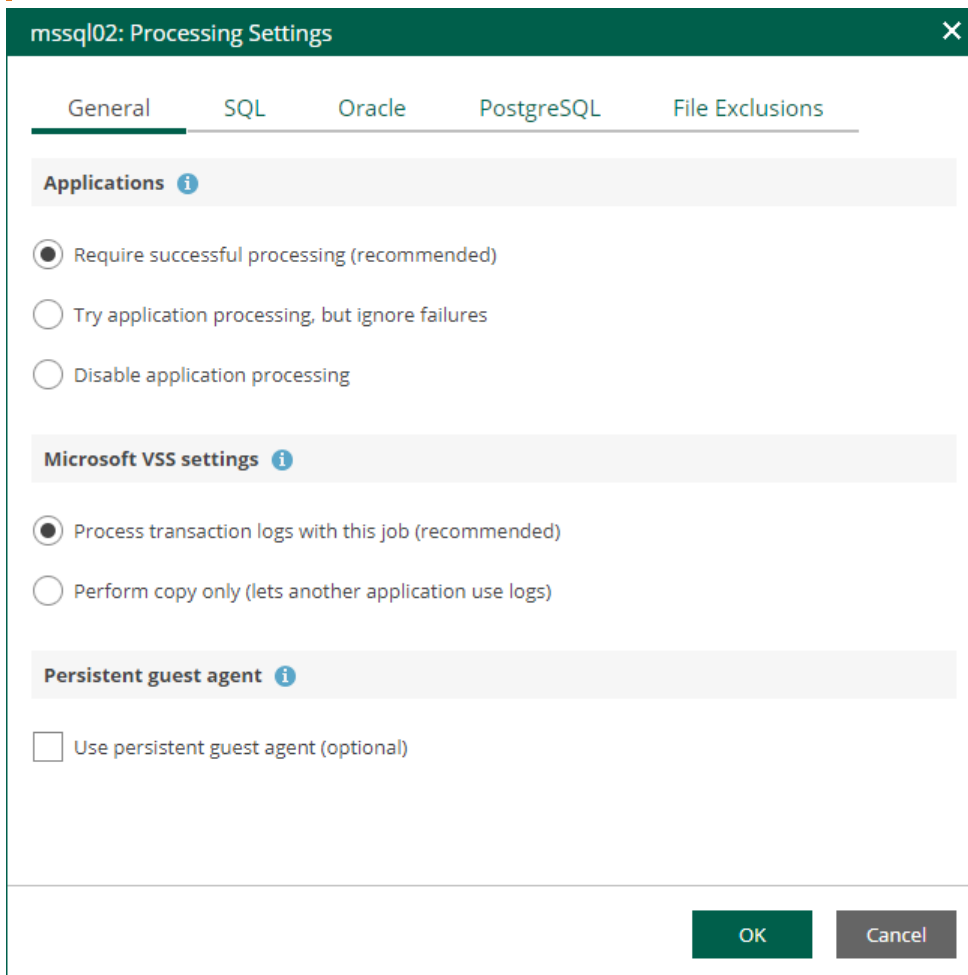
Oracle Archived Log Settings

If you back up a VM where Oracle Database is deployed, you can specify how Veeam Backup & Replication must process archived redo logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the Oracle VM from the list and click **Edit**.
4. On the **General** tab of the **VM Processing Settings** window, make sure that either the **Require successful processing** or **Try application processing, but ignore failures** option is selected.

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.



5. On the **Oracle** tab of the **VM Processing Settings** window, specify log processing settings.
 - a. Specify a user account that will connect to the Oracle database and perform Oracle archived logs backup and deletion.
 - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.

- Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

Make sure the specified account has sufficient rights. For details, see the [Permissions](#) section of the Veeam Explorers User Guide.

b. Specify how Veeam Backup & Replication must process archived redo logs on the Oracle VM.

- Select **Do not delete archived logs** to preserve archived redo logs on the original Oracle server.

Select this option for databases in the NOARCHIVELOG mode. If the database is in the ARCHIVELOG mode, archived logs on the VM guest OS may grow large and consume all disk space. In this case, database administrators must take care of archived logs themselves.

- Select **Delete logs older than <N> hours / Delete logs over <N> GB** to delete archived logs that are older than <N> hours or larger than <N> GB. The log size threshold refers not to the total size of all logs for all databases, but to the log size of each database on the selected Oracle VM.

When the parent backup job (job creating an image-level backup) runs, Veeam Backup & Replication will wait for the backup to complete successfully, and then trigger archived logs deletion on the Oracle VM over Oracle Call Interface (OCI). If the primary job does not manage to back up the Oracle VM, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

TIP

Veeam Backup & Replication removes redo logs only after the parent backup job session. To remove redo logs more often, you can schedule the job to run more often.

c. To back up Oracle archived logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archived log backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

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. Thus, you need to set up backup schedule and log removal conditions appropriately.

d. If you have selected the **Backup logs every <N> minutes** option, specify retention policy for the archived logs stored in the backup repository. For the **Retain log backups** setting, select one of the following:

- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level 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 image-level backups. For more information, see the [Retention for Archived Log Backups](#) section of the Veeam Backup & Replication User Guide.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport archived logs. For more information, see the [Oracle Archived Log Settings](#) section of the Veeam Backup & Replication User Guide.

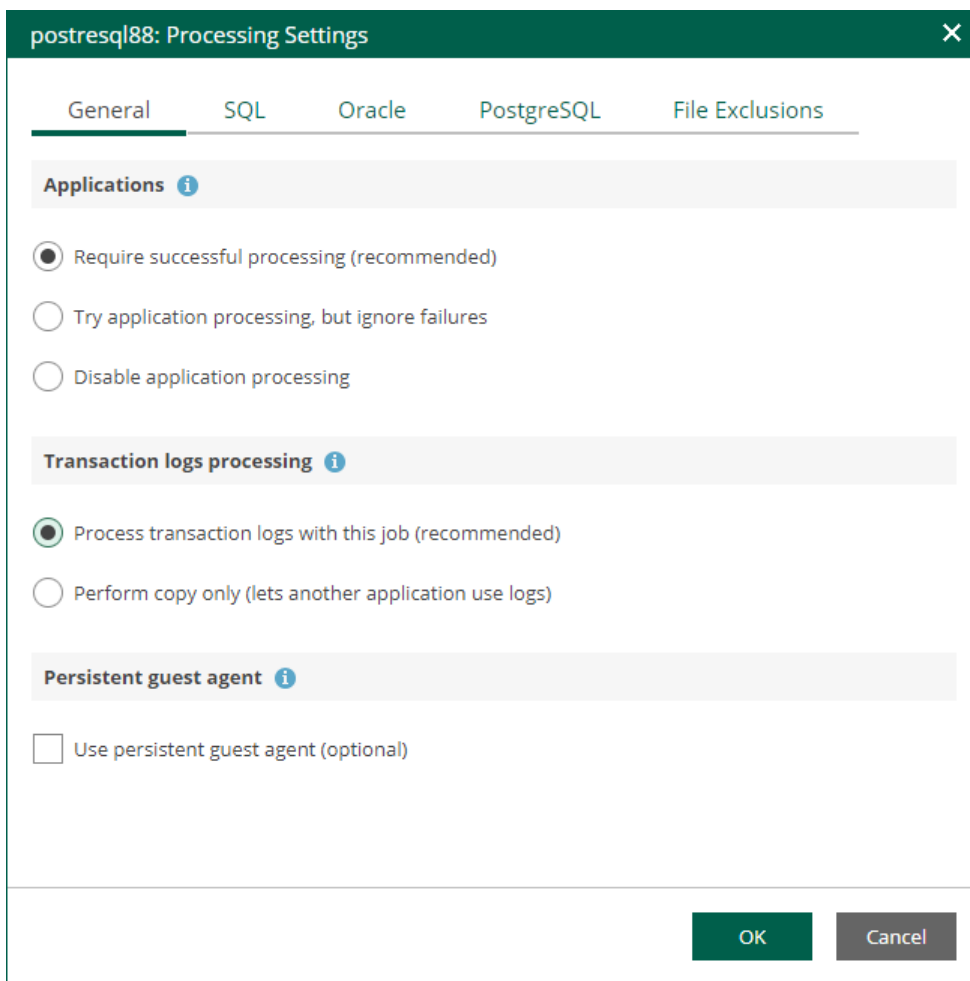
The screenshot shows a dialog box titled "linorcl01: Processing Settings" with a close button (X) in the top right corner. The dialog has five tabs: "General", "SQL", "Oracle" (which is selected and highlighted), "PostgreSQL", and "File Exclusions". Below the tabs, there is a section titled "Choose how this job should process Oracle archived logs". Under this section, there is a label "Specify Oracle account with SYSDBA privileges:" followed by a dropdown menu containing "admin (admin)" and a "+ Add" button. Below the dropdown, there are four radio button options: "Do not delete archived logs", "Delete logs older than:" (selected), "Delete logs over:", and "Backup logs every:". The "Delete logs older than:" option has a numeric input field set to "48" and the unit "hours". The "Delete logs over:" option has a numeric input field set to "10" and the unit "GB". The "Backup logs every:" option has a numeric input field set to "15" and the unit "minutes". Below these options is a section titled "Retain log backups:" with two radio button options: "Until the corresponding image-level backup is deleted" (selected) and "Keep only last" (with a numeric input field set to "15" and the unit "days"). At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

PostgreSQL Archive Log Settings

If you back up a VM where PostgreSQL is deployed, you can specify how Veeam Backup & Replication must process PostgreSQL archive logs on this VM.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select the PostgreSQL VM from the list and click **Edit**.

4. On the **General** tab of the **VM Processing Settings** window, make sure that either the **Require successful processing** or **Try application processing, but ignore failures** option is selected.



5. On the **PostgreSQL** tab of the **VM Processing Settings** window, specify settings for PostgreSQL logs processing.
 - a. Specify an account that will connect to the PostgreSQL instance and perform PostgreSQL archive logs backup and deletion. The `pg_hba.conf` configuration file of the PostgreSQL instance must contain a record with the account.
 - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the PostgreSQL instance.
 - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

Make sure the specified account has sufficient rights. For details, see the [Permissions](#) section of the Veeam Explorers User Guide.
 - b. Specify an authentication method for the selected user account.
 - Select **Database user with password** if you have specified an account with password-based authentication. In this case, you must provide Veeam Backup & Replication with the account password that will be stored in the Veeam Backup & Replication database.
 - Select **Database user with password file (.pgpass)** if you have specified an account with password-based authentication. In this case, you do not have to specify the account password when adding the account in Veeam Backup & Replication. Instead, the account password must be specified in the PGPASS password file stored in the user's home directory.

- Select **System user without password (peer)** if you have specified a local system account with peer authentication.
- c. To back up PostgreSQL archive logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archive log backup. By default, archive logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
- d. If you have selected the **Backup logs every <N> minutes** option, specify retention policy for the archive logs stored in the backup repository. For the **Retain log backups** setting, select one of the following:
- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
 - Select **Keep only last <N> days** to keep archive logs for a specific number of days. By default, archive logs are kept for 15 days. If you select this option, you must make sure that retention for archive logs is not greater than retention for the image-level backups. For more information, see the [Retention for PostgreSQL WAL Files](#) section of the Veeam Backup & Replication User Guide.
- e. In the **PostgreSQL archive logs local temporary storage** field, specify a path on the PostgreSQL machine that Veeam Backup & Replication will use to temporarily store PostgreSQL archive logs until they are backed up. Veeam Backup & Replication does not create the temporary storage folder so the folder must exist on the machine. Make sure the temporary location has enough free space for storing the log files.

NOTE

Using the Veeam Backup & Replication console, you can also specify log shipping servers that you want to use to transport archive logs. For more information, see the [Retention for PostgreSQL WAL Files](#) section of the Veeam Backup & Replication User Guide.

The screenshot shows a dialog box titled "rhel02: Processing Settings" with a close button (X) in the top right corner. The dialog has five tabs: "General", "SQL", "Oracle", "PostgreSQL", and "File Exclusions". The "PostgreSQL" tab is selected. Below the tabs, there is a section titled "Choose how this job should process PostgreSQL transaction logs". Under this section, there is a label "Specify PostgreSQL account with superuser privileges:" followed by a dropdown menu showing "Use guest credentials" and a "+ Add" button. Below this, there is a label "The specified user is:" followed by three radio button options: "Database user with password" (selected), "Database user with password file (.pgpass)", and "System user without password (peer)". There is also a checked checkbox "Backup logs every" followed by a spinner box set to "15" and the word "minutes". Below this, there is a label "Retain log backups:" followed by two radio button options: "Until the corresponding image-level backup is deleted" (selected) and "Keep only last" followed by a spinner box set to "15" and the word "days". At the bottom, there is a label "PostgreSQL archive logs local temporary storage:" followed by a text input field containing "/tmp". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

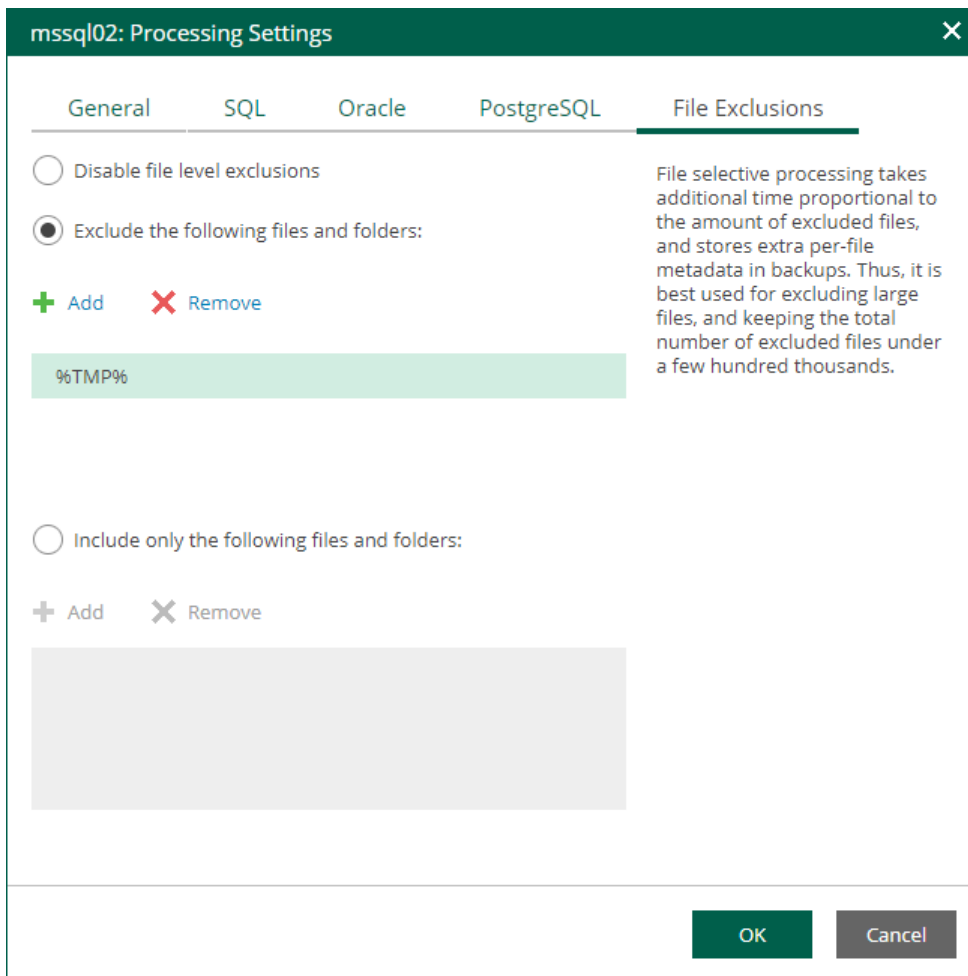
VM Guest OS File Exclusion

If you do not want to back up specific files and folders on the VM guest OS, you can exclude them from the backup. Exclusions can help decrease the backup file size. However, selective processing takes additional time that depends on the number of excluded files. It also 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.

1. At the **Guest Processing** step of the wizard, make sure the **Enable application-aware processing** check box is selected.
2. Click the **Customize Application** link.
3. In the displayed window, select a VM from the list and click **Edit**.
4. On the **File Exclusions** tab, specify the files that must be excluded from the backup.
 - Select **Exclude the following files and folders** to remove individual files and folders from the backup.
 - Select **Include only the following files and folders** to leave only the specified files and folders in the backup.

5. 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.

