Veeam Backup Enterprise Manager

Version 13

User Guide

November, 2026

© 2026 Veeam Software.

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

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

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE 9
ABOUT THIS GUIDE 10
ABOUT VEEAM BACKUP ENTERPRISE MANAGER 11
How Enterprise Manager Works 12
Enterprise Manager Components 13
PLANNING AND PREPARATION 15
System Requirements 16
Permissions 23
Ports 25
DEPLOYMENT 35
Enterprise Manager Deployment on Linux 36
Veeam Software Appliance Installation 37
Veeam Software Appliance Update 58
Enterprise Manager Deployment on Windows 65
Installing Enterprise Manager 66
Upgrading to Enterprise Manager 13.1 84
Updating Enterprise Manager 94
Uninstalling Enterprise Manager 95
Migrating Enterprise Manager 96
Silent Installation, Upgrade and Uninstallation 101
Migrating Enterprise Manager from Windows to Linux 115
Connecting Enterprise Manager to Another Configuration Database 118
Connecting to Another Database Using Wizard 119
Connecting to Another Database in Unattended Mode 127
HOST MANAGEMENT 132
About Veeam Host Management 133
Accessing Veeam Host Management Console 136
Configuring Veeam Host Management Localization Settings 139
Configuring Network Settings 140
Changing Server Name 141
Managing Domain Settings 143
Configuring Network Interfaces 144
Configuring HTTPS Proxies 151
Configuring Server Time Settings 153
Managing Storage 159
Configuring Remote Access Settings 163
Managing Users and Roles 169

Configuring Users 170
Performing Initial Security Officer Login 174
Managing User Authentication 176
Managing Certificates 182
Configuring Backup Infrastructure Settings 184
Managing Updates 185
Performing Maintenance Tasks 186
Performing Security Officer Tasks 194
ACCESSING ENTERPRISE MANAGER 199
EXPLORING ENTERPRISE MANAGER 201
Viewing Dashboard 204
CONFIGURING ENTERPRISE MANAGER 207
Initial Configuration 208
Managing Backup Servers 209
Adding Backup Servers 210
Editing Backup Servers 213
Removing Backup Servers 214
Collecting Data from Backup Servers 215
Reports on Backup Servers 218
Audit Reports 220
Customizing Dashboard Chart 224
Viewing vCenter Servers 225
Managing Encryption Keys 226
Generating Enterprise Manager Keyset 227
Activating Enterprise Manager Keyset 228
Specifying Retention Settings for Enterprise Manager Keyset 229
Exporting and Importing Enterprise Manager Keyset 230
Deleting Enterprise Manager Keyset 232
Handling Password Recovery Requests 233
Configuring Accounts and Roles 235
Accounts and Roles Overview 236
Managing Accounts 239
Configuring SAML Authentication Settings 252
SAML Authentication Support 257
Configuring AD FS for SAML Authentication 260
Configuring Retention Settings for Index and History 262
Managing TLS Certificates 265
How Enterprise Manager Authenticates to Backup Servers 266
Installing Certificates 267
Using Certificate Signed by Internal CA 270

Licensing 272
Installing License 274
Viewing License Details 275
Updating License 277
Revoking License 281
Removing License 282
Managing Monthly Usage Reports 283
Configuring Updates Mirror 288
Configuring Notification Settings 290
Mail Server Settings 291
Notifications on Job Results 296
Notifications on Restore Operations 298
Notifications on Licensing 299
Notifications on Key Management 301
Notifications on Updates 302
Viewing Information About Enterprise Manager 303
Managing Languages 304
Language Files Overview 305
Adding Languages 306
MANAGING JOBS 310
Viewing Jobs 311
Starting, Stopping and Retrying Jobs 312
Enabling and Disabling Jobs 313
Editing Jobs 314
Step 1. Launch Wizard 315
Step 2. Edit Job Name and Retention Settings 316
Step 3. Edit List of VMs 318
Step 4. Change VM Processing Order 321
Step 5. Configure Guest Processing Settings 322
Step 6. Edit Job Schedule 342
Creating Active Full Backups 346
Cloning Jobs 347
Deleting Jobs 348
MANAGING CDP POLICIES 349
Viewing Policies 350
Enabling and Disabling Policies 352
Editing Policies 353
Step 1. Launch Edit Policy Wizard 354
Step 2. Edit Policy Name and Description 355
Step 3. Edit List of VMs 356

Step 4. Edit Policy Schedule 359
Step 5. Configure Guest Processing Settings 362
Deleting Policies 374
WORKING WITH UNSTRUCTURED DATA 375
Viewing Unstructured Data Backups 376
Browsing for Items in Unstructured Data Backups 378
Searching for Items in Unstructured Data Backups 380
Data Recovery 381
Instant File Share Recovery 382
Restoring Specific Files 395
Deleting Backups 402
WORKING WITH MACHINES 403
Viewing Machines 404
Deleting Machine from Backup 406
Quick Backup 407
VM Recovery 409
Instant Recovery 410
Entire VM Restore 441
Virtual Disk Restore 469
VM Failover 477
Failover Plans 482
GUEST OS FILE RESTORE 484
Veeam Backup Catalog 486
Veeam Backup Search Capabilities 487
File-Level Restore Capabilities 489
How Indexing Works 490
Indexing Data 491
Indexing Data Retention 496
Preparing for File Browsing and Searching 498
Performing Catalog Replication and Indexing 499
Preparing for File Search and Restore (non-Windows machines) 500
Browsing Machine Backups for Guest OS Files 502
Searching for Guest OS Files in Machine Backups 504
Performing Simple Search 505
Performing Advanced Search 506
Performing 1-Click File Restore 507
Restoring Files to Original Location 508
Downloading Files to Local Machine 510
Using Restore Lists 512
Restoring Files to Another Location 514

Using Self-Service File Restore Portal to Restore Guest Files 518
APPLICATION ITEM RESTORE 521
Restoring Microsoft Exchange Items 522
Restoring Microsoft SQL Server Databases 525
Restore to Original Location 526
Restore with Custom Settings 528
Restoring Oracle Databases 534
Restore to Original Location 535
Restore with Custom Settings 537
Restoring PostgreSQL Instances 545
Restore to Original Location 546
Restore with Custom Settings 548
VEEAM AGENTS SUPPORT 554
Guest File Browsing and 1-Click Restore 555
Preparing for File Browsing and Restore 556
Browsing and Restoring Guest OS Files 559
Application Item Restore 561
VSPHERE SELF-SERVICE BACKUP PORTAL 562
Configuring Delegation Mode 564
Managing Tenant Accounts 566
Adding Tenant Account 567
Editing Tenant Account 571
Exporting List of Tenant Accounts 573
Removing Tenant Account 574
Using vSphere Self-Service Backup Portal 575
Viewing Self-Service Backup Portal Statistics 577
Managing Backup Jobs 579
Managing VMs 582
Restoring Guest OS Files 585
Restoring Application Items 586
VEEAM PLUG-IN FOR VMWARE VSPHERE CLIENT 587
Plug-in Deployment 588
Installing vSphere Client Plug-in 589
Uninstalling vSphere Client Plug-in 590
Accessing vSphere Client Plug-in 591
Veeam Plug-in for VMware vSphere Client Authentication 592
Examining Backup Infrastructure 593
Creating Restore Points with VeeamZIP and Quick Backup 594
Creating Full VM Backup with VeeamZIP 595
Creating Incremental VM Backup with Quick Backup 598

VEEAM SELF-SERVICE BACKUP PORTAL FOR CLOUD DIRECTOR 599
Managing Configurations for Cloud Director Organizations 601
Before You Begin 602
About Organization Quota 604
Viewing Organization Configurations 605
Adding Organization Configuration 606
Mapping Jobs and CDP Policies to Organization Configurations 609
Editing Organization Configuration 610
Removing Organization Configuration 611
Exporting Configuration Report 613
Configuring Veeam Self-Service Backup Portal UI 614
Using Veeam Self-Service Backup Portal 615
Access Control 616
Accessing Veeam Self-Service Backup Portal 617
Working with Veeam Self-Service Backup Portal 621
GETTING SUPPORT 667
Enterprise Manager Logs 668

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

About This Guide

This guide provides information on how to install and use Veeam Backup Enterprise Manager 13 until it is replaced with a newer version of the product.

Intended Audience

The user guide is intended for IT administrators, consultants, analysts and other IT professionals using the product. This guide assumes that you have a good understanding of Veeam Backup & Replication and VMware vSphere.

About Veeam Backup Enterprise Manager

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

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 jobs and policies across the backup infrastructure, analyze operation statistics of Veeam backup servers, perform restore operations, and so on.

In particular, with Veeam Backup Enterprise Manager you can:

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

How Enterprise Manager Works

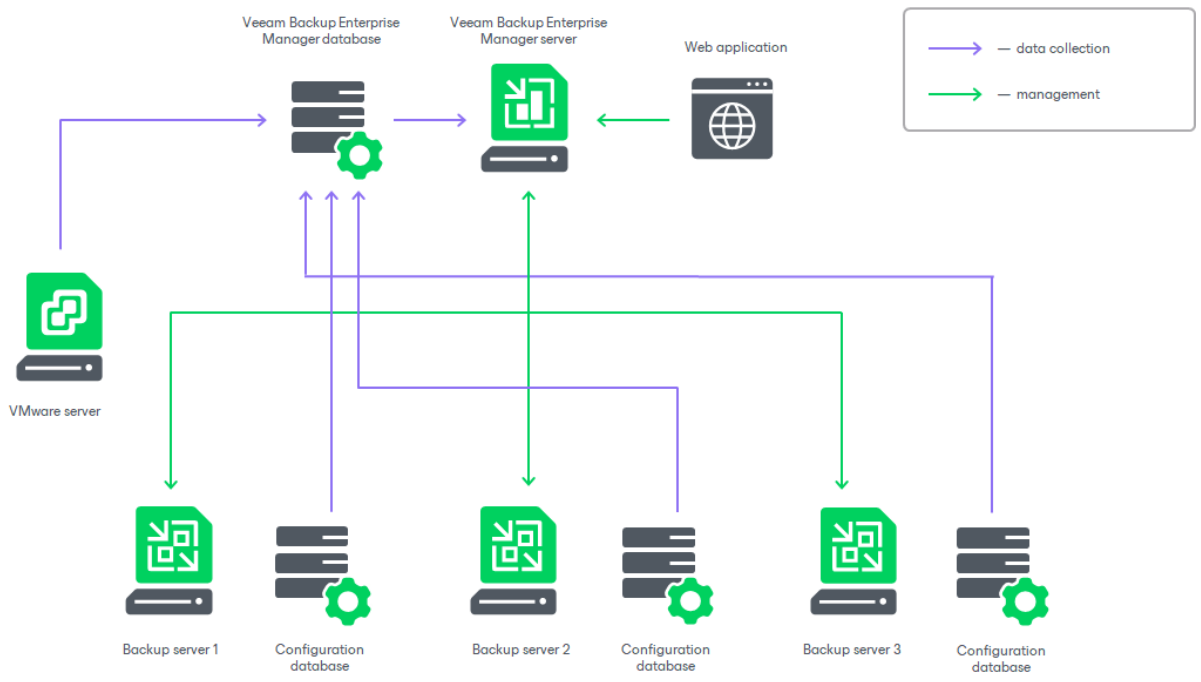
Veeam Backup Enterprise Manager aggregates data from multiple backup servers, as well as from the underlying VMware vCenter Servers.

1. Veeam Backup Enterprise Manager retrieves data from managed 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 backup servers.

   If a backup server is added as a High Availability cluster, Enterprise Manager collects the data from an active cluster node. After a node switchover, Enterprise Manager will automatically collect the data from the other active node.

2. Collected data is stored to the Veeam Backup Enterprise Manager database and can be accessed by multiple users from the web interface. This web interface also allows for modifying job settings, license management, installing Veeam plug-in on vCenter Server, and other tasks.

3. When a user modifies a backup job using Veeam Backup Enterprise Manager, these changes are communicated to the backup server that manages the job and stored in its configuration database.



If you have a Veeam Agent integrated with Veeam Backup & Replication, you can use Veeam Backup Enterprise Manager to browse and restore guest OS files and application items from a backup stored in a Veeam backup repository. These processes involve appropriate backup job setup, as well as mount and data transfer operations. For more information, see Veeam Agents Support.

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. On Microsoft Windows machines, the 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.
- *Veeam Enterprise Manager Identity Service* manages authentication and identity-related operations for Veeam Backup Enterprise Manager.
- *Veeam Catalog Service* is used for guest OS file indexing, index data retention and its synchronization with the information on backup servers. It comprises a Windows service named Veeam Guest Catalog also installed on the Veeam Backup Enterprise Manager server. For more information, see Veeam Backup Catalog.
- *Veeam Enterprise Manager Web UI Service* hosts and delivers the Veeam Backup Enterprise Manager web application when deployed on Linux-based systems.
- *Veeam Backup Enterprise Manager REST API Service* allows you to communicate with Veeam Backup Enterprise Manager using HTTP and HTTPS protocols and the principles of REST. For more information, see the Veeam Backup Enterprise Manager REST API Reference.
- Veeam Backup Update Service enables the update of Enterprise Manager. The service runs locally and does not connect to the internet. It only requires a connection to the Enterprise Manager configuration database.
- [For Linux-based Enterprise Manager] *Veeam Updater* and *Veeam Updater package manager* are used to manage Veeam Software Appliance updates, this includes OS and Enterprise Manager updates. For details, see Veeam Software Appliance Update.
- [For Linux-based Enterprise Manager] *Veeam Host Management Service* allows you to configure host settings. For details, see Host Management.
- *Veeam Plug-in for VMware vSphere Client Service* allows vSphere administrators to manage backup infrastructure of the virtual environment. For more information, see Veeam Plug-in for VMware vSphere Client.
- [For Microsoft Windows-based Enterprise Manager] *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 Exploring Enterprise Manager.
    - *Veeam Self-Service File Restore Portal* that allows administrators to restore files or folders from the guest OS of a virtual or physical machine. For more information, see Using Self-Service File Restore Portal to Restore Guest OS Files.
    - *Veeam Self-Service Backup Portal* and *Veeam Plug-in for VMware Cloud Director* that provide members of VMware Cloud Director organizations with a UI for self-service operations on machine protection. For more information, see Veeam Self-Service Backup Portal for Cloud Director.

- *VMware vSphere Self-Service Backup Portal* that provides Service Providers with a UI for managing access permissions and vSphere quotas for their customers. For more information, see vSphere Self-Service Backup Portal.

> **NOTE**
>
> Veeam Self-Service File Restore Portal, Veeam Self-Service Backup Portal, Veeam Plug-in for VMware Cloud Director and VMware vSphere Self-Service Backup Portal features are available in the Enterprise Plus edition license.

- *PostgreSQL or Microsoft SQL Server database* is used to store configuration and performance data. Note that you can use a Microsoft SQL Server database with Microsoft Windows-based Enterprise Manager only.
- *Veeam Backup Search* is an optional component used for guest OS file indexing of protected machines. This component is included in the installation package to provide backward compatibility with older existing deployments. For a new deployment, there is no need to install Veeam Backup Search since all operations related to guest OS file indexing and search will be performed by Veeam proprietary built-in indexing engine. For more information, see Veeam Backup Search Capabilities.

Planning and Preparation

Before you install Veeam Backup Enterprise Manager, you must check that the virtual environment and machines that you plan to use as backup infrastructure components meet the product hardware recommendations and system requirements.

In This Section

- System Requirements
- Permissions
- Ports

System Requirements

Make sure that machines that you plan to use as Veeam Backup Enterprise Manager infrastructure components meet the following system requirements.

Veeam Backup Enterprise Manager

Server Side

Enterprise Manager on Linux (Veeam Software Appliance)

Specification	Requirement

Hardware	CPU: x86-64 processor with a minimum of 2 cores (vCPUs). 4 or more cores (vCPUs) are recommended, depending on the load. Memory: Minimum of 6 GB RAM. 16 GB RAM is recommended. *Disk Selection Logic*: When selecting a disk for system and adjacent functions, Veeam Software Appliance automatically chooses an SSD over an HDD, and selects the smaller disk of the two available. The sizing recommendations for Disk 1 below remain valid for the system disk. *Disk 1*: 240 GB[1] minimum. This disk hosts Veeam JeOS, Enterprise Manager Veeam Backup & Replication software, configuration database and instant recovery cache. **Recommended** sizing depends on the number of protected workloads. Sizing also accounts for configuration database growth as you add more workloads to protect: • 480 GB[1] SSD for small environments (up to a few hundred workloads). • 960 GB[1] SSD for medium-sized environments (up to a few thousand workloads). • Multi-TB[1] SSD for large environments. Larger capacity increases the disk space available to instant recovery cache, allowing for running more machines for longer time. **Note**: Resizing existing local disks is not supported. A ready-to-use Microsoft Hyper-V virtual machine image is also available for Veeam Software Appliance deployment, in addition to the ISO and OVA files. *Disk 2*: 240 GB[1] minimum. This disk hosts guest file system catalogs and backups, therefore recommended sizing depends on your backup storage needs. Any additional disks found in the system during Veeam Software Appliance deployment will be automatically joined with Disk 2 into the single Logical Volume Manager (LVM) spanned volume. **Note**: During deployment, Veeam Software Appliance supports only local disks and hardware RAID. RAID controller with battery or capacitor backed write cache is highly recommended for performance and reliability reasons. After deployment, you can add Fibre Channel and iSCSI storage devices, including multipathing. For more information, see <%TARGETTITLE%>. *Network*: 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported. *Server Hardware*: Veeam offers Veeam Ready - Appliance certification for hardware vendors. This certification guarantees verified and certified compatibility, delivering an optimal customer experience through additional requirements for direct technical collaboration between vendors. Veeam also acknowledges that some customers may need to use existing hardware. As a current compatibility guidance, we expect that most systems compatible with RHEL 9.6 listed on the RHEL Hardware Compatibility List (HCL) will be compatible with Veeam Software Appliance. Hardware that is not listed on the RHEL HCL will likely work, but no official compatibility support will be provided. [1] Here GB is considered as 10^9 bytes, TB as 10^12 bytes.

Specification	Requirement
OS	Veeam JeOS (Just Enough Operating System), the operating system underpinning Veeam Software Appliance, is built on Rocky Linux from CIQ (RLC Pro), which provides long-term support and FIPS 140-3 validated packages.
Configuration Database	If you are planning to use a remote installation of the PostgreSQL on Linux, ensure that the following packages are installed on it: • postgresql17.x86_64 • postgresql17-contrib.x86_64 • postgresql17-libs.x86_64 • postgresql17-plperl.x86_64 • postgresql17-server.x86_64 All of them must be of version 17.6 or later.
Software	• VMware vSphere ESXi 7.0 U2 (7.0.2) or later for OVA deployments. • Veeam Software Appliance ISO deployment to a virtual machine is supported for all hypervisors for which Veeam offers host-based VM backup functionality. For details, see Supported Platforms, Applications and Workloads.

Enterprise Manager on Windows

Specification	Requirement
Hardware	• CPU: x86-64 processor. • Memory: 8 GB RAM (minimum recommended). • Hard disk space: 2 GB for product installation plus sufficient disk space to store guest file system catalog from connected backup servers (according to data retention policy). • Network: 1 Mbps or faster connection to Veeam Backup & Replication servers. Slow or unstable links will impact the performance of Veeam Backup Enterprise Manager data collection operations from Veeam Backup servers.
OS	64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (from version 22H2 to version 25H2) • Microsoft Windows 10 22H2 • Microsoft Windows 10 LTSC 2021

Specification	Requirement
PostgreSQL	Local or remote installation of PostgreSQL 14.x, 15.x or 17.x (version 17.10 is included in the setup). Note that Veeam Backup Enterprise Manager does not support PostgreSQL installations on cloud database services (for example, Amazon Relational Database Service (RDS).
Microsoft SQL Server	Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported): • Microsoft SQL Server 2025 • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 All editions of Microsoft SQL Server are supported. The usage of Microsoft SQL Server Express Edition is limited by the database size up to 10 GB. If you plan to have larger databases, use other editions of Microsoft SQL Server. Veeam Backup & Replication and Veeam Backup Enterprise Manager configuration databases can be deployed in Microsoft SQL AlwaysOn Availability Groups. For more information, see this Veeam KB article.
Software	During setup, the system configuration check is performed to determine if all prerequisite software is available on the machine where you plan to install Enterprise Manager. If some of the required software components are missing, the setup wizard will offer you to install missing software automatically. This refers to the following software: • Microsoft .NET Framework 4.8 • Microsoft .NET Hosting 10.0 • Microsoft SQL Server System CLR Types 2014 (both for SQL Server and PostgreSQL) • Microsoft Visual C++ 2017-2026 Redistributable 14.50.35719.0 • Application Request Routing 3.0.05311 • ASP.NET Core Module 8.0.21 The following software must be installed manually if missing: • Microsoft Windows Installer 5.0 • Microsoft Internet Information Services 7.5 or later • Microsoft URL Rewrite 2.0 for IIS 7

Client Side

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

[Optional] VMware Cloud Director

Specification	Requirement
VMware Cloud Director	VMware Cloud Director 10.4.x to 10.6.x.
Other software	If your Enterprise Manager deployment uses IIS 8.5, a URL rewrite module is required to work with Veeam Self-Service Backup Portal for VMware Cloud Director.

[Optional] Veeam Plug-in for VMware vSphere Client

Specification	Requirement
VMware vSphere	VMware vSphere 7.0 to 9.0.

Permissions

This section provides information on the account permissions required for installing, upgrading and using Veeam Backup Enterprise Manager on Microsoft Windows machines.

Veeam Backup Enterprise Manager

Account	Required Permissions
Setup accounts	The account used to run the setup must have the local Administrator permissions on the target machine.
	[Configuration database on PostgreSQL] The PostgreSQL account must be a superuser.
	[Configuration database on Microsoft SQL Server] Your account must have the following Microsoft SQL Server permissions: • To create a new Veeam Backup Enterprise Manager database during the setup process, the account must have the CREATE ANY DATABASE permission on the Microsoft SQL Server level. After the database is created, this account automatically gets the *db_owner* role and can perform all operations with the database. If a database is created in advance (by a database administrator or Microsoft SQL Server administrator), the setup account must have the *db_owner* role for the database. • To upgrade an existing Microsoft SQL Server database, the account must have the *db_owner* role.

Account	Required Permissions
Veeam Backup Enterprise Manager service account	Use the Local System account as the Veeam Backup Enterprise Manager Service account. If you set another account to run this service, this account must have the following permissions: • *Local Administrator* permissions on the Veeam Backup Enterprise Manager server. • *Log on as a service* permission (granted automatically to the Veeam Backup Enterprise Manager Service account). • [Configuration database on PostgreSQL] The PostgreSQL account must be a superuser. • [Configuration database on Microsoft SQL Server] *Db_datareader* and *db_datawriter* roles, as well as permissions to execute stored procedures for the Enterprise Manager configuration database. Alternatively, you can assign this account the *db_owner* role for the this database to the service account. • *Full Control* NTFS permissions for the *VBRCatalog* or another folder where index files are stored. To add Active Directory user or group accounts to the Veeam Backup Enterprise Manager roles, the Veeam Backup Enterprise Manager service must be started under the Active Directory service account that has permissions to enumerate Active Directory domains. Active Directory users have enough permissions to enumerate Active Directory domains by default. If you use the local machine account instead, you will get the "*Cannot find user account DOMAIN|username*" error.
Enterprise Manager user	To work with the Veeam Backup Enterprise Manager web UI, users must be assigned the Portal Administrator, Portal User, or Restore Operator role. For more information, see Configuring Accounts and Roles.
vSphere Client Plug-in for Veeam Backup & Replication (optional)	The account used to install the plug-in and the vCenter Server account must belong to the same Active Directory domain in case of cross-domain access. The account used to install the plug-in must be assigned the following vCenter Server permissions: • To install the plug-in: **Extension** > **Register extension** • To uninstall the plug-in: **Extension** > **Unregister extension**
vSphere Self-Service Backup Portal user	The account used to work with vSphere Self-Service Backup Portal must have interactive logon permissions on the Enterprise Manager server.

Ports

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

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

Veeam Backup Enterprise Manager on Linux (Veeam Software Appliance)

From	To	Protocol	Port	Notes
Veeam Software Appliance	Linux-based backup server	TCP	443	Default port required for initial connection to a backup server and to its Identity Service. This is also the default port used by the Veeam Guest Catalog service for catalog replication.
			6162, 2500 to 3300	Ports used to replicate guest OS index data, trasfer audit logs and restore files.
	Microsoft Windows-based backup server	TCP	9405	Default certificate port used by Enterprise Manager for collecting data from backup servers with version 12 installed.
			9392	Default port required for initial connection to a backup server.
			443	Default port used by the Veeam Guest Catalog service for catalog replication. This is also the default certificate port used by Enterprise Manager for collecting data from backup servers with version 13 installed.
			6162, 2500 to 3300	Ports used to replicate guest OS index data, trasfer audit logs and restore files.

From	To	Protocol	Port	Notes
			49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.
	PostgreSQL hosting the Enterprise Manager configuration database	TCP	5432	Default port used for communication with PostgreSQL hosting the Enterprise Manager configuration database.
	VMware vCenter Server	TCP	443	Default port used for connection to a vCenter Server and deploying the Veeam Plug-in for vSphere Client.
	DNS server with forward/reverse name resolution of all backup servers	UDP	53	Port used for communication with the DNS Server.
	Active Directory domain controller	TCP, UDP	389	Port used by Enterprise Manager service to communicate with Active Directory through the LDAP protocol.
		TCP	636	Port used by the Enterprise Manager service to communicate with Active Directory through the LDAPS (LDAP over TLS/SSL) protocol.
		TCP	3268	Port used by the Enterprise Manager service to communicate with LDAP Global Catalog.
		TCP	3269	Port used by the Enterprise Manager service to communicate with LDAP Global Catalog through TLS/SSL.
		TCP	49152 to 65535	Ports used by the Enterprise Manager service to communicate with Active Directory. These ports are also used during restore through Veeam Self-Service File Restore Portal. This is a default dynamic port range. For more information, see Microsoft Support KB 832017.

From	To	Protocol	Port	Notes
	Veeam Update Repository (*repository.veeam.com*)	TCP	443	Port used by Veeam Software Appliance to connect to the Veeam Update Repository, a public Veeam-maintained repository that provides product, operating system, and security updates. For more information, see How Updates Work.
	Veeam Update Repository (*<localmirror.domain>*)	TCP	80	Port used by Veeam Software Appliance to connect to a local mirror of the Veeam Update Repository. For more information, see Configuring Updates.
	Veeam License Update Server (*vbr.butler.veeam.com*, *autolk.veeam.com*)	TCP	443	Default port used to automatically update license from the Veeam License Update Server through HTTPS.
			80	Required for certificate validation when Enterprise Manager connects to Veeam License Update Server to check if the new license is available and download it. Certificate verification endpoints: • `*.ss2.us` • `*.amazontrust.com` Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate details in the following fields: • *CRL Distribution Points* • *Authority Information Access*
Veeam Backup Enterprise Manager web application (Nginx)	Veeam Backup Enterprise Manager Service	TCP	9394	Default internal port used by Nginx to communicate with Veeam Backup Enterprise Manager through gRPC.

From	To	Protocol	Port	Notes
Browser	Veeam Backup Enterprise Manager web application (Nginx)	TCP	443	Default ports used to communicate with the Enterprise Manager website and Identity Service through HTTPS. When you work with Veeam Self-Service Backup Portal (accessed by the portal URL or from the native VMware Cloud Director environment) and vSphere Self-Service Backup Portal, your browser also communicates with the Veeam Backup Enterprise Manager website through this port.
Veeam Backup Enterprise Manager REST API client and VMware vSphere Client plug-in	Veeam Backup Enterprise Manager REST API	TCP	9398	Default port used to communicate with Veeam Backup Enterprise Manager REST API through HTTPS.
Veeam ONE Server (optional)	Veeam Backup Enterprise Manager Service	TCP	50001	If you add the Enterprise Manager server to the Veeam ONE monitoring scope, this port is used for data collection through gRPC.
Management client PC (remote access)	Veeam Backup Enterprise Manager Service	TCP	10443	Default port used by the Linux-based Enterprise Manager to connect to Veeam Host Management.

Veeam Backup Enterprise Manager on Windows

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager	Linux-based backup server	TCP	443	Default port required for initial connection to a backup server and to its Identity Service. This is also the default port used by the Veeam Guest Catalog service for catalog replication. You can customize the port when you add a backup server. For more information, see Adding Backup Servers.
			6162, 2500 to 3300	Ports used to replicate guest OS index data, trasfer audit logs and restore files.
	Microsoft Windows-based backup server	TCP	9405	Default certificate port used by Enterprise Manager for collecting data from backup servers with version 12 installed.
			9392	Default port required for initial connection to a backup server.
			443	Default port used by the Veeam Guest Catalog service for catalog replication. This is also the default certificate port used by Enterprise Manager for collecting data from backup servers with version 13 installed.
			6162, 2500 to 3300	Ports used to replicate guest OS index data, trasfer audit logs and restore files.
			49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.
	PostgreSQL hosting the Enterprise Manager configuration database	TCP	5432	Default port used for communication with PostgreSQL hosting the Enterprise Manager configuration database.

From	To	Protocol	Port	Notes
	Microsoft SQL Server hosting the Enterprise Manager configuration database	TCP	1433	Default port used for communication with Microsoft SQL Server hosting the Enterprise Manager configuration database. Additional ports may be needed depending on your configuration. For more information, see the Microsoft SQL Docs Configure the Windows Firewall to Allow SQL Server Access article.
	VMware vCenter Server	TCP	443	Default port used for connection to a vCenter Server and deploying the Veeam Plug-in for vSphere Client. Can be customized during Enterprise Manager installation. For more information, see Specify Service Ports.
	DNS server with forward/reverse name resolution of all backup servers	UDP	53	Port used for communication with your DNS Server.
	Active Directory domain controller	TCP, UDP	389	Port used by the Enterprise Manager service to communicate with Active Directory through the LDAP protocol.
		TCP	636	Port used by the Enterprise Manager service to communicate with Active Directory through the LDAPS (LDAP over TLS/SSL) protocol.
		TCP	3268	Port used by the Enterprise Manager service to communicate with LDAP Global Catalog.
		TCP	3269	Port used by the Enterprise Manager service to communicate with LDAP Global Catalog through TLS/SSL.

From	To	Protocol	Port	Notes
		TCP	49152 to 65535	Ports used by the Enterprise Manager service to communicate with Active Directory. These ports are also used during restore through Veeam Self-Service File Restore Portal. This is a default dynamic port range. For more information, see Microsoft Support KB 832017.
	Veeam License Update Server (*vbr.butler.veeam.com*, *autolk.veeam.com*)	TCP	443	Default port used to automatically update license from the Veeam License Update Server through HTTPS.
			80	Required for certificate validation when Enterprise Manager connects to Veeam License Update Server to check if the new license is available and download it. Certificate verification endpoints: • `*.ss2.us` • `*.amazontrust.com` Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate details in the following fields: • *CRL Distribution Points* • *Authority Information Access*
Veeam Backup Enterprise Manager website (IIS extension)	Veeam Backup Enterprise Manager service	TCP	9394	Default port used by IIS extension to communicate with Veeam Backup Enterprise Manager. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.

From	To	Protocol	Port	Notes
Browser	Veeam Backup Enterprise Manager website (IIS extension)	TCP	9080	Default ports used to communicate with the website through HTTP. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports. When you work with Veeam Self-Service Backup Portal (accessed by the portal URL or from the native VMware Cloud Director environment) and vSphere Self-Service Backup Portal, your browser also communicates with the Veeam Backup Enterprise Manager website through this port.
		TCP	9443	Default ports used to communicate with the website through HTTPS. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports. When you work with Veeam Self-Service Backup Portal (accessed by the portal URL or from the native VMware Cloud Director environment) and vSphere Self-Service Backup Portal, your browser also communicates with the Veeam Backup Enterprise Manager website through this port.
Veeam Backup Enterprise Manager REST API client and VMware vSphere Client plug-in	Veeam Backup Enterprise Manager REST API	TCP	9399	Default port used to communicate with Veeam Backup Enterprise Manager REST API through HTTP. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.
		TCP	9398	Default port used to communicate with Veeam Backup Enterprise Manager REST API through HTTPS. Can be customized during Veeam Backup Enterprise Manager installation. For more information, see Specify Service Ports.

From	To	Protocol	Port	Notes
Veeam ONE Server (optional)	Veeam Backup Enterprise Manager server	TCP	Dynamically assigned ports	If you add the Enterprise Manager server to the Veeam ONE monitoring scope, this port is used for data collection through gRPC.

NOTE

Consider the following:

- For communication between Enterprise Manager and backup servers, Kerberos authentication is used by default.
- During installation, Enterprise Manager 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.

Data Recovery Operations

Guest OS File Restore (Windows)

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager server	Mount server associated with backup repository	TCP	6162, 2500 to 3300	Ports used for file download.

Guest OS File Restore (non-Windows)

From	To	Protocol	Port	Notes
Veeam Backup Enterprise Manager server	Mount server (helper host or helper appliance)	TCP	6162, 2500 to 3300	Ports used for file download. For more information on the mount server, see Preparing for File Search and Restore (non-Windows machines).

NOTE

Consider the following:

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

Application Item Restore

When you restore application items, Enterprise Manager sends a command to the required backup server to trigger the components involved in the restore process. For details on the required ports, see the *Ports* sections of the Veeam Backup & Replication User Guide:

- Veeam Exrplorer for Microsoft Exchange
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Oracle
- Veeam Exrplorer for PostgreSQL

Deployment

You can deploy Veeam Backup Enterprise Manager on a Linux or Microsoft Windows machine.

In This Section

- Enterprise Manager Deployment on Linux
- Enterprise Manager Deployment on Windows
- Migrating Enterprise Manager from Windows to Linux

Enterprise Manager Deployment on Linux

To begin working with Veeam Backup Enterprise Manager on Linux, you must install Veeam Software Appliance on a machine that meets the system requirements. Veeam Software Appliance is a software solution that packages Enterprise Manager or Veeam Backup & Replication together with the Rocky Linux operating system.

Using Veeam Software Appliance simplifies both installation and update processes. When installing Veeam Software Appliance, the setup deploys both Rocky Linux and the selected product. To update Veeam Software Appliance, you can use Veeam Updater, which allows you to manually check for updates, install them and view update history.

Veeam Software Appliance Installation

To start working with Veeam Backup Enterprise Manager on Linux, you must deploy an Enterprise Manager server — install Veeam Software Appliance on a machine that meets the system requirements. To do this, you can use the ISO or OVA file.

After you install Veeam Software Appliance, you can access the Veeam Backup Enterprise Manager website. For details, see Accessing Enterprise Manager.

In This Section

- Considerations and Limitations
- Installing Veeam Software Appliance from ISO
- Reinstalling Veeam Software Appliance from ISO
- Installing Veeam Software Appliance from Microsoft Hyper-V Template
- Automated Veeam Software Appliance Installation

Considerations and Limitations

Before you install Veeam Software Appliance, review known issues and limitations described in release notes. Also, consider the following:

- Veeam Software Appliance must be installed on a dedicated empty machine that meets the system requirements. For more information, see System Requirements.
- Veeam Software Appliance cannot be installed on machines that have pre-existing multipath storage devices. However, you can configure multipath storage devices after you complete the installation process. For more information, see <%TARGETTITLE%>.
- Enterprise Manager on Linux cannot be deployed from OVA files.
- Enterprise Manager on Linux is supported only with the Enterprise Plus edition license.
- You cannot install other backup infrastructure components on the machine where Enterprise Manager is installed. This includes the backup server, backup repository, proxy server and other components.
- Do not connect the same disk (for example, over iSCSI or NFS) to more than one Veeam Software Appliance or Veeam Infrastructure Appliance at the same time — otherwise, you risk data loss.
- Essentials license holders can deploy Veeam Software Appliance only on any hypervisor supported by Veeam and on Veeam Ready — Appliance certified hardware.
- When you install Veeam Software Appliance, the Rocky Linux operating system, Veeam Backup Enterprise Manager and other Veeam Software Appliance components are installed with predefined settings, including volume partitioning and user account creation. After installation is complete, you need to proceed with the initial configuration of Veeam Software Appliance, which includes setting up host users, and configuring server time and network settings.
- You cannot install 3rd party software on a Veeam Software Appliance.
- You cannot use 3rd party software to back up or restore a Veeam Software Appliance.
- You cannot use trusted domain authentication on a Veeam Software Appliance.

- You cannot use Veeam Software Appliance or Veeam Agent for Linux to back up or restore a Veeam Software Appliance.
- You can use the High Availability Cluster feature to reduce Veeam Software Appliance downtime.
- [VMware only] Veeam Software Appliance supports the Network and Virtual Appliance (HotAdd) transport modes. The Virtual Appliance transport mode must be enabled in the Host Management console. For more information, see Configuring Backup Infrastructure Settings.
- [Microsoft Hyper-V only] Linux-based Veeam Software Appliance does not support the SCVMM High Availability feature.
- Veeam Software Appliance is compliant with most SCAP Security Guide DISA STIG for RHEL 9 requirements except for the following ones:
  - V-258241 — RHEL 9 must implement a FIPS 140-3-compliant systemwide cryptographic policy.
  - V-270180 — The RHEL 9 `fapolicy` module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.
  - V-257937 — The RHEL 9 firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.
  - V-258122 — RHEL 9 must enable certificate based smart card authentication.

    IMPORTANT

    If you have infrastructure that does not support the TLS Extended Master Secret, Veeam Software Appliance will not be fully FIPS-compliant.
- If you use a Veeam Software Appliance and enable four-eyes authorization, you cannot disable or reduce the immutability period on the default Veeam Software Appliance repository without additional approval.

Installing Veeam Software Appliance from ISO

To install and configure Veeam Software Appliance, perform the following steps:

1. Mount the ISO image.
2. Select the product.
3. Begin installation.
4. Read and accept license agreements.
5. Specify the hostname.
6. Review network settings.
7. Review server time settings.
8. Configure the default host administrator account.
9. Configure the default security officer account.
10. Finish the configuration.

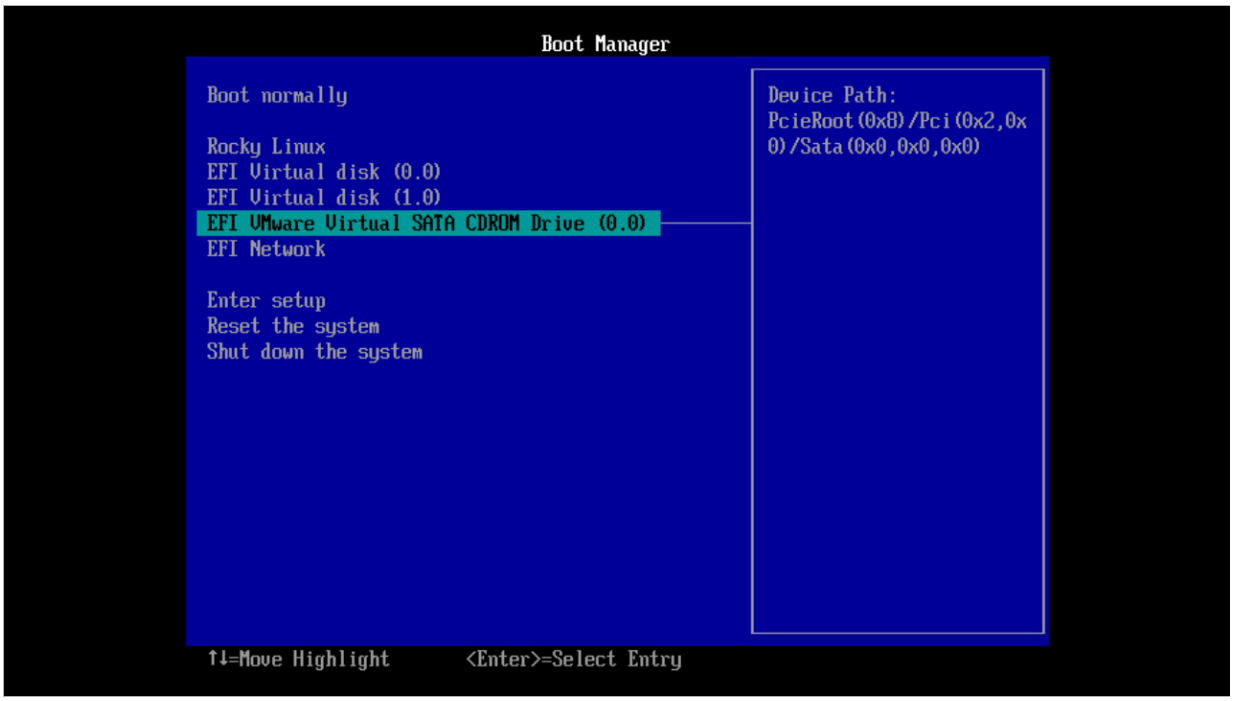
Step 1. Mount ISO File

To start the setup wizard, perform the following steps:

1. Download the latest version of the ISO file from the Product Downloads section of your Veeam account.
2. Mount the ISO file to the machine where you plan to install Veeam Software Appliance or burn the ISO file to a flash drive or other removable storage device. If you plan to install Veeam Software Appliance on a virtual machine, use the built-in tools of the virtualization management software to mount the ISO file.

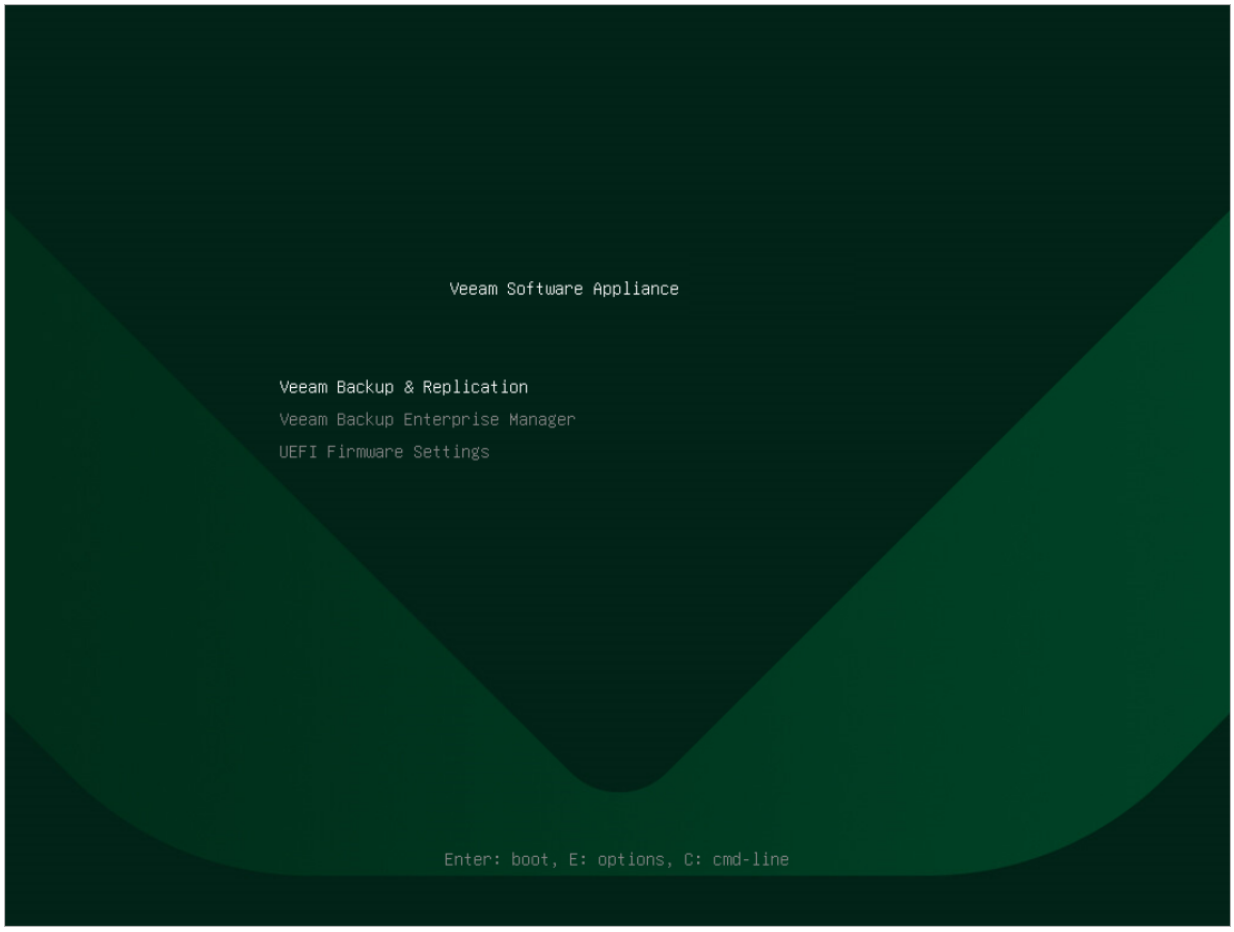
> **NOTE**
>
> To create a bootable USB stick, it is recommended that you use Rufus with the default settings. Note that you need to select **Write in DD Image mode** option when prompted.

3. In the Boot Manager, select the drive where you mounted the ISO file and press [Enter].



Step 2. Select Product

In the installation menu, select **Veeam Backup Enterprise Manager** and press [Enter].



Step 3. Begin Installation

In the installation menu, select **Install** and press [Enter].



When the installer is loaded, confirm the operation.

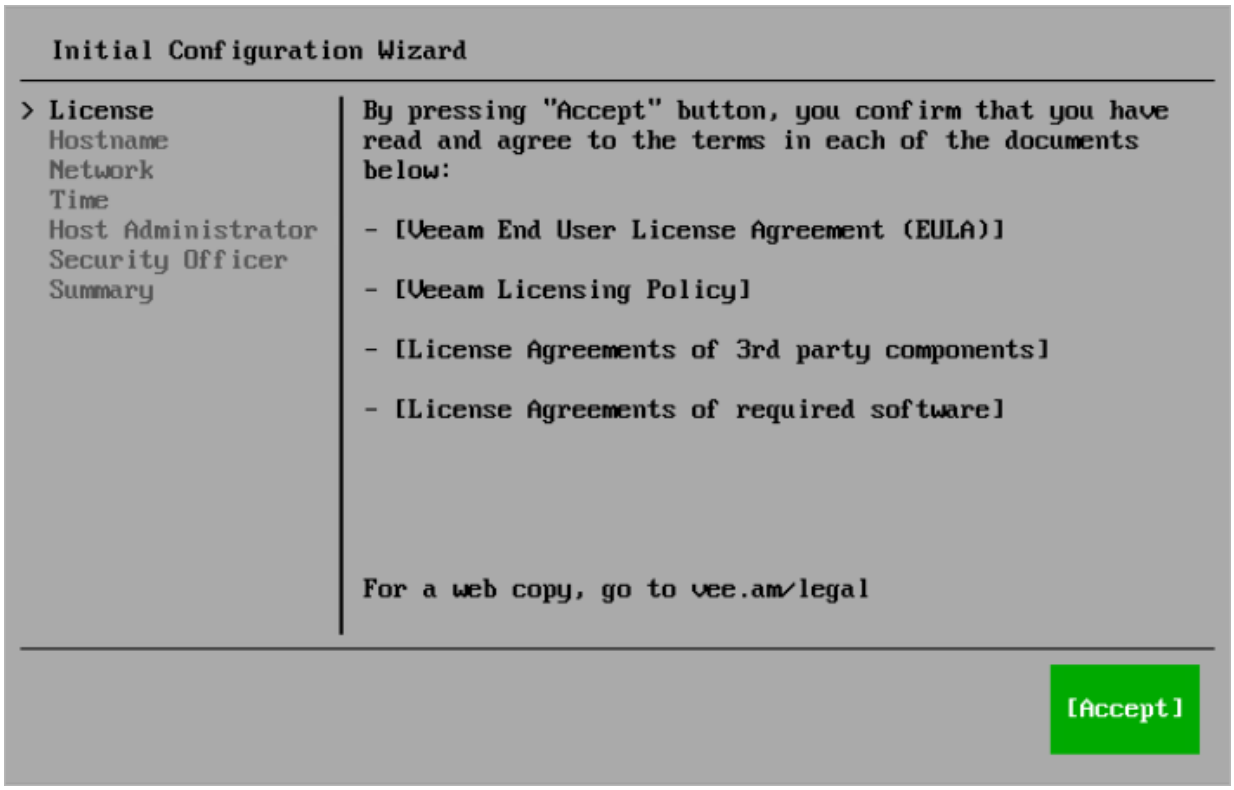
After the installation is complete, do the following:

1. Select **Reboot System** or wait for the system to reboot automatically.
2. After the system reboots, complete the **Initial Configuration** wizard.

