## Contents

CONTACTING VEEAM SOFTWARE ................................................................................................................................. 7
ABOUT THIS DOCUMENT ...................................................................................................................................................... 8
ABOUT VEEAM BACKUP ENTERPRISE MANAGER ........................................................................................................ 9
   WHAT’S NEW .................................................................................................................................................................. 10
   HOW VEEAM BACKUP ENTERPRISE MANAGER WORKS .......................................................................................... 12
   ENTERPRISE MANAGER COMPONENTS .................................................................................................................. 13
   VEEAM BACKUP CATALOG ......................................................................................................................................... 15
      Veeam Backup Search Capabilities .................................................................................................................. 16
      File-Level Restore Capabilities ..................................................................................................................... 18
      How Indexing Works ....................................................................................................................................... 19
      Indexing Data .................................................................................................................................................. 20
      Indexing Data Retention ................................................................................................................................ 25
PLANNING AND PREPARATION ......................................................................................................................................... 27
   SYSTEM REQUIREMENTS .......................................................................................................................................... 28
   REQUIRED PERMISSIONS ........................................................................................................................................ 31
   USED PORTS ............................................................................................................................................................ 33
LICENSING ......................................................................................................................................................................... 39
   VIEWING AND CHANGING CURRENT LICENSE .................................................................................................... 40
   REVOKING LICENSE .............................................................................................................................................. 44
DEPLOYMENT ........................................................................................................................................................................ 45
   INSTALLING VEEAM BACKUP ENTERPRISE MANAGER ........................................................................................ 46
   MAINTAINING VEEAM BACKUP ENTERPRISE MANAGER .................................................................................... 60
   UPGRADE SIN VEEAM BACKUP ENTERPRISE MANAGER .................................................................................... 61
   UNINSTALLING VEEAM BACKUP ENTERPRISE MANAGER .................................................................................... 63
GETTING TO KNOW VEEAM BACKUP ENTERPRISE MANAGER .................................................................................. 64
   ACCESSING ENTERPRISE MANAGER WEBSITE .................................................................................................... 65
   VEEAM BACKUP ENTERPRISE MANAGER UI .......................................................................................................... 66
CONFIGURING VEEAM BACKUP ENTERPRISE MANAGER ............................................................................................ 69
   INITIAL CONFIGURATION ....................................................................................................................................... 70
   MANAGING VEEAM BACKUP SERVERS .................................................................................................................. 71
   COLLECTING DATA FROM BACKUP SERVERS ....................................................................................................... 73
   CONFIGURING RETENTION SETTINGS FOR INDEX AND HISTORY ........................................................................ 75
   CONFIGURING SECURITY SETTINGS .................................................................................................................. 78
      Managing Accounts and Roles ........................................................................................................................... 79
      Configuring Restore Scope .................................................................................................................................. 83
      Restrictions for Delegated Restore .................................................................................................................... 86
## Veeam Backup & Replication Server Roles

88

## Configuring Notification Settings

90

- Email Server Settings ............................................. 91
- Notifications on Job Results........................................ 92
- Notifications on Lab Requests ........................................ 94
- Notifications on Restore Operations ............................ 95
- Notifications on Licensing ........................................ 96
- Notifications on Key Management .............................. 97

## Viewing Statistical Reports

98

- Operation Statistics .................................................. 99
- Reports on Backup Servers ......................................... 101
- Job Statistics ............................................................. 102
- Processed Machines Statistics ...................................... 103
- Viewing vCenter Server Information ........................... 104
- Viewing Information About Enterprise Manager ........... 105

## Managing Backup Jobs in Veeam Enterprise Manager

106

- Starting, Stopping and Retrying Jobs ............................ 107
- Enabling and Disabling Jobs ........................................ 108
- Editing Job Settings .................................................. 109
- Creating Active Full Backups ...................................... 129
- Cloning Backup and Replication Jobs ........................... 130
- Deleting a Job .......................................................... 131

## Support for Veeam Agents

132

- Managing Veeam Agent Licenses ................................. 133
- Guest File Browsing and 1-Click Restore ...................... 135
  - Preparing for File Browsing and Restore .................... 136
  - Browsing and Restore Procedures ............................. 138
- Application Item Restore .......................................... 139

## Working with Machines

140

- Viewing, Searching, Deleting Machines ...................... 141
- Performing Quick Backup ......................................... 143
- Performing 1-Click Restore ........................................ 144
- Failover Plan .......................................................... 146

## Restoring Guest OS Files

148

- Preparing for File Browsing and Searching .................. 149
  - Performing Catalog Replication and Indexing ............. 150
  - Preparing for Linux Guest Files Search and Restore ..... 151
- Browsing Machine Backups for Guest OS Files ............. 152
- Searching Machine Backups for Guest OS Files ............. 154
CONTROLLING BACKUP INFRASTRUCTURE WITH VSPHERE WEB CLIENT PLUG-IN ................................................229
  GETTING STARTED ................................................................................................................................. 230
  CONFIGURING PLUG-IN SETTINGS ........................................................................................................... 233
  EXAMINING BACKUP INFRASTRUCTURE ..................................................................................................... 235
  CREATING RESTORE POINTS WITH VEEAMZIP AND QUICK BACKUP ...................................................... 237

WORKING WITH VSPHERE SELF-SERVICE BACKUP PORTAL ........................................................................... 240
  MANAGING TENANTS ............................................................................................................................... 241
  WORKING WITH vSPHERE VMs VIA vSPHERE SELF-SERVICE BACKUP PORTAL ...................................... 247
    Viewing Statistics on vSphere User Backups ............................................................................................ 248
    vSphere User Backup Jobs ....................................................................................................................... 250
    Managing vSphere User VMs ................................................................................................................... 253
    vSphere User Files Restore ..................................................................................................................... 255
    vSphere User Items Restore .................................................................................................................... 256

APPENDIX A. LICENSE UPDATE SESSION DATA ............................................................................................. 257

APPENDIX B. INSTALLING VEEAM BACKUP SEARCH (OPTIONAL) ................................................................. 258
  ADDING A SEARCH SERVER (OPTIONAL) .................................................................................................... 266
Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, 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.

Document Revision History

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 5</td>
<td>7/16/2019</td>
<td>Updated for Veeam Backup &amp; Replication 9.5 Update 4b.</td>
</tr>
<tr>
<td>Revision 4</td>
<td>4/8/2019</td>
<td>Minor changes throughout the document.</td>
</tr>
<tr>
<td>Revision 3</td>
<td>3/26/2019</td>
<td>Updated for Veeam Backup Enterprise Manager Update 4a.</td>
</tr>
<tr>
<td>Revision 2</td>
<td>2/19/2019</td>
<td>Minor changes throughout the document.</td>
</tr>
<tr>
<td>Revision 1</td>
<td>1/22/2019</td>
<td>Initial version of the document for Veeam Backup Enterprise Manager 9.5 Update 4.</td>
</tr>
</tbody>
</table>
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 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).
- 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 accounts and support their administrators with the VMware vSphere Self-Service 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

What's New in v9.5

The following features and enhancements are supported in Veeam Backup Enterprise Manager 9.5:

- Restore of Oracle databases to the state as of in the selected restore point and to the required point in time. For details, see the Backup and Restore of Oracle Databases.
- Web-based management UI for VMware vCloud Director organization administrators (providers) — to control organization settings, including repository quotas and backup job schedule, and Veeam Self-Service Backup Portal for tenants — to manage backup jobs and restore machines, vApps, files and application items.
- Extended job management — now you can modify job name and retention settings.

What's New in v9.5 Update 2

The following features and enhancements are supported in Veeam Backup Enterprise Manager 9.5 Update 2:

- License management for Veeam Agent for Windows or Veeam Agent for Linux via Enterprise Manager web UI.
- 1-Click restore of guest OS files from the backups of physical machines created by Veeam Agent.
- Restore of the application items from such backups.

IMPORTANT!

These features will be available if your infrastructure meets the following requirements:

1. You have Enterprise or Enterprise Plus edition of Veeam Backup & Replication 9.5 Update 2.
2. For 1-Click restore of guest OS files and for restore of application items, you must have Server edition of Veeam Agent for Windows 2.0 or later, or Server edition of Veeam Agent for Linux 1.0 Update 1 or later.
3. Veeam Agent must be integrated with Veeam Backup & Replication. For more information on Veeam Agent integration with Veeam Backup & Replication, see the Using with Veeam Backup & Replication section of the Veeam Agent for Windows User Guide and Using with Veeam Backup & Replication section of the Veeam Agent for Linux User Guide.

What's New in v9.5 Update 3

The following features and enhancements are supported in Veeam Backup Enterprise Manager 9.5 Update 3:

- Veeam Backup Enterprise Manager web UI is now updated to display both virtual and physical machines availability.
What's New in v9.5 Update 3a

The following features and enhancements are supported in Veeam Backup Enterprise Manager 9.5 Update 3a:

- Veeam Backup Enterprise Manager now supports VMware vCloud Director version 9.1.
- vSphere Web Client Plug-in now supports vCenter version 6.7 with a new HTML 5 user interface.

What's New in v9.5 Update 4

The following new features and enhancements are supported in Veeam Backup Enterprise Manager 9.5 Update 4:

- New graphical user interface redesigned to match modern Veeam web UI design guidelines.
- Extended support for Veeam Agents:
  - Use the Machines tab to view Veeam Agent backups and the Jobs tab to view Veeam Agent jobs.
  - Manage instance consumption by Veeam Agent machines.
  - Users with the Restore Operator or Portal User roles now can have Protection Groups as Managed Scope Objects added to their Restore Scope. For more information on Enterprise Manager roles and their functions, see Managing Accounts and Roles.
  