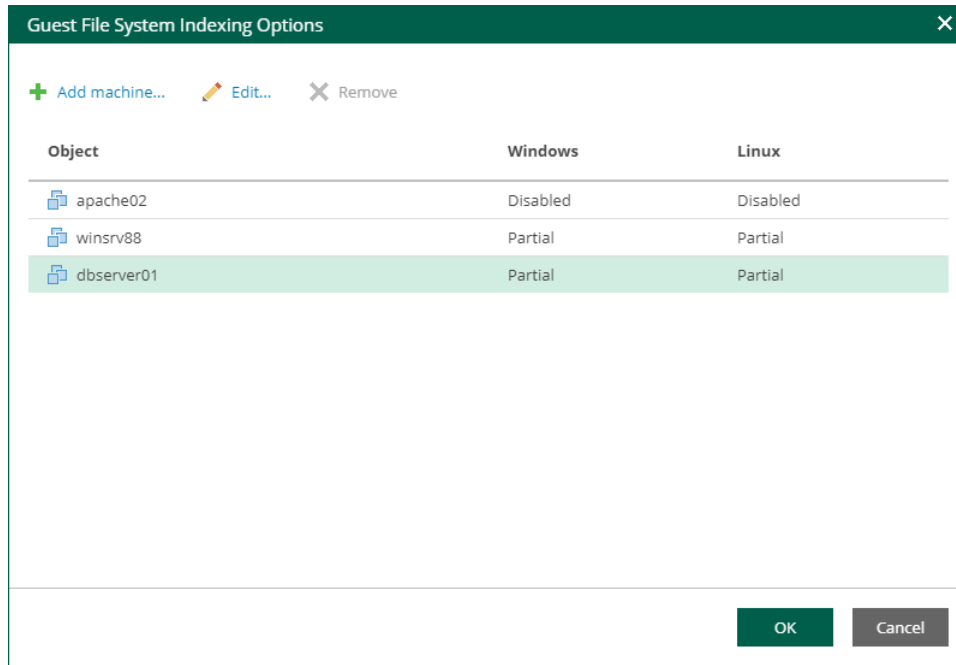
To provide granular indexing options for individual machines:

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:

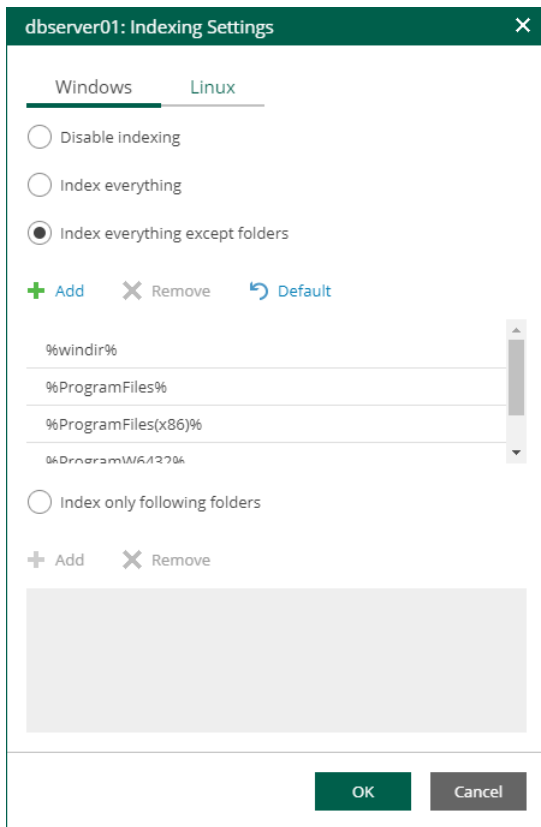
- To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add Machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
- To discard custom settings of a machine, 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

If you specify guest OS credentials, Veeam Backup & Replication deploys a runtime process on the VM guest OS to coordinate guest processing activities. The process runs only during guest processing and is stopped immediately after the processing is finished.

If you have Management Agent installed on a Linux VM, you have an option to use it for coordinating guest processing activities. In this case, guest OS credentials are not stored in the configuration database, which makes using Management Agent a more secure option. For more information, see the [Persistent Agent Components](#) section of the Veeam Backup & Replication User Guide.

NOTE

VMware Cloud Director system administrators can access guest OS credentials available for their organizations. They can also supply new credentials for guest OS processing.

Create Backup Job

Job Settings

Virtual Machines

Guest Processing

Job Schedule

Email Notifications

Choose guest OS processing options available for running VMs

Enable application-aware processing **i**

Customize Application

Customize application handling options for individual VMs and applications

Enable guest file system indexing **i**

Customize Indexing

Customize advanced guest file system indexing options for individual VMs

Guest OS credentials

Credentials:

william.fox (Guest OS credentials) **+** Add **E**dit **X** Delete

Customize Credentials

Customize guest OS credentials for individual VMs and operating systems

Previous **Next** Cancel

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, you can choose one of the following options:
 - If Management Agent is installed on the VM, you can select the **Use management agent** option.
 - If Management Agent is not installed on the VM, 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.

- i. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
- ii. 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.
- iii. 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

Linux Credentials

Username: Administrator

Password:

Private key is required for this connection

Private Key: key01.ppk [Browse...](#)

Passphrase:

SSH port: 22

Non-root account

Elevate specified account to root

Add account to the sudoers file automatically

Use "su" if "sudo" fails

Root password:

Description: Linux account for srv12

OK Cancel

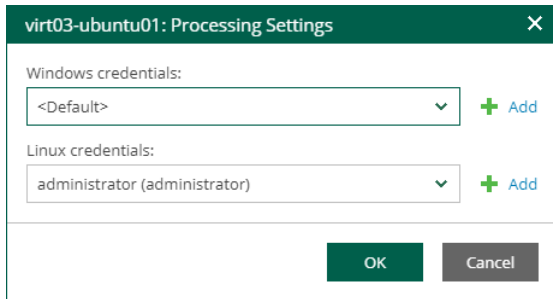
Special Credentials for Machine

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**.



The screenshot shows a dialog box titled "virt03-ubuntu01: Processing Settings". It has a close button (X) in the top right corner. Under "Windows credentials:", there is a dropdown menu showing "<Default>" and a "+ Add" button. Under "Linux credentials:", there is a dropdown menu showing "administrator (administrator)" and a "+ Add" button. At the bottom, there are two buttons: "OK" and "Cancel".

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. Configure 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 [Schedule 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.

The screenshot shows the 'Create Backup Job' wizard in the 'Job Schedule' step. The left sidebar contains 'Job Settings', 'Virtual Machines', 'Guest Processing', 'Job Schedule' (highlighted), and 'Email Notifications'. The main area is titled 'Specify the job scheduling options' and includes the following sections:

- Run the job automatically:** Run the job automatically:
- Daily at this time:** Daily at this time: 10:00 pm, On these days: On these days, Days...
- Monthly at:** Monthly at: 10:00 pm, Fourth, Saturday, Months...
- Periodically every:** Periodically every: 1, Hours, Schedule...
- After this job:** After this job: [dropdown]

Automatic retry

- Retry failed VM processing: 2 times
- Wait before each attempt for: 10 minutes

Backup window

- Terminate job if it gets out of allowed backup window Window...

At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

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.

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.

The screenshot shows a 'Select Period' dialog box with a 7-day grid. The grid has columns for hours 1-12 for AM and 1-12 for PM. The 'Permitted' time window is highlighted in green, spanning from 9:00 AM to 5:00 PM on all days. The 'Denied' time window is highlighted in grey. Below the grid, there are radio buttons for 'Denied' and 'Permitted', with 'Permitted' selected. There are also 'Deny All' and 'Permit All' buttons. At the bottom, there is a 'Start time within an hour' field set to 0 minutes, and 'OK' and 'Cancel' buttons.

- 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.

Step 7. Configure Email Notifications

At the **Email Notifications** step, you can configure email notifications.

Email notifications will be sent if you configure global email notification settings in Veeam Backup Enterprise Manager. For more information, see [Notifications on Job Results](#).

1. Select the **Enable e-mail notifications** check box if you want to receive notifications about the job completion status by email.
2. In the **Recipients** field, specify recipient's email address. You can enter several addresses separated by a semicolon.
3. 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 VMs in the job) and *%Issues%* (number of VMs in the job that have finished with the Warning or Failed status).
4. Select **Notify on success** to receive an email notification when the job completes successfully.
5. Select **Notify on warning** to receive an email notification when the job completes with a warning.
6. Select **Notify on error** to receive an email notification when the job fails.
7. 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.
8. To create the job, click **Finish**.

Other job settings are obtained from the job configuration specified for the organization. For more information, see [Adding Organization Configuration](#).

The screenshot shows the 'Create Backup Job' dialog box with the 'Email Notifications' tab selected. The dialog has a dark green header with the title 'Create Backup Job' and a close button. On the left, there is a sidebar with navigation options: 'Job Settings', 'Virtual Machines', 'Guest Processing', 'Job Schedule', and 'Email Notifications' (which is highlighted). The main area is titled 'Specify recipients and settings for the job status emails:'. It contains the following elements:

- Enable e-mail notifications
- Recipients:
- Subject:
- Notify on success
- Notify on warning
- Notify on error
- Suppress notifications until the last retry

At the bottom right, there are three buttons: 'Previous' (disabled), 'Finish' (active), and 'Cancel' (disabled).

Deleting Jobs

Members of a VMware Cloud Director organization can delete Cloud Director backup jobs created by members of the organization. After deletion, this job will be removed and no longer appear in Veeam Self-Service Backup Portal, Veeam Backup & Replication console and in Veeam Backup Enterprise Manager.

To delete a job:

1. On the **Jobs** tab, select a job from the list.
2. On the toolbar, click **Job > Delete**.

Managing Cloud Director VMs and vApps

On the **VMs** tab, members of a VMware Cloud Director organization can perform the following tasks:

- Browse VMs and vApps
- [Restore VMs](#)
- [Restore vApps](#)
- [Restore VM disks](#)
- [Delete VMs and vApps from Backups](#)

Recovering VMs

You can recover VMs from backups to the original (production) vApp or another vApp within your organization.

You can perform the following types of VM recovery:

- [Instant Recovery](#)
- [Entire VM Restore](#)

Instant Recovery

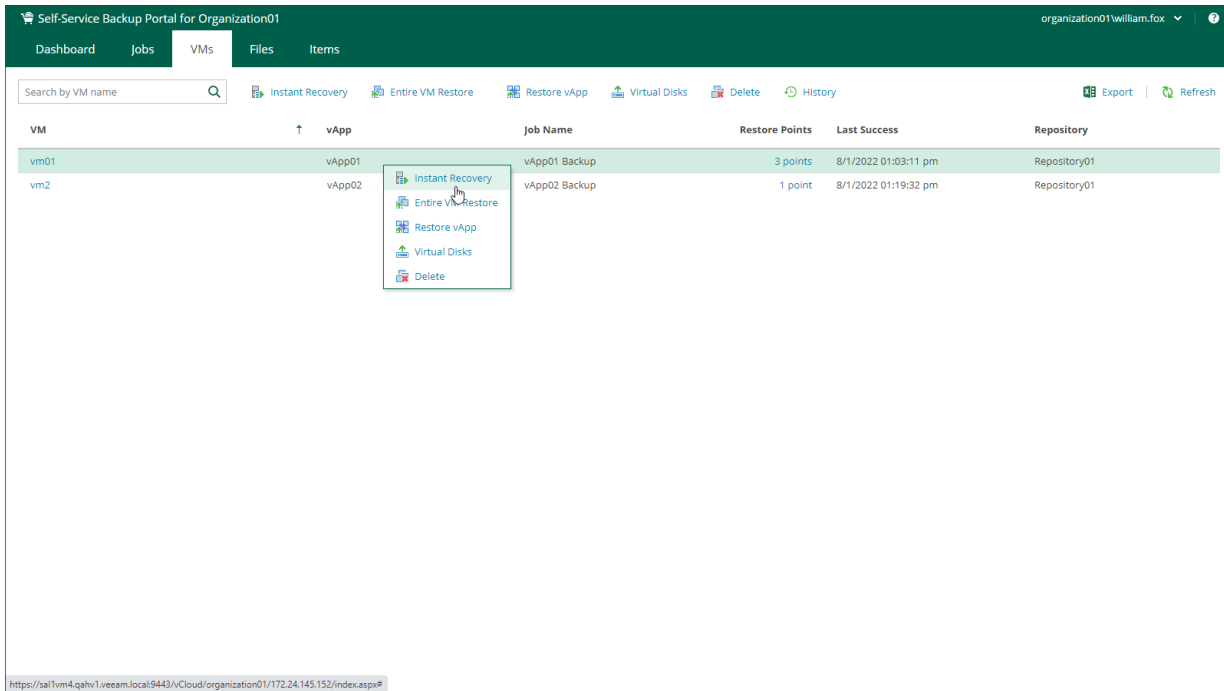
You can instantly recover VMware Cloud Director VMs from backups to the original vApp or another vApp that belongs to your VMware Cloud Director organization.

To instantly recover a VM, do the following:

1. On the **VMs** tab, select a VM you want to recover. To quickly find the necessary VM, use the search field at the top of the window.
2. On the toolbar, click **Instant Recovery**.

Alternatively, you can right-click the VM and select **Instant Recovery**.

3. Follow the steps of the **Instant Recovery** wizard. For more information, see [Instant Recovery to VMware Cloud Director](#).



Entire VM Restore

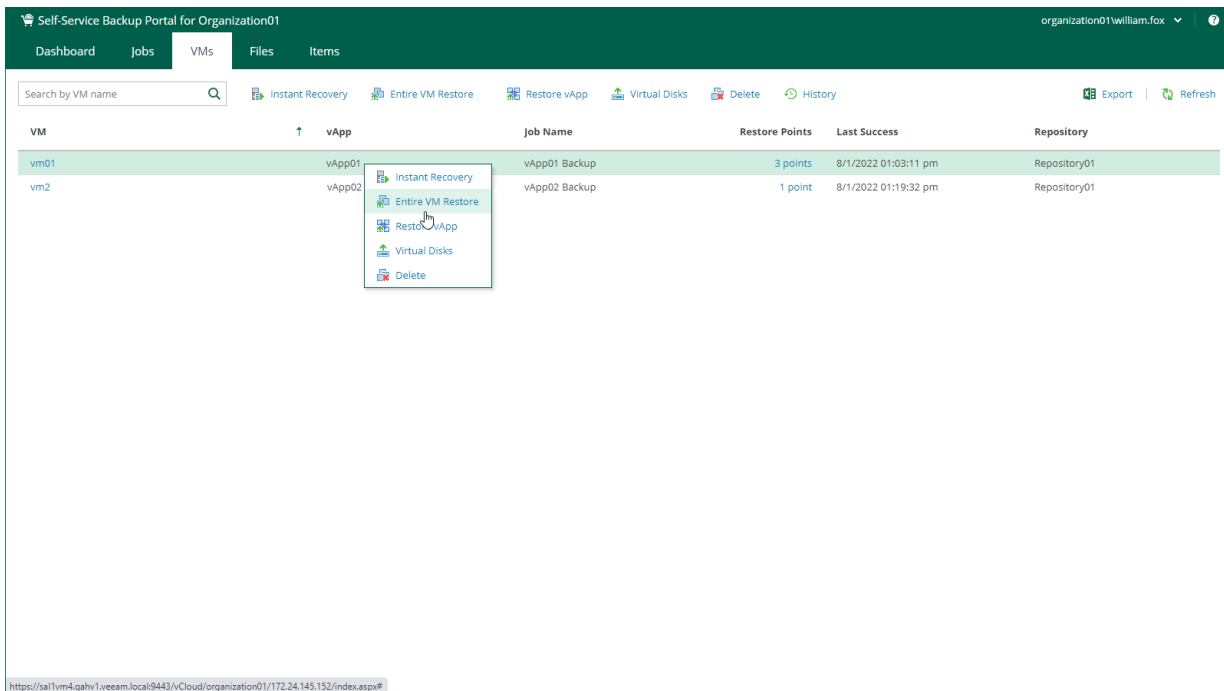
You can restore VMware Cloud Director VMs from backups to the original vApp or another vApp that belongs your VMware Cloud Director organization.

To restore an entire VM, do the following:

1. On the **VMs** tab, select a VM you want to restore. To quickly find the necessary VM, use the search field at the top of the window.
2. On the toolbar, click **Entire VM Restore**.

Alternatively, you can right-click the VM and select **Entire VM Restore**.

