© 2020 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.
VIEWING AND SEARCHING FILE SHARE BACKUPS ................................................................. 154
BROWSING FILE SHARE BACKUPS ...................................................................................... 156
PERFORMING FILE RESTORE ............................................................................................... 158
  Restoring Files to Original Location ....................................................................... 159
  Downloading Files ...................................................................................................... 161
  Restoring Multiple Files ......................................................................................... 163
DELETING FILE SHARE BACKUPS ...................................................................................... 165

WORKING WITH MACHINES ................................................................................................. 166
VIEWING, SEARCHING, DELETING MACHINES ................................................................. 167
PERFORMING QUICK BACKUP ........................................................................................... 169
PERFORMING 1-CLICK RESTORE ....................................................................................... 170
PERFORMING VIRTUAL DISK RESTORE ............................................................................. 172
RUNNING FAILOVER PLANS ............................................................................................... 177

RESTORING GUEST OS FILES ............................................................................................... 179
PREPARING FOR FILE BROWSING AND SEARCHING ......................................................... 180
  Performing Catalog Replication and Indexing ................................................................. 181
  Preparing for Linux Guest Files Search and Restore ....................................................... 182
BROWSING MACHINE BACKUPS FOR GUEST OS FILES ................................................ 183
SEARCHING GUEST OS FILES IN MACHINE BACKUPS .................................................. 185
PERFORMING 1-CLICK FILE RESTORE ............................................................................... 187
  Restoring Files to Original Location ....................................................................... 188
  Downloading Files to Local Machine ..................................................................... 190
  Restoring Multiple Files ......................................................................................... 192
USING SELF-SERVICE FILE RESTORE PORTAL TO RESTORE MACHINE GUEST FILES .............................................................................................................................. 194

BACKUP AND RESTORE OF APPLICATION ITEMS ................................................................ 197
BACKUP AND RESTORE OF MICROSOFT EXCHANGE ITEMS ........................................... 198
  Preparing Application-Consistent Backup ................................................................. 199
  Providing Access Rights ....................................................................................... 201
  Restore Procedure ............................................................................................... 203
BACKUP AND RESTORE OF MICROSOFT SQL SERVER DATABASES ................................ 205
  Preparing Application-Consistent Backup ................................................................. 206
  Providing Access Rights ....................................................................................... 210
  Restore Procedure ............................................................................................... 211
BACKUP AND RESTORE OF ORACLE DATABASES ............................................................ 217
  Preparing Application-Consistent Backup ................................................................. 218
  Providing Access Rights ....................................................................................... 222
  Restore Procedure ............................................................................................... 223

MANAGING ENCRYPTION KEYS ........................................................................................... 230
GENERATING ENTERPRISE MANAGER KEYSET ................................................................. 231
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 at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

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

Online Support

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

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

This guide is intended for IT managers, virtual infrastructure administrators, and other personnel responsible for the product deployment and operation.

This document describes the features included in the Veeam Backup Enterprise Manager. It also provides usage examples and gives step-by-step instructions that will help you better understand how to install the Veeam Backup Enterprise Manager and monitor your Veeam Backup infrastructure, services and jobs.

Intended Audience

The document is intended for backup administrators and other IT professionals who plan to deploy and use Veeam Backup Enterprise Manager. This guide assumes that you have a good understanding of Veeam Backup & Replication and VMware vSphere.
About Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager (Enterprise Manager) is a management and reporting component that allows you to manage multiple Veeam Backup & Replication installations from a single web console. Veeam Backup Enterprise Manager helps you optimize performance in remote office/branch office (ROBO) and large-scale deployments and maintain a view of your entire virtual environment.

The distributed architecture of Veeam Backup & Replication allows you to create a custom backup infrastructure that meets your company needs. Veeam Backup Enterprise Manager manages backup and replication according to your administrative, business and security requirements and restrictions. With a number of Veeam Backup & Replication instances installed on different servers, Veeam Backup Enterprise Manager acts as a single management point. It allows you to control license distribution, manage backup jobs across the backup infrastructure, analyze operation statistics of Veeam backup servers, perform restore operations, and so on.

In particular, with Veeam Backup Enterprise Manager you can:

- Manage jobs across a number of Veeam backup servers.
- View on-going reporting data for all jobs running on these servers, set up email notifications to get information on the status of all jobs.
- Search for machines, file shares, and guest files in backups and replicas.
- Perform recovery operations for VMs and physical machines, including 1-Click restore, 1-click guest OS file restore and application items restore (for Microsoft Exchange mailboxes, Microsoft SQL Server databases and Oracle databases); perform 1-Click restore for file share backups.
- Centrally manage and update licenses to ensure compliance.
- Delegate permissions for restore operations to personnel in charge.
- Manage VMware vCloud Director organizations and support their administrators with the Veeam Self-Service Backup Portal.
- Manage vSphere user accounts and support them with the vSphere Self-Service Backup Portal.
- Install vSphere Web Client plug-in on vCenter servers.
- Implement data encryption and decryption processes for the Veeam solutions.
- Provide operation automation via Veeam Backup RESTful API.
What's New in Version 10

The following features and enhancements are supported in Veeam Backup Enterprise Manager 10:

- NAS backup. Veeam Backup Enterprise Manager displays file share backup jobs and backups created with these jobs. Users can monitor file share backup job performance, manage file share backup jobs and restore files from file share backups. For more information, see Working with File Shares.

- SAML authentication. Veeam Backup Enterprise Manager administrators can set up single sign-on for Veeam Backup Enterprise Manager users. To learn more, see SAML Authentication Support.

- VM disk restore. Users of Enterprise Manager web UI, Veeam Self-Service Backup Portal and vSphere Self-Service Backup Portal can restore disks of VMware vSphere VMs to the original location or a new location. To learn more, see Performing Virtual Disk Restore, Restoring vCloud Director VMs and vApps and Managing VMs.

- Starting from Veeam Backup & Replication 10, configurations with Veeam Backup Search on Microsoft Search Server are not supported.
How Veeam Backup Enterprise Manager Works

Veeam Backup Enterprise Manager aggregates data from multiple Veeam backup servers, as well as from the underlying VMware vCenter servers.

1. Veeam Backup Enterprise Manager retrieves data from the managed Veeam backup servers using a data collection job. This job gets information about the backup and replication jobs, processed machines, and other data from the Configuration databases used by Veeam backup servers.

2. Collected data is stored to the Veeam Backup Enterprise Manager database (hosted on SQL Server) and can be accessed by multiple users via the web interface. This web interface also allows for modifying Veeam 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 corresponding Veeam backup server and stored in its Configuration database.

If you have Veeam Agent for Microsoft Windows or Veeam Agent for Linux integrated with Veeam Backup & Replication, then 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 Restoring Guest OS Files.
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 Started with Veeam Backup Enterprise Manager.
  - **Veeam Self-Service File Restore Portal** allows administrators to restore files or folders from the guest OS of a virtual or physical machine. For more information on the Self-Service File Restore Portal, see Using Self-Service Portal to Restore Machine Guest Files.
  - **Veeam Self-Service Backup Portal** provides vCloud Director organization administrators with a UI for self-service operations on machine protection. For more information on the Self-Service Backup Portal, see Working with vCloud Director VMs via Self-Service Backup Portal.
  - **VMware vSphere Self-Service Backup Portal** provides Service Providers with a UI for managing access permissions and vSphere quotas for their customers. For more information on the vSphere Self-Service Backup Portal, see Working with vSphere Self-Service Backup Portal.

**NOTE:**


- **SQL Server database** is used to store configuration and performance data. For more information, see Deployment.

- **Veeam Backup Catalog** is used for guest OS file indexing, index data retention and its synchronization with the information on a Veeam backup server. It comprises a Windows service named Veeam Guest Catalog also installed on the Veeam Backup Enterprise Manager server. For more information, see Veeam Backup Catalog.

- **Veeam Backup Search** is an optional component used for guest OS file indexing of protected machines. This component is included in the installation package to provide backward compatibility with older existing deployments. For a new deployment, there is no need to install Veeam Backup Search, since all operations related to guest OS file indexing and search will be performed by Veeam's proprietary built-in indexing engine. For more information, see Veeam Backup Search Capabilities.
• **Veeam Cloud Connect Portal** is an optional component that comprises the Veeam Cloud Connect Portal website (IIS extension) and UI. It is intended for the tenants of Service Providers. For more information, see the [Veeam Cloud Connect Guide](#).

• **Veeam Backup Enterprise Manager RESTful 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 & Replication RESTful API Reference](#).

• **Veeam VMware vSphere Web Client plug-in** allows vSphere administrators to manage backup infrastructure of the virtual environment. For more information, see the [Controlling Backup Infrastructure with vSphere Web Client Plug-in](#).
Veeam Backup Catalog

Veeam Backup Catalog is a feature that stands for VM guest OS file indexing. Veeam Backup Catalog comprises Veeam Guest Catalog services that run on the following servers in the backup infrastructure: Veeam backup server and Veeam Backup Enterprise Manager server.

- Veeam Guest Catalog service on the Veeam backup server works as a local catalog service. It collects index data for backup jobs on this specific Veeam backup server and stores this data locally in the Veeam Backup Catalog folder.

- Veeam Guest Catalog service on Veeam Backup Enterprise Manager works as a federal catalog service. It communicates with Veeam Guest Catalog services on Veeam backup servers connected to Veeam Backup Enterprise Manager and performs the following tasks:
  - Replicates index data from Veeam backup servers to create a federal catalog
  - Maintains index data retention
  - Lets you search for machine guest OS files in backup files
Veeam Backup Search Capabilities

Veeam Backup Enterprise Manager allows you to browse the guest OS file system in a machine backup, search for guest OS files and restore necessary files. These operations are also supported for the backups of physical machines created by Veeam Agents (Server edition is needed).

**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 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 Guest Processing section of the Veeam Agent for Windows User Guide and the File System Indexing section of the Veeam Agent for Linux User Guide. For more information on the Veeam Agents guest file browsing and restore through Veeam Backup Enterprise Manager, see Guest File Browsing and 1-Click Restore section of this 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 and/or restore the necessary file(s) and finish the restore session, 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 and/or restore the necessary file(s) and finish the restore session, 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, and 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.

Consider that Veeam Backup & Replication supports file-level restore not only for machines included in guest catalog, but also for those that were not indexed — for example, if indexing was disabled at restore point creation time, or if indexing operation failed. For such a machine, its selected restore point will be mounted to:

- A corresponding Veeam backup server (the one that manages the job processing this machine) — for Windows machines.
- A Linux appliance — for Linux machines.

Then a user will be able to locate the necessary file(s) or folder(s) and perform restore operation. To learn more about mount operation, refer to the Veeam Backup & Replication User Guide and to the Search and Restore of Machine Guest Files section of this guide.
Indexing Data

Veeam Backup & Replication stores indexing data in the Veeam Backup Catalog folder. By default, the Veeam Backup Catalog is located in the `C:\VBRCatalog` folder on the Veeam backup server and on Veeam Backup Enterprise Manager.

Veeam Backup Catalog comprises the following data:

- Machine index
- Session index

Machine Index

Machine index reproduces the structure of files and folders on the machine guest OS. Veeam Backup & Replication uses the file index to search for guest OS files within machine backups.

For every machine whose file system has been indexed, there is a dedicated folder that contains indexing data for all restore points available for the machine.
Session Index

Veeam Backup Catalog keeps information for every backup job session. Session indexing data describes which machine restore points correspond with a specific backup job session and what sets of files are required to restore a machine to a specific point in time.

Session indexing files vary for incremental and reverse incremental backup chains:

- **For incremental backup chains**, a session indexing file contains information about only one restore point — the restore point that is created with this backup job session. Additionally, it contains information about a set of files that is required to restore a machine to this point in time. For example, if a backup chain contains 5 restore points, the 5th session indexing file will contain information about the 5th restore point and a group of 5 files that are required to restore the machine to this point in time.

```
BackupServer=BACKUP01
JobName=srv04
SessionDateUtc=05/13/2014 08:05:57.081

# OIBS
oib0.VmName=srv04
oib0.BackupTimeUtc=05/13/2014 08:02:04.988
oib0.OibUID=f81f790c-103e-4351-81a4-e4ec8a8c290c
oib0.Platform=EVmware
oib0.Group=grp0

# BACKUP FILE GROUPS
grp0.file0.Server=BACKUP01
grp0.file0.Path=c:\backup\srv04\srv042014-05-13T010101.vib
grp0.file0.ModifyDateUtc=05/13/2014 08:04:10.293
grp0.file1.Server=BACKUP01
grp0.file1.Path=c:\backup\srv04\srv042014-05-13T004536.vib
grp0.file1.ModifyDateUtc=05/13/2014 07:47:52.077
grp0.file2.Server=BACKUP01
grp0.file2.Path=c:\backup\srv04\srv042014-05-13T000053.vib
grp0.file2.ModifyDateUtc=05/13/2014 07:04:24.38
grp0.file3.Server=BACKUP01
grp0.file3.Path=c:\backup\srv04\srv042014-05-12T230102.vib
grp0.file3.ModifyDateUtc=05/13/2014 06:04:25.003
grp0.file4.Server=BACKUP01
grp0.file4.Path=c:\backup\srv04\srv042014-05-12T220051.vib
grp0.file4.ModifyDateUtc=05/13/2014 05:03:53.817
grp0.file5.Server=BACKUP01
grp0.file5.Path=c:\backup\srv04\srv042014-05-12T210105.vbk
grp0.file5.ModifyDateUtc=05/13/2014 04:07:55.047
```
For reverse incremental backup chains, a session indexing file contains information about all restore points engaged in the backup job session. In a reverse incremental chain, the last restore point is always a full backup. To produce a full backup and calculate incremental changes, Veeam Backup & Replication needs to address all points in the job. For this reason, the session indexing file refers not only to the restore point created with the backup job session, but also to all restore points preceding it. Additionally, a session indexing file describes groups of files that are required to restore a machine to all possible restore points. For every restore point, there is a separate group of files.

For example, if you have a reverse incremental chain of 3 restore points, the session indexing file for the last backup job session will contain information about 3 restore points and will describe three groups of files:

- Group 0 will list restore points that are required to restore the machine to the 1st, the earliest restore point.
- Group 1 will list restore points that are required to restore the machine to the 2nd restore point.
- Group 2 will list restore points that are required to restore the machine to the 3rd, the latest restore point.

```plaintext
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
```
A full backup file “moves forward” with every new backup job run, and Veeam Backup & Replication updates groups of files, correspondingly. 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 on 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:

\[ \text{Retention period} = \max (\text{Catalog Retention}, X) \]

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 backup jobs.

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:

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

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 jobs.

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 is 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 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 Enterprise Manager without the need to provide a password of the Enterprise Manager user account.

SAML authentication scenario in Veeam Backup Enterprise Manager comprises the following parties:

- Veeam Backup Enterprise Manager user.
- Service provider (SP) — an application accessed by the user. In the Veeam backup infrastructure, the service provider is Veeam Backup Enterprise Manager itself.
- Identity provider (IdP) — an external service (hosted on premises or in the public cloud) that facilitates single sign-on capabilities for Veeam Backup Enterprise Manager. 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 Veeam Backup Enterprise Manager web UI 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 was 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 was not previously logged in with the single sign-on service, the user specifies the password of their account on the single sign-on webpage.

5. The IdP issues a SAML assertion and redirects it to Veeam Backup Enterprise Manager in the SAML response. The SAML assertion must meet the following requirements:
   - Contain a User Principal Name (UPN) of the user in the <NameID> element of the SAML response.
   - Specify that the UPN type is Persistent.
6. The user gains access to Veeam Backup Enterprise Manager and can perform operations in Enterprise Manager 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 Specifying Service Provider Settings.

5. Create user accounts. To provide users of a single sign-on service with access to Enterprise Manager, the administrator must create for these users accounts of the External User or External Group type. For more information, see Managing Accounts and Roles.

On the IdP side, the IdP must configure trust relationship with Veeam Backup Enterprise Manager and configure rules that define what information to provide to the SP. Depending on the IdP, these rules may be configured in the form of claims, attribute statements and so on. For an example of how to perform this task in AD FS, see Appendix B. Configuring AD FS for SAML Authentication.
Planning and Preparation

Before you install Veeam Backup Enterprise Manager, you must check that the virtual environment and machines that you use as backup infrastructure components meet the product system requirements, required user rights and permissions, and the list of ports needed for communication between solution components, which are described below in this guide.
System Requirements

Make sure that servers that you plan to use as Veeam Backup Enterprise Manager infrastructure components meet system requirements listed below:

- Veeam Backup Enterprise Manager
- Veeam Cloud Connect Portal
- VMware vCloud Director

Veeam Backup Enterprise Manager

It is recommended to install the same product version on the Veeam Backup Enterprise Manager server and Veeam backup servers.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
</tbody>
</table>
|               | *CPU:* x64 processor  
|               | *Memory:* 4 GB RAM (minimum recommended).  
|               | *Hard disk space:* 2 GB on the system disk (required to extract all components from the setup package during the product installation).  
|               | *Network:* 1 Gbps recommended due to backup performance considerations.  |
| **OS**        |             |
|               | 64-bit versions of the following operating systems are supported:  
|               |  
|               | • Microsoft Windows Server 2019  
|               | • Microsoft Windows Server 2016  
|               | • Microsoft Windows Server Semi-Annual Channel (including version 1909)  
|               | • Microsoft Windows Server 2012 R2  
|               | • Microsoft Windows Server 2012  
|               | • Microsoft Windows 2008 R2 SP1  
|               | • Microsoft Windows 10 (starting from version 1607 up to version 1909)  
|               | • Microsoft Windows 8.1  
|               | • Microsoft Windows 7 SP1  |
| **SQL Server**|             |
|               | Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported):  
|               |  
|               | • Microsoft SQL Server 2019  
|               | • Microsoft SQL Server 2017  
|               | • Microsoft SQL Server 2016 (Microsoft SQL Server 2016 SP1 Express Edition is included in the setup)*  
|               | • Microsoft SQL Server 2014 with Microsoft SQL Server 2014 Management Objects and Microsoft System CLR for SQL Server 2014  
|               | • Microsoft SQL Server 2012 (Microsoft SQL Server 2012 SP4 Express Edition is included in the setup)**  
|               | • Microsoft SQL Server 2008 R2  
|               | • Microsoft SQL Server 2008  

* SQL Server 2016 SP1 Express Edition is included in the setup  
** SQL Server 2012 SP4 Express Edition is included in the setup
Notes:

- SQL Server 2008 databases and later with compatibility to SQL Server 2005 are not supported.
- Veeam Backup Enterprise Manager configuration database can be deployed in Microsoft SQL AlwaysOn Availability Groups. For more information, see this Veeam Knowledge Base article.

Other software

- Microsoft .NET Framework 4.7.2 (included in the setup).
- Microsoft Internet Information Services 7.5 or later: support for extensionless URLs for IIS 7.5 or later, ASP.NET 4.5, .NET Extensibility 4.5 for IIS 8.0.
- For IIS 8.5, the URL rewrite module is required if you plan to use Veeam Self-Service Backup Portal for vCloud Director or VMware vSphere Self-Service Backup Portal.

Browsers: Microsoft Internet Explorer 11.0 or later, Microsoft Edge, latest versions of Mozilla Firefox and Google Chrome are supported. The browser must have JavaScript and WebSocket protocol enabled.

Microsoft Excel 2007 or later is required to view report data exported from Veeam Backup Enterprise Manager.

* For machines running Microsoft Windows Server 2012 or later.
** For machines running Microsoft Windows 7 or Microsoft Windows Server 2008 R2.

**IMPORTANT**!

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

Veeam Cloud Connect Portal

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and software</td>
<td>Refer to hardware system requirements and software system requirements for Veeam Backup Enterprise Manager.</td>
</tr>
<tr>
<td>Supported browsers</td>
<td>For PC:</td>
</tr>
</tbody>
</table>

- Microsoft Internet Explorer 11.0 or later
- Microsoft Edge
- Latest versions of Mozilla Firefox and Google Chrome

For portable devices (tablets) latest versions of Apple Safari for iOS or Google Chrome for Android.
## VMware vCloud Director (Optional)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMware vCloud Director</strong></td>
<td>Supported versions are 8.x up to 9.7.</td>
</tr>
<tr>
<td><strong>Other software</strong></td>
<td>If your Enterprise Manager deployment uses IIS 8.5, then URL rewrite module is required to work with Veeam Self-Service Backup Portal for vCloud Director.</td>
</tr>
</tbody>
</table>
# Required Permissions

This section provides information on the account permissions required for installing/upgrading and using Veeam Backup Enterprise Manager and its components.

## Veeam Backup Enterprise Manager

<table>
<thead>
<tr>
<th>Account</th>
<th>Required Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account used to run the setup</strong></td>
<td>The account used for product installation must have the <em>local Administrator</em> permissions on the target machine.</td>
</tr>
<tr>
<td></td>
<td>To create a new Veeam Backup Enterprise Manager database during the setup process, the account must have the CREATE ANY DATABASE permission on the SQL Server level. After the database is created, this account automatically gets a <em>db_owner</em> role and can perform all operations with the database.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If a database is created in advance (by a database administrator or SQL Server administrator), the setup account must have the <em>db_owner</em> role for the database.</td>
</tr>
<tr>
<td></td>
<td>To upgrade an existing Enterprise Manager database, the account must have the <em>db_owner</em> role.</td>
</tr>
<tr>
<td><strong>Veeam Backup Enterprise Manager service account</strong></td>
<td>It is recommended to use the <em>Local System</em> 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:</td>
</tr>
<tr>
<td></td>
<td>• <em>Local Administrator</em> permissions on the Veeam Backup Enterprise Manager server.</td>
</tr>
<tr>
<td></td>
<td>• <em>Log on as service</em> right (granted automatically to the Veeam Backup Enterprise Manager Service account).</td>
</tr>
<tr>
<td></td>
<td>• <em>Db_datareader</em> and <em>db_datawriter</em> roles, as well as permissions to execute stored procedures for the Enterprise Manager database on the Microsoft SQL Server. Alternatively, you can assign this account the <em>db_owner</em> role for the Enterprise Manager database.</td>
</tr>
<tr>
<td></td>
<td>• <em>Full Control</em> NTFS permissions for the <em>VBRCatalog</em> or another folder where index files are stored.</td>
</tr>
<tr>
<td></td>
<td>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 &quot;Cannot find user account DOMAIN\username&quot; error.</td>
</tr>
<tr>
<td><strong>Enterprise Manager user</strong></td>
<td>To be able to work with the Veeam Backup Enterprise Manager web UI, users must be assigned the <em>Portal Administrator</em>, <em>Portal User</em> or <em>Restore Operator</em> role. For more information, see Configuring Security Settings.</td>
</tr>
</tbody>
</table>
| **vSphere Web Client Plug-in for Veeam Backup & Replication (optional)** | The account used to install the plug-in and the vCenter server account must belong to the same Active Directory domain in case of cross-domain access. The account used to install the plug-in must be assigned the following vCenter Server permissions:

- To install the plug-in — Extension > Register extension
- To uninstall the plug-in — Extension > Unregister extension |
| **vSphere Self-Service Backup Portal user** | The account used to work with vSphere Self-Service Backup Portal must have interactive logon permissions on the Enterprise Manager server. |
Used Ports

This section covers typical connection settings for Veeam Backup Enterprise Manager, including:

- **Enterprise Manager Operation Ports**
- **Ports for Restore Operations**

**NOTE:**
For more information on ports specific for Veeam Backup & Replication infrastructure components, see the Used Ports section of the Veeam Backup & Replication User Guide.

Veeam Backup Enterprise Manager Connections

The following ports must be opened to ensure proper operation of Veeam Backup Enterprise Manager and communication between components:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Enterprise Manager</td>
<td>Veeam backup server</td>
<td>TCP</td>
<td>9392</td>
<td>Default port used by Veeam Backup Enterprise Manager for collecting data from Veeam backup servers. Can be customized during Veeam Backup &amp; Replication installation. For more information, see Specify Service Ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9393</td>
<td>Default port used by the Veeam Guest Catalog service for catalog replication. Can be customized during Veeam Backup &amp; Replication installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2500 to 2600</td>
<td>Ports used by the Veeam Guest Catalog service for replicating catalog data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>135</td>
<td>Default RPC port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>49152 to 65535 (for Microsoft Windows 2008 and later)</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article.</td>
</tr>
<tr>
<td>SQL Server hosting the Enterprise Manager configuration database</td>
<td></td>
<td>TCP</td>
<td>1433</td>
<td>Default port used for communication with Microsoft SQL Server hosting a Veeam Backup Enterprise Manager database. For more information, see Specify Installation Settings. Additional ports may be needed depending on your configuration. For more information, see the Microsoft SQL Docs Configure the Windows Firewall to Allow SQL Server Access article.</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port(s)</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>vCenter Server</td>
<td>TCP</td>
<td>443</td>
<td>Default port used for connection to a vCenter Server and deploying the Veeam Plug-in for vSphere web client. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.</td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain Controller</td>
<td>TCP, UDP</td>
<td>389</td>
<td>Port used by Enterprise Manager service to communicate with Active Directory over the LDAP protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>636</td>
<td>Port used by Enterprise Manager service to communicate with Active Directory over the LDAPS (LDAP over TLS/SSL) protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3268</td>
<td>Port used by Enterprise Manager service to communicate with LDAP Global Catalog.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3269</td>
<td>Port used by Enterprise Manager service to communicate with LDAP Global Catalog over TLS/SSL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>49152 to 65535</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>9394</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Veeam Backup Enterprise Manager website (IIS extension)</td>
<td>TCP</td>
<td>9397</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Veeam Cloud Connect Portal website (IIS extension)</td>
<td>TCP</td>
<td>9399</td>
<td>Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.</td>
<td></td>
</tr>
<tr>
<td>Browser</td>
<td>HTTP</td>
<td>9080</td>
<td>Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td>9443</td>
<td>Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td>6443</td>
<td>Default ports used to communicate with the website. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.</td>
<td></td>
</tr>
</tbody>
</table>
### Veeam Backup Enterprise Manager RESTful API client and VMware vSphere web client plug-in

| Veeam Backup Enterprise Manager | Veeam Backup Enterprise Manager Restful API | HTTPS | 9398 | Default ports used to communicate with Veeam Backup Enterprise Manager Restful API. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports. |

| Veeam ONE Server (optional) | Veeam Backup Enterprise Manager | TCP | Dynamically assigned ports | If you use Veeam Availability Suite and add a Veeam Backup Enterprise Manager server to Veeam ONE monitoring scope, you must open ports required to gather data through WMI. For more information on enabling and disabling WMI traffic, see Microsoft Windows Dev Cener Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection articles. |

---

**NOTE:**

Consider the following:

- During installation, Veeam Backup & Replication automatically creates firewall rules for default ports to allow communication for the application components.
- For more information on Enterprise Manager network connectivity, refer to the Enterprise Manager article of the Veeam Backup and Replication Best Practices documentation.