    For more information on Veeam Agent support, see Support for Veeam Agents.

- New licensing paradigm and a new license management interface. For more information, see Licensing.

- Veeam Backup Enterprise Manager 9.5 Update 4 introduces vSphere Self-Service Backup Portal — a feature allowing vSphere administrators to create and manage vSphere tenants configurations. For more information, see Working with vSphere Self-Service Backup Portal.

- New wizard for Microsoft SQL Server restore to a custom location. For more information, see Backup and Restore of Microsoft SQL Server Databases.

- Support for a new type of a granular scope management object — VM groups for Hyper-V 2016 and later. For more information, see Configuring Restore Scope.
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** that 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** that 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** that 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.

Veeam Backup Search Server

You have an option to engage the Veeam Backup Search component and Microsoft Search Server in the indexing process. However, consider that this component is mainly intended for existing deployments of Veeam Backup & Replication, providing for backward compatibility.

The Veeam Backup Search component from the installation package should be in this case installed on a machine running Microsoft Search Server. The Veeam Backup Search server runs the MOSS Integration Service that invokes updates of index databases on Microsoft Search Server. Veeam Backup Search uses Microsoft Search Server functionality to crawl aggregated index files in the Veeam Backup Enterprise Manager catalog and create a content index on the Search Server that is used to process search queries. The service also sends search queries to Microsoft Search Server which processes them and returns necessary search results to Veeam Backup Enterprise Manager. For more information, see Appendix B. Installing Veeam Backup Search (optional).

NOTE:

Using Veeam’s proprietary mechanism for indexing and search is the best practice.
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:

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

```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
```
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 help the user to 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 > Guest file catalog section** in Veeam Backup Enterprise Manager.

<table>
<thead>
<tr>
<th>Account</th>
<th>Chart Settings</th>
<th>Session History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Guest file system catalog</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention period: 3 month(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By default, guest file system catalog only keeps data for backups currently on disk. With Standard Edition, guest file system catalog only keeps data for backups currently present in backup repositories. With Enterprise Edition, catalog is also kept for archived backups according to the set retention period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Event history</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep all</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep only last: S3 week(s)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Veeam Backup Enterprise Manager UI](image-url)
Indexing Data Retention

The retention policy for Veeam Backup Catalog helps you to maintain the necessary amount of indexing data on the Veeam Backup Enterprise Manager server.

The retention policy for Veeam Backup Catalog is controlled by two values:

- Retention policy for a backup job on the Veeam backup server: the number of restore points in the backup chain
- Retention period for indexing data in Veeam Backup Enterprise Manager

The retention period is calculated differently for backup chains created with different backup methods:

- Retention for forward incremental backup chains
- Retention for reverse incremental backup chains

Retention for Forward Incremental Backups

The retention policy for the forward incremental backup chain is calculated by the following formula:

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

where:

- Catalog Retention is the retention period specified in Veeam Backup Enterprise Manager.
- \(X\) is the amount of time for which restore points are kept by a backup 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:

- \textit{Catalog Retention} is the retention period specified in Veeam Backup Enterprise Manager.
- \( X \) is the amount of time for which restore points are kept by a backup job.

For example, the retention policy settings are specified in the following manner:

- The retention policy for the backup job is set to 3 points. The backup job is run daily.
- The retention period in Veeam Backup Enterprise Manager is set to 1 month, or 30 days.

In this case, Veeam Backup Enterprise Manager will retain in Veeam Backup Catalog indexing data for 30 days plus indexing data for 3 restore points in the backup chain.

**IMPORTANT!**

The longer 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.
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 Search

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>CPU: x64 processor</td>
</tr>
<tr>
<td></td>
<td>Memory: 4 GB RAM (minimum recommended).</td>
</tr>
<tr>
<td></td>
<td>Hard disk space: 2 GB on the system disk (required to extract all components from the setup package during the product installation).</td>
</tr>
<tr>
<td></td>
<td>Network: 1Gbps recommended due to backup performance considerations.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>64-bit versions of the following operating systems are supported:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server Semi-Annual Channel (including version 1903)</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 2008 R2 SP1</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 2008 SP2</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 10 (including version 1903)</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 8.x</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 7 SP1</td>
</tr>
</tbody>
</table>
SQL Server

Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported):

- 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

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 4.6 (included in the setup).
- Microsoft Internet Information Services 7.0 or later: IIS 6 Metabase Compatibility and Windows Authentication components required for IIS 7.0, support for extensionless URLs for IIS 7.0 or later, ASP.NET 4.5, .NET Extensibility 4.5 for IIS 8.0.
- Directory Browsing component, Default Document component, HTTPS Errors component, Static Content component.
- [Optional] 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 2003 or later is required to view report data exported from Veeam Backup Enterprise Manager.

[Optional] For Agent Management features, Veeam Backup Enterprise Manager requires Veeam Agents integrated with Veeam Backup & Replication v9.5 Update 2 (and later):

- Veeam Agent for Linux 1.0 Update 1 (and later)
- Veeam Agent for Windows 2.0 (and later)

*For machines running Microsoft Windows Server 2012 or later.
**For machines running Microsoft Windows 7, Microsoft Windows Server 2008 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>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 10.0 or later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>• Latest versions of Mozilla Firefox and Google Chrome</td>
</tr>
<tr>
<td></td>
<td>For portable devices (tablets) latest versions of Apple Safari for iOS or Google Chrome for Android.</td>
</tr>
</tbody>
</table>

VMware vCloud Director (Optional)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCloud Director</td>
<td>Supported versions are 8.x up to 9.5.</td>
</tr>
<tr>
<td>Other software</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>

Veeam Backup Search (Optional)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Refer to system requirements for the Microsoft Search Server version that you use in your environment.</td>
</tr>
<tr>
<td>OS</td>
<td>Both 32-bit and 64-bit versions of the following operating systems are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2003</td>
</tr>
<tr>
<td></td>
<td>All the latest service packs and security updates must be installed.</td>
</tr>
<tr>
<td>Software</td>
<td>• Microsoft Search Server 2010 (including Express edition)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Search Server 2008 (including Express edition)</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>1. <em>Local Administrator</em> permissions on the Veeam Backup Enterprise Manager server.</td>
</tr>
<tr>
<td></td>
<td>2. <em>Log on as service</em> right (granted automatically to the Veeam Backup Enterprise Manager Service account).</td>
</tr>
<tr>
<td></td>
<td>3. <em>Db_datareader</em> and <em>db_datawriter</em> roles, as well as permissions to execute <em>stored procedures</em> 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>4. <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;<em>Cannot find user account DOMAIN\username</em>&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** |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Search Server (optional, used for compatibility with legacy deployments)</td>
</tr>
</tbody>
</table>
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 - 65535 (for Microsoft Windows 2008 and later) 1025 to 5000 (for Microsoft Windows 2003)</td>
<td>Dynamic RPC port range. For more information, see Microsoft Support KB 832017 and Microsoft Support KB 929851.</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port(s)</td>
<td>Additional Information</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SQL Server hosting the Enterprise Manager configuration database</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>
<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</td>
<td>TCP</td>
<td>49152 - 65535 (for Microsoft Windows 2008 and later) 1025 to 5000 (for Microsoft Windows 2003)</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>Microsoft Search Server (optional)</td>
<td>TCP</td>
<td>9395</td>
<td>Default port used by the optional Veeam Backup Search component. Can be customized during Veeam Backup Search installation. For more information, see the Specify Service Account Settings step of the Veeam Backup Search installation guide.</td>
<td></td>
</tr>
<tr>
<td><strong>Veeam Backup Enterprise Manager website (IIS extension)</strong></td>
<td>Veeam Backup Enterprise Manager service</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>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>-----</td>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Veeam Cloud Connect Portal website (IIS extension)</strong></td>
<td>Veeam Backup Enterprise Manager service</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>
</tr>
<tr>
<td><strong>Browser</strong></td>
<td>Veeam Backup Enterprise Manager website (IIS extension)</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>
</tr>
<tr>
<td></td>
<td>Veeam Backup Enterprise Manager website (IIS extension)</td>
<td>HTTPS</td>
<td>9443</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veeam Cloud Connect Portal website (IIS extension)</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>
</tr>
<tr>
<td><strong>Veeam Backup Enterprise Manager RESTful API client and VMware vSphere web client plug-in</strong></td>
<td>Veeam Backup Enterprise Manager RESTful API</td>
<td>HTTP</td>
<td>9399</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Veeam Backup Enterprise Manager RESTful API</td>
<td>HTTPS</td>
<td>9398</td>
<td></td>
</tr>
</tbody>
</table>
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 - 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 - 6000</td>
<td>Ports used for file download. For more information on the helper appliance, see <em>Preparing for Linux Guest Files Search and Restore</em>.</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</td>
<td>TCP</td>
<td>3260 - 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 - 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>49152-65535</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 - 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>Oracle on Linux server</td>
<td></td>
<td>TCP</td>
<td>22</td>
<td>Default SSH port used as a control channel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>2500 - 5000</td>
<td>Default port range for data transmission.</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 which is stated for each type of protected workloads (for per-instance licenses) or applies a license to the protected hosts (for per-socket licenses).

Veeam Backup Enterprise Manager collects information about the type of license installed on Veeam backup servers connected to it and the amount of instances left. 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.

**NOTE:**

For more information about 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 User Guide.