3. Follow the steps of the **Entire VM Restore** wizard. For more information, see [Restoring Entire VM to VMware Cloud Director](#).



Restoring vApps

You can restore a vApp to the original (production) 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.

- [Optional] To start VMs in the restored vApp immediately after recovery, select **Power on VM after restoring**.

Backup Date	Type	Job Name
11/25/2020 07:59:58 pm	Increment	Backup Job 1
11/22/2020 09:01:39 am	Full	Backup Job 1
11/15/2020 09:01:37 am	Full	Backup Job 1

Power on VM after restoring

Finish Cancel

- Click **Finish**.
- 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 VMware Cloud Director VMs.

To restore a virtual disk:

- 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.
- Click **Virtual Disks**.
- Follow the steps of the **Virtual Disk Restore** wizard. For details, see [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.

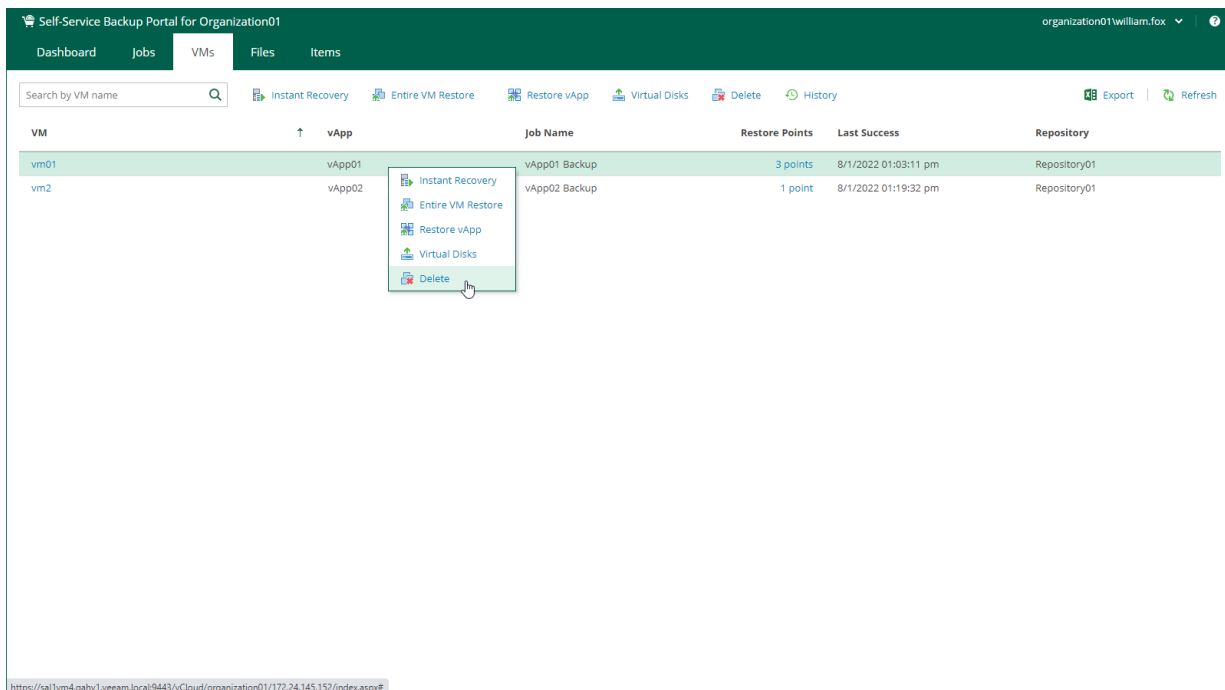
If you delete a VM that has GFS backups, they will not be deleted. You can delete them in Veeam Backup Enterprise Manager. For more information, see [Deleting Machine from Backup](#).

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 a VMware Cloud Director 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 a helper host or 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 a VMware Cloud Director organization can perform item-level recovery of Microsoft SQL Server, Oracle and PostgreSQL databases from application-aware backups. For more information, see [Restoring Microsoft SQL Server Databases](#), [Restoring Oracle Databases](#) and [Restoring PostgreSQL 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.

Veeam Plug-in for VMware vSphere Client

Veeam Plug-in for VMware vSphere Client 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 the Veeam Backup & Replication infrastructure and create restore points ad-hoc, using no other tool but vSphere Client.

In particular, vSphere administrators can view success, warning and 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 Client.

Veeam Backup Enterprise Manager offers the following configurations of the vSphere Client plug-in:

- For vSphere Client 7.0.0 or earlier, the plug-in is installed locally on the vCenter Server. For more information, see [Local vSphere Client Plug-in](#).
 - For vSphere Client versions 6.0 – 6.5, the plug-in is available with the flex/flash interface.
 - For vSphere Client versions 6.7 – 7.0.0, the plug-in offers HTML5 user interface. The earlier versions of the client do not support HTML5.
- For vSphere Client versions 7.0.1 or later, the plug-in is installed remotely on the Veeam Backup Enterprise Manager server. For more information, see [Remote vSphere Client Plug-in](#).

The screenshot displays the Veeam Backup & Replication interface within the vSphere Client. The interface is divided into several sections:

- Summary:** Shows the Veeam Backup & Replication logo and a table of infrastructure components:

Backup servers:	2
Proxy servers:	6
Repository servers:	5
Running jobs:	0
Scheduled jobs:	13
- Successful VM Backups:** A bar chart showing the status of VM backups:

Successful VM Backups	15 (83%)
VMs with warnings	3 (17%)
Failed VMs	0 (0%)
- VMs Overview:** A table showing the status of VMs:

Protected VMs:	11
Backed Up	10
Replicated	1
Restore points:	14
Full backup size	68.35 MB
Incremental backup size	5.41 GB
Replica restore points size	32.00 bytes
Source VMs size	160.30 GB
Successful backup sessions ratio	100%
- Job Statistics:** A table showing the status of backup jobs:

Running jobs:	0
Scheduled jobs:	13
Backup	10
Replica	3
Total jobs runs:	13
Successful jobs	9
Jobs with warnings	3
Jobs with errors	1
Max job duration:	3 hours 52 mins

Deploying vSphere Client Plug-in

You can install Veeam Plug-in for VMware vSphere Client using Veeam Backup Enterprise Manager under an account with the Portal Administrator role. For more information, see [Installing vSphere Client Plug-in](#).

For more information on VMware vSphere Client, see [this VMware article](#).

Before installing the plug-in, make sure the following requirements are met:

- The plug-in supports vSphere Client version 6.0 and later.
 - For vSphere Client 7.0.0 or earlier, the plug-in is installed locally on the VMware vCenter Server. For more information, see [Local vSphere Client Plug-in](#).
 - For vSphere Client versions 6.0 - 6.5, the plug-in is available with the flex/flash interface.
 - For vSphere Client versions 6.7 - 7.0.0, the plug-in offers HTML5 user interface. The earlier versions of the client do not support HTML5.
 - For vSphere Client versions 7.0.1 and later, plug-in is installed remotely on the Veeam Backup Enterprise Manager server. For more information, see [Remote vSphere Client Plug-in](#).

- The vCenter Server must be added to the backup server infrastructure.

For more information, see the [Adding VMware vSphere Servers](#) section of the Veeam Backup & Replication User Guide.

- The backup server that contains the vCenter Server in its infrastructure must be connected to Enterprise Manager.

For more information, see [Adding Backup Servers](#).

- The Enterprise Manager server must be able to resolve the FQDN of the vCenter Server and must have access to the vCenter Server over HTTPS. In particular, this is necessary if the plug-in uses default vCenter Single Sign-On for authentication.

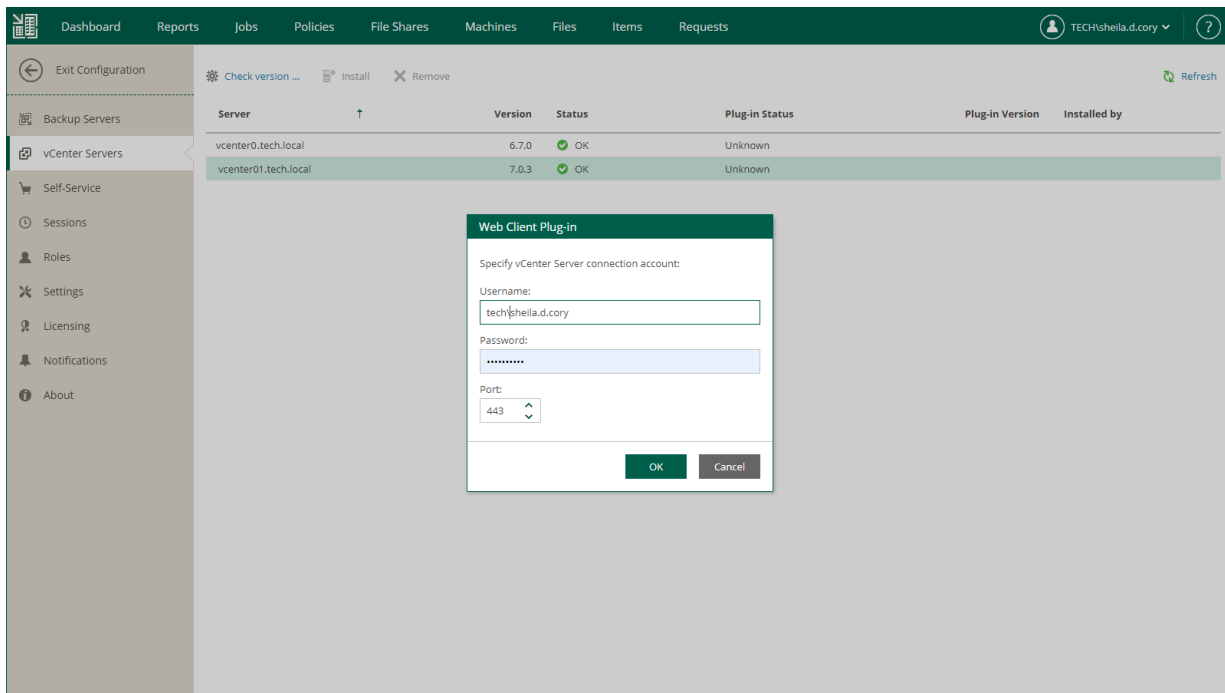
For more information on the authentication process, see [Configuring Plug-in Settings](#).

- 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

Installing vSphere Client Plug-in

To install Veeam Plug-in for VMware vSphere Client, take the following steps:

1. Log in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, go to the **vCenter Servers** section.
4. Select the vCenter Server you need, and click **Check version**.
5. In the **Web Client Plug-in** window, enter a user name and password to connect to the vCenter Server, and specify a connection port (default port is 443). Veeam Backup Enterprise Manager will use these credentials to access the vCenter Server and check if Veeam plug-in has been already installed there. If discovered, the plug-in version will be displayed in the **Plug-in Version** column.
6. 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.
7. After installation, the plug-in will be displayed in the list of vCenter Servers and plug-ins.



Uninstalling vSphere Client Plug-in

To uninstall Veeam Plug-in for VMware vSphere Client, take the following steps:

1. Log in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. Click **Configuration** in the top right corner.
3. In the **Configuration** view, go to the **vCenter Servers** section.
4. Select the vCenter Server you need, and click **Remove**.
5. In the displayed window, click **Yes** to confirm the removal.

NOTE

For details on reinstalling the local vSphere Client plug-in (the plug-in installed on the vSphere Client 7.0 or earlier), see [this Veeam KB article](#).

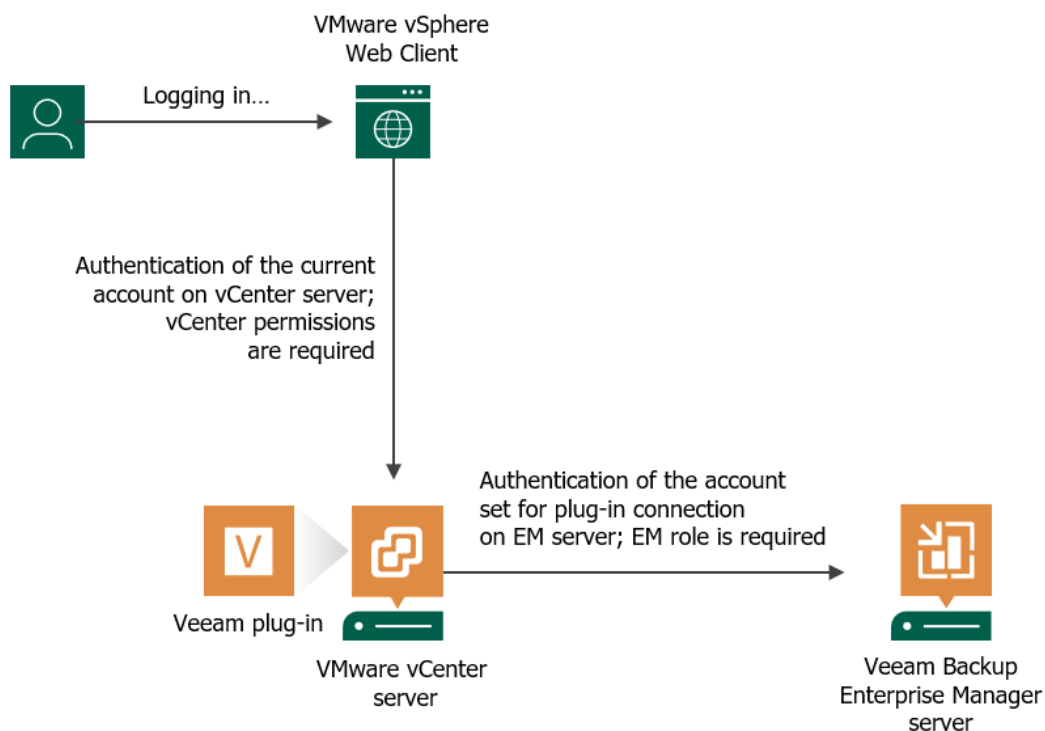
Local vSphere Client Plug-in

If you use VMware vSphere Client versions 7.0.0 or earlier, Veeam Plug-in for VMware vSphere Client is installed locally on the vCenter Server.

When using the plug-in, consider that authentication process includes the following stages:

1. A user logs in to VMware vSphere Client. To work with the VMware vCenter Server where Veeam plug-in runs, this user account requires the following minimal privileges on the 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, it must have sufficient security permissions to perform the necessary backup operation (VeeamZIP or Quick Backup). The permissions are granted by assigning a security role – Portal Administrator or Portal User. For more information, see [Configuring Accounts and Roles](#).



Accessing vSphere Client Plug-in

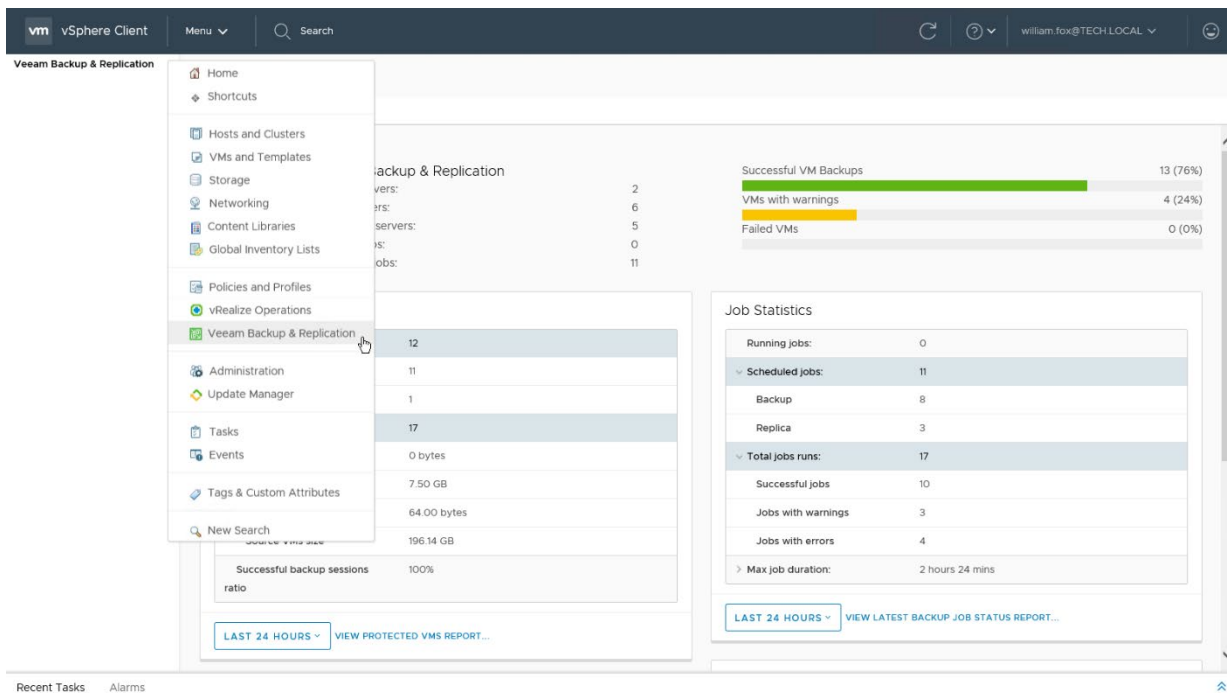
To access the plug-in, launch the vSphere Client and select **Veeam Backup & Replication** from the menu.