### Ports for Restore Operations

#### Guest OS File Restore (Windows)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Enterprise Manager</td>
<td>Veeam backup server</td>
<td>TCP</td>
<td>2500 to 6000</td>
<td>Ports used for file download.</td>
</tr>
</tbody>
</table>

#### Guest OS File Restore (Linux)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Enterprise Manager</td>
<td>Linux helper appliance</td>
<td>TCP</td>
<td>2500 to 6000</td>
<td>Ports used for file download. For more information on the helper appliance, see Preparing for Linux Guest Files Search and Restore.</td>
</tr>
</tbody>
</table>
**NOTE:**

Consider the following:

- For more information on the list of ports used by the mount server associated with the backup repository during file-level restore, see the Mount Server Connections section of the Veeam Backup & Replication User Guide.
- For more information on the list of ports used by the components involved in 1-Click Restore to Original Location, see the Used Ports section of the Veeam Backup & Replication User Guide.

### SQL Server Database Restore

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target remote SQL Server</td>
<td>Mount server associated with backup repository</td>
<td>TCP</td>
<td>3260 to 3270</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Oracle Database Restore (1-Click)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target remote machine to which application items are restored</td>
<td>Machine running mount service*</td>
<td>TCP</td>
<td>3260 to 3270</td>
<td>Range of ports used by Veeam Backup and Replication for iSCSI traffic. Ports are open only during the application item restore session.</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine running mount service*</td>
<td>Oracle on Windows server</td>
<td>TCP</td>
<td>49152 to 65535</td>
<td>Recommended dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see Microsoft Support KB 832017.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>1025 to 1034</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>22</td>
<td>Default SSH port used as a control channel.</td>
</tr>
<tr>
<td>Oracle on Linux server</td>
<td>TCP</td>
<td>2500 to 5000</td>
<td>Default port range for data transmission.</td>
<td></td>
</tr>
</tbody>
</table>

* The mount server associated with the repository (if restoring from backup), or the Veeam backup server (if restoring from replica).

**NOTE:**

For more information on the process of database restore with custom settings, see [Restore with Custom Settings](#).
Licensing

The Veeam Backup & Replication infrastructure requires license instances to process backup and replication jobs.

When you run a job, Veeam Backup & Replication uses an amount 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 amount of instances in the license. When Veeam Enterprise Manager replicates databases from backup servers, it also synchronizes license data (that is, 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.
Viewing and Changing Current License

To work with licenses for Veeam Backup & Replication servers added to Veeam Backup Enterprise Manager:

1. Log on to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. Open the Configuration view.
3. Open the Licensing section on the left of the Configuration view.

The Summary view of the Licensing section displays information about the license edition, license state and a spreadsheet of the available and used instances per each type of protected workloads: virtual machines, physical servers and workstations, cloud machines, applications and file shares.

Each type of workloads processed by Veeam Backup & Replication consumes a specific number of instances in the license. For more information on Veeam licensing, see Veeam Licensing Policy.

TIP:

You can configure Veeam Backup Enterprise Manager to send notifications if your license expires. For more information on the Veeam Backup Enterprise Manager notification functionality, see the Configuring Notification Settings section of this guide.

NOTE:

Veeam Backup Enterprise Manager does not display information about instances consumed in the Veeam Cloud Connect service provider license by tenant workloads. This information is available only in the Veeam backup console on the Veeam backup server of the service provider. For more information, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.
To display detailed information about the current license, including license type, expiration date and the number of instances, click the **Details** link.

**TIP:**

You can also view detailed information about current license usage. To do this, click the **Report** link.

<table>
<thead>
<tr>
<th>License Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Valid</td>
</tr>
<tr>
<td>Type</td>
<td>Subscription</td>
</tr>
<tr>
<td>Edition</td>
<td>Enterprise Plus Edition</td>
</tr>
<tr>
<td>Support ID</td>
<td>00276360</td>
</tr>
<tr>
<td>Licensed to</td>
<td>Veeam Software AG</td>
</tr>
<tr>
<td>Package</td>
<td>Backup</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instances</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td>100</td>
</tr>
<tr>
<td>Expiration date</td>
<td>6/1/2020</td>
</tr>
</tbody>
</table>

[Update license key automatically]

[Update now]

[Save] [Cancel]
Installing License

To install a license:

1. In the Summary view, click Install license.
2. Select the necessary .LIC file and click Open.

The new license will be applied to all connected Veeam backup servers automatically.

Updating License

To update your license (ad-hoc update):

1. In the Summary view, click Details.
2. Click the Update now link.

Veeam will connect to the web license management portal to obtain a new key (data will be communicated securely using HTTPS).
You can instruct Veeam Backup Enterprise Manager to schedule automatic connection with Veeam licensing server and periodically send requests for a new license. For that, on the Details window, select the Update license key automatically check box. With this setting enabled, Veeam will start requesting a new license weekly, and 7 days before current license expiration date — daily.

**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.

Veeam also supports a grace period after the license expiration date. For subscription license, it lasts for 30 days, for rental license — 2 months. During this period the product will be running, but a warning about license expiration (grace period) will appear in the main window and in the sessions information.

You must update your license before the end of the grace period.

For more information on Veeam licensing, see the Veeam licensing article on the Frequently Asked Questions website.

Messages that can appear in the automatic license update session log are listed in the Appendix A. (Similar messages are received as pop-ups after you force the immediate update.)
Revoking License

You can use Enterprise Manager to revoke instances from machines — that is, reclaim the instance used for a machine to apply it to another machine.

To revoke licenses:

1. Log on to Veeam Backup Enterprise Manager using an account with the **Portal Administrator** role.
2. Open the **Configuration** view.
3. Open the **Licensing** section on the left of the **Configuration** view.
4. Click the **Instances** tab.
5. Select the required machine or file share in the list and click **Revoke**.

![Image of the Configuration view showing the Instances section with a list of machines and file shares, including their names, hosts, and licenses.](image-url)
Managing License Usage Reports

Veeam Cloud & Service Providers (VCSPs) who have a rental license installed in Veeam Backup Enterprise Manager must periodically submit a license usage report from Enterprise Manager. This process happens monthly, starting from the first day of the month. Veeam offers two methods of license usage reporting: automatic reporting and manual reporting. 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 license usage report on the first day of the month. The report is based on the current number of used instances. You can perform the following actions with the license usage report:

- [For automatic reporting] Submit the license usage report to Veeam
- Review the license usage report
- [For manual reporting] Save the license usage report
- Adjust the number of processed VMs in the report
- Postpone the review of the report
Submitting License Usage Report

On the first day of the month, when you access Veeam Backup Enterprise Manager UI, Veeam Backup Enterprise Manager displays a notification informing that you must submit a license usage report. In case of automatic license usage reporting, you can submit the report immediately without review.

To submit the report:

1. In the monthly usage report notification, click the submit link.
2. In the Monthly Usage Report window, check the number of managed instances for the previous month and click Send.

NOTE:

Submission of the license usage report from the Veeam Backup Enterprise Manager UI is not available for manual reporting. You must download the report and then send it to Veeam. For more information, see Saving License Usage Report.
Reviewing License Usage Report

You can review a license 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.

In case of automatic license usage reporting, you can submit the report immediately after review. To submit the report, click Send.

If you want to change the number of reported instances, you can adjust the report. To learn more, see Adjusting License Usage Report.

You can save the report to the specified folder. To do this, click Download and select the format in which to save the report: PDF or JSON.
TIP:

In case of manual license usage reporting, you can also save the report without review, directly from the Monthly Usage Report window. For more information, see Saving License Usage Report.
Saving License Usage Report

If you perform manual license usage reporting, you must save the license usage report after review for future submission. You can choose to save the report to a file in the PDF format or JSON format.

To save a license usage report:

1. In the monthly usage report notification, click the submit link.

2. In the Monthly Usage Report window, click Download and select the format in which to save the report: PDF or JSON.

**TIP:**

In case of automatic license usage reporting, you can save the report as part of the review process. For more information, see Reviewing License Usage Report.
Adjusting License Usage Report

You can remove specific managed VMs from a license 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. In the monthly usage report, 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.
Postponing License Usage Report Review

You can postpone the license usage report review. When you postpone the report review, Veeam Backup Enterprise Manager will close the Monthly Usage Report window. Veeam Backup Enterprise Manager will display the notification about the need to submit the report every time you open the Veeam Backup Enterprise Manager UI until the report is sent to Veeam.

For automatic license usage reporting, if you do not send the report to Veeam within 10 days, Veeam Backup & Replication will send the report automatically on the eleventh day of the month. If you perform manual reporting, 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 postpone the report review:

1. In the monthly usage report notification, click the submit link.
2. In the Monthly Usage Report window, click Postpone.
Deployment

To start working with Veeam Backup Enterprise Manager, you must install Veeam Backup Enterprise Manager components on a machine that meets the system requirements. To do this, you can use the setup wizard or install the product in the unattended mode.

You can install Veeam Backup Enterprise Manager either on a physical or virtual machine, co-install it with Veeam Backup & Replication or install it separately.
Installing Veeam Backup Enterprise Manager

Before you install Veeam Backup Enterprise Manager, check prerequisites. Then use the Veeam Backup Enterprise Manager setup wizard to install the product.

1. Start the setup wizard.
2. Read and accept the license agreement.
3. Provide a license file.
4. Review components and select an installation folder.
5. Install missing software.
7. Specify service account settings.
8. Select Microsoft SQL Server.
9. Specify service ports.
10. Specify data locations.

For more information on Veeam Backup Enterprise Manager installation in unattended mode, see Veeam Backup Enterprise Manager Server subsection of the Installing Veeam Backup & Replication in Unattended Mode section of the Veeam Backup & Replication User Guide.
Before You Begin

Before you install Veeam Backup Enterprise Manager, check the following prerequisites:

- A machine on which you plan to install Veeam Backup Enterprise Manager must meet the system requirements. For more information, see System Requirements.
- A user account that you plan to use for installation must have sufficient permissions. For more information, see Required Permissions.
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see Used Ports.
- .NET 3.5.1 WCF HTTP Activation Windows component prevents Veeam Backup Enterprise Manager from functioning. Make sure there is no .NET 3.5.1 WCF HTTP Activation Windows component on the Veeam Backup Enterprise Manager server prior to the installation.
- Local antivirus or antimalware software can interfere with Veeam Backup Enterprise Manager installation and upgrade. If you receive the "Failed to create website 0x80070020" message, disable your local antivirus or antimalware software and run the installation process again. You can re-enable your antivirus software once the installation process completes. For more information, see this Veeam KB article.
- Check the Known Issues section of the Veeam Backup & Replication 10 Release Notes.

Step 1. Start Setup Wizard

To start the setup wizard:

2. Use disk image emulation software to mount the installation image to the machine where you plan to install Veeam Backup Enterprise Manager or burn the image file to a blank CD/DVD. If you plan to install Veeam Backup Enterprise Manager on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM. To extract the content of the ISO, you can also use the latest versions of utilities that can properly extract data from ISOs of large size and can properly work with long file paths.
3. After you mount the image or insert the disk, Autorun will open a splash screen with installation options. If Autorun is not available or disabled, run the Setup.exe file from the image or disk.
4. In the Standalone components section of the splash screen, click Install Veeam Backup Enterprise Manager.
5. Before installing the product, the setup will analyze the prerequisites and prompt to install .NET Framework if it is missing on the machine. Click OK to install this component. After you install the component, you will have to reboot your computer.
IMPORTANT!

It is strongly recommended that you install Veeam Backup Enterprise Manager using Autorun or the Setup.exe file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup Enterprise Manager may not work as expected.
Step 2. Read and Accept License Agreement

At the License Agreement step of the wizard, you must accept the license agreement for Veeam and 3rd party components that Veeam incorporates. If you do not accept the license agreements, you will not be able to pass to next step of the setup wizard.

1. Read the license agreement. To view the license agreement for 3rd party components, click View.

2. Select the I accept the terms of the Veeam license agreement check box.

3. Select the I accept the terms of the 3rd party components license agreements check box.
Step 3. Provide License File

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

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

If a valid license is already installed on the machine, the setup wizard will inform you about it. In this case, you can skip the **Provide License** step and move to the next step of the wizard.

To install a license:

1. Next to the **License file for Veeam Backup Enterprise Manager** field, click **Browse**.
2. Select a valid license file for Veeam Backup Enterprise Manager.
Step 4. Review Components and Select Installation Folder

At the Program features step of the wizard, you can select what Enterprise Manager components to install on the machine and specify the installation folder.

Selecting Components

For on-site deployments, the setup wizard offers the following components:

- Veeam Backup Enterprise Manager
- Veeam Backup Catalog

Service providers can also install Veeam Cloud Connect Portal. For more information on Veeam Cloud Connect Portal, see the Veeam Cloud Connect Guide.

To choose components to install:

1. Click the hard drive icon next to a component.
2. Select the This feature will be installed on local hard drive option.

If the Veeam Backup Catalog or Cloud Connect Portal for Service Providers component is already installed, the setup will exclude it from the list of components to install.

The setup wizard also installs components in the background. For more information on the installed components, see Enterprise Manager Components.

Selecting Installation Folder

To choose the installation folder:

1. On the right of the Install to field, click Browse.
2. In the Browse for Folder window, select the installation folder for the product. The default installation folder is %ProgramFiles%\Veeam\Backup and Replication.

![Veeam Backup Enterprise Manager Setup](image)
Step 5. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup wizard checks if all prerequisite software is installed on the machine. If required software components are missing, the setup wizard will offer you to install them.

You can install missing components automatically or manually.

- To install missing components automatically, click **Install**. The setup wizard will not interrupt the installation process and install the missing components during the current work session.

- To install missing components manually:
  - a. Click **Cancel** and exit the setup wizard.
  - b. Install and enable the necessary components manually on the machine.
  - c. Start the setup wizard again, pass to the **System Configuration Check** step of the wizard and click **Re-run** to repeat the verification.

**NOTE:**

If all required components are already installed on the machine, the **System Configuration Check** step will be skipped. For more information on the necessary software, see **System Requirements**.
Step 6. Specify Installation Settings

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

By default, the setup wizard installs Veeam Backup Enterprise Manager with the following settings:

- **Installation folder**: C:\Program Files\Veeam\Backup and Replication.

- **Guest catalog folder**: the VBRCatalog folder on a volume with the maximum amount of free space, for example, C:\VBRCatalog.
  
The guest catalog folder stores indexing data for VM guest OS files. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore.

- **Catalog service port**: 9393. The catalog service port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager.

- **Service account**: LOCAL SYSTEM. The service account is the account under which the Veeam Backup Enterprise Manager runs.

- **Service port**: 9394. The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers.

- **SQL Server**: LOCALHOST\VEEAMSQL2012 or LOCALHOST\VEEAMSQL2016. During installation, the Veeam Backup Enterprise Manager setup installs a new instance of Microsoft SQL Server locally on the backup server:
  
  - For machines running Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup installs Microsoft SQL Server 2012 SP3 Express Edition.
  
  - For machines running Microsoft Windows Server 2012 and later, the setup installs Microsoft SQL Server 2016 SP2 Express Edition.

- **Database name**: VeeamBackupReporting. Veeam Backup Enterprise Manager deploys the Veeam Backup Enterprise Manager configuration database on the locally installed instance of Microsoft SQL Server.

- **Web UI ports**: 9080 (for HTTP protocol) and 9443 (for HTTPS protocol). These ports are used for accessing Veeam Backup Enterprise Manager web interface.

- **RESTful API ports**: 9399 (for HTTP protocol) and 9398 (for HTTPS protocol). These ports are used for accessing Veeam Backup Enterprise Manager RESTful API.

- **Cloud Connect Portal port**: 6443. This port is used for accessing Veeam Cloud Connect Portal by tenants.
To use default installation settings:

1. Leave the **Let me specify different settings** check box not selected.
2. Click **Install**. The installation process will begin.

To use custom installation settings, select the **Let me specify different settings** check box. The setup wizard will include additional steps that will let you configure installation settings.
Step 7. Specify Service Account Settings

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

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

- LOCAL SYSTEM account (recommended, used by default)
- Another user account

The user name of the custom account must be specified in the `DOMAIN\USERNAME` format.

**NOTE:**

The user account must have **Veeam Backup Enterprise Manager service account** permissions to run the Veeam Backup Enterprise Manager Service. For more information, see Required Permissions.
Step 8. Select Microsoft SQL Server

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

You can select a Microsoft SQL Server on which you want to deploy the configuration database, and choose the authentication mode.

1. Select a Microsoft SQL Server:
   - If a Microsoft SQL Server is not installed locally or remotely, select the **Install new instance of SQL Server** option. The setup will install Microsoft SQL Server locally on the backup server:
     - For machines running Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup will install Microsoft SQL Server 2012 SP3 Express Edition.
     - For machines running Microsoft Windows Server 2012 and later, the setup will install Microsoft SQL Server 2016 SP2 Express Edition.
   - If a Microsoft SQL Server is already installed locally or remotely, select the **Use existing instance of SQL Server** option. Enter the instance name in the \HOSTNAME\INSTANCE format. In the Database field, specify a name for the Veeam Backup Enterprise Manager configuration database.

2. Select an authentication mode to connect to the Microsoft SQL Server instance: Microsoft Windows authentication or Microsoft SQL Server authentication. If you select the SQL Server authentication, enter credentials for the Microsoft SQL Server account.

If the configuration database already exists on the Microsoft SQL Server (for example, it was created by a previous installation of Veeam Backup Enterprise Manager), the setup wizard will notify about it. To connect to the detected database, click **Yes**. If necessary, Veeam Backup Enterprise Manager will automatically upgrade the database to the latest version.
Step 9. Specify Service Ports

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

You can customize port number values that will be used for communication between backup infrastructure components.

**NOTE:**

For more information about Veeam Backup Enterprise Manager used ports, see [Used Ports](#).

Provide HTTP and HTTPS port numbers and select the certificate to be used by Veeam Backup Enterprise Manager. This certificate is needed to establish secure communication with the Enterprise Manager website using HTTPS (default port **9443**); Veeam plug-in for vSphere Web Client and RestAPI client also will use this certificate to receive data using HTTPS protocol.

If the setup wizard does not find an appropriate certificate to be used, it will generate a self-signed certificate.

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

To enable TLS 1.2 secure connection protocol for the network connections, select the **High security mode** check box.

**NOTE:**

This mode enforces TLS 1.2 protocol and disables weak ciphers setup option using system-wide settings, and thus may be not compatible to other 3rd party software running on the same server.

If you are installing Veeam Cloud Connect Portal, you can also provide port number that will be used by browser to access its website (default port is **6443**).
Step 10. Specify File Locations

The **File Locations** step is available if you have selected to install Veeam Backup Catalog at the **Program features** step of the wizard and to configure installation settings manually at the **Default Configuration** step of the wizard.

You can specify location for the guest file system catalog folder. Specify a path to the folder where index files must be stored.

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

![File Locations Dialog Box](image)
Step 11. Begin Installation

The **Ready to Install** step of the wizard is available if you have selected to configure installation settings manually. You can review the Veeam Backup Enterprise Manager installation settings and start the installation process:

1. Click **Install** to begin the installation.
2. Wait for the installation process to complete and click **Finish** to exit the setup wizard.
Maintaining Veeam Backup Enterprise Manager

You can repair your installation of Veeam Backup Enterprise Manager. For that:

1. Start the setup wizard on the Veeam Backup Enterprise Manager server. For more information, see Start Setup Wizard.

2. Read and accept the License Agreement. For more information, see Read and Accept License Agreement.

3. At the Maintenance Mode step of the setup wizard, select the Repair option and click Next.

4. Specify the service account credentials that will be used during the Veeam Backup Enterprise Manager repair. For more information, see Specify Service Account Settings.

5. At the Ready to Install step of the Setup Wizard check the installation prerequisites and click Install.

The setup wizard will re-install the Veeam Backup Enterprise Manager components. Wait for the installation process to complete and click Finish to exit the setup wizard.
Upgrading Veeam Backup Enterprise Manager

Before You Start Upgrade

Upgrade of Veeam Backup Enterprise Manager to version 10 is supported for version 9.5 Update 3 and later. To upgrade from earlier versions, contact Veeam Customer Support.

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

1. With Veeam Backup Enterprise Manager and managed Veeam backup servers connected to it, remember to begin the backup infrastructure upgrade process with Veeam Backup Enterprise Manager. Veeam backup servers should be upgraded after that. If you have Veeam backup server installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server.

2. It is recommended to disable local antivirus and antimalware software to prevent it from interfering with Veeam Backup Enterprise Manager setup. You can enable it after the upgrade procedure is completed. For more information, see this Veeam KB article.

3. Ensure there is no active processes, such as any running jobs and restore sessions. We recommend that you do not stop running jobs, and let them complete successfully instead. Disable any periodic and backup copy jobs, so that they do not start during upgrade.

4. Perform backup of the SQL Server configuration databases used by Veeam backup servers and Veeam Backup Enterprise Manager server, so that you can easily go back to a previous version in case of issues with upgrade. Note that built-in configuration backup functionality does not protect Veeam Backup Enterprise Manager configuration.

Upgrade Procedure

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

1. Download the latest version of Veeam Backup & Replication ISO from the Veeam website.

2. Mount the product ISO and use autorun, or run the Setup.exe file.

3. Click Upgrade Veeam Backup Enterprise Manager.

4. Follow the setup wizard steps. At the SQL Server Instance step, select the SQL server, instance and database that was used by the previous version of Veeam Backup Enterprise Manager.

5. If you have Veeam Backup & Replication installed on the same machine, upgrade it immediately after completing upgrade of the Veeam Backup Enterprise Manager server, otherwise this local backup server will not be able to run jobs.

6. Proceed with upgrade of your Veeam backup servers.
IMPORTANT!

After you upgrade Veeam Backup & Replication servers to version 10, Veeam Backup Enterprise Manager starts maintenance jobs to optimize the state of its database. The initial maintenance jobs session may take significant amount of time (up to an hour, depending on the database size). After the job finishes, the database will be brought to an optimal state, and subsequent maintenance job sessions will take much less time.

7. New features of Veeam Backup Enterprise Manager version 10 will be available after all managed Veeam backup servers are upgraded, and initial collection of data from these servers in Veeam Backup Enterprise Manager completes successfully.

Uninstalling Veeam Backup Enterprise Manager

To uninstall Veeam Backup Enterprise Manager:

1. From the Start menu, select Control Panel > Programs and Features.
2. In the programs list, right-click Veeam Backup & Replication and select Uninstall.
3. In the Uninstall window, make sure the check box next to Veeam Backup Enterprise Manager is selected. If this component is co-installed with the Veeam Backup & Replication server, make sure the check box next to Veeam Backup & Replication is cleared. Click Remove and wait for the process to complete.

The Veeam Backup Enterprise Manager configuration database (default name is VeeamBackupReporting) is not removed during the uninstall process. All configuration data stored in the database remains as well.
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
- Veeam Backup Enterprise Manager UI
Accessing Enterprise Manager Website

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 address to the address bar:

   `https://<hostname>:9443`

   For example:

   `https://vbr-em:9443`

2. In the **Sign in** field, enter a user name of an account with a **Portal Administrator**, **Site Administrator** or **Portal Operator** role, and click **Next**.

   - To sign in to Veeam Backup Enterprise Manager under an account that requires providing a password, enter the user account name in the `DOMAIN\Username` format.
   
   - To sign in to Veeam Backup Enterprise Manager under an account that uses a single sign-on service, enter the user account name in the `Username@DOMAIN` format.

3. In the **Enter password** field, enter a password of the provided user account.

   Alternatively, if you sign in to Veeam Backup Enterprise Manager under an account that uses a single sign-on service, Veeam Backup 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 Veeam Backup 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 Veeam Backup Enterprise Manager. For future work, you can create other users in Veeam Backup Enterprise Manager. For more information, see [Managing Accounts and Roles](#).

4. [Optional] Select the **Remain signed in** check box to save the entered credentials for future access.

5. Click **Sign In**.

When you log in under a user account which is not assigned a security 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 Veeam Backup Enterprise Manager security roles, see [Managing Accounts and Roles](#).

---

**NOTE:**

If you cannot access web UI over HTTPS, this can be due to several reasons. For more information, see this Veeam Knowledge Base article.

**TIP:**

If you use Internet Explorer, then to be able to access the Enterprise Manager website using an account currently logged on to the Microsoft Windows OS, you can add this website to Local intranet sites in the Internet Options. In case the current user cannot be authenticated using this method, the Enterprise Manager login window will be displayed. This method works only for Internet Explorer. If you use other web browser, you may be prompted for login.