For more information on licensing, see Veeam Licensing Policy.

Using the Licensing section of the Veeam Backup Enterprise Manager UI reduces administration overhead. You can manage and activate licenses for the whole backup infrastructure from a single web console. You can view to which machines the instances are currently applied, install a new license file, or revoke the licenses.
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 tab.
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, license days remaining and a spreadsheet of the available and used instances per each of the Veeam Backup & Replication infrastructure categories: virtual, physical and cloud machines.

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.

Each job for a respective type of the Veeam Backup & Replication infrastructure uses own multiplier per each instance. Instance cost multipliers depend on the product edition. For example, one Workstation machine consumes one license instance multiplied by 1 with the Standard Edition, by 0.5 with the Enterprise Edition and by 0.33 with the Enterprise Plus Edition. For more information on the Veeam Instance Licensing conversion, see Veeam Licensing Policy.
To display detailed information about the current license, including type, expiration date and the number of instances, click the Details link.

<table>
<thead>
<tr>
<th>License Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Valid</td>
</tr>
<tr>
<td>Expiration date</td>
<td>9/9/2020 (602 days left)</td>
</tr>
<tr>
<td>Type</td>
<td>Subscription</td>
</tr>
<tr>
<td>Edition</td>
<td>Enterprise Plus Edition</td>
</tr>
<tr>
<td>Licensed to</td>
<td>Veeam Software AG</td>
</tr>
<tr>
<td>Contact person</td>
<td>Dev and QA Departments</td>
</tr>
<tr>
<td>Instances</td>
<td>1000</td>
</tr>
<tr>
<td>Support ID</td>
<td>00276360</td>
</tr>
<tr>
<td>Support expiration date</td>
<td>9/9/2020 (602 days left)</td>
</tr>
</tbody>
</table>

- **Update license key automatically**
  - **Update now**

### 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** tab, and open the **Licensing** section on the left of the **Configuration** view.
3. Click on the **Instances** tab in the **Licensing** section, select the required machine in the list and click **Revoke**.
Deployment

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

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

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

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

For more information on Veeam Backup Enterprise Manager installation in unattended mode, see 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 9.5 Update 4 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 components the setup wizard will install on the machine and choose the installation folder.

### Selecting Components

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

- Veeam Backup Enterprise Manager
- Veeam Backup Catalog

For service providers the setup wizard will also offer you to install Veeam Cloud Connect Portal.

**NOTE:**

For more information on Veeam Cloud Connect Portal, see the [Veeam Cloud Connect Guide](#).

To choose the components to install:

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

If Veeam Backup Catalog or Veeam Cloud Connect Portal is already installed, the setup will exclude them from the list of installed components.

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

### Selecting Installation Folder

To choose the installation folder:

1. On the right of the **Install to** field, click **Browse**.
2. In the **Browse for Folder** window, select the installation folder for the product. The default installation folder is `%ProgramFiles%\Veeam\Backup and Replication`.
Step 5. Install Missing Software

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

You can install missing components automatically or manually.

- To install missing components automatically, click **Install**. The setup wizard will not interrupt the installation process and install the missing components during the current work session.
- To install missing components manually:
  1. Click **Cancel** and exit the setup wizard.
  2. Install and enable the necessary components manually on the machine.
  3. 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** 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 **Port 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** checkbox.

**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**).

<table>
<thead>
<tr>
<th>Port Configuration</th>
<th>HTTP Port 9580</th>
<th>HTTPS Port 9443</th>
</tr>
</thead>
<tbody>
<tr>
<td>RestAPI HTTP Port</td>
<td>9388</td>
<td>RestAPI HTTPS Port 9388</td>
</tr>
<tr>
<td>Enterprise Manager service port</td>
<td>9384</td>
<td></td>
</tr>
<tr>
<td>Cloud Connect Portal port</td>
<td>5443</td>
<td></td>
</tr>
<tr>
<td>Catalog service port</td>
<td>9365</td>
<td></td>
</tr>
<tr>
<td>Use certificate</td>
<td>Generate new self-signed certificate</td>
<td>View certificate</td>
</tr>
</tbody>
</table>

- **High security mode** (forces TLS 1.2 usage and disables weak ciphers)
- These server-wide settings may not be compatible with legacy applications running on the same server.

![Veeam Backup Enterprise Manager Setup](image_url)
Step 10. Specify File Locations

The **File Locations** step is available if you have selected to install Veeam Backup Catalog at the **Review Components and Select Installation Folder** step of the wizard and to configure installation settings manually at the **Specify Installation Settings** 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**.

![Image of Veeam Backup Enterprise Manager Setup with the File Locations step highlighted, showing the default location `C:\VBRCatalog` and a `Browse` button.]
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 the Upgrade

Upgrade of Veeam Backup Enterprise Manager to version 9.5 Update 4 is supported for version 9.0 Update 2 (build 9.0.0.1715) and later. To upgrade from earlier versions, contact Veeam Technical 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 a backup of the corresponding SQL Server configuration databases used by Veeam backup server(s) and Veeam Backup Enterprise Manager server, so that you can easily go back to 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:


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 the 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 9.5 Update 4, 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 9.5 Update 4 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 dialog, 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 **Username** and **Password** fields, specify credentials of a Portal Administrator, Site Administrator or Portal Operator.

   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**.

   The user account 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**.

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 dialog 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 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 \textbf{Home} view you can click \textbf{Configuration} to open the \textbf{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 \textbf{Configuration} view of the Veeam Backup Enterprise Manager UI:

- Add, edit or remove Veeam Backup servers using the \textbf{Backup Servers} tab. For more information, see \textit{Managing Veeam Backup Servers}.
- Work with vCenter servers managed by Enterprise Manager using the \textbf{vCenter Servers} tab. For more information, see \textit{Viewing vCenter Server Information}.
- Manage vCloud Director organizations and vSphere tenant accounts using the \textbf{Self-Service} tab. For more information, see \textit{Working with VMware vCloud Director} and \textit{Working with vSphere Self-Service Backup Portal}.
- Work with search servers using the \textbf{Search Servers} tab. For more information, see \textit{Adding a Search Server (optional)}.
- View and manage data collection job sessions using the \textbf{Sessions} tab. For more information, see \textit{Collecting Data from Backup Servers}.
- Configure Enterprise Manager security roles using the \textbf{Roles} tab. For more information, see \textit{Managing Accounts and Roles}.
- Configure Enterprise Manager settings using the \textbf{Settings} tab. For more information, see \textit{Configuring Retention Settings for Index and History} and \textit{Customizing Dashboard Appearance}.
- Manage licenses and view detailed reports on license consumption using the \textbf{Licensing} tab. For more information, see \textit{Licensing}.
- Set email notifications using the **Notifications** tab. For more information, see *Configuring Notification Settings*.

- Manage password recovery for encrypted backups using the **Key Management** tab. For more information, see *Managing Encryption Keys*.

- 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 cannot add cloned backup servers of the added servers.
- You cannot add configuration restored servers of an added server.
- You can add one backup server only to a single instance of Veeam Backup Enterprise Manager.
- You cannot add backup servers that process the same machines.
- You cannot add backup servers that process the same backups.
- 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 9.0 Update 2 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. 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:

For setting up self-service recovery delegation scope, consider that reverse DNS lookup on Veeam Backup Enterprise Manager server must be functional.

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/or Files tab  
• Access reports for these machines  
• Run Quick Backup for machines from the restore scope on the Machines tab  
• Perform restore operations as permitted by the delegation settings |
| 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.

**NOTE:**

Consider the following:

- If you clear the Allow restore of: Entire virtual machines check box, then Portal User will be able to view all machines processed by managed backup server(s) — on the Machines tab.
- If you clear the Allow restore of: Guest files check box, then Portal User will be able to browse guest OS files for all machines processed by managed backup server(s) — on the Files tab.

This refers to all editions of the product.
Assigning Role

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

1. Open the Configuration tab.
2. Open the Roles section on the left of the Configuration view.
3. Click Add on the toolbar.
4. In the Account type field, select the type of account you want to add: User or Group.
5. In the Account field, specify the user account in the DOMAIN\Username format.
6. From the Role list, select the necessary portal role to be assigned: Portal User, Portal Administrator or Restore Operator.
7. In the Restore scope section, you can allow a user to restore all machines processed by managed backup servers or the selected machines 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.

![Add Role dialog box](image)

- **Account type**: User
- **Account**: techivanessa.scott
- **Role**: Restore Operator

**Restore scope**: All machines

**Allow restore of**:
- Entire virtual machines
- Guest files
  - Allow in-place file restores only
  - Allow restore of files with these extensions only:
    - [ ]
- Microsoft Exchange items
- Databases
  - [ ] Microsoft SQL Server databases
  - [ ] Oracle databases
- Deny in-place database restores (safer)

[OK] [Cancel]
NOTE:

To be able to assign any of these roles to Active Directory domain users and/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.)

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 non-administrative role includes **All machines** 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** dialog:

1. In the **Restore scope** section, select the **Selected machines only** option, and click **Choose**.

![Add Role dialog](image)
2. In the **Manage Scope Objects** dialog, click **Add object** and select what objects to display: Hyper-V, vSphere, vCloud or Protection Groups.

![Manage Scope Objects dialog](image)

3. Select the objects you allow the user to restore:

![Add Objects dialog](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.

Users then will be able to view the machines and/or files included in their scope on the corresponding tabs after they log in to Enterprise Manager.