Make sure, the account used to connect to the Veeam Backup Enterprise Manager server and (optionally) Veeam ONE server has required permissions.

- 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 vSphere Client, or specific account configured in the plug-in [settings](#)) must have an Enterprise Manager role.
 - To create a VeeamZIP backup or Quick Backup, the Portal Administrator or Portal User role is required.
 - To browse backup infrastructure, the Restore Operator role is enough.

For more information on Enterprise Manager roles, see [Configuring Accounts and Roles](#).

- If you have Veeam ONE deployed in your environment and you want to open Veeam ONE reports from the plug-in (optional capability), the accounts used to connect to Enterprise Manager must be also included in the *Veeam ONE Power Users*, *Veeam ONE Read-Only Users* or *Veeam ONE Administrators* group on the machine where Veeam ONE Server is installed. For more information, see the [Security Groups](#) section of the Veeam ONE Deployment Guide.



Configuring Plug-in Settings

To configure a connection to the Veeam Backup Enterprise Manager server and (optionally) Veeam ONE server, take the following steps:

1. To open Veeam plug-in for vSphere Client, launch the vSphere Client and select **Veeam Backup & Replication** from the menu.
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.

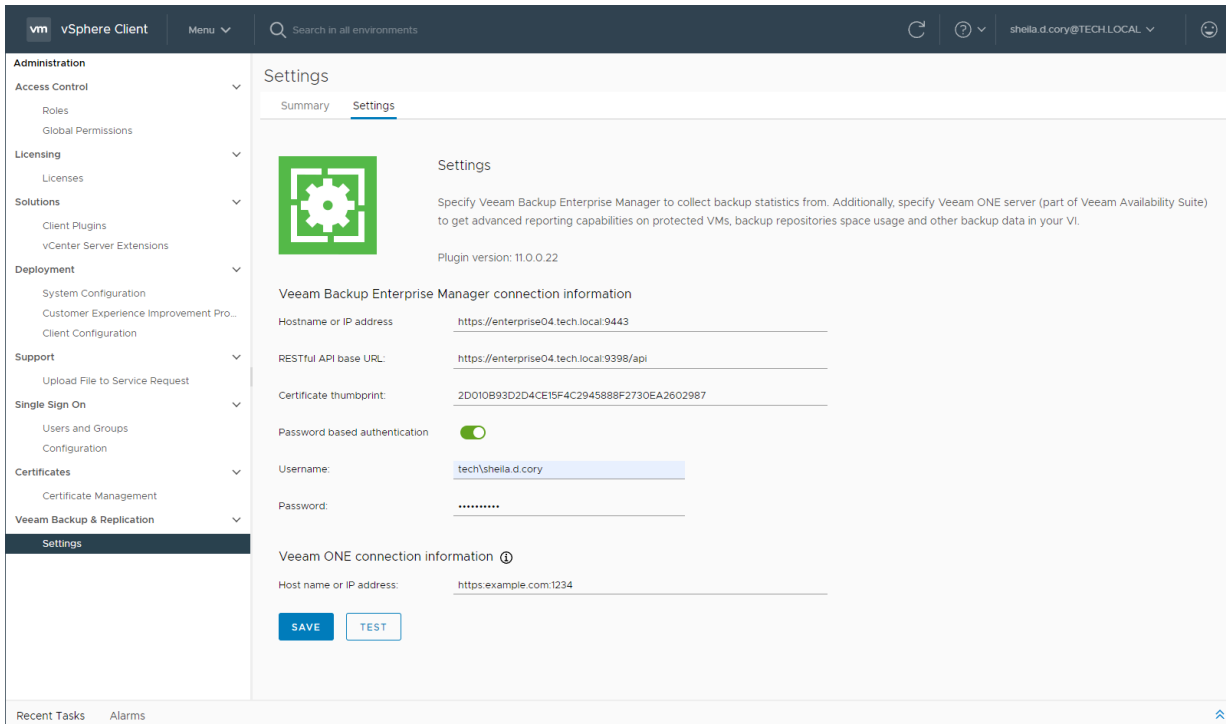
Make sure the account intended for connection to Enterprise Manager has the Portal Administrator or Portal User role assigned. For more information, see [Configuring Accounts and Roles](#).

4. [Optional] If you have Veeam ONE deployed in your environment and you want to open Veeam ONE reports from the plug-in, specify the Veeam ONE server name and connection port. Default is HTTP port 1239.

In this case, the account intended for connection to Enterprise Manager must be also a member of the *Veeam ONE Power Users*, *Veeam ONE Read-Only Users* or *Veeam ONE Administrators* group on the machine where Veeam ONE Server is installed. For more information, see the [Security Groups](#) section of the Veeam ONE Deployment Guide.

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).

The screenshot displays the Veeam Backup & Replication Summary page within the vSphere Client. The interface includes a top navigation bar with 'vm vSphere Client', a search bar, and a user profile 'william.fox@TECH.LOCAL'. The main content area is titled 'Summary' and contains several widgets:

- Veeam Backup & Replication Summary:** A central widget showing system metrics:

Backup servers:	2
Proxy servers:	6
Repository servers:	5
Running jobs:	0
Scheduled jobs:	13
- Successful VM Backups:** A bar chart showing the status of backup jobs:

Successful VM Backups	15 (83%)
VMs with warnings	3 (17%)
Failed VMs	0 (0%)
- VMs Overview:** A table providing details on protected VMs and restore points:

Protected VMs:	11
Backed Up	10
Replicated	1
Restore points:	14
Full backup size	68.35 MB
Incremental backup size	5.41 GB
Replica restore points size	32.00 bytes
Source VMs size	160.30 GB
Successful backup sessions ratio	100%
- Job Statistics:** A table summarizing the execution of backup jobs:

Running jobs:	0
Scheduled jobs:	13
Backup	10
Replica	3
Total jobs runs:	13
Successful jobs	9
Jobs with warnings	3
Jobs with errors	1
Max job duration:	3 hours 52 mins

At the bottom of the summary section, there are two buttons: 'LAST 24 HOURS' and 'VIEW PROTECTED VMS REPORT...' on the left, and 'LAST 24 HOURS' and 'VIEW LATEST BACKUP JOB STATUS REPORT...' on the right. The bottom of the interface shows 'Recent Tasks' and 'Alarms' tabs.

Creating Restore Points with VeeamZIP and Quick Backup

You can quickly create a VM restore point using VeeamZIP (full backup) or Quick Backup (incremental backup) right from VMware vSphere Client, with no need to use the Veeam Backup & Replication 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](#).

Creating Full VM Backup with VeeamZIP

You can use Veeam plug-in for vSphere Client to create an ad-hoc VeeamZIP backup of a VM. For more information on VeeamZIP, see the [VeeamZIP](#) section of the Veeam Backup & Replication User Guide.

Configuring VeeamZIP Settings

To configure the settings for VeeamZIP (VBK file creation), do the following:

1. In vSphere 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.

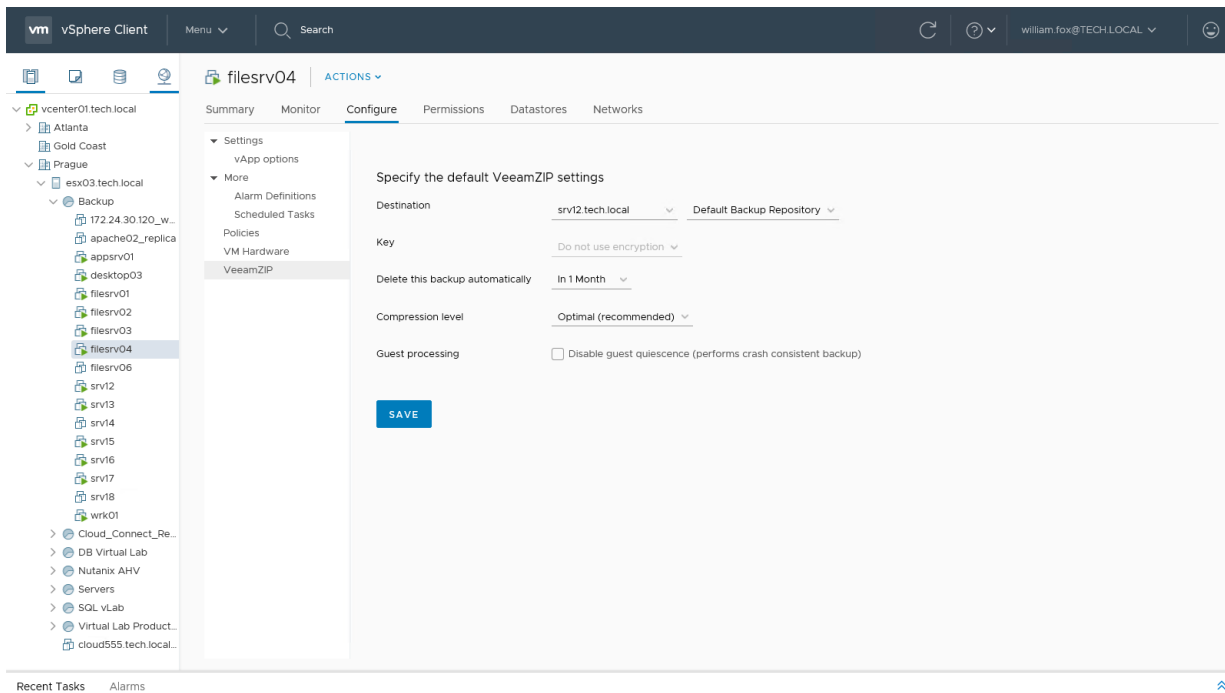
5. In the **Key** section, specify the encryption key if necessary.
6. In the **Delete this backup automatically** section, specify whether the resulting backup file should be automatically deleted after a certain time interval.
7. In the **Compression level** section, select the necessary compression 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

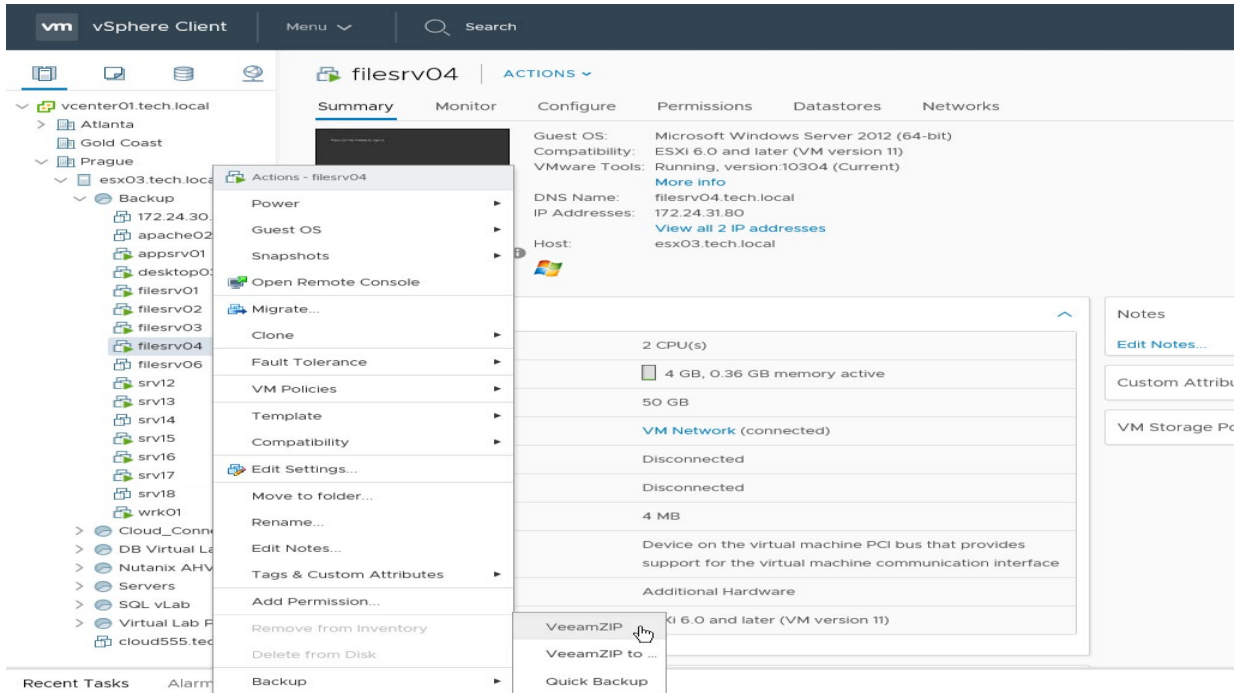
You can use Veeam plug-in for vSphere Client to create an ad-hoc VeeamZIP backup of a VM. To create a full VM backup with VeeamZIP:

1. In vSphere 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:

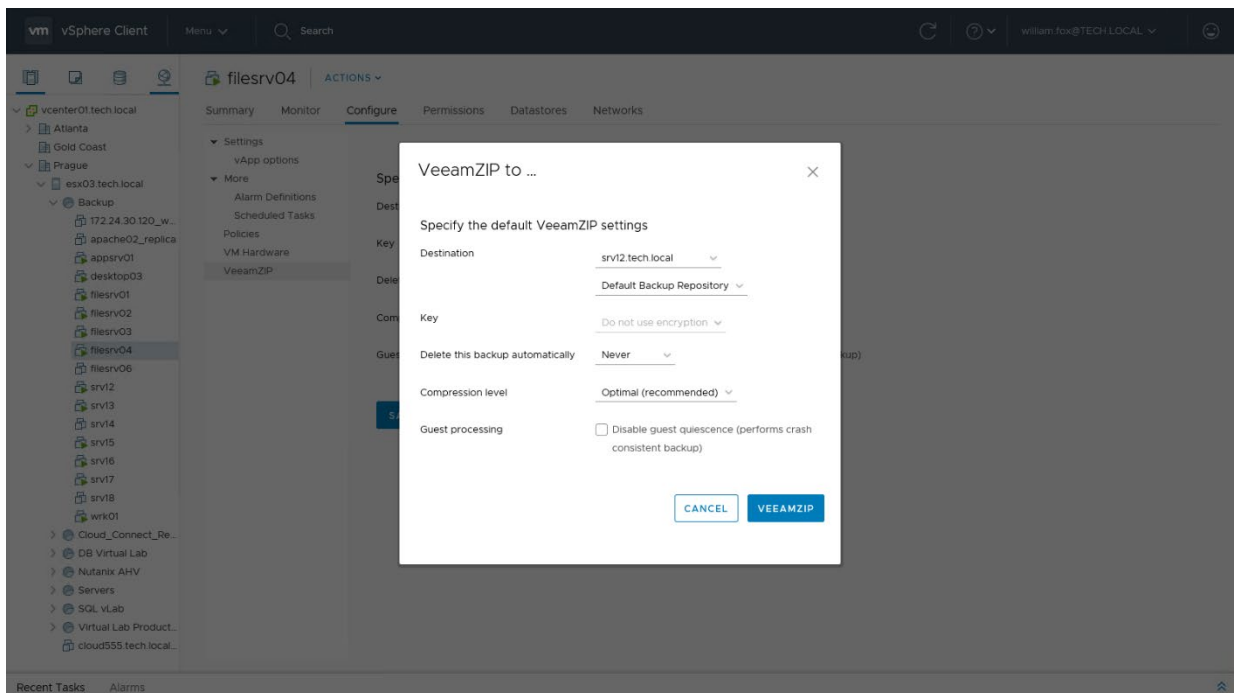
- Select **Backup > VeeamZIP** if you want to create a backup using the default VeeamZIP settings specified earlier. Alternatively, use the **Actions > Backup > VeeamZIP** option.

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 Client.