After you finish working with the Enterprise Manager website, or if you need to switch the user account, click a user name in the top right corner of the main window and then click **Log 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 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 Backup Jobs in Veeam Enterprise Manager.
- Browse for file share backups, search for file shares, delete file shares and perform tile-level restore from file share backups using the **File Shares** tab. For more information, see Working with File Shares.
- Browse for machine backups, search for machines, delete machines and perform failover and replication operations with managed virtual or physical machines using the **Machines** tab. For more information, see Working with Machines.
- Browse the guest OS file system in a machine backup, search for guest OS files and restore necessary files using the **Files** tab. For more information, see Restoring Guest OS Files.
• Perform item-level recovery from application-aware backups created by Veeam Backup & Replication using the **Items** tab. For more information, see *Backup and Restore of Application Items*.

• Approve submitted virtual lab requests, reject them or prolong the time for which a requested virtual lab should be up using the **Requests** tab. For more information, see *Working with Virtual Lab Requests*.

---

**Configuration View**

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

The tabbed pane, located on the left of the window, allows you to navigate to the configuration settings you need – for example, notifications, security roles, and others. The working area is located on the right; it allows you to view data, perform the necessary operations or manage the settings you need.

Below is the list of operations that you can perform in the **Configuration** view of the Veeam Backup Enterprise Manager UI:

• Add, edit or remove Veeam Backup servers using the **Backup Servers** tab. For more information, see *Managing Veeam Backup Servers*.

• Work with vCenter servers managed by Enterprise Manager using the **vCenter Servers** tab. For more information, see *Viewing vCenter Server Information*.

• Manage vCloud Director organizations and vSphere tenant accounts using the **Self-Service** tab. For more information, see *Working with VMware vCloud Director* and *Working with 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 Dashboard 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 Veeam backup servers
- Collect data from backup servers
- Configure retention settings for index and history
- Configure security settings
- Configure notification settings

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

To start working with Veeam Backup Enterprise Manager, perform the following steps:

1. Log in to the Veeam Backup Enterprise Manager website. For more information, see Accessing Enterprise Manager Website.

2. Add backup servers you want to manage. For more information, see Adding Veeam Backup Servers.

3. Retrieve data from added backup servers. For more information, see Collecting Data from Backup Servers.

4. Assign Portal Administrator, Restore Operator or Portal User roles to users who will work with Veeam Backup Enterprise Manager. For more information, see Configuring Security Settings.

5. Provide email notification settings to be able to receive emails with summary on performed backup and replication jobs, lab request status changes and file restore operations. For more information, see Configuring Notification Settings.

Once you have performed initial configuration, you can start working with managed backup servers. You can change the necessary settings in the Configuration view at any time.

NOTE:

The initial configuration tasks can be performed either by the user who installed Veeam Backup Enterprise Manager or any of the users listed in the local Administrators group (these accounts are automatically included in the Portal Administrators group).
Managing Veeam Backup Servers

This section describes actions that you can take with Veeam Backup & Replication backup servers through Veeam Backup Enterprise Manager UI. With Veeam Backup Enterprise Manager, you can:

- Add Veeam backup servers
- Edit managed Veeam backup servers
- Remove managed Veeam backup servers

Adding Veeam Backup Servers

Veeam Backup Enterprise Manager allows users to manage jobs across several Veeam Backup & Replication servers and perform restore operations with backups using the information from these Veeam backup servers. To add a Veeam backup server to the Enterprise Manager infrastructure:

1. Log in to Enterprise Manager using an administrative account, and click Configuration to open the Configuration view.
2. Go to the Backup Servers section on the left.
3. Click Add at the top of the Backup Servers section.
4. In the Backup Server Settings window, enter a full DNS name or IP address of the server you want to add, and provide a server description.
5. Provide name and password of the user with administrative rights on the added server. Veeam Backup Enterprise Manager user must have Veeam Backup Administrator role permissions on the Veeam backup server. For more information see Veeam Backup & Replication Server Roles.
6. Specify the port used by Veeam Backup Service. By default, port 9392 is used.
7. Click OK to add the server.
Limitations for Adding Backup Servers

Consider these limitations when you add Veeam backup servers to the Veeam Enterprise Manager infrastructure:

- You must add one backup server only to a single instance of Veeam Backup Enterprise Manager.
- You must not add cloned backup servers of the added servers.
- You must not add a configuration restored server of a backup server that was previously added to Enterprise Manager (even after the original backup server was removed from Enterprise Manager).
- You must not add backup servers that have identical objects in Veeam Backup & Replication configuration databases. Data collection will fail when Veeam Backup Enterprise Manager attempts to insert duplicate records about identical objects to its configuration database. Identical objects can appear in Veeam Backup & Replication configuration databases in the following cases:
  - Jobs on several backup servers process the same machines.
  - The same backups are imported to the Veeam Backup & Replication console on several backup servers (for example, the same backup repository is shared between several backup servers, backups are copied between different machines and these machines are added to the Veeam Backup & Replication console on different backup servers, and so on).
- Install the same product version on the Veeam Backup Enterprise Manager server and Veeam backup servers. If you use different versions of Veeam Backup Enterprise Manager and Veeam Backup & Replication, you may not be able to leverage all features in Veeam Backup Enterprise Manager.

Veeam Backup Enterprise Manager supports adding backup servers with Veeam Backup & Replication 9.5 Update 3 and later.

Editing Veeam Backup Servers

To edit settings of a server after it was added, select the server in the Backup Servers list and click Edit on the toolbar.

Removing Veeam Backup Servers

To delete an added Veeam backup server, select it in the Backup Servers list and click Remove on the toolbar.
Collecting Data from Backup Servers

Veeam Backup Enterprise Manager retrieves data from added backup servers using the data collection job. The data collection job collects information about backup and replication jobs from Veeam Backup & Replication databases on the managed backup servers. The collected data is stored to the Veeam Backup Enterprise Manager configuration database and can be accessed by multiple users via 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:**

Consider the following:

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

**Periodic Data Collection**

By default, Veeam Backup Enterprise Manager collects data from added backup servers every 15 minutes. To change the data collection interval, do the following:

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 that case, you can only start the data collection job manually.

To disable periodic data collection, do the following:

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, do the following:

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, do the following:

1. Select **Sessions** on the left of the **Configuration** view.
2. In the list of sessions, select the necessary session and click the **View** link in the **Log** 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.
Configuring Retention Settings for Index and History

Veeam Backup Enterprise Manager allows for configuring retention settings for the index files, as well as for the event history.

- If you are using 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 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. Open the Configuration tab.
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. Default value is 3 months, minimal allowed — 1 month, maximum allowed — 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 to **Keep all**. By default, retention period for session data is set to **Keep only last 53 weeks** — here 53 is maximum allowed number of weeks, minimal allowed is 1 week.

   b. When finished, click the **Save** button below the section. New retention settings will be saved in the Enterprise Manager database, and pop-up message notifying you on the update will be displayed at the top of the window.
Note that the retention settings you specify in Veeam Backup Enterprise Manager are propagated to all Veeam backup servers connected to it. These settings override the Session history retention values specified at the level of the Veeam backup server.

For example, if the retention options of the Veeam backup server are configured to keep the session history for 50 weeks, and in Veeam Backup Enterprise Manager you select to Keep only last 53 weeks, the latter value will be propagated to the Veeam backup server; so the history will be kept for 53 weeks.
Configuring Security Settings

 Updating Security Certificate

This certificate is needed to establish secure communication with the Enterprise Manager website using HTTPS. You can specify path to existing certificate or generate a new self-signed certificate during Enterprise Manager installation. In case of installing on the same machine with Enterprise Manager, this certificate will be also used by Veeam plug-in for vSphere Web Client and RestAPI client to receive data using HTTPS protocol.

If you need to update security certificate, consider that:

- To update Enterprise Manager certificate, you can use Internet Information Services (IIS) Manager. For more information, see this Microsoft Docs article.
- For RestAPI, certificate should be updated using the `netsh` command. For more information, see the Updating SSL Certificate section of the Veeam RESTful API Reference.

Configuring User Roles

You should also assign security roles to users who will be working with the Veeam Backup Enterprise Manager web portal.
Managing Accounts and Roles

Veeam Backup Enterprise Manager implements security by limiting access to web management website features and data, based on user roles. This empowers administrators to delegate permissions in a very granular way, on an as-needed basis, to the individuals who will complete the restore process. It is possible, for example, to delegate permissions to recover files without actually being able to see the contents of the files.

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 Serf-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 using the Self-service tab of the Configuration view. For more information, see Managing Tenant Accounts.

To be able to log in to the Veeam Backup Enterprise Manager website, a user must have the Portal Administrator, Restore Operator or Portal User role assigned.

<table>
<thead>
<tr>
<th>Enterprise Manager Role</th>
<th>How is Assigned</th>
<th>Access to Configuration</th>
<th>Allowed Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Administrator</td>
<td>Initially by default to the users listed in the local Administrators group and the user who installed Veeam Backup Enterprise Manager. By an existing Portal Administrator in the Enterprise Manager &gt; Configuration &gt; Roles</td>
<td>Yes</td>
<td>Full access to all available operations on all tabs of the web UI.</td>
</tr>
</tbody>
</table>
| Portal User             | By Portal Administrator in the Enterprise Manager > Configuration > Roles | No | • Access machines 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 backup jobs on the Dashboard, Reports and Jobs tabs |
| Restore Operator        | By Portal Administrator in the Enterprise Manager > Configuration > Roles | No | • Access machines from the restore scope on the Machines and/or Files tab  
  • 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 machines that can be recovered by appropriate personnel. For example, database administrators can restore database servers (SQL, Oracle, or other) — this is their restore scope; Exchange administrators’ restore scope will include Exchange server machines, and so on. Depending on their role configuration, non-administrative users can access the *Machines* and/or *Files* tab of Veeam Backup Enterprise Manager website.

**IMPORTANT!**

Restore scope (list of machines a user can recover) can be customized if you have 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. For more information, see *Restrictions for Delegated Restore*.

**Assigning Role**

To specify security settings for a user or group of users:

1. Open the *Configuration* view.
2. Click the *Roles* tab on the left of the *Configuration* view.
3. Click *Add* on the toolbar.
4. From the *Account type* list, select the type of account you want to add: *User, Group, External User or External Group*.
   - Users who access Veeam Backup Enterprise Manager under an account of the *User or Group* type will have to provide a password to log in to Enterprise Manager.
   - Users who access Veeam Backup Enterprise Manager under an account of the *External User or External Group* type will be able to log in to Enterprise Manager using a single sign-on service. For more information, see *SAML Authentication Support*.
5. In the *Account* field, specify the name of the account:
   - For an account of the *User or Group* type, specify the name in the *DOMAIN\Username* format.
   - For an account of the *External User or External Group* type, specify the name in the *Username@DOMAIN* format.
6. From the *Role* list, select the portal role that you want to assign to the account: *Portal Administrator, Portal User or Restore Operator*.
7. [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*.
8. In the *Allow restore of* section, you can configure additional restrictions for the restore scope. For more information, see *Restrictions for Delegated Restore*. 
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.)

![Add Role Form](image-url)
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.

To delete an added user or group, select it in the list and click **Remove** on the toolbar.
Configuring Restore Scope

Default restore scope for users with a non-administrative role includes All objects from available backups. If you have Enterprise Plus edition of Veeam Backup & Replication deployed in your environment, you can customize restore scope for non-administrative users.

To narrow the restore scope, when creating or editing the profile of a Portal User or Restore Operator, do the following in the Add Role or Edit Role window:

1. In the Restore scope section, select the Selected objects only option and click Choose.
2. 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 object*, *vSphere object*, *vCloud object*, *Protection Groups*, *File share* or *AHV object*.

![Manage Scope Objects](image)

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

**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.

![Add Objects](image)
TIP:
Consider the following:

- For VMware objects, you can switch between **Hosts and Clusters, VMs and Templates, Datastores and VMs** and **Tags and VMs** views.
- For Hyper-V objects, you can switch between **Hosts and VMs, Hosts and Volumes, Hosts and VM Groups** views.

4. **Click OK** to save the settings.

After a user logs in to Enterprise Manager, they will be able to view objects and/or files included in their restore scope on the corresponding UI tabs.

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 also after any role modification. It may happen that some newly created machines, file shares and backups are not yet presented to users in the **Machines, File Shares or Files** tabs right after the login to Enterprise Manager. If you cannot find an object after making a search query, click the link **I don't see my VM** to refresh the view. This link, however, will not be visible until you have made an unsuccessful search.

Administrative user can click **Rebuild Roles** in the **Roles** section of the **Configuration** page to refresh all scopes of all accounts manually. Consider that this operation will affect all configured roles.

**Portal Administrators** can watch the progress of security scope rebuild process on the **Sessions** page.
Configuring Restrictions for Delegated Restore

By default, users can restore all types of files from available backups. Files can be restored either to the local machine or the original location. For security purposes, you can configure additional restrictions for the restore scope. For example, you can specify the list of file types available to the operator or prohibit downloading of restored files at all.

To restrict the restore operator actions, perform the following steps when creating or editing user account settings.

1. Open the Roles section of the Configuration view.

2. Click Add to create a new user account or select an existing account and click Edit to edit the selected account.

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 Guest files check box. If you select this check box, you can also select the following options:
   - Allow in-place file restores only — select this option to allow file-level restore to the original location only. Consider that the restored files will be available only to accounts that have access to the original machine.
   - Allow restore of files with these extensions only — select this option to define which file types are allowed for restore. In the text box, enter a list of extensions for allowed file types, separated by commas.

5. To allow restore of Microsoft Exchange items (mail, calendars, tasks), select the Microsoft Exchange items check box.
6. To allow restore of databases, select the **Databases** check box. If you select this check box, you can also select the following options:

   - **Microsoft SQL Server databases** — select this option to allow restore of Microsoft SQL databases on machines included in the user’s restore scope.
   - **Oracle databases** — select this option to allow restore of Oracle databases on machines included in the user’s restore scope.
   - **Deny in-place database restores** — select this option to restrict the restore operator from overwriting the original databases during the database restore process.

7. Click **OK**.
Configuring Veeam Backup Server Roles

To perform actions on the Veeam backup servers, Veeam Backup Enterprise Manager uses one of the following accounts:

- The account specified when adding a Veeam backup server (see Adding Veeam Backup Servers).
- The account under which the Veeam Enterprise Manager Service runs, for example, if you have upgraded your Enterprise Manager (with backup servers connections preserved).

The account used to interact with the backup server must have Veeam Backup Administrator role permissions on the backup server side. This is because on the Veeam backup server side all operations are performed by Veeam Backup Service that verifies beforehand if the account that is used to interact with the backup server has rights to accomplish the necessary actions.

Adding Enterprise Manager User to Veeam Backup Server Administrators Group

To add an Enterprise Manager user to the Administrators group on the backup server side:

1. Log on to the Veeam backup server as a user with Veeam Backup Administrator role permissions.
2. Select Users and Roles from the main menu of Veeam Backup & Replication.
3. Click Add.
4. In the User or group field, specify the account that Veeam Backup Enterprise Manager will use to interact with this backup server. Enter the name of a user or group in the DOMAIN\Username format.
5. From the Role list, select the Veeam Backup Administrator role.
Editing Veeam Backup Server Administrators Group

To edit settings of an added user or group, select it in the list of roles and click **Edit** on the right. Then edit user or group settings as required.

Deleting Users from Veeam Backup Server Administrators Group

To delete an added user or group, select it in the list and click **Remove** on the right.
Configuring SAML Authentication Settings

Organizations who use a single sign-on service in their IT infrastructure can allow users to access Enterprise Manager without providing a password. To do this, the Enterprise Manager administrator must configure SAML authentication settings.

To configure SAML authentication settings:

1. In Veeam Backup Enterprise Manager, open the Settings section of the Configuration view.
2. Click the SAML Authentication tab.
3. Click the Enable SAML 2.0 check box.
4. In the Identity Provider Configuration section, specify IdP settings. For details, see Specifying Identity Provider Settings.
5. [Optional] If you want to use a certificate to encrypt and sign SP SAML requests, specify certificate settings. For details, see Selecting SP Certificate.
6. [Optional] Click the Advanced Settings link and specify advanced SAML authentication settings. For details, see Specifying Advanced SAML Authentication Settings.
7. In the Enterprise Manager Configuration section, specify SP settings. For details, see Specifying Service Provider Settings.
8. Click Save.

After you configure SAML authentication settings, you can register user accounts that will be able to log in to Enterprise Manager using a single sign-on service. For details, see Managing Accounts and Roles.
Specifying Identity Provider Settings

To set up SAML authentication, you must obtain IdP SAML authentication settings from the IdP and specify them in Enterprise Manager. You can specify IdP settings in one of the following ways:

- Import IdP settings from a SAML metadata file obtained from the IdP.
- Specify IdP settings manually.

To import IdP 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 IdP settings manually:

1. In the Identity Provider Configuration section, in the Entity ID field, specify a unique ID of the IdP.
2. In the Login URL field, specify the URL of the single sign-on login page provided by the IdP.
3. From the Binding list, select a SAML binding used by the IdP 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 IdP.
Selecting SP Certificate

If you want to sign and encrypt authentication requests sent from Veeam Backup Enterprise Manager to the IdP, 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 IdP. The IdP will use this certificate to decrypt requests and validate the request signature. For more information, see Specifying Service Provider Settings.

TIP:

Consider the following:

- To change the SP 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 SP metadata. For more information, see Specifying Advanced SAML Authentication Settings.
Specifying Advanced SAML Authentication Settings

To specify advanced settings for SAML authentication:

1. To include in the SP SAML metadata a security certificate required to decrypt SP authentication requests and validate the signature of the signed requests, in the Service Provider Settings section of the SAML Advanced Settings window, select the Include encryption certificate in metadata and Include signing certificate in metadata check boxes.

2. 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.

3. By default, to provide for single sign-on authentication for groups of users, Veeam Backup Enterprise Manager accepts information about groups from the IdP 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.

4. If you want to sign authentication requests sent from Enterprise Manager to the IdP with a digital certificate, in the Identity Provider Settings section, select the Sign AuthnRequests to IdP check box.

5. From the Authentication context comparison list, select a comparison method for authentication context: Exact, Minimum, Maximum or Better.

6. Click Apply.
Specifying Service Provider Settings

To set up SAML authentication, you must pass SP SAML authentication settings to the IdP. You can prepare SP settings in one of the following ways:

- Export SP settings to a SAML metadata file. To do this, in the Enterprise Manager Configuration section of the SAML Authentication view, click the Download link. Veeam Backup Enterprise Manager will download the SP metadata as a file of the XML that conforms to the SAML 2.0 Metadata Schema. Note that if you plan to use a certificate to sign end encrypt SAML authentication requests, and need to pass the public key certificate to the IdP, you must include the certificate in the metadata file. For more information, see Specifying Advanced SAML Authentication Settings.

- Copy SP settings manually. To do this, click the Copy Link links next to the SP Entity ID / Issuer and Assertion consumer URL fields. If you have selected a certificate that will be used to sign end encrypt SAML authentication requests, you must also pass the public key certificate to the IdP. To copy the certificate, click the Download link next to the Certificate field.
Configuring Notification Settings

You can configure Veeam Backup Enterprise Manager to send email notifications.

To receive email notifications, configure SMTP server settings. For more information, see Email Server Settings.

After that, you can switch on or off the necessary notifications. You can configure the following notifications:

- Job Summary
- Lab Requests
- Restore Operations
- License Information
- Key Management
Email Server Settings

SMTP server is a server that is used for sending emails to the specified email address.

To configure email server settings:

1. Open the **Notifications** section of the **Configuration** view.

2. On the **Server Settings** tab, specify a full DNS name or IP address of the SMTP server. If necessary, change the port number that will be used to communicate with the mail server. The default port number is **25**.

3. In the **Timeout** field, specify a timeout for email server — this should be a value from 1 to 3600 seconds. Default is **100** seconds.

4. If the SMTP server requires SSL connection, select the **Use SSL** check box.

5. If the SMTP server requires authentication, select the **Requires authentication** check box and specify authentication credentials.

6. Click **Save**.
Notifications on Job Results

You can configure Veeam Backup Enterprise Manager to send daily notification emails with the results of finished jobs. The notification email contains a report about the number of jobs performed with the Error, Warning and Success statuses, and provides a link to the Veeam Backup Enterprise Manager web UI so that you can see jobs statistics in detail.

To receive daily email notifications about job results, do the following:

1. Open the Notifications section of the Configuration view.
2. Open the Job Summary tab.
3. Select the Send daily notification at check box and specify the time when you want a notification email to be sent.
4. In the From field, enter an email address of the notification sender.
5. In the To field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. In the Subject field, enter a subject of email notifications. You can use the following variables in the subject:
   - %1 — number of jobs that ended with errors for the last 24 hours
   - %2 — number of jobs that ended with warnings for the last 24 hours
   - %3 — number of jobs that ended successfully for the last 24 hours
     Job retries performed in the last 24 hours are also included in the report.
   - %4 — number of jobs whose last session ended with an error.
   - %5 — number of jobs whose last session ended with a warning.
   - %6 — number of jobs whose last session ended successfully.
     Jobs which were in Disabled state during the last session are also included in the report.
7. Click Save.
TIP:

To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.
Notifications on Lab Requests

You can configure Veeam Backup Enterprise Manager to send notification emails about virtual lab requests created by users who need to perform universal application item-level restore.

To receive notifications about lab requests, do the following:

1. Open the Notifications section of the Configuration view.
2. Open the Lab Requests tab.
3. Select the Send lab request notifications check box.
4. In the From field, enter an email address of the notification sender.
5. In the To field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Specify the subject of the email message.
7. Select request statuses for a report. The notification email will be sent if the request is Pending, Ready, Canceled, Approved, Failed or Stopped.
8. Click Save.

TIP:
To verify that you have configured email settings correctly, click Test. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.

For more information about the universal application item-level restore, see Veeam Universal Application Item Recovery Guide.
Notifications on Restore Operations

You can configure Veeam Backup Enterprise Manager to send notification emails about performed file restore operations.

To receive notifications about performed file restore operations, do the following:

1. Open the **Notifications** section of the **Configuration** view.
2. Open the **Restore Operations** tab.
3. Select **Send notifications on restore operations**.
4. In the **From** field, enter an email address of the notification sender.
5. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
6. Click **Save**.

**TIP:**

To verify that you have configured email settings correctly, click **Test**. Veeam Backup Enterprise Manager will send a test email to all specified email addresses.
Notifications on Licensing

You can configure Veeam Backup Enterprise Manager to send notifications about support expiration, starting 14 days before the expiration date, and license usage in the backup infrastructure.

To receive license notifications, do the following:

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.

If you do not want to receive notifications about the support expiration, select the **Disable support contract expiration 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. 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 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 Statistical Reports

Veeam Backup Enterprise Manager provides reporting functionality that is based on job data collected from managed backup servers. Veeam Backup Enterprise Manager offers a wide range of reporting options, presenting information about performed jobs in various profiles. Being a common business requirement to IT infrastructure, reports allow you to get granular information about all jobs created on managed backup servers:

- Jobs performed for the last 24 hours
- Jobs performed for the last 7 days
- Data for jobs on specific backup servers
- Data for all performed jobs
- Data for all file shares engaged in jobs
- Data for all machines engaged in jobs

You can view on-going reporting data using the web browser as well as export reports to files that can be saved for documenting and archiving purposes. A report file can be open on the client machine using the associated application.
Operation Statistics

On the **Dashboard** tab of the home page, Veeam Backup Enterprise Manager displays on-going data for two time periods — data collected for the last day and data collected for the last week. To switch between these views, click the **Last 24 hours** or **Last 7 days** correspondingly. The following information will be displayed:

- The **Summary** block shows the total number of managed backup servers, performed jobs, processed machines and file shares.
- The **Image Data** block shows the average processing speed, total size of processed machines, full backups and incremental backups.
- The **File Data** block shows the average processing speed, total size of processed file shares, backed-up and archived files.
  
  This block is displayed only if one or more file shares are added on a backup server connected to Veeam Backup Enterprise Manager.
- The **Last 24 hours/Last 7 days** block shows the total number of job runs, successful jobs, jobs with warnings and failed jobs.
- The **Status** block shows the status of backup files, managed backup servers, Veeam Backup Enterprise Manager management server, and licenses. License status is displayed as follows:
  
  - *OK* - valid current license
  - *Warning* - working in grace period or failed to update license
  - *Error* - license 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.

To visualize on-going backup jobs data, Veeam Backup Enterprise Manager uses graphs showing time and date when backup jobs were performed, and the network throughput rate during backup jobs. Jobs related to one backup server have separate colors on the graph. The legend on the right interprets the color scheme used for all managed backup servers.

The highlighted part of the graph represents the configured backup window. You can configure the backup window in the dashboard settings. For more information, see Customizing Dashboard Appearance.
Customizing Dashboard Appearance

If required, you can customize the appearance of graphs in the main Veeam Backup Enterprise Manager view. Do the following:

1. Open the **Configuration** view.
2. Click the **Settings** section on the left of the **Configuration** view.
3. Use the **Activity graph scale** options on the **Chart Settings** tab to switch between graph types: **Linear** and **Logarithmic**.
4. By default, the time interval specified under the selected **Show backup window** check box is highlighted on the activity graph. Default interval is from 8:00 PM to 8:00 AM. You can change the highlighted interval to correlate with your planned backup window by editing the start and stop time. If you do not want to highlight the backup window on the graph, clear the **Show backup window** check box.
5. Save the changes.
Reports on Backup Servers

To view information about managed Veeam backup servers, open the Reports tab.

You can drill down into this data by clicking the necessary link in the corresponding column of the displayed list 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. The file then can be open on the client machine using the associated application.
Job Statistics

To view information about all jobs from managed backup servers, open the Jobs tab in the main view of Veeam Backup Enterprise Manager. 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 description.