NOTE:

The **Machines** tab displays only machines that have been backed up, and 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 and backups are not yet presented to users in the **Machines** or **Files** tab right after the login to Enterprise Manager. If you cannot find a VM after making a search query, click the link **I don't see my VM** to refresh the view. This link, however, will not be visible until you have made an unsuccessful search.

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

**Portal Administrators** can watch the progress of security scope rebuild process on the **Sessions** page.
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. On top of the Roles section view, 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 included in the restore scope, select the Entire virtual machines 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**.

![Add Role](image)
Veeam Backup & Replication 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 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
   - %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.
4. If you do not want to receive notifications about the support expiration, select the Disable support contract expiration notifications check box.
5. In the From field, enter an email address of the notification sender.
6. In the To field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
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 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 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 virtual machine templates.
- The **Data** block shows the average processing speed, total sizes of processed machines, full backups and increments.
- 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:
  - **Success** – 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** button 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 machines 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.

Besides the information presented in the list of jobs, the Jobs tab allows you to view advanced job data:

- To see a list of job sessions, click the job name link in the Name column.
- To see detailed statistics on the last job run, click the state link in the Status column.

NOTE:

You can export displayed information to a file using the Export button 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.

Besides the information presented in the list of machines, the Machines tab allows you to view advanced data about each machine:

- To see detailed information about a machine, click its name in the Machine column.
- To see detailed information about machine restore points, click a link in the Restore Points column.

NOTE:

You can export displayed information to a file using the Export button on the toolbar. This file then can be opened on the client machine using the associated application.
Viewing vCenter Server Information

On the **vCenter Server** page, you can view the information on vCenter servers added to your Veeam Backup infrastructure. Use the corresponding commands to perform the operation you need, in particular:

- **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 (see the “Controlling Backup Infrastructure with vSphere Web Client” section of this guide for details).

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

**IMPORTANT!**

To perform these operations, you should supply user account(s) with sufficient permissions to access vCenter server. (Currently, user account information is not imported from Veeam Backup database into 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**.

Supplementary to the information above, the **About** view displays log paths to the Enterprise Manager services and Catalog services. You can access the log files following the paths below:

- **Veeam Backup Enterprise Manager Service logs**
  
  C:\ProgramData\Veeam\Backup\Svc.VeeamBES.log

- **Veeam Catalog Data Service logs**
  
  C:\ProgramData\Veeam\Backup\Svc.VeeamCatalog.log

- **Web Site Information 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 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 Find 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.
- Rerun 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 the 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!**

This capability is not available for physical machine backups. It is available if you have Enterprise or Enterprise Plus license installed. Also, consider that using the Veeam Backup Enterprise Manager web console, you can change only some settings of Veeam Backup & Replication jobs, as described below. If you have Veeam backup servers of earlier versions added to Enterprise Manager, note that their jobs cannot be modified using Enterprise Manager.

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.

**IMPORTANT!**

Backup copy jobs cannot be modified through Veeam Backup Enterprise Manager. To edit backup copy job settings, use the Veeam Backup & Replication console.
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. Enter 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 Veeam Knowledge Base article KB1799.

![Edit Backup Job](Image)

**Job Settings**

Specify the job name, description and retention policy

<table>
<thead>
<tr>
<th>Virtual Machines</th>
<th>Guest Processing</th>
<th>Job Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job name:</strong> Backup Job 1</td>
<td><strong>Description:</strong> Created by VBR954\Administrator at 1/16/2019 9:56 AM.</td>
<td></td>
</tr>
</tbody>
</table>

**Retention policy**

Restore points to keep on disk: 3

[Next] [Finish] [Cancel]
Step 2. Edit the 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>Edit Backup Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Settings</td>
</tr>
<tr>
<td>Virtual Machines</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>srv30</td>
</tr>
</tbody>
</table>
```

2. In the displayed virtual infrastructure tree, select the necessary object.

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>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv08</td>
<td>VirtualMachine</td>
</tr>
<tr>
<td>srv21</td>
<td>VirtualMachine</td>
</tr>
<tr>
<td>srv30</td>
<td>VirtualMachine</td>
</tr>
</tbody>
</table>
```
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** button.
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, as described in the paragraphs that follow.

![Application-Aware Processing Options](image-url)
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 application processing** (default option) if you want Veeam Backup & Replication to stop the backup job if any error occurs.

- Select **Ignore application processing 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 (recommended)** 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:
  
  o  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.

  o  Settings for SQL Server transaction log handling can be configured separately on the **SQL** tab — it becomes available to you with this option selected.

  o  Similarly, you can configure settings for Oracle database archived logs processing on the **Oracle** tab.

- Select **Perform copy only (lets another application use logs)** 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.

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** button, then in the dialog displayed select the machine in the list 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 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.
   - To discard custom settings of a machine, select the machine in the list and click **Remove**.

<table>
<thead>
<tr>
<th>Object</th>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>snv08</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>snv21</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>snv30</td>
<td>Partial</td>
<td>Partial</td>
</tr>
</tbody>
</table>

**Guest File System Indexing Options**

[Add machine... Edit... Remove]
2. In the **Indexing Settings** dialog 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 dialog.
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.
• 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:
  o For Active Directory accounts — `DOMAIN\Username`
  o 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

**Linux Credentials**

- **Username:** User
- **Password:** ************
- **Private key is required for this connection**
  - **Private Key:** ~/.ssh/id_rsa
  - **Passphrase:** ************
- **SSH port:** 22

**Non-root account**

- **Elevate specified account to root**
  - **Add account to the sudoers file automatically**
  - **Use “su” if “sudo” fails**
  - **Root password:** ************
  - **Description:** Test Linux server connection

[Image of Linux Credentials dialog box]
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 button 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. Schedule the Job

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

<table>
<thead>
<tr>
<th>Job Settings</th>
<th>Specify the job scheduling options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Run the job automatically:</strong></td>
</tr>
<tr>
<td></td>
<td>✔️ Daily at this time: 10:00 pm</td>
</tr>
<tr>
<td></td>
<td>Everyday</td>
</tr>
<tr>
<td></td>
<td>✔️ Monthly at:</td>
</tr>
<tr>
<td></td>
<td>10:00 pm</td>
</tr>
<tr>
<td></td>
<td>Fourth</td>
</tr>
<tr>
<td></td>
<td>Saturday</td>
</tr>
<tr>
<td></td>
<td>✔️ Periodically every: 1 Hours</td>
</tr>
<tr>
<td></td>
<td>✔️ After this job:</td>
</tr>
</tbody>
</table>

### 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**
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’ 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.

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 Backup and Replication 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 Veeam Agent 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 a Job

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

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. Then you will be prompted whether to delete backup files, too. To delete them, select the corresponding 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.

NOTE:

This feature is supported for Veeam Backup & Replication 9.5 only, so if you have backup servers of earlier versions, also managed by Enterprise Manager, this operation will not be available for their jobs.
Support for Veeam Agents

Enterprise Manager supports browsing and restore operations for the guest OS files and application items from the 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 9.5 Update 2 or later.
2. For 1-Click restore of guest OS files and for restore of application items, you should have Server edition of Veeam Agent for Microsoft Windows 2.0 (or later) or Server edition of Veeam Agent for Linux 1.0 Update 1 (or later).
3. Veeam Agent should be integrated with Veeam Backup & Replication, as described in the product documentation.
Managing Veeam Agent Licenses

If you have a license for Veeam Agent for Windows or Veeam Agent for Linux and plan to integrate this product with Veeam Backup & Replication, consider managing its license using Enterprise Manager.

For such centralized management, you should take the following steps:

1. Configure Veeam Agent to work with Veeam Backup & Replication. For more information on using Veeam Agent with Veeam Backup & Replication, see the Veeam Agent for Microsoft Windows User Guide or Veeam Agent for Linux User Guide.

2. Make sure you have a valid license installed and visible in Veeam Backup & Replication console. For more information on Veeam Agent license management with Veeam Backup & Replication, see the Veeam Agent for Microsoft Windows User Guide or Veeam Agent for Linux User Guide, section Managing License.

3. Also, make sure that Veeam backup server which manages Veeam Agent was added to Enterprise Manager, and its data was successfully collected.

When these prerequisites are met, the corresponding fields of the Instances table (Servers or Workstations) are populated in the Licensing section of the Configuration view in Veeam Backup Enterprise Manager web UI.
Here you can install a new license for Veeam Agent(s), view detailed license information and examine the list of Veeam backup servers managing the licensed Agents.

- To view the list of Agents servers and workstations select the **Instances** tab.
- To download the list as the **excelreport.xls** file, click **Report**, then close the dialog.

If the machine where Veeam Agent ran is no longer functioning, you can reset the corresponding license counter on the managing Veeam backup server. For that, in the **Licensing** pane of the **Configuration** view select the Veeam backup server that used to be associated with the Agent and click **Reset**.
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.

**In This Section**

- Preparing for File Browsing and Restore
- Browsing and Restore Procedures
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 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 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. If there are failover plans created for machines included in user's scope, the user can also implement 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 machine(s), open the Machines tab.

Here you can filter the list by backup server, or in the Name search field, supply the machine name or a part of it, and click Find.

Here are the details for some machines:

**appsrv01.tech.local: Restore Points**

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17/2019 01:00:45 pm</td>
<td>Increment</td>
</tr>
<tr>
<td>1/15/2019 01:00:41 pm</td>
<td>Increment</td>
</tr>
<tr>
<td>1/14/2019 01:01:39 pm</td>
<td>Full</td>
</tr>
</tbody>
</table>

141 | Veeam Backup Enterprise Manager | User Guide | REV 5
For each machine, you can click the link in the **Restore Points** column to view the list of all restore points created for it, either on schedule or on demand.