Step 4. Read and Accept License Agreements

At the **License** step of the **Initial Configuration** wizard, read and accept Veeam license agreements and policies.

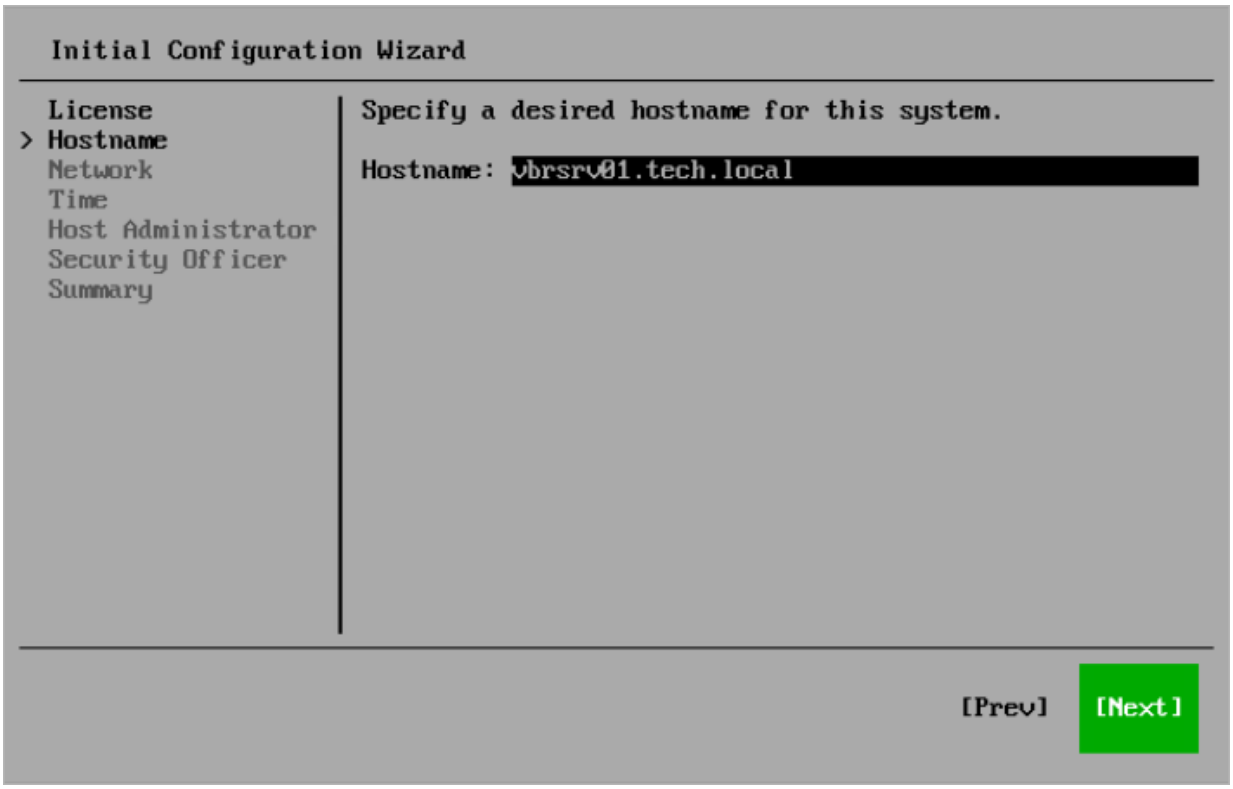
> **TIP**
>
> To close a document you have read, press [Q].



Step 5. Specify Hostname

At the **Hostname** step of the **Initial Configuration** wizard, specify the name of the server and select **Next**.

> **NOTE**
>
> Consider the following:
>
> - It is recommended that you use a Fully Qualified Domain Name as a hostname.
> - If you use a keyboard with a layout other than US English, you can change the keyboard layout used in the wizard. To do this, press [Ctrl+K], find and select the layout you want to use, and press [Enter].
> - You can change the server name later in the Host Management console. For more information, see Changing Server Name.



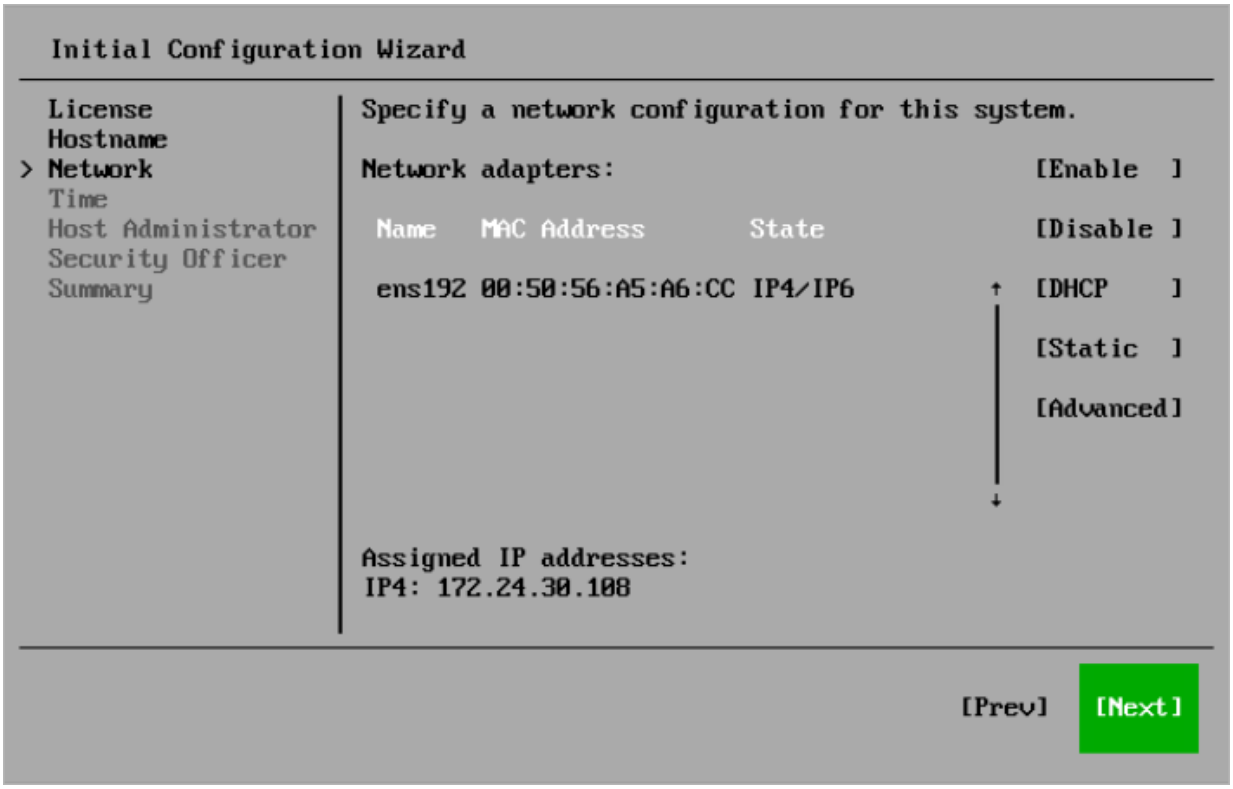
Step 6. Review Network Settings

At the **Network** step of the **Initial Configuration** wizard, review the network configuration.

By default, all enabled network adapters will be configured to use DHCP. To specify a static IP address, select **Static**.

> **NOTE**
>
> For advanced network configuration through the `nmtui` tool, select **Advanced**.

You can change network settings later in the Host Management console. For more information, see Configuring Network Interfaces.



Step 7. Review Server Time Settings

At the **Time** step of the **Initial Configuration** wizard, review server time configuration. Server time affects multi-factor authentication and backup operations, for example, backup job schedule.

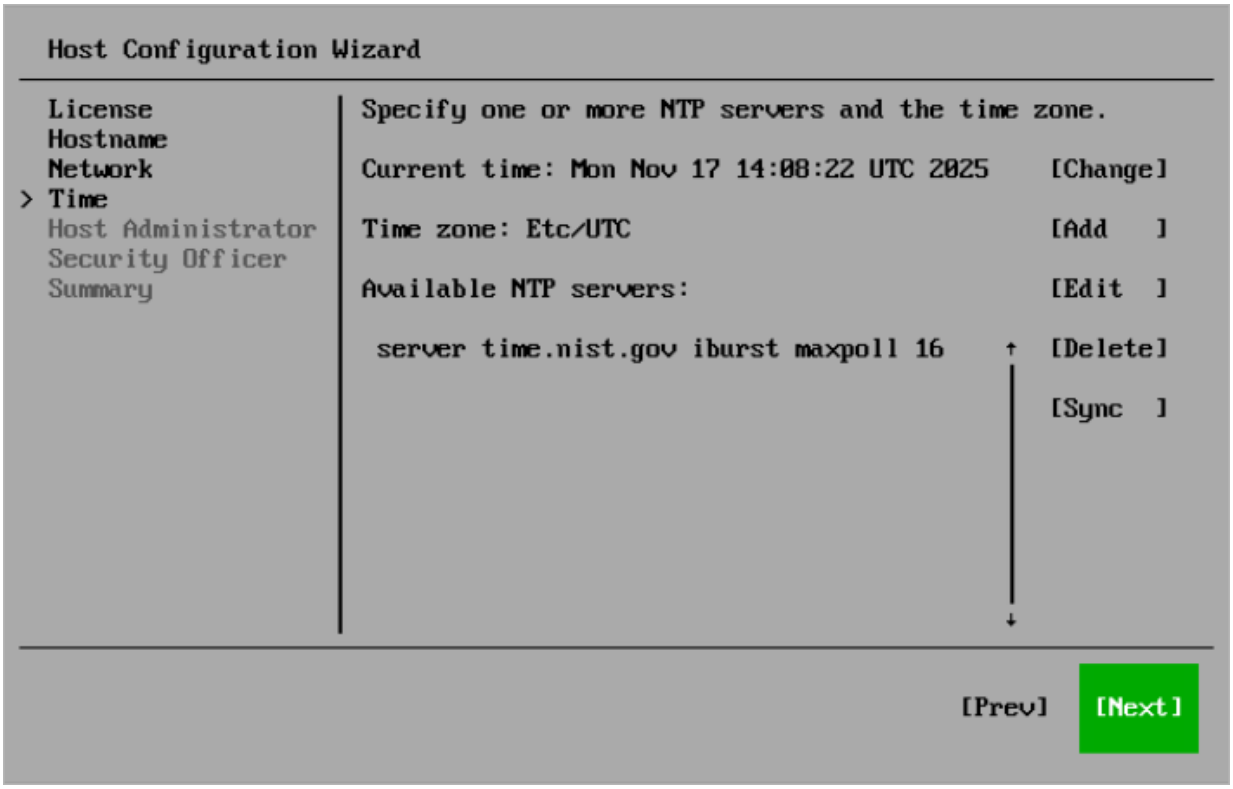
Configure the following server time settings:

- **Time zone**. By default, UTC is used. To specify another time zone, select **Change**.
- **Available NTP servers**. By default, the *time.nist.gov* NTP server is used. You can add multiple NTP and NTS servers. It is recommended to use a minimum of 3 to mitigate timing issues.

  > **NOTE**
  >
  > NTS servers must use a certificate signed by a public certificate authority.

  To synchronize time on the backup server with the NTP servers, select **Sync**.

You can change server time settings later in the Host Management console. For more information, see Configuring Server Time Settings.



Step 8. Configure Host Administrator Account

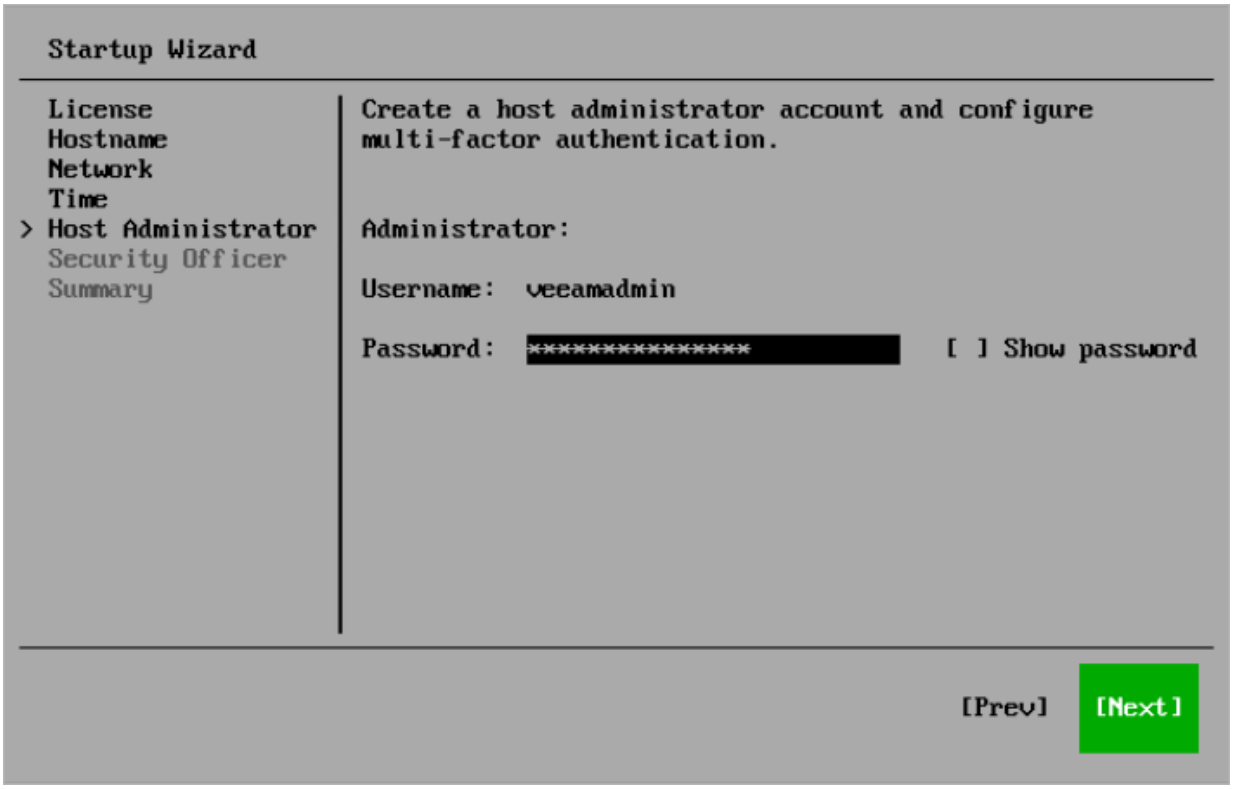
At the **Host Administrator** step of the **Initial Configuration** wizard, configure the default host administrator account to perform administrator activities in the Host Management console — *veeamadmin*. For more information about operations available for this role, see Managing Users and Roles.

To configure the host administrator account, perform the following steps:

1. In the **Password** field, specify the password for the *veeamadmin* user. The password must comply with the following requirements:
   - 15 characters minimum.
   - 1 upper case character.
   - 1 lower case character.
   - 1 numeric character.
   - 1 special character.
   - No more than 4 characters of the same class in a row. For example, more than 4 lowercase or 4 numerical characters in sequence.

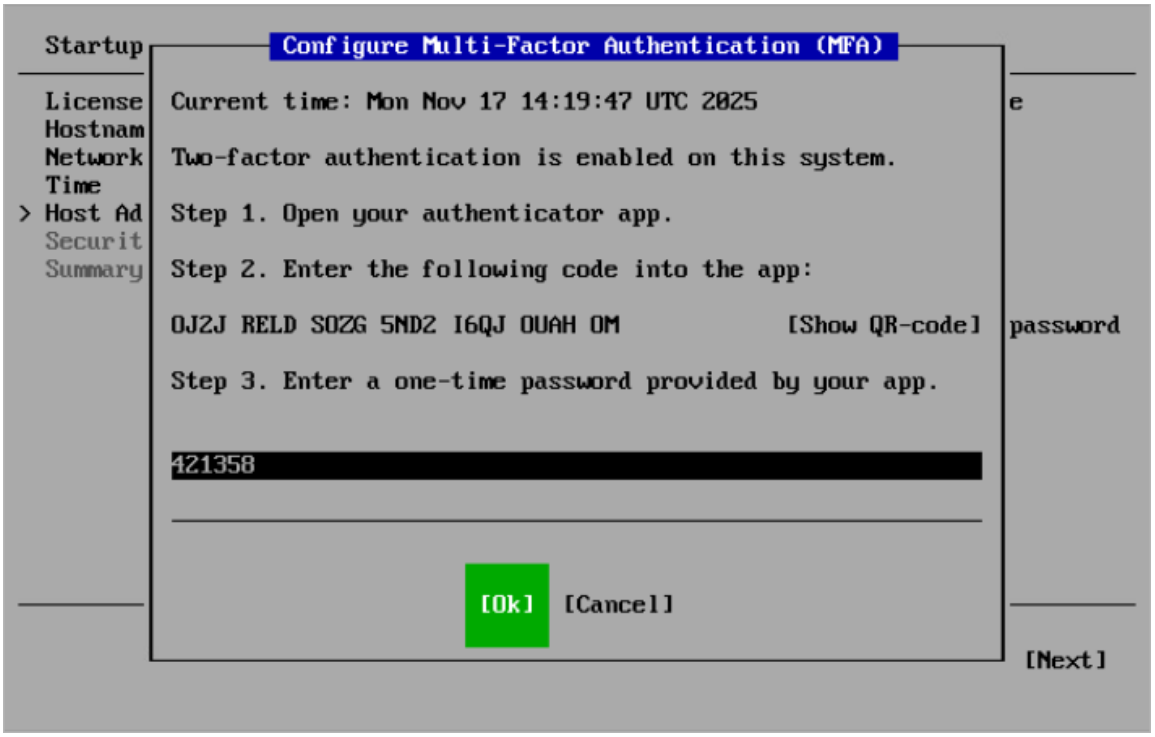
   TIP

   To view the password, select **Show Password** and press the spacebar.



2. Configure your multi-factor authentication (MFA) settings. Perform one of the following actions:
   a. To configure MFA immediately:
      i. Open your authentication application. Enter the code or scan the QR code.
      ii. Specify the one-time code provided by the application in the **Configure Multi-Factor Authentication** dialogue box.

iii. Press [OK].



b. To configure MFA in the Host Management console after completing the **Initial Configuration** wizard:

i. When the **Configure Multi-Factor Authentication** dialogue box opens, press [Escape].

ii. Select [OK].

c. To disable MFA entirely:

i. Press [F8].

ii. Type OK in the field.

IMPORTANT

If you disable MFA in the **Initial Configuration** wizard, you can enable it later in the Host Management console. After you enable MFA, users are prompted to set it up at their next login.

NOTE

Multi-factor authentication is compatible with mobile authentication applications that support RFC4226 and RFC6238.

3. Select **Next**.

Step 9. Configure Security Officer Account

At the **Security Officer** step of the **Initial Configuration** wizard, configure the default security officer account to perform specific operations in the Host Management console — *veeamso*. This account type provides an additional security layer to protect your infrastructure against malicious system administration. For more information about operations available for this role, see Managing Users and Roles.

> **NOTE**
>
> If you do not want to configure the security officer account, select **Skip setting up Security Officer**. To enable this account later, you will have to reinstall Veeam Software Appliance and complete the initial configuration.

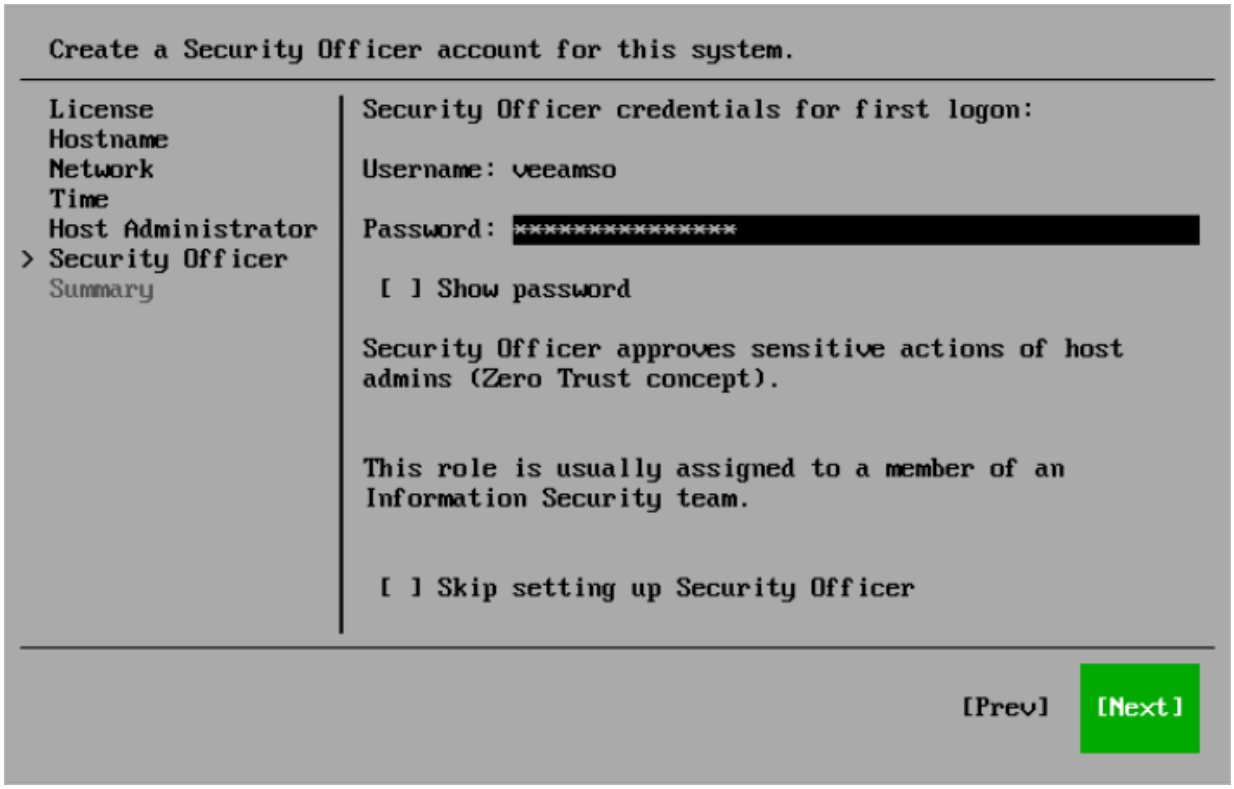
To configure the security officer account, do the following:

1. In the **Password** field, specify the password for the *veeamso* user. The password must comply with the following requirements:
   - 15 characters minimum.
   - 1 upper case character.
   - 1 lower case character.
   - 1 numeric character.
   - 1 special character.
   - No more than 4 characters of the same class in a row. For example, more than 4 lowercase or 4 numerical characters in sequence.

   > **TIP**
   >
   > To view the password, select **Show Password** and press the spacebar.

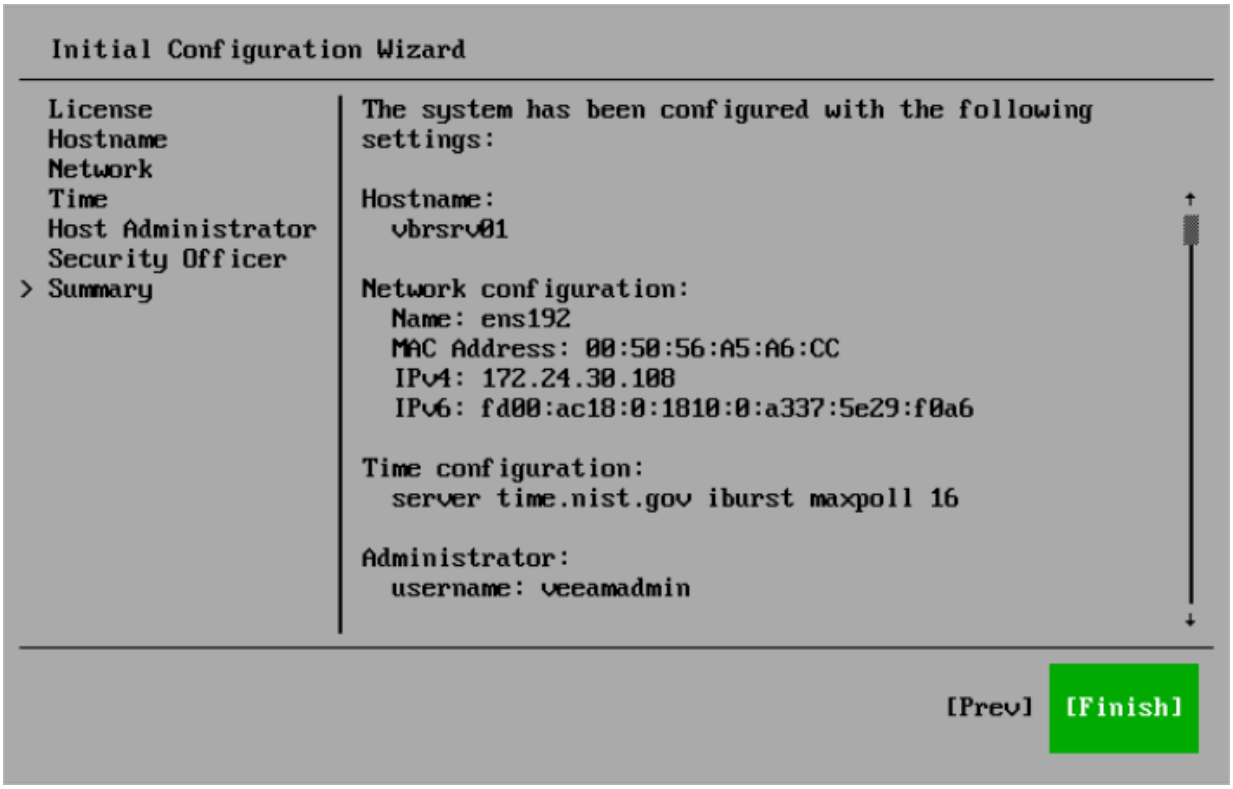
2. Select **Next**.

When a security officer first logs in to the Host Management console, they must complete the initial setup. For more information, see Performing Initial Security Officer Login.



Step 10. Finish Configuration

At the **Summary** step of the **Initial Configuration** wizard, review the system configuration and select **Finish**. The system will apply the configuration and restart required services.



After you finish the initial configuration, general information about the server will be displayed. You can use it to log in to the Host Management console or Veeam Backup & Replication web UI and continue configuring Veeam Software Appliance and Veeam Backup & Replication.

> **IMPORTANT**
>
> If you did not configure or disabled multi-factor authentication in the **Initial Configuration** wizard, Veeam Backup & Replication and the Web UI will be unavailable until you have configured MFA in the Host Management console.

Related Topics

- Host Management
- Configuring Enterprise Manager

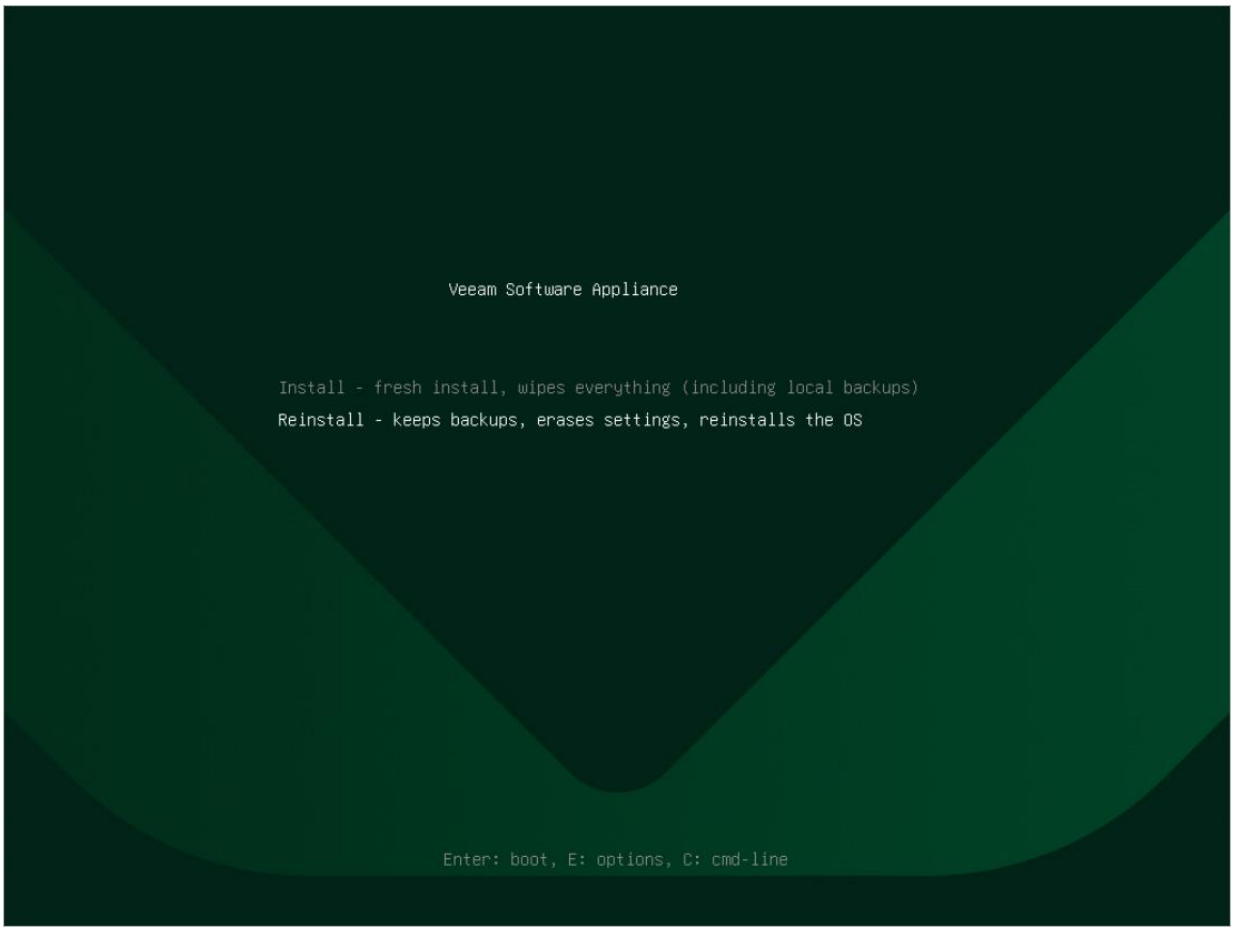
Reinstalling Veeam Software Appliance from ISO

To recover the operating system, you can reinstall Veeam Software Appliance. During this procedure, your backup data will not be affected.

To reinstall Veeam Software Appliance, perform the following steps:

1. Boot from the Veeam Software Appliance ISO file.
2. In the installation menu, select the product. Then, select **Reinstall**.

3. When the installer is loaded, confirm the operation.
4. After the installation is complete, do the following:
   a. Select **Reboot System** or wait for the system to reboot automatically.
   b. After the system reboots, complete the **Initial Configuration** wizard as described in the Installing Veeam Software Appliance from ISO section.



Installing Veeam Software Appliance from Microsoft Hyper-V Template

You can use the Microsoft Hyper-V template to deploy a VM on a Microsoft Hyper-V host with predefined hardware and Veeam Software Appliance ready for configuration. The template is supplied as a set of `.vhdx` files with Veeam Software Appliance preinstalled: a system disk (`os-disk.vhdx`) and a data disk (`data-disk.vhdx`).

> **NOTE**
>
> Consider the following before deploying a Veeam Software Appliance from the Microsoft Hyper-V template:
>
> - The Hyper-V server must meet the platform requirements for virtual infrastructure. For more information, see the Microsoft Hyper-V section of the Veeam Backup & Replication User Guide.
> - The virtual machine must be of **Generation 2** because the Veeam Software Appliance disks use the UEFI/GPT layout. Allocate at least 8 virtual processors and 16 GB RAM, plus 500 MB RAM for each concurrent job. For more information, see Considerations and Limitations.

To deploy Veeam Software Appliance using the Microsoft Hyper-V template, perform the following steps:

1. Download the latest version of the Microsoft Hyper-V template from the Product Downloads section of your Veeam account.
2. Extract the files from the `.ZIP` file.
3. Copy the Microsoft Hyper-V template files (`os-disk.vhdx` and `data-disk.vhdx`) to a dedicated folder in the storage of the Microsoft Hyper-V host. It is recommended that you deploy the VM from copies and keep the original files as a master template.
4. In Microsoft Hyper-V Manager, create a new VM. When you run the **New Virtual Machine Wizard**, specify the following settings:
   - **Specify Generation**: select **Generation 2**.
   - **Assign Memory**: specify **16384** MB or more. Do not enable **Dynamic Memory**.
   - **Configure Networking**: connect the network adapter to the virtual switch that provides the appliance with network access.
   - **Connect Virtual Hard Disk**: select **Use an existing virtual hard disk** and specify the copied `os-disk.vhdx` file.
5. In the settings menu of the VM, perform the following steps:
   a. Add the `data-disk.vhdx` file as a new hard drive.
   b. In the **Processor** settings, set the **Number of virtual processors** to **8** or more.
   c. In the **Security** settings, make sure that **Enable Secure Boot** is selected and set the **Template** to **Microsoft UEFI Certificate Authority**.
   d. In the **Firmware** settings, move the hard drive with the `os-disk.vhdx` file to the top of the boot order.
6. Start the virtual machine and connect to it.
7. Select **Veeam Backup & Replication** in the boot menu. Veeam Backup & Replication will launch the **Initial Configuration** wizard.
8. To complete the **Initial Configuration** wizard, follow the procedure described in the Installing Veeam Software Appliance from ISO section, starting from the Read and Accept License Agreements step.

Veeam Software Appliance Installation in Unattended Mode

You can install Veeam Software Appliance in the unattended automated mode by editing the ISO file. This section describes changes that must be made to allow automated installation and configuration.

In This Section

- Automating Installation Without Initial Configuration
- Automating Installation with Initial Configuration

Automating Installation Without Initial Configuration

You can modify the Veeam Software Appliance ISO file to allow unattended installation. This allows you to deploy Veeam Software Appliance automatically. After the installation is complete, you must configure Veeam Software Appliance manually using the **Initial Configuration** wizard.

> **IMPORTANT**
>
> Installing additional Linux packages, third-party applications, or changing OS settings (other than those that can be controlled by the Veeam Host Management Console) on Veeam Appliances is not supported. Veeam Customer Support cannot provide technical support for appliances with unsupported modifications due to their unpredictable impact on the security, stability, and performance of the appliance. For more information, see this KB article.

To automate the installation of Veeam Software Appliance, do the following:

1. Download the latest version of the ISO file from the Product Downloads section of your Veeam account.
2. Unpack the ISO file.
3. Make the following changes to the `%path_to_unpacked_ISO_folder%\EFI\BOOT\grub.cfg` file to automate the installation process:
   a. To set the default menu entry, change the `set default` parameter to `"Veeam Backup Enterprise Manager>Install - fresh install, wipes everything"`.
   b. To set a GRUB menu timeout, change the `set timeout` parameter to any positive value.
   c. To set all questions to be answered automatically, add `inst.assumeyes` to the end of the install menu entry `LABEL=VeeamSA:/vbem-ks.cfg quiet`.

   > **NOTE**
   >
   > You can automate additional options in the `grub.cfg` file. To do this, add `inst.assumeyes` to the end of the appropriate lines.

   d. Save the changes.
4. Repack the ISO file. To rebuild the modified Veeam Software Appliance ISO image on Linux, you can use the free open-source utility xorriso (available for most Linux distributions and also works under Windows WSL).
5. Mount the ISO file to the machine where you plan to install Veeam Software Appliance, or burn the ISO file to a flash drive or other removable storage device. If you plan to install Veeam Software Appliance on a virtual machine, use the built-in tools of the virtualization management software to mount the ISO file.

   > **NOTE**
   >
   > To create a bootable USB stick, it is recommended that you use Rufus with the default settings. Note that you need to select **Write in DD Image mode** option when prompted.

6. The automatic installation finishes at the Read and Accept License Agreements step. To complete the **Initial Configuration** wizard, continue the process described in the Installing Veeam Software Appliance from ISO section.

Automating Installation with Initial Configuration

You can modify the Veeam Software Appliance ISO file to allow unattended installation and configuration. This allows you to automatically deploy Veeam Software Appliance with preconfigured users, passwords, multi-factor authentication codes, and other settings.

> **IMPORTANT**
>
> Installing additional Linux packages, third-party applications, or changing OS settings (other than those that can be controlled by the Veeam Host Management Console) on Veeam Appliances is not supported. Veeam Customer Support cannot provide technical support for appliances with unsupported modifications due to their unpredictable impact on the security, stability, and performance of the appliance. For more information, see this KB article.

Required Edits

To automate the installation and configuration of Veeam Software Appliance, do the following:

1. Download the latest version of the ISO file from the Product Downloads section of your Veeam account.
2. Unpack the ISO file.
3. Make the following changes to the `%path_to_unpacked_ISO_folder%\EFI\BOOT\grub.cfg` file to automate the installation process:
   a. To set the default menu entry, change the `set default` parameter to `"Veeam Backup Enterprise Manager>Install - fresh install, wipes everything"`.
   b. To set a GRUB menu timeout, change the `set timeout` parameter to any positive value.
   c. To set all questions to be answered automatically, add `inst.assumeyes` to the end of the install menu entry `LABEL=VeeamSA:/vbem-ks.cfg quiet`.

      > **NOTE**
      >
      > You can automate additional options in the `grub.cfg` file. To do this, add `inst.assumeyes` to the end of the appropriate lines.

   d. Save the changes.
4. Make the following changes to the `vbem-ks.cfg` file to automate the configuration process:

   > **IMPORTANT**
   >
   > The changes must be added between `%post` and `# post end`.

   a. To disable the initialization wizard, add the following line right after `log "Veeam post install commands":`

   ```
   touch /etc/veeam/host_management_disable_init
   ```

   b. To create a configuration file that contains answers for the initialization wizard, add the following code with your specified answers:

```
cat << EOF >> /etc/veeam/vbr_init.cfg
veeamadmin.password=Ex@mp13C0mpl3xP@ssw0rd
veeamadmin.mfaSecretKey=JVDECICTMVRXEZLU
veeamadmin.isMfaEnabled=false
veeamso.password=Ex@mp13C0mpl3xP@ssw0rd2
veeamso.mfaSecretKey=JVDECICTMVRXEZLU
veeamso.isMfaEnabled=true
veeamso.recoveryToken={8*}-{4*}-{4*}-{4*}-{12*}
veeamso.isEnabled=true
ntp.servers=myntp01.example.local
ntp.runSync=true
vbr_control.runInitIso=true
vbr_control.runStart=true
EOF
```

NOTE

Consider the following when specifying your answers:

- The passwords for the `veeamadmin` and `veeamso` account must meet the following requirements:
  - 15 characters minimum.
  - 1 upper case character.
  - 1 lower case character.
  - 1 numeric character.
  - 1 special character.
  - No more than 4 characters of the same class in a row. For example, you cannot use more than 4 lowercase or 4 numerical characters in sequence.
- The passwords for the `veeamadmin` and `veeamso` accounts must be different.
- To avoid timing issues with multifactor authentication, it is recommended to set `ntp.runSync=true`.
- You cannot specify an NTS server as an answer to `ntp.servers=`.
- To specify multiple NTP servers, you must use the following format: `ntp.servers=myntp01.example.local;myntp02.example.local;myntp03.example.local`.
- The multifactor authentication secret key must be specified as a 16 digit, Base32-encoded string.
- The recovery token must be specified using hexadecimal values — 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Note that you can generate an appropriate string with the `New-Guid` cmdlet in Microsoft PowerShell.

If your specified answers do not meet these requirements, the configuration process will fail. To troubleshoot errors, you can use the Live OS ISO to view the `/var/log/VeeamBackup/veeam_hostmanager/veeamhostmanager.log` file and the system logs files in the `/var/log/anaconda` directory.

c. To create a script that will complete the configuration process using the answer file, add the following code:

```
set -e
cat << EOF >> /etc/veeam/veeam-init.sh
#!/bin/bash
set -eE -u -o pipefail
/opt/veeam/hostmanager/veeamhostmanager --apply_init_config /etc/veeam/
vbr_init.cfg
systemctl disable veeam-init
EOF
chmod +x /etc/veeam/veeam-init.sh
```

d. Add a `systemd` service definition and enable the service to run the script once after the first boot:

```
cat << EOF >> /etc/systemd/system/veeam-init.service
[Unit]
Description=One-shot daemon to run /opt/veeam/hostmanager/veeamhostmana
ger at next boot
[Service]
Type=oneshot
ExecStart=/etc/veeam/veeam-init.sh
RemainAfterExit=no
[Install]
WantedBy=multi-user.target
EOF
systemctl enable veeam-init.service
```

5. Repack the ISO. To rebuild the modified Veeam Software Appliance ISO image on Linux, you can use the free open-source utility xorriso (available for most Linux distributions and also works under Windows WSL).
6. Mount the ISO file to the machine where you plan to install Veeam Software Appliance, or burn the ISO file to a flash drive or other removable storage device. If you plan to install Veeam Software Appliance on a virtual machine, use the built-in tools of the virtualization management software to mount the ISO file.

> **NOTE**
>
> To create a bootable USB stick, it is recommended that you use Rufus with the default settings. Note that you need to select **Write in DD Image mode** option when prompted.

7. Boot the machine and wait for the installation and configuration processes to finish. When the machine is ready to use, the Veeam Host Management console will be displayed.

Optional Edits

You can also configure several additional parameters, but this is optional. To do this, edit the `vbem-ks.cfg` file as described in the following sections.

Setting Hostname

To set a specific hostname, edit the `hostname` parameter in the `network` command :

```
network --bootproto=dhcp --nodns --hostname=examplehostname
```

> **NOTE**
>
> If you want to add the machine to a Microsoft Windows domain, the hostname cannot contain more than 15 characters.

Setting Static IP Address

To set a static IP address, edit the `bootproto` parameter and add the `ip`, `netmask`, `nameserver`, and `gateway` parameters:

```
network --bootproto=static --ip=192.0.2.1 --netmask=255.255.255.0 --gateway=192
.0.2.254 --nameserver=192.168.2.1,192.168.3.1 --hostname=vbr-MACH_HASH
```

Enabling Data Collection

To allow data collection for remote monitoring and management systems immediately after deployment, add the following lines to your configuration file answers:

```
externalManagersInstallation.enabled = true
externalManagersInstallation.timeout = <X>sec
```

Omit the `externalManagersInstallation.timeout` line to use the default 1-hour timeout period.

For more information on data collection, see Configuring Backup Infrastructure Settings.

Veeam Software Appliance Update

Update operations are managed by Veeam Updater — a Veeam service that runs on Veeam Software Appliance.

The following updates can be installed:

- Operating system and security updates — mandatory, installed automatically and cannot be skipped or canceled.
- Veeam Backup Enterprise Manager security updates — mandatory, installed automatically and cannot be skipped or canceled.
- Veeam Backup Enterprise Manager updates including major releases, minor releases and private fixes — optional.

You can access Veeam Updater in the following ways:

- In the Veeam Host Management console, click **Updates** in the management pane.
- In Veeam Backup Enterprise Manager, select **Configuration** > **About** and click **Check for Updates**.

How Updates Work

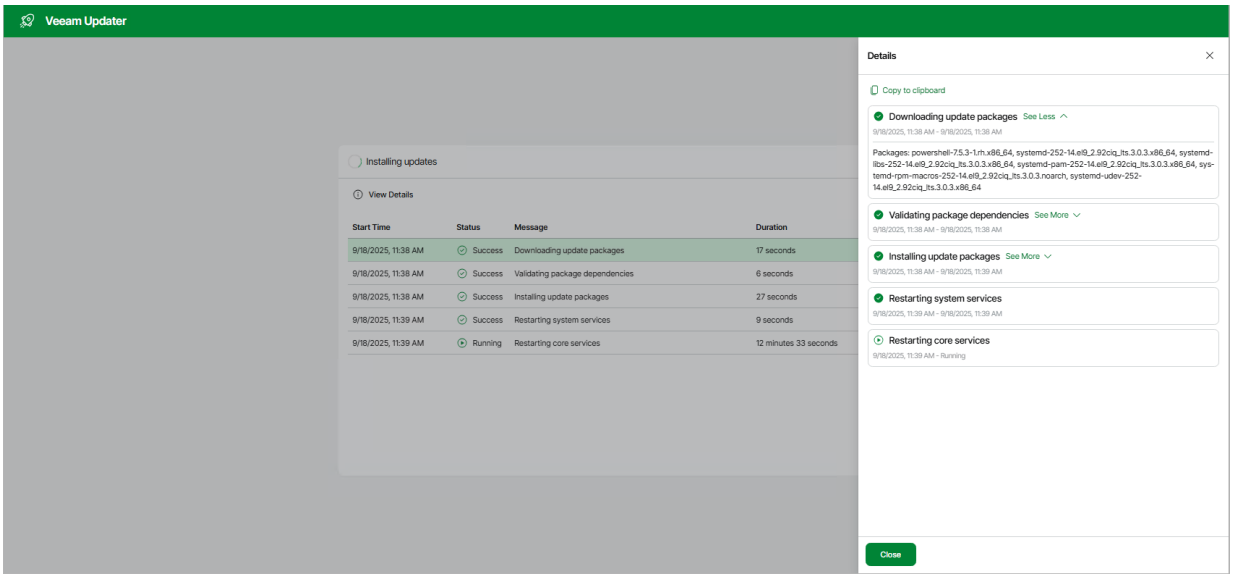
Update operations work in the following way:

- Every 12 hours Veeam Updater sends a request to *repository.veeam.com* to get information about last updates and saves information to the service database located on Veeam Software Appliance. If there are updates for Veeam Updater itself, the service automatically updates and restarts. These operations are also performed if you click **Check for updates** in the Veeam Updater UI.
- Veeam Backup Enterprise Manager requests Veeam Updater to check for updates in the following cases:
  - When you install a new license.
  - When you check for updates manually. For more information, see Checking for Updates.

  Veeam Updater sends a request to *repository.veeam.com* to get information about last updates and saves the information to the service database. Veeam Backup & Replication saves the information received from Veeam Updater to the configuration database.
- At the scheduled time or when the user initiates manual installation, Veeam Updater installs required updates on Veeam Software Appliance. During this operation, Veeam Updater performs the following steps:
  a. Downloads update packages.
  b. Validates package dependencies.
  c. Installs update packages.
  d. Restarts system services.
  e. Restarts Veeam core services.

f. Restarts the server if required. Note that during restart, the Veeam Host Management console and Veeam Backup Enterprise Manager will not be available.

The detailed information on installation process includes the list of the packages that will be installed and the state of each installation step. Veeam Updater log files are stored in the `/var/log/veeam/veeam-updater/` directory.



For more information on automatic and manual update installation, see Installing Updates.

> **NOTE**
>
> If your license has expired or is not valid, update operations will fail, and the Veeam Updater UI will be unavailable.

Configuring Updates

To set up Veeam Software Appliance updates, perform the following steps:

1. Log in to the Veeam Host Management console.
2. In the management pane, click **Updates**.
3. On the **Settings** tab, configure the following settings:
   - Updates for automatic installation. By default, only security updates are installed automatically. You can also include optional updates, except for major releases.
   - Maintenance window. You can schedule automatic update installation to run on a weekly or monthly basis. If you want to install updates manually, select *None*.
   - Compliance deadline. By default, updates you selected for automatic installation are forcibly installed after 30 days. You can postpone this operation up to 90 days.