### Job Statistics

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Platform</th>
<th>Backup Server</th>
<th>Status</th>
<th>Latest Run</th>
<th>Next Run</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webserver Backup</td>
<td>Backup</td>
<td>Vmware</td>
<td>srv12 tech.local</td>
<td>Success</td>
<td>46 minutes ago</td>
<td>11/10/2019 11:00:00 PM</td>
<td>Backup of ABC Company webserver</td>
</tr>
<tr>
<td>DB Backup</td>
<td>Agent Backup</td>
<td>Vmware Agent for...</td>
<td>srv13 tech.local</td>
<td>Success</td>
<td>4 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Backup of database system</td>
</tr>
<tr>
<td>Appserver Backup</td>
<td>Backup</td>
<td>nginx</td>
<td>appserver1 tech.local</td>
<td>Success</td>
<td>4 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Backup of application server</td>
</tr>
<tr>
<td>Webserver Replication</td>
<td>Replication</td>
<td>Vmware</td>
<td>appserver1 tech.local</td>
<td>Success</td>
<td>3 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Replication of web server</td>
</tr>
<tr>
<td>Test Server Backup</td>
<td>Backup</td>
<td>Vmware</td>
<td>appserver2 tech.local</td>
<td>Success</td>
<td>5 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Backup of test lab</td>
</tr>
<tr>
<td>SharePoint Backup</td>
<td>File Share</td>
<td>File Share</td>
<td>S12/SMB/Loc</td>
<td>Success</td>
<td>5 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Backup of SMB file share</td>
</tr>
<tr>
<td>CRM Backup</td>
<td>Backup</td>
<td>Vmware</td>
<td>appserver2 tech.local</td>
<td>Success</td>
<td>4 hours ago</td>
<td>11/10/2019 08:00:00 PM</td>
<td>Backup of CRM system</td>
</tr>
<tr>
<td>Server Replication</td>
<td>Replication</td>
<td>Vmware</td>
<td>srv13 tech.local</td>
<td>Warning</td>
<td>10 hours ago</td>
<td>11/10/2019 08:00:00 AM</td>
<td>Replication of ABC Company server</td>
</tr>
<tr>
<td>Reovery Backup</td>
<td>Backup</td>
<td>Vmware</td>
<td>srv12 tech.local</td>
<td>Success</td>
<td>16 hours ago</td>
<td>11/16/2019 08:00:00 AM</td>
<td>Backup of ABC Company Reovery server</td>
</tr>
</tbody>
</table>

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 status 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.
Processed File Shares Statistics

To view information about file shares processed by backup jobs, 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.

Besides the information presented in the list of file shares, the **File Shares** tab allows you to view advanced data about each file share:

- To see detailed information about a file share, click its name in the **File Share** column.
- To see detailed information about file restore points, click a link in the **Restore Points** column.

**NOTE:**

You can export displayed information to a file using the **Export** link on the toolbar. This file then can be opened on the client machine using the associated application.
Processed Machines Statistics

To view information about all machines engaged in performed jobs, open the **Machines** tab. Each entry in the list contains the following data: machine name, path to backup file, number of restore points, backup server to which the job relates, job name and status of the last job run.

### Machine Information
- **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.

### Exporting Information
- 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.
Viewing vCenter Server Information

On the **vCenter Servers** page, you can view the information on vCenter servers added to your Veeam backup infrastructure. You can also perform the following operations with vCenter servers:

- **Check version** — use this command to request vCenter server version and operation status. If Veeam plug-in for vSphere Web Client is deployed, its version, status and installation account will be also displayed.

- **Install** — use this command to install Veeam plug-in for vSphere Web Client on the selected server. For details, see **Controlling Backup Infrastructure with vSphere Web Client**.

- **Remove** — use this command to uninstall Veeam plug-in for vSphere Web Client from selected server.

**IMPORTANT!**

To perform these operations, you should supply a user account with sufficient permissions to access vCenter Server. (Currently, user account information is not imported from the Veeam Backup & Replication configuration database to the Enterprise Manager database for security reasons.)
Viewing Information About Enterprise Manager

To view detailed information about Enterprise Manager and its components, URLs of RESTful API and Veeam Self-Service File Restore Portal, go to the Configuration view and click About.

In addition to this information, the About view displays paths to the Enterprise Manager logs. The log files are available in 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 site logs**
  
  C:\ProgramData\Veeam\Backup\Veeam.WebApp.log
Managing Backup Jobs in Veeam Enterprise Manager

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 and retry, edit selective job settings or clone jobs.

**NOTE:**

Veeam Agent jobs are not manageable from Veeam Backup Enterprise Manager; management capabilities for Veeam Agent backups are described in this section.

To view the list of jobs, click the **Jobs** tab in the main view of Veeam Backup Enterprise Manager.

You can use the filter and the search field to quickly find the necessary job. Use the **Backup server** field to view jobs of the selected backup server only. Use the **Status** filter and the search field at the top of the view. You can filter jobs by a backup server and a job status. Once you have selected necessary filter criteria, click the **Apply** button to apply them.
Starting, Stopping and Retrying Jobs

Veeam Backup Enterprise Manager allows you to control the job runs without the need to access the Veeam Backup & Replication console on the corresponding backup server. For backup and replication jobs, you can perform the following operations:

- Run a job — for that, select it in the list on the Jobs tab, then click Start on the toolbar.
- Stop a job — for that, select it in the list on the Jobs tab, then click Stop on the toolbar.
- Re-run a job that has failed — for that, select it in the list on the Jobs tab, then click Retry on the toolbar.

You can see the current state (including the latest job run status) in the Current State column of the jobs list.

**NOTE:**

For more information on starting and stopping a backup copy job and database (Oracle or SQL) server backup job with transaction log processing enabled, see the Backup and Backup Copy sections of the Veeam Backup & Replication User Guide.
Enabling and Disabling Jobs

Veeam Backup Enterprise Manager allows you to enable and disable backup jobs, replication jobs, and backup copy jobs.

A backup copy job runs continuously, but it can be disabled for some time. If disabled, it does not monitor source backup repositories and does not copy restore points to the target backup repository.

When you disable an SQL server backup job, remember that transaction log processing (if enabled for that job) will be also switched to Disabled state.

NOTE:

For more information on starting and stopping a backup copy job and database (Oracle or SQL) server backup job with transaction log processing enabled, see the Backup and the Backup Copy sections of the Veeam Backup & Replication User Guide.

To enable or disable a job:

1. Select the required job in the list on the Jobs tab
2. Click Job on the toolbar.
3. Select Enable or Disable from the list of commands.
Editing Job Settings

Veeam Backup Enterprise Manager allows you to modify settings of VMware and Hyper-V backup and replication jobs that have been previously configured on managed backup servers. Backup job settings can be edited with Veeam Backup Enterprise Manager if you have Enterprise or Enterprise Plus license installed. You can change only a subset of the job configuration settings through the web UI, as described in this document. If you have Veeam backup servers of earlier versions added to Enterprise Manager, jobs managed by these servers cannot be modified or deleted using Veeam Backup Enterprise Manager.

**IMPORTANT!**

Consider the following:

- The edit operation is available if you have Enterprise or Enterprise Plus license installed.
- You cannot edit Veeam Agent backup jobs, file share backup jobs, and backup copy jobs in Veeam Backup Enterprise Manager. To edit settings of such jobs, use the Veeam Backup & Replication console.

Working via the Veeam Backup Enterprise Manager web UI, you can change a number of job settings:

- Specify job name, description and retention settings for the restore points.
- Manage the list of machines that the job should process (add and remove machines or containers to/from the list, exclude individual machines from containers, change the order in which the job will process machines).
- Configure guest processing settings.
- Change the job schedule.

**NOTE:**

If the `Location` property 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.

These settings will take effect starting with the next job run. Other job settings can be configured via the Veeam Backup & Replication console only.
Job settings are modified by means of a web-based wizard. To run the wizard, do the following:

1. Open the Jobs tab and select the necessary job in the list.
2. On the toolbar, click Job and expand the list of available actions.
3. Select Edit.

The next sections will guide you through all steps of the wizard and provide explanation on available options.
Step 1. Edit Job Name and Retention Settings

At the first 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. In the **Retention policy** section, 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. Please consider that the number of restore points doesn’t correspond to the number of days to store restore points. For more information on retention, see the Retention Policy section in 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 weekly, monthly and yearly full backups must be retained. For more information, see the GFS Retention Policy section of the Veeam Backup & Replication User Guide.

---

**Edit Backup Job**

<table>
<thead>
<tr>
<th>Job Settings</th>
<th>Specify the job name, description and retention policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Machines</strong></td>
<td>Job name: CRM Backup</td>
</tr>
<tr>
<td><strong>Guest Processing</strong></td>
<td>Description: Backup of CRM system</td>
</tr>
<tr>
<td><strong>Job Schedule</strong></td>
<td>Retention policy: 5 Restore points</td>
</tr>
<tr>
<td></td>
<td><strong>Keep certain full backups longer for archival purposes</strong></td>
</tr>
<tr>
<td></td>
<td>1 yearly</td>
</tr>
</tbody>
</table>

---

[Image of the Edit Backup Job window with options for job name, description, and retention policy settings.]
Step 2. Edit List of Virtual Machines

You can change the list of machines that the job will process by adding or removing individual machines and machine containers (for example, entire hosts or clusters). Jobs with machine containers are dynamic in their nature: if a new machine is added to the container after a job is created, the job will be automatically updated to include the added machine.

To add a machine or a machine container to the list:

1. Click the **Add** button on top of the window.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>crm01</td>
<td>VirtualMachine</td>
</tr>
<tr>
<td>dbserver01</td>
<td>VirtualMachine</td>
</tr>
</tbody>
</table>
2. In the displayed virtual infrastructure tree, select the necessary object.

![Add Objects](image)

To facilitate objects selection, you can do the following:

- Switch between virtual infrastructure views using the buttons in the top right corner.
- Search for objects: type a name or part of a name in the search field at the top of the window. Specify the type of the object from a scroll list next to the search field.

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

To remove a machine or machine container, select it in the list, and click **Remove**. If required, you can also exclude individual machines from machine containers (for example, if you need to back up the whole VMware or Hyper-V server excluding several machines running on this server).

To exclude machines from a machine container:

1. Select a machine container in the list and click **Exclusions** on the right.
2. In the **Exclusions** section, click **Add** and select machines that should be excluded.
Step 3. Define Machine Processing Order

If specific machines included in a job must be processed first, you can change a machine processing order. The machine processing order can be helpful if you want to ensure that processing of a machine does not overlap with other scheduled activities, or that it is completed before the certain time.

To change the machine 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, however, that if you choose to back up a container, machines inside the container will be processed at random. To ensure that machines are processed in the defined order, you should add them as standalone machines, not as part of a container.

<table>
<thead>
<tr>
<th>Edit Backup Job</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Settings</strong></td>
</tr>
<tr>
<td><strong>Virtual Machines</strong></td>
</tr>
<tr>
<td><strong>Guest Processing</strong></td>
</tr>
<tr>
<td><strong>Job Schedule</strong></td>
</tr>
<tr>
<td><strong>Select virtual machines to process</strong></td>
</tr>
<tr>
<td><img src="image" alt="Add" /> <strong>Add</strong></td>
</tr>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><img src="image" alt="crm01" /></td>
</tr>
<tr>
<td><img src="image" alt="dbserv01" /></td>
</tr>
<tr>
<td><img src="image" alt="srv08" /></td>
</tr>
</tbody>
</table>

---

129 | Veeam Backup Enterprise Manager | User Guide
Step 4. Configure Guest Processing Settings

At the Guest Processing step of the wizard, you can select to create a transactionally consistent backup, configure transaction log handling settings, and enable guest file system indexing.

Application-Aware Image Processing Settings

If you want to create a transactionally consistent backup or replication ensuring successful recovery of machine applications without any data loss, take the following steps:

1. Select the Enable application-aware image processing check box.
2. Click the Customize Applications link.
3. To define custom settings for a machine in the list, select it and click Edit. Consider the following:
   - To customize settings of a machine added to the job as part of a container, the machine should be included in the list as a standalone instance. For that, click Add Machine and select a machine whose settings you want to customize. Next, select the machine in the list and click Edit to define the necessary custom settings.
   - To discard custom settings of a machine, select the machine in the list and click Remove.
4. Configure the necessary settings for the selected application server:
   - General Settings
   - SQL Server Processing Settings
   - Oracle Server Processing Settings
   - File Exclusions

![Application-Aware Processing Options](image)

<table>
<thead>
<tr>
<th>Object</th>
<th>VSS</th>
<th>Transaction logs</th>
<th>Excludes</th>
</tr>
</thead>
<tbody>
<tr>
<td>crm01</td>
<td>Require success</td>
<td>Exchange: Truncate, SQL: Truncate:</td>
<td>Disable</td>
</tr>
<tr>
<td>dbserver01</td>
<td>Require success</td>
<td>Exchange: Truncate, SQL: Truncate:</td>
<td>Disable</td>
</tr>
<tr>
<td>srv02</td>
<td>Require success</td>
<td>Exchange: Truncate, SQL: Truncate:</td>
<td>Disable</td>
</tr>
</tbody>
</table>

OK  Cancel
General Settings

Applications Section

In this section, select the option that corresponds to a transactionally-consistent backup creation scenario of your choice:

- **Select Require successful processing** (default option) if you want Veeam Backup & Replication to stop the backup job if any error occurs.

- **Select Try application processing, but ignore failures** if you want to continue backing up the machines even if errors occur. This option is recommended to guarantee 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 quiescencing for the machines at all. In this case, log processing settings (the section below) will become unavailable.

Transaction Logs Processing Section

In this section, specify whether this job should process transaction logs upon a successful backup:

- **Select Process transaction logs with this job** if you want Veeam Backup & Replication to handle transaction logs. With this option enabled (default setting), Veeam will support log pruning for Microsoft Exchange and Microsoft SQL Servers, as well as for Oracle databases archived logs:
  
  - Truncation of transaction logs for Microsoft Exchange server will be performed after the job completes successfully: the Veeam runtime process will wait for the machine backup to complete and then trigger truncation of transaction logs. If truncation of transaction logs is not possible for some reason, the logs will remain untouched in the machine guest OS until the next start of the Veeam runtime process.
  
  - Settings for SQL Server transaction log handling can be configured separately on the SQL tab — it becomes available to you with this option selected.
  
  - Similarly, you can configure settings for Oracle database archived logs processing on the Oracle tab.

- **Select Perform copy only** if you want to use native application means or a third-party tool to process transaction logs. Veeam Backup & Replication will create a copy-only backup for the selected machine. The copy-only backup preserves a chain of full/differential backup files and transaction logs, so Veeam Backup & Replication will not trigger transaction log truncation. This option is recommended if you are using another backup tool to perform the machine guest-level backup, and this tool maintains consistency of the database state. To learn more, see the Guest Processing section of the Veeam Backup & Replication User Guide.
NOTE:
With this option selected, the **SQL** and **Oracle** tabs will not be available.

### sry04: Processing Settings

<table>
<thead>
<tr>
<th>General</th>
<th>SQL</th>
<th>Oracle</th>
<th>File Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Require successful processing (recommended)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Try application processing, but ignore failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Disable application processing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Transaction logs processing**

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

- Process transaction logs with this job (recommended)
- Perform copy only (lets another application use logs)

---

### SQL Server Processing Settings

For more information on configuring **Microsoft SQL Server** processing settings, see Backup and Restore of Microsoft SQL Server Databases.

### Oracle Server Processing Settings

For more information on configuring **Oracle** processing settings, see Backup and Restore of Oracle Databases.
File Exclusions

On the **File Exclusions** tab, specify whether to exclude or include specific files in the backup. Exclusions can help to decrease the backup file size. However, remember that selective processing takes additional time that depends on the number of excluded files; also, it requires obtaining per-file metadata (stored in backups). Thus, it is recommended to use this option for excluding large files. By default, exclusions are disabled.

- **Exclude the following files and folders** — with this option selected, you can specify what files and folders must be excluded from the backup.
- **Include only the following files and folders** — with this option selected, you can specify exactly what files and folders must be only included in the backup.

Click **Add** and specify what files and folders you want to include or exclude.

To form the list of exclusions or inclusions, you can use full paths to files and folders, environmental variables and file masks with the asterisk (*) and question mark (?) characters. For more information, see VM Guest OS File Exclusion section of the Veeam Backup & Replication User Guide.
Indexing Options

To facilitate browsing and searching for guest OS files in backup, select the Enable guest file system indexing check box. This setting will provide, 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 will be able to use only quick search within the selected restore point.

NOTE:

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

To provide granular indexing options for individual machines:

1. Click the Customize Indexing link, then in the window displayed select the machine in the list and click Edit. Consider the following:
   
   o To customize settings of a machine added to the job 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. Next, select the machine in the list and click Edit to define the necessary custom settings.
   
   o To discard custom settings of a machine, select the machine in the list and click Remove.

## Guest File System Indexing Options

<table>
<thead>
<tr>
<th>Object</th>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>crm01</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>dbserver01</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>srv08</td>
<td>Partial</td>
<td>Partial</td>
</tr>
</tbody>
</table>

[Table of Guest File System Indexing Options]
2. 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.

3. Click **OK** to save the settings and close the window.
Guest OS Credentials

To coordinate proper VSS and indexing activities, Veeam Backup & Replication deploys a small executable file inside a machine. It is installed only during VSS quiescence procedure and removed immediately after the processing is finished (depending on the selected option, during the backup job or after it is finished), thus producing low impact on machine performance and stability. To learn more, please refer to Veeam Backup & Replication User Guide.
In the **Guest OS credentials** section, you need to specify an account with sufficient privileges for deploying this executable file on the guest OS (Windows or Linux). You can select credentials from the list, or click the **Add** button to add new credentials.

### Credentials

<table>
<thead>
<tr>
<th>Username:</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
<td>**********</td>
</tr>
<tr>
<td>Description:</td>
<td>Windows credentials</td>
</tr>
</tbody>
</table>

- For Windows guest OS, you must supply 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 must supply username, password, and SSH port (default is **22**). Use corresponding options to elevate the specified account to root and to add it to the `sudoers` file automatically. In the `sudoers` file, enable the `NOPASSWD:ALL` option for the user account that you want to elevate to root (otherwise, jobs addressing a Linux server will fail as `sudo` will request the password). To prevent `sudo` from fail use the `Use "su" if "sudo" fails` option. In that case, if for some reason `sudo` fails, the specified account will be elevated to `su` instead.

**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 – usually in the encrypted form. To decrypt a private key, you will 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:

- Username
- Passphrase for private key
- Private key stored on the client side (Veeam backup server)
- SSH port (default is 22)
- Non-root account elevation options

<table>
<thead>
<tr>
<th>Linux Credentials</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username:</strong></td>
<td>User</td>
</tr>
<tr>
<td><strong>Password:</strong></td>
<td>*********</td>
</tr>
<tr>
<td><strong>Private key is required for this connection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Private Key:</strong></td>
<td>.pem</td>
</tr>
<tr>
<td><strong>Passphrase:</strong></td>
<td>*********</td>
</tr>
<tr>
<td><strong>SSH port:</strong></td>
<td>22</td>
</tr>
</tbody>
</table>

**Non-root account**

- Elevate specified account to root
  - Add account to the sudoers file automatically
  - Use “su” if “sudo” fails

| Root password: | ********* |
| Description:   | Test Linux server connection |

[Image of the Linux Credentials section with fields filled in]

[Image of the Non-root account options with checkboxes checked]

[Options for non-root account elevation, such as root password and description]

[Buttons: 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.

- If a different account should be used to deploy the agent inside a specific machine, select the machine in the list, click Set User and enter custom guest OS credentials.
- To discard custom credentials for a machine, select it in the list and click the Remove button.

NOTE:

To customize settings of a machine added to the job 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 5. Edit Job Schedule

The **Job Schedule** step of the wizard allows you to choose to manually run the job, schedule the job to start at a specific time — for example, the least busy hours to reduce impact on the environment — or define a schedule for the job to run on a regular basis. To specify the job schedule, select the **Run the job automatically** check box. If this check box is not selected, the job is supposed to be run manually.

---

**Edit Backup Job**

**Job Settings**

**Virtual Machines**

**Guest Processing**

**Job Schedule**

**Specify the job scheduling options**

- **Run the job automatically:**
  - Daily at this time: 02:00 pm
  - Monthly at: 10:00 pm
  - Periodically every: 1 hours
  - After this job: Test Server Backup

**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

---

[Image of the Edit Backup Job interface]
You can choose to perform the job at specific time on defined week days, monthly and with specific periodicity.

You can also select to back up a machine continuously. In this case, the next run of a backup job will be started once the previous one is complete, maintaining your backup always in the most recent state. For that, select the **Periodically every** option, then choose **Continuously** from the drop-down list on the right.

### Periodic Job Runs

You can choose to run the job repeatedly throughout a day with a set time interval. For that, select **Periodically every**, then specify the required time interval and select the necessary time unit: **Hours** or **Minutes**. The job will be started for the first time as soon as the nearest start time comes - that is, if you created a job at 16:30 and configured it to run periodically every 4 hours, the initial run will take place at 20:00.

**NOTE:**

Remember that reference time for periodicity is midnight (12:00 AM).
If you need to define permitted and denied hours for the job run, click **Schedule** on the right and use the timetable. In this case, the job will be started for the first time as soon as the denied interval is over, and then it will run according to the specified schedule. For example, if you created a job at 16:30, configured it to run periodically every 4 hours, and set denied interval to 9:00 - 19:00, then initial run will take place at 19:00, and the next runs will be at 20:00 and 24:00 (since reference time for periodicity is midnight).

You can also specify an 'offset' for the job to start within the specified time interval (hours or minutes). For that, in the **Start time within an hour** field, specify the desired value in minutes. Then the job will run every hour at `<hour>:<offset>`.

**NOTE:** Generally, if a denied period is configured so that one or more periodic intervals fall into it, the next job run will take place as soon as the denied interval is over, with the offset applied (if any), and then the job will run according to the specified schedule.

### Examples

- Remember that offset is applied to the job start time within an hour, firstly at 12:00 AM (as midnight is a reference time for periodic runs). Therefore, if you set up the job to run periodically every 30 minutes, and specify an offset interval as 10 minutes, with no denied hours, the job will run at 00:10, 00:40, 01:10, and so on.

- If you configure some denied hours, then remember that offset will be also applied to the moment when the job starts after the end of denied interval. Therefore, if you set up the job to run **Periodically at 3 Hours** and specify **Denied** hours from 8:00 AM to 8:00 PM, and also set an offset interval to 15 minutes, then the job will run at 00:15 AM, at 3:15 AM, at 6:15 AM, then at 8:15 PM, 9:15 PM (as this is a 3x3-hour interval referencing midnight, plus offset), and so on.

- If you set up the job to run with a 2-hour interval but the job's first run at 10:00 AM exceeds the elapsed time, overlapping the next scheduled run (for example, the job lasted 2 hours 30 min and completed at 12:30 PM), then the second run will start at the nearest scheduled run (at 2:00 PM).
Other Settings

You can also chain the jobs. In the common practice, jobs start one after another: when the job "A" finishes, the job "B" starts and so on. If you want to create a chain of jobs, you should 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.

In the **Automatic retry** section, define whether Veeam Backup & Replication should attempt to run the job again in case it fails for some reason. A repeatedly run job will include failed machines only. Enter the number of attempts to run the job and define time spans 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.

In the **Backup window** section, determine a time span within which the backup job must be completed. The backup window prevents the job from overlapping with production hours and ensures it does not provide unwanted overhead on your virtual environment. To set up a backup window for the job:

1. Select the **Terminate job if it gets out of allowed backup window** check box.
2. Click **Window**.
3. Define the allowed window and prohibited hours for the job. If the job exceeds the allowed window, it will be terminated.

**NOTE:**

If the **Location** property of the source object and target object do not match, you will receive a warning message after you click **Finish**. For example, you may have a backup job targeted at repository located in Sydney, and source machines located in London.
Creating Active Full Backups

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

**NOTE:**
Creating active full backups is unavailable for backup copy jobs and file share backup jobs.

To perform an active full backup:

1. Select the required job in the list on the **Jobs** tab.
2. Expand the menu commands by clicking **Job**, then select **Active Full**.
Cloning Jobs

In addition to performing job editing tasks, you can add new jobs by means of job cloning. Job cloning allows you to create an exact copy of any backup or replication job available in the job list. The recommended practice is to configure a set of 'job templates' in advance, using the Veeam Backup & Replication console on every managed Veeam backup server. These job templates can be used by Enterprise Manager Portal Administrators for cloning and further editing.

**NOTE:**

Consider the following:

- The job cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- The job cloning functionality is not available for file share backup jobs.

To clone an existing job:

1. Open the **Jobs** tab.
2. Select the necessary job in the list.
3. Expand the menu commands by clicking **Job**, then select **Clone**.

Job clone name is created automatically, with the original job name and suffix of the following format: _clone<n>_ where <n> is the sequential number of the clone.

Once a job is cloned, you can edit its settings. For details, see **Editing Job Settings**. Note, however, that not all of the job settings can be changed with the Enterprise Manager web UI. For example, you cannot change the backup repository and backup proxies used for the job or define advanced job settings.

Configuration details of a created job clone are written to the same SQL database that stores configuration details of the original job — thus, the job copy is available and can be managed both via the Veeam Backup Enterprise Manager web UI and via the Veeam Backup & Replication console on a corresponding Veeam backup server. The backup file produced by clone will be located on the same repository as the backup file of the original job.
Deleting Jobs

You can delete the job from configuration and also instruct Enterprise Manager to delete backup files created by this job in the backup repository.

To delete a job:

1. Select the required job in the list on the Jobs tab
2. Expand the menu commands by clicking Job, then select Delete.
3. You will be prompted to delete backup files. To delete backup files, select the Delete backup files check box and click Yes to confirm the operation.