To delete a machine from a backup stored by a backup job in the repository, select the machine and click the **Delete** button, 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.

Firstly, the corresponding records from Veeam Backup Configuration database will be deleted, and machine will be no longer displayed in the UI. Once the machine is deleted from the Veeam Backup server, user will receive a notification.

**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 the Quick Backup button.

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

Authorized users can restore the 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, take the following steps:

1. On the Machines tab, locate the necessary machine backup in the list of machines displayed, or use search by machine name.
2. For the selected machine backup, click the Restore button.
3. Select if you want to Overwrite or Keep the machine in the production.

**NOTE:**

Veeam Backup Enterprise Manager supports machine restore to its original location only. If you choose to restore with Overwrite, the machine in the production environment will be shut down and replaced by machine from backup. If you choose to Keep the machine in production, the machine from backup will be restored next to the machine in the production environment.

4. Select the point that will be used to restore the machine.
5. Additionally, you can select to Power on machine after restoring or Quick rollback (restore changed blocks only) option.
6. After you click **Restore**, you will get a message notifying you of the operation effect (machine from backup will replace production machine, if present in the original location). Click **Proceed** or **Cancel** the operation.

You can view machine restore progress in the **Machines** page after you click **View history**.

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

1. On the **Machines** tab, locate the necessary machine processed by replication job.
2. Click the **Restore** button on the toolbar to view available restore point, and select the restore point you need.
3. By default, the machine will be powered on after restoring. Additionally, you can select the **Quick rollback (restore changed blocks only)** option.
4. Click **Restore**, then confirm the operation of the production machine deletion, or **Cancel** the operation.
Failover Plan

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** dialog, 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. 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 file(s) 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.

And, optionally, you can install and add a search server, as described in the Appendix B.
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, select **Search Servers** on the left of the **Configuration** view and click **Sync Catalog Now** on the toolbar.

- To automatically run catalog replication after every backup job, select **Search Servers** on the left of the **Configuration** view and click **Schedule** on the toolbar. In the displayed window, select **Automatically after every backup job** and specify other options as necessary.

Every run of a catalog replication job initiates a new job session which can be tracked under **Sessions** in the **Configuration** view. To view detailed information for a specific session, find it in the **Sessions** view and click the corresponding **click here** link in the **Log** 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.

Starting with Veeam Backup & Replication v9, however, 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. Select the machine that you want to browse, either by typing in a machine name or by picking it from the list.
3. In the Restore point field you can select a necessary date of backup and a restore point. Note that dates when backup of the selected machine was performed are highlighted in the calendar.
4. If the machine was backed up without guest indexing, then click **Mount**. If the machine guest OS information was not collected during the backup, you will be 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 to find a necessary file, or use the Quick search field in the top left corner.

Consider that depending on the number of files on the machine, the search process may take some time.

**IMPORTANT!**

For machine processed without indexing, you can only use browsing or Quick search to find the necessary file(s) 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 Machine Backups for Guest OS Files

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 selected machine backup at the latest restore point only. To perform simple search:

1. Open the Files tab and go to the Search tab.
2. In the Machine name field, select the machine that you want to browse.
3. In the Search field, type in the name of the necessary file or a part of it and click the search icon on the right.
The advanced search allows you to search for guest OS files in the selected machine backup and all restore points and filter search results by certain criteria. To perform advanced search:

1. Open the Files tab and click the No Filter link in the search field to open the Set Options window.

2. Expand the Advanced search section and define the necessary search criteria:
   - Location — select a specific folder on the machine to search in.
   - Last modification time – specify approximate time when the file was last modified or set a time interval.
   - Backup time — choose to search through the latest backup of the specified machine or all backups of the machine created within a certain time interval.
   - Owner — select to search for files with a specific owner.
   - Type — select to search for files of specific type or with a certain extension.
   - Size — specify approximate size of file or set a size range.

3. Click the search icon to the right of the Search field.
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 simply provide users with local administrator rights 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.
- 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.

![Files tab](image)

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.
Downloading Files to Local Machine

If you choose to download the restored file, Veeam Backup Enterprise Manager interacts with the corresponding 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, follow the next steps:

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 the Download button.

3. Click Yes to confirm the operation.

4. Wait for restore session to complete and the file to be retrieved from the backup.
5. In the **Log** tab, go to the last record in the session log ("Restored files are available for download"), and click the **download** link.

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).
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!**

1. 1-Click file restore capability is available if you have Enterprise or Enterprise Plus edition.
2. 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:**

1. 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.
2. 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, follow the next steps:

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 the **Restore** button, or right-click the file and select **Restore** from the shortcut menu. Select how files should be handled:
   - If you select **Overwrite**, the file from machine backup (being restored) will replace the file on target.
   - If you select **Keep**, both files will be kept on target; file from machine backup will have **Restored** prefix.

3. Click **Yes** to confirm the operation.

4. The result of the operation will be displayed after you click **View history**.

**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.
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 the Add to restore list button, or use the file shortcut menu command.

When a file is added to the restore list, the Pending Restore tab becomes available on the left.

**IMPORTANT!**

Veeam Backup Enterprise Manager keeps files in the restore list until you leave the Files section. When you switch to another section of the management website, the restore list is cleared.

Select the necessary files from the restore list and use the Restore or Download buttons to perform the corresponding restore operation for all selected files. You can remove selected files from the list using the Remove selected link at the top-right of the list. Use the Select all and Clear all links to facilitate the file selection process.

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

1. Click the View History link in the bottom right corner.
2. Select the necessary restore operation.
3. Open the Log tab and click Download.
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 & 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 an 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 Applications button, then in the dialog displayed, select the Exchange server machine from the list and click Edit.
5. Go to the General tab and make sure you have the Require successful application processing option selected in the Applications section.

6. In the Transaction logs processing section, the Process transaction logs with this job (recommended) option is selected by default.
7. Click OK to save the settings and close the dialog.
8. Next, 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 **Customise Credentials** button and then click **Set User**. Then you can specify custom guest OS credentials for the selected machine:

   ![Guest OS Credentials](image)

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

9. On 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 Edit Role dialog 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** and in the **Account** section 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 the [Configuring Exchange Impersonation in Exchange 2010](https://docs.microsoft.com/en-us/exchange/configure/configure-exchange-impersonation) Microsoft Docs article.

After specifying 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. Go to the Items tab, then click Mailbox items.

3. 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. Choose a restore point.

**NOTE:**
- 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. Select a type of item you need 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 that using Veeam Backup Enterprise Manager you can only restore deleted items to the production mailbox.

If specified mailbox does not exist in the machine restore point you select, then you will get a corresponding 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 Enterprise & Enterprise *Plus* editions of Veeam Backup & Replication.

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

Database restore from storage snapshots with Veeam Backup Enterprise Manager is not supported.
Preparing an 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, then in the dialog displayed, select the SQL server machine from the list and click Edit.
   a. On the General tab, make sure you have the Require successful application processing option selected in the Applications section.
   b. Also, to be able to specify transaction log handling options, make sure the Process transaction logs with this job (recommended) option is selected. Otherwise, if you select Perform copy only (lets another application use logs) 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 sections of the Veeam Backup & Replication User Guide.
5. Next, go to the **SQL** tab and specify how SQL transaction logs will be handled:

- Select **Truncate logs (prevents logs from growing forever)** 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 (requires simple recovery model)** if you do not want Veeam Backup & Replication to truncate logs at all.

**IMPORTANT!**

- If you prefer 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 **Backup logs** 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** nor **Truncate logs** option is selected, then logs will increase in size and occupy disk space.

- Select **Backup logs periodically (backed up logs are truncated)** 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.

### mercury: Processing Settings

<table>
<thead>
<tr>
<th>General</th>
<th>SQL</th>
<th>Oracle</th>
<th>File Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="#" alt="Truncate logs" /></td>
<td><img src="#" alt="Do not truncate logs" /></td>
<td><img src="#" alt="Backup logs periodically" /></td>
</tr>
<tr>
<td></td>
<td>Truncate logs (prevents logs from growing forever)</td>
<td>Do not truncate logs (requires simple recovery model)</td>
<td>Backup logs periodically (backed up logs are truncated)</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Backup logs every" /> minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retain log backups:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="#" alt="Until the corresponding image-level backup is deleted" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="#" alt="Keep only last" /> days</td>
<td></td>
</tr>
</tbody>
</table>

---

**173 | Veeam Backup Enterprise Manager | User Guide | REV 5**
6. If you selected to backup transaction 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 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.

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

8. On the **Job schedule** step, make sure the scheduled run is enabled for the job, otherwise, log backup will not be activated.

9. Finish the wizard.
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 checkbox in the Account dialog.

If necessary, select the Deny in-place database restores (safer) check box.

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

For more information, 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.

For more 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 an available restore point back in the original location. For that, click the Restore button for the selected database.

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.

TIP:
If you are restoring 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:

1. Select the Alternative location option as a restore destination.
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 Timeline. For more information, see Using the Point in Time Timeline.

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. Click the Restore button.
SQL Restore Wizard

When you click the **Restore** button you will open an SQL Restore wizard. Follow the steps of the wizard described below:

- **At the Target Server step** enter the target **Server Name** and credentials for it. Specify the name of the target database. You can enter separate credentials for accessing the target database, picking the **Use the following credentials to access the database** option. You can also **Use SQL Server authentication** if needed, by picking the according option. Once you are done, click the **Next** button to take you to the next step of the wizard.