NOTE

A VeeamZIP backup 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.

Creating Incremental VM Backup with Quick Backup

You can use Veeam plug-in for vSphere Client to create a quick backup for the selected VM. For more information on quick backup, see the [Quick Backup](#) section of the Veeam Backup & Replication User Guide.

You can perform quick backup 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, do the following:

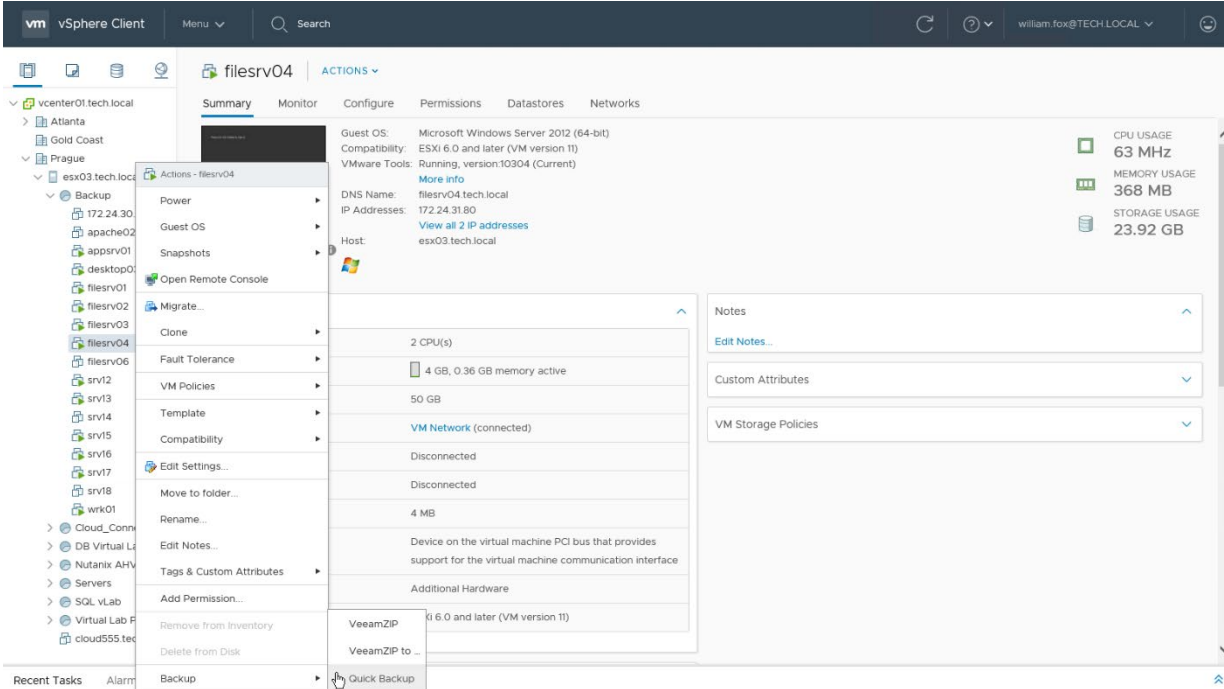
1. In the **vCenter Inventory**, select the necessary VM.
2. Right-click the VM and select **Quick Backup**. Alternatively, you can use the **Actions** menu command.

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 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.

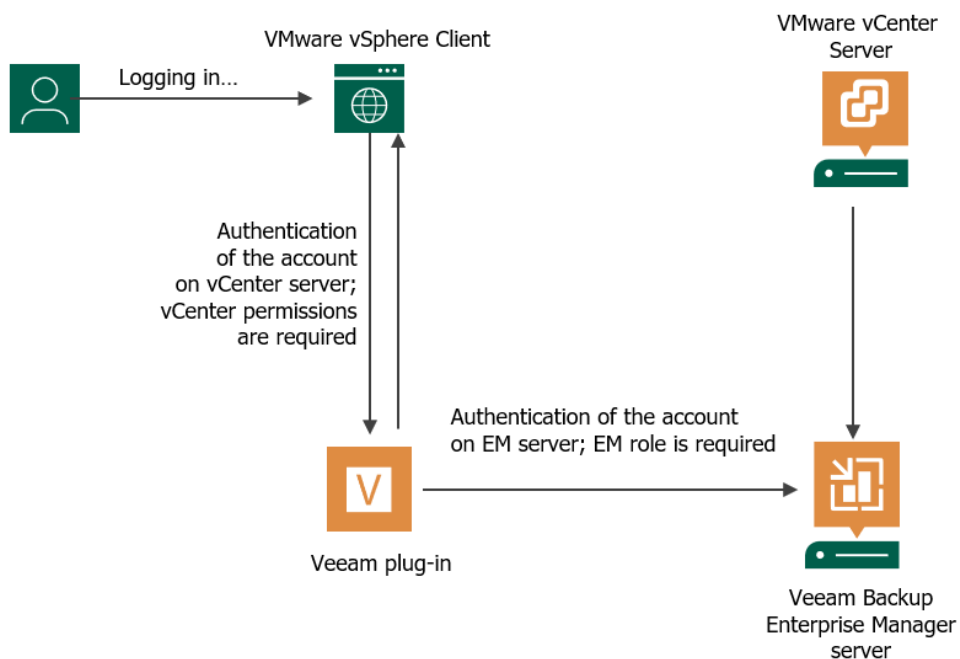


Remote vSphere Client Plug-in

If you use VMware vSphere Client versions 7.0.1 or later, Veeam Plug-in for VMware vSphere Client is installed remotely on the Veeam Backup Enterprise Manager server. While deploying the plug-in, the installer registers the plug-in as an extension on the vCenter Server, and the vCenter Server downloads the plug-in manifest file. This lets the *vsphere-ui* service define where the plug-in extends the VMware vSphere Client UI. The back-end service of the plug-in runs on the Enterprise Manager server.

When using the plug-in, consider that authentication process includes the following stages:

1. A user logs in to VMware vSphere Client. To work with the Veeam Plug-in, this user account must be a member of the vCenter Server role that is paired with an Enterprise Manager role. For more information on assigning Enterprise Manager roles, see [Configuring VMware vSphere Roles](#).
2. Veeam Plug-in connects to Veeam Backup Enterprise Manager, and Veeam Backup Enterprise Manager verifies the user account. The account must have sufficient security permissions to perform the necessary backup operation (VeeamZIP or Quick Backup).



Accessing vSphere Client Plug-in

To access the plug-in, launch the vSphere Client and select **Veeam Plug-in for VMware vSphere Client** from the menu.

Make sure, the account used to access the plug-in has permissions to connect to the Veeam Backup Enterprise Manager server and (optionally) Veeam ONE server.

- To launch the plug-in and successfully obtain statistics from Veeam Backup Enterprise Manager, you need to pair a vCenter Server role with an Enterprise Manager role. Then you can use an account with this vCenter Server role to log in to the vSphere Client and access the plug-in. For more information on assigning Enterprise Manager roles, see [Configuring VMware vSphere Roles](#).
 - To create a VeeamZIP backup or Quick Backup, the Portal Administrator or Portal User role is required.
 - To browse backup infrastructure, the Restore Operator role is enough.
- If you have Veeam ONE deployed in your environment and you want to open Veeam ONE reports from the plug-in (optional capability), the accounts used to log in to the vSphere Client must be also included in the *Veeam ONE Power Users*, *Veeam ONE Read-Only Users* or *Veeam ONE Administrators* group on the machine where Veeam ONE Server is installed. For more information, see the [Security Groups](#) section of the Veeam ONE Deployment Guide.

The screenshot shows the vSphere Client interface. In the left sidebar, the 'Veeam Plug-in for VMware vSphere Client' menu item is highlighted. The main content area displays a 'Replication' dashboard. It includes a bar chart showing replication progress for different categories: 6 (7%), 0 (0%), and 83 (93%). Below the chart is a table showing replication statistics for 'Last 24 hours' and 'Last month'. The 'Last 24 hours' table shows 100, 15, and 85. The 'Last month' table shows -, 20, and -. Below this is a table showing storage capacity for different types of VMs.

Type	Capacity	Used space	Free space
Windows	219.45 GB	165.46 GB	53.99 GB
Windows	199.45 GB	87.49 GB	111.96 GB
Windows	499.45 GB	276.05 GB	223.40 GB

Below the storage table is an 'Errors and Warnings (last 24 hours)' section. It shows 91 errors and 0 warnings. A table lists the errors:

VM name	Status	Start time	Job type
as2016DC	Error	02/08/2023, 10:00:19 AM	Backup
as2016DC	Error	02/08/2023, 9:32:34 AM	Backup
as2016DC	Error	02/08/2023, 9:21:59 AM	Backup
as2016DC	Error	02/08/2023, 9:11:00 AM	Backup
as2016DC	Error	02/08/2023, 9:00:02 AM	Backup
as2016DC	Error	02/08/2023, 8:31:42 AM	Backup
as2016DC	Error	02/08/2023, 8:21:20 AM	Backup
as2016DC	Error	02/08/2023, 8:10:52 AM	Backup
as2016DC	Error	02/08/2023, 8:00:14 AM	Backup
as2016DC	Error	02/08/2023, 7:32:06 AM	Backup
as2016DC	Error	02/08/2023, 7:21:32 AM	Backup
as2016DC	Error	02/08/2023, 7:10:37 AM	Backup
as2016DC	Error	02/08/2023, 7:00:15 AM	Backup
as2016DC	Error	02/08/2023, 6:31:54 AM	Backup
as2016DC	Error	02/08/2023, 6:21:27 AM	Backup
as2016DC	Error	02/08/2023, 6:10:34 AM	Backup
as2016DC	Error	02/08/2023, 6:00:02 AM	Backup

Examining Backup Infrastructure

On the Veeam Plug-in for VMware vSphere Client main page, you can view statistics on the Veeam Backup & Replication infrastructure. The statistics are shown for the VMs that are included in the restore scope specified for your vCenter Server role. For more information on the restore scope, see [Configuring VMware vSphere Roles](#).

You can view the following statistics:

- **Protection Status** – statistics on the status of VM backup and replication jobs for the last 24 hours.
 - **Successful VM backups** – number of successfully backed up or replicated VMs
 - **VMs with Warnings** – number of VMs that were backed up or replicated with a warning
 - **Failed VMs** – number of VMs that were backed up or replicated with an error
- **Errors and Warnings** – statistics on backup and replication sessions that completed with a warning or error for the last 24 hours.
- **VMs Overview** – statistics about all available VMs for the last 24 hours and last month.
 - **Total VMs** – number of all available VMs
 - **Protected VMs** – number of VMs that were backed up or replicated
 - **Not protected VMs** – number of VMs that were not backed up or replicated
- **Repositories** – information about backup repositories, including repository name, type, overall capacity, backup size and free space.
- **Active Sessions** – statistics about all active backup and replication sessions for all vCenter Server VMs.

The screenshot displays the Veeam Backup & Replication interface within the vSphere Client. The interface is divided into several sections:

- Protection Status (last 24 hours):** A bar chart showing the status of VM backups. It indicates 6 (7%) Successful VM backups, 0 (0%) VMs with warnings, and 82 (93%) Failed VMs.
- VMs Overview:** A table comparing VM statistics for the last 24 hours and the last month. The table shows 100 Total VMs, 15 Protected VMs, and 85 Unprotected VMs in the last 24 hours, and 0 Total VMs, 20 Protected VMs, and 0 Unprotected VMs in the last month.
- Repositories:** A table listing backup repositories with columns for Name, Type, Capacity, Used space, and Free space. The table shows three repositories: Default Backup Repository (Windows, 219.45 GB Capacity, 165.46 GB Used space, 53.99 GB Free space), Default Backup Repository (Windows, 199.45 GB Capacity, 87.49 GB Used space, 111.96 GB Free space), and Backup Repository 1 (Windows, 499.45 GB Capacity, 276.05 GB Used space, 223.40 GB Free space).
- Errors and Warnings (last 24 hours):** A table listing backup sessions that completed with an error. It shows 90 Errors and 0 Warnings. The table columns are VM name, Status, Start time, and Job type. All listed sessions are 'Backup' jobs for VMs named 'as2016DC' that failed at various times on 02/08/2023.

Creating Restore Points with VeeamZIP and Quick Backup

You can quickly create a VM restore point using VeeamZIP (full backup) or Quick Backup (incremental backup) right from VMware vSphere Client, with no need to use the Veeam Backup & Replication console. To utilize these capabilities, you need to pair a vCenter Server role of your account with the Portal Administrator or Portal User role of Enterprise Manager. For more information on assigning Enterprise Manager roles, see [Configuring VMware vSphere Roles](#).

Creating Full VM Backup with VeeamZIP

You can use Veeam Plug-in for VMware vSphere Client to create an ad-hoc VeeamZIP backup of a VM. For more information on VeeamZIP, see the [VeeamZIP](#) section of the Veeam Backup & Replication User Guide.

Configuring VeeamZIP Settings

Before you create a full VM backup with VeeamZIP, you need to configure VeeamZIP settings. The specified configuration is stored for the user account in your browser settings.

To configure the VeeamZIP settings, do the following:

1. In VMware vSphere Client, open the vCenter Server inventory.
2. In the inventory tree, select a VM.
3. On the **Configure** tab, select **Veeam Plug-in for VMware vSphere Client > VeeamZIP**.
Alternatively, you can right-click the VM and select **Veeam Web Client plug-in > VeeamZIP**.
4. In the **Destination** section, select the Veeam backup server that will process the VM and the repository where to store the VeeamZIP file.

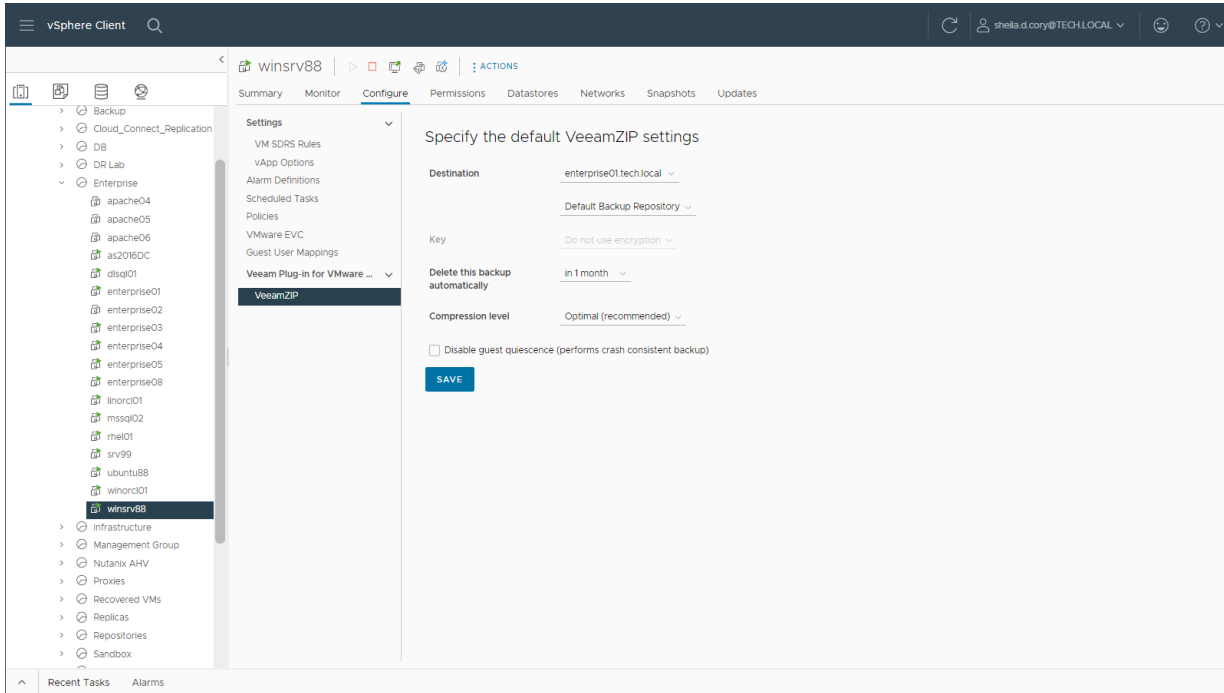
The plug-in displays Veeam backup servers added to the Veeam Backup Enterprise Manager infrastructure and backup repositories created in the backup infrastructure of these backup servers.

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. 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.

For more information about guest OS quiescence, see the [VMware Tools Quiescence](#) section of the Veeam Backup & Replication User Guide.