Information about deleted jobs will be removed from Veeam Backup configuration database (and Enterprise Manager database, as well), and these jobs will no longer appear in the UI. If you agreed to delete backup files, they will be removed from backup repository.
Support for Veeam Agents

Enterprise Manager supports browsing and restore operations for guest OS files and application items from backups of physical servers created with Veeam Agent for Microsoft Windows or Veeam Agent for Linux. To use this functionality, make sure the following prerequisites are met:

1. You have 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 Agent for Microsoft Windows or Server edition of Veeam Agent for Linux.
3. Veeam Agent should be integrated with Veeam Backup & Replication, as described in the product documentation.
Guest File Browsing and 1-Click Restore

If you have Veeam Backup & Replication and Veeam Agent that both meet the prerequisites described above, then you can benefit from their integration when browsing, searching and restoring guest OS files from the backups created by Veeam Agent for Windows or Veeam Agent for Linux.

IMPORTANT!

1-Click file-level restore for physical servers is supported only for the Server edition of Veeam Agents. For more information, see https://www.veeam.com/backup-version-standard-enterprise-editions-comparison.html.
Preparing for File Browsing and Restore

Veeam is capable of browsing and restoring files from a backup of physical server created by Veeam Agent with or without enabling guest indexing. Take some preparatory steps for your Windows or Linux server processed by Veeam Agent:

- Preparing for restore from a Windows Server backup
- Preparing for restore from a Linux 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 files indexing, take these steps:

1. Enable guest file system indexing on the Guest Processing step of the backup job wizard. For details, see the Specify Guest Processing Settings > Indexing section of the Veeam Agent User Guide.
2. Run the backup job with guest file system indexing enabled.
3. Make sure the indexing data was imported to Veeam backup database, and catalog replication completed successfully. For details, see the Performing Catalog Replication and Indexing section.

If restoring from an indexed guest, there is no need to mount the restore point for browsing purposes - guest files 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 a user locates 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 files restore to the original location, you will be prompted for the credentials to access the target Windows server. Enter the user name and password; make sure that the account has sufficient access rights.
Linux Server

Preparing Backup

You can restore files from a backup of a physical Linux server created with or without indexing. To prepare a backup with guest files indexing, take these steps:

1. Check for the following utilities to be installed on the Linux server: `mlocate`, `gzip`, and `tar`. These utilities are required for guest indexing; if they are not found, you will be prompted to deploy them to support index creation.
2. Enable guest file system indexing using the backup job wizard. For details, see the corresponding section of the Veeam Agent User Guide.
3. Run the backup job with guest file system indexing enabled.
4. Make sure the indexing data was imported to Veeam backup database, and catalog data replication completed successfully. For more information, see the Performing Catalog Replication and Indexing section.

Whether you will be restoring from a backup with or without guest files indexing, you will need to prepare a machine to operate as an FLR helper appliance.

Preparing FLR Helper Appliance

To perform Linux guest files restore, you should configure an FLR helper appliance on the Veeam backup server with which Veeam Agent is integrated. FLR helper configuration is similar to that described in the Multi-OS File Level Recovery section of the Veeam Backup & Replication User Guide. The only difference is that for restore of a physical machine, you can configure a helper appliance to work on a machine running on the platform of your choice (VMware or Hyper-V). Helper appliance settings are saved in Veeam Backup & Replication database on per-user basis; they will be applied each time the certain user starts Linux file-level restore.

When Linux guest file-level restore is started from Veeam Backup Enterprise Manager, FLR helper configuration settings are obtained from the database of the corresponding Veeam backup server. If no FLR helper configuration is found for the current user account, Veeam will use the default settings (those set during the latest FLR appliance configuration process in Veeam backup console). Thus, before starting Linux file-level restore from Enterprise Manager, make sure that Linux FLR helper settings were configured on Veeam backup server.

**NOTE:**

If you plan to deploy multiple FLR helper appliances in order to restore Linux machines backed up by Veeam Agents integrated with different Veeam backup servers, consider that their initial configuration should be performed on the corresponding Veeam backup servers. Centralized configuration via Enterprise Manager is not supported in the current version.

Other Prerequisites

1. Make sure that then DNS name of the target (original) Linux server where you plan to restore the files is resolved properly.
2. During guest files restore to the original location, you will be prompted for the credentials to access the target Linux server. Specify 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 the server whose file system you want to browse (you can type in server name or pick it from the list). Note that physical Windows or Linux server will have a corresponding OS icon, like shown below.

3. If the server was backed up without guest indexing, then 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 you can 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 machine **guest file search**.

6. To restore a file, take the steps similar to the machine 1-Click File restore.

**IMPORTANT!**

When restoring files to the original location, you will be 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 Server edition of Veeam Agent, and other prerequisites are met, you can use the backups of the physical application servers (Microsoft SQL Server, Microsoft Exchange Server), in particular, to restore the necessary application items of your choice with Veeam Backup Enterprise Manager. For that, follow the procedures described in the corresponding sections of this guide, selecting the restore point of the machine your need.
Working with File Shares

With Veeam Backup Enterprise Manager, authorized users can perform a number of management operations with file shares processed by Veeam Backup & Replication: search and view file share backups, restore files from these backups and delete backups.

IMPORTANT!

Restore scope (list of objects a user can recover) can be customized if you have Enterprise Plus edition of Veeam Backup & Replication; in other editions, this list includes all objects and cannot be customized. However, you can delegate recovery of entire file shares or selected file types. Possible delegation options are described in the Restrictions for Delegated Restore section.
Viewing and Searching File Share Backups

You can view file share backups created by backup jobs configured on Veeam backup servers added to Veeam Backup Enterprise Manager. To do this, in Enterprise Manager, open the **File Shares** tab.

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. To search for specific file shares, no special permissions are required.

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.

- 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.
For each file share, you can click the link in the **Restore Points** column to view the list of restore points created for the file share.

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/19/2019 03:00:15 pm</td>
<td>Backup</td>
<td>✔️ Success</td>
</tr>
<tr>
<td>11/18/2019 03:00:15 pm</td>
<td>Backup</td>
<td>✔️ Success</td>
</tr>
<tr>
<td>11/17/2019 03:00:29 pm</td>
<td>Backup</td>
<td>✔️ Success</td>
</tr>
<tr>
<td>11/16/2019 03:00:22 pm</td>
<td>Backup</td>
<td>✔️ Success</td>
</tr>
</tbody>
</table>
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. Veeam Backup & Replication will mount the file share from the backup to the backup server. Wait for the process to complete.
4. Veeam Backup Enterprise Manager will display contents of the backed-up file share. You can choose whether to browse files contained in all restore points created by the file share backup job or select a specific restore point.
   - By default, the All restore points option is selected in the restore point field. 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 was created. If you want to restore a file from the backup, and the backup contains more than one version of this file, you will be able to select the necessary file version during the restore process. For more information, see Performing File Restore.
To select a specific restore point in which to browse 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.

If you select a specific restore point, Enterprise Manager displays only those file versions that are contained in this restore point. If you want to restore a file from the backup, Enterprise Manager will restore the version of the file in the selected restore point. For more information, see Performing File Restore.

**TIP:**
You can use the search field at the top of the working area to search for specific files and folders. Consider that depending on the number of files in the file share, the search process may take some time.
Performing File Restore

After you locate the necessary file, you can use Veeam Backup Enterprise Manager to restore it from the backup. You can choose to restore a file to the original location or download it to the local machine.

Restore operations are only available to authorized users according to their security settings. Users with the Portal Administrator role can both restore files to the original location or download them to the local machine.

For users with the non-administrative roles, you can configure additional restriction settings. For example, you can prohibit restore operators to download files to the local machine so that they will be able to restore files to the original location only. Additionally, you can specify the types of files that can be restored by operators (this can be helpful if you want to limit operators’ access to sensitive data). For details, see Configuring Security Settings.
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 and Searching 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 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. 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 and Searching 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. 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.

Restored files are stored in a ZipDownload package named `FLR_<date>_<time>.zip` by default in the **Downloads** folder. They are periodically cleaned up by Veeam Backup & Replication — files older than 24 hours are automatically deleted (built-in value).
Restoring Multiple Files

In addition to restoring single files from selected restore points, Veeam Backup Enterprise Manager supports bulk restore. If you need to restore multiple files at once, you can select more than one file in the preview pane when browsing, and then use the Restore command, or add the necessary files to the restore list and then restore all files at once. Unlike the Restore command, using the restore list helps you to prepare for restore files from different file shares and restore points.

To add a file to the restore list:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For more information, see Viewing and Searching File Share Backups and Browsing File Share Backups.
2. Click Add to Restore List.
3. If you browsed for files in all restore points created for the file share, and the restore points contain multiple versions of the file that you want to restore, Veeam Backup Enterprise Manager will prompt you to select the file version. In the Select version window, select the restore point that contains the necessary file version and click OK.

NOTE:

You cannot add multiple versions of the same file to the restore list using the Select version window. If you want to restore multiple versions of a file, browse to this file in a specific restore point and add this file to the restore list.

When a file is added to the restore list, the Pending restore notification appears at the top of the Enterprise Manager UI window.
To restore files added to the restore list:

1. In the restore list notification, click **Pending restore**.
2. In the **Pending Restore** window, select check boxes next to the files that you want to restore. Use the check box next to the header of the **Name** column to select all files in the list at once.
   If you want to remove a file from the restore list, select the file and click **Delete**.
3. Click the **Restore** or **Download** link to perform the necessary restore operation for the selected files.
4. In the displayed window, click **Yes**.
5. [For the download operation] Wait for restore session to complete. In the **Log** tab of the **File Restore History** view, click the **download** link.

**TIP:**

Veeam Backup Enterprise Manager keeps links for downloaded files in the history for one day. To download a file that was previously restored:

1. In the **Files** tab, click **History**.
2. In the **File Restore History** view, select the necessary restore session.
3. In the **Log** tab, click the **download** link.
Deleting File Share Backups

You can delete file share data from a backup created by a backup job in a backup repository. The deleted file share is not removed from the list of file shares immediately. The file share will be removed from the list after records about the file share are removed from the configuration database on the Veeam backup server. Once this operation completes, a notification will appear at the top of the Enterprise Manager UI window.

To delete a file share backup:

1. In Veeam Backup Enterprise Manager, open the File Shares tab.
2. In the list of file share backups, select the necessary backup and click Delete.
   
   To locate the necessary backup, you can filter file share backups by the backup server or search by the file share name.

3. In the displayed window, click Yes.

NOTE:

If several file shares are processed by the same backup job, deletion of the selected file share backup will not affect other file shares in the job.
Working with Machines

With Veeam Backup Enterprise Manager, authorized users can perform a number of management operations over machines: browse machines backups, search for machines, delete machines backups, create on-demand incremental backups (quick backups) for machines, and restore machines and VM disks. If there are failover plans created for machines included in the user’s restore scope, the user can also run selected failover plan for these machines.

IMPORTANT!

Restore scope (list of machines a user can recover) can be customized if you have 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 Restrictions for Delegated Restore section.
Viewing, Searching, Deleting Machines

To search for specific machines, no special permissions are required. To find the necessary machines, open the Machines tab.

You can filter machines in the list by the backup server or search for specific machines by machine name. To search for a machine, enter its name or part of the name in the Search field.
For each machine, you can click the link in the **Restore Points** column to view the list of restore points created for the machine, either on schedule or on demand.

### Deleting Machine Backups

To delete a machine from a backup created by a backup job in a backup repository, select the machine and click **Delete**, then confirm the operation. The deleted machine is not removed from the list of machines immediately. The machine will be removed from the list after records about the machine are removed from the configuration database on the Veeam backup server. Once this operation completes, a notification will appear at the top of the Enterprise Manager UI window.

**NOTE:**

Consider the following:

- This operation is applicable only to backups created by backup jobs.
- If several machines are processed by the same backup job, deletion of the selected machine will not affect other machines in the job.
- The delete operation is not available for replica machines, storage snapshots and machines backed up to tape.
Performing Quick Backup

You can create an ad-hoc incremental backup for one or more machines — quick backup. This backup will be added to the backup chain in the corresponding backup repository. Quick backup can be helpful if you want to produce an additional restore point for one or more machines in the backup job and do not want to configure a new job or modify the existing one.

Quick backup can be performed for machines that meet the following requirements:

- A backup job processing the machine exists on the backup server.
- A full backup file for the machine exists in the backup repository.

**NOTE:**

Quick backup is not available for vCloud Director VMs and Veeam Agent machines.

To perform quick backup, on the Machines tab, select the machine you need and click **Quick Backup**.

Veeam Backup & Replication will trigger a backup job to create a new incremental restore point for the selected machine(s). Details of the running quick backup operation are displayed in the job session window.
Performing 1-Click Restore

Authorized users can restore machines included in their scope with a single click.

**IMPORTANT!**
Consider the following:

1. This functionality is available in Enterprise or Enterprise Plus edition of Veeam Backup & Replication.
2. 1-Click Restore from any storage snapshots, Veeam Agent backups and backups created with Veeam Plug-ins for Enterprise Applications are not supported by Veeam Backup Enterprise Manager.

Users with *Portal Administrator* role have no scope limitations; they can restore machines to their original location. Restore scope for other users is defined as described in the Configuring Restore Scope section.

To restore a machine from backup:

1. On the *Machines* tab, select the necessary machine backup in the list of machines. You can also use search by machine name or filter machines by the backup server.
2. Click *Restore* and select one of the following restore options:
   - Select **Overwrite** if you want to replace the original machine in the production environment with the machine from the backup.
   - Select **Keep** if you want to restore the machine from the backup next to the original machine in the production environment.

**NOTE:**
Veeam Backup Enterprise Manager supports machine restore to the original location only. You cannot restore a VM to another location or with different settings (such as network settings, format of restored virtual disks and so on).

3. In the *Restore* window, select a restore point that will be used to restore the machine.
4. [Optional] Instead of restoring an entire machine from a backup file, you can instruct Enterprise Manager to recover only those data blocks that are necessary to revert the machine to the selected restore point. To do this, select the **Quick rollback** check box. Quick rollback significantly reduces the recovery time and has little impact on the production environment.

For more information on quick rollback, see the Quick Rollback section of the Veeam Backup & Replication User Guide.
5. [Optional] To start a machine immediately after recovery, select the **Power on machine after restoring** check box.

6. **Click Restore.** Veeam Backup Enterprise Manager will display a message notifying you of the operation effect (machine from backup will replace the production machine if it is present in the original location). **Click Yes** in the message window to start the restore operation.

<table>
<thead>
<tr>
<th>Backup Date</th>
<th>Type</th>
<th>Job Name</th>
<th>Last Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/20/2019 8:01:42 am</td>
<td>Full</td>
<td>ABC Company Information Backup</td>
<td>11/19/2019 9:01:29 am</td>
</tr>
<tr>
<td>11/19/2019 9:00:00 am</td>
<td>Increment</td>
<td>ABC Company Information Backup</td>
<td>11/18/2019 8:01:22 am</td>
</tr>
<tr>
<td>11/18/2019 8:01:22 am</td>
<td>Increment</td>
<td>ABC Company Information Backup</td>
<td>11/17/2019 7:00:00 am</td>
</tr>
<tr>
<td>11/17/2019 7:00:00 am</td>
<td>Increment</td>
<td>ABC Company Information Backup</td>
<td>11/16/2019 6:00:00 am</td>
</tr>
</tbody>
</table>

   Similar steps can be taken to fail over to a VM replica (this feature is not available for physical machine backups):

1. On the **Machines** tab, select the necessary machine processed by a replication job.
2. **Click Restore.**
3. In the **Restore** window, select the restore point you need.
4. **Click Failover,** then click **Yes** in the displayed window to confirm the operation.

   Veeam Backup Enterprise Manager will perform failover from the original VM to the VM replica. The VM replica will be powered on after the failover operation completes.

To view the progress of the machine restore operation, on the **Machines** tab, click **History.**
Performing Virtual Disk Restore

Authorized users can restore virtual disks of machines included in their restore scope. This may be helpful if a VM disk becomes corrupted for some reason. The restored virtual disk can be attached to the original VM to replace a corrupted drive, or connected to any other VM.

For more information on virtual disk restore, see the Virtual Disks Restore section of the Veeam Backup & Replication User Guide.

**IMPORTANT!**

Consider the following:

1. This functionality is available in Enterprise or Enterprise Plus edition of Veeam Backup & Replication.
2. The disk restore operation is supported for backups of VMware vSphere VMs only.

Users with 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. You can also use search by machine name or filter machines by the backup server.
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.

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>Select the desired restore point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Mapping</td>
<td></td>
</tr>
<tr>
<td>Secure Restore</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Backup Date</td>
<td>Type</td>
</tr>
<tr>
<td>11/19/2019 06:00:58 am</td>
<td>Increment</td>
</tr>
<tr>
<td>11/18/2019 06:01:22 am</td>
<td>Increment</td>
</tr>
<tr>
<td>11/17/2019 06:00:52 am</td>
<td>Increment</td>
</tr>
<tr>
<td>11/16/2019 06:01:05 am</td>
<td>Increment</td>
</tr>
<tr>
<td>11/14/2019 06:01:18 am</td>
<td>Full</td>
</tr>
</tbody>
</table>
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* (*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.

---

![Virtual Disk Restore](image-url)
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.
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:

- Select the **Scan the restored disk for malware prior to performing recovery** check box.
- 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.
- 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.

<table>
<thead>
<tr>
<th>Virtual Disk Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure Restore</strong></td>
</tr>
<tr>
<td>Scan the restored disk for malware prior to performing recovery</td>
</tr>
<tr>
<td>If malware is found:</td>
</tr>
<tr>
<td>- Proceed with recovery but do not attach infected disks to the target VM</td>
</tr>
<tr>
<td>- Abort disk recovery</td>
</tr>
<tr>
<td>- Scan the entire image</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Restore Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Restore</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Restore</td>
</tr>
</tbody>
</table>

Summary
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**.

<table>
<thead>
<tr>
<th>Virtual Disk Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td>Please review the restore settings before continuing. The restore process will begin after you click Finish.</td>
</tr>
<tr>
<td><strong>Restore point:</strong></td>
</tr>
<tr>
<td>Original VM name:</td>
</tr>
<tr>
<td>Restore point:</td>
</tr>
<tr>
<td>Target VM name:</td>
</tr>
<tr>
<td>Target host:</td>
</tr>
<tr>
<td><strong>Restored disks type (same as source):</strong></td>
</tr>
<tr>
<td>Source file:</td>
</tr>
<tr>
<td>Target datastore:</td>
</tr>
<tr>
<td>Virtual device node:</td>
</tr>
<tr>
<td><strong>Secure restore:</strong></td>
</tr>
<tr>
<td>Scan restored disk for malware:</td>
</tr>
<tr>
<td>If malware is found:</td>
</tr>
</tbody>
</table>

- Power on target VM after disk is restored

To view the progress of the virtual disk restore operation, on the **Machines** tab, click **History**.
Running Failover Plans

This feature is not available for physical machine backups. If your infrastructure comprises machines running interdependent applications (for example, Exchange server and domain controller), it is reasonable to failover them one by one, as a group. To do this automatically, you can prepare a failover plan using Veeam Backup & Replication management console. This 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, please 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 Veeam Backup & Replication management console must be used.
To implement failover plan using Enterprise Manager, you need to log in using the administrative account or user account whose restore scope contains the machines from failover plan. Do the following:

1. Log in to Enterprise Manager using the appropriate account.

2. Go to the **Machines** tab and click **Failover Plan**.

3. In the **Failover Plan** window, select the necessary plan from the list, then specify the starting option you need.

   The following options are available for a failover plan:
   - **Start now** – use this option if you need to fail over to the replicas’ latest restore point.
   - **Start to most recent replica prior to** — use this option if you need to fail over to a certain restore point. For example, you may want your application server to failover to a state prior to the upgrade. In this case, for each machine participating in failover, Veeam will find the closest restore point (prior to the specified date and time) and fail over to it.
   - **Undo** — use this option to switch the workload back to source machines discarding the changes that were made to the replicas during failover.

4. Click **OK** and wait for the process to complete. You can examine session details in the **Machines > Restore sessions**.
Restoring Guest OS Files

Veeam Backup Enterprise Manager allows you to browse the guest OS file system in a machine backup, search for guest OS files and restore the necessary files. You can locate and restore files from the machine restore point created with or without guest OS file indexing.

IMPORTANT!

Veeam Backup 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.

If you have Veeam Agent for Microsoft Windows or Veeam Agent for Linux integrated with Veeam Backup & Replication, then you can use Veeam Backup Enterprise Manager to browse and restore guest OS files and application items from the physical machine backup stored in a Veeam backup repository. These processes involve appropriate backup job setup, as well as mount and data transfer operations.

When you restore files from the restore point created with machine guest OS file indexing enabled, Veeam Backup & Replication uses the following workflow:

1. To provide for browsing and search, Veeam 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 and/or restore the necessary file(s) and finish the restore session, machine disks will be unmounted.

When you restore files from the restore point that was created without machine guest OS file indexing, Veeam Backup & Replication uses the following workflow:

1. To provide for browsing, disks of the machine from the backup file are mounted to the Veeam backup server. If you then select to download the necessary files, Veeam will copy these files from the backup server to the destination location, using this mount point.
2. If you select to restore files from the backup to the original location on the production machine, an additional mount point will be created on the mount server associated with the backup repository storing the backup file.
3. If you restore files from replica, a single mount point for all these operations (browsing, download, restore to original location) will be created on the Veeam backup server.
4. After you download and/or restore the necessary files and finish the restore session, machine disks will be unmounted.
Preparing for File Browsing and Searching

If you already have Veeam Backup & Replication and Veeam Backup Enterprise Manager installed, you can use Veeam indexing capabilities to facilitate file browsing and search features:

1. Enable guest file system indexing on the Guest Processing step of the backup job wizard. For more information, see Configure Guest Processing Settings.
2. Run the backup job with guest file system indexing enabled.
3. Perform catalog replication. For more information, see Performing Catalog Replication and Indexing.

Alternatively, you can process the machine without guest file system indexing. Veeam Backup & Replication supports file-level restore not only for machines included in guest catalog, but also for those that were not indexed - for example, if indexing was disabled at restore point creation time, or if indexing operation failed. For such a machine, its selected restore point will be mounted to:

- A corresponding Veeam backup server (the one that manages the job processing this machine) — for Windows machines.
- A Linux appliance — for Linux machines.

Then a user will be able to locate the necessary file(s) or folder(s) 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, you need to 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 Linux Guest Files Search and Restore

To be able to view, search and restore machine guest files for Linux machines, you should take several preparatory steps as described below:

1. If you want to enable Linux guest files indexing, use the corresponding machine backup job options (Index everything, Index everything except, or Index only following folders option). For more information, see the Indexing Options section of this guide and the VM Guest OS File Indexing section of the Veeam Backup & Replication User Guide.

   Keep in mind that indexing is optional — you can browse and restore machine guest files from the restore points created without guest indexing. For more information, see Browsing Machine Backups for Guest OS Files and Performing 1-Click File Restore.

   **NOTE:**

   If you want Veeam Backup Enterprise Manager to display symbolic links to folders when browsing through the machine file system at 1-click file restore, then you should enable indexing in the backup job for that machine (running Linux or other non-Windows OS).

2. For proper Linux 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 will be prompted to deploy them to support index creation.

3. By default, guest files restore to the original location will be performed using the account specified in the corresponding machine backup job. If it does not have sufficient access to target machine, you will be prompted for the credentials. Specify user account and password 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.

Linux FLR Helper Appliance

To perform Linux machine guest files restore, FLR helper appliance should be configured on the corresponding Veeam backup server (one that controls the backup job processing selected machine). For details on FLR helper configuration, please refer to the Restoring VM Guest OS Files (Multi-OS) section of the Veeam Backup & Replication User Guide. These settings are saved in Veeam Backup & Replication database on per-user basis; they will be applied each time the certain user starts Linux file-level restore.

When Linux guest file-level restore is then started from Enterprise Manager, FLR helper configuration settings are obtained from the database of the corresponding Veeam backup server. If no FLR helper configuration is found for current user account, Veeam Backup & Replication will use default settings (those set during the latest FLR appliance configuration process in Veeam backup console). Thus, before starting Linux machine file-level restore from Enterprise Manager, make sure that Linux FLR helper settings had been configured on Veeam backup server.

   **NOTE:**

   If you plan to deploy multiple FLR helper appliances in order to restore Linux machines backed up by different Veeam backup servers, their initial configuration should be performed on the corresponding Veeam backup servers. Centralized configuration with 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 was backed up without guest indexing, click Mount. If the machine guest OS information was not 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 was 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 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 the **No Filter** link 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 and click **Apply**. You can define the following 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. 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 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 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 Security Settings.

**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 other non-Windows OS).
Restoring Files to Original Location

In this restore scenario, Veeam Backup Enterprise Manager will extract the file from the backup and restore it to the original production machine. Restoring guest OS files to the original location is the most secure file recovery method, as the user who initiates the file restore operation in the Veeam Backup Enterprise Manager web UI cannot access the file itself.

**IMPORTANT!**

This type of restore is only possible if the original machine is powered on and resides in the original location.

To restore a file to the original location:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. Multiple selection is also possible. For details, see Browsing Machine Backups for Guest OS Files or Searching Machine Backups for Guest OS Files.

2. Click **Restore** and select how to restore selected files:
   - If you select **Overwrite**, the file from the backup will replace the original file on the target machine.
   - If you select **Keep**, the file from the backup will be restored next to the original file on the target machine; the file from machine backup will have the *Restored* prefix in the file name.

3. In the displayed window, click **Yes**.

Veeam Backup Enterprise Manager will start the restore operation and display the progress and result of the operation in the **File Restore History** view.
IMPORTANT!