     The date of the first found update is used as the start date for calculating compliance deadline. When the compliance deadline is reached, Veeam Updater installs all available updates selected for automated installation.

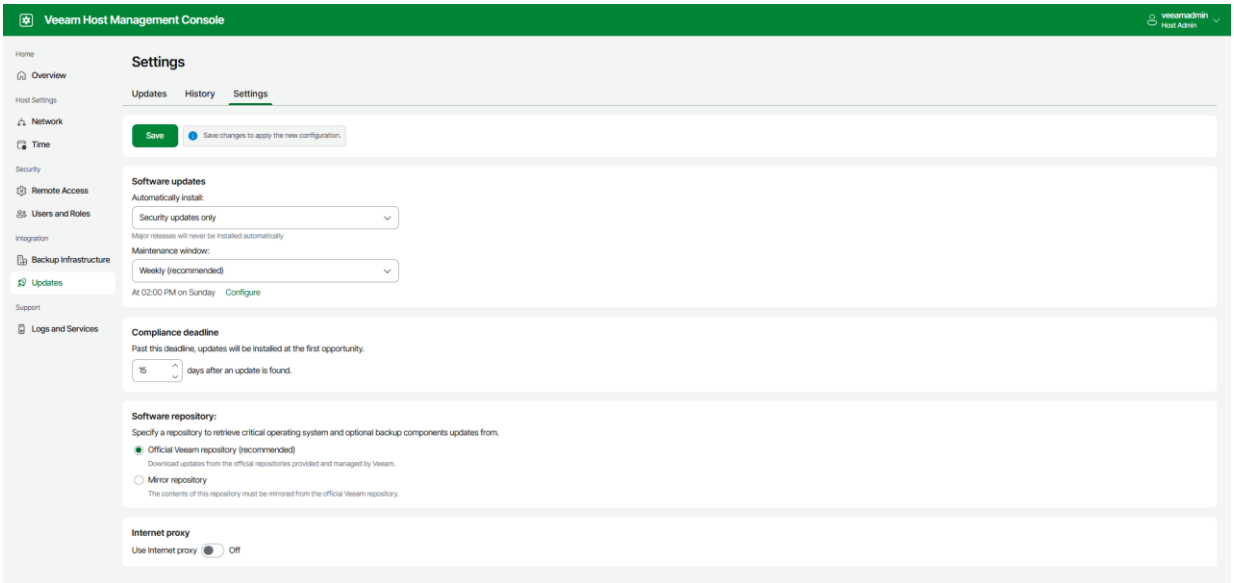
> **IMPORTANT**
>
> Consider the following:
>
> - If you select manual installation in the maintenance window, mandatory updates will be still automatically installed when the compliance deadline is reached.
> - If you schedule automatic update installation or miss the compliance deadline, updates will be installed even if you have running jobs. Recovery operations performed by these jobs will fail.

- Software repository. By default, updates are installed from the Veeam official repository (`https://repository.veeam.com/vsa`). If your backup server does not have internet access, you can specify a local mirror of the Veeam repository, for example, `https://repository.tech.local`. For the HTTPS repository, you also need to specify a certificate.

> **IMPORTANT**
>
> If you use a local mirror repository, the file structure of your mirror repository must be identical to the Veeam official repository, excluding the primary URL.
>
> For example:
>
> - `https://repository.tech.local/<veeamosreleaseversion>/vbr/<veeamproductversion>/mandatory/`
> - `https://repository.tech.local/<veeamosreleaseversion>/vbr/<veeamproductversion>/optional/`
> - `https://repository.tech.local/<veeamosreleaseversion>/external-mandatory/`

- Internet proxy. Add a proxy server if you use one.

4. Click **Save**.



Checking for Updates

Veeam Backup Enterprise Manager automatically notifies you about updates that must be installed or can be installed to enhance your experience with the product. Update notifications eliminate the risk of using out-of-date components in the backup infrastructure or missing critical updates that can have a negative impact on data protection and disaster recovery tasks.

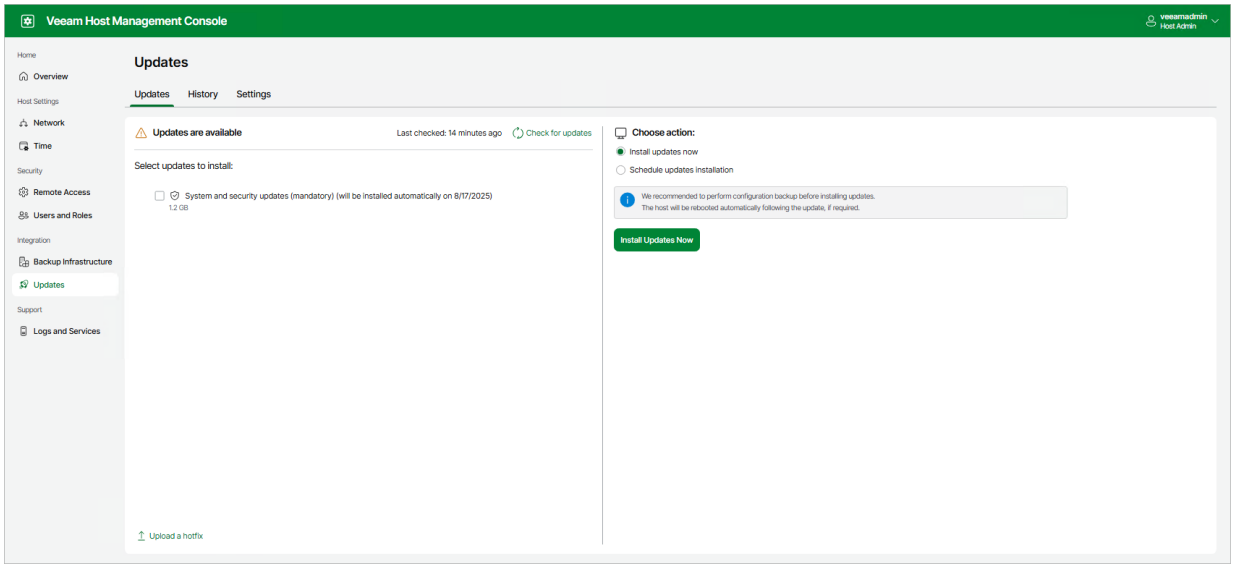
Veeam Backup Enterprise Manager shows update notifications at the top of the window. Alternatively, you can check for updates manually.

To manually check for updates, perform the following steps:

1. Log in to the Veeam Host Management console.
2. In the management pane, click **Updates**.
3. On the **Updates** tab, click **Check for updates**.

Alternatively, you can open Veeam Backup Enterprise Manager, select **Configuration** > **About** > **Check for Updates**.

> **NOTE**
>
> If there are updates for Veeam Updater itself, the service automatically updates and restarts.



Installing Updates

Updates can be installed manually or automatically. For more details on the installation process, see How Updates Work.

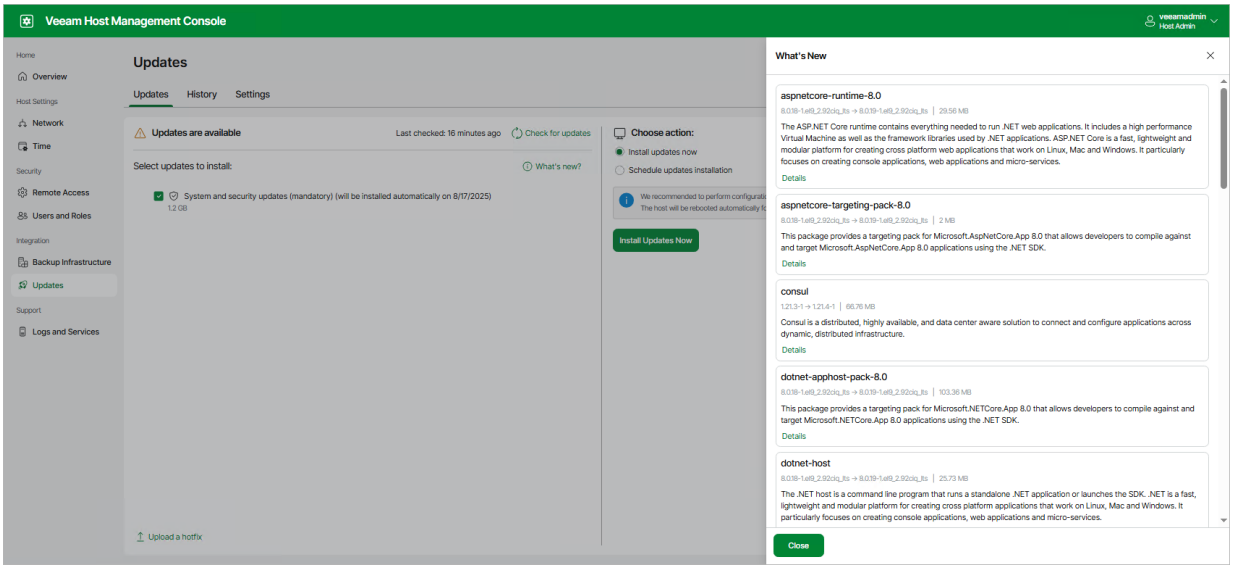
Installing Updates Manually

To install updates manually, perform the following steps:

Installing Updates Manually

To install updates manually, perform the following steps:

1. Log in to the Veeam Host Management console installed on Veeam Backup Enterprise Manager.
2. In the management pane, click **Updates**.
3. On the **Updates** tab, select updates that you want to install. To view detailed information about changes included in updates, click *What's new?*. For optional updates, a license agreement is also displayed if applicable.
4. Select the action:
   - To install updates immediately, click **Install Updates Now** and confirm the operation.
   - To schedule update installation, set up the schedule and click **Schedule Updates**.



Installing Updates Automatically

To install updates automatically, set up the maintenance window in the update configuration. For more information, see Configuring Updates.

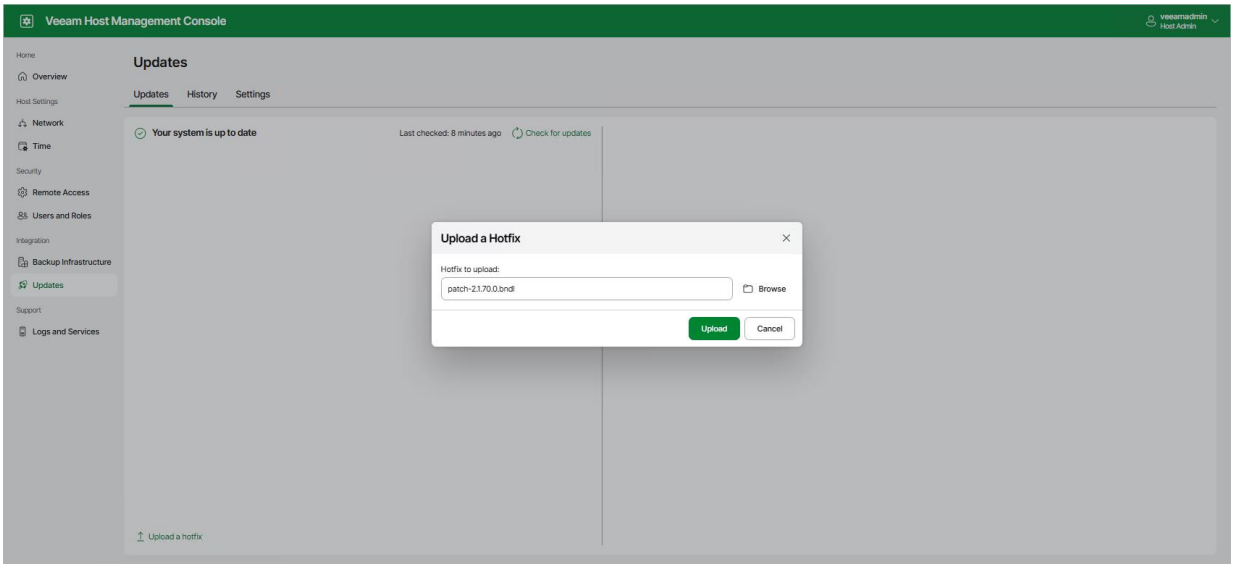
> **NOTE**
>
> If automatic update installation fails, Veeam Updater retries it after 1 minute, 10 minutes, 1 hour, 3 hours, 6 hours and 12 hours. Each interval starts when the previous attempt ends. If these attempts fail, Veeam Updater retries installation once a day until 7 days pass after the first failed attempt. Then the retry cycle starts again.

Installing Private Hotfixes

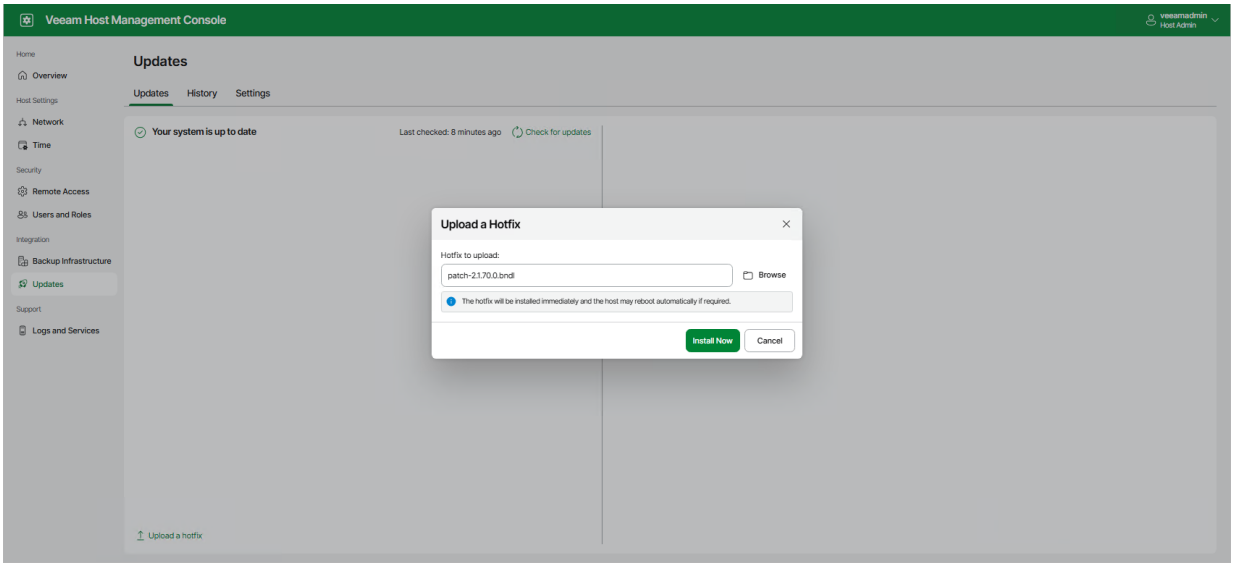
If you get a private hotfix provided by Veeam, you can install it manually. To do this, perform the following steps:

1. Make sure that you do not have running jobs. Otherwise, recovery operations performed by these jobs will fail.

2. Log in to the Veeam Host Management console installed on Veeam Backup Enterprise Manager.
3. In the management pane, click **Updates**.
4. On the **Updates** tab, click **Upload a hotfix**.
5. Select the file and click **Upload**.



6. After the file is uploaded, click **Install Now**. If a hotfix has a license agreement, you need to agree with it before the installation process starts.

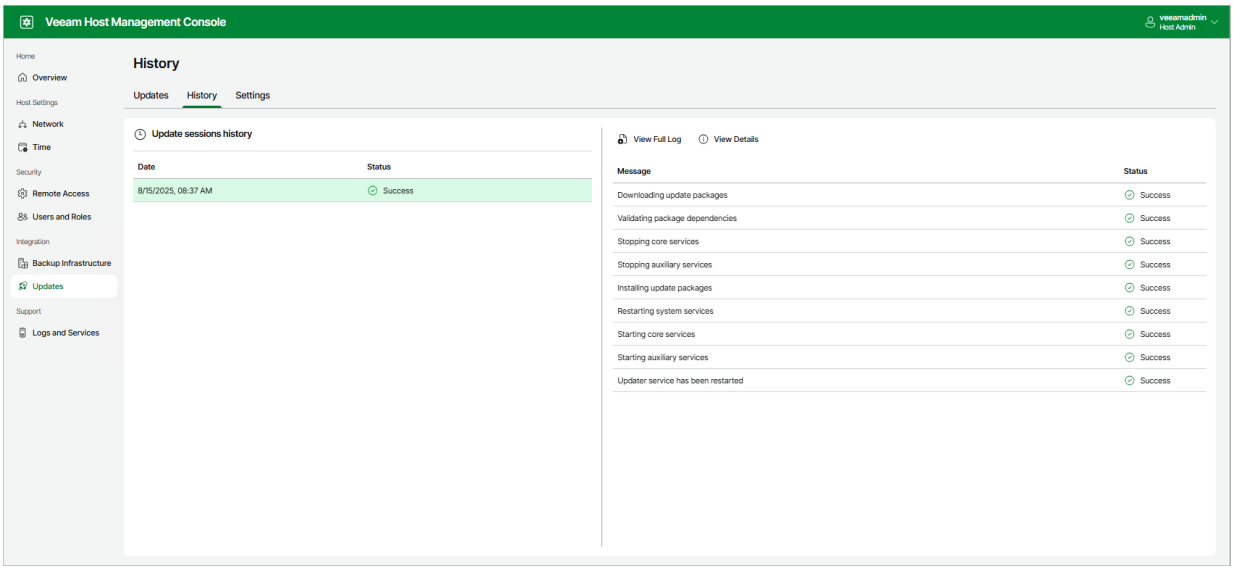


Viewing Update History

To view detailed information about update sessions, do the following:

1. Log in to the Veeam Host Management console.
2. In the management pane, click **Updates**.
3. On the **History** tab, select the date to view update events.
4. Click **View Details**.

To download a full log file, click **View Full Log**.



Enterprise Manager Deployment on Windows

To begin working with Veeam Backup Enterprise Manager, you must install it 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.

In This Section

- Installing Enterprise Manager
- Upgrading to Enterprise Manager 13.1
- Updating Enterprise Manager
- Uninstalling Enterprise Manager
- Migrating Enterprise Manager
- Silent Installation, Upgrade and Uninstallation

Installing Enterprise Manager

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

1. Start the setup wizard.
2. Select Enterprise Manager as a product to install.
3. Read and accept the license agreements.
4. Provide a license file.
5. Install missing software.
6. Review the default installation settings.
7. Specify a service account.
8. Specify a database server.
9. Specify data locations.
10. Specify service ports.
11. Begin installation.

Before You Begin

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

- A machine on which you plan to install Veeam Backup Enterprise Manager must meet the system requirements. For more information, see System Requirements.
- A user account that you plan to use for installation must have sufficient permissions. For more information, see Permissions.
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see Ports.
- Local antivirus or antimalware software can interfere with Veeam Backup Enterprise Manager installation. If you receive the *Failed to create website 0x80070020* message, disable your local antivirus or antimalware software and run the installation process again. You can re-enable your antivirus software once the installation completes. For more information, see this Veeam KB article.
- .NET 3.5.1 WCF HTTP Activation Windows component prevents Veeam Backup Enterprise Manager from functioning. Make sure there is no .NET 3.5.1 WCF HTTP Activation Windows component on the Veeam Backup Enterprise Manager server prior to the installation.
- Make sure there is no Microsoft Search Server installed on the machine. If you have Microsoft Search Server, uninstall it prior to the Veeam Backup Enterprise Manager installation.
- If you want to use an already installed PostgreSQL instance for the Enterprise Manager configuration database, make sure the instance can use sufficient resources. For more information, see Configuring PostgreSQL Instance.

- If you want to use an already installed PostgreSQL instance for the Enterprise Manager configuration database, make sure the instance contains the default *postgres* database. If you allow the setup to install a new PostgreSQL instance, the *postgres* database will be created on the instance automatically.

  Since Enterprise Manager connects to the *postgres* database to access the configuration database, do not rename the *postgres* database upon the Enterprise Manager installation.

- Check the *Known Issues* section of the Veeam Backup & Replication Release Notes.

Configuring PostgreSQL Instance

When you create a new PostgreSQL instance, the default setup is configured to consume a minimum amount of resources, which may not be enough for Enterprise Manager performance.

When installing Veeam Backup Enterprise Manager, you can choose what PostgreSQL instance to use for the Enterprise Manager configuration database. You can use an existing PostgreSQL instance or create a new one.

- If you let the setup create a new PostgreSQL instance, it will be configured automatically.
- If you want to use an existing PostgreSQL instance, make sure that the instance configuration is sufficient for the Enterprise Manager performance.

To adjust the configuration of an existing PostgreSQL instance, take the following steps before you install Enterprise Manager:

1. On a backup server, run the Set-VBRPSQLDatabaseServerLimits cmdlet. The cmdlet generates the necessary PostgreSQL configuration and saves it to a dump SQL file.

   ```
   Set-VBRPSQLDatabaseServerLimits -OSType <String> -CPUCount <number of CPU
   cores> -RamGb <RAM in GB> -DumpToFile <file path>
   ```

   For example:

   ```
   Set-VBRPSQLDatabaseServerLimits -OSType Windows -CPUCount 16 -RamGb 32 -Du
   mpToFile "C:\config.sql"
   ```

2. On the machine with the PostgreSQL instance where you want to deploy the Enterprise Manager configuration database, use the `psql` tool to apply the configuration from the dump file.

   The tool is located in the PostgreSQL installation folder.

   ```
   psql -U <user> -f <file path>
   ```

   For example:

   ```
   psql -U postgres -f "C:\config.sql"
   ```

3. Include the pg_stat_statements library to the PostgreSQL configuration. To add the library, you can manually edit the `shared_preload_libraries` option in the `postgres.conf` file.

   Alternatively, you can do it by by executing the SQL code:

   a. Check the content of the `shared_preload_libraries` variable.

   ```
   SELECT * FROM pg_settings
   WHERE name = 'shared_preload_libraries';
   ```

   b. Add the `pg_stat_statements` library to the shared preloaded libraries.

   - If the `shared_preload_libraries` value is empty, assign `pg_stat_statements` to the `shared_preload_libraries` variable.

   ```
   ALTER SYSTEM SET shared_preload_libraries = pg_stat_statements;
   ```

   - If the `shared_preload_libraries` value is not empty, add `pg_stat_statements` to the current value separated by comma.

   ```
   ALTER SYSTEM SET shared_preload_libraries = <existing libraries>, pg
   _stat_statements;
   ```

4. Restart the PostgreSQL service for the new configuration to take effect.
5. Install the `pg_stat_statements` extension. The extension is used to analyze the PostgreSQL performance.

   ```
   CREATE EXTENSION IF NOT EXISTS "pg_stat_statements";
   ```

Step 1. Start Setup Wizard

To start the setup wizard, take the following steps:

1. Download the latest version of the Veeam Backup & Replication installation image from the Veeam Product Downloads page.
2. Mount the installation image to the machine where you plan to install Veeam Backup Enterprise Manager or burn the image file to a flash drive or other removable storage device. If you plan to install Veeam Backup Enterprise Manager on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

   To extract the content of the ISO file, you can also use the latest versions of utilities that can properly extract data from ISO files of large size and can properly work with long file paths.
3. After you mount the image or insert the disk, Autorun opens a splash screen. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. Click **Install**.

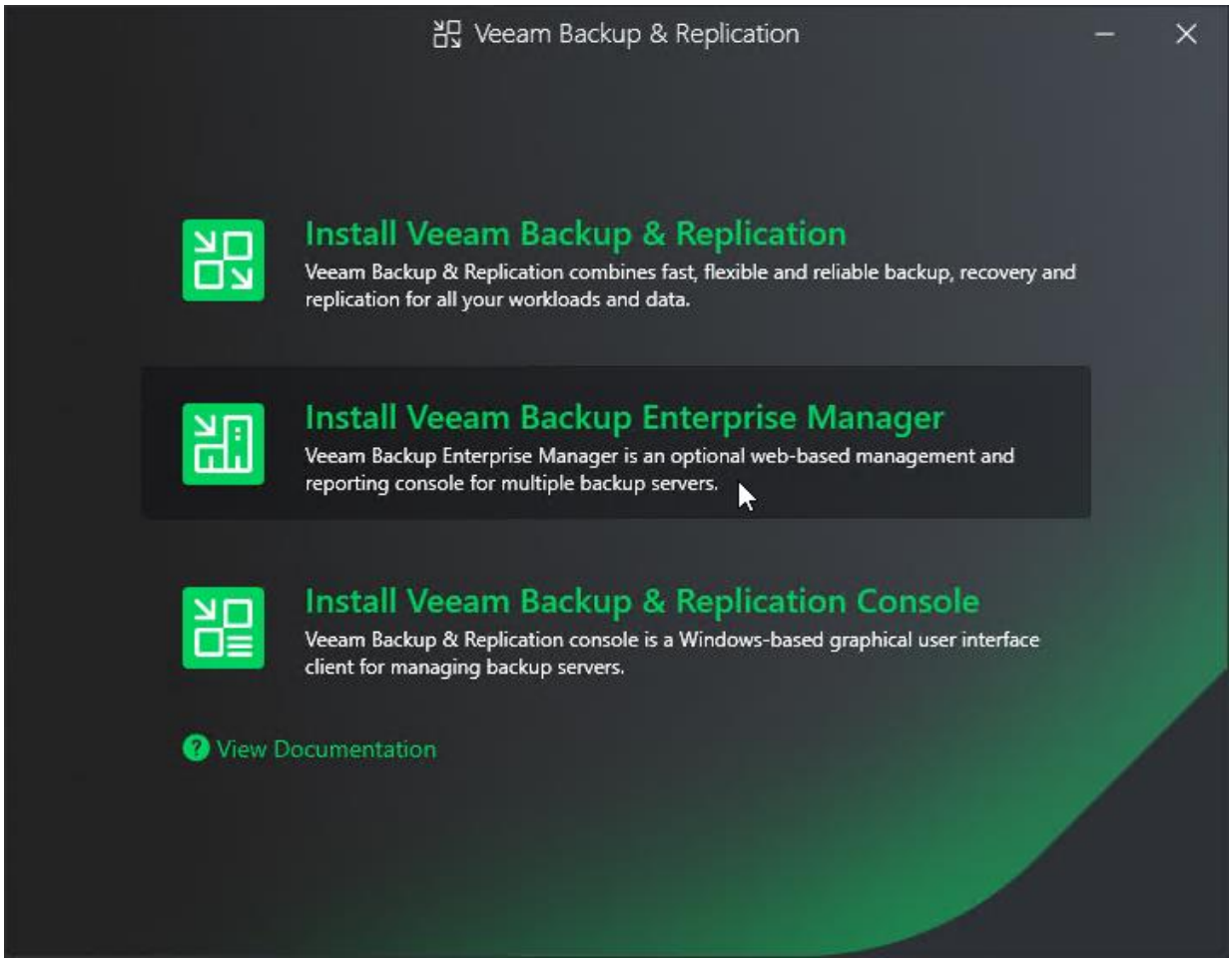
> **IMPORTANT**
>
> It is strongly recommended that you install Veeam Backup Enterprise Manager using Autorun or the `Setup.exe` file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup Enterprise Manager may not work as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



Step 2. Select Product

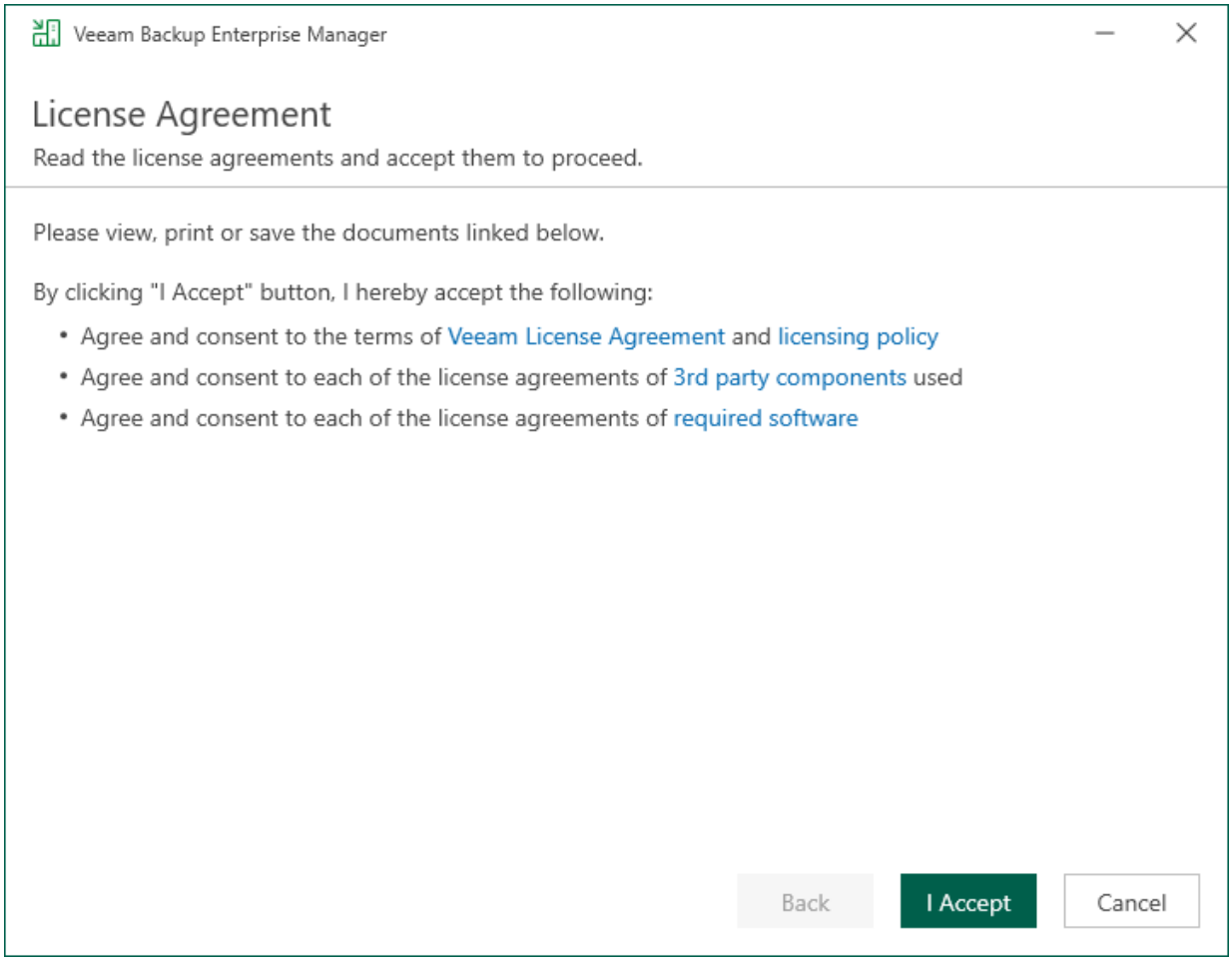
At this step of the wizard, select **Install Veeam Backup Enterprise Manager**.

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



Step 3. Read and Accept License Agreements

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



Step 4. Provide License File

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

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

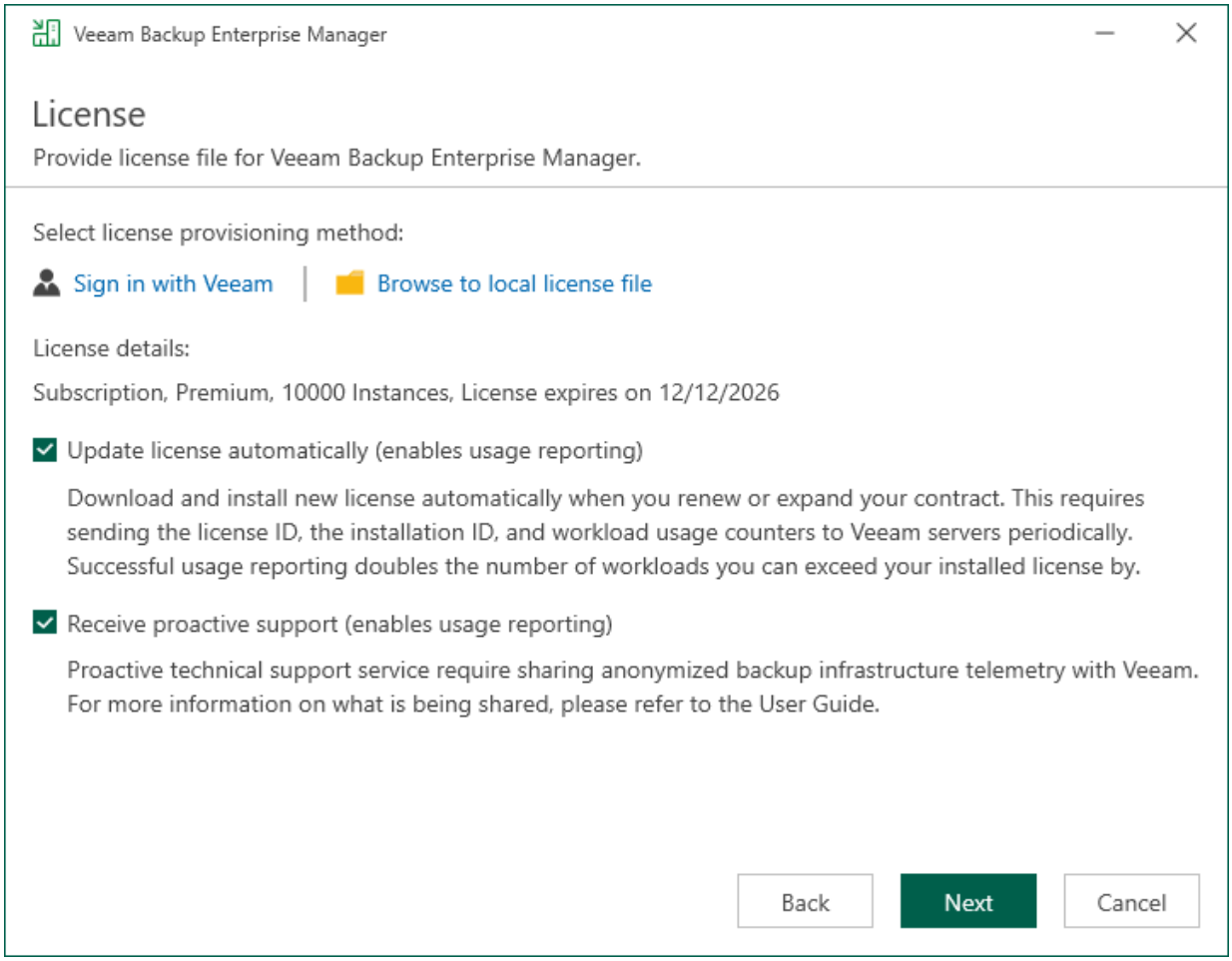
If a valid license is already installed on the machine, the setup wizard will display the license details. In this case, you can skip the **License** step and move on to the next step of the wizard.

To install a license, choose one of the following options:

- Browse your local server or network locations for a license file:
  a. Click **Browse to local license file**.
  b. Choose a valid license file for Veeam Backup Enterprise Manager.
- Select a license from your account at the Veeam website:
  a. Click **Sign in with Veeam**.
  b. Enter your credentials for accessing the Veeam website and click Sign in.
  c. Select one of the available licenses and click **Install selected license**.

To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. For more information on license update, see Updating License.

To receive proactive technical support services, select the Receive proactive support check box. Selecting this option also enables diagnostic data sharing. To learn how sensitive data is processed, see Processing of Sensitive Data in Veeam Technical Support.

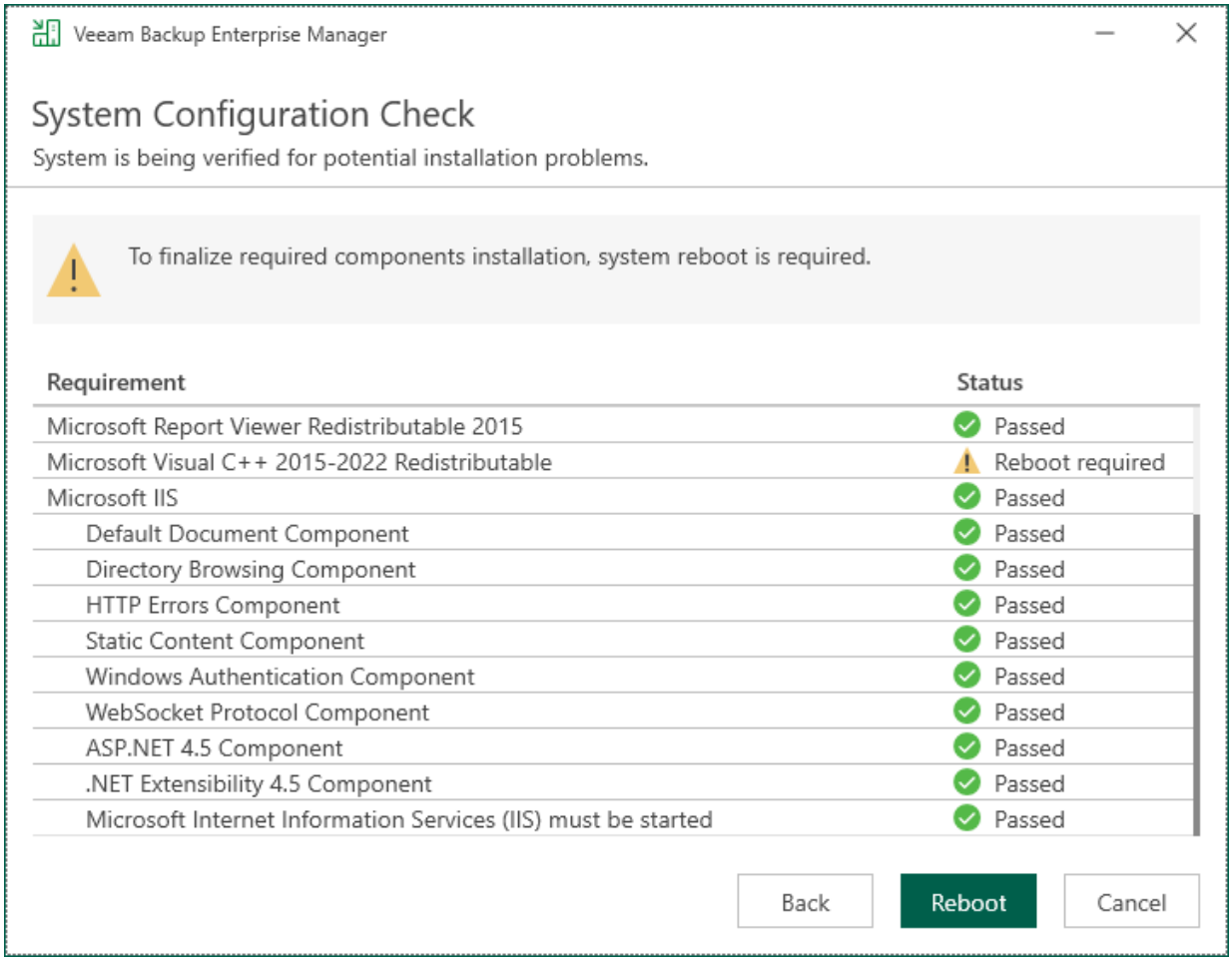


Step 5. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup checks whether required software is installed on the machine.

- If some of the required components are missing, the setup will try to install them automatically. After the components are installed successfully, reboot is required. When you are ready to reboot the machine, click **Reboot**.
- If the setup is not able to install some of the required software automatically, install it manually and click **Retry**.

> **NOTE**
>
> If all required software is already installed on the machine, the **System Configuration Check** step will be skipped. For more information on the necessary software, see System Requirements.



Step 6. Review Default Installation Settings

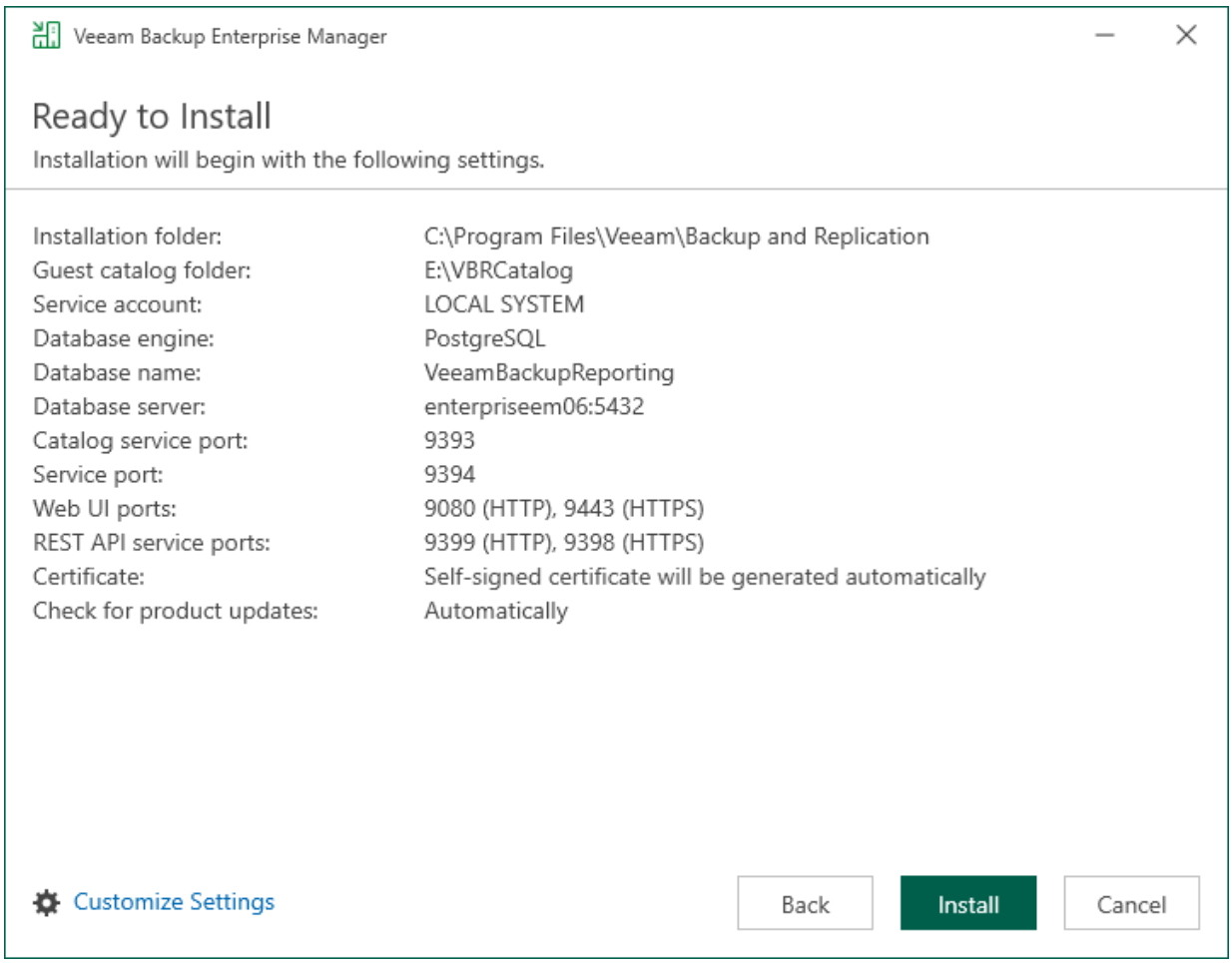
At the **Ready to Install** step of the wizard, you can select to install Veeam Backup Enterprise Manager with default installation settings or specify custom installation settings.

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

The table below lists the default installation settings.

Setting	Default Value	Description
Installation folder	*%ProgramFiles%\Veeam\Backup and Replication*	Folder where Veeam Backup Enterprise Manager is installed.
Guest catalog folder	*C:\VBRCatalog*	The `VBRCatalog` folder on a volume with the maximum amount of free space. The guest catalog folder stores indexing data for VM guest OS files. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore.
Service account	*LOCAL SYSTEM*	Account under which the Veeam Backup Enterprise Manager runs.
Database engine	*PostgreSQL*	The setup installs PostgreSQL locally on the Veeam Backup Enterprise Manager server.
Database name	*VeeamBackupReporting*	The setup deploys the Veeam Backup Enterprise Manager configuration database on the locally installed instance of PostgreSQL.
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 port	*9394*	The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers.
Web UI ports	For HTTP protocol: *9080* For HTTPS protocol: *443*	These ports are used for accessing Veeam Backup Enterprise Manager web interface.

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



Step 7. Specify Service Account

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

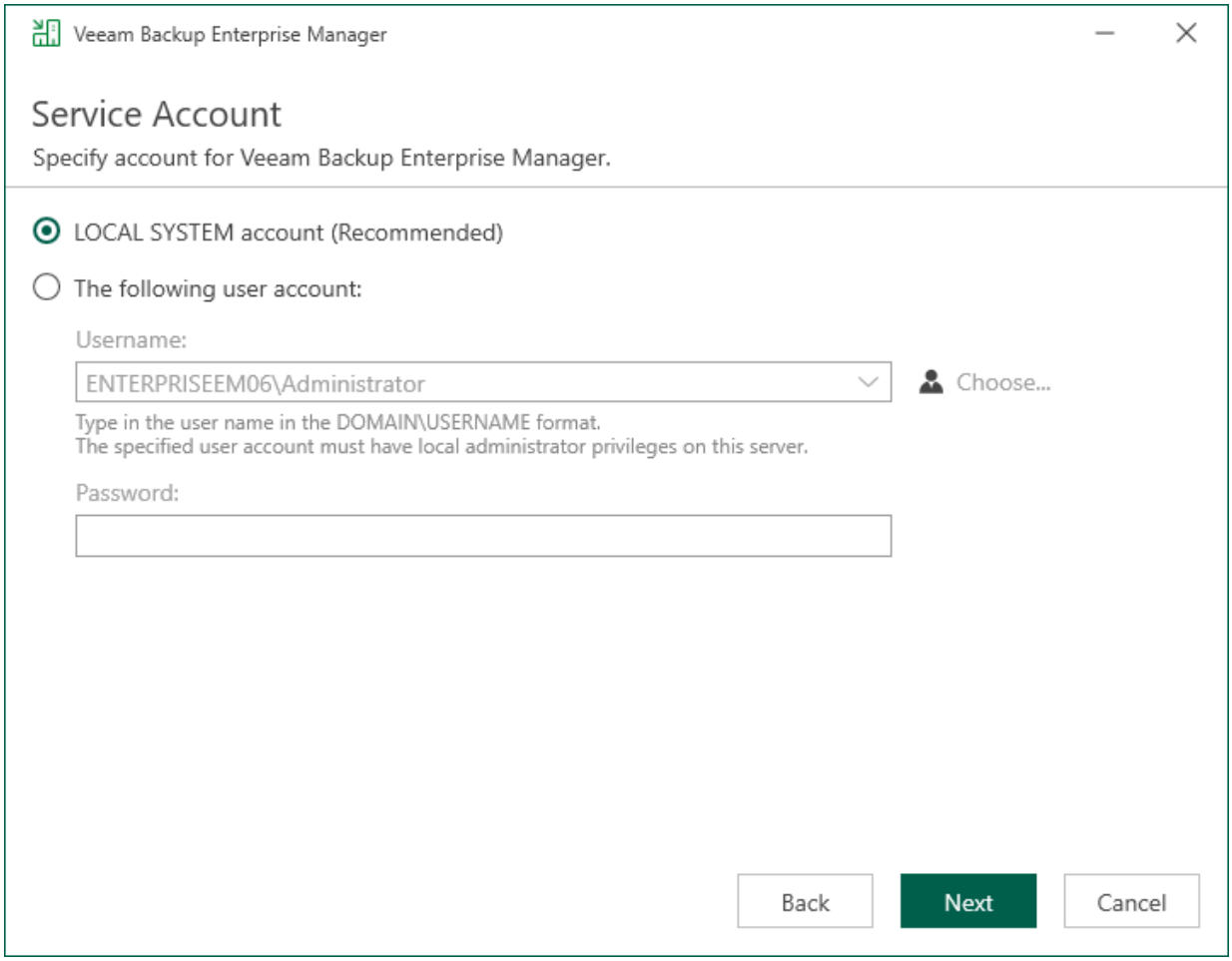
You can select an account under which you want to run the Veeam Backup Enterprise Manager Service:

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

  The user name of the custom account must be specified in the *DOMAIN|USERNAME* format.