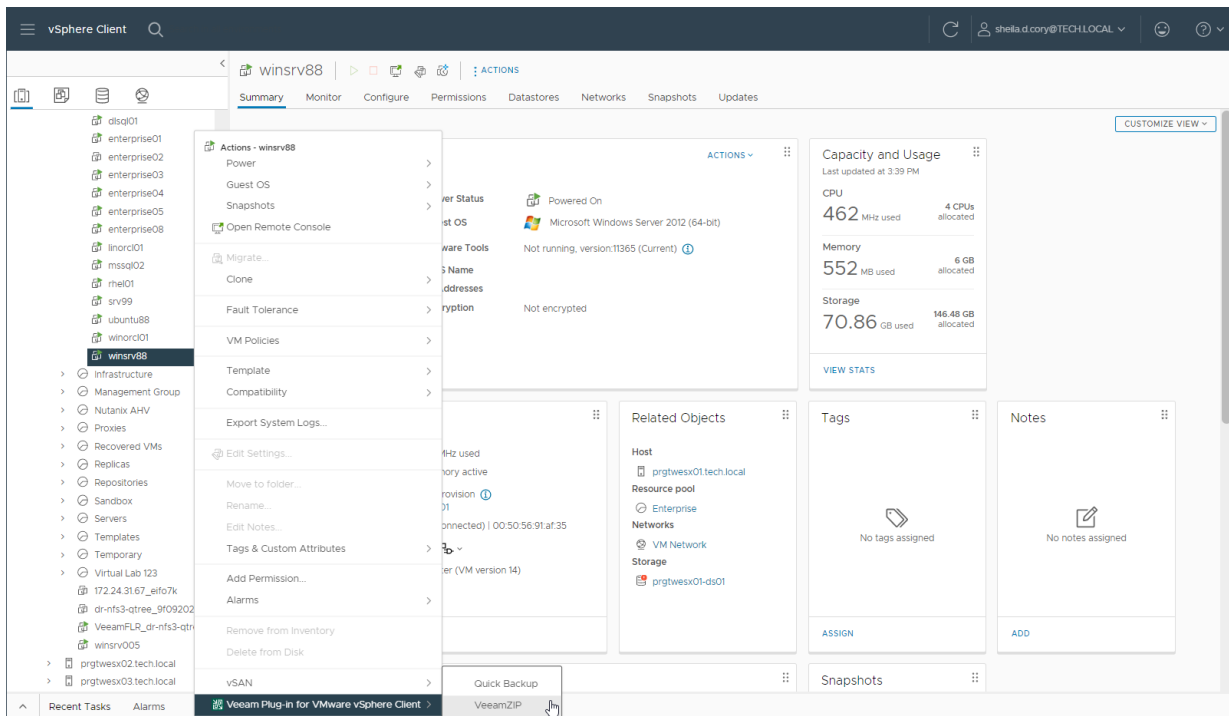
9. Click Save.



Creating Full VM Backup with VeeamZIP

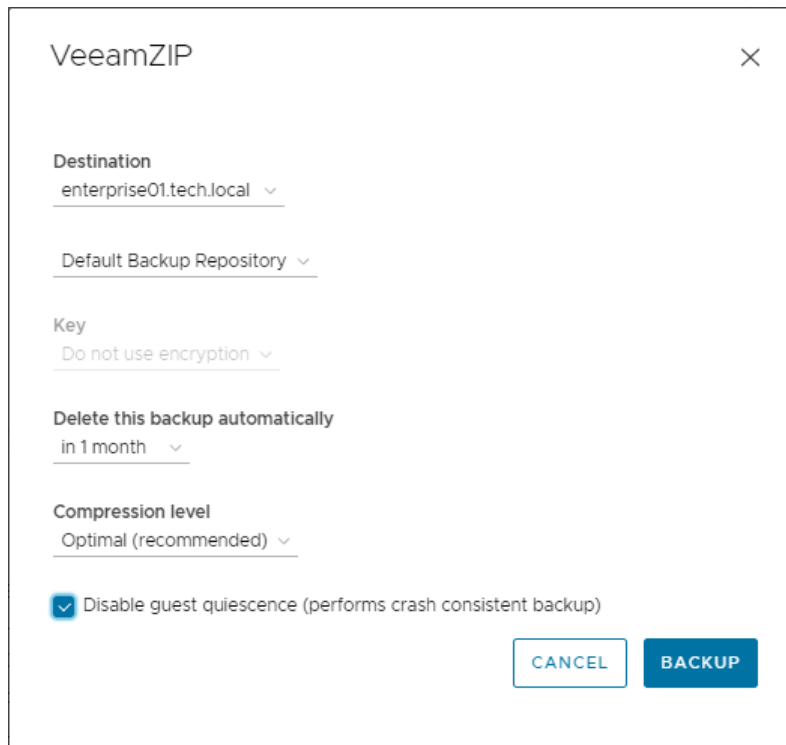
To create a full VM backup with VeeamZIP, do the following:

1. In vSphere Client, the vCenter Server inventory.
2. In the inventory tree, right-click the VM that you want to back up and select **Veeam Web Client plug-in > VeeamZIP**.



3. If you have already configured VeeamZIP settings, review the settings and click **Backup**.

If you have not configured VeeamZIP settings, specify the settings in the **VeeamZIP** window in the same way as described in the [Configuring VeeamZIP Settings](#).



VeeamZIP

Destination
enterprise01.tech.local

Default Backup Repository

Key
Do not use encryption

Delete this backup automatically
in 1 month

Compression level
Optimal (recommended)

Disable guest quiescence (performs crash consistent backup)

CANCEL BACKUP

You can view the backup creation progress in the **Recent Tasks** pane of vSphere Client.

NOTE

A 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.

Creating Incremental VM Backup with Quick Backup

You can use Veeam Plug-in for VMware vSphere Client to create a quick backup for the selected VM. For more information on quick backup, see the [Quick Backup](#) section of the Veeam Backup & Replication User Guide.

You can perform quick backup for any VM that meets the following requirements:

- A backup job processing the VM exists on the backup server that is added to Veeam Backup Enterprise Manager.
- There is a full backup file for this VM in the backup repository.

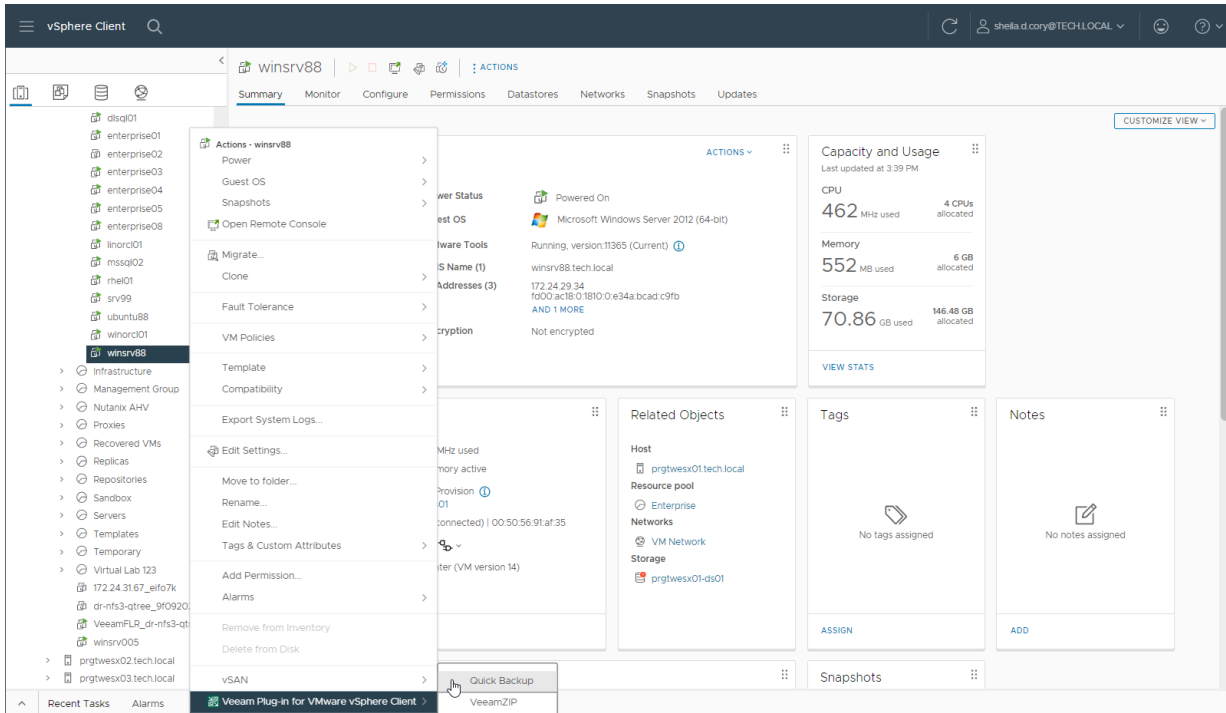
To perform quick backup, do the following:

1. In VMware vSphere Client, open the vCenter Server inventory.
2. In the inventory tree, select a VM.
3. Right-click the VM and select **Veeam Plug-in for VMware vSphere Client > Quick Backup**.

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.

NOTE

A quick backup 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, you can 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 VMware Cloud 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 Cloud Director organizations and their configurations. For more information, see [Working with VMware Cloud 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 the 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 VMware Cloud 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.

Delegation Mode ✕

vSphere tags
Users can manage all VMs with tags specified in the corresponding self-service configuration.

vSphere role: [Select Role...](#)
Users can manage all VMs for which they have the specified vSphere role assigned.

VM privilege: [Select Privilege...](#)
Users can manage all VMs for which they have the specified vSphere permission.

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	<i>DOMAIN Username</i> Domain is optional
Group	AD group	By specifying a user name and password	<i>DOMAIN Groupname</i> Domain is optional
External User	IdP user	By using single sign-on*	<i>Username@Suffix</i>
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

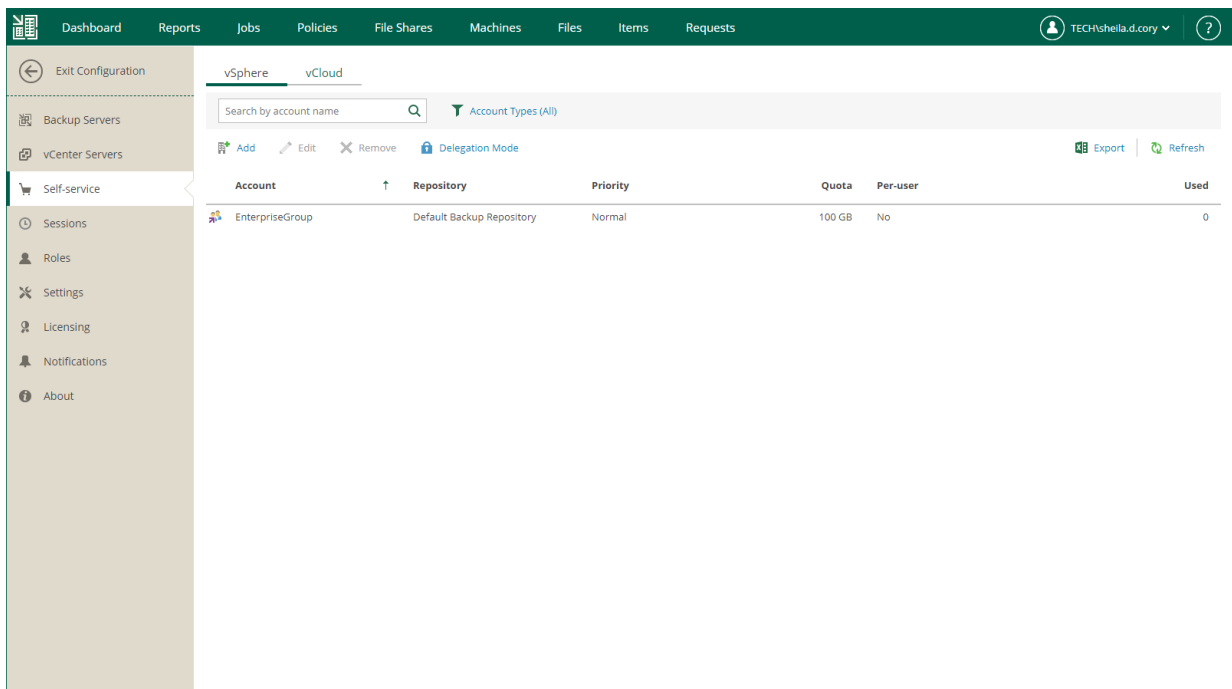
If you plan to provide a user with access to vSphere Self-Service Backup Portal only, and not to the main Enterprise Manager UI, you do not need to configure an account for this user in the **Roles** tab of the **Configuration** view.

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 VMware Cloud 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.

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Type: Group
- Account: tech.local\Tech Admins
- Repository: Backup Repository 5 (enterprise05.tech.local)
- Quota: 500 GB
- Job scheduling: Allow: Tenant has full access to all job scheduling o
- Job priority: High
- vCenter scope: vcenter01.tech.local
- Assign a separate quota to each group member

At the bottom of the dialog, there is a link "Show Advanced Job Settings", a "Save" button, and a "Cancel" button.

15. [Optional] Specify advanced settings for backup jobs of the tenant:
- Click the **Show Advanced Job Settings** link.
 - In the **Advanced job settings** section, view the currently used backup job settings.
 - 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.
 - 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**.

Add ✕

Type:

Account:

Repository:

Quota:

Job scheduling:

Job priority:

vCenter scope:

Assign a separate quota to each group member

Advanced job settings:

Backup	
Backup mode	Incremental
Create synthetic full backups periodically on	Saturday
Storage	
Enable inline data deduplication	Yes
Exclude swap file blocks	Yes
Exclude deleted file blocks	Yes
Compression level	Optimal
Storage optimization	Local target
vSphere	
Use changed block tracking data	Yes

Copy from:

Editing Tenant Account

The 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 VMware Cloud 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 and click **Save**. For details, see [Adding Tenant Account](#).

Edit [X]

Type: Group [v]

Account: tech.local\Tech Admins

Repository: Backup Vol 01 (srv12.tech.local) [v]

Quota: 100 [up/down] GB [v]

Job scheduling: Allow: Tenant has full access to all job scheduling o [v]

vCenter scope: 172.17.52.34 [x] [v]

vSphere tags: Infrastructure [x] [v]

Assign a separate quota to each group member

Advanced job settings:

Backup

Backup mode: Incremental [up]

Create synthetic full backups periodically on: Saturday

Storage

Enable inline data deduplication: Yes

Exclude swap file blocks: Yes

Exclude deleted file blocks: Yes

Compression level: Optimal

Storage optimization: Local target

vSphere

Use changed block tracking data: Yes [down]

Copy from: Default settings [v] [Apply]

[Hide Advanced Job Settings] [Save] [Cancel]

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 VMware Cloud 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 VMware Cloud 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://enterprise01.tech.local: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](#).

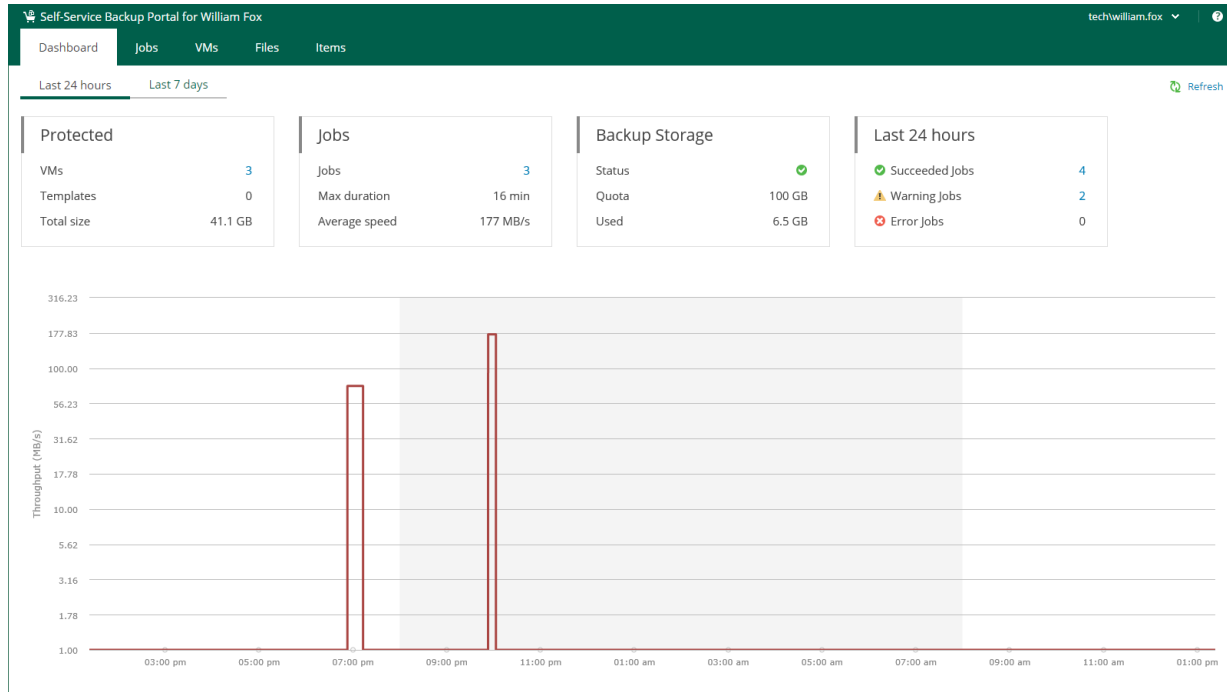
Working with Portal

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 Dashboard Chart](#).