By default, guest files restore to the original location will be 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 will be 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 the file to be retrieved from the backup.

5. 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.

Restored files are stored in ZipDownload package named `FLR <date>_<time>.zip` by default in the **Downloads** folder. They are periodically cleaned up by Veeam Backup & Replication — files older than 24 hours are automatically deleted (built-in value).
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 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 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.
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's runtime process which performs guest system indexing and also identifies local administrative accounts. Communication with the self-service web page is performed using HTTPS or HTTP. In particular, such delegation capabilities and self-service web portal can be used in enterprise deployments to elevate the 1st line support to perform in-place restores without administrative access.

Considering the Limitations

**NOTE:**

Consider the following:

- This functionality is supported only in the Veeam Backup & Replication Enterprise Plus Edition.
- Self-Service File Restore Portal is available only for users of Microsoft Windows machines. For Linux-based machines, guest OS file restore is performed in the Veeam Backup Enterprise Manager UI under a user account configured in Enterprise Manager. For more information, see [Managing Accounts and Roles](#).
- Veeam Backup Enterprise Manager does not support guest OS files restore from storage snapshots. You can use Veeam Backup & Replication management console instead.

To provide a user account with the ability to access the Self-Service File Restore Portal UI and functionality, make sure the following prerequisites are met:

1. 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.
2. The account has local administrative rights for the required machine guest OS, local user rights are insufficient.

**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 corresponding 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:

- A Veeam backup server managing the corresponding job was not added to Enterprise Manager. For more information on how to add a Veeam backup server, see Adding Veeam Backup Servers.

- The recent backup job data has not been yet collected from a Veeam backup server (default time interval is every 15 min). For more information on how to run data collection manually, see Collecting Data from Backup Servers.

- The **Enable guest file system indexing** option was 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 can not 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.
Backup and Restore of Application Items

Veeam Backup Enterprise Manager supports item-level recovery from application-aware backups created by Veeam Backup & Replication. This capability can be helpful, for example, to restore operators at Help Desk, as well as other authorized personnel; corresponding settings and instructions are described in the sections that follow.
Backup and Restore of Microsoft Exchange Items

Restore personnel can be delegated the ability to recover the necessary Microsoft Exchange items (emails, tasks, calendars) from the Microsoft Exchange server machine backups. This functionality is provided in Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

**IMPORTANT!**

To be able to restore Microsoft Exchange items from the Veeam Backup Enterprise Manager UI, make sure Veeam Backup Enterprise Manager is installed on the domain member server from the Microsoft Active Directory forest in which Microsoft Exchange mailboxes are located.

Veeam supports restore from backups created with Veeam Backup & Replication version 8.0, 9.0 and 9.5.

Application item restore from storage snapshots via Enterprise Manager is not supported.
Preparing Application-Consistent Backup

To provide for recoverability of Microsoft Exchange items, make sure you have an application-consistent backup (with VSS enabled) of your Microsoft Exchange server machine created successfully.

To check and configure corresponding job settings, you can do the following in Veeam Backup Enterprise Manager:

1. Go to the Jobs tab and select your Exchange server backup job.
2. Click Job on the toolbar and select Edit to start the job wizard.
3. Proceed to the Guest Processing step of the wizard and make sure the Enable application-aware image processing check box is selected.
4. Click the Customize Application link. In the displayed window, select the Exchange server machine from the list and click Edit.
5. On the General tab, make sure that the Require successful processing option is selected in the Applications section.

```
<table>
<thead>
<tr>
<th>General</th>
<th>SQL</th>
<th>Oracle</th>
<th>File Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

1. Require successful processing (recommended)
2. Try application processing, but ignore failures
3. Disable application processing

Transaction logs processing

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

1. Process transaction logs with this job (recommended)
2. Perform copy only [lets another application use logs]
```
6. In the **Transaction logs processing** section, the **Process transaction logs with this job** option is selected by default.

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

8. In the **Guest OS credentials** section you can edit the account credentials under which guest OS will be accessed.
   - By default, for all machines in the job Veeam will use common credentials provided in the **Guest OS credentials** section — for that, you can select the account from the list, or click on the ‘+’ sign and select Windows (or Linux) OS. Then you will be prompted to enter user name and password for guest OS access. Click **OK** to save the settings and return to the **Guest Processing** page.
   - Alternatively, you can click the **Customize Credentials** link and then click **Set user**. Then you can specify custom guest OS credentials for the selected machine.

For more information on specifying guest OS access credentials, see **Guest OS Credentials**.

9. At the final step of the wizard, verify job schedule and click **Finish**.
Providing Access Rights

Users responsible for Exchange items restore should be assigned a security role in Enterprise Manager roles, with the corresponding options enabled. For that, use the **Microsoft Exchange items** check box in the **Add Role / Edit Role** window when you configure user access rights. For more information, see Configuring Security Settings.

The **Items** tab of Veeam Backup Enterprise Manager web UI will become available to these users after they log in to Enterprise Manager.
Next, go to the **Configuration > Settings > Directory Account** and specify Active Directory account that will be used to restore Exchange items. Make sure it has sufficient rights to access AD and mailboxes: *Exchange Administrator* rights and *Administrator* rights for all mailboxes are required.

To assign these rights, you can use Exchange impersonation or provide **Full Access**. For more information on the Exchange impersonation, see [Microsoft Docs](#).

After specifying the user name and password, click **Save**.
Restore Procedure

To restore a Microsoft Exchange item to the production Exchange Server, do the following:

1. Log on to Veeam Backup Enterprise Manager, using the account with the sufficient permissions. For more information, see Providing Access Rights.

2. Open the Items tab, then click Mailbox Items.

3. In the Username field, enter the account of Active Directory user whose mailbox will be restored, or use search to display the list of mailboxes currently existing in the production environment. You can click on the search icon to display all mailboxes of the forest, or enter search criteria. Veeam 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 corresponding VM backup or replica and its restore points.

4. In the Restore point field, select a restore point.

**NOTE:**

Consider the following:

- Restore points on tape are not supported (only those stored in repository can be used).
- Restore to another domain is supported within the same forest only.

5. In the Items section, select the type of item you want to restore:
   - Mail
   - Calendar
   - Contacts

You can select to Only restore missing items created or received during the certain time period; use the drop-down list to specify the period you need.

6. Click the Restore button. Items that meet specified conditions will be restored to the production Exchange Server.

To view item restore session information, click History.
NOTE:

Consider the following:

- You can use Veeam Backup Enterprise Manager to restore deleted items to the production mailbox only.
- If the specified mailbox does not exist in the machine restore point that you selected for restore, Veeam Backup Enterprise Manager will display an error message.
Backup and Restore of Microsoft SQL Server Databases

Authorized personnel can use Veeam Backup Enterprise Manager to restore the necessary SQL databases from Microsoft SQL Server machine backups.

**NOTE:**

This functionality is provided in the Enterprise and Enterprise *Plus* edition of Veeam Backup & Replication.

Veeam Backup Enterprise Manager supports restore from backups created with Veeam Backup & Replication version 8.0 and later.

Database restore from storage snapshots with Veeam Backup Enterprise Manager is not supported.
Preparing Application-Consistent Backup

To provide for recoverability of SQL database, make sure you have an application-consistent backup (with VSS enabled) of your SQL server machine created successfully. Also, if you plan to restore the database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then transaction log processing should be configured, as described below, as well as in the Veeam Backup & Replication User Guide.

To configure corresponding job settings, you can do the following in Enterprise Manager:

1. Go to the **Jobs** tab and select your SQL server backup job.
2. Click **Job** on the toolbar and select **Edit** to start the job wizard.
3. Proceed to the **Guest Processing** step of the wizard and make sure the **Enable application-aware image processing** check box is selected.
4. Click the **Customize Application** link. In the displayed window, select the SQL server machine from the list and click **Edit**.
5. On the **General** tab, make sure the **Require successful processing** option is selected in the **Applications** section.
6. To be able to specify transaction log handling options, make sure the **Process transaction logs with this job** option is selected. Otherwise, if you select the **Perform copy only** option, Veeam Backup & Replication will create a copy-only backup, and transaction logs will not be purged — that is why the **SQL** tab with log handling settings will be deactivated in this case. For more information, see the Microsoft SQL Server Transaction Log Settings section of the Veeam Backup & Replication User Guide.
7. Open the **SQL** tab and specify how SQL transaction logs will be handled:

   - Select **Truncate logs** if you want Veeam Backup & Replication to trigger truncation of transaction logs only after the job is finished successfully. If truncation of transaction logs is not possible for some reason, the logs will remain untouched in the machine guest OS until the next start of the Veeam runtime process responsible for application-aware processing.

   - Select **Do not truncate logs** if you do not want Veeam Backup & Replication to truncate logs at all.

   - Select **Backup logs periodically** if you need to backup transaction logs of SQL server machine, storing them to backup repository next to server backup. After transaction logs are placed to repository, they will be truncated on guest. With this option selected, you should also specify how often Veeam will process these transaction logs, uploading them to repository. To set the processing frequency, enter the required value in the **Backup logs every <N> minutes** field (default is every 15 minutes).

The last option allows you to restore the SQL database to a selected restore point or to a selected point in time, using Enterprise Manager. Restore to specific transaction can be performed using Veeam backup management console. For more information, see the Microsoft SQL Server Transaction Log Settings sections of the Veeam Backup & Replication User Guide.
**IMPORTANT!**

Consider the following:

- If you select the **Do not truncate logs** option, make sure the recovery model for the necessary databases on the SQL server is set to simple (otherwise, logs may drastically increase in size).

- For the **Backup logs periodically** option to take effect, you should ensure that full or bulk-logged recovery model is turned on for the required databases on the SQL server machine. If recovery model is set to simple, no transaction logs will be backed up. If full model is enabled but neither **Backup logs periodically** nor **Truncate logs** option is selected, then logs will increase in size and occupy disk space.

![srv04: Processing Settings](image)

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

**Backup logs every** 15 minutes

**Retain log backups:**

- **Until the corresponding image-level backup is deleted**
- **Keep only last** 15 days
8. If you selected to back up transaction logs, specify how long they should be kept using options in the **Retain log backups** section.

**IMPORTANT!**

It is recommended to keep logs **Until the corresponding image-level backup is deleted**; otherwise, you must manually check and ensure that your database and log backup retention policies are consistent, providing all the machine restore points and log backups required for database restore.

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

10. At the **Job Schedule** step of the wizard, make sure the schedule is enabled for the job. Otherwise, log backup will not be activated.

11. Click **Finish**.
Providing Access Rights

Users responsible for SQL database restore should be assigned an Enterprise Manager role with the corresponding option enabled. To allow for database restore, select the **Microsoft SQL Server databases** check box in the Add Role / Edit Role window.

If necessary, select the **Deny in-place database restores** check box.

The **Items** tab will become available to these users after they log in to Enterprise Manager.

For more information on how to configure user access rights, see Configuring Security Settings.
Restore Procedure

To restore a Microsoft SQL Server item, a user should do the following:

1. Log on to Veeam Backup Enterprise Manager using an account with the sufficient permissions. For more information, see Providing Access Rights.

2. Go to the **Items** tab and click **SQL Database**.

3. Enter a name of SQL Server hosting the database you need to restore; use the `server_name\instance_name` format. Alternatively, click the **Pick from List** link to select from the list of available SQL Server machine backups.

4. The list of available databases will be displayed. Select the database you need. Consider that user credentials for carrying out the restore procedure via Enterprise Manager will be picked as follows:
   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the SQL Server machine.
   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), user will be prompted to provide the necessary credentials.

**NOTE:**

For more information on the account roles in Veeam Backup Enterprise Manager that allow the user to restore SQL databases, see Providing Access Rights.

5. Perform restore following the required scenario. For information on the possible restore scenarios, see 1-Click Restore to Original Location and Restore with Custom Settings.
Scenario 1: 1-Click Restore to Original Location

This scenario allows you to restore the selected database to the latest available state back in the original location. For that, make sure the Original location option is selected in the Restore to section and click Restore.

When you restore database items to the original location, Enterprise Manager selects user credentials for the restore procedure according to the following rules:

a. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the SQL Server machine.

b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), the Enterprise Manager user will be prompted to provide the necessary credentials.

**NOTE:**

For more information on the account roles in Veeam Backup Enterprise Manager that allow a user to restore SQL databases, see Providing Access Rights.

When performing database restore to the original location, a temporary iSCSI connection is established between the target SQL server (it acts as an iSCSI initiator) and mount server associated with the backup repository (it acts as an iSCSI target). For that, Veeam opens a TCP port from the port range 3260-3270; it closes this port after restore session is over.

**NOTE:**

If you restore a database that belongs to an AlwaysOn Availability Group, this database will be restored to the original server and added to the corresponding Availability Group.
Scenario 2: Restore with Custom Settings

Alternatively, you can carry out the restore procedure with custom settings, specifying the restore point and destination location you need. Do the following:

1. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date.

2. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relatively to the currently selected SQL server restore point):
   - **Beginning** — refers to the previous restore point of the SQL Server machine that contains the selected database backup. If the previous restore point (server backup) was not found, or the database backup does not exist in it, then **Beginning** will refer to current restore point.
   - **End** — refers to the next restore point which contains the selected database backup. If the next restore point (server backup) and the corresponding transaction log backup were not found, or if the database backup does not exist in the server backup, then **End** will refer to the current restore point. If the next restore point (server backup) was not found, but the transaction log backup exists for the preceding period, then **End** will refer to the latest log backup time.

**NOTE:**

For more information on the transaction log backup, see Microsoft SQL Server Logs Backup and Restore section of the Veeam Backup & Replication User Guide.

3. In the **Restore to** section, select the **Alternative location** option.

4. Click **Restore**.
5. At the **Target Server** step of the wizard, specify settings to connect to the target server and database:

   a. In the **Target Server** section, enter the name of the target database in the `SERVER\DATABASE` format and credentials of the account that will be used to connect to the target server.

   b. If you want to use a separate account for connection to the target database, in the **Target Database** section, select the **Use the following credentials to access the database** check box and specify credentials of the necessary account.

   c. If you want to use SQL Server authentication when connecting to the database, select the **Use SQL Server authentication** check box.
6. If AlwaysOn Availability Groups are present on the target server, at the **SQL Server Always On** step of the wizard, you can add the restored database to an Availability Group.

![SQL Restore Interface]

**Specify Always On cluster restore parameters**

- **Add database to the following Availability Group:**
  - AON1

**Database will be replicated to the following nodes:**

- **Primary**
  - SQLSRV031VEEAMSQL2012

- **Secondary**
  - SQLSRV031VEEAMSQL2012_2
  - SQLSRV031VEEAMSQL2012_3
7. At the **Files** step of the wizard, you can specify paths to database files on the target server. You can specify separate target locations for the primary database file and secondary database file with logs.

<table>
<thead>
<tr>
<th>SQL Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Server</strong></td>
</tr>
<tr>
<td><strong>Files</strong></td>
</tr>
<tr>
<td>Primary database file</td>
</tr>
<tr>
<td>Secondary database and log files</td>
</tr>
</tbody>
</table>

8. Click **Finish**. Veeam Backup Enterprise Manager will start the restore operation and display the status of the restore process on the **Items** tab.
Backup and Restore of Oracle Databases

Authorized personnel can use Veeam Backup Enterprise Manager to restore the necessary databases from Oracle Server machine backups.

**NOTE:**

This functionality is provided in the Enterprise and Enterprise *Plus* edition of Veeam Backup & Replication.

Veeam Backup Enterprise Manager supports restore from backups created with Veeam Backup & Replication versions 9.0 and later.

Database restore from storage snapshots via Enterprise Manager is not supported.
Preparing Application-Consistent Backup

To provide for recoverability of Oracle database, make sure you have an application-consistent backup of your Oracle server machine created successfully. For more information on an application-consistent backup, see Application-aware Image Processing Settings. Also, if you plan to restore the database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then log processing should be configured, as described below.

To configure corresponding job settings, you can do the following in Enterprise Manager:

1. Go to the Jobs tab and select your Oracle server backup job.
2. Click Job on the toolbar and select Edit to start the job wizard.
3. Proceed to the Guest Processing step of the wizard and make sure the Enable application-aware image processing check box is selected.
4. Click the Customize Application link. In the displayed window, select the Oracle server machine from the list and click Edit.
5. On the General tab, make sure the Require successful processing option is selected in the Applications section.
6. To be able to specify transaction log handling options, make sure the Process transaction logs with this job option is selected. Otherwise, if you select the Perform copy only option, Veeam Backup & Replication will create a copy-only backup, and Oracle archived logs will not be deleted — that is why the Oracle tab with log handling settings will be deactivated in this case. For more information, see the Oracle Archived Log Settings section of the Veeam Backup & Replication User Guide.
IMPORTANT!

If both Microsoft SQL Server and Oracle are installed on one machine, and this machine is processed by a job with log backup enabled for both applications, Veeam Backup & Replication will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.

7. Open the Oracle tab and specify how archived logs will be handled:

a. Specify a user account that will connect to Oracle system and perform Oracle archived logs backup and/or deletion. You can select Use guest credentials — then Veeam will use the account specified for guest processing in the job configuration for both guest OS access and for connection to the Oracle system. You can also specify another account. To do this, select the necessary account from the drop-down list or click Add and add a new account. In any case, make sure the account you specify has sufficient rights. For details, see the Required Permissions section in the Veeam Explorer for Oracle guide.

b. Specify whether archived logs should be deleted on the Oracle server machine, and whether Veeam should back them up them to repository. Veeam Backup & Replication supports the following options:

- **Do not delete archived logs** — this option instructs Veeam to preserve archived redo logs (if any) on the original Oracle server. With this option selected, your database administrator will have to take care of database logs. Applicable restore scenario — database restore to the state as of the currently selected machine restore point, to the selected point in time and to the selected transaction.
- **Delete logs older than <N> hours / Delete logs over <N> GB** — with this option selected, Veeam will wait for the image-level machine backup to complete, and then it will trigger archived log deletion from guest, using the specified condition (log age or size). If archived logs cannot be deleted for some reason, these logs will remain untouched in the guest machine until the next start of the Veeam runtime process.

- With any of these options, you can also use the **Backup logs every <N> minutes** check box. If you select this check box, Veeam Backup & Replication will periodically ship archived logs to the backup repository and store them next to the Oracle server machine backup. Make sure that Oracle ARCHIVELOG mode is turned on (contact your database administrator, if necessary). This option will support any database restore scenario: to the state as of in currently selected machine restore point, to any point in time or to the state before particular transaction.

**IMPORTANT!**

If you plan to use this option together with archived logs deletion from Oracle machine guest, make sure that these settings are consistent: logs should be deleted after they are backed up to repository, not vice versa. Thus, you need to set up backup schedule and log removal conditions appropriately. Default log backup interval is 15 minutes, maximum interval is 480 minutes.

---

**srv04: Processing Settings**

**Oracle**

**Choose how this job should process Oracle archived logs**

Specify Oracle account with SYSDBA privileges:

- Use guest credentials

**Retain log backups:**

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

---

**General**

- Do not delete archived logs
- Delete logs older than: 24 hours
- Delete logs over: 10 GB
- Backup logs every: 15 minutes

**SQL**

- Add

**File Exclusions**

**OK**  **Cancel**
8. If you selected to back up archived logs, specify how long they should be kept using the **Retain log backups** options.

**IMPORTANT!**

It is recommended to keep logs **Until the corresponding image-level backup is deleted**; otherwise, you should manually check and ensure that your database and log backup retention policies are consistent, providing all the machines restore points and log backups required for database restore.

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

10. At the **Job Schedule** step of the wizard, make sure the schedule is enabled for the job. Otherwise, log backup will not be activated.

11. Click **Finish**.
Providing Access Rights

Users responsible for Oracle database restore should be assigned an Enterprise Manager role with the corresponding option enabled.

To allow users with Restore Operator or Portal User role to restore Oracle databases:

1. In the Add Role / Edit Role window, select the Databases check box.
2. Select the Oracle databases check box.
3. [Optional] If necessary, select the Deny in-place database restores check box.
4. Click OK.

The Items tab will become available to these users after they log in to Enterprise Manager.

For more details on role assignment, see the Configuring Security Settings section.
Restore Procedure

To restore a database item, a user should do the following:

1. Log on to Veeam Backup Enterprise Manager, using the account with the sufficient permissions. For more information, see the Providing Access Rights.

2. Go to the Items tab and click Oracle Database.

3. Enter the name of Oracle server hosting the database you need to restore. Alternatively, click the Pick from List link to select from the list of available Oracle server machine backups.

4. Select Oracle home and the database you need. Consider that user credentials for carrying out the restore procedure via Enterprise Manager will be picked as follows:
   
   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Oracle server machine, or the account which is currently logged in.
   
   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on Windows server, then you may need to enter password for Oracle home.

   **NOTE:**

   The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see Providing Access Rights.

5. Perform restore following the required scenario. For information on the possible restore scenarios, see Scenario 1: 1-Click Restore to Original Location and Scenario 2: Restore with Custom Settings.

   To view restore session log, click History.
Scenario 1: 1-Click Restore to Original Location

This scenario allows you to restore the selected database to the latest available state back in the original location. For that, make sure the **Original location** option is selected in the **Restore to** section and click **Restore**.

When performing database restore to the original location, a temporary iSCSI connection is established between the target Oracle server (it acts as an iSCSI initiator) and mount server associated with the backup repository (it acts as an iSCSI target). For that, Veeam opens a TCP port from the port range 3260-3270; it closes this port after restore session is over.
Scenario 2: Restore with Custom Settings

Alternatively, you can carry out the restore procedure with custom settings, specifying the restore point and destination location you need. Do the following:

1. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date.

   - **Beginning** — refers to the previous restore point of Oracle server machine that contains selected database backup. If the previous restore point (server backup) was not found, or the database backup does not exist in it, then **Beginning** will refer to current restore point.
   
   - **End** — refers to the next restore point which contains selected database backup. If the next restore point (server backup) and corresponding transaction log backup were not found, or if the database backup does not exist in the server backup, then **End** will refer to the current restore point. If the next restore point (server backup) was not found, but transaction log backup exists for the preceding period, then **End** will refer to the latest log backup time.

2. If you backed up archived redo logs for the database, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relatively to the currently selected Oracle database restore point):

   - **Beginning** — refers to the previous restore point of Oracle server machine that contains selected database backup. If the previous restore point (server backup) was not found, or the database backup does not exist in it, then **Beginning** will refer to current restore point.
   
   - **End** — refers to the next restore point which contains selected database backup. If the next restore point (server backup) and corresponding transaction log backup were not found, or if the database backup does not exist in the server backup, then **End** will refer to the current restore point. If the next restore point (server backup) was not found, but transaction log backup exists for the preceding period, then **End** will refer to the latest log backup time.

**NOTE:**

For more information on log backup, see Preparing and Application-Consistent Backup.
3. To specify a location where you want to restore the database items, select the necessary option in the **Restore to** section:

   - If you want to restore items to the original database, select **Original location**. If you select this option, consider that Enterprise Manager will select user credentials for the restore procedure according to the following rules:
     
     i. Veeam Backup Enterprise Manager will try to use the account specified in the backup job that contains the Oracle server machine or the account which is currently logged in.
     
     ii. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on a Microsoft Windows server, you may need to enter password for the Oracle home.

   **NOTE:**

   The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see [Providing Access Rights](#).

   - If you want to restore items to another database, select **Alternative location**. If you select this option, you will need to specify restore settings using the **Oracle Restore** wizard. For details, see [Using Oracle Restore Wizard](#).

4. Click **Restore**.

   - In case of restore to the original location, the restore process will start immediately.
   
   - In case of restore to another location, Enterprise Manager will launch the **Oracle Restore** wizard. For more information, see [Using Oracle Restore Wizard](#).

---

**Using Oracle Restore Wizard**

If you restore Oracle database items to another location, specify restore settings using the **Oracle Restore** wizard:
1. At the **Target Server** step of the wizard, specify settings to connect to the server where the database should be restored:

   1. For database restore on a Microsoft Windows server, specify connection settings in the following way:

      i. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Microsoft Windows server.

      ii. In the **Account** and **Password** fields, specify credentials of the account that will be used for connection with the target Windows-based Oracle server. Make sure the account has the **sysdba** rights on that server (Windows authentication will be used). To be able to copy archived logs from backup to the target server for further replay (in case of restore to certain point in time), the account should be also granted sufficient permissions to access the administrative share on that machine (for example, `\myserver\C$`): **Read** and **Write** are minimum required, **Full Control** recommended.

以下是Oracle Restore界面的截图，显示了设置的输入字段：

**Oracle Restore**

**Specify credentials for the target Windows server**

- **Target server**
  - DNS name or IP address: `serv45.tech.local`

- **Specify account to connect to the server with**
  - Account: `serv45Administrator`
  - Password: `***********`
For database restore on a Linux server, specify connection settings in the following way:

i. Server name (or IP address) and SSH port — default port is 22.

ii. Account to be used to access the server. This should be a root account or account elevated to root and added to the sudoers file. To elevate the account and add it to the sudoers file, click Settings and use the corresponding options.

You can use authentication by a user name and password or by a private key.

4. At the Oracle step of the wizard, select Oracle Home and specify Global database name and Oracle SID where to restore the database from backup.

Consider that if database with the specified Oracle SID exists on the target Oracle home, the restore process by design will delete it and replace with the database from backup. Thus, before starting the restore process, a message will be displayed, asking you to confirm the operation.

<table>
<thead>
<tr>
<th>Oracle Restore</th>
<th>Specify Oracle home settings for the target server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Server</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Home: OraDB12Home1</td>
</tr>
<tr>
<td>Database Files</td>
<td>Global database name: orcltech.local</td>
</tr>
<tr>
<td></td>
<td>Oracle SID: orcl</td>
</tr>
</tbody>
</table>

Previous  Next  Cancel
5. At the **Database Files** step of the wizard, specify paths to database files on the target server.