NOTE

The user account must have **Veeam Backup Enterprise Manager service account** permissions to run the Veeam Backup Enterprise Manager Service. For more information, see Permissions.



Step 8. Specify Database Server

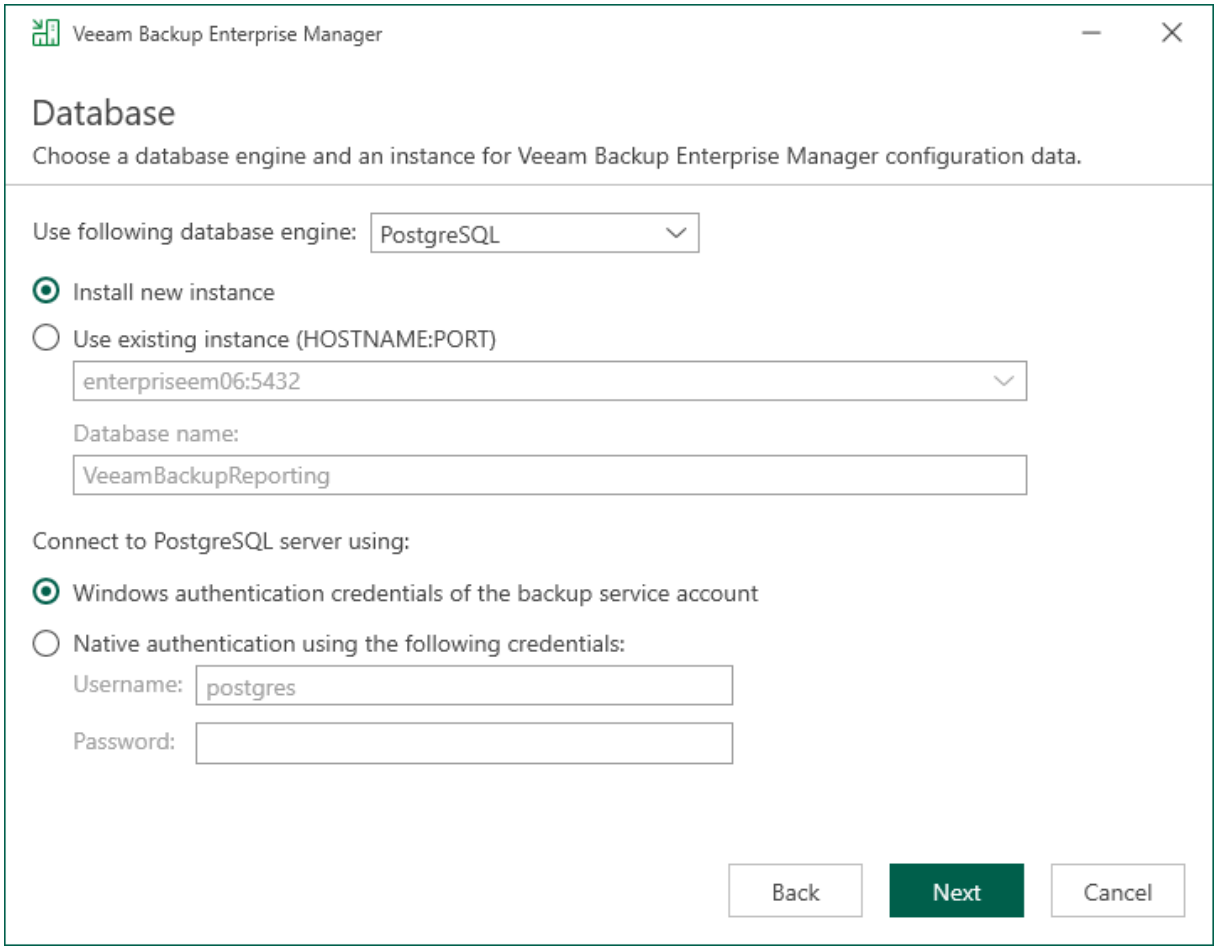
The **Database** step of the wizard is available if you have selected to configure installation settings manually.

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

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

     IMPORTANT

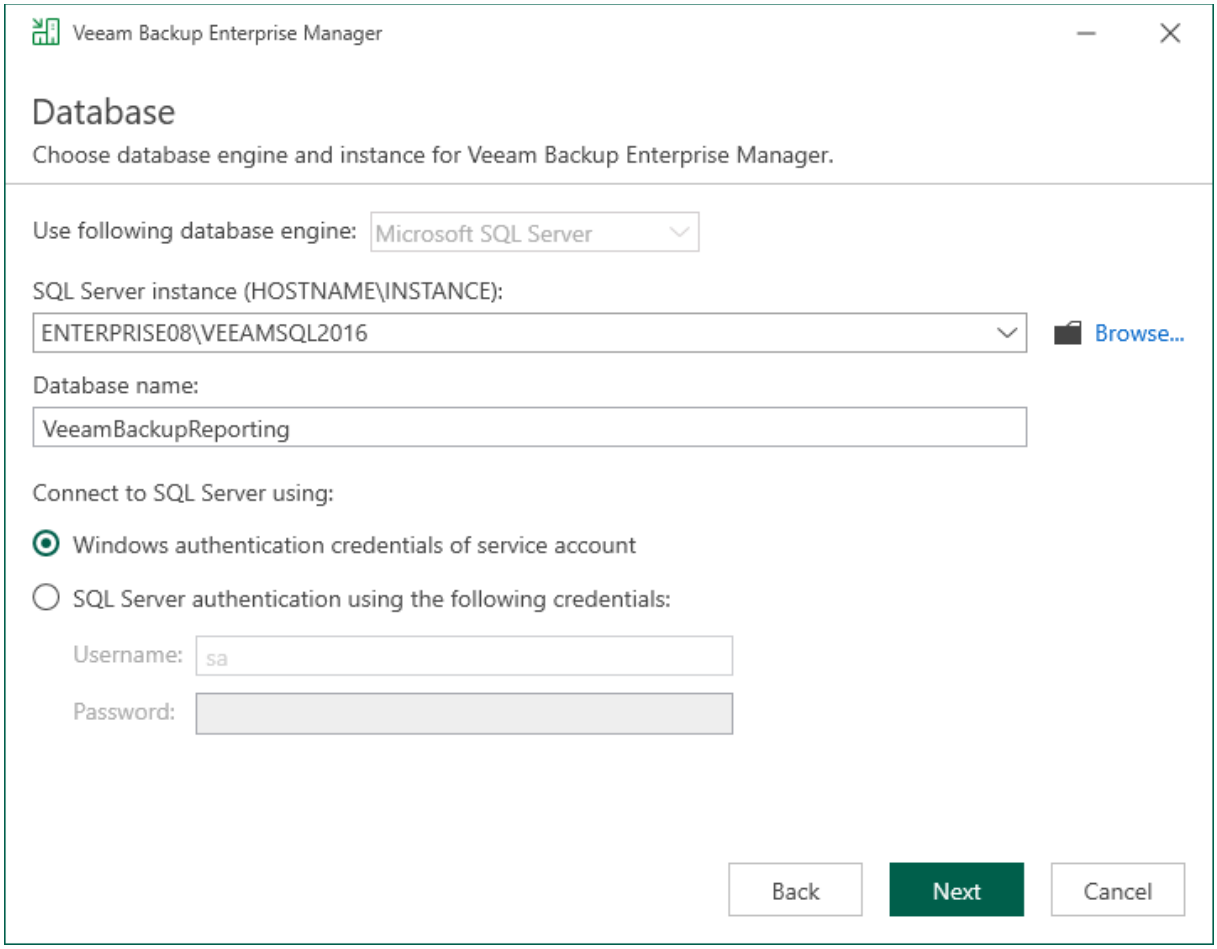
     If you want to use an existing PostgreSQL instance, make sure that the instance can use sufficient resources. For more information, see Configuring PostgreSQL Instance.



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

  i. In the **SQL Server instance** field, enter the instance name in the *HOSTNAME\INSTANCE* format or select an instance from the drop-down list. You can also click **Browse** to choose a Microsoft SQL Server on a remote machine.

ii. In the **Database name** field, specify a name for the Enterprise Manager configuration database.



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

If a configuration database with the specified name already exists (for example, it was created by a previous installation of Enterprise Manager), the setup wizard will notify about it. To connect to the detected database, click **Yes**. If necessary, Enterprise Manager will automatically upgrade the database to the latest version.

Step 9. Specify Data Locations

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

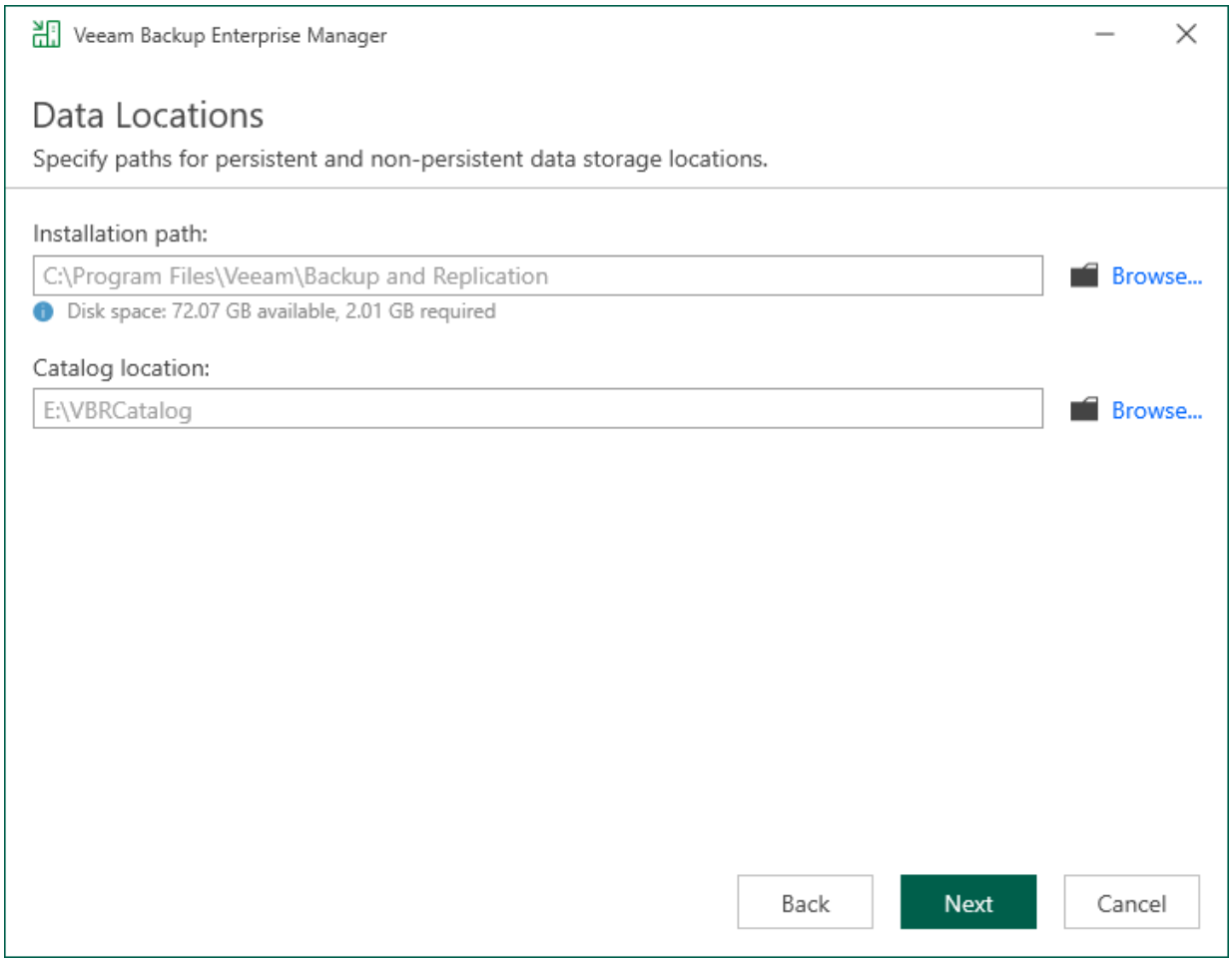
At this step of the wizard, you can specify an installation folder and a folder for the guest file system catalog.

1. To change the default installation folder, click **Browse** next to the **Installation path** field.

   The default installation folder is `%ProgramFiles%\Veeam\Backup and Replication`.

2. To change a path to the folder where index files must be stored, click **Browse** next to the **Catalog location** field. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore.

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



Step 10. Specify Service Ports

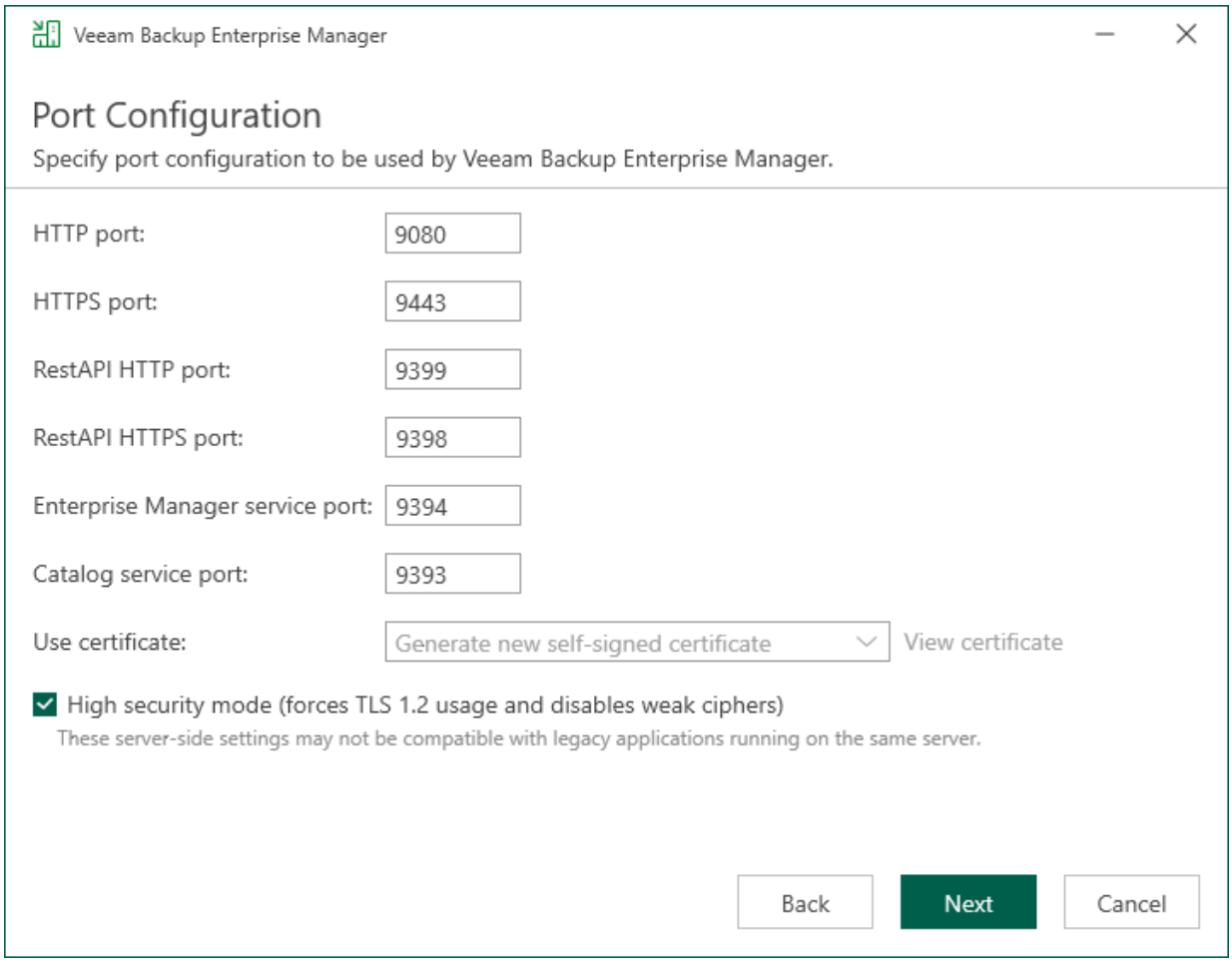
The **Port Configuration** step of the wizard is available if you have selected to configure installation settings manually.

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

1. Provide HTTP and HTTPS port numbers.
2. Specify the certificate to be used by Veeam Backup Enterprise Manager. This certificate is needed to establish secure communication with the Enterprise Manager website using HTTPS; Veeam plug-in for vSphere Client and REST API client also will use this certificate to receive data using HTTPS protocol. If the setup wizard does not find an appropriate certificate, it will generate a self-signed certificate.

   Click **View certificate** to review the details of the selected certificate.
3. To enforce TLS 1.2 encryption protocol for network connections, select the **High security mode** check box.

   This option disables using weak ciphers for all communications with the machine on which Veeam Backup Enterprise Manager runs. This may interfere with the operation of 3rd party software installed on the same machine.

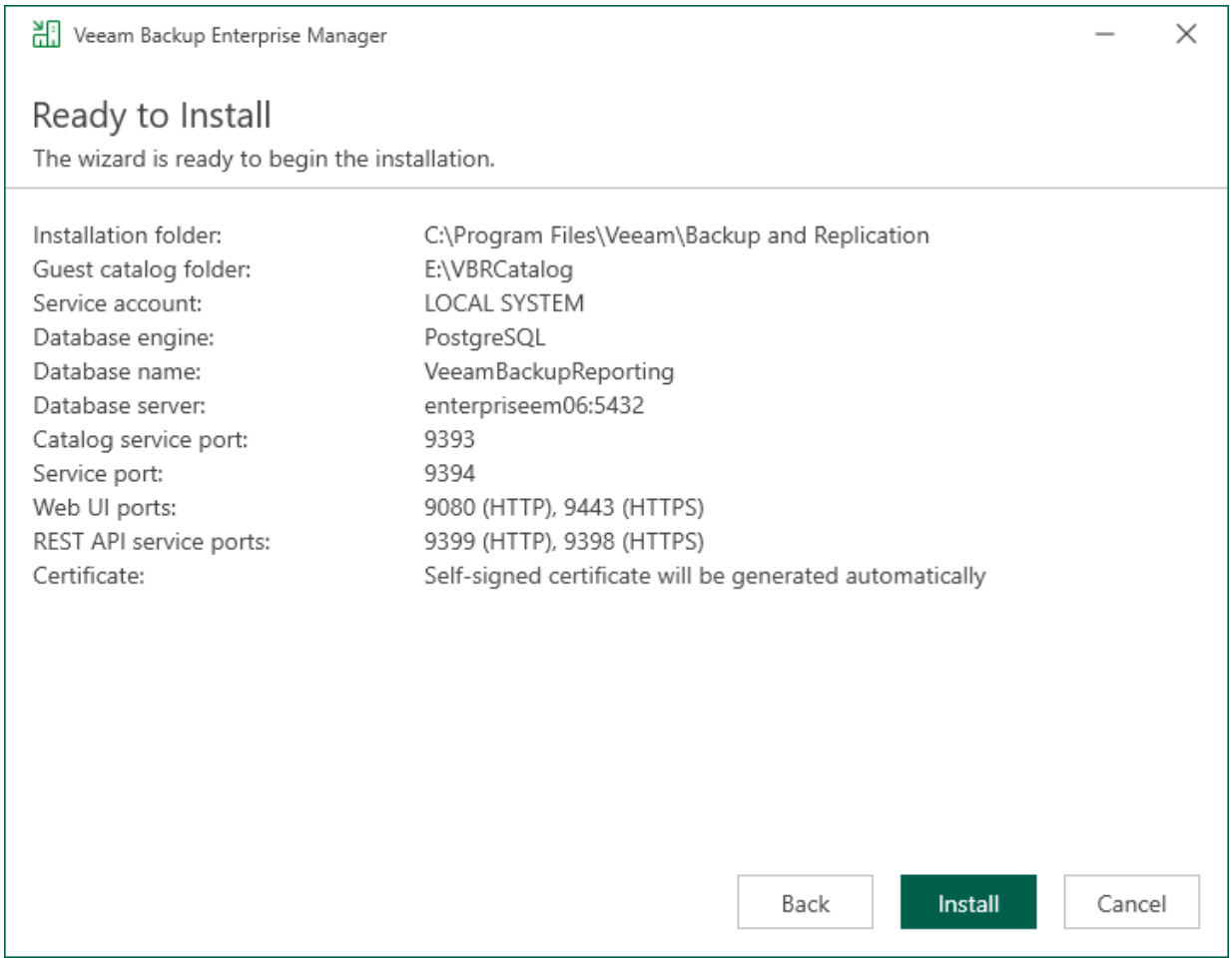


Step 11. Begin Installation

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

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

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



Upgrading to Enterprise Manager 13.1

Before you upgrade Veeam Backup Enterprise Manager to version 13.1, check prerequisites.

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

1. Start the upgrade wizard.
2. Select Enterprise Manager as a product to upgrade.
3. Read and accept the license agreements.
4. Provide a license file.
5. Install missing software.
6. Review the components that will be upgraded and begin the upgrade process.
7. Finalize the upgrade.

Before You Begin

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

- To upgrade Veeam Backup Enterprise Manager to version 13.1, you must be running version 12.3.1 or later. To upgrade from earlier versions, contact Veeam Customer Support.
- A machine on which you plan to install Enterprise Manager must meet the system requirements. For more information, see System Requirements.
- A user account that you plan to use for upgrade must have sufficient permissions. For more information, see Permissions.
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see Ports.
- Check the *Known Issues* section of the Veeam Backup & Replication Release Notes.
- With Enterprise Manager and connected backup servers, begin the backup infrastructure upgrade process with Enterprise Manager. Backup servers must be upgraded after that. When you use different versions of Veeam Backup Enterprise Manager and Veeam Backup & Replication, you may not be able to leverage all features of Veeam Backup Enterprise Manager. Moreover, data collection from backup servers of earlier versions takes more time, which can be critical if many backup servers are added to Enterprise Manager.

  If you have a backup server installed on the same machine, upgrade it immediately after completing upgrade of the Enterprise Manager server. Otherwise, Veeam Backup Catalog, malware detection and the Configuration Database Connection Settings utility will not work properly for Veeam Backup & Replication. For more information about the utility, see Connecting Enterprise Manager to Another Configuration Database.
- In Enterprise Manager, you cannot edit jobs that are managed by backup servers with earlier versions installed until you upgrade the backup servers. Additionally, you cannot create and edit jobs of such backup servers in Veeam Self-Service Backup Portal for Cloud Director and vSphere Self-Service Backup Portal. For example, if you upgrade Enterprise Manager to version 13.1, you will not be able to edit jobs managed by a backup server with version 12.3 until you upgrade the backup server to version 13.1.

- Local antivirus or antimalware software can interfere with Enterprise Manager upgrade. If you receive the *Failed to create website 0x80070020* message, disable your local antivirus or antimalware software and start the upgrade process again. You can re-enable your antivirus software once the upgrade completes. For more information, see this Veeam KB article.
- .NET 3.5.1 WCF HTTP Activation Windows component prevents 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.
- If you use SAML authentication to log in to Enterprise Manager, update the service provider (SP) settings in your identity provider either before or immediately after the Enterprise Manager upgrade. When you configure SP settings for Enterprise Manager version 13, SSO is enabled for both the Enterprise Manager website and vSphere Self-Service Backup Portal; separate configuration for vSphere Self-Service Backup Portal is no longer required. For more information on how to update the SP settings, see Configuring SAML Authentication Settings.

  The following table lists the updated SP settings for Enterprise Manager version 12 and 13.

Setting	Version 12	Version 13
SP Entity ID / Issuer	`https://<host>:<port>/Saml2`	`https://<host>:<port>/oauth/Saml2`
Assertion Consumer URL	`https://<host>:<port>/Saml2/Acs`	`https://<host>:<port>/oauth/Saml2/Acs`

Step 1. Start Upgrade Wizard

To start the upgrade wizard, take the following steps:

1. Download the latest version of the Veeam Backup & Replication installation image from the Veeam Product Downloads page.
2. Mount the installation image to the machine where Veeam Backup Enterprise Manager is installed, or burn the image file to a flash drive or other removable storage device. If you plan to upgrade Veeam Backup Enterprise Manager on a VM, use built-in tools of the virtualization management software to mount the image to the VM.

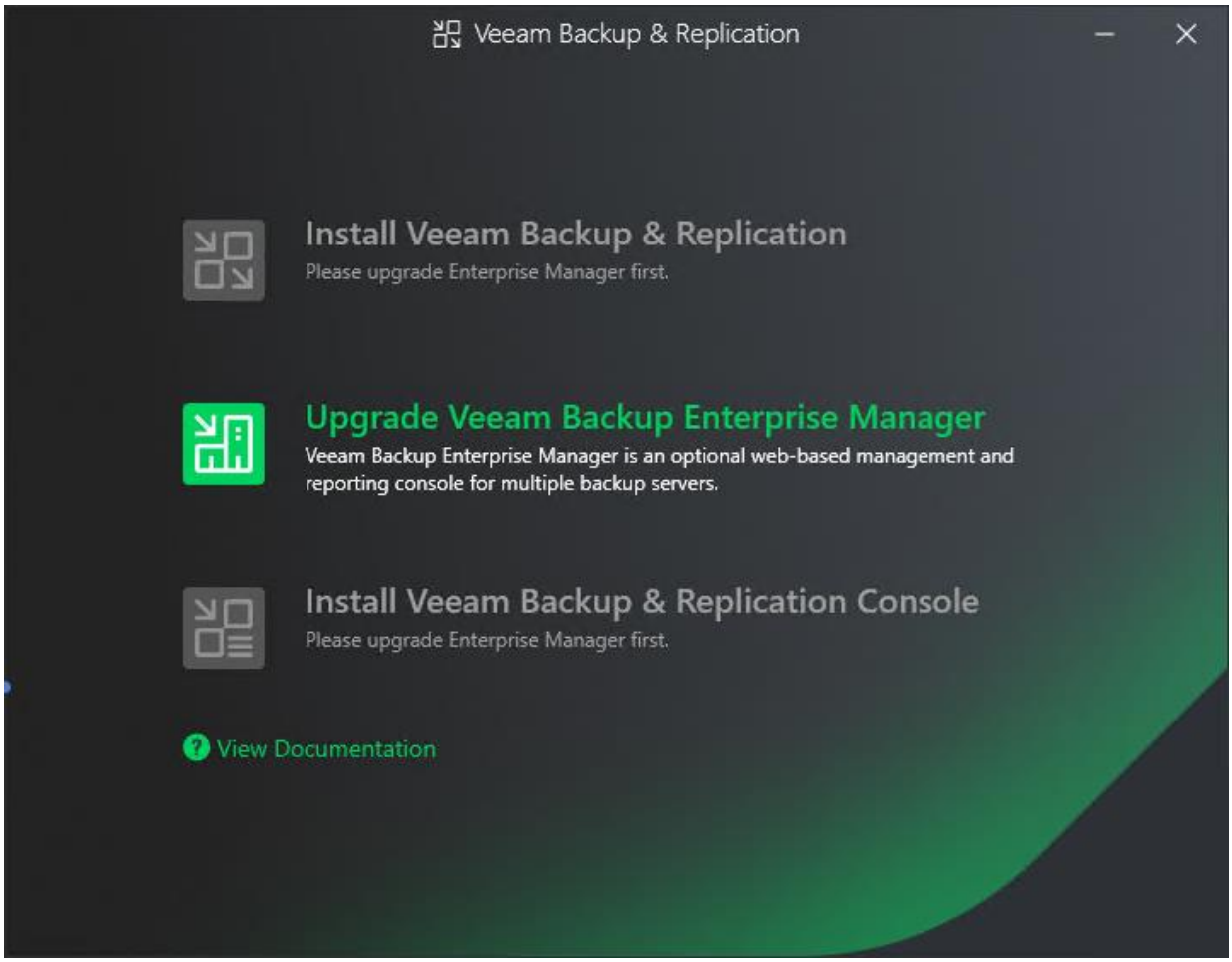
   To extract the content of the ISO file, you can also use the latest versions of utilities that can properly extract data from ISO files of large size and can properly work with long file paths.
3. After you mount the image or insert the disk, Autorun opens a splash screen. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. Click **Upgrade**.



Step 2. Select Product

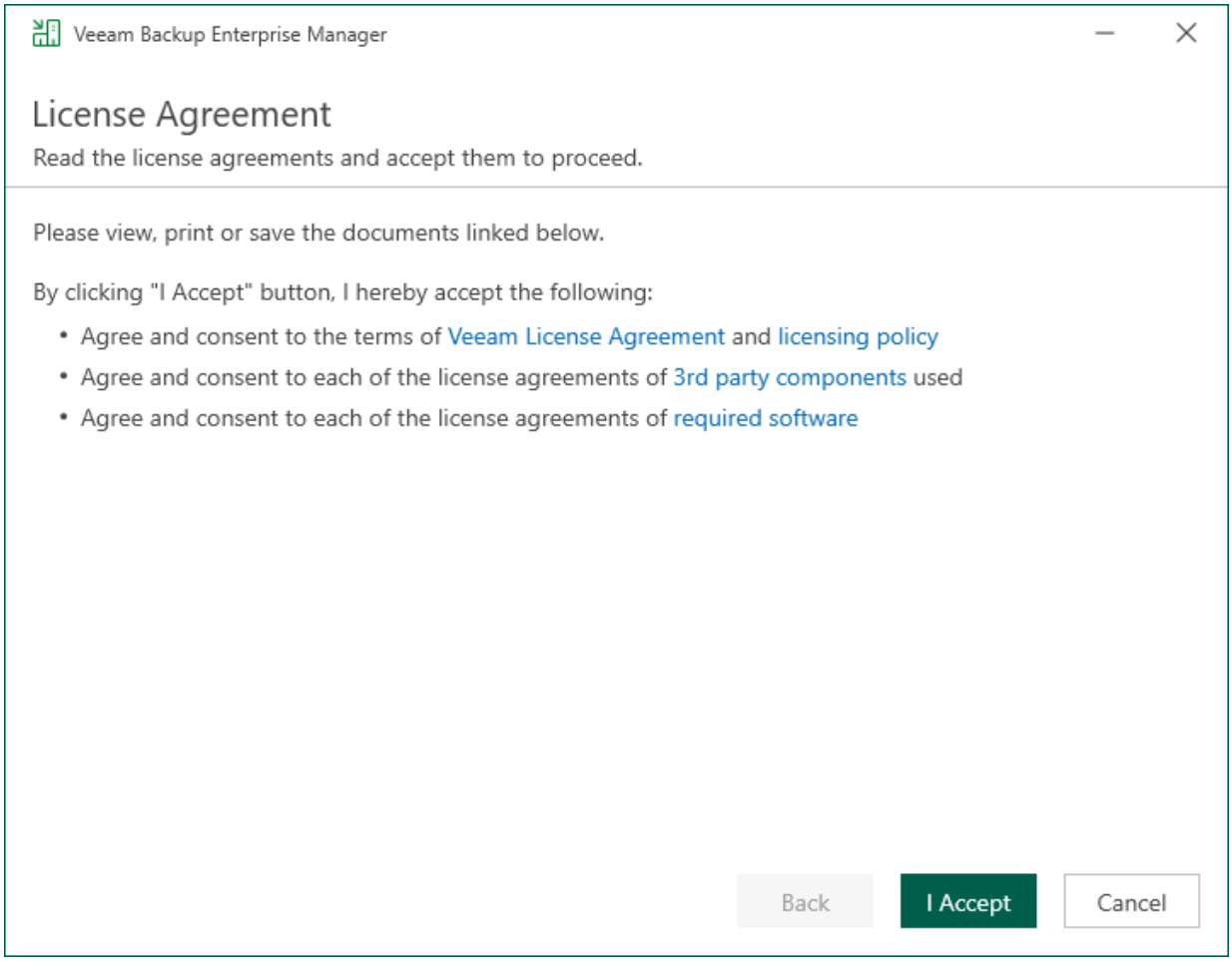
At this step of the wizard, select **Upgrade Veeam Backup Enterprise Manager**.

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



Step 3. Read and Accept License Agreements

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



Step 4. Provide License File

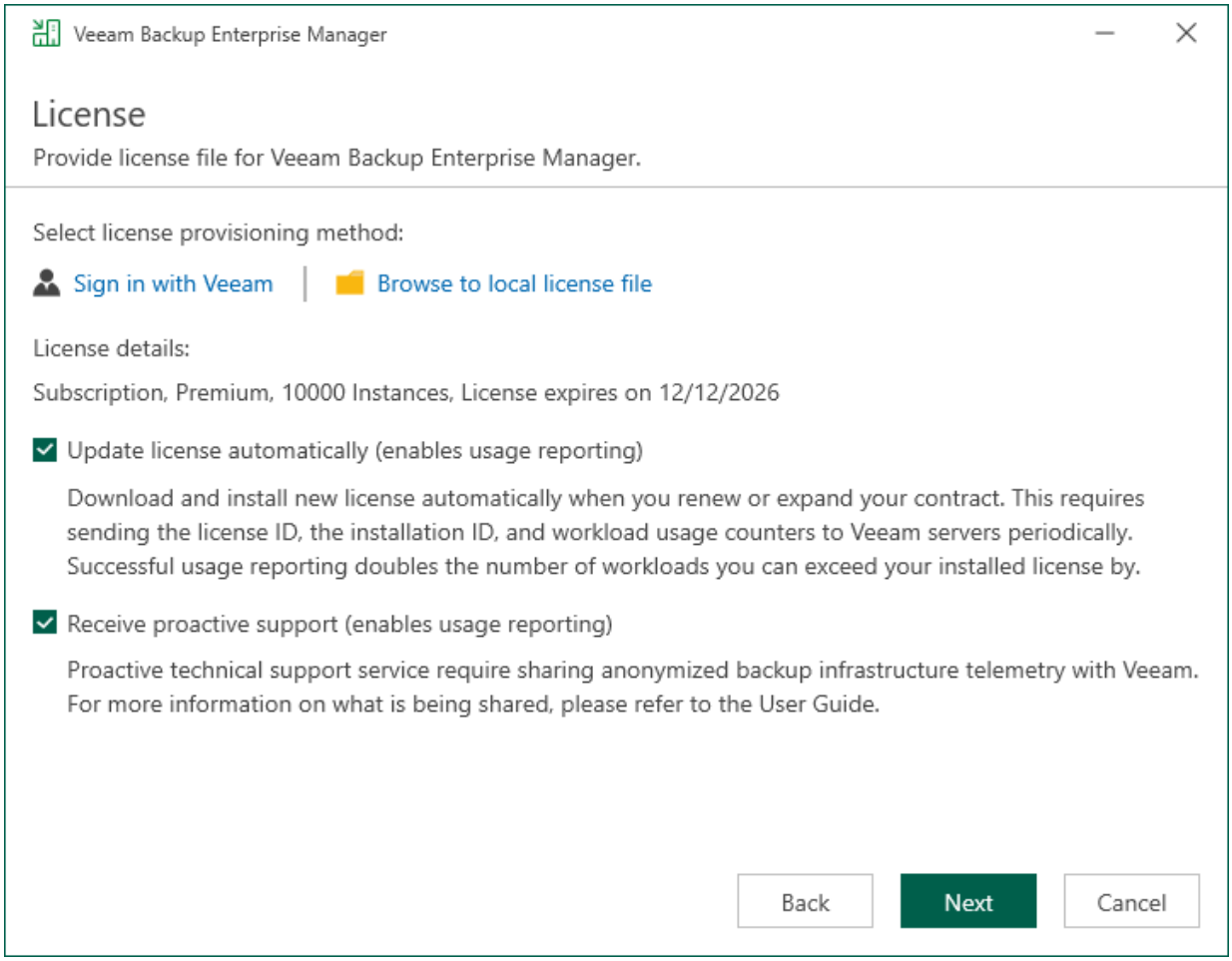
At the **License** step of the wizard, specify what license you want to install for Veeam Backup Enterprise Manager. You can leave the license file used in the previous version of Veeam Backup Enterprise Manager or install a new one.

To install a license, choose one of the following options:

- Browse your local server or network locations for a license file:
  a. Click **Browse to local license file**.
  b. Choose a valid license file for Veeam Backup Enterprise Manager.
- Select a license from your account at the Veeam website:
  a. Click **Sign in with Veeam**.
  b. Enter your credentials for accessing the Veeam website and click Sign in.
  c. Select one of the available licenses and click **Install selected license**.

To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. For more information on license update, see Updating License.

To receive proactive technical support services, select the Receive proactive support check box. Selecting this option also enables diagnostic data sharing. To learn how sensitive data is processed, see Processing of Sensitive Data in Veeam Technical Support.

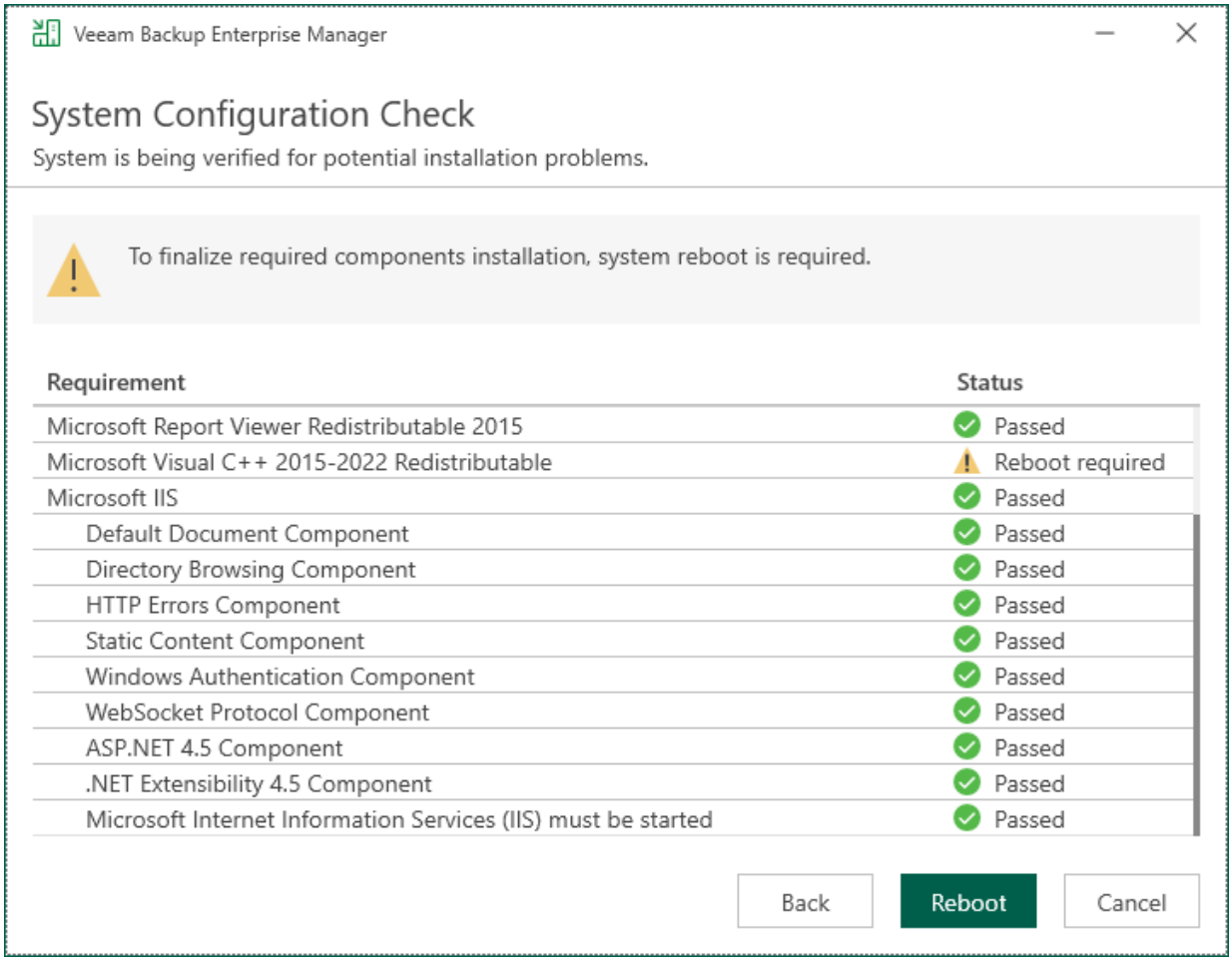


Step 5. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup checks whether required software is installed on the machine.

- If some of the required components are missing, the setup will try to install them automatically. After the components are installed successfully, reboot is required. When you are ready to reboot the machine, click **Reboot**.
- If the setup is not able to install some of the required software automatically, install it manually and click **Retry**.

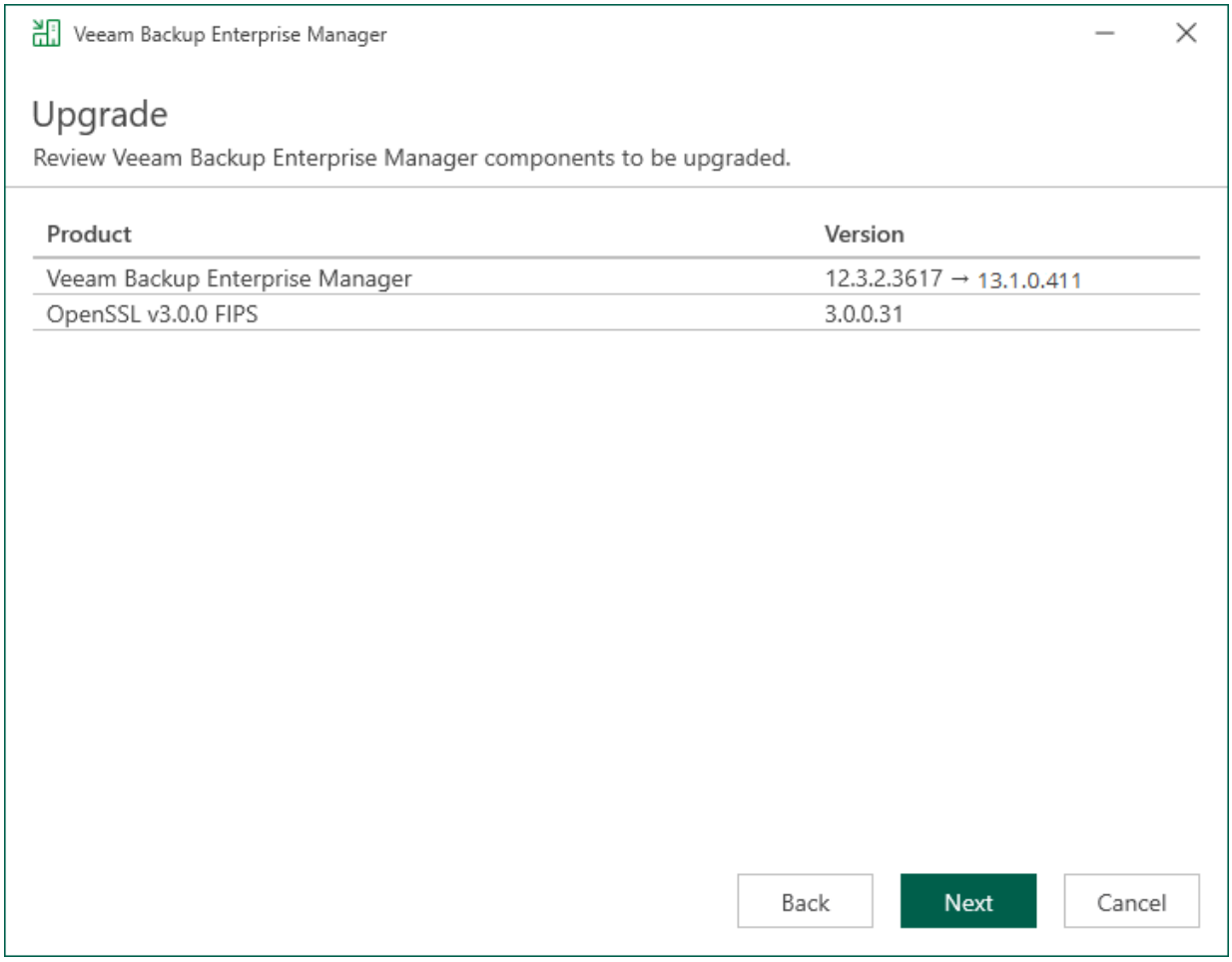
> **NOTE**
>
> If all required software is already installed on the machine, the **System Configuration Check** step will be skipped. For more information on the necessary software, see System Requirements.



Step 6. Review Components and Begin Upgrade

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

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



Step 7. Finalize Upgrade

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

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

   After you upgrade backup servers, Veeam Backup Enterprise Manager starts a maintenance job to optimize the state of its database. The initial maintenance job session may take significant amount of time (up to an hour, depending on the database size). After the job finishes, the database will be brought to an optimal state, and subsequent maintenance job sessions will take much less time.
3. New features of Veeam Backup Enterprise Manager will be available after all connected backup servers are upgraded, and initial collection of data from these servers in Veeam Backup Enterprise Manager completes successfully.
4. Download and install the latest available update (if any).

Updating Enterprise Manager

Apart from version releases of Veeam Backup Enterprise Manager (for example, 13, 13.1), Veeam Software provides updates (for example, update 13.0.1 P1 and 13.0.1 P2). Updates include bug fixes, performance enhancements, and new features.

This article describes how to install updates for Enterprise Manager on Windows. Updated for Enterprise Manager on Linux can be installed automatically. For details, see Veeam Software Appliance Update.

Before You Begin

Before you install an update for Enterprise Manager 13, check the following prerequisites:

- Make sure you have Enterprise Manager 13.1 (build 13.1.x.x) of any earlier patch installed.

  For information on how to upgrade from version 12.3.1 or later, see Upgrading to Enterprise Manager 13.1.

- With Enterprise Manager and connected backup servers, start the update process with Veeam Backup Enterprise Manager. Backup servers should be updated after that. If you have Veeam Backup & Replication and Veeam Backup Enterprise Manager installed on the same machine, the update wizard will update both products at once.

  For more information on the backup server update procedure and prerequisites, see the Updating Veeam Backup & Replication on Windows section of the Veeam Backup & Replication User Guide.

Performing Update

To install the latest update for Enterprise Manager, perform the following steps:

1. Review this Veeam KB article to check if a cumulative patch is available for the version of Veeam Backup Enterprise Manager that is installed.
2. If a cumulative patch is available, click the Veeam KB article link for that cumulative patch.
3. In the **Download Information** section of the Veeam KB article, click **DOWNLOAD PATCH**.
4. To launch the update wizard, unzip the downloaded archive and run the `Setup.exe` file.
5. To install the update, follow the prompts in the update wizard.