Managing Backup Jobs

In the **Jobs** tab of Self-Service Backup Portal, you can perform the following operations with backup jobs:

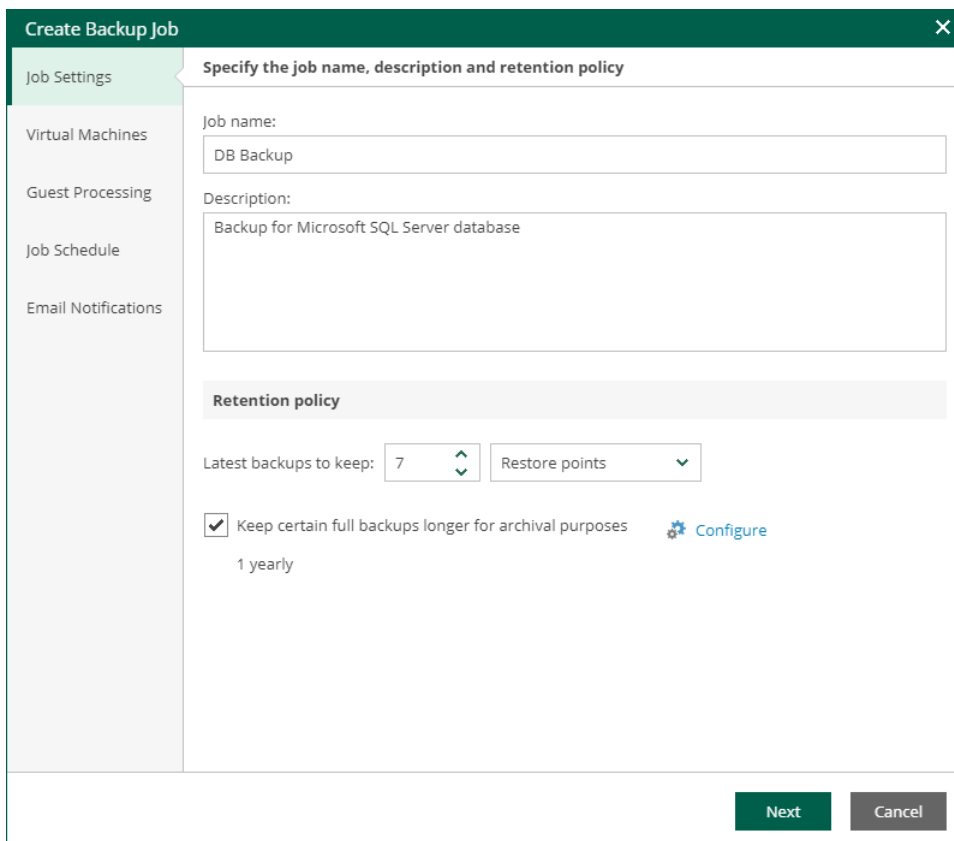
- [Create a new backup job for vSphere VMs](#)
- [Start, stop and retry jobs](#)
- [Enable and disable jobs](#)
- [Edit backup job settings](#)
- [Delete backup jobs](#)

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.



The screenshot shows the 'Create Backup Job' wizard in the 'Job Settings' step. The title bar reads 'Create Backup Job' with a close button. The main heading is 'Specify the job name, description and retention policy'. On the left, a sidebar lists navigation options: 'Job Settings' (selected), 'Virtual Machines', 'Guest Processing', 'Job Schedule', and 'Email Notifications'. The main area contains the following fields and controls:

- Job name:** A text input field containing 'DB Backup'.
- Description:** A text area containing 'Backup for Microsoft SQL Server database'.
- Retention policy:** A section with a header 'Retention policy' and the following settings:
 - 'Latest backups to keep:' is set to '7' with up/down arrows.
 - 'Restore points' is set to 'Restore points' with a dropdown arrow.
 - A checkbox is checked for 'Keep certain full backups longer for archival purposes', with a 'Configure' link and a gear icon.
 - The archival period is set to '1 yearly'.

At the bottom right, there are 'Next' and 'Cancel' buttons.

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 **Notify on success** to receive an email notification when the job completes successfully.
 - d. Select **Notify on warning** to receive an email notification when the job completes with a warning.
 - e. Select **Notify on error** to receive an email notification when the job fails.
 - f. 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 and 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

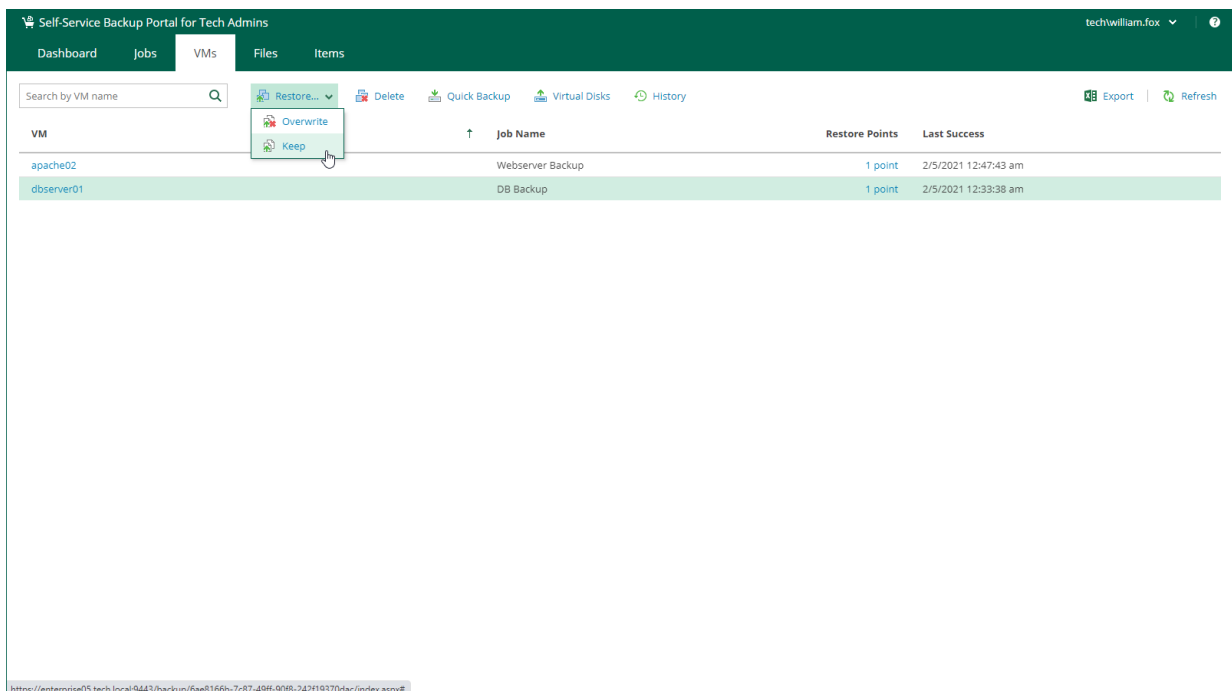
You can use vSphere Self-Service Backup Portal to perform the following operations with backed-up VMs:

- Search VMs and view VMs details
- [Restore VMs](#)
- [Restore VM disks](#)
- [Delete VMs](#)

Restoring VMs

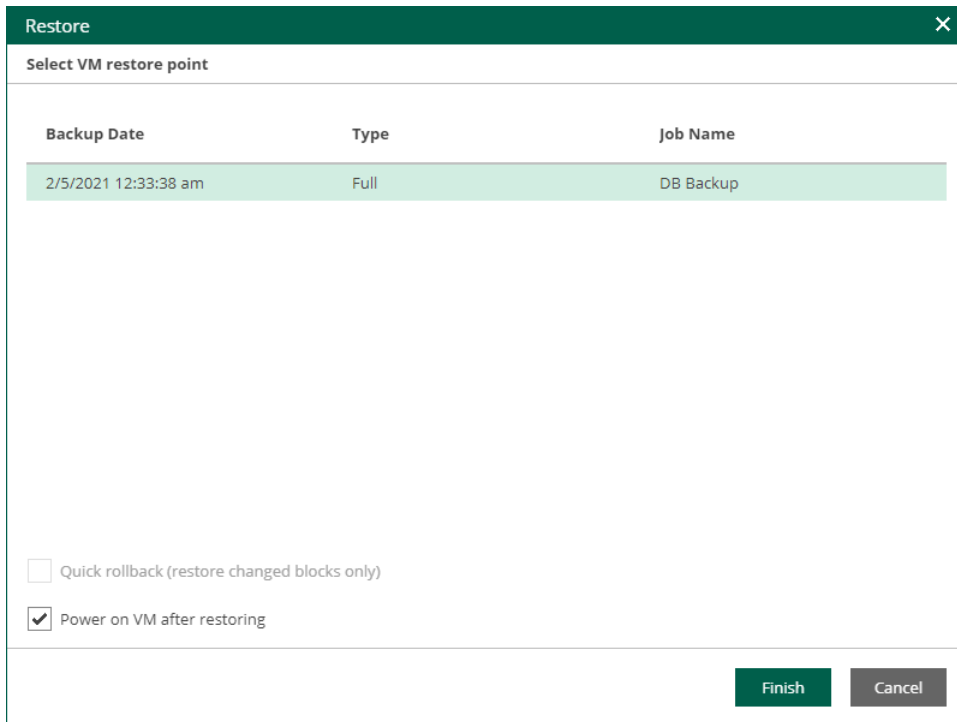
You can restore vSphere VMs to the original (production) location using flexible restore options. To restore a VM, do the following:

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.



Backup Date	Type	Job Name
2/5/2021 12:33:38 am	Full	DB Backup

Quick rollback (restore changed blocks only)

Power on VM after restoring

Finish **Cancel**

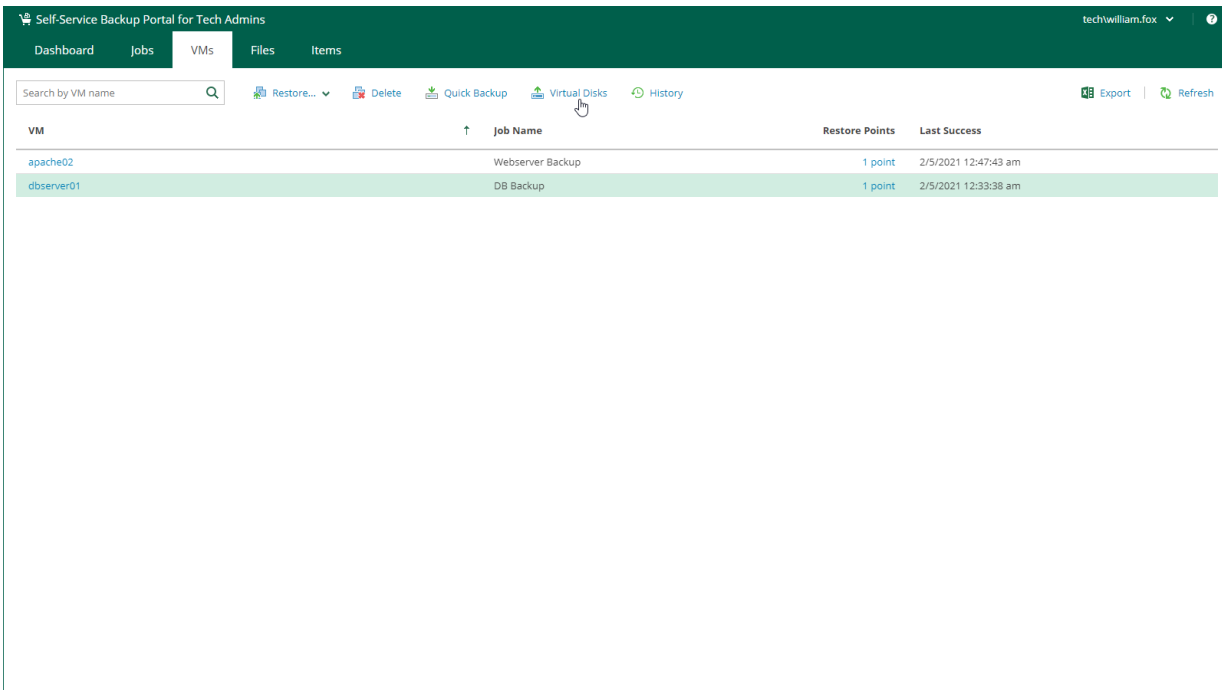
5. Click **Finish**.
6. Veeam Backup Enterprise Manager will display a message notifying that the VM from the backup will replace the original VM if this VM is present in the original location. Click **Proceed** to start the VM restore operation.

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 [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 a helper host or 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, Oracle databases and PostgreSQL instances.

For more information, see the following sections:

- [Restoring Microsoft SQL Server Databases](#)
- [Restoring Oracle Databases](#)
- [Restoring PostgreSQL Instances](#)

Veeam Backup Enterprise Manager Utilities

You can use the following Veeam Backup Enterprise Manager utilities to perform advanced administration tasks in the Enterprise Manager infrastructure:

- [Enterprise Manager Database Migration Utility](#)
- [Veeam Configuration Database Connection Utility](#)

Enterprise Manager Database Migration Utility

The Enterprise Manager Database Migration utility allows you to backup the Enterprise Manager configuration database based on Microsoft SQL Server and restore it to PostgreSQL. This lets you change the engine of the Enterprise Manager configuration database and keep the existing Enterprise Manager configurations such as notification settings, Enterprise Manager accounts, self-service configurations and so on.

After you restore the database, connect Veeam Backup Enterprise Manager to the restored database using the Configuration Database Connection Settings utility. For more information, see [Veeam Configuration Database Connection Utility](#).

NOTE

Veeam Backup Enterprise Manager collects data from backup servers with configuration databases that run on the same database engine as the Enterprise Manager configuration database. This means that after you migrate the Enterprise Manager database, you must migrate Microsoft SQL Server configuration databases of already added backup servers and add them again to the Enterprise Manager infrastructure. For more information, see the [Migrating Configuration Database to PostgreSQL Server](#) section of the Veeam Backup & Replication User Guide.

The Enterprise Manager Database Migration utility comes with Veeam Backup Enterprise Manager and is located on the Enterprise Manager server in the installation folder. The default path is the following:

```
%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\Veeam.EM.DB.Migration.exe.
```

To run the utility, use a command-line shell. The utility requires access to the registry so you must run the shell as administrator.

Syntax

With the Enterprise Manager Database Migration utility, you can perform the following operations:

- Back up a Microsoft SQL Server database to an EMCO backup file:

```
Veeam.EM.DB.Migration.exe /file:value /backupemdatabase [/encryptionpassword:value] [/encryptionhint:value] [/verbose]
```

- Restore a Microsoft SQL Server database from a backup file to PostgreSQL:

```
Veeam.EM.DB.Migration.exe /file:<value> /restoreemdatabase [/encryptionpassword:<value>] [/servername:<value>] [/serverport:<value>] [/initialcatalog:<value>] [/login:<value>] [/password:<value>] [/verbose]
```

- Display the utility help:

```
Veeam.Backup.Configuration.Tool /?
```

Parameters

The table below describes parameters that you can use to backup and restore the Enterprise Manager configuration database.