6. Click **Finish**. Veeam Backup Enterprise Manager will start the restore operation and display the status of the restore process on the **Items** tab.
Managing Encryption Keys

The concept, terms and procedures of data encryption and decryption are described in detail in Veeam Backup & Replication User Guide. Being a part of the process, Enterprise Manager keys help you to restore encrypted data in case of lost or forgotten password used for encryption. During Enterprise Manager installation, the setup automatically generates a new keyset containing a public Enterprise Manager key and a private Enterprise Manager key.

NOTE:

To work with Enterprise Manager keysets, make sure the Enable encryption password loss protection check box is selected in the Configuration > Settings > Key Management section.
Generating Enterprise Manager Keyset

For safety's sake, it is recommended to periodically generate new Enterprise Manager keys that should be used in the encryption process. Regular change of encryption keys raises the encryption security level.

When you create new Enterprise Manager keys, Veeam Backup Enterprise Manager generates a keyset of two matching keys:

- Public Enterprise Manager key.
- Private Enterprise Manager key.

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 create a new keyset of 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, 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:

- Public Enterprise Manager key encrypts storage keys on Veeam 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.

After you create a new keyset, you need to activate it. As a result of activation, Veeam Backup Enterprise Manager performs the following actions:

- Public Enterprise Manager key is propagated to all Veeam backup servers connected to Veeam Backup Enterprise Manager.
- Private Enterprise Manager key remains on Veeam Backup Enterprise Manager and marked as active.

You can activate a keyset manually. For that, do the following:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select an inactive keyset in the list and click **Activate**.

Note that manual activation can be performed for any keyset in the list (generated manually or automatically).

If you want your automatically generated keysets to be activated automatically upon creation, then you should configure the retention policy settings. For more information, see **Specifying Retention Settings for Enterprise Manager Keyset**.

**NOTE:**

Consider that manually generated keysets will require manual activation.
Specifying Retention Settings for Enterprise Manager Keyset

In some cases, government regulations and internal company policies require that you regularly change encryption keys. The shorter is the lifetime of an encryption key, the smaller amount of data is encrypted with this key and the higher is the level of encryption security.

Lifetime of Enterprise Manager keys is controlled by a key retention period. The key retention period defines for how long Enterprise Manager keys must remain in effect and must be used for encryption and decryption.

You can specify a retention period for an Enterprise Manager keyset.

To specify retention policy for Enterprise Manager keys:

1. In Veeam Backup Enterprise Manager, open the Settings section of the Configuration view.

2. On the Key Management tab, in the Managed keys section, select the necessary options:
   - If you want to set a retention period for Enterprise Manager keysets, select the Key retention period check box and specify the number of weeks for which Enterprise Manager keys must remain in effect (default is 4 weeks). After the retention period is over, and with key auto-generation is turned off, a user will receive a notification email and should then manually create and activate a new keyset. After a new keyset is ready, old keyset is marked as inactive.
   - If you want Veeam Backup Enterprise Manager to automatically generate a new keyset, select the Auto-generate new keys check box. After the current keyset expires, Veeam Backup Enterprise Manager will automatically generate a new keyset and mark it as active. During the next data synchronization session, Veeam Backup Enterprise Manager will propagate the newly created public Enterprise Manager key to all connected Veeam backup servers. The private Enterprise Manager key will remain on Veeam Backup Enterprise Manager and will be used for data decryption.

3. Click Save to save the settings.
Exporting and Importing Enterprise Manager Keyset

It is important to regularly back up your Enterprise Manager keys or save their copies in a safe place. If you lose a password for an encrypted backup or tape, you can unlock this backup or tape with the private Enterprise Manager key and the Enterprise Keys Restore wizard.

However, in some situations, a matching private Enterprise Manager key may be not available. This can happen, for example, if your Veeam Backup Enterprise Manager database has failed or you use a new installation of Veeam Backup Enterprise Manager and a new database. In this case, Veeam Backup Enterprise Manager will not find a matching private Enterprise Manager key in the database and will be unable to unlock the backup or tape encrypted with the public Enterprise Manager key.

You can create a backup copy of an Enterprise Manager keyset with the export operation in Veeam Backup Enterprise Manager. The exported keyset is saved as a file of .PEM format and contains private and public Enterprise Manager keys. You can save the exported keyset on the local disk or on a network share. An exported keyset can be imported back to Veeam Backup Enterprise Manager any time you need.

To export a keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select a keyset you want to back up and click **Export**.
3. Save the resulting .PEM file on the local disk or in a network shared folder.

To import a previously exported keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, click **Import**.
3. Click **Browse** next to the **File** field and select a previously exported keyset.
4. In the **Hint** field, Veeam Backup Enterprise Manager displays a hint that you provided when creating the imported keyset.
5. Click **Import**.
When you import a keyset, it is saved to the Veeam Backup Enterprise Manager database and displayed in the keyset list in Veeam Backup Enterprise Manager.

**NOTE:**

An imported keyset has the Inactive state. You must activate it to be able to use the keys from the keyset for backup encryption (for restore procedures, activation is not necessary). For more information, see Activating Enterprise Manager Keyset.
Deleting Enterprise Manager Keyset

You can delete an Enterprise Manager keyset in case it is no longer needed.

Only keys in the **Inactive** state can be deleted. You cannot delete keys that are currently active.

To delete a keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select the necessary keyset in the list and click **Delete Key**.

**IMPORTANT!**

It is strongly recommended that you export a keyset before you delete it. If you delete a keyset and do not make its backup copy, you will not be able to restore data from a backup or tape encrypted with keys from this keyset in case a password is lost. For more information, see **Exporting and Importing Enterprise Manager Keyset**.
Handling Password Recovery Requests

When an encrypted backup file or tape media is imported to the Veeam backup server, a password is required to decrypt data. In some cases, however, a password can be lost or forgotten. Veeam Backup & Replication offers a way to restore data from encrypted backups or tapes even if a password is not available. For that, Veeam Backup Enterprise Manager Administrator runs the Password Recovery wizard within the following context:

1. As a Veeam Backup Enterprise Manager Administrator, you receive a request for password restore, for example, via 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, via 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, the corresponding public key will be deleted from the Enterprise Manager database.
- If a new configuration database is created on Veeam backup server, then a new public key will be automatically generated for that Veeam backup server on Enterprise Manager, replacing its existing key.

For details on Enterprise Manager keysets, encryption passwords and password restore, see the Data Encryption section of the Veeam Backup & Replication User Guide.
Working with Virtual Lab Requests

The Requests tab allows you to create, approve and reject virtual lab requests, as well as prolong the time of virtual lab running which are part of the U-AIR process. The corresponding procedures are described in the following sections:

- Creating Virtual Lab Requests
- Approving Virtual Lab Requests

For detailed information, see Veeam Universal Application Item-Level Restore User Guide.
Creating Virtual Lab Requests

Users with *Portal Administrator* Enterprise Manager role assigned can create Virtual Lab requests directly from Enterprise Manager web UI. For that:

1. Log in to Veeam Backup Enterprise Manager using administrative account
2. Go to the **Requests** tab.
3. Click the **Create** link in the top left corner.
4. Veeam Backup Enterprise Manager will launch the **New Lab Request** wizard. At the **Lab Request** step of the wizard, specify the required virtual machine name or IP address and other request settings. By default, lab usage duration is 30 minutes. If necessary, change this value. Optionally, supply the description for your request.

![New Lab Request Wizard](image)
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).

<table>
<thead>
<tr>
<th>Machine</th>
<th>Backup server</th>
<th>Type</th>
<th>Restore points</th>
</tr>
</thead>
<tbody>
<tr>
<td>serv45</td>
<td>srv12.tech.local</td>
<td>Backup</td>
<td>5</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>New Lab Request</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lab Request</strong></td>
</tr>
<tr>
<td><strong>Backup</strong></td>
</tr>
<tr>
<td><strong>Restore Point</strong></td>
</tr>
<tr>
<td><strong>SureBackup Job</strong></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
</tbody>
</table>

Select date and time to restore machine to

- **Backup date**
  - 11/25/2019 01:06:51 pm
  - 11/25/2019 01:03:02 pm

- **Show all available restore points**
7. At the **SureBackup Job** step, select one of existing SureBackup jobs that you want to run to create an isolated sandbox in which the selected machine should be started. The application group and virtual lab used by this SureBackup job will be displayed in the **Selected Job details** section.

By default, the list of jobs displays only those jobs that contain the selected machine. If you want to display all SureBackup jobs that were created, select the **Show all available SureBackup jobs** check box.
8. At the **Summary** step, review the settings you have configured for the virtual lab and click **Finish**. Veeam Backup & Replication will perform verification of the selected restore point.

The request will be added to the list of requests and wait for authorized administrator’s approval.
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, Enterprise Manager **Portal Administrator** role is required.

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.

8. An 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 management console, and right-click the necessary SureBackup job and select **Start job to** from the shortcut menu.

   If the SureBackup job is not running, Enterprise Manager will launch the selected SureBackup job, start the virtual lab and run the machine with the necessary application to the restore point selected.
Working with VMware vCloud Director

Veeam Backup & Replication supports VMware vCloud Director, allowing users to back up and restore single VMs, vApps, Organization vDC and whole Organizations. Service providers have an ability to allow self-service restore operations to their customers via friendly and convenient web UI based on Veeam Backup Enterprise Manager.

- Administrators on service providers side are granted administrative rights for Enterprise Manager. Thus, they have access to Configuration view in its web UI where they can configure vCloud Director organization settings (on the vCloud tab), including repository quota and backup job template. As a rule, these administrators also have access to Veeam Backup & Replication management console, controlling vCloud Director as part of backup infrastructure on the provider side.

- Users on the tenant side do not need administrative rights for Enterprise Manager — instead, they get access to the Veeam Self-Service Backup Portal. There they can manage their vCloud Director jobs, as well as restore VMs, files and application items within their scope. As a rule, these users are vCloud Director administrators in charge of data protection in their vCloud Director Organizations.

Supported Configurations

The VMware vCloud Director machines must meet system requirements. For more information, see System Requirements.

**IMPORTANT!**

1. Make sure that you have only one vCloud Director server in Veeam Backup Enterprise Manager. (If you have several Veeam backup servers added to Enterprise Manager, check that these Veeam backup servers have the same vCloud Director server in their backup infrastructures.)

2. Consider that if you have a vCloud Director server included in the backup infrastructure with version earlier than 9.5, that server will not be supported.
How It Works

Veeam leverages the native vCloud Director authentication technology to authorize users to 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 on provider side, as now a tenant only needs to be configured once in vCloud Director, and then any change like a new password or a 'Disable' operation will be immediately reflected in Veeam Enterprise Manager.

What Administrators on the Provider Side Can Do?

As for the service providers, the administrators on that side can perform the following operations, as described later in this chapter:

- Configure settings for the tenants (vCloud Director Organizations), including backup job templates to be used, backup destination and repository quota.
- Apply restrictions to particular tenant users’ ability to schedule the jobs, for example, preventing 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’s built-in load balancing, these capabilities allow administrators to ensure infrastructure is protected from excessive resource consumption.
What Users on the Tenant Side (vCloud Director Organization Administrators) Can Do?

Once such users log in to Veeam Backup Enterprise Manager using their vCloud Director credentials, Veeam identifies the resources included in their scope — that is, entities such user is allowed to see and manage - and automatically filters vCloud Director objects when displaying them. These tenant-side users then can perform the following operations, as described later in this chapter:

- Create new backup jobs for the objects in their scope, based on the pre-defined templates. Tenant users are allowed to configure essential job settings (such as VMs to backup, retention, schedule, notifications, and guest OS processing options).
- Modify or delete the jobs.
- Enable or disable the jobs.
- Start, stop, retry the jobs.
- View statistics on vCloud Director backups.
- Restore vCloud 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 the tenant-side users, advanced job parameters (like backup mode and repository settings) are automatically populated from the job templates. These templates are assigned by administrator on service provider side to the particular tenant.
Managing vCloud Director Organizations

Starting with Veeam Backup & Replication 9.5, you can empower administrators of VMware infrastructure to configure vCloud Director organization settings for the vCloud Director deployed in their environment, using Enterprise Manager web interface. For that, log in to Enterprise Manager with administrative account and take the following preliminary steps:

1. Add a vCloud Director server to backup infrastructure on Veeam backup server, as described here.
2. Add this Veeam backup server to Veeam Backup Enterprise Manager, as described here.
3. Wait for scheduled data collection to complete, or run data collection from that Veeam backup server manually, as described here.
4. Make sure the account that will be used to control vCloud Director organization settings was assigned Portal Administrator role in Enterprise Manager, as described here.

If these prerequisites are met, the vCloud tab will be displayed in the Configuration view of the Enterprise Manager web UI.

Including a vCloud Director organization in this list (except for default organization) means that its configuration is individual, different from default. Vice versa, for all organizations that do not appear in this list, default configuration settings will be applied. See the Configuring vCloud Director Organization Settings section for details.

As Veeam Backup Enterprise Manager administrator, you can perform the following actions on this tab:

- Specify a new configuration for vCloud Director organization, applying custom settings.
- Modify current vCloud Director organization settings.
- Remove vCloud Director organization from the list of managed configurations with custom settings - after that, default settings will be applied to this organization.
Configuring vCloud Director Organization Settings

To configure vCloud Director organization settings:

1. Log in to the Enterprise Manager web UI using the administrative account.

2. Click **Configuration** and select **Self-service** view on the left. On the **vCloud** tab, you will see the list of vCloud Director organization configurations that you can manage.

3. By default, initially a sample organization is created and displayed in the preview pane on the right. It has the following settings:
   - **Organization** – *Other vCloud organizations*
   - **Repository** – repository server from backup infrastructure that has the maximum free space
   - **Quota** – default value is 1 TB

   These settings will be applied to all vCloud Director organizations without individual settings, that is, for those not included in this list of managed configurations. vCloud Director backup job settings for such organizations will be copied from default job settings as they are shown in the Veeam backup console. For more information, see the Veeam Backup & Replication User Guide. By default, the sample organization is inactive (the **Repository** column contains *Disable self-service backup for other organizations* value). For more information on modifying the sample organization configuration, see **Modifying vCloud Director Organization Settings**.

4. Click **Add** to add a new configuration.

5. In the displayed window, select the **Organization** from the list of those available to you. These are vCloud Director organizations from vCloud Director servers processed by Veeam backup servers that are added to Enterprise Manager.

6. Assign the **Repository** that will be used by organization VMs. The list includes repositories configured for managed Veeam backup servers.
IMPORTANT!

Consider that you cannot assign cloud-based repositories, as well as NetApp or Nimble storage systems storing snapshots created by Veeam snapshot-only jobs.

7. Specify repository storage **Quota** that will be applied. You can choose GB or TB from the drop-down list and enter the required quantity.

8. Select how **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.
     Make sure that the backup window is configured within the Enterprise Manager UI and not within the Veeam Backup & Replication backup job settings. For more information on the backup window configuration, see **Customizing Dashboard Appearance**.
   - **Deny**: Creates job with no schedule assigned.

For more information on job scheduling, see **Schedule the Job**.
9. You can click **Show Advanced Job Settings** link to specify what backup job will be used as a template for vCloud Director organization VMs processing. Then select the backup job which settings will be copied and used as a template - for that, use the **Copy from** list:

- **Default job settings** — backup job will be configured with the standard default vCloud Director backup job settings as they are shown in the Veeam backup console. For more information, see the [Veeam Backup & Replication User Guide](#).

- **<job_name>** — select the vCloud Director backup job from which settings will be obtained. When finished, click **Apply**.

   ![Add Job Settings](image)

**IMPORTANT!**

Backup repository settings specified for organization at step 6 (global settings) will take priority over those prescribed by selected job template.

10. If you do not use the **Show Advanced Job Settings** link, default job settings will be applied to template.

**NOTE:**

To populate the list of job templates, you need at least one vCloud Director backup job to be configured in Veeam backup console.

11. Click **Save** to save configuration.

Also, as an Enterprise Manager administrator, you can modify existing settings or remove the organization from the list of managed configurations.
Report on vCloud Organization Configuration

To download a report on configuration of vCloud Director organizations, click Export. The report will be saved to the excelreport file in the default location (local Downloads folder). This report includes information on existing organizations with configuration different from default, and organizations that have default configuration with assigned repository quota. (Thus, sample organization named Other vCloud organizations will not be included in the report.)

NOTE:

Make sure proper connection is established between Veeam backup server and Enterprise Manager, otherwise changes in the list of managed configurations will not be stored in the Veeam configuration database, and vCloud Director infrastructure in Veeam management console will not reflect the updates.
Modifying vCloud Director Organization Settings

To modify vCloud Director organization settings:

1. On the vCloud tab, select the organization you need and click Edit.

2. Edit the organization settings as necessary. If you want to display job settings applied to backup jobs for this organization, click Show advanced job settings in the window:
   - In the Advanced job settings section you can examine existing job configuration.
   - In the Copy from field you will see the name of a vCloud Director job previously selected as a template for this organization.

3. To change the job that should be used as a template from that point forward, from the Copy from list select the job you need and click Apply.
Considerations and Limitations

Consider the following recommendations for modifying organization settings:

- If you plan to modify job template for the selected vCloud Director organization, remember that new settings will be applied only to the new jobs created for that organization; existing jobs will not be affected.

- If you need to enable and modify sample configuration, then you should make sure that it does not have default repository setting — for that, from the list of repositories select the value different from Disable self-service backup for other organizations.

- If you want existing backup job (template) to store backups to another repository instead of the currently configured for organization, then backup administrator should do the following:
  
  a. Move corresponding backups of vCloud Director objects to the new repository.
  
  b. Modify backup job (template) and vCloud Director organization settings so that job would point to the new repository.

Otherwise, data will be stored to the old repository, exceeding the quota.
Removing Custom vCloud Director Organization Settings

You can remove a vCloud Director organization from the list of managed configurations. When you remove an organization, its configuration will be still effective for the old jobs. New vCloud Director backup jobs created after this removal will use default organization settings until you apply a new configuration to the corresponding organization.

To remove a vCloud Director organization, on the vCloud tab of the Self-service view, select the organization you need and click the Remove.

Keep in mind that the default configuration cannot be removed from the list — instead, you can deactivate it. For that:

1. Select the default organization configuration in the preview pane.
2. Click Edit.
3. From the list of repositories, select **Disable self-service backup for other organizations**.

![Edit Organization Settings](image)
Working with vCloud Director VMs via Self-Service Backup Portal

Veeam offers a web-based portal for vCloud Director Organization administrators. It facilitates self-service operations for vCloud Director VMs protection, including VMs and files restore. These operations do not require to create specific user accounts or assign specific roles to them at the Veeam Enterprise Manager level. For restore operations, an administrator just accesses the Self-Service Backup Portal using the default URL.

Accessing Portal

To access the portal, connect to the following URL:
https://<EnterpriseManagerServer>:9443/vcloud/<OrgName>

Log in to the portal using vCloud Director organization administrator credentials.

Working with Portal

Using the Self-Service Backup portal you can perform the following operations:

- On the Jobs tab — examine and export job sessions data, search for jobs, create new jobs and edit jobs.
- On the VMs tab — search for and restore virtual machines and vApps with a single click to their original location (preserving or overwriting the production VM or vApp).
- 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).

IMPORTANT!

Consider the following:

- To manage vCloud Director organization objects (VMs, vApps), users must have the following permissions assigned in VMware vCloud Director: General > Administrator, View General > Administrator, Control User > View Group/User.
- To authenticate users, Self-Service Backup Portal uses LDAP and local user authentication. SAML authentication is not supported.
- To log in to the web portal, vCloud Director organization administrators will need their vCloud Director credentials.
Viewing Statistics on vCloud Director Backups

The **Dashboard** tab contains statistics on the vCloud Director backup jobs created by your vCloud Director organization administrators, including information on the VMs, job runs and backup storage. Views for the last 24 hours and last 7 days are available.

The **Protected** widget reports on:
- **vApps** — displays the number of vApps for which restore points were successfully created during the specified period.
- **VMs** — displays 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 reports on:
- Number of jobs created by currently logged in administrator
- Max job duration
- Average data transfer speed.

The **Backup Storage** widget reports on status of the backup storage assigned to the organization, on the storage quota assigned, and on the storage size used. Status indicators are as follows:
- 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.
The **Last 24 hours / Last 7 days** widget reports on the job session results for the corresponding period.

To visualize on-going jobs data, the **Dashboard** tab also comprises a graph showing time and date when jobs were performed, and the network throughput rate during the job.

**NOTE:**

Only vCloud Director backup jobs for this vCloud Director organization are displayed, all managed by the corresponding Veeam backup server.

The highlighted part of the graph represents the configured backup window if this option was specified in the dashboard settings.
Working with vCloud Director Backup Jobs

Using the Jobs tab of the Self-Service Backup Portal, you can perform the following operations with vCloud Director backup jobs:

- Create a new vCloud Director backup job
- Start, stop or retry a job
- Disable or enable a job
- Edit job settings

Creating Backup Jobs

To create a new vCloud Director backup job:

1. Go to the Jobs tab of the Self-Service Backup Portal and click Create.

2. Specify job name, description and retention settings, that is, how many restore points should be stored in repository for future restores.

   For more information, see the Retention Policy section of the User Guide.

3. Add vApps and/or VMs from the vCloud Director organization to the job.

4. Follow the wizard steps to configure other settings available to you (guest processing, schedule, notifications on job completion). These steps are described in detail the corresponding sections of the Enterprise Manager User Guide and in the Veeam Backup & Replication User Guide.
NOTE:
Consider the following:

- When specifying guest OS access credentials, consider that vCloud Director organization administrators can access guest processing credentials available for their organizations; they can also supply new credentials for guest OS processing, as described here.
- When you add new tenants as Self-Service Backup Portal users, they cannot see the jobs that were created earlier for their vCloud organization. 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.

You can map only jobs of your own organization.

Remaining settings (repository, processing mode, etc.) will be obtained from the repository and from the job template assigned by Enterprise Manager administrator to this vCloud Director organization.

The jobs you create will be shown in Veeam backup management console under the Jobs node, having the `<vCloud Director_org_name>` prefix.

Managing Backup Jobs

Other job management actions are performed as described in the procedures for the standard Enterprise Manager UI:

- Starting, stopping and retrying jobs
- Enabling and disabling jobs
- Editing job settings

To delete a job, select it on the Jobs tab and then on the toolbar click Job > Delete. After deletion, this job will be removed from configuration and no longer appear in web portal and in Veeam backup management console.
Considerations and Limitations

- Job cloning is not available.
- The following limitations apply to scenario involving VM backup and subsequent restore via Self-Service Backup Portal:
  1. You create a backup job that will process a VM added explicitly (that is, not as a part of a vApp container).
  2. This job runs, creating a number of restore points.
  3. Then you restore this VM to the original location via Self-Service Backup Portal. After restore, the VM identifier changes in vCloud 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 vCloud Director hierarchy cache), you should first click Refresh in the Add Objects window.
  4. At the next job run, a new full backup will be created for this VM. However, if you try to perform file-level restore via the Self-Service Backup 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.
Restoring vCloud Director VMs and vApps

You can perform the following tasks using the **VMs** tab of Self-Service Backup Portal:

- Search and browse VMs and vApps
- Restore VMs and vApps
- Restore VM disks
- Delete VMs

## Restoring VMs

vCloud Director VMs can be restored to the original (production) vApp using flexible restore options. Do the following:

1. On the **VMs** tab, select the necessary VM backup in the list of VMs. To quickly find the necessary VM, use the search field at the top of the window.

2. Click **Restore VM** and select the option you need:
   - Select **Overwrite** if you want to restore the VM from the backup to the original vApp, replacing the production VM.
   - Select **Keep** if you want to keep both VMs in the original vApp. The VM from the backup will be located next to the original production VM and will have the same name with the *restored* suffix.
3. Select the restore point that will be used to restore the VM.

4. Additionally, you can select to **Power on VM after restoring** or use the **Quick rollback** option. For VMware VMs, you can also select to **Restore VM tags**.

5. After you click **Restore**, you will get a message notifying you about the operation effect: the VM from the backup will replace the production VM if it is present in the original location. Click **Proceed** or **Cancel** the operation.

You can view the VM restore progress in the **Machines** tab after you click **View history**.

**IMPORTANT!**

Restore of a standalone VM to the original location with the **Keep** option selected will result in an unpredictable behavior and possible failure of the restore job.
Restoring vApps

Similar steps can be taken to restore a vApp:

1. On the VMs tab, select the necessary vApp backup. To quickly find the necessary vApp, use the search field at the top of the window.
2. For the selected backup, click Restore vApp and select the option you need:
   - Select **Overwrite** if you want to restore the vApp from the backup to the original vDC, replacing the production vApp.
   - Select **Keep** if you want to keep the original vApp in the original vDC. The vApp from the backup will be located next to the original production vApp and will have the same name with the _restored suffix. Names of VMs in the vApp will remain the same.
3. Select the restore point that will be used to restore the vApp.

4. Additionally, you can select to **Power on VM after restoring**.

5. After you click **Restore**, you will get a message notifying you about the operation effect — remember that with the **Overwrite** option selected, the existing vApp and all its VMs will be replaced with the vApp from the backup. Click **Proceed** or **Cancel** the operation.

**IMPORTANT!**

*Restore job of a vApp with a standalone VM will return an ordinary and not standalone VM.*
Restoring Virtual Disks

You can restore individual virtual disks from backups of vCloud Director VMs:

1. On the **VMs** tab, select the backup of the VM whose disks you want to restore. To quickly find the necessary VM, use the search field at the top of the window.

2. Click **Virtual Disks**.

3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Performing Virtual Disk Restore.