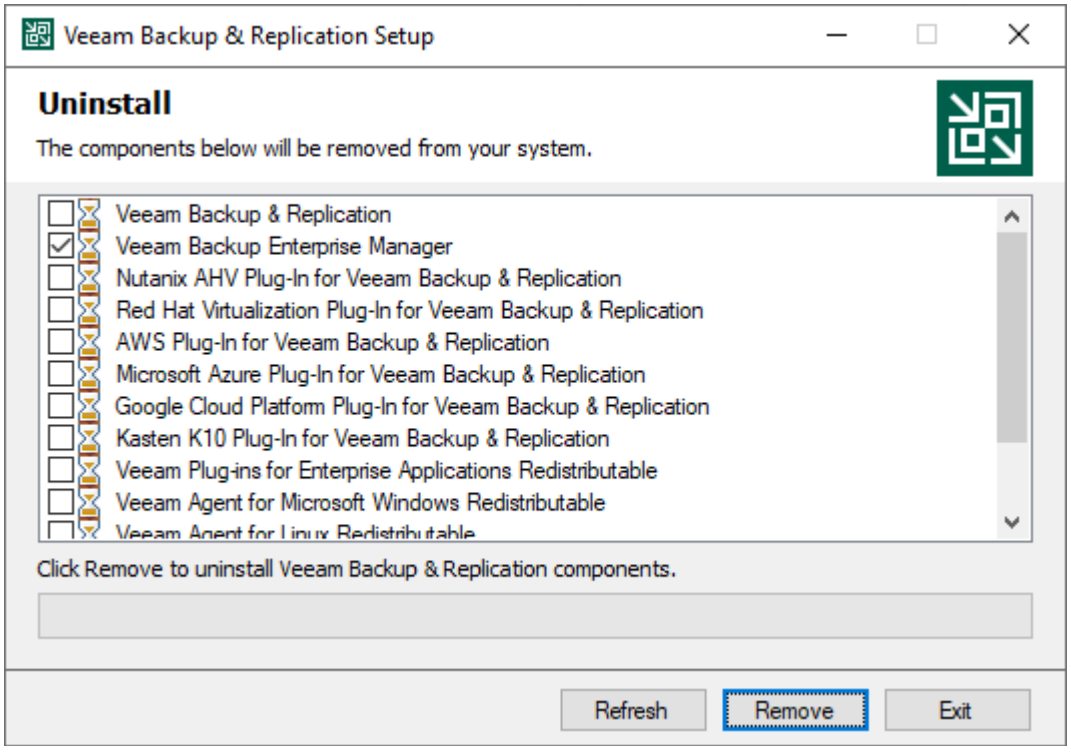
Uninstalling Enterprise Manager

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

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

To uninstall Veeam Backup Enterprise Manager:

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



Migrating Enterprise Manager

You can migrate Veeam Backup Enterprise Manager, its configuration database or both to another machine.

- To migrate the configuration database, use the `Veeam.EM.DB.Migration.exe` utility. You can migrate the Enterprise Manager configuration database only from Microsoft SQL Server to PostgreSQL. If you want to migrate the configuration database from one Microsoft SQL Server instance to another Microsoft SQL Server instance or from one PostgreSQL instance to another PostgreSQL instance, contact Veeam Customer Support. For more information, see Migrating Enterprise Manager from Microsoft SQL Server to PostgreSQL.
- To migrate Enterprise Manager to another machine, uninstall Enterprise Manager from the current machine and install it on a new one. If you also want to migrate the database, manually back up the database and restore it on a new machine. Use the dbconfig tool to connect Enterprise Manager to a different configuration database. Before you migrate Enterprise Manager, you must export Enterprise Manager keysets and prepare the credentials stored in the Enterprise Manager configuration database so you will be able to re-enter the credentials on a new server. If you migrate the Enterprise Manager configuration database only, the credentials and keysets will remain valid.

Migrating Enterprise Manager from Microsoft SQL Server to PostgreSQL

You can migrate the Enterprise Manager configuration database from Microsoft SQL Server to PostgreSQL. If you want to migrate the configuration database from one Microsoft SQL Server instance to another Microsoft SQL Server instance or from one PostgreSQL instance to another PostgreSQL instance, contact Veeam Customer Support.

When performing the migration, you back up the Enterprise Manager configuration database based on Microsoft SQL Server and restore it to PostgreSQL.

Enterprise Manager migration lets you change the engine of the Enterprise Manager configuration database and keep existing Enterprise Manager configurations including notification settings, Enterprise Manager accounts and roles, retention settings for index files and event history, self-service configurations for the Veeam Self-Service Backup Portal and vSphere Self-Service Backup Portal, SAML authentication settings, directory account settings, key management settings and encryption keys.

Before You Begin

Before you migrate the Enterprise Manager configuration database from Microsoft SQL Server to PostgreSQL, consider the following:

- Source Microsoft SQL Server and target PostgreSQL must be set up and running.
- To migrate the configuration database from Microsoft SQL Server to PostgreSQL and attach it to a newer version of Enterprise Manager, first upgrade Enterprise Manager to the newer version to ensure the database structure matches the new version, and then migrate the database from Microsoft SQL Server to PostgreSQL.
- Data that Enterprise Manager collects from backup servers (such as backup jobs, session logs, backed-up objects and so on) is not migrated. This data will be collected again after the first data collection run after migration. For details, see Collecting Data from Backup Servers.

Account Permissions

The Enterprise Manager Database Migration utility requires access to the registry so you must run the command-line shell as administrator. In addition, make sure that the accounts used to run the utility and connect to the target PostgreSQL database have the necessary permissions.

Command	Required Permissions
/backupemdatabase	The account that runs the `/backupemdatabase` command must either be the Enterprise Manager service account or any other account with the following permissions: • *Local Administrator* permissions on the Enterprise Manager server. • *Log on as a service* permission. • The account must also be assigned either of the following roles on the level of the Microsoft SQL Server database: o *db_owner* role o *db_datareader* and *db_datawriter* roles
/restoreemdatabase	The account that you specify to authenticate against a PostgreSQL server in the `/login` parameter must be a superuser. If you don't specify any parameter, the utility will use the account under which the Veeam Backup Enterprise Manager Service is running.

Performing Migration

To migrate Enterprise Manager, you can use the Enterprise Manager Database Migration utility. The utility supports both local (when the database is located on the same machine with Enterprise Manager) and remote Microsoft SQL Server databases (when the database is located on another machine).

The Enterprise Manager Database Migration utility comes with Veeam Backup Enterprise Manager and is located on the Enterprise Manager server in the installation folder. The default path is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\Veeam.EM.DB.Migration.exe`. To run the utility, use a command-line shell.

To migrating Enterprise Manager from Microsoft SQL Server to PostgreSQL, follow these steps:

1. Back up the Enterprise Manager configuration database to an EMCO backup file.

   ```
   Veeam.EM.DB.Migration.exe /file:"C:\EM Configuration\02.emco" /backupemdat
   abase /encryptionpassword:"Password&01" /encryptionhint:"that password"
   ```

   where:

   - `/file:"C:\EM Configuration\02.emco"` — file name and location of the backup file. If you specify a folder that does not exist, the utility will create it. If a file with the specified name already exists, it will be rewritten.
   - `/backupemdatabase` — utility backup mode.
   - `/encryptionpassword:"Password&01"` — encryption password for the backup file.

- /encryptionhint:"that password" — password hint.

Microsoft SQL Server connection settings are not required in the command, the utility gets them from the registry.

2. Restore the Enterprise Manager configuration database from an EMCO backup file to PostgreSQL.

```
Veeam.EM.DB.Migration.exe /file:"C:\EM Configuration\02.emco" /restoreemda
tabase /encryptionpassword:"Password&01" /servername:enterprise05 /initial
catalog:VeeamBackupReporting_01 /serverport:5432 /login:postgres /password
:"Password&02"
```

where:

- /file:"C:\EM Configuration\02.emco" — file name and location of the backup file.
- /restoreemdatabase — utility restore mode.
- /encryptionpassword:"Password&01" — encryption password for the backup file.
- /servername:enterprise05 — name of the target PostgreSQL server.
- /initialcatalog:VeeamBackupReporting_01 — target PostgreSQL instance.
- /serverport:5432 — port number of the target PostgreSQL instance.
- /login:postgres — account name used to authenticate against the PostgreSQL server.
- /password:"Password&02" — password used to authenticate against the PostgreSQL server.

3. Connect Enterprise Manager to the restored database using the Configuration Database Connection Settings utility. For more information, see Connecting Enterprise Manager to Another Configuration Database.

Utility Syntax

With the Enterprise Manager Database Migration utility, you can perform the following operations:

- Back up a Microsoft SQL Server database to an EMCO backup file:

```
Veeam.EM.DB.Migration.exe /file:value /backupemdatabase [/encryptionpasswo
rd:value] [/encryptionhint:value] [/verbose]
```

- Restore a Microsoft SQL Server database from a backup file to PostgreSQL:

```
Veeam.EM.DB.Migration.exe /file:<value> /restoreemdatabase [/encryptionpas
sword:<value>] [/servername:<value>] [/serverport:<value>] [/initialcatalo
g:<value>] [/login:<value>] [/password:<value>] [/verbose]
```

- Display the utility help:

```
Veeam.EM.DB.Migrati
on.exe /?
```

> **TIP**
>
> Use double quotation marks (") around parameter values that contain spaces or special characters.

Utility Parameters

The table below describes parameters that you can use to back up and restore the Enterprise Manager configuration database.

Parameter	Description
/?	Displays help.
/file:<value>	Specifies file name and location of an EMCO backup file.
/encryptionpassword:<value>	Specifies a password for backup file encryption.
/encryptionhint:<value>	Specifies a hint for the encryption password.
/backupemdatabase	Backs up the Enterprise Manager configuration database based on Microsoft SQL Server to an EMCO backup file. Note the command cannot back up a PostgreSQL database.
/restoreemdatabase	Restores the Enterprise Manager configuration database from an EMCO backup file to PostgreSQL.
/servername:<value>	Specifies a name or IP address of the target host with PostgreSQL server. The default value is *localhost*. If you skip the parameter, the default value is used.
/serverport:<value>	Specifies a port number of a PostgreSQL instance. The default value is *5432*. If you skip the parameter, the default value is used.
/initialcatalog:<value>	Specifies a name of a target PostgreSQL database. The default value is *VeeamBackupReporting*. If you skip the parameter, the default value is used. If a database with the specified name (or the default name) exists, the utility adds an increment postfix to the database name, for example: *VeeamBackupReporting_00*, *VeeamBackupReporting_01*.
/login:<value>	Specifies an account name that the utility uses to authenticate against a PostgreSQL server. By default, the utility uses the account under which the Veeam Backup Enterprise Manager Service is running. The chosen PostgreSQL account must be a superuser.

Parameter	Description
/password:<value>	Specifies a password that the utility uses to authenticate against a PostgreSQL server. By default, the utility uses the account under which the Veeam Backup Enterprise Manager Service is running.
/verbose	Enables verbose logging mode. Logs are stored in the following directory: `%PROGRAMDATA%\Veeam\Backup\Utils\Util.EmTransfer`.

Silent Installation, Upgrade and Uninstallation

You can install, upgrade and uninstall Veeam Backup Enterprise Manager in the silent mode with a special XML answer file by using the command line interface. The answer file contains all the necessary installation settings in the proper order and their thorough description.

You can find the template answer file on the Veeam Backup & Replication installation disk in the `\Setup\Silent\AnswerFiles\EM` folder. This folder contains the following templates of answer files:

- `EmAnswerFile_install.xml` — for installing Enterprise Manager
- `EmAnswerFile_uninstall.xml` — for uninstalling Enterprise Manager
- `EmAnswerFile_upgrade.xml` — for upgrading Enterprise Manager

In This Section

- Installing Enterprise Manager in Silent Mode
- Upgrading Enterprise Manager in Silent Mode
- Uninstalling Enterprise Manager in Silent Mode

Installing Enterprise Manager in Silent Mode

You can install Veeam Backup Enterprise Manager in the silent mode with a special XML answer file by using the command line interface. The answer file contains all the necessary installation settings in the proper order and their thorough description.

Before You Begin

Before starting the installation of Veeam Backup Enterprise Manager in the silent mode, consider the following:

- The user account that you use to run the silent installation must be in the local Administrators group on the machine where the silent installation will run. The silent installation cannot be run under the LocalSystem and NetworkService accounts.
- If the user account that you use to run the silent installation is logged on the machine using the network logon method, the silent installation will fail. To avoid this, use an additional `/SkipNetworkLogonErrors` command line key. For example, it is required when the silent installation is started using a remote PowerShell session.
- When configuring the answer file, remove or comment out unused `[Optional]` parameters. Otherwise, the installation session will fail.

Installing Veeam Backup Enterprise Manager

To install Veeam Backup Enterprise Manager in the silent mode with, take the following steps:

1. Copy the `EmAnswerFile_install.xml` file to your local drive.

   You can find the template answer file on the Veeam Backup & Replication installation disk in the `\Setup\Silent\AnswerFiles\EM` folder.

2. Configure installation parameters according to your needs. For details, see Configuration Parameters.

   Check that the answer file has the correct bundle (`Em`) and mode (`install`) specified in line 2:

   ```
   <unattendedInstallationConfiguration bundle="Em" mode="install" version="1
   .0">
   ```

3. After you make all the necessary changes in your answer file, start the installation by running the `Veeam.Silent.Install.exe` file located on the Veeam Backup Enterprise Manager installation disk in the `\Setup\Silent` folder. Use the following command line keys in your command:

   ```
   D:\Setup\Silent\Veeam.Silent.Install.exe /AnswerFile E:\MyAnswerFileEMInst
   all.xml /SkipNetworkLogonErrors
   ```

   where:

   - `/AnswerFile` — required key for specifying the path to your custom answer file, for example: `E:\MyAnswerFileEMInstall.xml`.
   - `/SkipNetworkLogonErrors` — optional key that allows skipping additional pre-installation validations that do not work under the network logon, which will block the silent installation from running.
   - `/LogFolder` — optional key for specifying the path where the setup should save log files if it is different from the default path. The default path is: `C:\ProgramData\Veeam\Setup\Temp`.

Configuration Parameters

The configuration file contains the following parameters:

Parameter	Required	Default Value	Description
ACCEPT_EULA	Yes	—	Specify `1` to accept the Veeam license agreement.
ACCEPT_LICENSING_POLICY	Yes	—	Specify `1` to accept the Veeam licensing policy.
ACCEPT_THIRDPARTY_LICENSES	Yes	—	Specify `1` to accept the license agreement for 3rd party components that Veeam incorporates.
ACCEPT_REQUIRED_SOFTWARE	Yes	—	Specify `1` to accept all required software license agreements.

Parameter	Required	Default Value	Description
VBREM_LICENSE_FILE	No	—	Path to the license file on the machine where you want to install Veeam Backup Enterprise Manager. If you do not specify this parameter (or leave it empty value), Veeam Backup Enterprise Manager will be installed using the current license file.
VBREM_LICENSE_AUTOUPDATE	No	1	Specify `1` to enable automatic license update and usage reporting. Specify `0` if you want to update the license manually. For NFR and Evaluation licenses, specify `1`. For licenses without ID information, specify `0`.
VBREM_SERVICE_USER	No	—	User account under which Veeam Backup Enterprise Manager Service will run. If you do not specify this parameter, the service will run under the LocalSystem account.
VBREM_SERVICE_PASSWORD	No		Password for the account under which Veeam Backup Enterprise Manager Service will run.
VBREM_SQLSERVER_INSTALL	Yes	1	Specify `0` to use an existing SQL server instance or specify `1` to create a new SQL server instance.
VBREM_SQLSERVER_ENGINE	No	1	Specify `0` to use PostgreSQL engine or specify `1` to use Microsoft SQL engine. Note that if you want to create a new SQL server instance, you can only choose the PostgreSQL engine.
VBREM_SQLSERVER_SERVER	No	localhost:5432	SQL server and instance (for Microsoft SQL) or SQL server an port (for PostgreSQL) where the configuration database will be deployed. Note that if you want to create a new SQL instance, you can only connect to a local host.

Parameter	Required	Default Value	Description
VBREM_SQLSERVER_DATABASE	No	VeeamBackupReporting	Configuration database name. If you do not specify this parameter, the default `VeeamBackupReporting` name is used.
VBREM_SQLSERVER_AUTHENTICATION	No	0	Authentication mode to connect to the SQL Server where the Veeam Backup & Replication configuration database is deployed. Specify `1` to use the SQL Server authentication mode or specify `0` to use the Microsoft Windows authentication mode.
VBREM_SQLSERVER_USERNAME	No	—	LoginID to connect to the SQL Server in the SQL Server authentication mode.
VBREM_SQLSERVER_PASSWORD	No	—	Password to connect to the SQL Server in the SQL Server authentication mode. The parameter is required if `VBREM_SQLSERVER_USERNAME` is specified.
VBRC_SERVICE_PORT	No	9393	TCP port to be used by the Veeam Guest Catalog Service. If you do not specify this parameter, the default `9393` port is used.
VBREM_SERVICE_PORT	No	9394	TCP port to be used by the Veeam Backup Service. If you do not specify this parameter, the default `9394` port is used. If the specified port number is already occupied, the setup will assign the next available port number to the component.
VBREM_TCPPORT	No	9080	TCP port be used by the Veeam Backup Enterprise Manager website. If you do not specify this parameter, the default `9080` port is used.

Parameter	Required	Default Value	Description
VBREM_SSLPORT	No	9443	SSL port be used by the Veeam Backup Enterprise Manager website. If you do not specify this parameter, the default `9443` port is used.
VBREM_RESTSERVICE_PORT	No	9399	TCP port used for communication with Veeam Backup Enterprise Manager REST API Service. If you do not specify this parameter, the default `9399` port is used.
VBREM_RESTAPISVC_SSLPORT	No	9398	SSL port used for Veeam Backup Enterprise Manager REST API Service. If you do not specify this parameter, the default `9398` port is used.
VBREM_THUMBPRINT	No	—	Certificate to be used by Veeam Backup Enterprise Manager Service and Veeam Backup Enterprise Manager REST API Service. If you do not specify this parameter, a new certificate will be generated by `openssl.exe`.
INSTALLDIR	No	C:\Program Files\Veeam\Backup and Replication	Path to the directory where Veeam Backup Enterprise Manager will be installed. If you do not specify this parameter, the default `%ProgramFiles%\Veeam\Backup and Replication` installation path is used.
VM_CATALOGPATH	No	C:\VBRCatalog	Path to the catalog folder where index files will be stored. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore. If you do not specify this parameter, a path is selected based on the free space across all available disks.

Parameter	Required	Default Value	Description
VBREM_CHECK_UPDATES	No	1	Specify 1 to automatically check for new product versions and updates. Specify 0 if you do not want Veeam Backup Enterprise Manager to check for updates automatically.
VBREM_CONFIG_SCHANNEL	No	1	Specify 1 if you want to use the TLS 1.2 protocol for secure communication with the Veeam Backup Enterprise Manager website.
REBOOT_IF_REQUIRED	No	0	Specify 1 if you want to reboot the machine where you install Veeam Backup Enterprise Manager after the installation finishes. Specify 0 if you do not want to reboot the machine.

Note that you must specify *1* in ACCEPT_EULA, ACCEPT_LICENSING_POLICY, ACCEPT_THIRDPARTY_LICENSES and ACCEPT_REQUIRED_SOFTWARE parameters to proceed with the installation.

Installation Result Codes

The installation result is written into the installation log file located at your selected log folder. It may show one of the following result codes:

Result Code	Result
0	success
1603	install failure
3010	reboot required
3011	logoff required

Installation Error Codes

The installation error codes accompanied by their detailed description are displayed in the command line dialog. They can also be found in the `UnattendedInstallationResult_%DATE%_%TIME%.xml` file in the log folder (by default, `C:\ProgramData\Veeam\Setup\Temp`). The error message may show one of the following error codes:

Error Code	Description
0	Installation has been completed successfully.
1	Product is already installed.
2	Uninstallation has been completed successfully.
11	Unable to start the setup program, because machine's reboot is pending.
12	Reboot is required to finalize prerequisites installation.
13	Reboot is required to finalize the product installation.
14	Logoff is required to finalize the product installation.
101	Failed to start the installer.
102	Invalid answer file provided.
103	Invalid launch conditions.
104	Failed to initialize setup properties.
105	Failed to validate setup properties.
106	System configuration check detected some issues.
107	Failed to install prerequisites.
108	Failed to install a database server.
109	Failed to install the product.

Error Code	Description
110	Failed to update the product.
111	Failed to change a service status.
112	Failed to uninstall the product.
113	Unexpected error occurred.

Upgrading Enterprise Manager in Silent Mode

You can upgrade Veeam Backup Enterprise Manager in the silent mode with a special XML answer file by using the command line interface. The answer file contains all the necessary upgrade settings in the proper order and their thorough description.

Before You Begin

Before starting the upgrade of Veeam Backup Enterprise Manager in the silent mode, consider the following:

- The user account that you use to run the silent upgrade must be in the local Administrators group on the machine where the silent upgrade will run. The silent upgrade cannot be run under the LocalSystem and NetworkService accounts.
- If the user account that you use to run the silent upgrade is logged on the machine using the network logon method, the silent installation will fail. To avoid this, use an additional `/SkipNetworkLogonErrors` command line key. For example, it is required when the silent installation is started using a remote PowerShell session.
- When configuring the answer file, remove or comment out unused `[Optional]` parameters. Otherwise, the upgrade session will fail.

Upgrading Veeam Backup Enterprise Manager

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

1. Copy the `EmAnswerFile_upgrade.xml` file to your local drive.

   You can find the template answer file on the Veeam Backup & Replication installation disk in the `\Setup\Silent\AnswerFiles\EM` folder.

2. Configure installation parameters according to your needs. For details, see Configuration Parameters.

   Check that the answer file has the correct bundle (`Em`) and mode (`upgrade`) specified in line 2:

   ```
   <unattendedInstallationConfiguration bundle="Em" mode="upgrade" version="1
   .0">
   ```

3. After you make all the necessary changes in your answer file, start the upgrade by running the `Veeam.Silent.Install.exe` file located on the Veeam Backup Enterprise Manager installation disk in the `\Setup\Silent` folder. Use the following command line keys in your command:

```
D:\Setup\Silent\Veeam.Silent.Install.exe /AnswerFile E:\MyAnswerFileEMUpgr
ade.xml /SkipNetworkLogonErrors
```

where:

- `/AnswerFile` — required key for specifying the path to your custom answer file, for example: `E:\MyAnswerFileEMUpgrade.xml`.
- `/SkipNetworkLogonErrors` — optional key that allows skipping additional pre-installation validations that do not work under the network logon, which will block the silent installation from running.
- `/LogFolder` — optional key for specifying the path where the setup should save log files if it is different from the default path. The default path is: `C:\ProgramData\Veeam\Setup\Temp`.

Configuration Parameters

The configuration file contains the following parameters:

Parameter	Required?	Default	Description
ACCEPT_EULA	Yes	—	Specify `1` to accept the Veeam license agreement.
ACCEPT_LICENSING_POLICY	Yes	—	Specify `1` to accept the Veeam licensing policy.
ACCEPT_THIRDPARTY_LICENSES	Yes	—	Specify `1` to accept the license agreement for 3rd party components that Veeam incorporates.
ACCEPT_REQUIRED_SOFTWARE	Yes	—	Specify `1` to accept all required software license agreements.
VBREM_LICENSE_FILE	No	—	Path to the license file on the machine where you want to upgrade Veeam Backup Enterprise Manager. If you do not specify this parameter (or leave it empty value), Veeam Backup Enterprise Manager will be upgraded using the current license file.
VBREM_LICENSE_AUTOUPDATE	No	1	Specify `1` to enable automatic license update and usage reporting. Specify `0` if you want to update the license manually. For NFR and Evaluation licenses, specify `1`. For licenses without ID information, specify `0`.

Parameter	Required?	Default	Description
VBREM_SERVICE_PASSWORD	No	—	Password for the account under which Veeam Backup Enterprise Manager Service will run.
VBREM_SQLSERVER_PASSWORD	No	—	Password to connect to the SQL Server in the SQL Server authentication mode.
REBOOT_IF_REQUIRED	No	0	Specify `1` if you want to reboot the machine where you install Veeam Backup Enterprise Manager after the installation finishes. Specify `0` if you do not want to reboot the machine.

Note that you must specify *1* in `ACCEPT_EULA`, `ACCEPT_LICENSING_POLICY`, `ACCEPT_THIRDPARTY_LICENSES` and `ACCEPT_REQUIRED_SOFTWARE` parameters to proceed with the installation.

Upgrade Result Codes

The installation result is written into the installation log file located at your selected log folder. It may show one of the following result codes:

Result Code	Result
0	success
1603	install failure
3010	reboot required
3011	logoff required

Upgrade Error Codes

The installation error codes accompanied by their detailed description are displayed in the command line dialog. They can also be found in the `UnattendedInstallationResult_%DATE%_%TIME%.xml` file in the log folder (by default, `C:\ProgramData\Veeam\Setup\Temp`). The error message may show one of the following error codes:

Error Code	Description
0	Installation has been completed successfully.
1	Product is already installed.
2	Uninstallation has been completed successfully.
11	Unable to start the setup program, because machine's reboot is pending.
12	Reboot is required to finalize prerequisites installation.
13	Reboot is required to finalize the product installation.
14	Logoff is required to finalize the product installation.
101	Failed to start the installer.
102	Invalid answer file provided.
103	Invalid launch conditions.
104	Failed to initialize setup properties.
105	Failed to validate setup properties.
106	System configuration check detected some issues.
107	Failed to install prerequisites.
108	Failed to install a database server.
109	Failed to install the product.

Error Code	Description
110	Failed to update the product.
111	Failed to change a service status.
112	Failed to uninstall the product.
113	Unexpected error occurred.

Uninstalling Enterprise Manager in Silent Mode

You can uninstall Veeam Backup Enterprise Manager in the silent mode with a special XML answer file by using the command line interface. The answer file contains all the necessary uninstallation settings in the proper order and their thorough description.

Before You Begin

Before starting the uninstallation of Veeam Backup Enterprise Manager in the silent mode, consider the following:

- The user account that you use to run the silent uninstallation must be in the local Administrators group on the machine where the silent uninstallation will run. The silent uninstallation cannot be run under the LocalSystem and NetworkService accounts.
- If the user account that you use to run the silent uninstallation is logged on the machine using the network logon method, the silent uninstallation will fail. To avoid this, use an additional `/SkipNetworkLogonErrors` command line key. For example, it is required when the silent uninstallation is started using a remote PowerShell session.
- When configuring the answer file, remove or comment out unused `[Optional]` parameters. Otherwise, the uninstallation session will fail.

Uninstalling Veeam Backup Enterprise Manager

To uninstall Veeam Backup Enterprise Manager in the silent mode with the answer file, take the following steps:

1. Copy the `EmAnswerFile_uninstall.xml` file to your local drive.

   You can find the template answer file on the Veeam Backup & Replication installation disk in the `\Setup\Silent\AnswerFiles\EM` folder.

2. Configure uninstallation parameters according to your needs. For details, see Configuration Parameters.

   Check that the answer file has the correct bundle (`Em`) and mode (`uninstall`) specified in line 2:

```
<unattendedInstallationConfiguration bundle="Em" mode="uninstall" version=
"1.0">
```

3. After you make all the necessary changes in your answer file, start the uninstallation by running the `Veeam.Silent.Install.exe` file located on the Veeam Backup Enterprise Manager installation disk in the `\Setup\Silent` folder. Use the following command line keys in your command:

```
D:\Setup\Silent\Veeam.Silent.Install.exe /AnswerFile E:\MyAnswerFileEMInin
stall.xml /SkipNetworkLogonErrors
```

where:

- `/AnswerFile` — required key for specifying the path to your custom answer file, for example: `E:\MyAnswerFileEMUninstall.xml`.
- `/SkipNetworkLogonErrors` — optional key that allows skipping additional pre-installation validations that do not work under the network logon, which will block the silent installation from running.
- `/LogFolder` — optional key for specifying the path where the setup should save log files if it is different from the default path. The default path is: `C:\ProgramData\Veeam\Setup\Temp`.

Configuration Parameters

The configuration file contains the following parameters:

Parameter	Required?	Default	Description
REBOOT_IF_REQUIRED	No	0	Specify `1` if you want to reboot the machine where you uninstall Veeam Backup & Replication after the uninstallation finishes. Specify `0` if you do not want to reboot the machine.

Uninstallation Result Codes

The installation result is written into the installation log file located at your selected log folder. It may show one of the following result codes:

Result Code	Result
0	success
1603	install failure
3010	reboot required
3011	logoff required

Uninstallation Error Codes

The installation error codes accompanied by their detailed description are displayed in the command line dialog. They can also be found in the `UnattendedInstallationResult_%DATE%_%TIME%.xml` file in the log folder (by default, `C:\ProgramData\Veeam\Setup\Temp`). The error message may show one of the following error codes:

Error Code	Description
1	Product is already installed.
2	Uninstallation has been completed successfully.
11	Unable to start the setup program, because machine's reboot is pending.
101	Failed to start the installer.
102	Invalid answer file provided.
103	Invalid launch conditions.
112	Failed to uninstall the product.
113	Unexpected error occurred.

Migrating Enterprise Manager from Windows to Linux

You can migrate Enterprise Manager from a Microsoft Windows-based machine to a Linux-based machine. To perform the migration, back up the Enterprise Manager configuration database and restore it to the Linux machine where Enterprise Manager is already deployed.

Enterprise Manager migration preserves existing Enterprise Manager configurations including notification settings, Enterprise Manager accounts and roles, retention settings for index files and event history, self-service configurations for the Veeam Self-Service Backup Portal and vSphere Self-Service Backup Portal, SAML authentication settings, directory account settings, key management settings and encryption keys.

Before You Begin

Before you migrate the Enterprise Manager configuration database from a Microsoft Windows-based machine to a Linux-based, consider the following:

- Enterprise Manager of the same build must be installed on both the Microsoft Windows and Linux machines. For deployment instructions, see Enterprise Manager Deployment on Linux and Enterprise Manager Deployment on Windows.
- The Microsoft Windows installation of Enterprise Manager must use PostgreSQL as its configuration database. If the database is based on Microsoft SQL Server, first migrate it to PostgreSQL. For details, see Migrating Enterprise Manager from Microsoft SQL Server to PostgreSQL.
- PostgreSQL must be set up and running on the source and target machines.
- Data that Enterprise Manager collects from backup servers (such as backup jobs, session logs, backed-up objects and so on) is not migrated. This data will be collected again after the first data collection run after migration. For details, see Collecting Data from Backup Servers.
- After you successfully migrate Enterprise Manager to Linux, local Microsoft Windows users will not be migrated (local Microsoft Windows groups may appear but cannot be used on Linux). Domain Active Directory users and groups will be preserved if Veeam Software Appliance is joined to the same Active Directory domain. The *veeamadmin* account will be automatically assigned the Enterprise Manager Administrator role.

Performing Migration

To migrate Enterprise Manager from Microsoft Windows to Linux, you can use the Enterprise Manager Database Migration utility. The utility supports both local (when the database is located on the same machine with Enterprise Manager) and remote PostgreSQL databases (when the database is located on another machine).

The Enterprise Manager Database Migration utility comes with Veeam Backup Enterprise Manager and is located on the Enterprise Manager server in the installation folder. The default path is the following:

- On Microsoft Windows-based machine:

```
%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\Veeam.EM.DB
.Migration.exe
```

- On Linux-based machine:

```
/opt/veeam/vbem/Veeam.EM.DB.Migration.dll
```

To migrate Enterprise Manager, follow these steps:

1. On the Microsoft Windows machine, back up the Enterprise Manager configuration database to an EMCO backup file. To create a configuration backup, use the `Veeam.EM.DB.Migration.exe` application. The utility requires access to the registry so you must run the command-line shell as administrator. In addition, make sure that the account that you specify to authenticate against a PostgreSQL server is a superuser.

```
Veeam.EM.DB.Migration.exe /file:"C:\em_configuration.emco" /backupemdataba
se /encryptionpassword:"Password&01" /encryptionhint:"that password"
```

2. Transfer the backup file to the Linux machine where Enterprise Manager is deployed as part of Veeam Software Appliance:

   a. To enable SSH connection on the Linux machine, use Veeam Host Management. For details, see Configuring Remote Access Settings.

   b. To transfer the backup file, you can run, for example, the `scp` command on the Microsoft Windows machine:

```
scp "C:\em_configuration.emco" veeamadmin@em.example.com:/tmp/em_config
uration.emco
```

3. Restore the configuration database on the Linux machine:

   a. To request root access on the Linux machine, use Veeam Host Management. For details, see Configuring Remote Access Settings.

   b. To restore the configuration database from the backup file, run the `Veeam.EM.DB.Migration.dll` application with the `dotnet` command:

```
# dotnet /opt/veeam/vbem/Veeam.EM.DB.Migration.dll /file:"/tmp/em_confi
guration.emco" /restoreemdatabase /encryptionpassword:'Password&01'
```

4. Update the configuration database name in the configuration file `/etc/veeam/veeam_backup_reporting.conf`:

```
[DatabaseConfigurations]
SqlActiveConfiguration=PostgreSql
[DatabaseConfigurations\MsSql]
[DatabaseConfigurations\PostgreSql]
SqlDatabaseName=VeeamBackupReporting_00
```

5. To apply the changes, restart all Enterprise Manager services using Veeam Host Management. For details, see Performing Maintenance Tasks.

6. To enable Enterprise Manager to collect data from added backup servers, re-enter credentials for each added backup servers. For details, see Editing Backup Servers.

Utility Parameters

The table below describes the `Veeam.EM.DB.Migration` parameters that you can use to migrate Enterprise Manager from Microsoft Windows to Linux.

Parameter	Description
/?	Displays help.
/file:<value>	Specifies file name and location of an EMCO backup file.
/encryptionpassword:<value>	Specifies a password for backup file encryption.
/encryptionhint:<value>	Specifies a hint for the encryption password.
/backupemdatabase	Backs up the Enterprise Manager configuration database to an EMCO backup file.
/restoreemdatabase	Restores the Enterprise Manager configuration database from an EMCO backup file.
/initialcatalog:<value>	Specifies a name of a target PostgreSQL database. The default value is *VeeamBackupReporting*. If you skip the parameter, the default value is used. If a database with the specified name (or the default name) exists, the utility adds an increment postfix to the database name, for example: *VeeamBackupReporting_00*, *VeeamBackupReporting_01*.
/verbose	Enables verbose logging mode.

Connecting Enterprise Manager to Another Configuration Database

The Configuration Database Connection Settings utility allows you to manage connection settings for Veeam Backup Enterprise Manager and Veeam Backup & Replication configuration databases.

Using this utility, you can perform the following tasks:

- Connect Enterprise Manager and Veeam Backup & Replication to a different database on the same or another server.
- Change authentication method for database connection. Possible options are Microsoft Windows authentication and database server authentication.

NOTE

- With the Configuration Database Connection Settings utility, you can connect Enterprise Manager (or Veeam Backup & Replication) to a configuration database of the same product version only. For example, you can connect Enterprise Manager 13.1 to a configuration database of version 13.1.
- The Configuration Database Connection Settings utility is shared between Veeam Backup & Replication and Veeam Backup Enterprise Manager. If they are installed on the same machine, make sure these products are of the same version.

To manage connection settings for the Enterprise Manager configuration database, do one of the following:

- Use the Configuration Database Connection Settings wizard. The wizard is available only for Enterprise Manager installed on Microsoft Windows. For details, see Connecting to Another Database Using Wizard.
- Run the utility in the unattended mode. In this mode, the utility reads connection settings from an answer file and does not require user input. The unattended mode is available for Enterprise Manager installed on Microsoft Windows and Linux. For details, see Connecting to Another Database in Unattended Mode.

Connecting to Another Database Using Wizard

The Configuration Database Connection Settings wizard is available only for Enterprise Manager installed on Microsoft Windows. To connect Enterprise Manager installed on Linux to another configuration database, use the unattended mode. For details, see Connecting to Another Database in Unattended Mode.

You can launch the Configuration Database Connection Settings utility from the **Start** menu by clicking **Configuration Database Connection Settings**.

Alternatively, you can run the `Veeam.Backup.DBConfig.exe` file. By default, the path is the following: `%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig`.

To run the utility, you must have administrative rights on the local machine, as long as the utility makes changes to the registry. If prompted at the launch, choose **Run as administrator**.

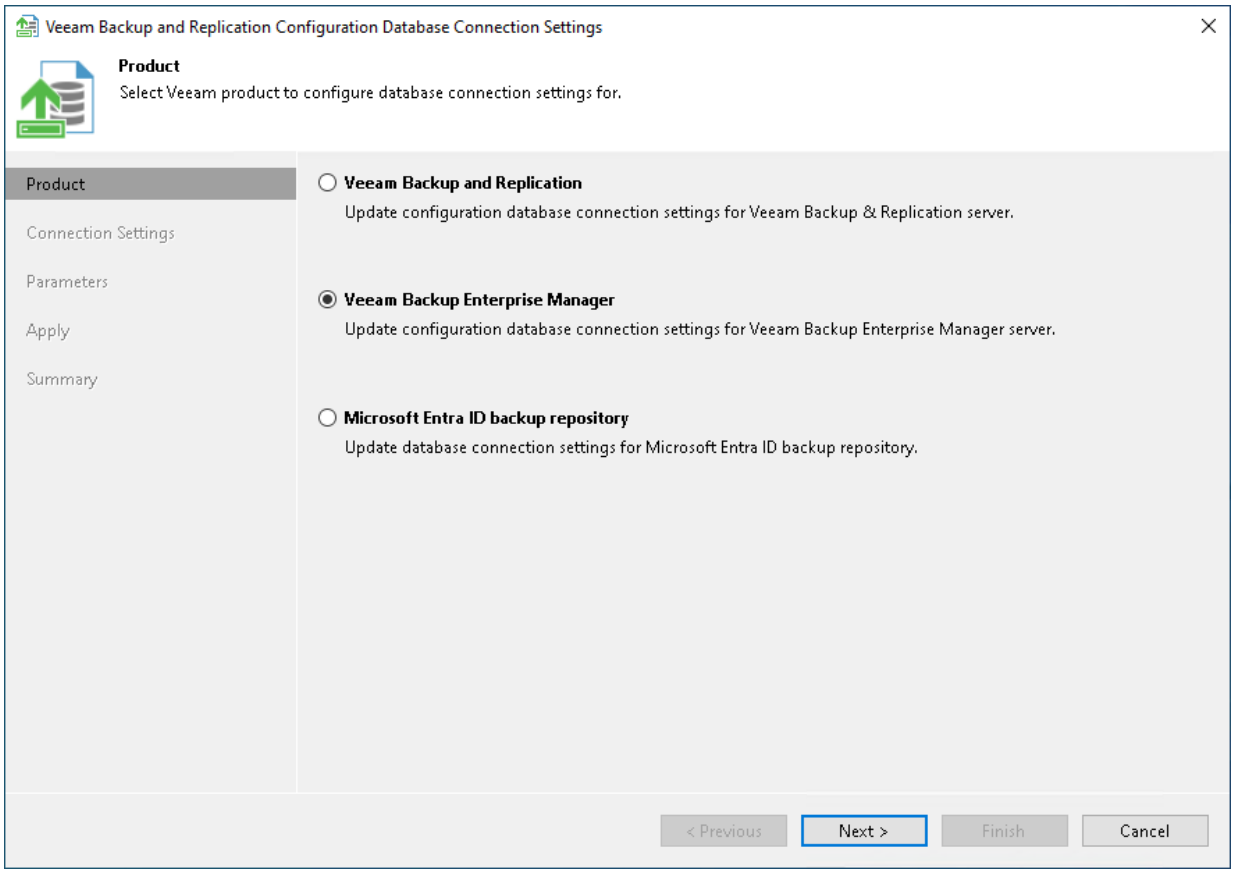
To manage connection settings for the Enterprise Manager configuration database, launch the utility and complete the wizard:

1. Select a product.
2. Specify database connection settings.
3. Review database issues, if the utility detects any.
4. Review parameters.
5. Apply connection settings.
6. Finish working with the wizard.

Step 1. Select Product

The **Product** step of the wizard is displayed if you have both a Veeam Backup Enterprise Manager server and backup server installed on the local machine. In this case, select a product whose configuration database settings you want to change.

If a backup server, Microsoft Entra ID backup repository or Enterprise Manager server is not installed on the machine, the **Product** step of the wizard is skipped.



Step 2. Specify Connection Settings

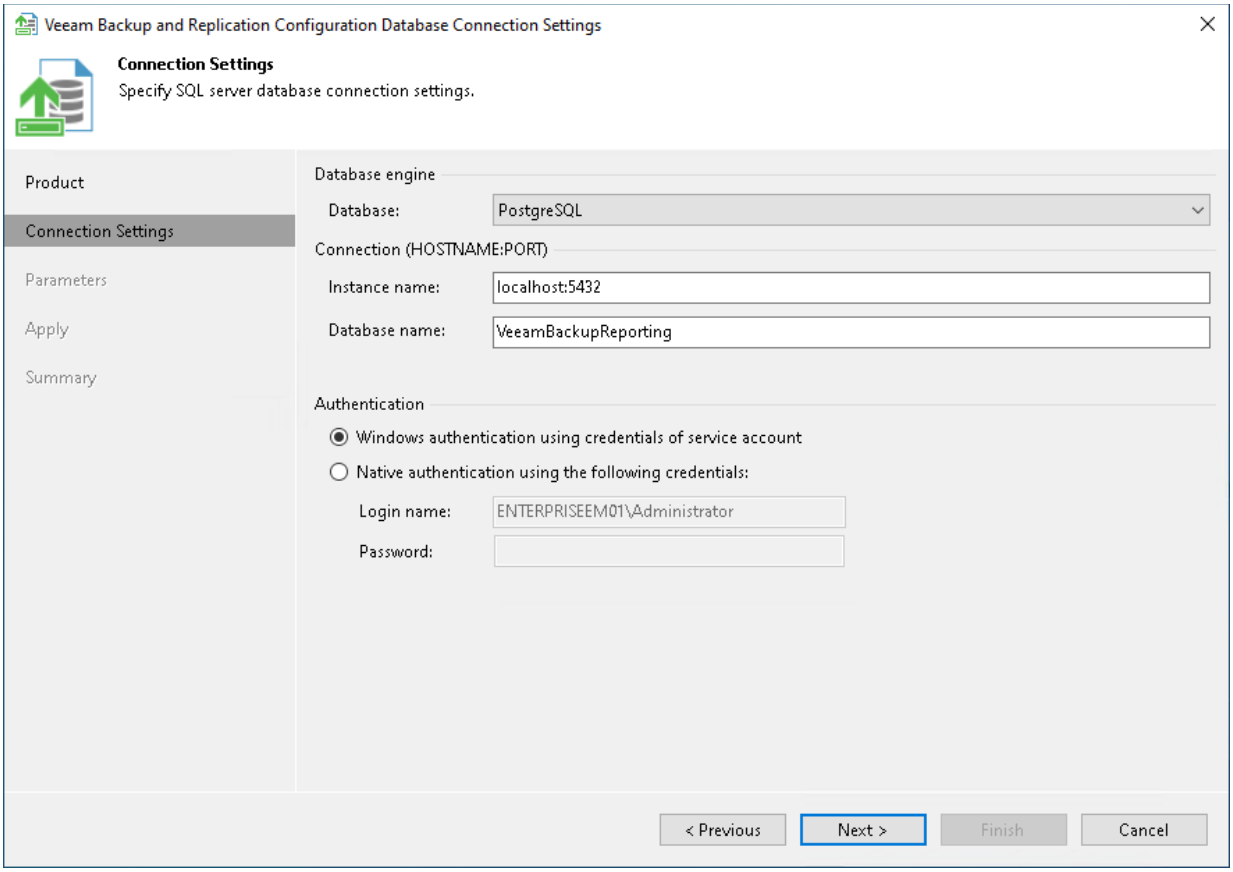
At the **Connection Settings** step of the wizard, provide the connection settings for the configuration database.

1. Select one of the following database engines:
   - PostgreSQL
   - Microsoft SQL Server
2. Specify database settings:
   - [For PostgreSQL] Specify the instance name in the *HOSTNAME:PORT* format. In the **Database name** field, specify a name for the Veeam Backup Enterprise Manager configuration database.
   - [For Microsoft SQL Server] Specify the Microsoft SQL Server instance and database name to which you want the Veeam Backup & Replication installation to connect. Both local and remote Microsoft SQL Server instances are supported. Microsoft SQL Server instances available on the network are shown in the **Server name** list. If necessary, click **Refresh** to get the latest information.

     If a database with the specified name does not exist on the selected Microsoft SQL Server instance, it will be created anew.
3. Select an authentication method that will be used for database connection:
   - If you plan to use the Microsoft Windows authentication, consider that the current service account will be used (that is, the account under which the Veeam Backup Enterprise Manager Service is running).
   - If you plan to use native database server authentication, provide a login name and password. To view the entered password, click and hold the eye icon on the right of the **Password** field.

   [For Microsoft SQL Server] When you migrate the configuration database to another server, you must use the Microsoft SQL Server credentials that have CREATE ANY DATABASE permission on the target Microsoft SQL Server. For details, see Microsoft Docs. After database creation, this account automatically gets a *db_owner* role and can perform all operations with the database. If the current account does not have this permission, a Database Administrator may create an empty database in advance and grant the *db_owner* role to the account that will be used for migration of the configuration database.

4. Click **Next**.



5. Before proceeding, the utility validates the specified settings to make sure that the specified user account has enough privileges to access the database.

   To ensure that the account (as well as the account under which the Veeam Backup Enterprise Manager Service is running) have sufficient privileges for database access, you can contact your database administrator. Refer to the list of required permissions for detailed information.

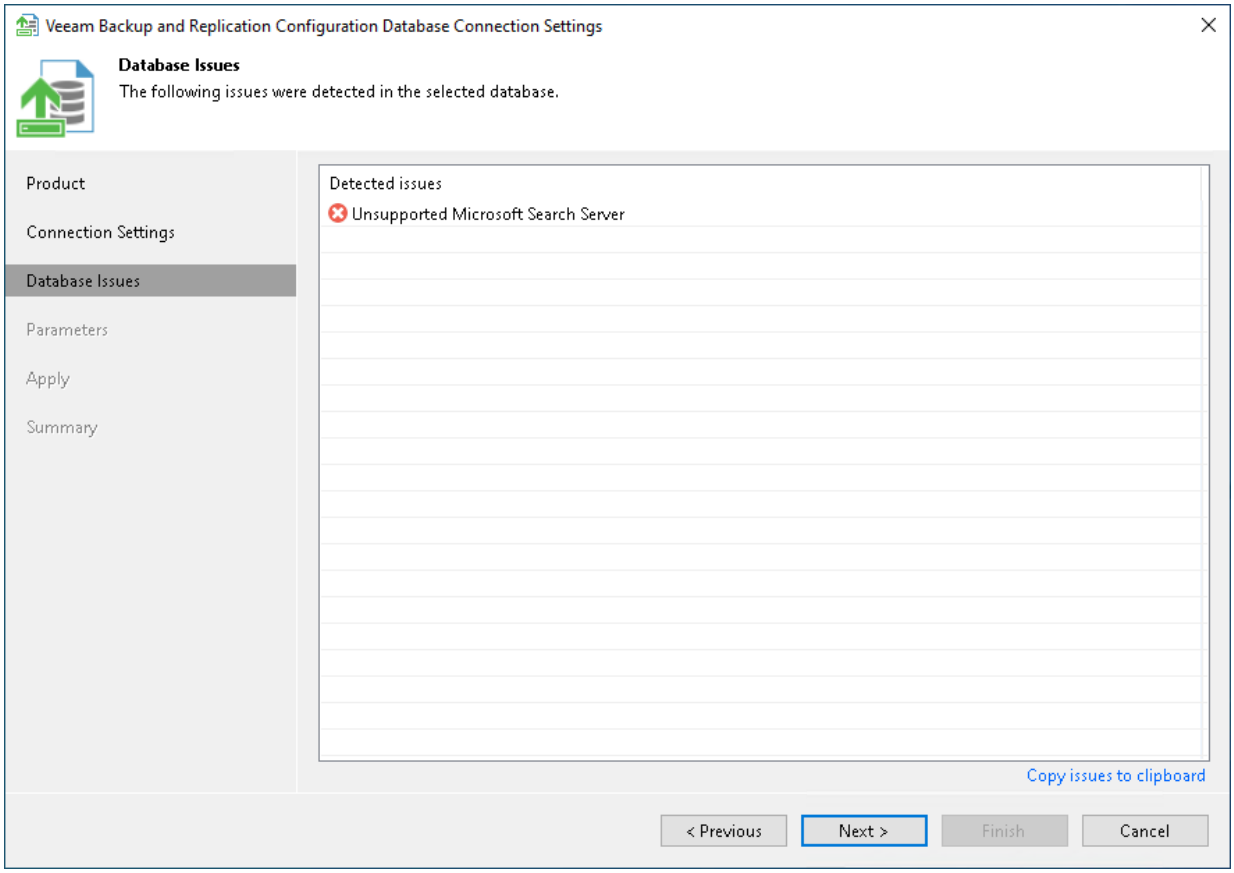
Step 3. Review Database Issues

At the **Database Issues** step of the wizard, review the issues that the utility detected in the selected database. The wizard displays this step only if the utility detects issues.