- **If you have Always On availability groups present on your target server**, the next step allows you to add the restored database to it.

- **On the Files step** you can choose specific paths for restore target locations. You can specify separate target locations for the primary database file and secondary database file with logs. Once you are done, click the **Finish** button.

Once you click the **Finish** button, you will be taken to the **Items** tab. There, you can watch the status of the restore procedure.

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**.
Using the Point in Time Timeline

The timeline includes the following timestamps (relatively to the currently selected SQL server restore point):

- **Beginning** — refers to the previous restore point of the SQL Server machine which 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 the *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 the *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 the *End* will refer to the latest log backup time.
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 Enterprise & Enterprise *Plus* editions of Veeam Backup & Replication.

Veeam supports restore from backups created with Veeam Backup & Replication version 9.5 and 9.0.
Database restore from storage snapshots via Enterprise Manager is not supported.
Preparing and 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 job 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 **Applications** button, then in the dialog displayed, select the Oracle server machine from the list and click **Edit**.

   a. On the **General** tab, make sure you have the **Require successful application processing** option selected in the **Applications** section.

   b. Also, to be able to specify transaction log handling options, make sure the **Process transaction logs with this job (recommended)** option is selected. Otherwise, if you select **Perform copy only (lets another application use logs)** option, Veeam Backup & Replication will create a copy-only backup, and transaction logs will not be purged — that is why the **Oracle** tab with log handling settings will be deactivated in this case. To read mode, refer to the copy-only backup description in the Veeam Backup & Replication User Guide.

**IMPORTANT!**

If both Microsoft SQL Server and Oracle Server 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.

Next, go to the **Oracle** tab and specify how archived logs will be handled:

![Oracle Processing Settings](image)

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

**Specify Oracle account with SYSDBA privileges:**

- Use guest credentials
  - + Add

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

**Retain log backups:**

- Until the corresponding image-level backup is deleted
- Keep only last 15 days

**OK** **Cancel**
1. 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 Oracle system - or specify another account, selecting it from the drop-down list or adding a new account. In any case, make sure the account you specify here has sufficient rights — see the **Required Permissions** section in the Veeam Explorer for Oracle guide for details.

2. 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 currently selected machine restore point, to selected point in time and to selected transaction.

   - **Delete logs older than <N> hours/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 selected, 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.

3. If you selected to backup 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.

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

5. On the **Job schedule** step, make sure the scheduled run is enabled for the job, otherwise, log backup will not be activated.

6. Finish the wizard.
Providing Access Rights

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

To allow for database restore by users with Restore Operator or Portal User role, in the Account dialog:

1. Select the Databases check box.
2. Select Oracle databases check box.

If necessary, select the Deny in-place database restores (safer) check box.

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, or click the link to **pick server** 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:
   - Firstly, Veeam will try to use the account of the backup job that contains Oracle server machine, or the account which is currently logged in.
   - 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:**

   Specified account's role in the Enterprise Manager should allow that user to restore Oracle databases. For more information, see Providing Access Rights.

Now you can perform the restore, following the required scenario. To view restore session log, click **History**.
Scenario 1: 1-Click Restore to Original Location

This scenario allows you to restore selected database to the latest available state back in the original location. For that, click the **Restore** button for selected database.

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. If necessary, click the link to **Pick another restore point**. Use the calendar control to choose from the available dates when restore points were created — they are marked with blue square outline; if more than one restore point per day was created, select the required time on the right.

2. If you backed up archived redo logs for the database, you can also select the required **Point in time** using the timeline and the slider.

**NOTE:**
For more information on log backup, see Preparing and Application-Consistent Backup.

The timeline includes the following timestamps (relatively to currently selected server restore point):

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

3. To specify target location, click the **Destination** link. Specify the location where you want the database items to be restored.
4. If you selected **Restore to the original location**, consider that user credentials for restore procedure will be picked as follows:

   o Firstly, Veeam will try to use the account of the backup job that contains Oracle server machine, or the account which is currently logged in.

   o 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:**

Specified account’s role in the Enterprise Manager should allow that user to restore Oracle databases. For more information, see *Providing Access Rights*.  

5. Another option is **Restore to alternative location**, described in the next section.

6. Click **Restore** to proceed.

   o If restoring to the original location, this will start the restore process.

   o If restoring to another location, this will launch restore wizard for you to follow. For more information, see *Using Oracle Restore Wizard*. 
Using Oracle Restore Wizard

1. Specify connection settings for target server where the database should be restored:

2. If you are restoring Oracle on Windows:
   a. Enter DNS name or IP address of the target Windows machine.
   b. Specify the account to 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 minimal required, **Full Control** recommended.

![Oracle Restore Wizard](image)

**Oracle Restore**

- **Target Server**: Specify credentials for the target Windows server
  - **Oracle**
    - **Target server**
  - **Database Files**
    - **DNS name or IP address**: `srv30.tech.local`
    - **Specify account to connect to the server with**
      - **Account**: `Administrator`
      - **Password**: `*********`
3. If you are restoring Oracle on Linux, specify connection settings for the target Linux server:
   - Server name (or IP address) and SSH port – default port is 22.
   - Account to be used to access the server. This should be a root account or account elevated to root and added to sudoers. To elevate the account and add it to sudoers, click Settings and use the corresponding options.
     You can use authentication by user name and password or by private key.

4. Next, select Oracle Home and specify Global database name and Oracle SID where to restore the database from backup.

5. 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.
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 > 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, go to the Configuration > Key Management section.
2. Click Generate in the Managed keys toolbar.
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, go to the Configuration > Key Management section.
2. Select an inactive keyset in the list.
3. Click Activate on the right of the list.

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, go to the Configuration > Key Management section.
2. In the Key retention settings 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, go to the Configuration > Key Management section.
2. In the keyset list, select a keyset you want to back up and click Export.
3. Save the resulting .PEM file on the local disk or on the network share.

To import a previously exported keyset:

1. In Veeam Backup Enterprise Manager, go to the Configuration > Key Management section.
2. Click Import next to the keyset list.
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 have provided when created 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, go to the Configuration > Key Management section.
2. Select a necessary keyset in the list and click Delete Key on the right.

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** tool button in the top left corner.
4. Follow the steps of the wizard. On the **Lab Request** step, 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.
5. On the **Backup** step of the wizard, you can select the backup or replica to restore the VM from (if the VM is included in more than one job).

6. On the **Restore Point** step, the restore point when the application was in the desired state. By default, Enterprise Manager will display restore points closest to the latest backup. If you want to display all restore points that are available for the selected backup, select the **Show all available restore points** check box.
7. **On 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. **On 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. On 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. Next, 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. 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. Select one of existing SureBackup jobs that you want to run to create an isolated sandbox in which the selected machine should be started. The application group and virtual lab used by this SureBackup job will be displayed in the Selected Job details section.

   By default, the list of jobs displays only those jobs that contain the selected machine. If you want to display all SureBackup jobs that were created, select the Show all available SureBackup jobs check box.

5. On 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.

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. Starting with v9.5, 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

In v9.5, 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 the **Add** button to add a new configuration.

5. In the dialog displayed, 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 (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.
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
     
     For more information on the backup window configuration, see Customizing Dashboard Appearance.

   - **Deny**: Creates job with no schedule assigned

For more detailed 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**.

   ![Advanced 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.
2. Click the Edit button in the top right corner to open the Edit dialog.
3. 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 dialog:
   - 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.
4. To change the job that should be used as a template from that point forward, in 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

To remove a vCloud Director organization from the list of managed configurations:

1. When on the vCloud tab of the Self-service view, select the organization you need in the preview pane.

2. Click the Remove button in the top left corner. When you remove an organization from the list of managed configurations, 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.

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 Configuration Form]

Organization: Other vCloud organizations
Repository: Disable self-service backup for other organizations
Quota: 1 TB
Job scheduling: Allow: Tenant has full access to all job scheduling

Show Advanced Job Settings  Save  Cancel
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 Machines 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 file(s) to the original location or download to the local machine.
- On the Items tab – perform application item-level restore (currently, for SQL Server and Oracle databases).

IMPORTANT!

- 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 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 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:
- 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.
vCloud Director Backup Jobs

Using 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 a Job

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.
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:**

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.
NOTE:
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, these 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.
Job Management

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 dialog.

  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.
vCloud Director VMs and vApps Restore

Using **Machines** tab of the Self-Service Backup Portal you can:

- Search and browse VMs and vApps
- Restore VMs and vApps
- 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 **Machines** tab, locate the necessary VM backup in the list of VMs displayed, or use search by VM name.

2. For the selected VM backup, click the **Restore VM** button, then select the option you need:
   - With the **Overwrite** option selected, the VM from backup will be restored to the original vApp, replacing the VM in production.
   - With the **Keep** option selected, both VMs will be kept in the original vApp — VM from backup will be located next to the original production VM and will have the same name with `_restored` suffix.

3. Select the restore point that will be used to restore the VM.

![Machines tab](image)
4. Additionally, you can select to **Power on VM after restoring** or **Quick rollback (restore changed blocks only)** option. For VMware VMs, you can also select to **Restore VM tags**.

5. After you click **Restore**, you will get a message notifying you of the operation effect (VM from backup will replace production VM, if present in the original location). Click **Proceed** or **Cancel** the operation.

You can view VM restore progress in the **Machines** tab after you click **View history**.