Parameter	Description
<code>/?</code>	Displays help.
<code>/file:<value></code>	Specifies file name and location of an EMCO backup file.
<code>/encryptionpassword:<value></code>	Specifies a password for backup file encryption.
<code>/encryptionhint:<value></code>	Specifies a hint for the encryption password.
<code>/backupemdatabase</code>	Backs up the Enterprise Manager configuration database based on Microsoft SQL Server to an EMCO backup file. Note the command cannot back up a PostgreSQL database.
<code>/restoreemdatabase</code>	Restores the Enterprise Manager configuration database from an EMCO backup file to PostgreSQL.
<code>/servername:<value></code>	Specifies a name or IP address of the target host with PostgreSQL server. The default value is <i>localhost</i> .
<code>/serverport:<value></code>	Specifies a port number of a PostgreSQL instance. The default value is <i>5432</i> .
<code>/initialcatalog:<value></code>	Specifies a name of a target PostgreSQL instance. The default value is <i>VeeamBackupReporting</i> . If an instance with the specified name (or the default name) exists, the utility adds an increment postfix to the instance name, for example: <i>VeeamBackupReporting_00</i> , <i>VeeamBackupReporting_01</i> .
<code>/login:<value></code>	Specifies an account name that the utility uses to authenticate against a PostgreSQL server. By default, the utility uses the account under which the Veeam Backup Enterprise Manager Service is running.
<code>/password:<value></code>	Specifies a password that the utility uses to authenticate against a PostgreSQL server. By default, the utility uses the account under which the Veeam Backup Enterprise Manager Service is running.
<code>/verbose</code>	Enables verbose logging mode. Logs are stored in the following directory: <code>%PROGRAMDATA%\Veeam\Backup\Utils\Util.EmTransfer.</code>

Examples

Example 1

This example shows how to back up the Enterprise Manager configuration database to an EMCO backup file.

```
Veeam.EM.DB.Migration.exe /file:"C:\EM Configuration\02.emco" /backupemdatabase /encryptionpassword:Password01 /encryptionhint:thatpass
```

where:

- /file:"C:\EM Configuration\02.emco" – file name and location of the backup file. If you specify a folder that does not exist, the utility will create it. If a file with the specified name already exists, it will be rewritten.
- /backupemdatabase – utility backup mode.
- /encryptionpassword:Password01 – encryption password for the backup file.
- /encryptionhint:thatpass – password hint.

Microsoft SQL Server connection settings are not required in the command, the utility gets them from the registry.

Example 2

This example shows how to restore the Enterprise Manager configuration database from an EMCO backup file to PostgreSQL.

```
Veeam.EM.DB.Migration.exe /file:"C:\EM Configuration\02.emco" /restoreemdatabase /encryptionpassword:Password01 /servername:enterprise05 /initialcatalog:VeeamBackupReporting_01 /serverport:5434 /login:postgres /password:Password02
```

where:

- /file:"C:\EM Configuration\02.emco" – file name and location of the backup file.
- /restoreemdatabase – utility restore mode.
- /encryptionpassword:Password01 – encryption password for the backup file.
- /servername:enterprise05 – name of the target PostgreSQL server.
- /initialcatalog:VeeamBackupReporting_01 – target PostgreSQL instance.
- /serverport:5434 – port number of the target PostgreSQL instance.
- /login:postgres – account name used to authenticate against the PostgreSQL server.
- /password:Password02 – password used to authenticate against the PostgreSQL server.

Configuration Database Connection Settings Utility

The Configuration Database Connection Settings utility allows you to manage connection settings for Veeam Backup Enterprise Manager and Veeam Backup & Replication configuration databases.

Using this utility, you can perform the following:

- Connect Veeam Backup Enterprise Manager and Veeam Backup & Replication to a different database on the same or another server.
- Change authentication method for database connection. Possible options are Microsoft Windows authentication and database server authentication.

NOTE

The Configuration Database Connection Settings utility supports only connection to configuration databases of the current product version. For example, you can connect Veeam Backup Enterprise Manager 12 to a configuration database of version 12.

To manage connection settings for the Veeam Backup Enterprise Manager configuration database, take the following steps:

1. [Launch the utility.](#)
2. [Select a product.](#)
3. [Specify database connection settings.](#)
4. [Apply connection settings.](#)
5. [Finish working with the wizard.](#)

Step 1. Launch Utility

You can launch the Configuration Database Connection Settings utility from the **Start** menu by clicking **Configuration Database Connection Settings**.

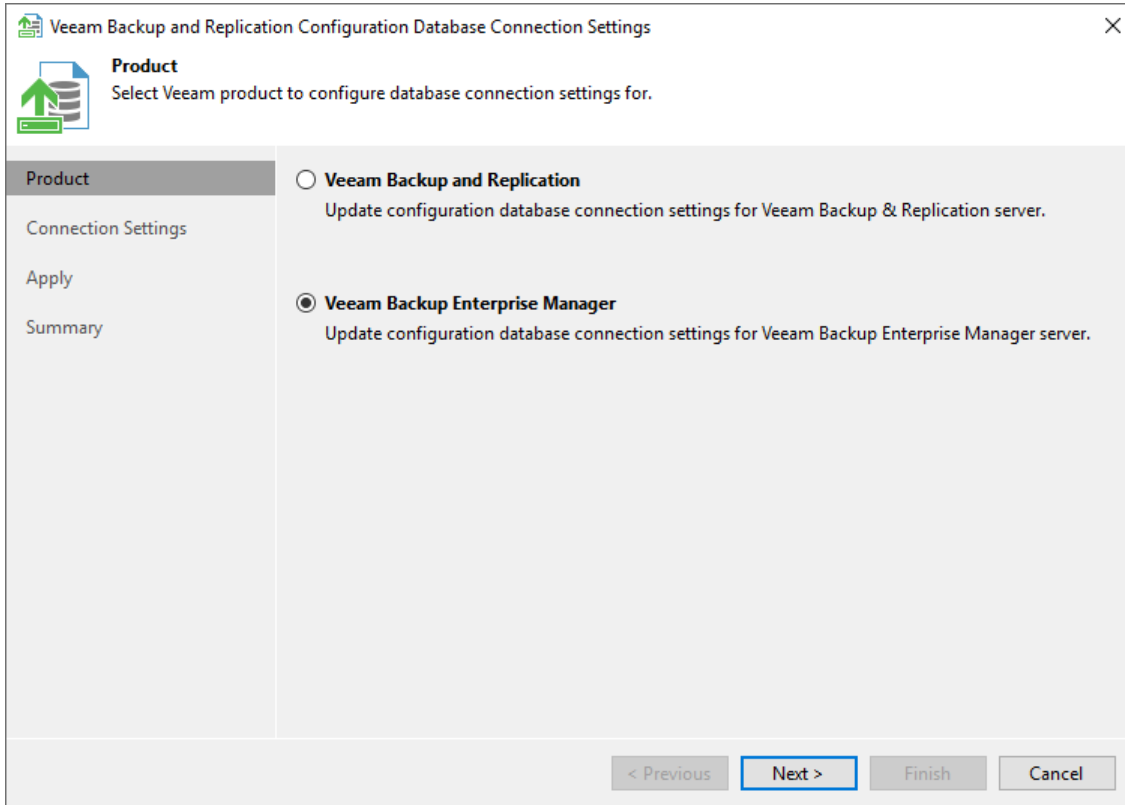
Alternatively, you can run the `Veeam.Backup.DBConfig.exe` file. By default, the path is the following:
`%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig`.

To run the utility, you must have administrative rights on the local machine, as long as the utility makes changes to the registry. If prompted at the launch, choose **Run as administrator**.

Step 2. Select Product

The **Product** step of the wizard is displayed if you have both a Veeam Backup Enterprise Manager server and backup server installed on the local machine. In this case, select a product whose configuration database settings you want to change.

If a backup server (or Enterprise Manager server) is not installed on the machine, the **Product** step of the wizard is skipped.



Step 3. Specify Connection Settings

At the **Connection Settings** step of the wizard, provide the connection settings for the configuration database.

1. Select one of the following database engines:
 - PostgreSQL
 - Microsoft SQL Server
2. Specify database settings:
 - [For PostgreSQL] Specify the instance name in the *HOSTNAME:PORT* format. In the **Database name** field, specify a name for the Veeam Backup Enterprise Manager configuration database.
 - [For Microsoft SQL Server] Specify the Microsoft SQL Server instance and database name to which you want the Veeam Backup & Replication installation to connect. Both local and remote Microsoft SQL Server instances are supported. Microsoft SQL Server instances available on the network are shown in the **Server name** list. If necessary, click **Refresh** to get the latest information.

If a database with the specified name does not exist on the selected Microsoft SQL Server instance, it will be created anew.
3. Select an authentication method that will be used for database connection:
 - If you plan to use the Microsoft Windows authentication, consider that the current service account will be used (that is, the account under which the Veeam Backup Enterprise Manager Service is running).
 - If you plan to use native database server authentication, provide a login name and password. To view the entered password, click and hold the eye icon on the right of the **Password** field.

[For Microsoft SQL Server] When you migrate the configuration database to another server, you must use the Microsoft SQL Server credentials that have CREATE ANY DATABASE permission on the target Microsoft SQL Server. For details, see [Microsoft Docs](#). After database creation, this account automatically gets a *db_owner* role and can perform all operations with the database. If the current account does not have this permission, a Database Administrator may create an empty database in advance and grant the *db_owner* role to the account that will be used for migration of the configuration database.

4. Click **Next**.

Veeam Backup and Replication Configuration Database Connection Settings

Connection Settings
Specify SQL server database connection settings.

Product

Connection Settings

Apply

Summary

Database engine

Database: PostgreSQL

Connection (HOSTNAME:PORT)

Instance name: localhost:5433

Database name: VeeamBackupReporting

Authentication

Windows authentication using credentials of service account

Native authentication using the following credentials:

Login name: TECH\sheila.d.cory

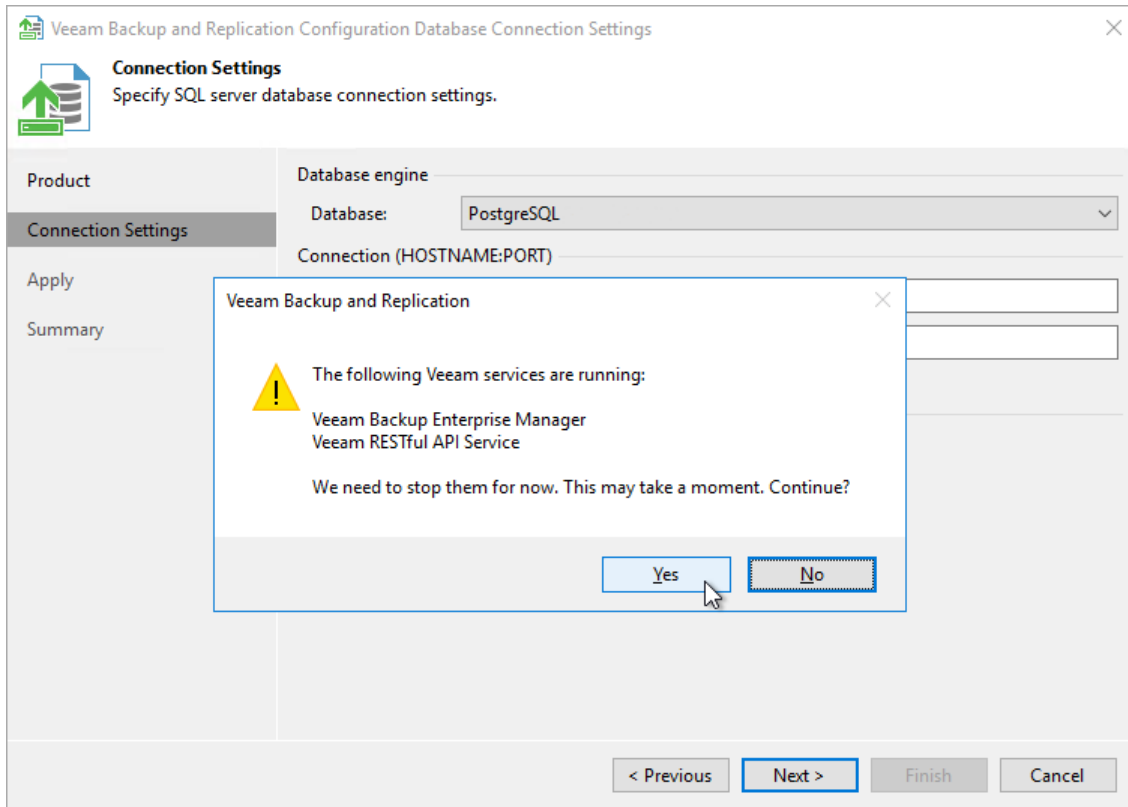
Password:

< Previous Next > Finish Cancel

5. Before proceeding, the utility validates the specified settings to make sure that the specified user account has enough privileges to access the database.

To ensure that the account (as well as the account under which the Veeam Backup Enterprise Manager Service is running) have sufficient privileges for database access, you can contact your database administrator. Refer to the list of [required permissions](#) for detailed information.

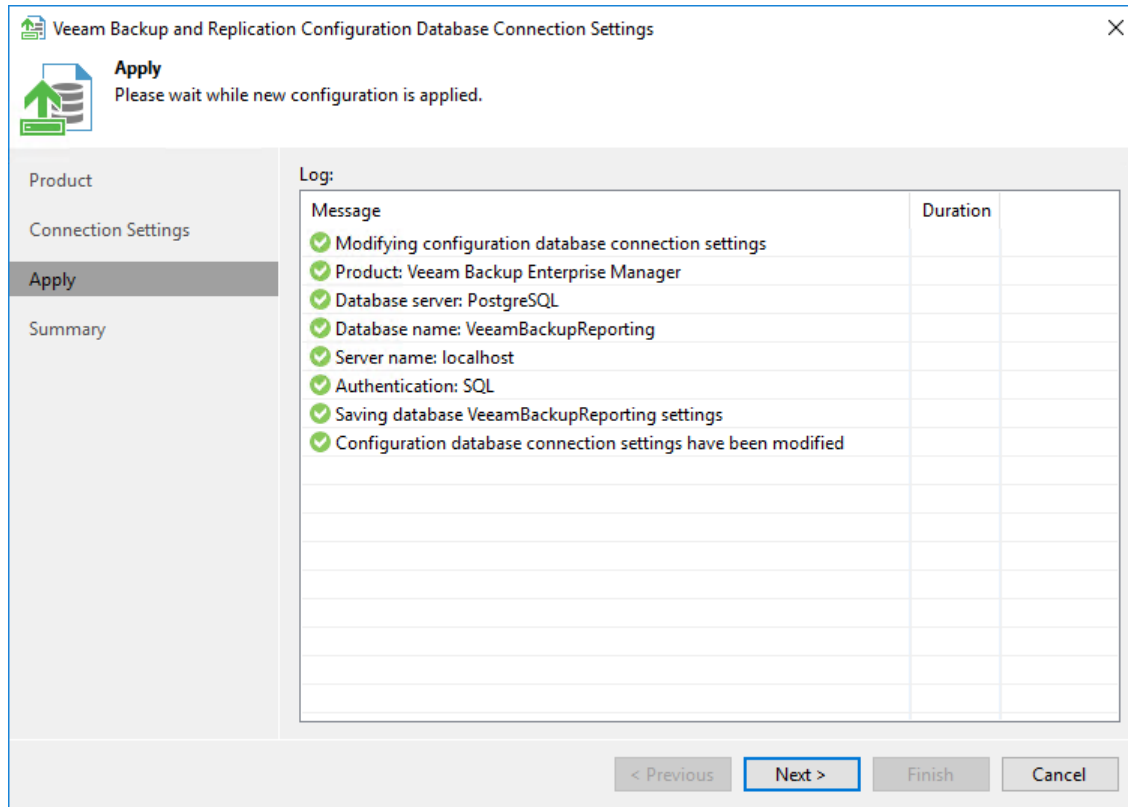
For the new settings to be applied, the utility needs to stop Veeam Backup Enterprise Manager services that are currently running. Before proceeding to the next step, you must confirm the operation by clicking **Yes**.



Step 4. Apply Connection Settings

At the **Apply** step of the wizard, the utility applies database connection settings. Wait for the operation to complete and click **Next** to proceed to the **Summary** step of the wizard.

Previously stopped services will be started again at this moment.



Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, view the information about the changes in database connection settings and click **Finish**.

NOTE

If you are configuring Veeam Backup & Replication database settings and you want the Veeam backup management console to start automatically after you finish working with the wizard, select the **Start the product automatically** check box. The option is not available for Veeam Backup Enterprise Manager.