The issues in the list have one of the following severities:

- **Warning**. The issue does not prevent you from proceeding. Click **Next** to proceed to the next step.
- **Error**. The issue prevents you from proceeding. When you click **Next**, the utility displays a message that the database contains critical errors. You can proceed only after you resolve the reported issues.

To copy the list of issues, click **Copy issues to clipboard**.



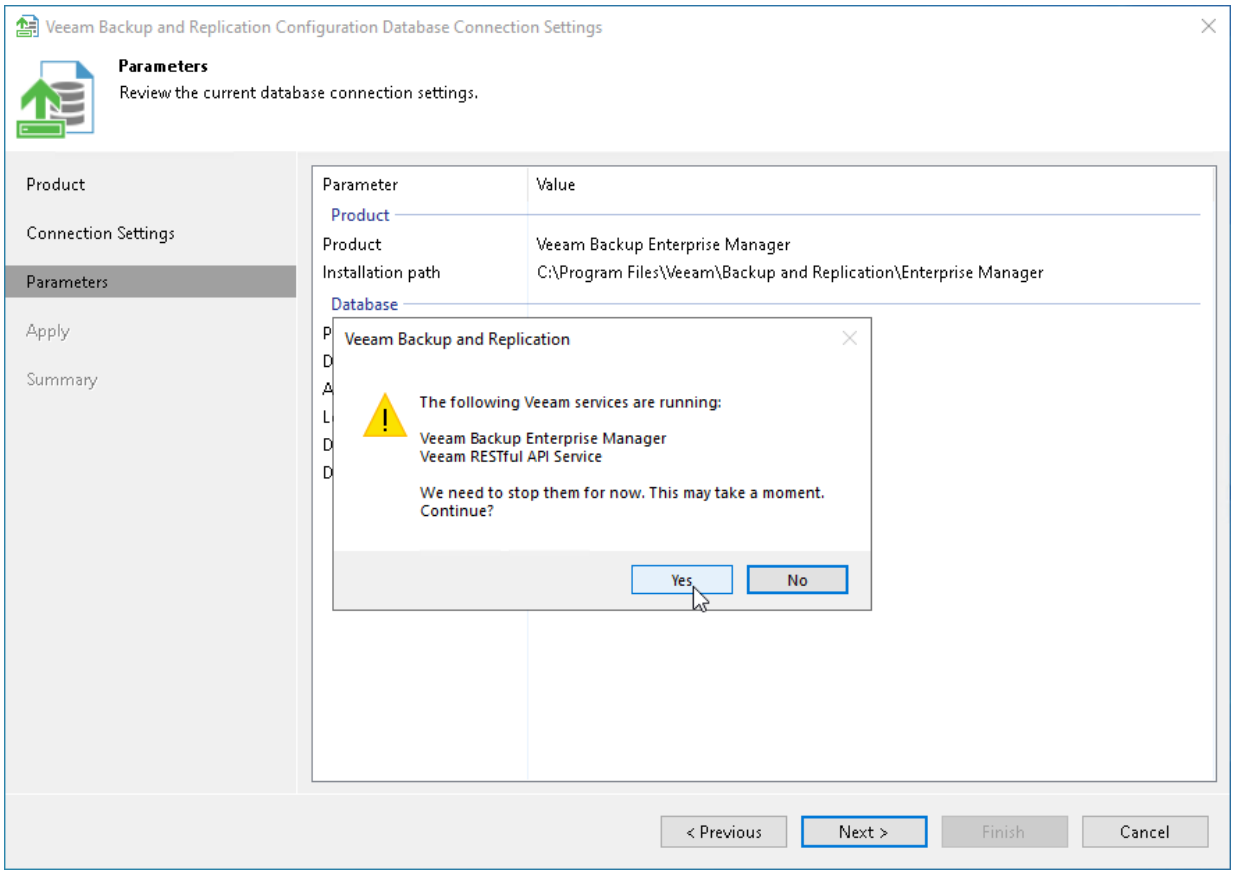
Step 4. Review Parameters

At the **Parameters** step of the wizard, review the database connection settings. The table shows the following parameters:

- **Product** and **Installation path**.
- The database server, **Database**, **Authentication** and **Login**.
- **Database upgrade required**.
- **Database is locked**.

After you click **Next**, the utility may ask you to confirm the following actions. To proceed, click **Yes** in the displayed prompt:

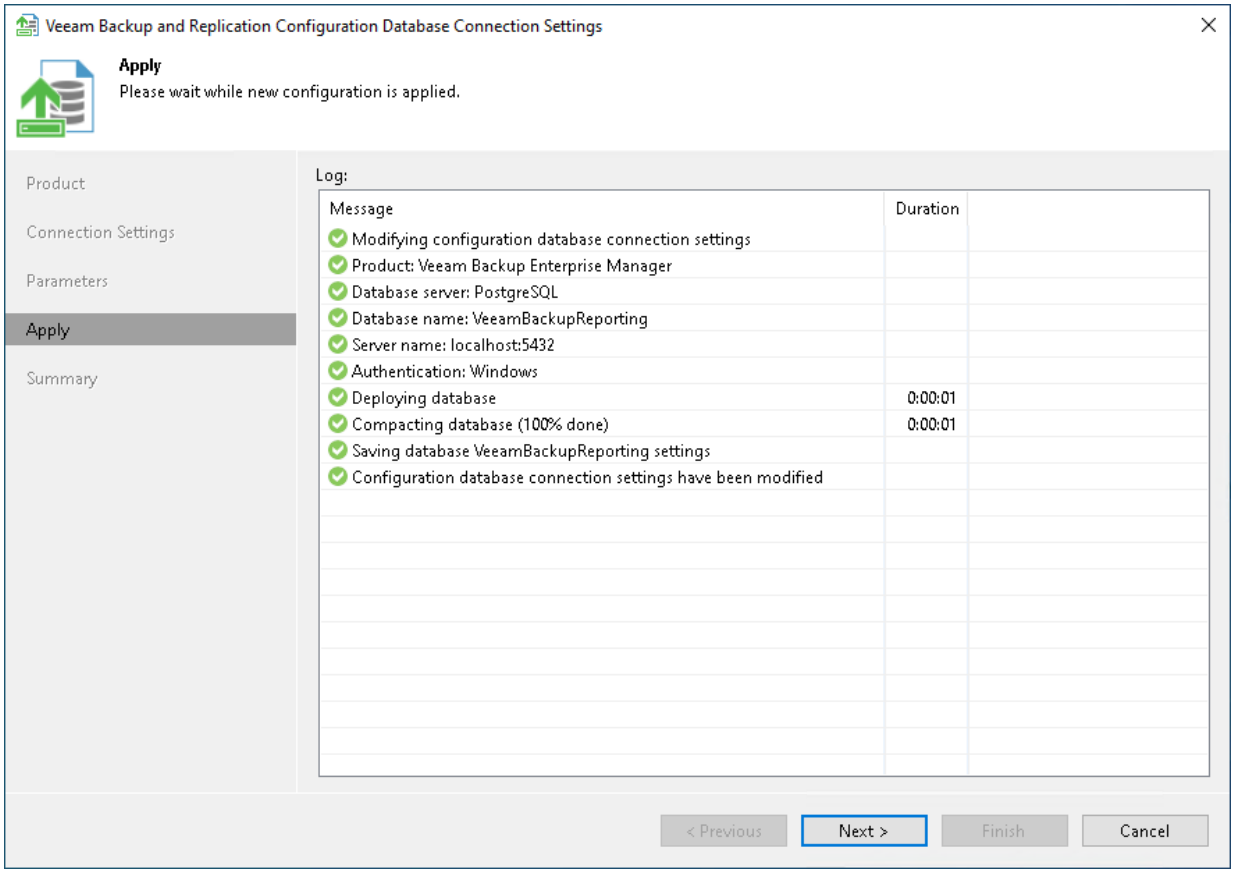
- Use a database that is used by another Enterprise Manager server. If you connect Enterprise Manager to this database, you will have to enter all saved passwords again.
- Upgrade the database schema. The utility displays this prompt if the schema version of the database is earlier than the schema version that the installed Enterprise Manager requires.
- Stop the running Veeam Backup Enterprise Manager services. The utility must stop the services to apply the new connection settings.



Step 5. Apply Connection Settings

At the **Apply** step of the wizard, the utility applies database connection settings. Wait for the operation to complete and click **Next** to proceed to the **Summary** step of the wizard.

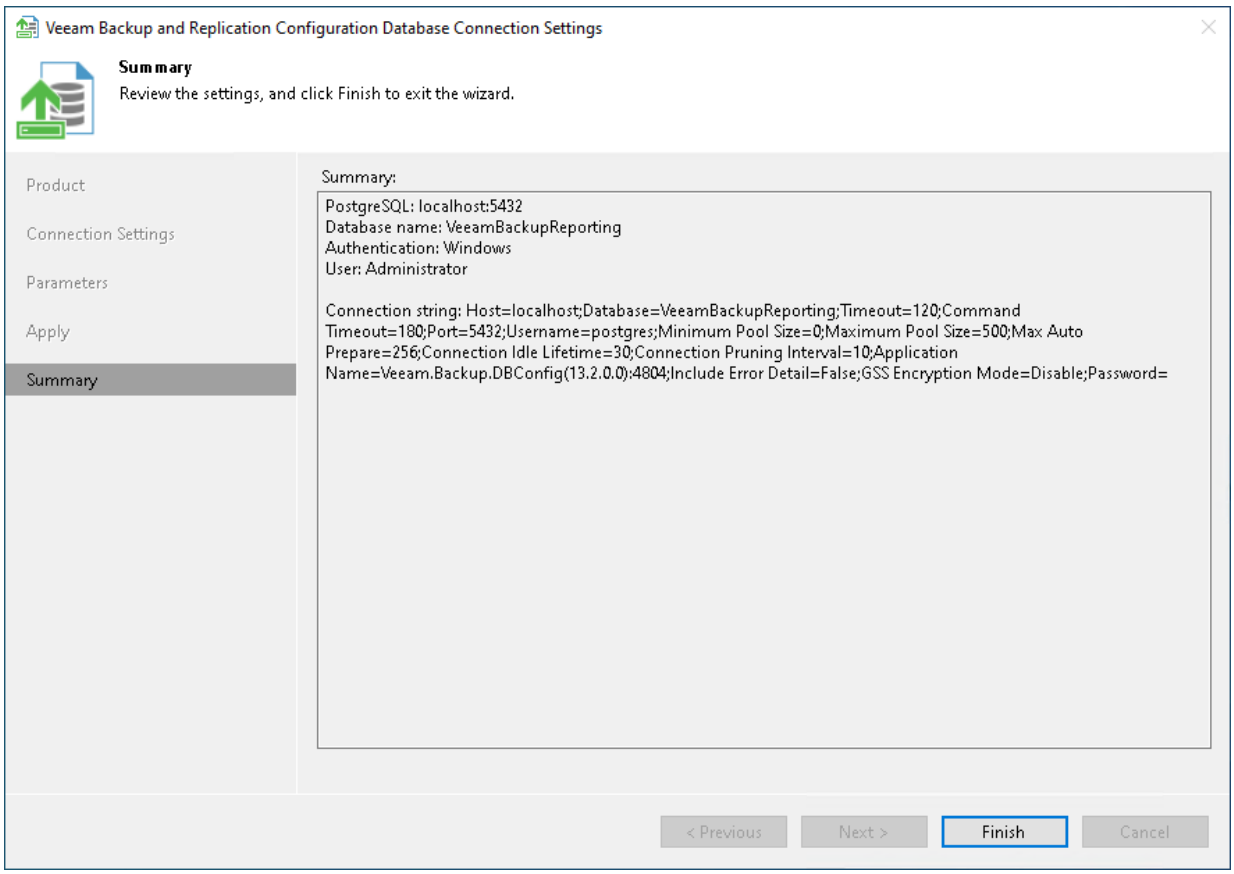
Previously stopped services will be started again at this moment.



Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, view the information about the changes in database connection settings and click **Finish**.

> **NOTE**
>
> If you are configuring Veeam Backup & Replication database settings and you want the Veeam backup management console to start automatically after you finish working with the wizard, select the **Start the product automatically** check box. The option is not available for Veeam Backup Enterprise Manager.



Connecting to Another Database in Unattended Mode

In the unattended mode, the Configuration Database Connection Settings utility reads database connection settings from an answer file and does not require user input. You can use the unattended mode for Enterprise Manager installed on Microsoft Windows and Linux.

The utility comes with Veeam Backup Enterprise Manager and is located on the Enterprise Manager server. The default path is the following:

- On a Microsoft Windows-based machine:

```
%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig\Veeam.Backup.DBConfig.Unattended.exe
```

- On a Linux-based machine:

```
/opt/veeam/dbconfig/Veeam.Backup.DBConfig.Unattended.dll
```

Before You Begin

Before you connect Enterprise Manager to another configuration database in the unattended mode, consider the following:

- On a Microsoft Windows-based machine, you must have administrative rights on the local machine. Run the command-line shell as administrator.
- On a Linux-based machine, you must have root access. To request root access, use Veeam Host Management. For details, see Configuring Remote Access Settings.
- If Enterprise Manager is installed on the backup server, run the utility from the `%PROGRAMFILES%\Veeam\Backup and Replication\Backup` folder.
- If the database requires a schema upgrade or all saved passwords must be entered again, you must allow these operations in the answer file. Otherwise, the utility stops with an error. For details, see the `ACCEPT_DATABASE_SCHEMA_UPGRADE` and `ACCEPT_STORED_PASSWORDS_LOSS` parameters.

To connect Enterprise Manager to another configuration database in the unattended mode, do the following:

1. Generate an answer file.
2. Edit the answer file.
3. Run the utility.

Step 1. Generate Answer File

Run the utility with the `/generate` parameter. In the parameter, specify the path where the utility must save the answer file:

- On a Microsoft Windows-based machine:

```
"%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig\Veeam.Backup.DBConfig.Unattended.exe" /generate:C:\answerfile.xml
```

- On a Linux-based machine:

```
dotnet /opt/veeam/dbconfig/Veeam.Backup.DBConfig.Unattended.dll /generate:/root/answerfile.xml
```

The utility saves a template of the answer file to the specified path.

Step 2. Edit Answer File

Open the answer file and do the following:

1. In the root element, set the `product` attribute to `em`. The utility always generates the answer file with the `vbr` value.

```
<unattendedDatabaseConfiguration product="em">
```

2. Specify the values of the parameters that you want to change. Always specify the `SQLSERVER_DATABASE` parameter. If you do not specify it, the utility uses the `VeeamBackup` database name, not the name of the Enterprise Manager configuration database.
3. Remove the optional parameters that you do not use.

> **NOTE**
>
> If the answer file contains the password for the database server account, store the file in a safe location.

Answer File Parameters

The answer file contains the following parameters:

Parameter	Description	Required
product	Specifies the product whose configuration database connection settings you want to change. This is an attribute of the root element. Set the attribute to em.	Yes

Parameter	Description	Required
SQLSERVER_ENGINE	Specifies the database engine. Supported values: postgresql or mssql. If you do not specify the parameter, the current product configuration is used.	No
DATABASE_SERVER	Specifies the database server on which the configuration database is deployed. Supported values: SERVER\INSTANCE for Microsoft SQL Server or HOSTNAME:PORT for PostgreSQL. If you do not specify the parameter, the current product configuration is used.	No
SQLSERVER_DATABASE	Specifies the name of the configuration database. If a database with the specified name does not exist, the utility creates it. If you do not specify the parameter, VeeamBackup is used. Make sure that you specify this parameter, for example, VeeamBackupReporting.	No
SQLSERVER_AUTHENTICATION	Specifies the authentication method. Supported values: 0 for Microsoft Windows authentication or 1 for native database server authentication. If you do not specify the parameter, the current product configuration is used.	No
SQLSERVER_USERNAME	Specifies the login name of the database server account. Required if SQLSERVER_AUTHENTICATION is set to 1. If you do not specify the parameter, the current product configuration is used.	No
SQLSERVER_PASSWORD	Specifies the password of the database server account. Required if SQLSERVER_USERNAME is specified. If you do not specify the parameter, the current product configuration is used.	No
RETRY_COUNT	Specifies the number of times the utility retries to start or stop services if the operation fails. If you do not specify the parameter, 3 is used.	No
STOP_PROCESSES	Specifies whether the utility stops the running product processes. Supported values: 1 for Yes or 0 for No. If you do not specify the parameter, 1 is used.	No

Parameter	Description	Required
ACCEPT_STORED_PASSWORDS_LOSS	Specifies whether the utility proceeds if all saved passwords must be entered again after you connect to the database. Supported values: 1 for Yes or 0 for No. If you do not specify the parameter, 0 is used. If the value is 0 and the passwords must be entered again, the utility stops with an error.	No
ACCEPT_DATABASE_SCHEMA_UPGRADE	Specifies whether the utility upgrades the database schema if the schema version of the database is earlier than the schema version that the installed Enterprise Manager requires. Supported values: 1 for Yes or 0 for No. If you do not specify the parameter, 0 is used. If the value is 0 and the database schema requires an upgrade, the utility stops with an error.	No

Step 3. Run Utility

Run the utility with the `/file` parameter. In the parameter, specify the path to the answer file:

- On a Microsoft Windows-based machine:

```
"%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig\Veeam.Backup.DBConfig.Unattended.exe" /file:C:\answerfile.xml
```

- On a Linux-based machine:

```
dotnet /opt/veeam/dbconfig/Veeam.Backup.DBConfig.Unattended.dll /file:/root/answerfile.xml
```

The utility analyzes the database for issues, validates the new connection settings, stops the running Enterprise Manager processes, saves the connection settings and starts the Enterprise Manager services. You do not need to start the services manually.

Specifying Parameters at Runtime

You can specify answer file parameters when you run the utility in the following ways:

- Use the `/property` parameter. Specify the parameter once for each answer file parameter. For example: `/property:SQLSERVER_DATABASE=VeeamBackupReporting`.
- Use an environment variable named `VEEAM_<parameter name>`. For example: `VEEAM_SQLSERVER_DATABASE`.

If you specify the same parameter in more than one place, the utility uses the value in the following order:

1. The `/property` parameter.
2. A non-empty value in the answer file.

3. The environment variable.

If you do not specify a parameter anywhere, the utility uses the default value of the parameter. If the parameter has no default value, the utility returns an error.

The utility does not write passwords to the log.

Host Management

If you use Enterprise Manager on Linux, you can manage host configurations using the Veeam Host Management console. The console allows administrators to perform configuration and maintenance tasks, including managing network settings, server time, host users and roles, backup infrastructure, OS and Enterprise Manager updates, maintenance operations, and security settings.

About Veeam Host Management

Veeam Host Management is the component used to configure Veeam Software Appliance. You can perform operations through the Veeam Host Management console that has a web UI and text-based UI (TUI). For more information, see Accessing Veeam Host Management Console.

The following table describes operations available in the Veeam Host Management console.

Operation	Host Management Web UI	Host Management TUI
Network		
Change the server name	+	+
Manage domain settings	+	–
Configure network interfaces	+	+
Configure multiple network connections	–	+
Configure HTTP/HTTPS proxies	–	+
Server Time		
Change the time zone	+	+
Configure time servers	+	+
Remote Access		
Disable the Veeam Host Management web UI	+	+
Enable the Veeam Host Management web UI	–	+
Enable and disable SSH access	+	+
Open the root shell	–	+
Users and Roles		

Operation	Host Management Web UI	Host Management TUI
Add a Veeam Host Management user	+	–
Edit a Veeam Host Management user	+	–
Change the Host Administrator password	+	+
Reset a Veeam Host Management user password	+	–
Unlock a Veeam Host Management user	+	–
Enable and disable multi-factor authentication	+	–
Reset multi-factor authentication	+	–
Reset password recovery token for Security Officer	+	–
Backup Infrastructure		
Enable remote data collection	+	–
Update		
Configure updates	+	–
Check for updates	+	–
Install updates	+	–
View update history	+	–
Maintenance		
Manage Veeam services	+	–
Restart Veeam Software Appliance	+	+

Operation	Host Management Web UI	Host Management TUI
View and export appliance events	+	–
Import and export Veeam configuration files	+	–
Export a Veeam component list	+	–
Install Veeam components manually	+	–
Download Veeam logs	+	–
View certificate thumbprints	+	+
Generate new Veeam Host Management web UI certificates	–	+
Security		
Approve and decline authorization requests	+	–
View authorization request events	+	–

Accessing Veeam Host Management Console

You can access the Veeam Host Management console using an account with Host Administrator or Security Officer permissions.

During the Veeam Software Appliance installation, the following user accounts are created:

- *veeamadmin* — a default user account with Host Administrator permissions.
- *veeamso* — a default user account with Security Officer permissions. The account can log in only to the Veeam Host Management web UI. This account is available only if you configured it in the **Initial Configuration** wizard. For details, see Configure Security Officer Account.

A Host Administrator can add additional user accounts to grant access to Veeam Host Management. For more information, see Managing Users and Roles.

> **NOTE**
>
> User accounts are locked after three failed login attempts. For more information on how to unlock them, see Unlocking Users.

Logging in to Web UI

To log in to the Veeam Host Management web UI, do the following:

1. In your web browser, navigate to the Veeam Host Management URL. The URL consists of an FQDN or IP address of the server where the appliance is installed, and the Veeam Host Management port. For example, `https://vbrsrv01.tech.local:10443`.

   > **NOTE**
   >
   > The Veeam Host Management web UI does not support the following browser versions:
   >
   > - Google Chrome — version 118 and earlier
   > - Microsoft Edge — version 118 and earlier
   > - Mozilla Firefox — version 116 and earlier

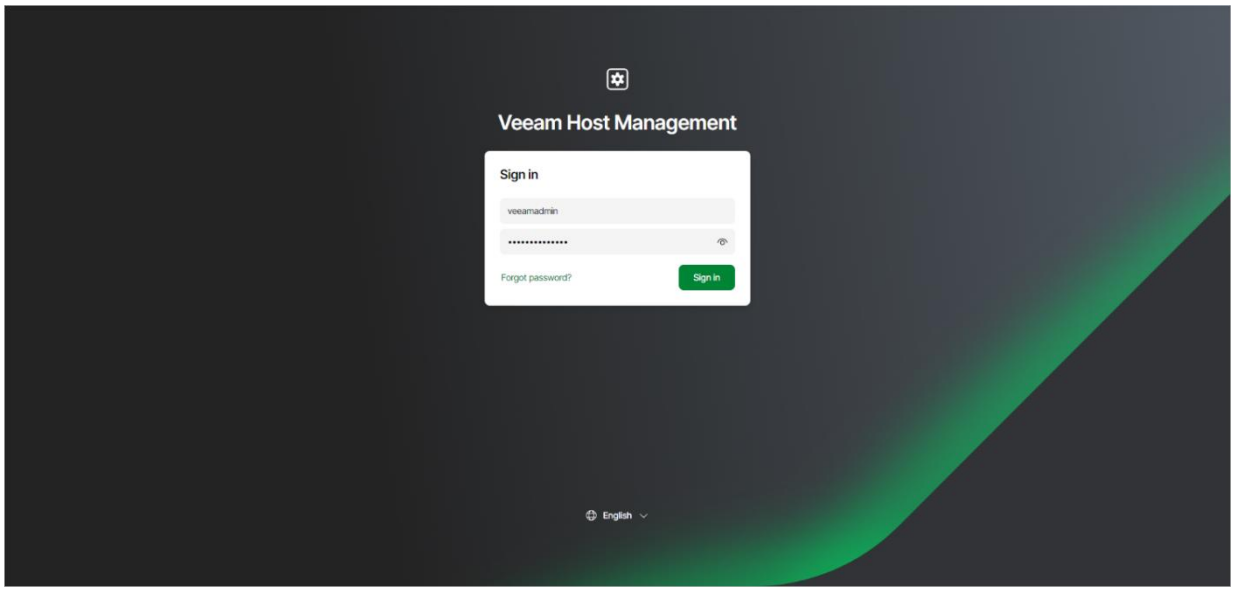
2. Select a language. This choice applies only to the current session and does not change your saved user settings.
3. Specify user credentials with Host Administrator or Security Officer permissions.

   > **TIP**
   >
   > If you have forgotten the password to your Host Administrator account, you can request a remote password reset by clicking **Forgot password?**
   >
   > This option is only available if the following conditions are met:
   >
   > - The appliance has a Security Officer account configured.
   > - Remote password resets are enabled in the **Password Policies** menu. For more information, see Configuring Password Policies.

4. Click **Sign in**.

5. If you enable multi-factor authentication (MFA) for the user, specify the confirmation code and click **OK**.

> **NOTE**
>
> If you skipped multi-factor authentication (MFA) configuration for *veeamadmin* during the appliance installation, you are prompted to set up MFA at first login to the Veeam Host Management console. Until you configure MFA, you cannot access Veeam Backup & Replication.



Logging in to TUI

To log in to the Veeam Host Management TUI, do the following:

1. Connect to the server where the appliance is installed through a physical console or a virtual remote console.

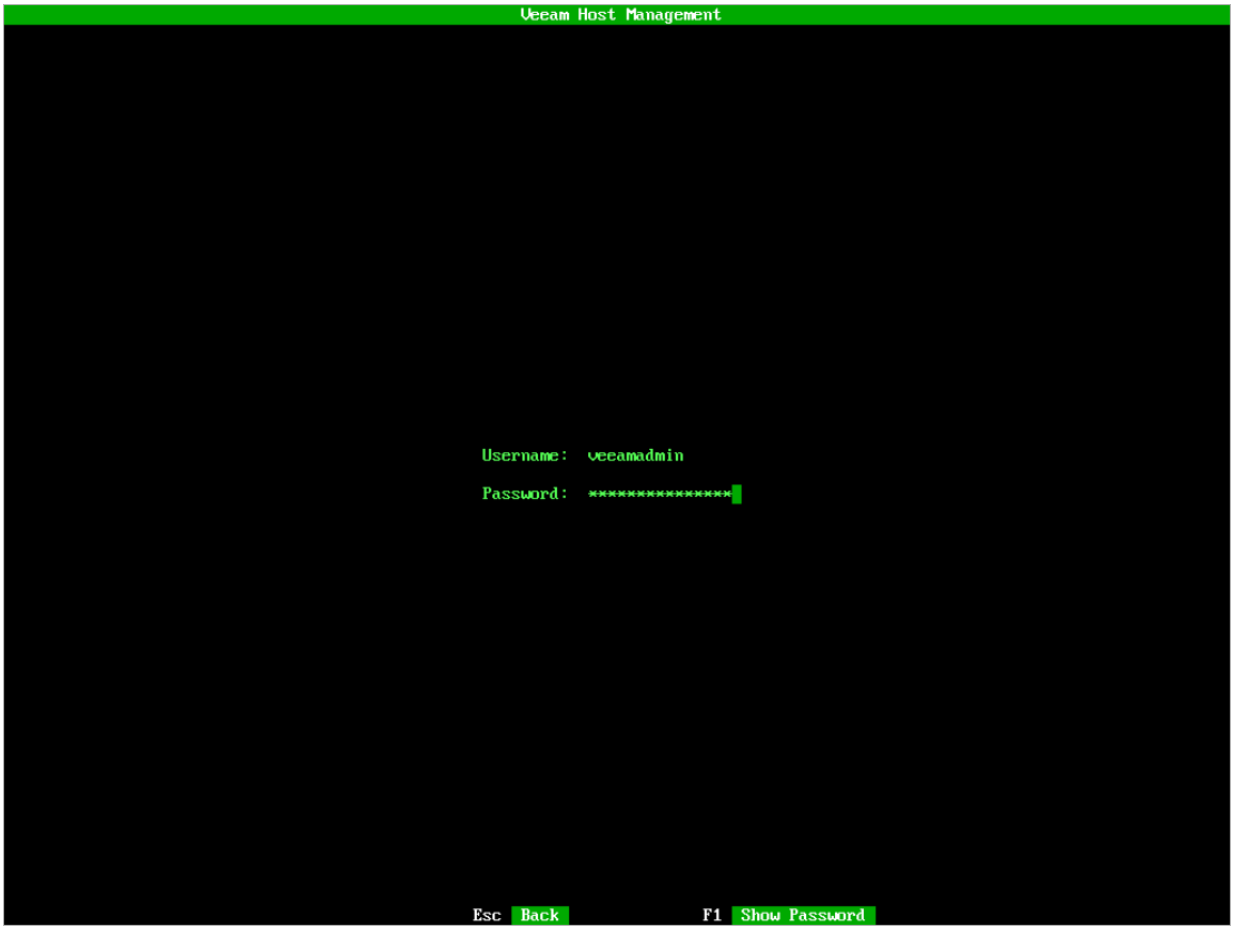
> **NOTE**
>
> You cannot log in to the Veeam Host Management TUI through SSH.

2. Specify user credentials with Host Administrator permissions.

> **TIP**
>
> To view the password, press [F1].

3. Press [Enter].
4. If you enabled multi-factor authentication (MFA) for the user, specify the confirmation code and press [OK].

> **NOTE**
>
> If you skipped multi-factor authentication (MFA) configuration for *veeamadmin* during the appliance installation, you are prompted to set up MFA at first login to the Veeam Host Management console. Until you configure MFA, you cannot access Veeam Backup & Replication.


Veeam Host Management
Username: veeamadmin
Password: **********
Esc Back
F1 Show Password

Configuring Veeam Host Management Localization Settings

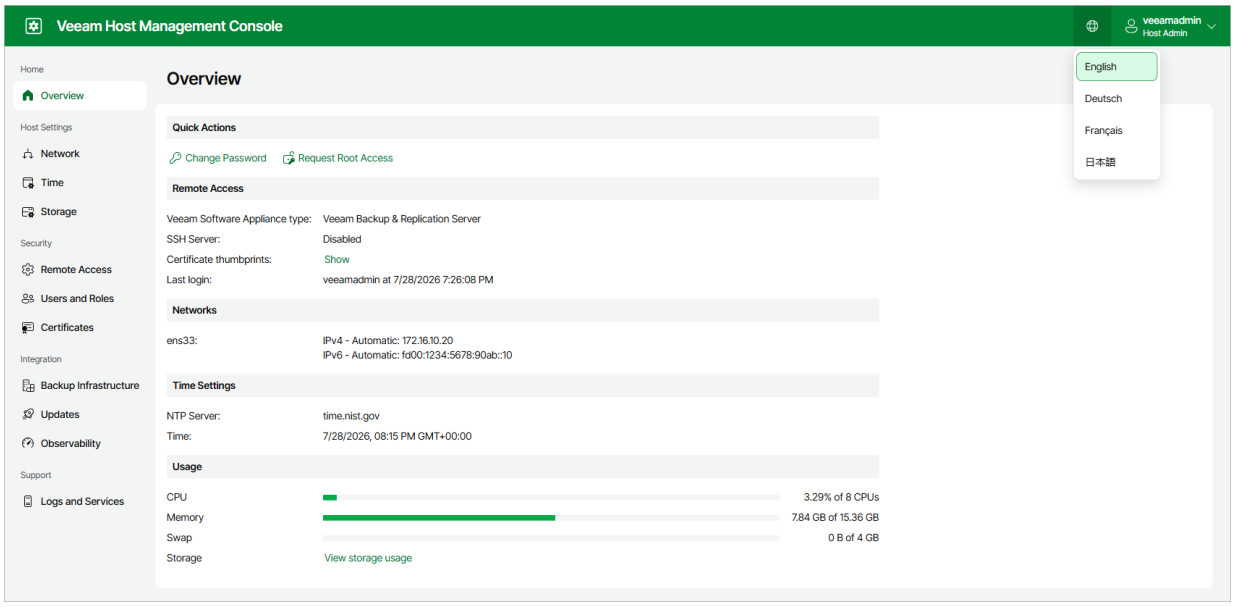
Users can perform the following operations to change the localization settings in the Veeam Host Management console:

- Change language settings in the web UI
- Change keyboard layout in the TUI

Changing Language Settings in Web UI

In the Veeam Host Management console web UI, you can change the interface language. The following languages are supported: English, German, French, and Japanese.

To change the language, click the globe icon in the top bar and select the language you want to use.



> **NOTE**
>
> The language is saved for each account individually.

Changing Keyboard Layout in TUI

In the Veeam Host Management TUI, you can change the keyboard layout. By default, the TUI uses the US English keyboard layout.

To change the keyboard layout, do the following:

1. On the login screen or main menu of the Veeam Host Management TUI, press [Ctrl+K].
2. Select the layout you want to use. The TUI lists layout codes alphabetically.
3. Press [Enter].

Configuring Network Settings

Users with Host Administrator permissions can perform the following operations within the network settings:

- Change the server name
- Manage domain settings
- Configure network interfaces
- Configure HTTPS proxies

Users with Security Officer permissions cannot configure network settings.

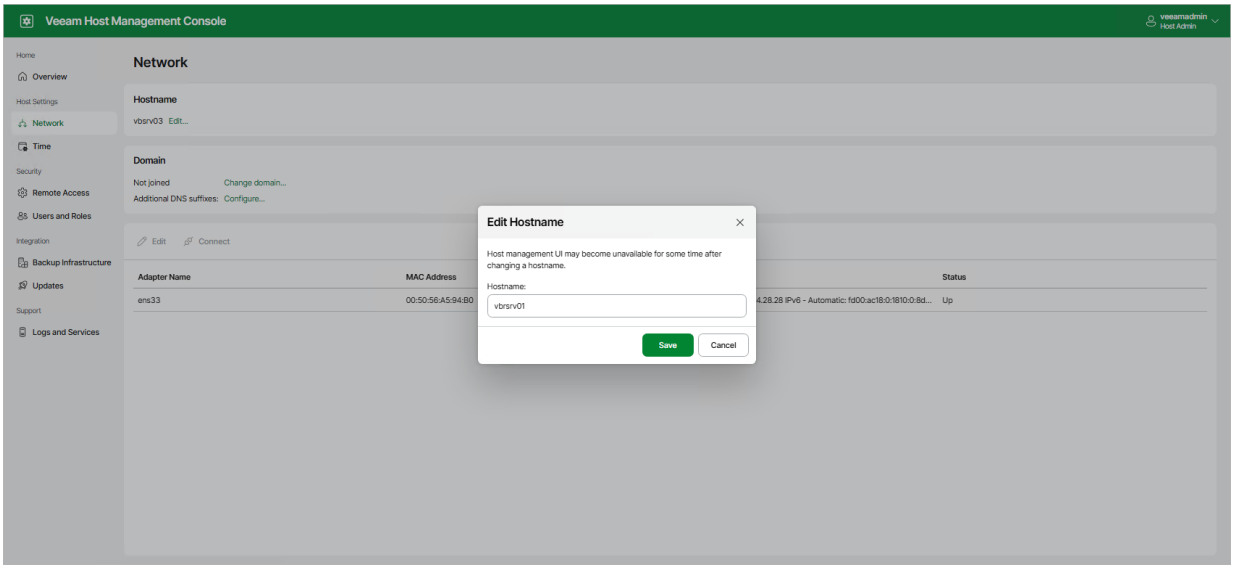
Changing Server Name

Before you change the server name, consider the following:

- If the server is a part of the domain, remove the server from the domain first. For more information on how to do it, see Managing Domain Settings.
- After you change the name, all services running on the server will be restarted.

If you use the Veeam Host Management web UI, perform the following steps:

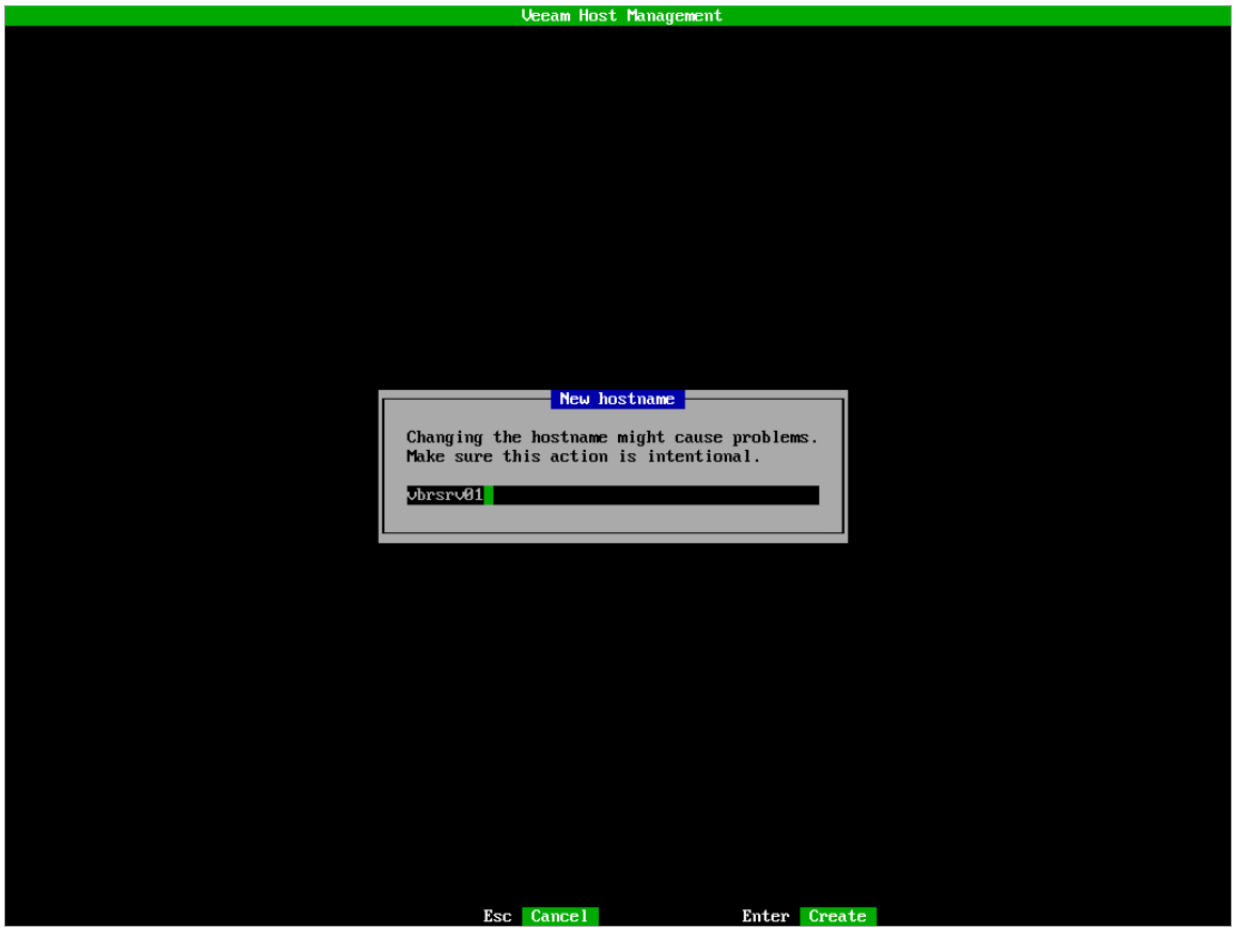
1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Network**.
3. In the **Hostname** section, click **Edit**.
4. Specify a new server name.
5. Click **OK**.



If you use the Veeam Host Management TUI, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Hostname**.

3. Specify a new server name and press [Enter].



Managing Domain Settings

In the Veeam Host Management web UI, you can change domain membership of the server. To do this, perform the following steps:

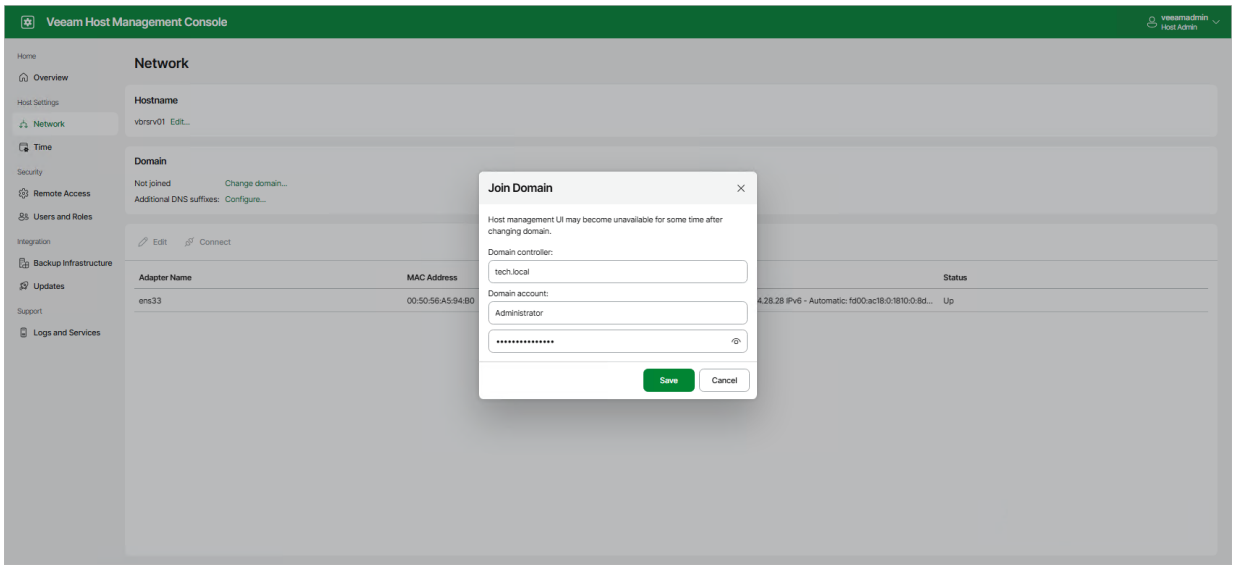
1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Network**.
3. In the **Domain** section, select one of the following options:
   - If the server is not a part of a domain, click **Change domain**. In the **Join Domain** window, specify the domain name and credentials with domain joining permissions. Then, click **Save**.

     > **NOTE**
     >
     > It is recommended to specify the domain name instead of the FQDN of a specific domain controller. This can mitigate domain joining issues if this domain controller is unavailable for some reason.

   - If the server is a part of a domain, click **Leave domain** and confirm the operation.

   After you change the domain membership, all services running on the server will be restarted.

To specify additional DNS suffixes, click **Configure** next to the setting name.



Configuring Network Interfaces

You can perform basic and advanced operations with network interfaces:

- Configure default network interface
- Manage network interfaces
- Configure multiple network connections — Virtual Local Area Networks (VLANs), bonds, tunnels, and other connection types

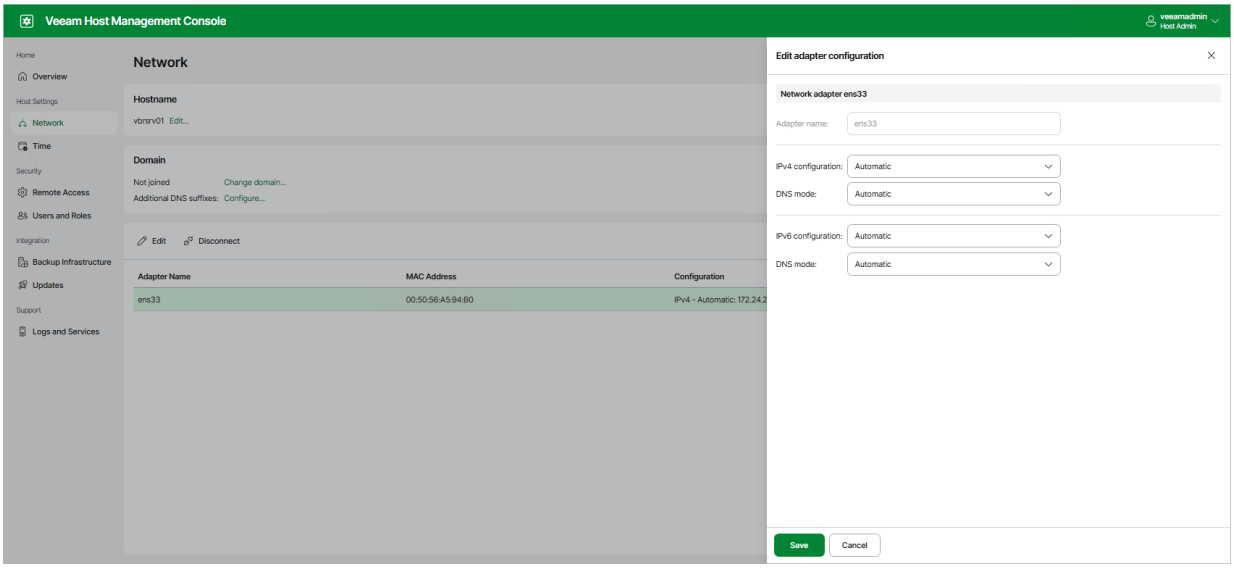
Configuring Default Network Interface

By default, Veeam Software Appliance uses one network interface that is configured automatically during the installation. You can change the default configuration in the Veeam Host Management web UI or TUI.

If you use the Veeam Host Management web UI, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Network**.
3. Select the network adapter and click **Edit**.
4. Configure required settings and click **Save**.

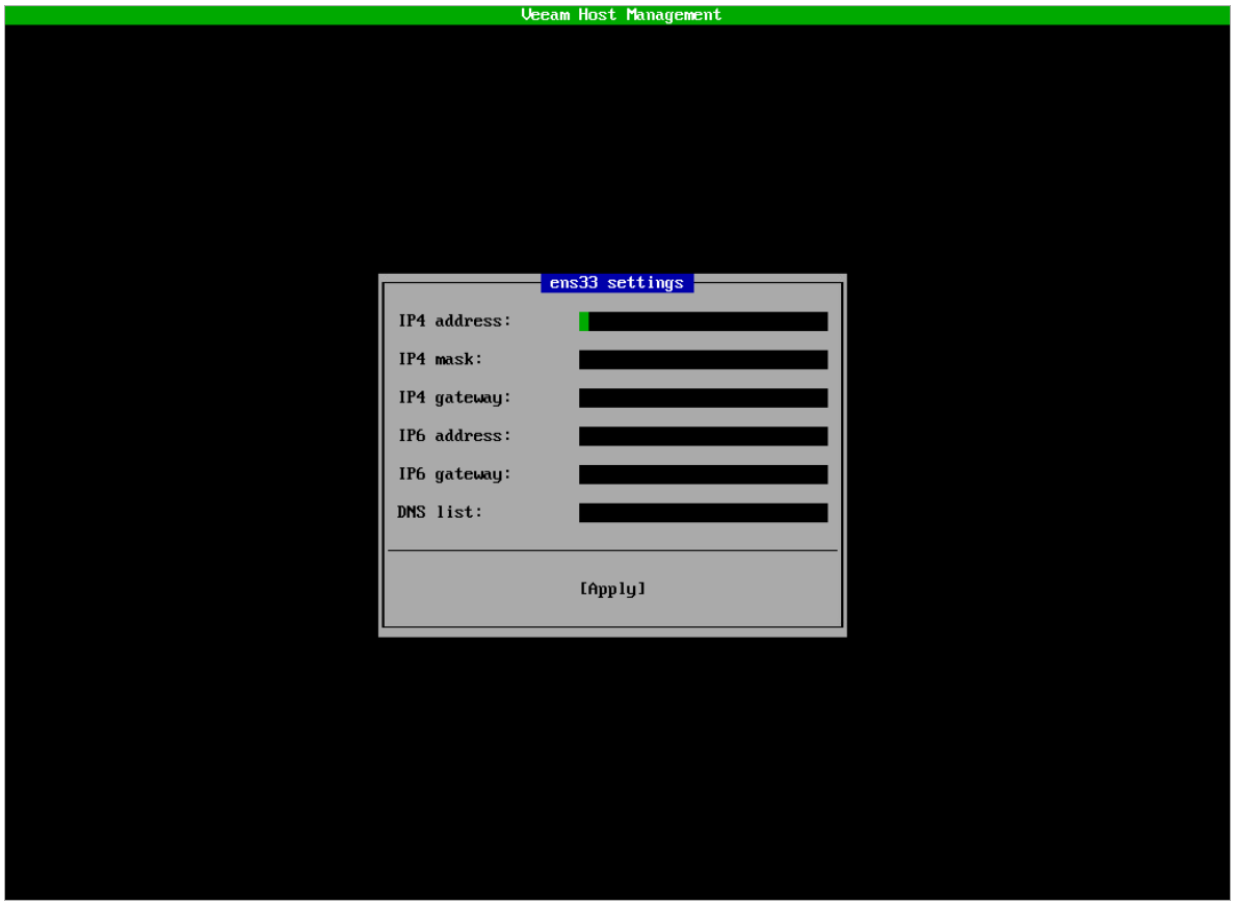
> **TIP**
>
> To specify multiple DNS servers, separate them by a comma.