Deleting VMs and vApps

Once you select a VM click the **Delete** button. If you are sure that you want to delete the selected VM press **Yes** in the appeared Delete VM window.

If the selected VM is the last one in its vApp, then it is deleted from the backup with its vApp. If this vApp is the last one in its backup, then the whole backup is deleted. In other cases, only the selected VM is deleted.

If you delete a vApp all of the VMs will be deleted from backup.

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 1 VM only.

When you remove data for deleted VMs from regular backup chains, it does not free up space on the backup repository. It marks the space as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.
Restoring VM Guest OS Files

The **Files** tab of the Self-Service Backup Portal allows users to browse the guest OS file system in a VM backup, search for guest OS files and restore necessary files.

To restore files from indexed and non-indexed VM guest file system, go to the **Files** tab and follow the 1-click restore procedure. For more information, see *Performing 1-Click File Restore*.

**NOTE:**
- If you plan to restore from non-indexed VM guest, consider that mount operation will be performed using mount server assigned to the corresponding backup repository.
- For more information on how to restore files from a Linux VM, see [this web page](#).
Restoring Application Items

The **Items** tab of Self-Service Backup Portal allows users to perform item-level recovery from application-aware backups (currently, SQL Server databases and Oracle databases).

To restore application items (SQL Server databases or Oracle databases), go to the **Items** tab and follow the steps described in the [Restore Procedure for SQL Server](#) databases and [Restore Procedure for Oracle](#) databases.

Information on these restore operations will be available in the “Restore Operators Activity” report from the [Veeam Backup & Replication Report Pack](#) available in Veeam ONE.
Controlling Backup Infrastructure with vSphere Web Client Plug-in

The vSphere Web Client plug-in for Veeam Backup & Replication facilitates vSphere administrators' daily routine of managing backup infrastructure in the organization. This plug-in allows authorized personnel to view detailed information on the status of Veeam Backup & Replication infrastructure and create restore points ad-hoc, using no other tool but vSphere Web Client.

In particular, vSphere administrators can view success, warning, failure counts for all jobs, as well as cumulative information on used and available storage space, and statistics on processed VMs. They can easily identify unprotected VMs and perform capacity planning, as well as create restore points for selected VMs using VeeamZIP and Quick Backup functions, all directly from vSphere Web Client.
Getting Started

The vSphere Web Client plug-in is installed from the **vCenter Servers** page of the **Configuration** view in Enterprise Manager. To access the **Configuration** view, a user must log on to Enterprise Manager with administrative account.

Before installing the vSphere Web Client plug-in, make sure the following requirements are met:

- The plug-in supports vSphere Web Client v5.1.0 build 880146 and later. For vSphere Web Client versions 5.1.0 build 880146 - 6.5 (including), the plug-in is available with the flex/flash interface. Starting with vSphere Web Client version 6.7, the plug-in offers HTML 5 user interface. The older versions of the client do not support the HTML 5 interface.

- Single Sign-On Service must be running on a server with FQDN (to be accessible from Enterprise Manager server via HTTPS).

- Account used to install the plug-in must have sufficient access rights for vCenter server (must belong to the same domain in case of cross-domain access):
  - **Extension > Register extension** — to install the plug-in
  - **Extension > Unregister extension** — to uninstall the plug-in

For more information on vSphere Web Client, see [this VMware article](#).
Installing vSphere Web Client Plug-in

To install Veeam plug-in for vSphere Web Client, do the following:

1. In the Enterprise Manager Configuration view, go to the vCenter Servers section.
2. Select the vCenter server you need, and click Check version.
3. In the Web Client Plug-in window, enter a user name and password to connect to vCenter Server, and specify connection port (default is 443). Veeam Backup Enterprise Manager will use these credentials to access vCenter Server and check if Veeam plug-in has been already installed there. If discovered, plug-in version will be displayed in the corresponding column.
4. If connection to vCenter was a success, and plug-in has not been installed yet, then the Install link will become active. Click it to install the plug-in.
5. After installation, the plug-in will be displayed in the list of vCenter Servers and plug-ins.

To explore plug-in status or to remove it from the server, use the corresponding commands on vCenter Server page of the Enterprise Manager Configuration view.
Accessing Plug-in from vSphere Web Client

To access the plug-in from VMware vSphere Web Client, launch the vSphere Web Client and select **Veeam Backup & Replication** from the menu.

**IMPORTANT!**

Check the following:

- To successfully obtain statistics from Veeam Backup Enterprise Manager, the accounts under which users connect to Enterprise Manager (that is, account currently logged on to the web client, or specific account configured in the Veeam plug-in settings) should have an appropriate **Enterprise Manager role** assigned (**Portal Administrator role** or **Portal User role**).
- To open Veeam ONE reports (optional capability), these accounts should be also included in **Veeam ONE Users** or **Veeam ONE Administrators** group on the machine where Veeam ONE Server component is installed.
Configuring Plug-in Settings

When using the plug-in, consider that authentication process includes the following stages:

1. A user logs on to vSphere Web Client. To work with a VMware vCenter server where Veeam plug-in runs, this user account requires the following minimal privileges on vCenter level: `VirtualMachine.Interact.Backup`, `Task.Create`, `Task.Update`.

2. Veeam plug-in connects to Veeam Backup Enterprise Manager which verifies its account. You can configure Veeam plug-in to use the account currently logged on, or to use specific account for that connection. For details, see the procedure description below. Whatever account is used, to perform the necessary backup operation (VeeamZIP or Quick Backup) it should have sufficient security permissions. They are granted via the Enterprise Manager roles — `Portal Administrator` or `Portal User`.

![Diagram of authentication process](image)

To configure a connection to Veeam Backup Enterprise Manager and (optionally) Veeam ONE server, open Veeam plug-in for vSphere Web Client and go to the **Settings** tab on the right.

1. On the **Settings** tab, you can view information about plug-in version and configure Veeam Backup Enterprise Manager connection settings:
   - Veeam Backup Enterprise Manager server (host name or IP address)
   - URL for Veeam Backup Enterprise Manager RESTful API
   - Certificate thumbprint to be used for connection

2. If you plan to connect to Enterprise Manager using a specific account, select the **Password based authentication** option and provide a user name and password. If this option is not selected, connection to Enterprise Manager will be performed using the account currently logged in. Make sure the account intended for connection has an appropriate Enterprise Manager role assigned.
3. If you have Veeam ONE deployed in your environment, you can specify Veeam ONE server name and connection port. Default is HTTP port 1239.

4. Click **Save** to apply the specified settings.
Examining Backup Infrastructure

All components of the Veeam Backup & Replication infrastructure — backup servers, proxy servers, and repository servers — are listed on top of the Summary page, as well as the count of running and scheduled jobs.

Next to the list, there are three key indicators that inform you how the VMs were protected during the specified period:

- Successful VM backups
- VMs with Warnings
- Failed VMs

In the dashboard pane under the summary information, you can explore backup infrastructure in more details.

- The VMs overview widget gives you the information on how your VMs are protected: number of protected VMs (backed up or replicated), number of restore points available, source VM size, full and incremental backup size, replica restore point size, and successful backup sessions ratio. To maximize the widget, click the Full screen icon in the widget’s top right corner; to change reporting period, click the gear icon and select the time period you need:
  - Last 24 hours
  - Last 7 days
  - Last 14 days

Additionally, if Veeam ONE is installed, you can click the link and examine the Protected VMs report that provides a list of VMs which are protected by Veeam Backup & Replication, and which are not.
• In the Jobs statistics widget, all running jobs are displayed, as well as scheduled jobs and max job duration. Additionally, if Veeam ONE is installed, you can click the link and examine the Latest BU Job Statistics report.

• In the Repositories widget, detailed information for each backup repository is displayed, including repository name, overall capacity, free space and backup size. Additionally, if Veeam ONE is installed, you can click the link and examine the Capacity Planning for Repositories report. It gives you an estimation of when the repositories may run out of space.

• The Processed VMs widget shows a graphical representation of how the jobs ran (1 week, 2 weeks, 1 month filters can be applied).
Creating Restore Points with VeeamZIP and Quick Backup

vSphere administrators can quickly create a restore point for a selected VM using VeeamZIP (full backup) or Quick Backup (incremental backup) right from VMware vSphere web client, with no need to use Veeam backup management console. To utilize these capabilities, a user account should be able to go through authentication process, so it must meet the requirements specified in Configuring Plug-in Settings.

Configuring VeeamZIP Settings

To configure the settings for VeeamZIP (VBK file creation), do the following:

1. In vSphere Web Client, open vCenter Inventory.
2. In the inventory tree, select a VM.
3. Click the Configure tab and select VeeamZIP.
4. In the Destination section, select the Veeam backup server to process the VM and the repository where to store the VeeamZIP file.

**NOTE:**

To be visible in this list, Veeam backup server should be added to Veeam Backup Enterprise Manager. Connected repositories from Veeam backup infrastructure will be shown automatically.

5. In the Key section, specify the encryption key, if necessary.
6. In the Delete this backup automatically section, specify whether the resulting backup file should be automatically deleted after a certain time interval.
7. In the Compression level section, select the necessary compression level for the backup.
8. By default, the Disable guest quiescence option is selected, meaning that guest OS quiescence is deactivated. So, if you want a crash-consistent backup, leave it that way. If you want, however, an application-consistent backup, then clear the Disable guest quiescence check box, and Veeam will create a transactionally consistent image of VMs using VMware Tools quiescence for guest OS.

**NOTE:**

For more information about guest OS quiescence, see the Transaction Consistency section of the Veeam Backup & Replication User Guide.
9. Click **Save**. The specified settings will be stored as default settings for the currently logged on user account and will be used for VeeamZIP backup.
Creating Full VM Backup with VeeamZIP

You can use Veeam plug-in for vSphere Web Client to create an ad-hoc VeeamZIP backup of a VM. To create a full VM backup with VeeamZIP:

1. In vSphere Web Client, open **vCenter Inventory**.

2. In the inventory tree, right-click the VM that you want to back up and select one of the following options:
   - Select **Backup > VeeamZIP** if you want to create a backup using the default VeeamZIP settings specified earlier. Alternatively, use the **Actions > Backup > VeeamZIP** menu command.

   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** menu command.

If you select this option, Veeam plug-in will display the **VeeamZIP to** window offering to specify VeeamZIP settings. Specify settings in the same way as described in the **Configuring VeeamZIP Settings** section and click **VeeamZIP**. Veeam will save the specified settings as default settings for VeeamZIP backup and start the VeeamZIP backup process.

You can view the backup creation progress in the **Recent Tasks** pane of vSphere Web Client.

### Creating Incremental VM Backup with Quick Backup

You can also create an incremental backup for selected VM with a single click, using Quick Backup capability. Quick Backup can be run for any VM that meets the following requirements:

1. A backup job processing the VM exists on the Veeam backup server which is added to Veeam Backup Enterprise Manager.
2. There is a full backup file for this VM in the corresponding backup repository.

To perform quick backup:

1. In the **vCenter Inventory**, select the necessary VM.
2. Right-click the VM and select **Quick Backup**. Alternatively, you can use the **Actions** menu command.

This will trigger a backup job processing the selected VM to create a new incremental restore point (VIB file) for the latest full backup found in the repository for this VM. Details of a running quick backup task can be seen in the **Recent Tasks** pane on the right.

To learn more about VeeamZIP and Quick Backup, refer to the Veeam Backup & Replication User Guide.
NOTE:

A Quick Backup or VeeamZIP job fails to start if the Location property of the VM and backup repository do not match — for example, if you try to use a repository with location set to Sydney to back up a VM with location set to Helsinki. To read more about location settings, refer to the Veeam Backup & Replication User Guide.
Working with 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 via 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 and 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 two types of tenant accounts: for a separate vSphere user and 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 Adding Tenant Accounts.

To simplify backup job management for tenants, advanced job settings (such as backup settings and storage settings) and schedule settings are automatically populated from job templates. The administrator can assign a separate template to each tenant account.

When working with vSphere Self-Service Backup Portal, administrators and tenants perform the following tasks:

- **Administrator tasks**
- **Tenant tasks**

Administrator Tasks

To let tenants work with vSphere Self-Service Backup Portal, the Veeam Backup Enterprise Manager administrator performs the following tasks:

1. **Specifies 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** tab in the **Configuration** view of the Enterprise Manager UI. If a vCloud Director server is added to your Veeam backup infrastructure, the working area of the **Self-service** tab will display two inner tabs: **vSphere** and **vCloud**. To work with vSphere Self-Service Backup Portal, make sure the **vSphere** tab is opened. The **vCloud** tab is used to work with VMware vCloud Director organizations and their configurations. For more information, see Working with VMware vCloud Director.

Tenant Tasks

Tenants access the vSphere Self-Service Backup portal using the portal URL obtained from the Veeam Backup Enterprise Manager administrator. To log in to the portal, the tenant uses credentials of the domain user 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.

To configure the delegation mode:

1. On the **Self-service** tab of the **Configuration** view, click **Delegation Mode**.

2. In the **Delegation Mode** window, select the delegation mode. You can select from the following options:
   - **vSphere tags** — select this option if you want 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 details, see Adding Tenant Account and Editing Tenant Account.
   - **vSphere role** — select this option if you want to allow tenants to work with VMs that are available to a specified vSphere role. To specify the vSphere role, do the following:
     i. In the **vSphere role** field, 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** — select this option if you want to allow tenants to work with VMs for which they have a specified vSphere privilege. To select the vSphere privilege, do the following:
     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, browse and select the required privilege.
     iii. Click **OK**.

3. 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**
  Users can manage all VMs for which they have the specified vSphere role assigned.

- **VM privilege**
  Users can manage all VMs for which they have the specified vSphere permission.

[OK] [Cancel]
Managing Tenant Accounts

Veeam Backup Enterprise Manager administrators can perform the following tasks with vSphere Self-Service Backup Portal 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

By default, Veeam Backup Enterprise Manager offers a group vSphere Self-Service Backup Portal tenant account for users of the domain that includes the Enterprise Manager server. To configure granular access to storage quotas and backup settings, you can create additional 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 the Enterprise Manager web UI using the administrative account.
2. Click Configuration and select the Self-service tab on the left. The Self-service tab is available if you added at least one Veeam backup server with a vCenter server as part of its infrastructure to Veeam Backup Enterprise Manager.
3. Click Add.
4. In the **Add** window, from the **Type** list, select the type of the account you want to create. You can select the **User** account type for a single vSphere user or the **Group** account type for a group of vSphere users.

5. In the **Account** field, enter the name of the user or group for which you want to create the tenant account. The name must be provided in the **DOMAIN\Username** format. You can create user accounts for users and groups of the domain that includes the Enterprise Manager server or a trusted domain.

**NOTE:**

You cannot create a vSphere Self-Service Backup Portal tenant account for a local user account.

6. In the **Repository** field, select from the list of backup repositories 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.

**IMPORTANT!**

Backup repository settings specified for the tenant account at the step 6 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.

7. 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.

8. In the **Job scheduling** field, 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.
   - Deny: Creates job with no schedule assigned.

For detailed information on job scheduling, see **Configure Job Scheduling**.
9. 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** list, select the necessary vCenter Servers. By default, the **All vCenter Servers** option is selected.

10. If you selected the **vSphere tags** option at the process of configuring the delegation mode, in the **vSphere tags** field, enter tags assigned VMs that will be available to the tenant.

11. [Optional] If you add a tenant account of the **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.

12. If you want to specify advanced settings for backup jobs of the tenant, click the **Show Advanced Job Settings** link and do the following:

   a. In the **Advanced job settings** section, view the currently used backup job settings.

   b. From the **Copy from** list, select what backup job settings will be applied to tenant jobs. You can select from the following options:

      - **Default job 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>** — select an existing backup job for vSphere VMs that will be used as a template for tenant backup jobs. The backup 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.

   c. 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.

13. Click **Save**.

![Add dialog box](image)

**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 settings

**Options:**
- Hide Advanced Job Settings
- Save
- Cancel
Editing Tenant Account

You can edit a tenant account at any time. For example, you may want to change backup scheduling settings or change other settings for the tenant backup jobs.

To change settings of a vSphere Self-Service Backup Portal tenant account:

1. In the **Configuration** view, open the **Self-service** tab.

2. On the **Self-service** tab, select the account you need and click **Edit** in the top left corner of the working area.

3. In the **Edit** window, edit tenant account settings as required. For details, see Adding Tenant Account.

4. Click **Save**.

---

![Edit window](image-url)
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 Enterprise Manager administrator can generate a report on tenant accounts configured for configured vSphere Self-Service Backup Portal. This report includes information on the account name, backup repository used by the account, and storage quota allocated to the account.

To generate a report:

1. In the Configuration view, open the Self-service tab.
2. On the Self-service tab, click the Export link in the top right corner of the working area.
3. In the pop-up window of your browser, click Save to confirm the download.

The report is saved to the excelreport.xls file in the default location (local Downloads folder).

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Account</td>
<td>Repository</td>
<td>Quota</td>
<td>Per user</td>
</tr>
<tr>
<td>2</td>
<td>John Smith</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Mark Green</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>William Fox</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
<td>No</td>
</tr>
</tbody>
</table>
Removing Tenant Account

To remove a vSphere Self-Service Backup Portal tenant account:

1. In the **Configuration** view, open the **Self-service** tab.
2. In the working area of the **Self-service** tab, select the account you want to remove.
3. In the top left corner of the working area, click **Remove**.
4. In the **Remove configuration** window, select the **Delete jobs** check box if you want to delete backup jobs created by the tenant and select the **Delete backup files** check box if you want to delete all backups created by the tenant, and 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. Connect to the following URL:
   https://<EnterpriseManagerServer>:9443/backup
   For example:
   https://vbr-em:9443/backup

2. In the Username and Password fields, specify credentials of the domain user for which the administrator created a vSphere Self-Service Backup Portal tenant account. The user name must be provided in the DOMAIN\Username format.

3. [Optional] Select the Remember me check box to save the user name for future access.

4. Click Login.

IMPORTANT!

SAML Authorization is not supported for vSphere Self-Service Backup Portal.

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 Appearance](#).
Managing Backup Jobs

Using the Jobs tab of vSphere Self-Service Backup Portal, you can perform the following operations with backup jobs:

- Create a new backup job for vSphere VMs
- Start, stop and retry jobs
- Enable and disable jobs
- Edit backup job settings
- Delete backup jobs

Creating Backup Job

To create a new vSphere backup job:

1. Open the Jobs tab of vSphere Self-Service Backup Portal and click Create.

2. At the Job Settings step of the wizard, specify the backup job name, description and retention policy settings. The retention policy defines how many restore points are kept in the backup repository and can be used for data restore.

For more information, see the Retention Policy section of the Veeam Backup & Replication User Guide.
3. At the **Virtual Machines** step of the wizard, select which vSphere VMs the job will process. For more information, see [Edit the List of Virtual Machines](#).

4. At the **Guest Processing** step of the wizard, select the guest OS processing options and guest OS credentials. For more information, see [Configure Guest Processing Settings](#).

5. At the **Job Schedule** step of the wizard, configure the backup job scheduling options. For more information, see [Schedule the Job](#).

   You can configure backup job scheduling options only if the Enterprise Manager administrator allowed this in the properties of the tenant account. For more information, see [Adding Tenant Account](#).

6. At the **Email Notifications** step of the wizard, select the **Enable e-mail notifications** check box and configure notification settings:

   a. In the **Recipients** field, enter email addresses of recipients separated by comma.

   b. [Optional] In the **Subject** field, specify the subject for notification emails.

   c. Select the **Notify on success**, **Notify on error** and/or **Notify on warning** check boxes to receive email notification if the job completes successfully, fails or completes with a warning.

   d. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.

7. Click **Finish**.

   The backup job will create backups in the backup repository that the Enterprise Manager administrator selected as the target repository in the properties of the tenant account. Advanced job settings such as the backup settings and storage settings will be obtained from the job template assigned to the tenant by the administrator. For more information, see [Editing Tenant Account](#).

### Editing Backup Job

You can edit a backup at any time you need. For example, you may want to change scheduling settings for the job or add VMs to the job.

To edit backup job settings, do the following:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal.

2. In the working area, select the job you want to edit and click **Edit**.

3. In the **Edit** window, edit backup job settings as required. You will follow the same steps as you have followed when creating the job. For more information, see [Creating Backup Job](#).
Removing Backup Job

You can permanently remove a backup job from the configuration database. To remove a job, do the following:

1. Open the Jobs tab of vSphere Self-Service Backup Portal.
2. In the working area of the Jobs tab, select the job you want to delete.
3. Click Delete.

Information about the deleted job will be removed from the Veeam Backup & Replication configuration database (and the Enterprise Manager database as well), and the job will no longer appear in the UI. If you agreed to delete backup files created with the job, they will be removed from backup repository.

**IMPORTANT!**

For vSphere Self-Service Backup Portal tenants, the job cloning operation is not available.
Managing VMs

You can use vSphere Self-Service Backup Portal to perform the following operations with backed-up VMs:

- Search VMs and view VMs details
- **Restore VMs**
- **Restore VM disks**
- **Delete VMs**

Restoring VMs

You can restore vSphere VMs to the original (production) location using flexible restore options. To restore a VM, do the following:

1. On the **VMs** tab, select the necessary VM in the list of VMs. You can also use the search field to search for the necessary VM by a VM name.
2. Click **Restore** and select the option you need:
   - Select the **Overwrite** option if you want to replace the VM in the original location with the VM in the backup. The current state of the VM will be deleted.
   - Select the **Keep** option if you want to save the current state of the VM. The restored VM will be located next to the original VM and will have the same name with the _restored suffix added to the VM name.
3. In the Restore window, select the restore point that will be used to restore the VM.

4. You can select additional options for the VM restore:
   
   - Select the **Quick rollback** check box if you want to restore only the changed data. This option is available only for VMs that were protected with the Changed Block Tracking (CBT) option.
   
   - Select the **Power on VM after restoring** check box if you want to turn on the VM once it is restored.
   
   - Select the **Restore VM tags** check box if you want to restore vSphere tags of the VM.

5. Click **Finish**.

6. Veeam Backup Enterprise Manager will display a message notifying that the VM from the backup will replace the original VM if this VM is present in the original location. Click **Proceed** to start the VM restore operation.

   You can view the VM restore progress. To do this, on the **VMs** tab, click **History**.
Restoring Virtual Disks

You can restore individual virtual disks from backups of vSphere VMs:

1. On the **VMs** tab, select the backup of the VM whose disks you want to restore. You can also use the search field to search for the necessary VM by a VM name.

2. Click **Virtual Disks**.

3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Performing Virtual Disk Restore.

Deleting VMs

You can delete a VM on vSphere Self-Service Backup Portal. This operation may be useful if you want to delete data of the backed-up VM from the backup repository.

When you delete a VM, Veeam Backup Enterprise Manager removes records about the VM from the UI and configuration database. In addition, Enterprise Manager removes data of the deleted VM from the backup.

To delete a VM, on the **VMs** tab, select the necessary VM and click **Delete**. Then press **Yes** in the **Delete VM** window.

The deleted VM is not removed from the list of VMs immediately. The VM will be removed from the list after records about the VM are removed from the configuration database on the Veeam backup server.
Restoring Guest OS Files

The **Files** tab of vSphere Self-Service Backup Portal allows you to browse the guest OS file system in a VM backup and restore individual files. You can restore files from indexed and non-indexed guest OS file systems.

To restore files from a VM guest file system, go to the **Files** tab and follow the 1-click restore procedure. This procedure does not differ from the same procedure performed in the main Veeam Backup Enterprise Manager UI. For details, see **Performing 1-Click File Restore**.

**NOTE:**

Consider the following:

- If you restore files from a non-indexed VM guest OS, the mount operation will be performed using the mount server assigned to the backup repository that contains the backup of the VM.
- If you restore files from a Linux VM, consider the recommendations provided in [this article](#).
Restoring Application Items

The Items tab of vSphere Self-Service Backup Portal allows you to perform item-level recovery from application-aware backups of Microsoft SQL Server databases and Oracle databases.

To restore application items, follow the steps described in the following sections:

- To restore Microsoft SQL Server databases, see Restore Procedure for SQL Server.
- To restore Oracle databases, see Restore Procedure for Oracle.
Appendix A. License Update Session Data

The table below lists the messages that can appear in the automatic license update session log. Similar messages are received as pop-ups after you force the immediate update. Recommendations for users (if applicable) are provided in the **Comment** field.

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

Active Directory Federation Service (AD FS) is a hosted identity provider (IdP) implemented as a feature in the Windows Server OS. It provides single sign-on capabilities for Active Directory (AD) users. If AD AF is used as the IdP in the organization, to let AD users log in to Veeam Backup Enterprise Manager using the single sign-on service, an IT administrator must register Enterprise Manager as a service provider (SP) in AD FS.

To add Veeam Backup Enterprise Manager as a SP in AD FS:

1. Obtain the SP 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 SP metadata exported from Veeam Backup Enterprise Manager.

3. Edit the Claim Assurance Policy for the added Relying Party Trust to add an assurance 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] If you want to provide single sign-on capabilities to AD groups, you must additionally add to the Claim Issuance Policy an assurance 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 to which a user attempting to access Enterprise Manager belongs.

     When a user who belongs to the specified group attempts to access Enterprise Manager, the IdP will issue an authentication assertion confirming that this user belongs to this 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 SP in authentication assertions.

     This value can be different from the User’s group value, for example, if you do not want to display AD group names in Enterprise Manager. This value must be the same as the name of the account of the External Group type to which a security role will be assigned in Enterprise Manager. For more information, see Managing Accounts and Roles.
For example, you want to provide single sign-on capabilities to users who belong to the Backup AD group. In Veeam Backup Enterprise Manager, a security role for these users will be assigned to the EnterpriseUsers account of the External Group type. The default group claim type is specified in advanced SAML settings in Enterprise Manager.

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