**IMPORTANT!**

Restore of a standalone VM into original location with the **Keep** option selected will result in an unpredictable behavior and possible fail of the restore job.
Restoring vApps

Similar steps can be taken to restore a vApp:

1. On the **Machines** tab, locate the necessary vApp, or use search by name.

2. For the selected backup, click the **Restore vApp** button, then select the option you need:
   
   - With the **Overwrite** option selected, the vApp from backup will be restored to the original vDC, replacing the vApp in production.
   
   - With the **Keep** option selected, both vApps will be kept in the original vDC — vApp from backup will be located next to the original production vApp and will have the same name with \_restored suffix. Names of VMs in the vApp will stay the same.

3. Select the point that will be used to restore the vApp.

4. Additionally, you can select to **Power on vApp after restoring**.
5. After you click Restore, you will get a message notifying you of the operation effect — remember that with the Overwrite option selected, the existing vApp and all its VMs will be replaced with 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.

**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.
vCloud Director Files Restore

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.
vCloud Director Items Restore

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 administrator 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 Configuration view in Enterprise Manager; to access 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:

- Veeam 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 Veeam plug-in is available under a flex/flash interface. Starting with vSphere Web Client version 6.7, the Veeam plug-in performs under HTML 5 user interface, which cannot be used for the older versions of the client.

- 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

Installing the 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 vCenter Servers section.
2. Select the vCenter server you need, and click Check version.
3. In the Web Client Plug-In dialog displayed, enter 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 to it yet, then the Install button 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 Enterprise Manager Configuration view.
Accessing the Plug-in from vSphere Web Client

To access the plug-in from VMware vSphere Web Client, launch the Web Client and from the navigation pane on the left, select **Veeam Backup & Replication**.

**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. First, 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.
To configure the connection to Veeam 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 **Use this account for authentication** check box and provide user name and password; then click **Test Connection**. If this check box is cleared, then 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. Also, 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

Now IT admins can quickly create a restore point for 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 and in the inventory tree select the VM you need to backup.
2. Right-click the VM and from its shortcut menu select Backup > VeeamZIP to. Alternatively, use the Actions > Backup > VeeamZIP to menu command.

Specify the default VeeamZIP settings

- Destination: rgw7:e4:team support: test: local
- Key: 12345
- Delete the backup automatically: Tonight
- Compression level: Optimal (recommended)
- Guest processing: Disable guest quiescence (performs crash consistent backup)

VeeamZIP settings:

- Specify the destination directory
- Enter the key
- Select the delete backup automatically option
- Select the compression level
- Select the guest processing option

Save the settings.
You will be taken to the VM’s Manage tab where you should specify VeeamZIP settings which then will be used as default for VeeamZIP backup.

3. Select Veeam backup server to process the VM.

**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.

4. Select the repository where to store the VeeamZIP file.

5. If necessary, specify the encryption key.

6. Specify whether this backup should be automatically deleted after certain time interval.

7. Select the necessary compression level for the backup.

8. By default, the **Disable guest quiescence (performs crash consistent backup)** 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 a transactionally consistent image of VMs using VMware Tools quiescence for guest OS.

**NOTE:**

To read more about guest OS quiescence, refer to the “Transaction Consistency” section of Veeam Backup & Replication User Guide.

9. Now you can click the **VeeamZIP** button to create a full VM backup (.VBK file) using the specified settings. You can view the backup creation progress in the **Recent Tasks** pane on the right.

The specified settings will be stored as defaults for currently logged on user account.
Creating a Full VM Backup with VeeamZIP

To create an ad-hoc VeeamZIP file with the specified settings, you can right-click the necessary VM and use the Backup > VeeamZIP command from its shortcut menu or from the Actions menu.

Creating an 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 read more about VeeamZIP and Quick Backup, refer to Veeam Backup & Replication User Guide.

NOTE:

A Quick Backup or VeeamZIP job fails to start if the Location property of the VM and repository do not match - for example, if you try to use a repository with location set to Sydney to backup a VM with location set to Helsinki. To read more about setting the Location, refer to the Veeam Backup & Replication User Guide.
Working with vSphere Self-Service Backup Portal

Veeam Backup & Replication allows administrators to permit tenants self-service backup and restore operations via the web UI-based on Veeam Backup Enterprise Manager — **vSphere Self-Service Backup Portal**. This feature is designed to add tenant role permissions management capabilities over the vCenter Server's backup and restore operations. Administrators and tenants have different capabilities using this functionality.

### Veeam Backup Enterprise Manager Administrator Capabilities

Veeam Backup Enterprise Manager administrators can grant tenants access configurations. Access configuration includes a tenant delegation mode, target repository, repository quota, job scheduling options and backup job template.

For more information, see [Managing Tenants](#).

### Tenants Capabilities

Tenants get access to the vSphere Self-Service Backup Portal. They can select virtual machines to manage backup jobs, as well as restore VMs, files and application items within their delegation mode. Tenants also are capable of managing retention, schedule and notification settings as well as guest OS processing options.

vSphere tenants log in to the vSphere Self-Service Backup Portal using their domain credentials. Enterprise Manager administrators select tenants' delegation mode. Tenants can manage resources only within their delegation mode — that is, virtual machines Enterprise Manager administrator has allowed to see and manage. Enterprise Manager administrator allows these tenants to configure essential job settings (such as):

- Create new backup jobs based on the pre-defined templates for the objects within tenants scope.
- Modify or delete jobs.
- Enable or disable jobs.
- Start, stop, retry jobs.
- View statistics on vSphere backups.
- Restore vSphere VMs to the original location.
- 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 tenants, advanced job parameters (like backup mode and repository settings) are automatically populated from the job templates. These templates are assigned by Enterprise Manager administrator for the particular account. For more information, see [Working with vSphere VMs via vSphere Self-Service Backup Portal](#).
Managing Tenants

Veeam Backup Enterprise Manager administrator can permit tenants to work with the VMs via the vSphere Self-Service Backup Portal. Tenants will be able to work only with VMs within their assigned delegation mode.

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

- **Add** a new configuration for a tenant
- **Edit** an already issued tenant configuration settings
- **Export** a list of the used tenant configurations
- **Remove** tenant configurations

Adding Tenant Configuration

To add tenant configuration settings:

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

2. Click **Configuration** and select **Self-service** tab on the left. On a **vSphere** tab you will see the list of tenant configurations that you can manage. The **Self-service** tab will become available after you add at least one Veeam backup server with a vCenter server as part of its infrastructure to Veeam Backup Enterprise Manager.

Select a **Delegation mode** that you will use to specify the scope of VMs, available to the tenant:

- **vSphere role** — tenants have within their scope only VMs where they have a certain vSphere role
- **VM privilege** — tenants have within their scope only VMs with a certain vSphere privilege
- **vSphere tags** — tenants have within their scope only VMs with certain vSphere tags
3. Click **Add** to add a new configuration.

4. In the dialog displayed, select the **Type** of the configuration you are adding (for users or groups of users) and a username of an **Account** for either a trusted domain or the same domain as Enterprise Manager host.

**NOTE:**
You cannot add configuration for a local account.

5. Assign the **Repository** from the list of those available to you. This repository will be used by the users backup jobs. The list includes repositories configured for managed Veeam backup servers.

**IMPORTANT!**
You cannot assign cloud-based repositories, as well as NetApp or Nimble storage systems storing snapshots created by Veeam snapshot-only jobs.

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

7. 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
   - Deny: Creates job with no schedule assigned
8. For more detailed information on job scheduling, see Configure Job Scheduling.

9. If you selected the **vSphere tags** as a **Delegation mode**, you can enter a set of tags, that will define the scope of vSphere VMs available for the users backup jobs.

10. If you are adding a **Group Type** of configuration, you can choose to **Assign a separate quota to each group member**. It means that each user within this vSphere group will have only its own VMs within his scope. Other users VMs and jobs will not be displayed.

11. Click **Show Advanced Job Settings** link to specify what backup job will be used as a template for vSphere users VMs processing. Select the backup job which settings will be copied and used as a template. For that, use the **Copy from** list:

   1. **Default job settings** – backup job will be configured with the standard default vSphere backup job settings as they are shown in the Veeam backup console. For more information, see Creating Backup Jobs. If you do not use the **Show advanced job settings** link, default job settings will be applied to template.

   2. **<job_name>** – select the vSphere backup job from which settings will be obtained. When finished, click **Apply**.

![Add Job Settings](image.png)
IMPORTANT!

Backup repository settings specified for vSphere user configuration at step 6 (global settings) will take priority over those prescribed by selected job template.

NOTE:

To populate the list of job templates, you need at least one vSphere backup job to be configured in Veeam backup console.

12. Click **Save** to save configuration.
Editing vSphere Users Configuration

As an Enterprise Manager administrator, you can modify existing configurations or remove them from the list of managed configurations.

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 vSphere infrastructure in Veeam management console will not reflect the updates.

To modify vSphere users configuration settings:

1. On the **vSphere** tab select the account you need.
2. Click **Edit** in the top left corner to open the **Edit** dialog.
3. Edit the configuration settings as necessary. If you want to display job settings applied to backup jobs for this configuration, click **Show Advanced Job Settings** in the dialog:
   - In the **Advanced job settings** section you can examine existing job settings.
   - In the **Copy from** field you will see the name of a vSphere job previously selected as a template for this vSphere user configuration.
4. To change the job that should be used as a template from that point forward, in the **Copy from** list select the job you need and click **Apply**.
Consider the following recommendations for modifying vSphere user configuration settings:

- If you plan to modify job template for a selected vSphere user configuration, remember that new settings will be applied only to the new jobs created for that user; existing jobs will not be affected.