If you use the Veeam Host Management TUI, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Network**.
3. Select the network adapter and press [Enter].
4. Select the **Manual** option.

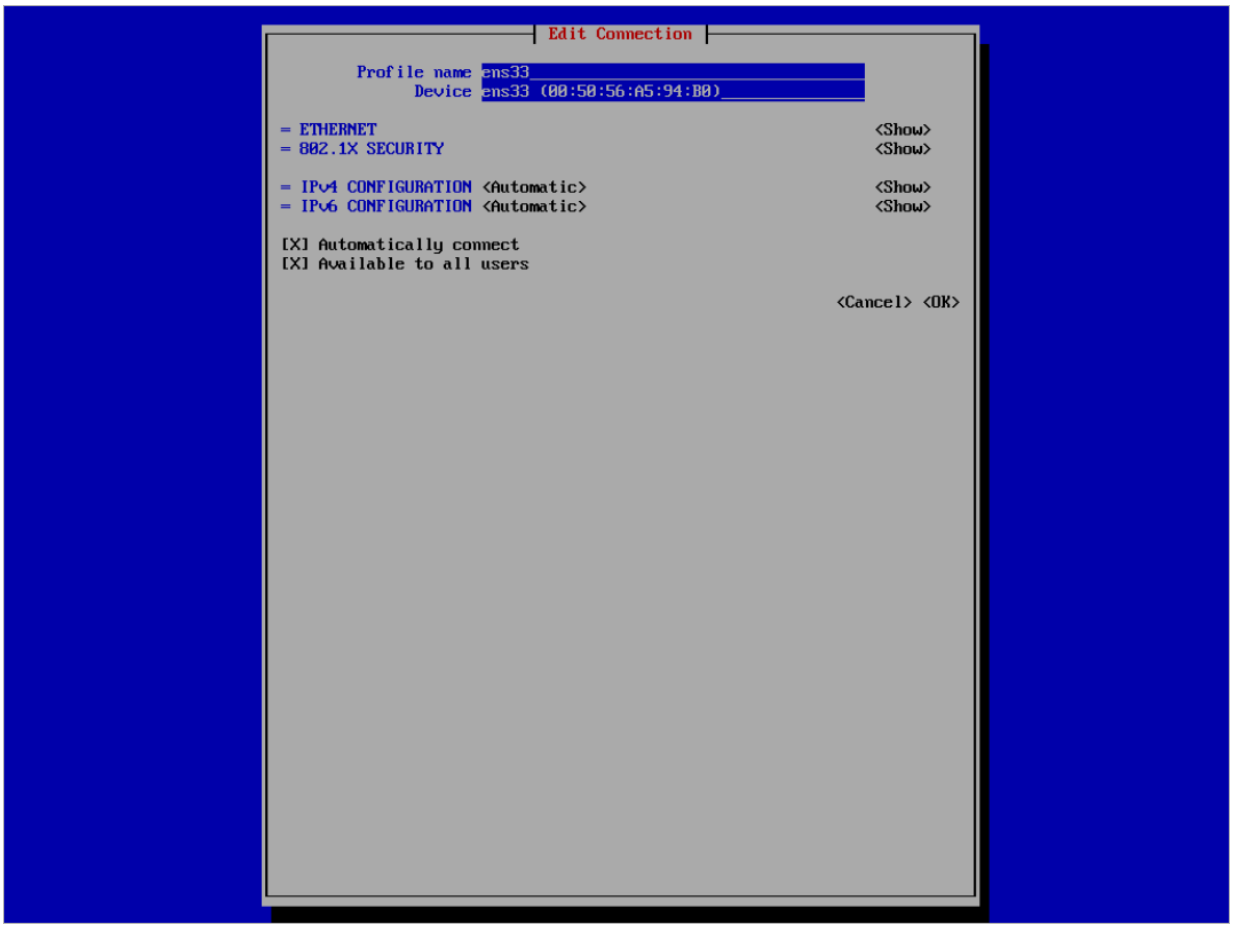
5. Configure required settings and press [Apply].



If you want to configure advance settings for the default network interface, do the following:

1. In the main menu, select **Host configuration** > **Advanced network**.
2. Select the network adapter and press [Edit].

3. Configure required settings and press [OK].



Managing Network Interfaces

You can do the following operations with the network interfaces:

- Disable network interface
- Enable network interface
- Restart network services

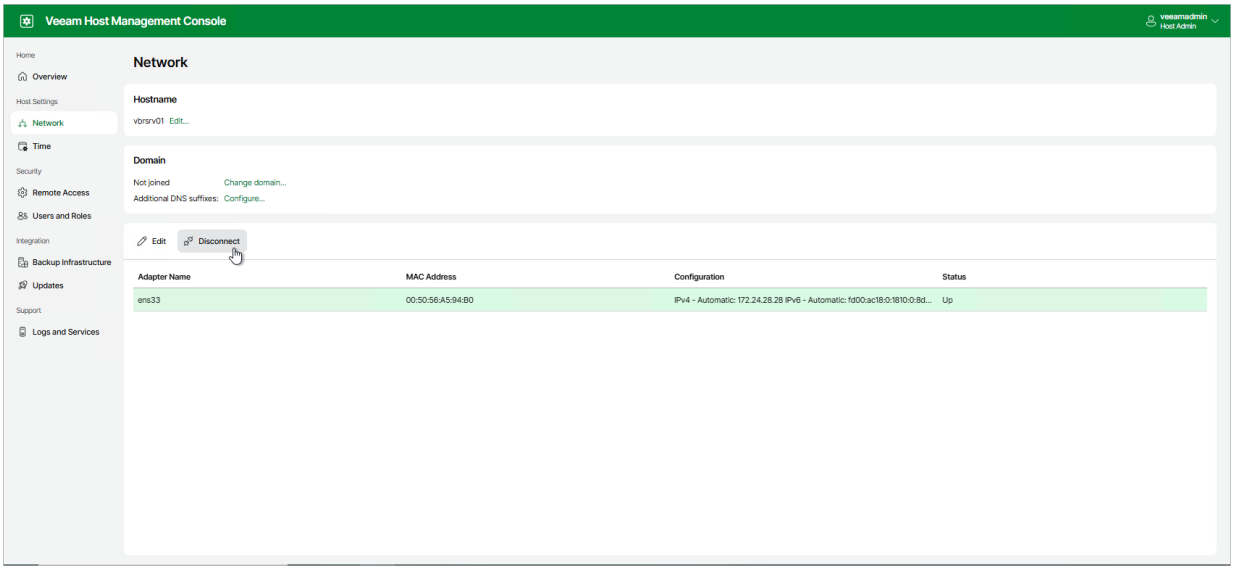
Disabling Network Interface

You can disable a network interface in the Veeam Host Management web UI and TUI.

If you use the Veeam Host Management web UI, perform the following steps:

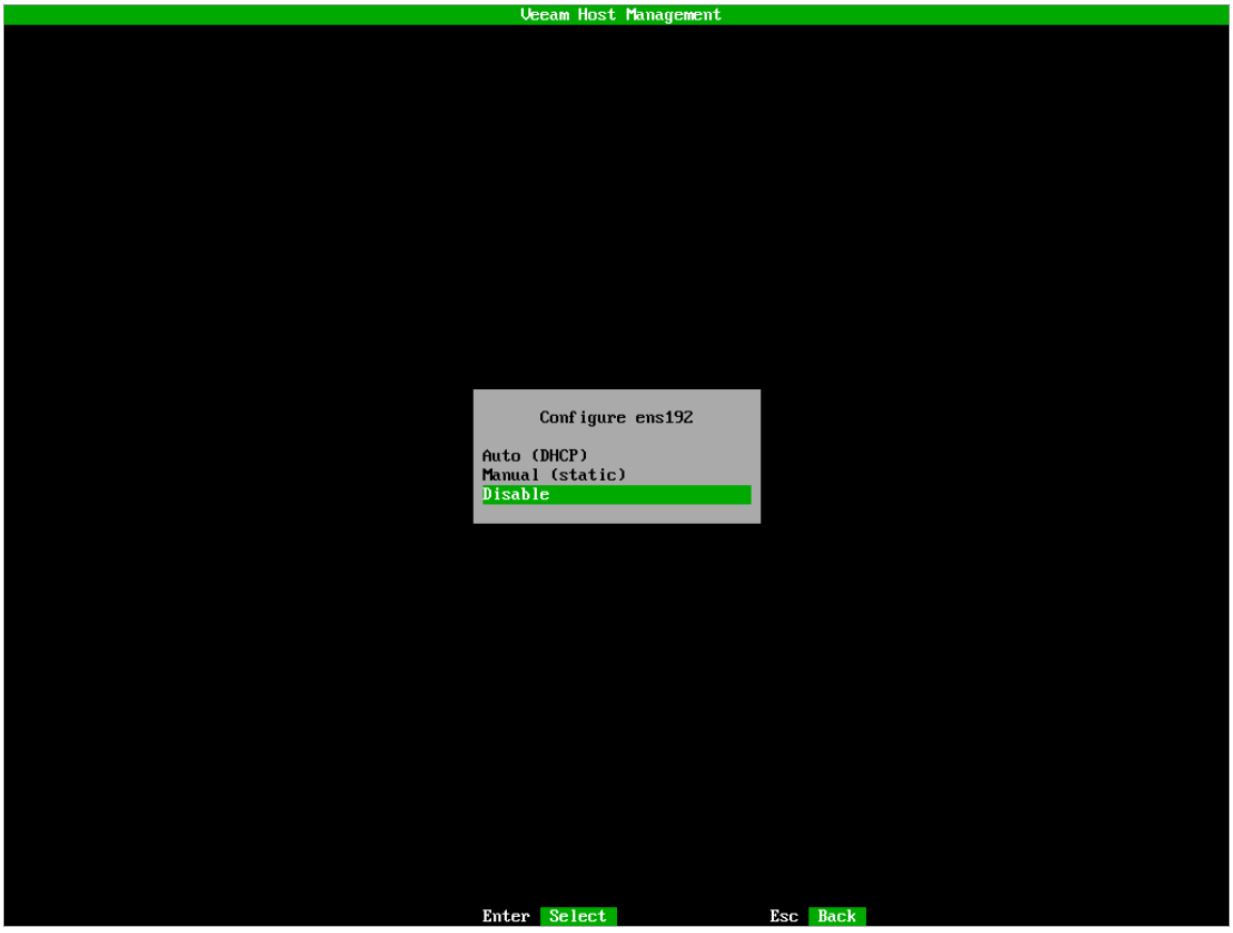
1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Network**.
3. Select the network interface and click **Disconnect**.

> **NOTE**
>
> If you disable the only network interface, the connection to the Veeam Host Management web UI will be lost. You can enable the interface again in the Veeam Host Management TUI.



If you use the Veeam Host Management TUI, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Network**.
3. Select the network interface and press [Enter].
4. Select **Disable** and press [Enter].



Enabling Network Interface

When you enable a network interface, consider the following:

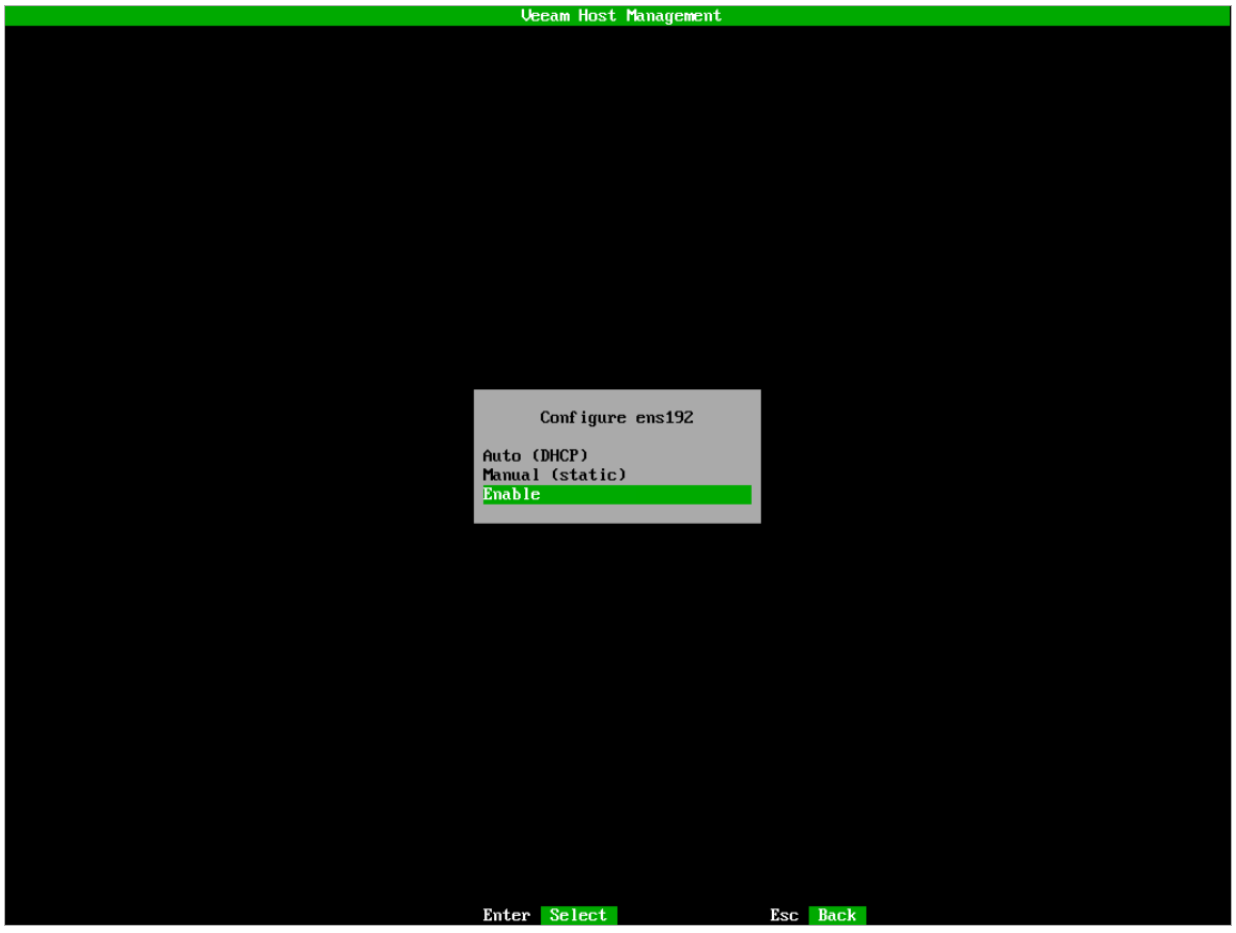
- If you use multiple network interfaces and want to enable one of them, you can do it in the Veeam Host Management web UI or TUI.
- If you disabled all network interfaces, you can enable them only in the Veeam Host Management TUI.

If you use the Veeam Host Management web UI, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Network**.
3. Select the network interface and click **Connect**.

If you use the Veeam Host Management TUI, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Network**.
3. Select the network interface and press [Enter].
4. Select **Enable** and press [Enter].



Restarting Network Services

To restart network services, perform the following steps in the Veeam Host Management TUI:

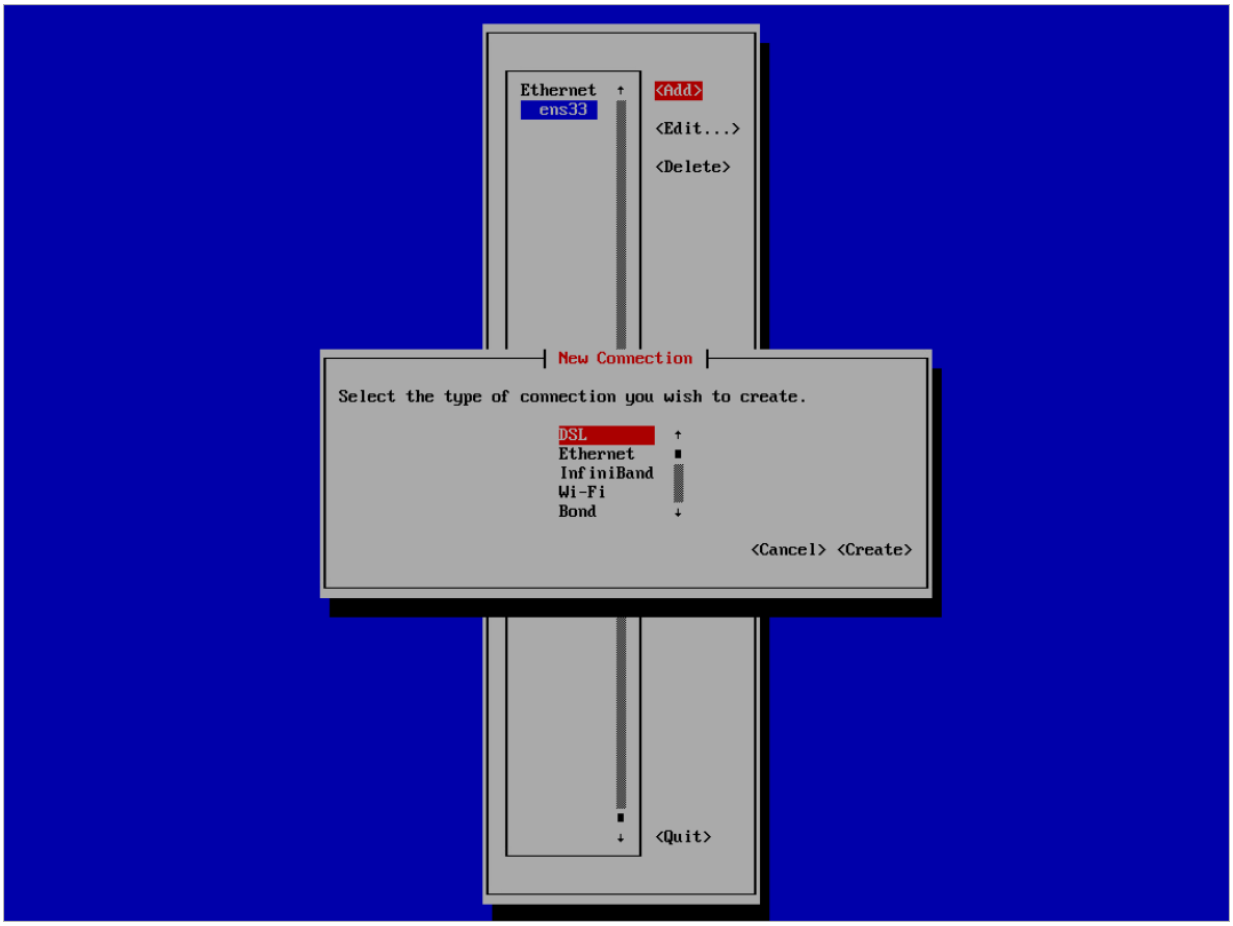
1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Advanced network** and press [F5].

Configuring Multiple Network Connections

In the Veeam Host Management TUI, you can use the `nmtui` tool to add multiple network connections including VLANs, bonds, tunnels, and so on. To do this, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator.
2. In the main menu, select **Host configuration** > **Advanced network**.
3. Press [Add].
4. Select the connection type and press [Create].
5. Configure specific settings for the selected connection type. For more information, see this Red Hat article.
6. Press [OK].

> **TIP**
>
> To combine a network bond with a VLAN, create the bond first. Then, configure VLAN tagging. For more information, see these Red Hat articles:
>
> - Configuring a network bond by using nmtui
> - Configuring VLAN tagging by using nmtui


Ethernet
ens33
<Add>
<Edit...>
<Delete>
New Connection
Select the type of connection you wish to create.
DSL
Ethernet
InfiniBand
Wi-Fi
Bond
<Cancel> <Create>
<Quit>

Configuring HTTPS Proxies

If the appliance does not have direct access to the internet, you can configure an HTTPS proxy in the Veeam Host Management TUI.

Enterprise Manager connects to added backup servers through the configured proxy. Make sure that each backup server added to Enterprise Manager is either accessible through the proxy or specified in the **Bypass** field. In the **Bypass** field, specify the same DNS name or IP address that you used to add the backup server to Enterprise Manager. For more information, see Adding Backup Servers.

To configure an HTTPS proxy, perform the following steps:

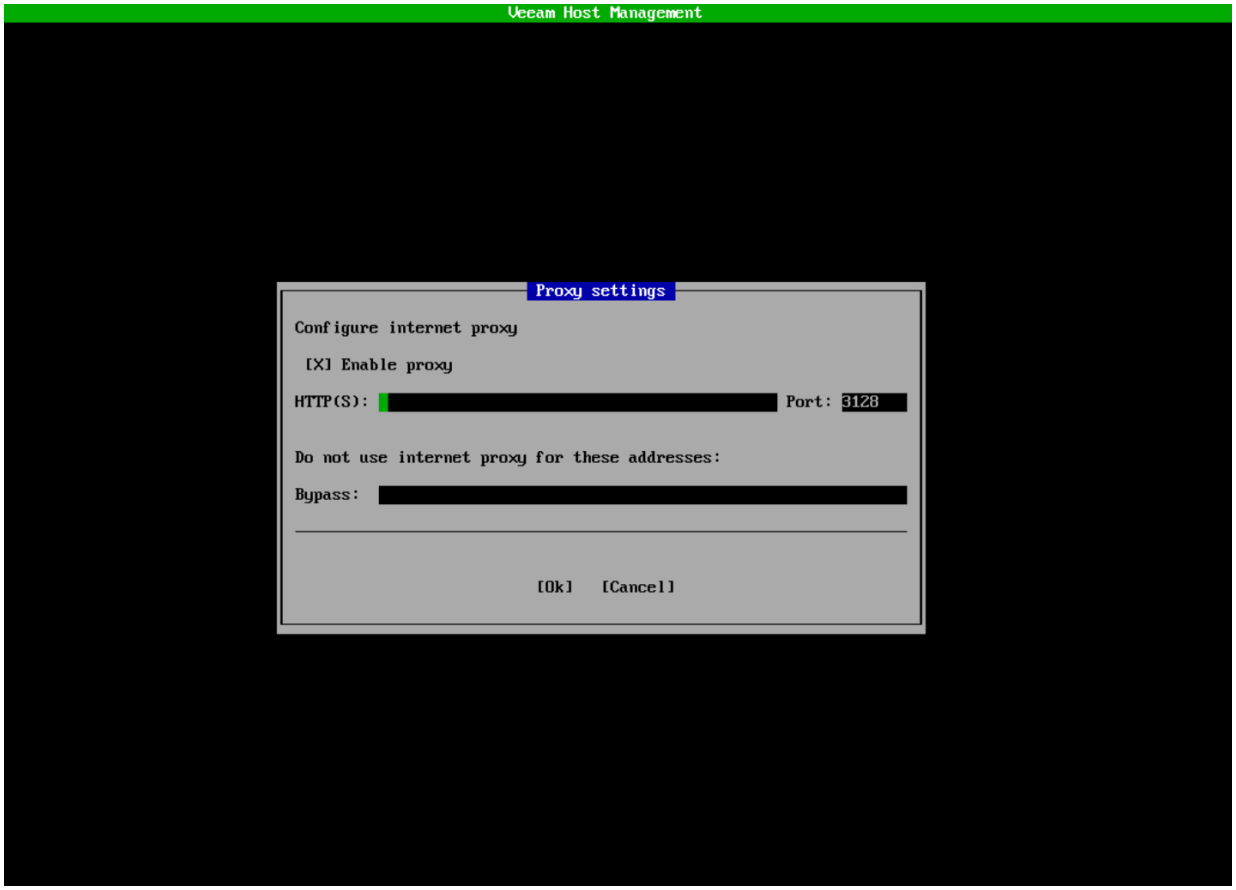
1. In the main menu, select **Host configuration** > **HTTP proxy**.
2. If you have not configured a proxy previously, select **Enable proxy** and press [Space].
3. Specify an HTTPS proxy and press [Enter].

After you configure a proxy, you can use the **Bypass** field to specify destinations that the appliance can connect to directly. You can specify the following types of destinations:

- Specific hostnames such as `server1` or `server1.domain.test`.
- Specific IP addresses such as `172.21.241.5`.

When specifying multiple addresses and hostnames, each one must be separated by a comma. For example, `172.21.241.5,server1.domain.test,server1`.

> **TIP**
>
> Any proxy settings configured in the Veeam Host Management TUI do not apply to Veeam Updater. You must configure it separately. For more information, see Veeam Software Appliance Update.


Veeam Host Management
Proxy settings
Configure internet proxy
[X] Enable proxy
HTTP(S):
Port: 3128
Do not use internet proxy for these addresses:
Bypass:
[Ok] [Cancel]

Configuring Server Time Settings

Users with Host Administrator permissions can perform the following operations within the server time settings:

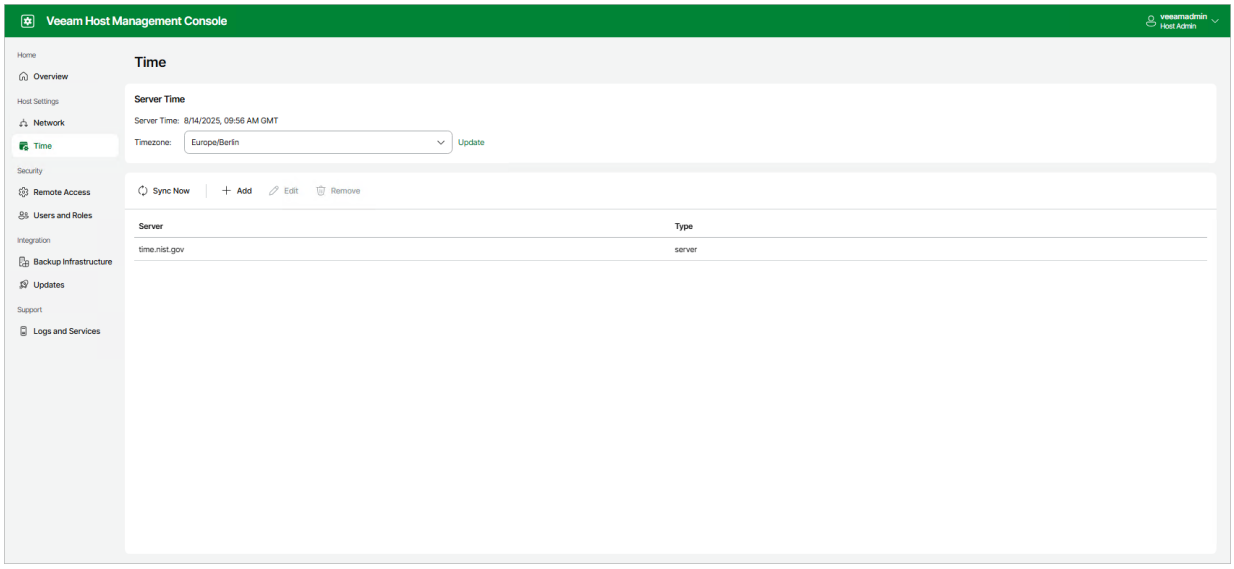
- Change the timezone
- Change the default time server
- Adding time servers
- Delete time servers

Users with Security Officer permissions cannot configure server time settings.

Changing Timezone

In the Veeam Host Management web UI, you can change the timezone of the server where the backup infrastructure component is installed. To do this, perform the following steps:

1. In the management pane, click **Time**.
2. In the **Server Time** section, select the required timezone and click **Update**.



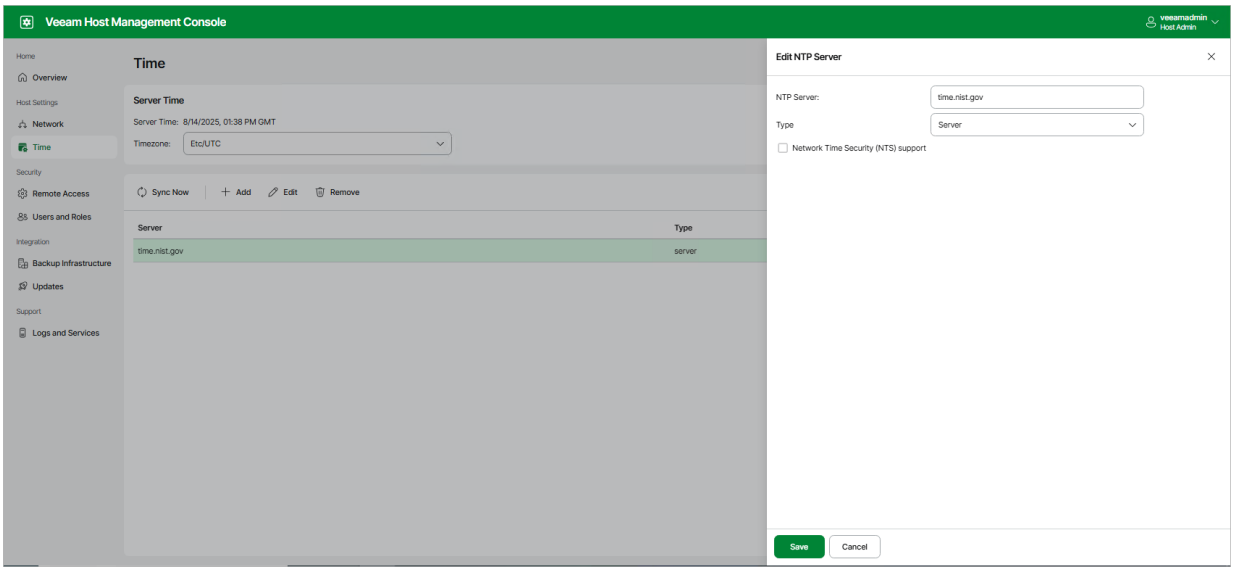
Changing Default Time Server

By default, Veeam Software Appliance uses one NTP server *time.nist.gov* that is configured automatically during the installation. You can change the default time server in the Veeam Host Management web UI or TUI.

If you use the Veeam Host Management web UI, perform the following steps:

1. In the management pane, click **Time**.
2. To change the default time server, select the name of the server and click **Edit**.
3. Specify the name and the type of the time server. Enable the NTS support if required.
4. Click **Save**.

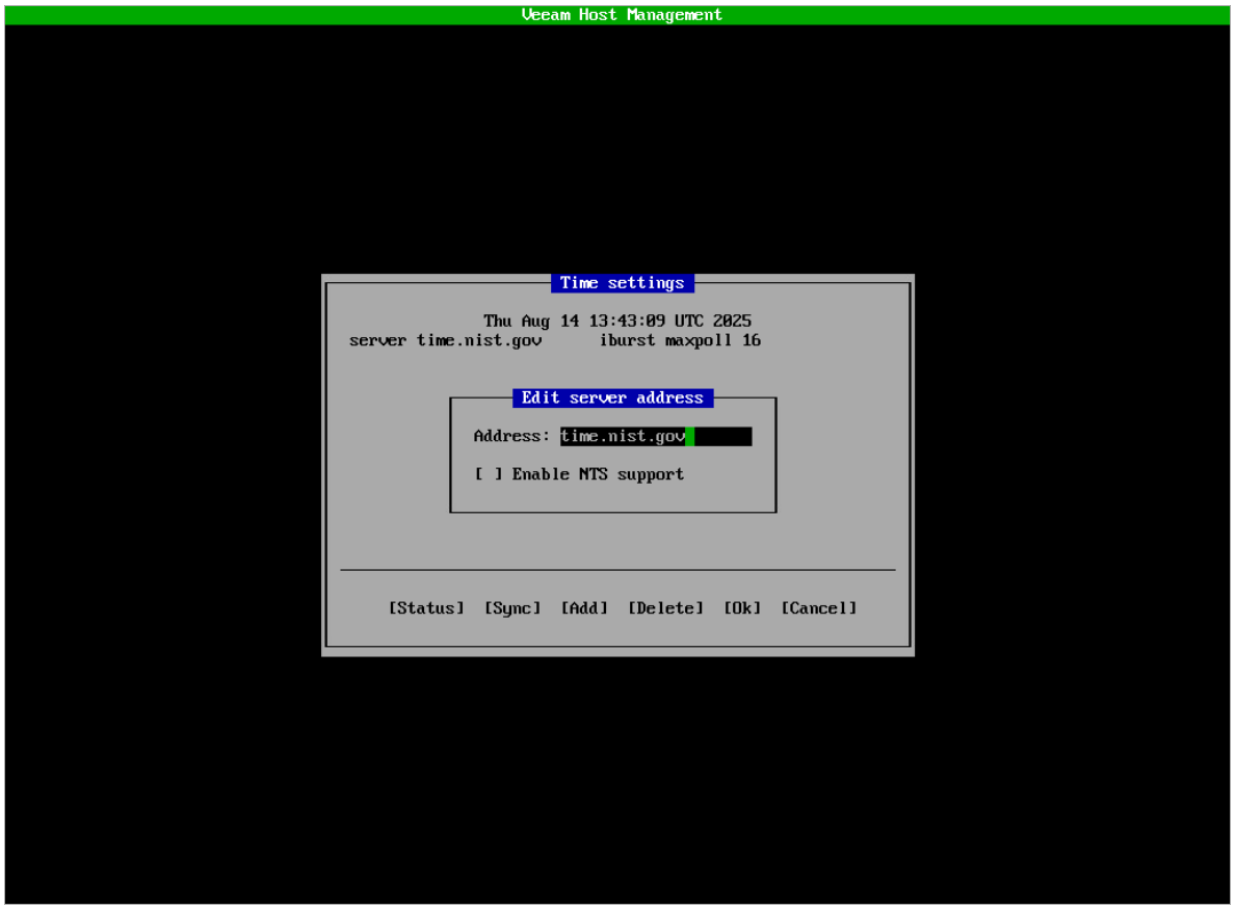
5. To synchronize server system time with the new time server, click **Sync Now**.



If you use the Veeam Host Management TUI, perform the following steps:

1. In the main menu, select **Host configuration** > **Time**.
2. Select the name of the server and press [Enter].
3. Configure required settings:
   - In the **Address** field, specify the name of the time server.
   - Enable the NTS support if required.
4. Press [Ok].

5. To check the status of the time server, press [Status].



Adding Time Servers

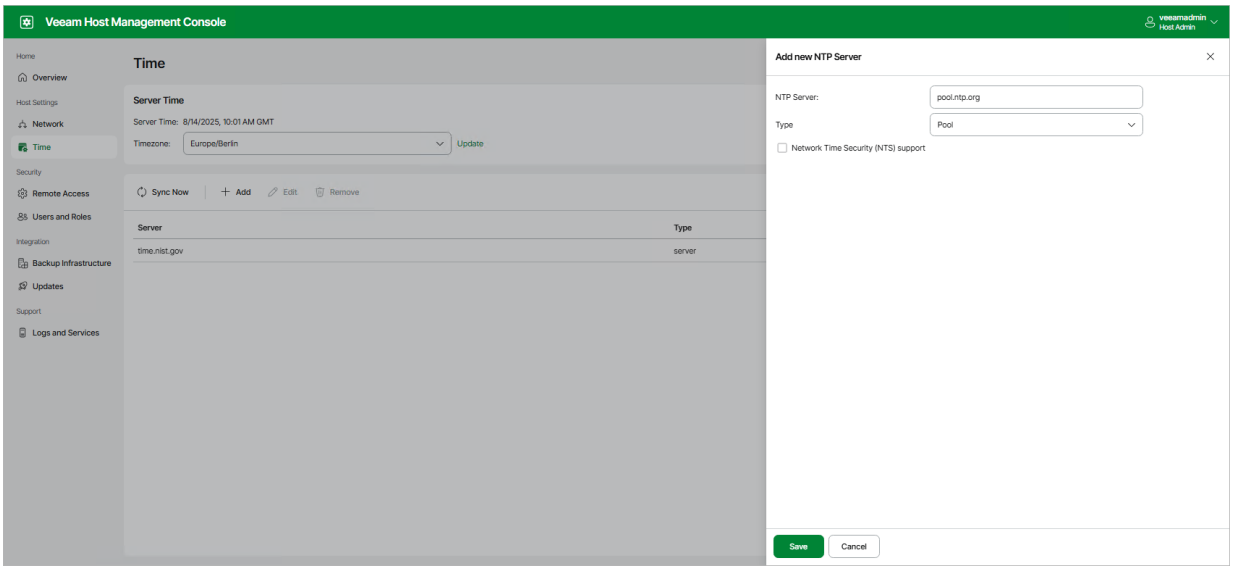
You can add several time servers in the Veeam Host Management web UI or TUI.

> **NOTE**
>
> Veeam Software Appliance supports NTP and public NTS time servers. It is recommended to use a minimum of 3 to mitigate timing issues.

If you use the Veeam Host Management web UI, perform the following steps:

1. In the management pane, click **Time**.
2. Click **Add**.
3. Specify the time server settings:
   - In the **NTP Server** field, specify the name of the time server.
   - From the **Type** drop-down list, select the type of the time server:
     - *Server* — A single time server.
     - *Pool* — A pool of public time servers.
   - Enable the NTS support if required.
4. Click **Save**.

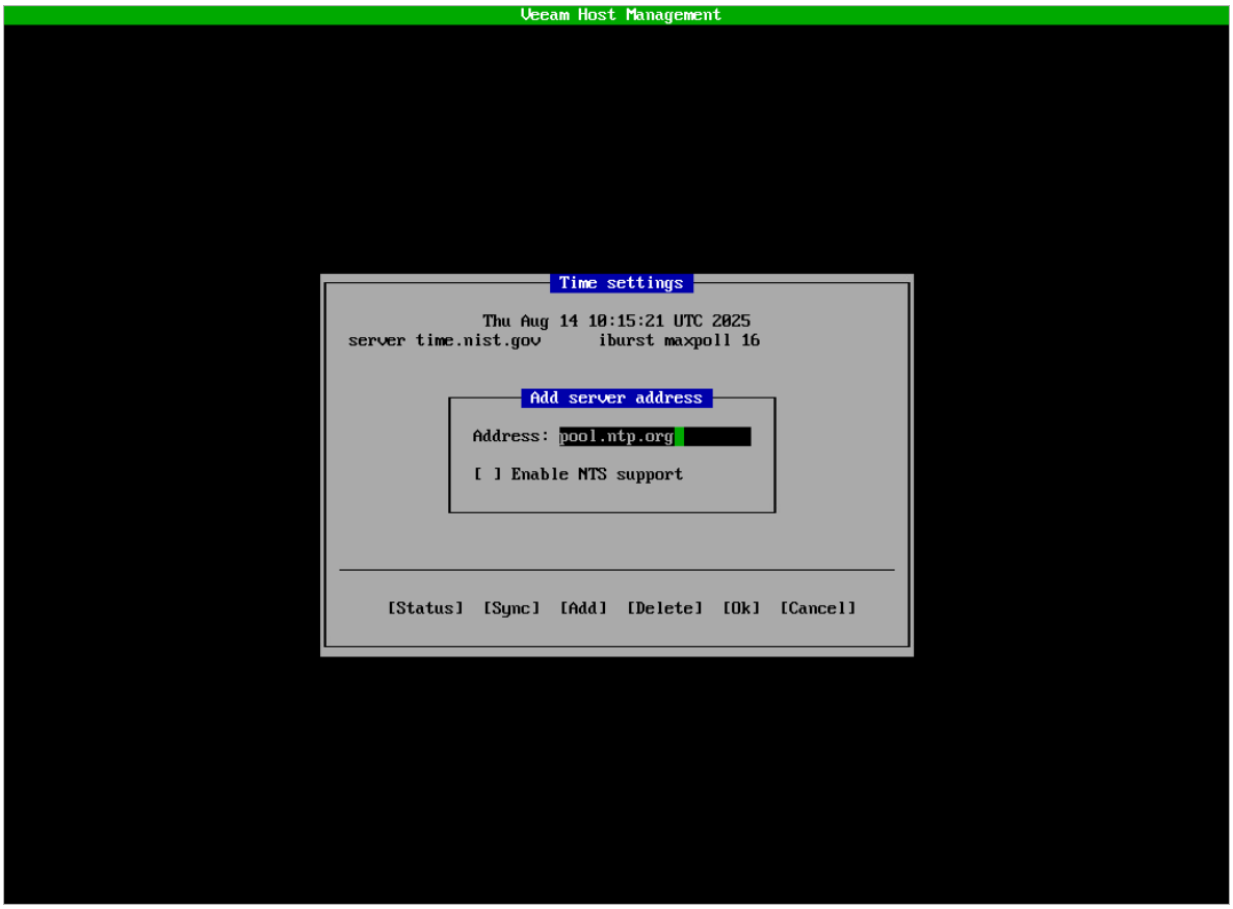
5. To synchronize server system time with time servers, click **Sync Now**.



If you use the Veeam Host Management TUI, perform the following steps:

1. In the main menu, select **Host configuration** > **Time**.
2. Press [Add].
3. Specify the time server settings:
   - In the **Address** field, specify the name of the time server.
   - Enable the NTS support if required.
4. Press [Ok].

5. To synchronize server system time with time servers, press [Sync].

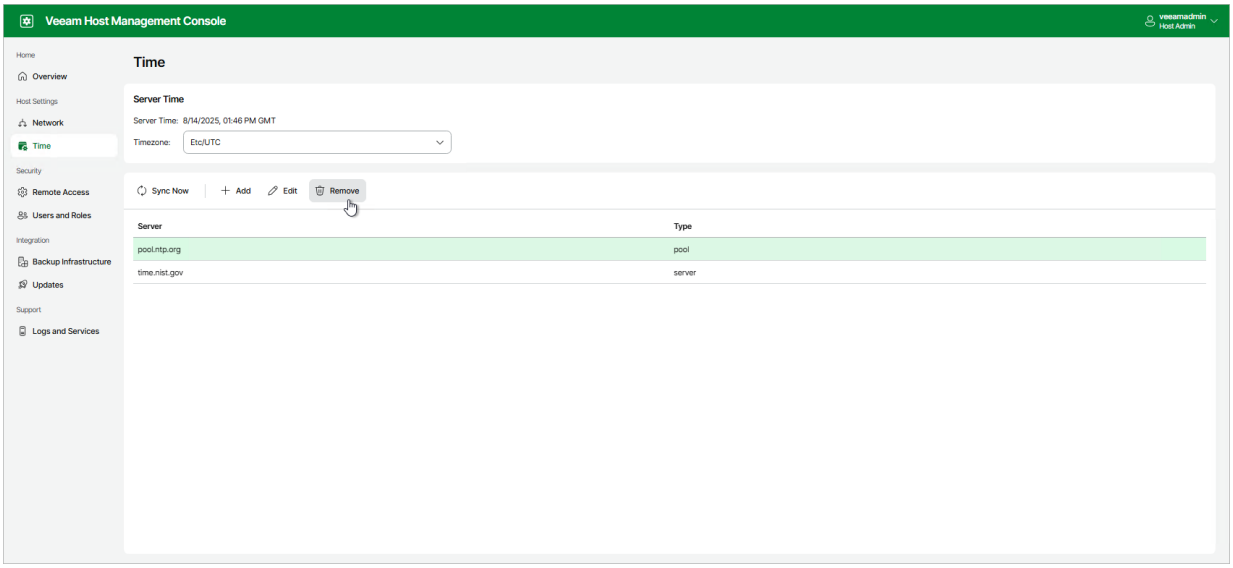


Deleting Time Servers

You can delete time servers in the Veeam Host Management web UI or TUI.

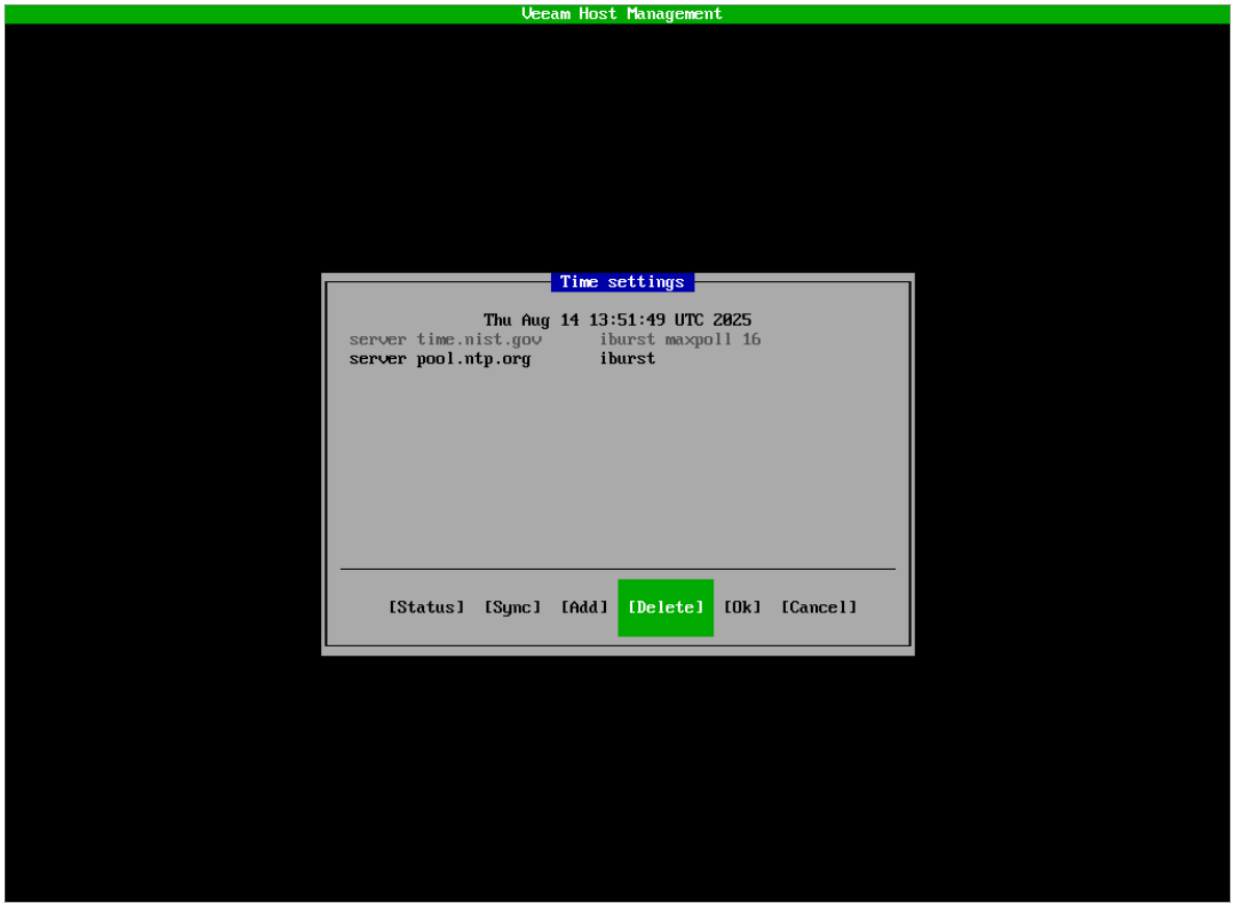
If you use the Veeam Host Management web UI, perform the following steps:

1. In the management pane, click **Time**.
2. Select the time server and click **Remove**.



If you use the Veeam Host Management TUI, perform the following steps:

1. In the main menu, select **Host configuration** > **Time**.
2. Select the time server and press [Delete].



Managing Storage

On the **Storage** page of the Veeam Host Management web UI, you can review storage usage on the appliance and attach additional storage devices. Users with Host Administrator permissions can perform the following operations with storage:

- View storage usage
- Add local, iSCSI and Fibre Channel storage
- Attach iSCSI LUNs
- View the host identifiers required for network storage
- View details, rescan, unmount, detach and forget attached devices

> **NOTE**
>
> Before you can attach network storage devices (iSCSI and Fibre Channel), you must enable Network Storage Management. For more information, see Configuring Backup Infrastructure Settings.