- If you want existing backup job (template) to store backups to another repository instead of the currently used in configuration, then backup administrator should do the following:
  
  a) Move corresponding backups of vSphere objects to the new repository.
  
  b) Modify backup job (template) and vSphere configuration settings so that job would point to the new repository.

Otherwise, data will be stored to the former repository, exceeding the quota.

### Exporting List of Configurations

To download a report on configurations of vSphere users, click Export. The report will be saved to the excelreport.xls file in the default location (local Downloads folder). This report includes information on the account name, used repository, space and quota in the existing configurations.

<table>
<thead>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>Invuser:10</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
</tr>
<tr>
<td>2</td>
<td>Invuser:20</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
</tr>
<tr>
<td>2</td>
<td>Invuser:50</td>
<td>Default Backup Repository</td>
<td>100 GB</td>
</tr>
<tr>
<td>2</td>
<td>Invuser:90</td>
<td>Default Backup Repository</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

### Removing vSphere Users Configurations

To remove a vSphere user configuration from the list of managed configurations:

1. When on the Self-Service tab of the Configuration view, select the configuration you need in the preview pane.
2. Click the Remove button in the top left corner.

IMPORTANT!

When you remove the vSphere users configuration, you will be asked if you want to delete all the jobs and backup files that come with it.
Working with vSphere VMs via vSphere Self-Service Backup Portal

**vSphere Self-Service Backup Portal** is a tool for vSphere users that facilitates operations with delegated VMs protection, including VM restore and files restore. These operations do not require access to Veeam backup management console. For backup and restore operations, the user accesses the **vSphere Self-Service Backup Portal**.

**Accessing Portal**

To access the portal, connect to the following URL:

https://<EnterpriseManagerServer>:9443/backup

Log in to the portal using domain user credentials.

**Working with Portal**

Using the vSphere self-service portal you can perform the following operations:

- View statistics on vSphere user backups on the **Dashboard tab**.
- Examine and export job sessions data, search for jobs, create new jobs and edit jobs on the **Jobs tab**.
- Search for virtual machines and restore virtual machines and containers with a single click to their original location on the **VMs tab**.
- Search for files on VM guest file system and restore the necessary file(s) to the original location or download to a local machine on the **Files tab**.
- Perform application item-level restore of SQL Server and Oracle databases on the **Items tab**.

**IMPORTANT!**

SAML Authorization is not supported for the vSphere Self-Service Backup Portal.
**Viewing Statistics on vSphere User Backups**

The *Dashboard* tab contains statistics on vSphere backup jobs, including information on protected VMs, job runs and backup storage. Views for the last 24 hours and last 7 days are available.

![Dashboard Screenshot](image)

**Protected** widget reports on:

- **VMs** — displays the number of VMs successfully protected during the specified period. At least one restore point was created for these VMs.
- **Templates** — displays the number of virtual machines templates, successfully protected during the specified period.
- **Total size** — total size of successfully protected VMs.

**Jobs** widget reports on:

- **Jobs** — number of jobs created by currently logged in user.
- **Max duration** — maximum time for job duration.
- **Average speed** — average data transfer speed.

**Backup Storage** widget reports on:

- **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** 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 vSphere backup jobs for this vSphere user are displayed.

The highlighted part of the graph represents the configured backup window if this option was specified in the [dashboard settings](#).
vSphere User Backup Jobs

Using Jobs tab of the vSphere self-service web portal, you can perform the following operations with vSphere backup jobs:

- Create a new vSphere backup job
- Start, stop or retry a job
-Disable or enable a job
-Edit job settings
-Delete jobs

Creating a Job

To create a new vSphere backup job:

1. Go to the Jobs tab of the self-service web 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 Veam Backup and Replication User Guide.
3. Add VMs from the vSphere 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 in the Editing Job Settings sections of this guide.

This job will automatically be targeted to the repository that is assigned to the user. Remaining settings (processing mode, etc.) will be obtained from the job template assigned by Enterprise Manager administrator to this vSphere user.
Job Management

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 the job on the Jobs tab and click Job > Delete on the toolbar. After deletion, this job will be removed from configuration and no longer appear in web portal.

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.

IMPORTANT!

Job cloning is not available.
Managing vSphere User VMs

On the VMs tab of the vSphere self-service portal you can:

- Search and browse VMs and browse VMs details
- Restore VMs
- 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, locate the necessary VM backup in the list of VMs displayed, or search by VM name.
2. For the selected VM backup, click Restore VM button, then select the option you need:
   - Select the Overwrite option if you want to replace the VM in production. 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 production VM and will have the same name with the _restored suffix added to the VM name.

3. Select the restore point that will be used to restore the VM.
4. You can select additional options for the VM restore:
   - Select the **Power on VM after restoring** option if you want to turn on the VM once it is restored.
   - Select the **Quick rollback (restore changed blocks only)** option if you want to restore only the changed data. This option is available only for VMs which were protected with the Changed Blocks Tracking (CBT) option.
   - Select the **Restore VM tags** option if you want to restore the vSphere VM tags of the VM.

5. After you click **Restore**, you will get a message notifying you of the operation effect (VM from backup will replace production VM, if present in the original location). Click **Proceed** or **Cancel** the operation.

   You can view VM restore progress in the **VMs** tab after you click **View history**.

### Deleting VMs

To delete a VM, select the VM and click **Delete**. Press **Yes** in the **Delete VM** window.

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.
vSphere User Files Restore

Files tab of the vSphere self-service portal allows you to browse 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. For details, see Performing 1-Click File Restore.

NOTE:
Consider the following:

- If you restore files from non-indexed VM guest, the mount operation will be performed using mount server assigned to the corresponding backup repository.
vSphere User Items Restore

**Items** tab of vSphere self-service portal allows you to perform item-level recovery from application-aware backups: SQL Server databases and Oracle databases.

To restore application items (SQL Server databases or Oracle databases), follow the steps described in the [Restore Procedure for SQL Server](#) databases and [Restore Procedure for Oracle](#) databases.
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. Installing Veeam Backup Search (optional)

Before you install Veeam Backup Search, check system requirements. Then use the follow the setup steps to install the product.
Step 1. Install Microsoft Search Server

Select a machine which will function as a search server and install Microsoft Search Server on this machine. Keep in mind that Microsoft Search Server can be installed on Windows Server machine only.

**NOTE:**

Microsoft Search Server must be installed by a user who has administrator permissions on the computer.

Step 2. Start Veeam Backup Search Setup Wizard

On the machine where Microsoft Search Server is installed, run the setup file (Veeam_Backup_Search_Setup_x86.exe or Veeam_Backup_Search_Setup_x64.exe) located in the Search folder of the mounted Veeam Backup & Replication installation image (.iso file) or the installation CD/DVD.
Step 3. Read and Accept License Agreement

Read and accept the terms in the license agreement to continue installation. If you select I do not accept the terms in the license agreement, the installation process will be terminated.
Step 4. Select Installation Folder

Specify the installation folder. Use the Change button to select a necessary installation folder.
Step 5. Specify Service Account Settings

Specify the user name and password to be used by the Veeam Backup Search service. Change the number of TCP port if it is necessary. By default, Veeam Backup Search uses port number **9395**.
Step 6. Begin Installation

Click **Install** to begin installation. Veeam Backup Search will be installed on your computer. Once installation is complete, click **Finish** to exit the setup wizard.
Step 7. Specify the Default Account for Crawling Content

Specify the default account that will be used by Microsoft Search Server for crawling indexing content. This account must have read access to the shared VBRCatalog folder on the Veeam Backup Enterprise Manager server.

For Microsoft Search Server 2010

1. Select Programs > Microsoft SharePoint 2010 Products > SharePoint 2010 Central Administration from the Start menu on the search server.
2. Click Application management on the left. In the Application Management section, click Manage service applications.
3. On the Manage Service Applications page, click the Search service application.
4. In the System Status section on the Search Administration page, locate the default content access account, which is in the form Domain\Username. Click the default content access account name and enter the required account data — user name and password — in the displayed Default Content Access Account window.

For Microsoft Search Server 2008

1. Select Programs > Search Server Administration from the Start menu on the search server.
2. Click Crawling on the left.
3. On the Crawling page, click Default content access account and enter the required account data — user name and password.
Adding a Search Server (optional)

To add a search server:

1. Open the **Configuration** tab.
2. Open the **Search Servers** section in the left pane of the **Configuration** view.
3. Click **Add** at the top of the **Search Servers** view.
4. In the **Search Server Settings** window, enter a full DNS name or IP address of the server you want to add. Provide a description if necessary.
5. By default, the account under which Veeam Backup Service is running will be used for the added server. To specify a different account, select **Use these credentials** and provide a name and a password of a user with administrative privileges on the search server.
6. Specify the port used by the Veeam Backup Search Server Integration Service. By default, port number **9395** is used.
7. In the **Capacity** section, select the type of database server you are planning to use to set a recommended capacity value for the indexing server. Specify the limit of index documents to be created. By default, the limit is set to **300,000** documents.
8. Click **OK** to add the server.

**NOTE:**

Microsoft Search Server crawls content in the shared **VBRCatalog** folder on the Veeam Backup Enterprise Manager server. Therefore, the search server account should be granted access to that folder. When you click **OK** to add a search server, Veeam Backup Enterprise Manager will verify if required permissions are granted, and display a warning message if permissions are not enough.

To edit the settings of an existing server, select it in the **Search Servers** list and click **Edit** on the toolbar.

To remove a search server, select it in the **Search Servers** list and click **Remove** on the toolbar.