Viewing Storage Usage

The **Volumes** tab of the **Storage** page shows the file system load of the appliance storage, grouped into the following storage groups:

- **System Storage** — appliance system components required for operation, including core binaries, configuration files, packages and application data.
- **Built-In Storage** — on-appliance backups. This group may also contain catalog data and application logs.
- **Additional Storage** — Linux-based backup repositories added after installation. This group appears only after you add storage.

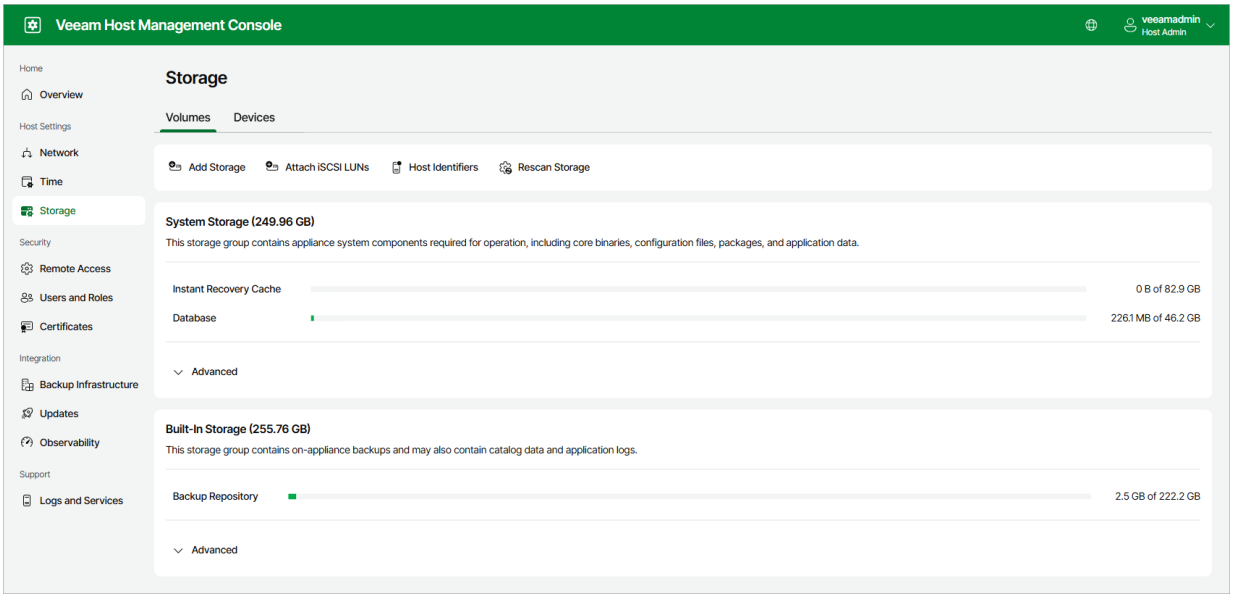
Each storage group shows the used and total space for its logical volumes. To see a detailed breakdown of a group, click **Advanced**.

To view storage usage, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Storage**.
3. Open the **Volumes** tab.

You can also review basic resource consumption of the appliance in the **Usage** section of the **Overview** page. To open the **Storage** page from there, click **View storage usage**.

If the usage of a volume exceeds 90%, the appliance generates an event. You can view the event in the Veeam Host Management web UI, on the **Events** tab of the **Logs and Services** page, and in the Veeam Backup & Replication console, in the **History** view under the **Events** node.



Adding Storage

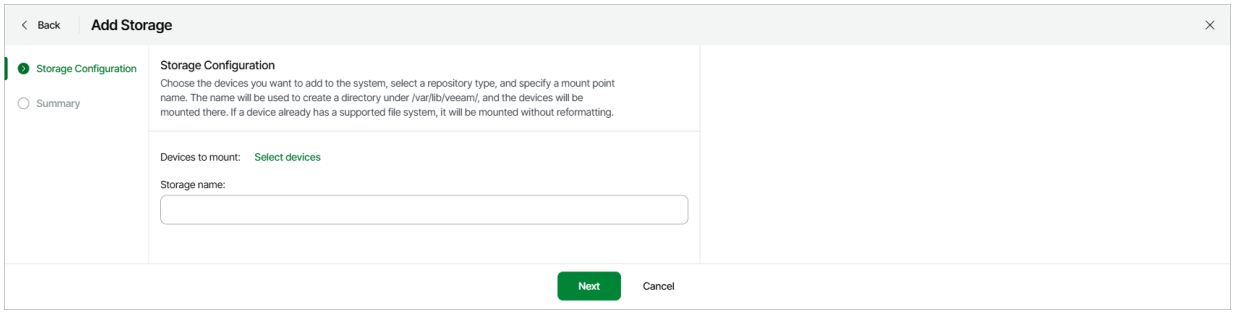
You can add local, iSCSI and Fibre Channel devices to the appliance and mount them for use as backup repositories. When you add storage, consider the following:

- If a device already has a supported file system (XFS or ZFS), it is mounted without reformatting. Blank devices are formatted before they are mounted.
- If you are configuring storage on a Veeam Infrastructure Appliance with the Hardened Repository role, you must also select a **Repository type** — *Linux / Hardened* for a hardened, immutable repository, or *Application Backup* for an Application Backup repository. *Application Backup* appears only after you enable it on the **Backup Infrastructure** page. For more information, see Configuring Backup Infrastructure Settings.

To add storage, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Storage**.
3. Click **Add Storage**.
4. In the **Add Storage** window, click **Select devices**.
5. Select the devices you want to mount.
6. Click **Select**.
7. In the **Storage name** field, enter a name for the storage.
8. If you are configuring storage on a Veeam Infrastructure Appliance with the Hardened Repository role, in the **Repository type** field, select the required repository type.
9. Click **Next**.

10. At the **Summary** step of the wizard, review the settings and click **Finish**.



Attaching iSCSI LUNs

To connect iSCSI storage, attach the iSCSI LUNs presented by your storage system. After the LUNs are attached, you can add them as storage as described in Adding Storage.

To attach iSCSI LUNs, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Storage**.
3. Click **Attach iSCSI LUNs**.
4. At the **iSCSI Portal Settings** step of the wizard, in the **Portal address** field, enter the address of the iSCSI portal. If the portal uses a non-default port, in the **Port** field, enter the port number.
5. If the portal requires CHAP authentication, set the **Requires authentication** toggle to *On* and enter the **Username** and **Password**.
6. Click **Next**.
7. At the **Select iSCSI Targets** step of the wizard, select the targets you want to attach and click **Next**. Multipathing is applied automatically where possible.
8. At the **Summary** step of the wizard, review the settings and click **Finish**.

> **NOTE**
>
> Consider the following:
>
> - Mounting the same iSCSI device on multiple hosts is not supported.
> - CHAP authentication works only if the storage system uses SHA-256 or SHA3-256 for CHAP.

Viewing Host Identifiers

To present network storage to the appliance, your storage system needs the host identifiers of the appliance. The **Host Identifiers** window shows the following identifiers:

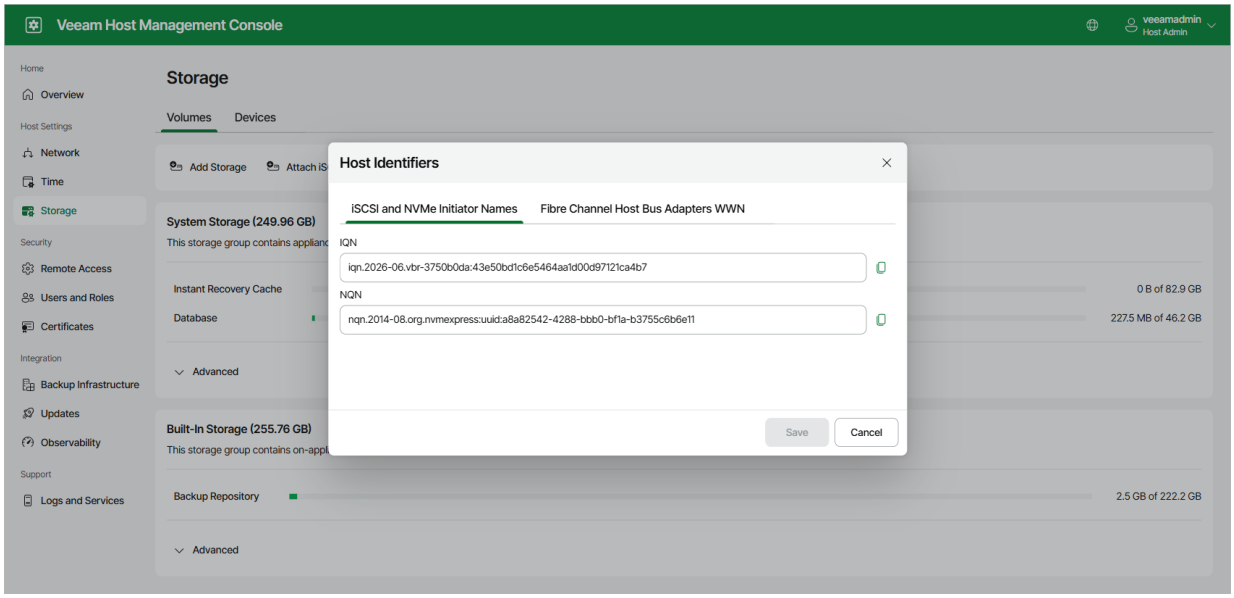
- The IQN and NQN initiator names, on the **iSCSI and NVMe Initiator Names** tab.
- The Fibre Channel host bus adapter WWNs, on the **Fibre Channel Host Bus Adapters WWN** tab.

To view the host identifiers, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Storage**.

3. Click **Host Identifiers**. To copy an identifier, click the copy icon next to it.

> **NOTE**
>
> Changing the host FQDN does not change the host identifiers. You can change the IQN as required, provided that it uses a valid format.



Managing Attached Devices

The **Devices** tab of the **Storage** page lists all attached devices and their details. On this tab, you can perform the following operations:

- To view detailed information about a device, select it and click **View Details**.
- To discover newly presented devices, click **Rescan Storage**.
- To unmount a device, select it and click **Unmount**.
- To detach an iSCSI LUN, select it and click **Detach iSCSI LUNs**.
- To detach a device from the appliance, select it and click **Forget Device**.

> **NOTE**
>
> When a device is detached, all drives connected to the same target are detached as well.

Configuring Remote Access Settings

Users with Host Administrator permissions can perform the following operations within the remote access settings:

- Enable and disable access to the Veeam Host Management web UI
- Enable and disable SSH access

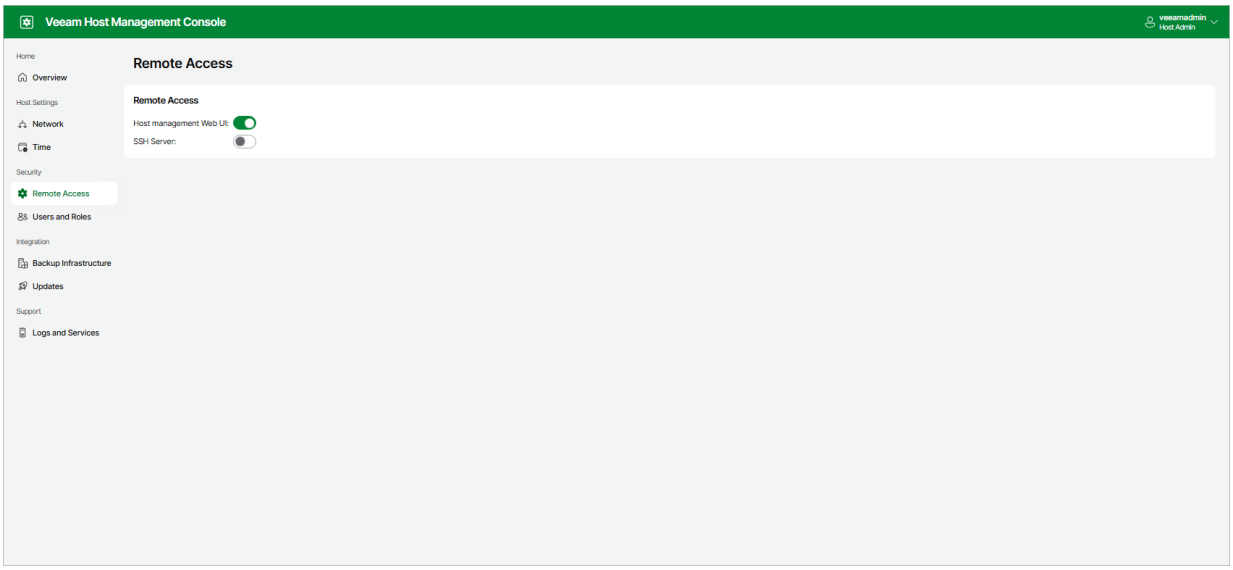
Users with Security Officer permissions can approve or reject requests from Host Administrator users for temporary access to the root shell. For more information, see Managing Root Shell Access.

Managing Access to Veeam Host Management Web UI

By default, you can configure Veeam Software Appliance through the Veeam Host Management web UI. If you want to disable web UI access, perform the following steps:

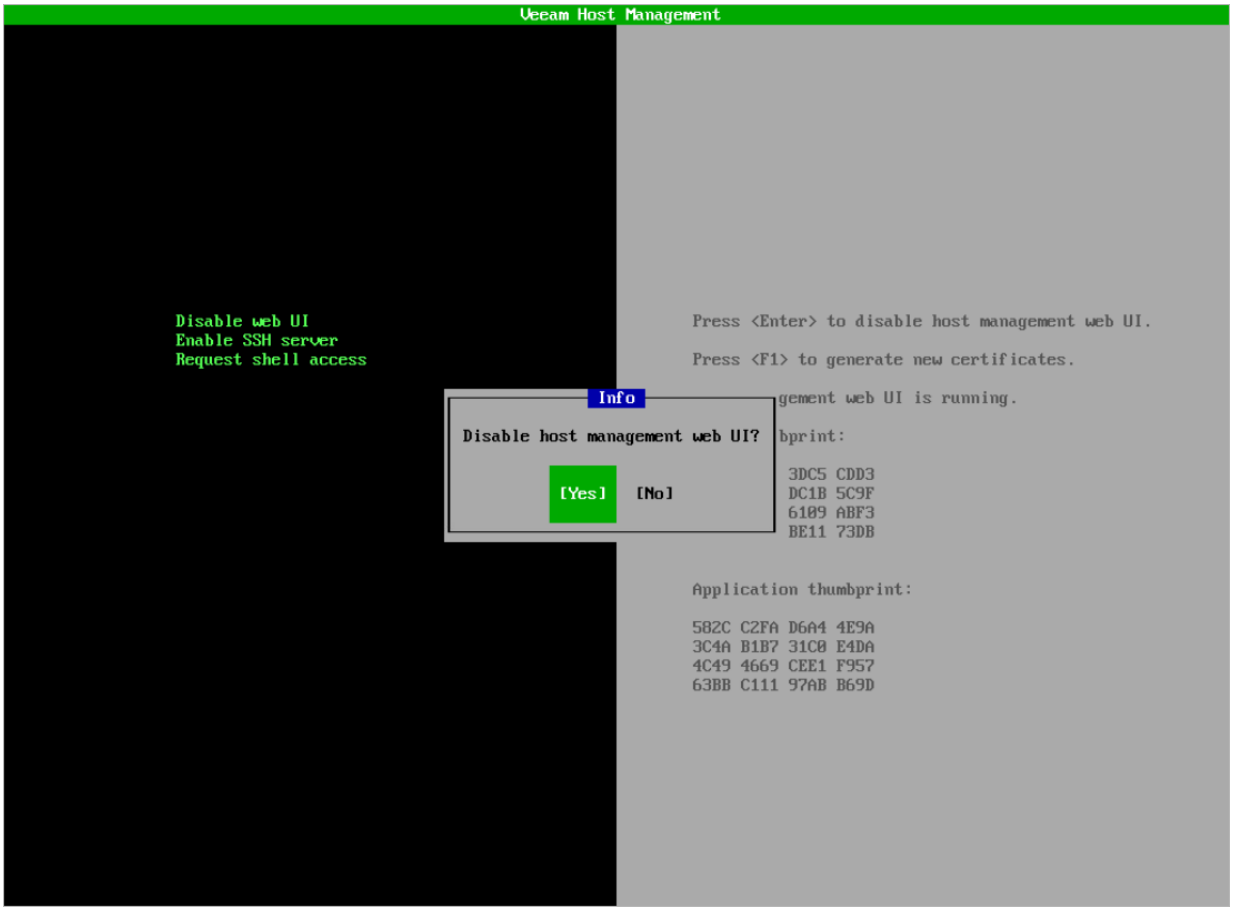
- If you use the Veeam Host Management web UI, do the following:
  a. In the management pane, click **Remote Access**.
  b. Set the **Host management Web UI** toggle to *Off*.

> **NOTE**
>
> If you disable web UI access, all active Veeam Host Management web UI sessions will be closed. You can enable web UI access again in the Veeam Host Management TUI.



- If you use the Veeam Host Management TUI, do the following:
  a. In the main menu, select **Remote access configuration**.
  b. Select **Disable web UI**, press [Enter] and confirm the operation.

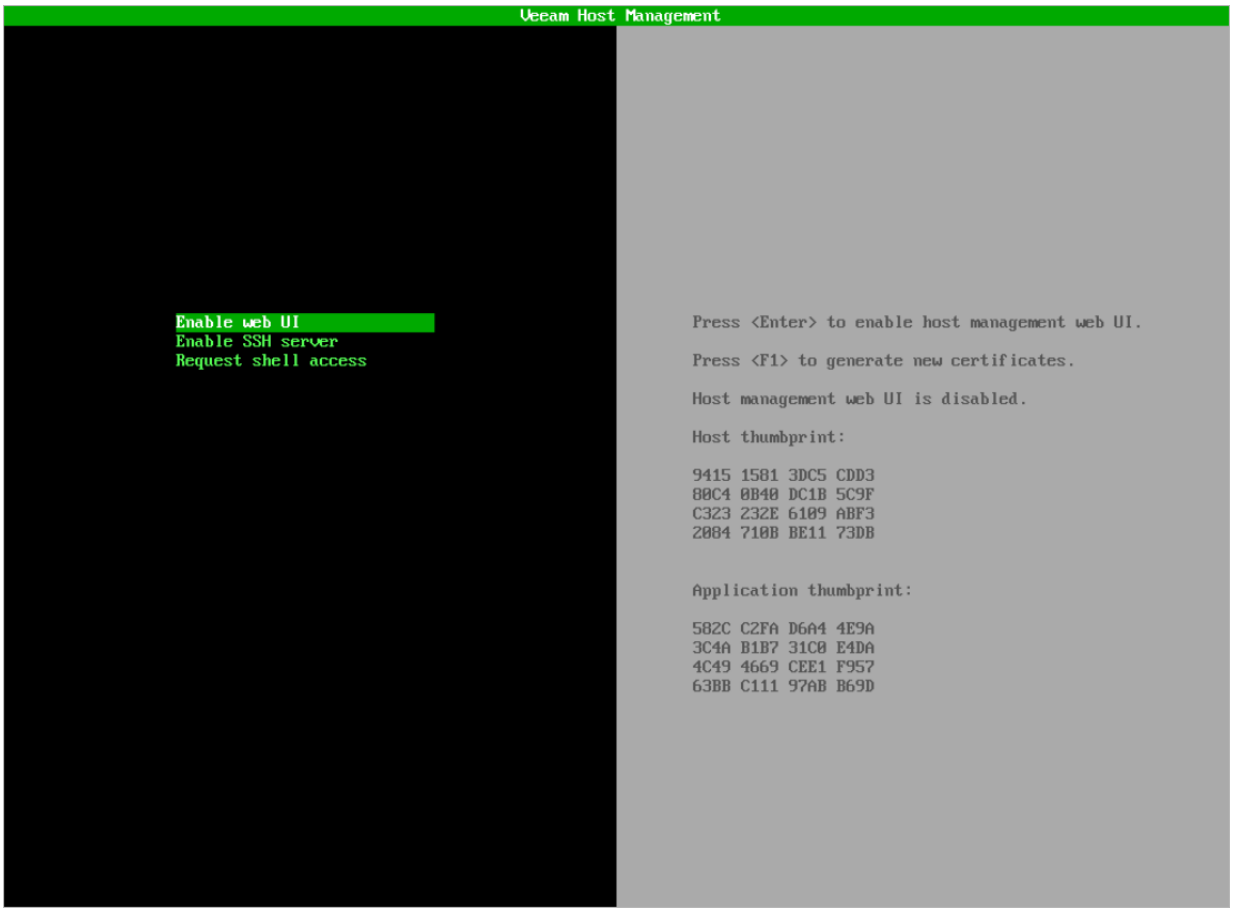
> **NOTE**
>
> If you disable web UI access, all active Veeam Host Management web UI sessions will be closed. You can enable web UI access again in the Veeam Host Management TUI.



To enable web UI access in the Veeam Host Management TUI, perform the following steps:

1. In the main menu, select **Remote access configuration**.

2. Select **Enable web UI** and press [Enter].



Managing SSH Access

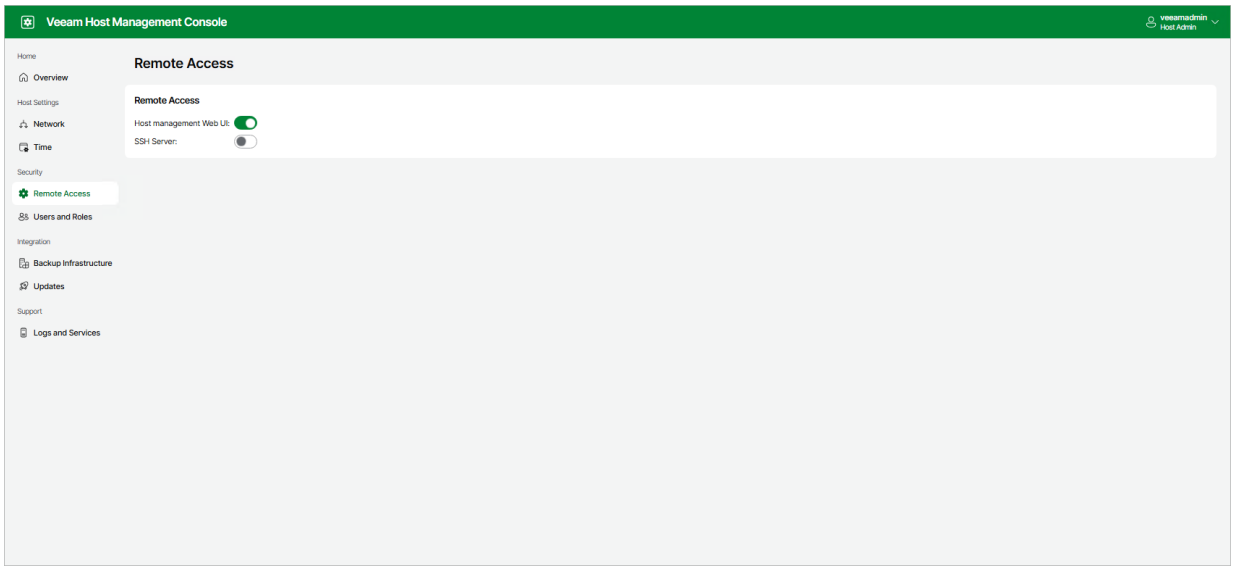
By default, you cannot connect to Veeam Software Appliance through SSH. If required, you can enable SSH access in the Veeam Host Management web UI or TUI.

If you did not configure the Security Officer account during the Veeam Software Appliance installation, SSH access will be available immediately. If you configured the Security Officer account, SSH access will be available after the Security Officer approves the request.

If you use the Veeam Host Management web UI, perform the following steps:

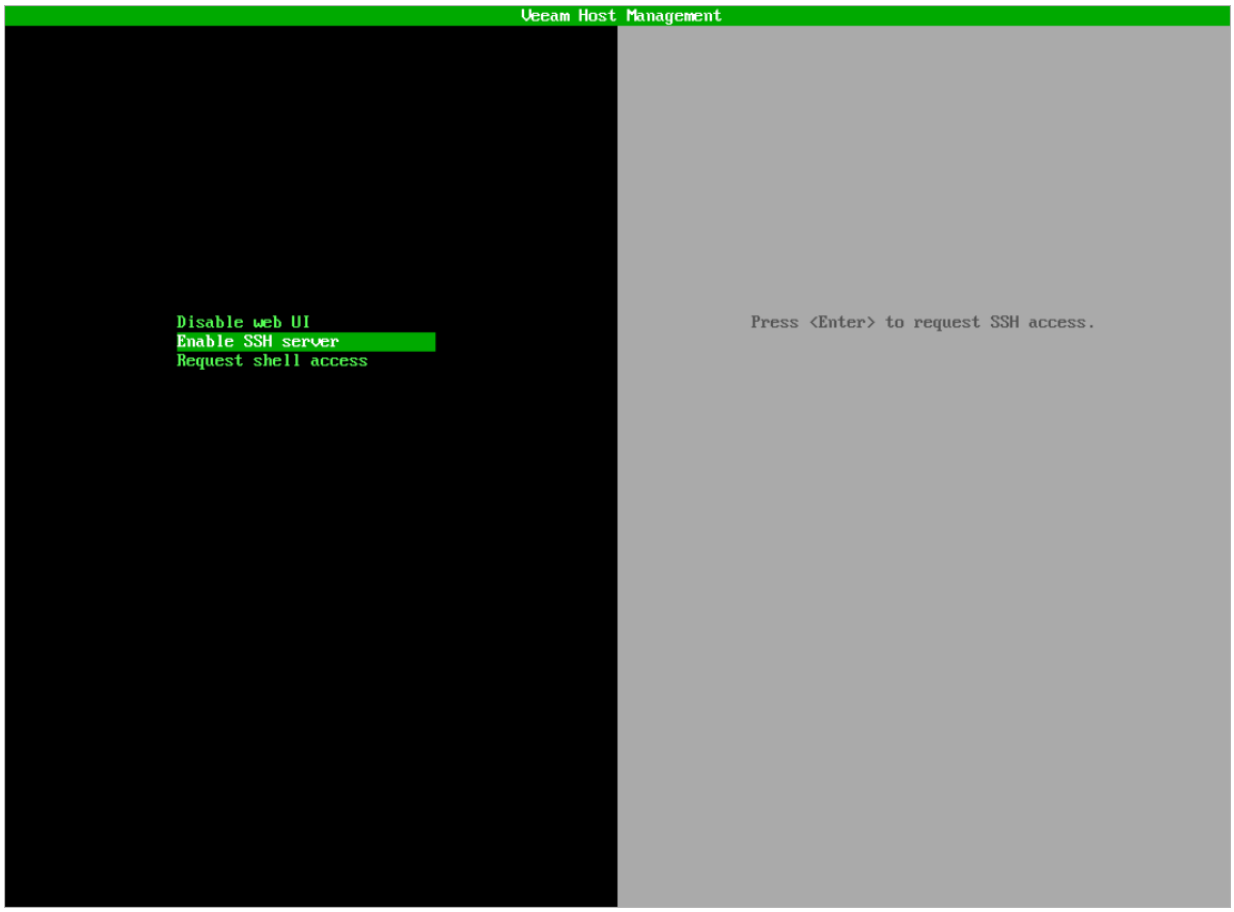
1. In the management pane, click **Remote Access**.

2. Set the **SSH Server** toggle to *On*.



If you use the Veeam Host Management TUI, perform the following steps:

1. In the main menu, select **Remote access configuration**.
2. Select **Enable SSH server** and press [Enter].



> **NOTE**
>
> If you disable SSH access, all active SSH sessions will be closed.

Managing Root Shell Access

For troubleshooting or other specific purposes, you can use the Veeam Host Management TUI root shell.

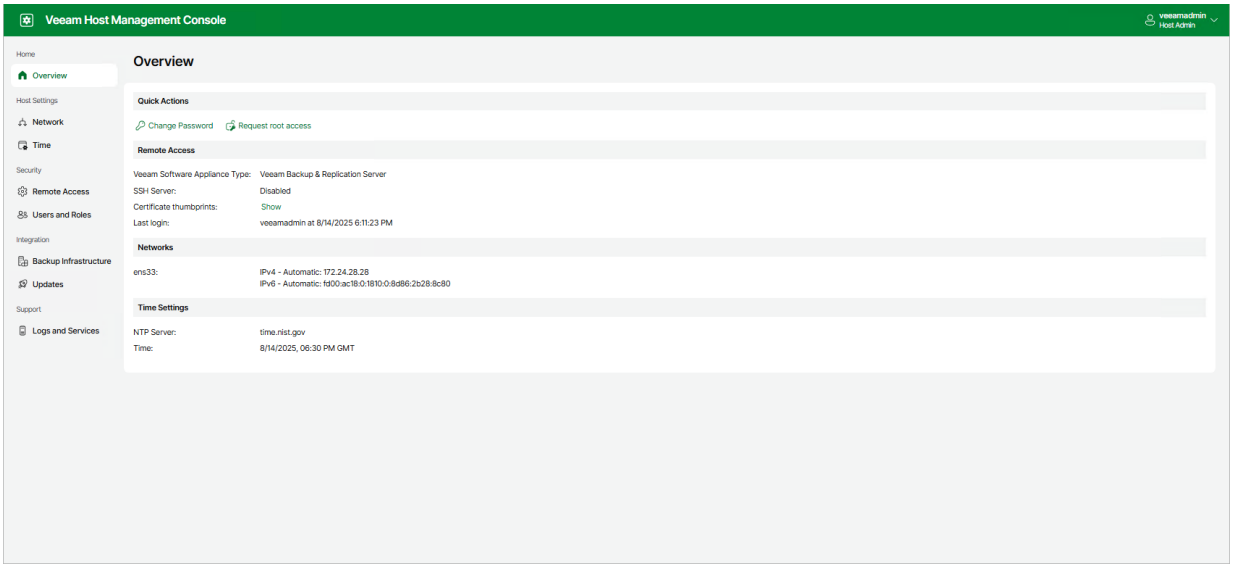
> **IMPORTANT**
>
> Consider the following:
>
> - You cannot access the TUI root shell through SSH. Only local connection through a physical console or a virtual remote console is supported.
> - The Host Administrator does not get root privileges. The TUI shell runs under the root account.
> - Use the TUI root shell carefully when you run any commands or change configuration files. Custom configurations are not supported by Veeam.

If you did not configure the Security Officer account during the Veeam Software Appliance installation, users with Host Administrator permissions have permanent access to the TUI root shell. To run the TUI root shell, perform the following steps:

1. Log in to the Veeam Host Management TUI.
2. In the main menu, select **Remote access configuration.**
3. Select **Enter shell** and press [Enter].

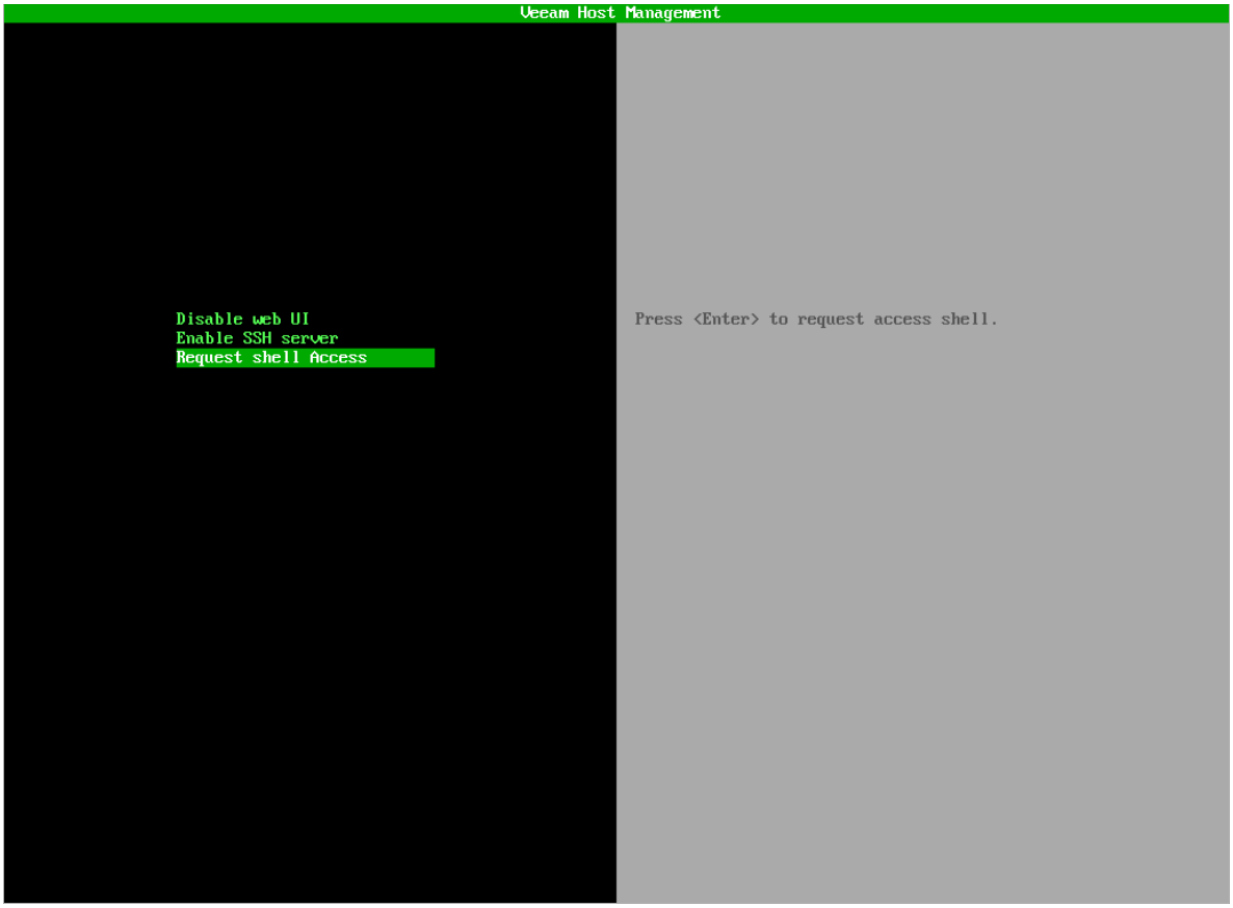
If you configured the Security Officer account during the Veeam Software Appliance installation, users with Host Administrator permissions must request temporary access to the TUI root shell. To do this, perform the following steps:

- If you use the Veeam Host Management web UI, do the following:
  a. Log in to the Veeam Host Management web UI.
  b. In the management pane, click **Overview**.
  c. In the **Quick Actions** section, click **Request root access**.



- If you use the Veeam Host Management TUI, do the following:
  a. Log in to the Veeam Host Management TUI.
  b. In the main menu, select **Remote access configuration**.

c. Select **Request shell access**, press [Enter] and confirm the operation.



If the Security Officer approves the request, access to the TUI root shell will be granted for 8 hours from the first login. The access is not revoked after activity timeouts. Once approved, the Security Officer can remove access before the 8 hours ends by later declining the same request.

Managing Users and Roles

This section describes how to configure local Veeam Software Appliance users.

Configuring Users

Users with Host Administrator permissions can perform the following operations related to configuring local Veeam Software Appliance users:

- Assign roles
- Create, edit, and remove user accounts

Users with Security Officer permissions cannot configure local users.

> **NOTE**
>
> When configuring users, consider the following:
>
> - If you have multi-factor authentication enabled, you must enter a one-time password before you can perform the following operations on Host Administrator accounts: create, edit, or remove users, assign roles, or reset multi-factor authentication. Authentication remains valid for 15 minutes.
> - A Host Administrator can enable or disable multi-factor authentication for other users at any time, including multi-factor authentication that was disabled during initial configuration. After you enable MFA, users are prompted to set it up at their next login. For more information, see <%TARGETTITLE%>.

User Roles

The following table describes roles you can assign to the local users.

Role	Description
Host Administrator	Can perform all administrative activities in the Veeam Host Management web UI and TUI: • Configure network settings • Configure server time settings • Configure remote access settings • Manage users and roles • Configure backup infrastructure integrations • Manage software updates • Perform maintenance tasks The default Host Administrator account is *veeamadmin*.

Role	Description
Security Officer	Can perform the following operations in the Veeam Host Management web UI: • Reset user passwords • Reset user multi-factor authentication • Manage authorization requests • Manage password recovery tokens • Manage configuration backups • Export events Security Officer does not have access to the Veeam Host Management TUI. The default Security Officer account is *veeamso*.
User	Manages backup and restore operations in accordance with the assigned backup server role. Use this role to create backup console users when the Veeam Software Appliance is not joined to a domain. User must reset their password at first sign-in. Has limited permissions to the system and no access to the Veeam Host Management console.

Creating Users

To create a new user, perform the following steps:

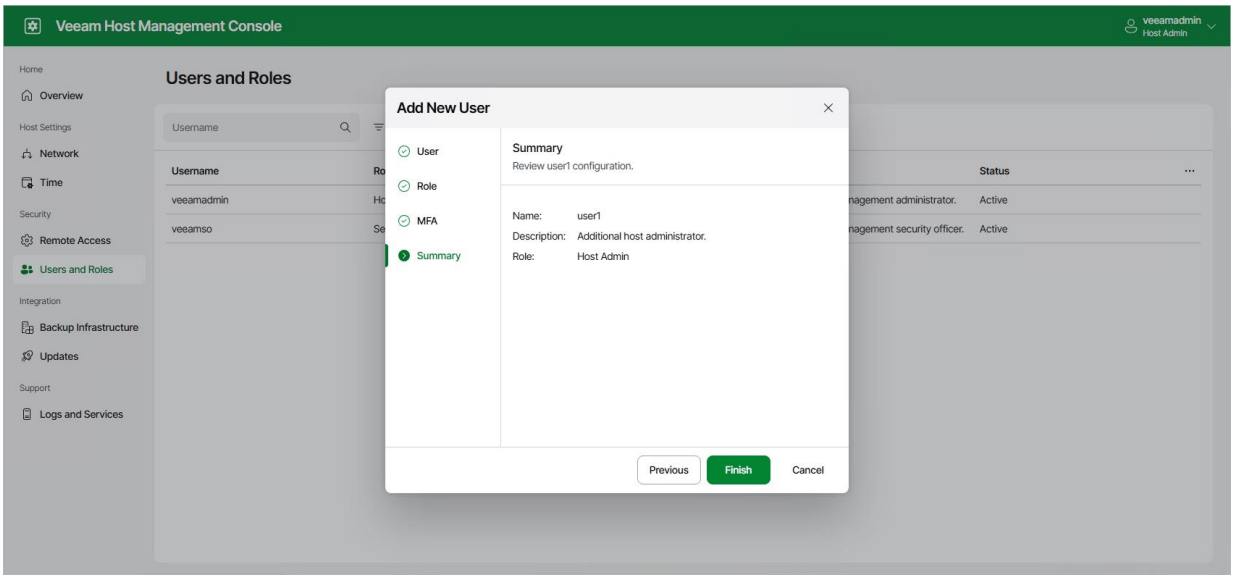
1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Click **Add**.
4. At the **User** step of the wizard, specify the name of the user, a password, and a description.

> **NOTE**
>
> Consider the following:
>
> - The password must meet the following requirements:
>   - 15 characters minimum.
>   - 1 upper case character.
>   - 1 lower case character.
>   - 1 numeric character.
>   - 1 special character.
>   - No more than 4 characters of the same class in a row. For example, more than 4 lowercase or 4 numerical characters in sequence.
> - By default, passwords stay valid for 60 days, after which a user must set a new password that meets the listed requirements. A Host Administrator can change this interval or disable password expiration. For more information, see Managing User Authentication.
> - After you add the user, you cannot change its name.

5. Click **Next**.
6. At the **Role** step of the wizard, select a role and click **Next**. You can assign only one role to the user.
7. At the **MFA** step of the wizard, enable or disable multi-factor authentication for the user and click **Next**.

> **NOTE**
>
> Consider the following:
>
> - If you add a user with the Security Officer role, you cannot disable MFA on that account.
> - If you add a user with the User role, this step will be skipped.

8. At the **Summary** step of the wizard, review the data and click **Finish**.

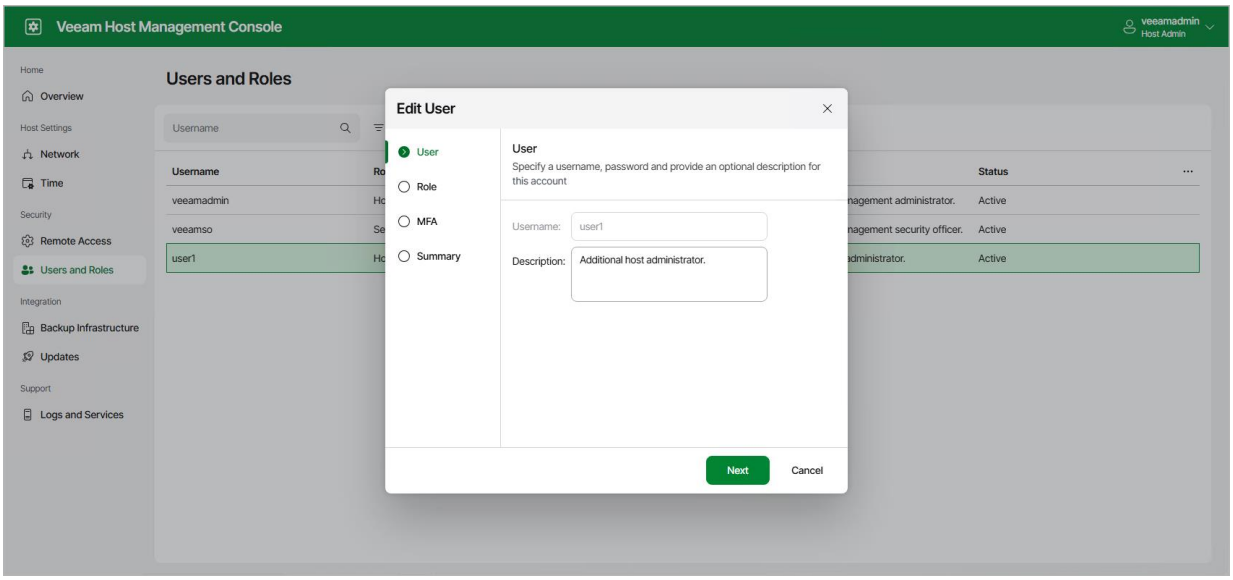


Editing Users

To edit a user, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Click **Edit**.
4. Change the description and roles if necessary. For Host Administrator accounts, you can also enable or disable multi-factor authentication.

5. Review the data and click **Finish**.

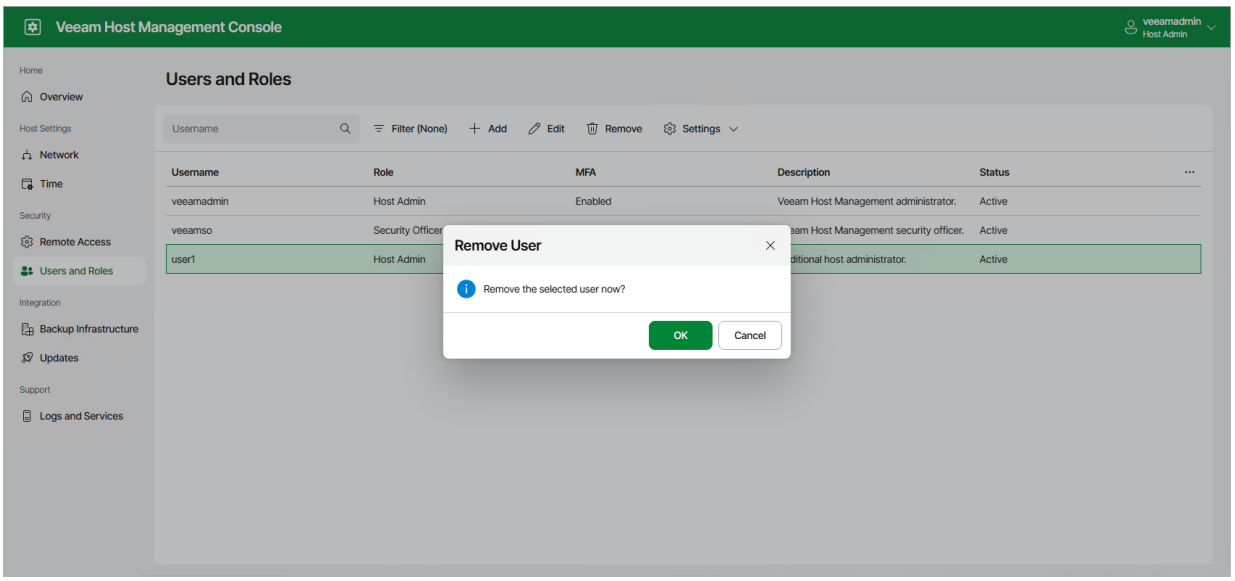


Removing Users

To remove a user, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Select the user, click **Remove** and confirm the operation.

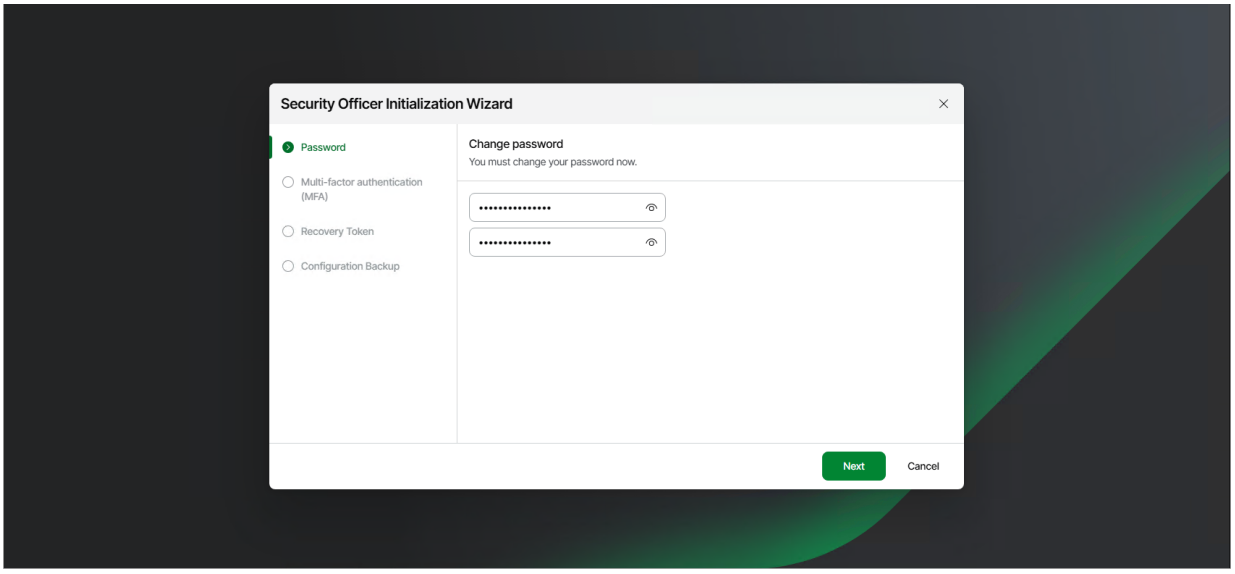
> **NOTE**
>
> You cannot remove the default *veeamadmin* and *veeamso* user accounts.



Performing Initial Security Officer Login

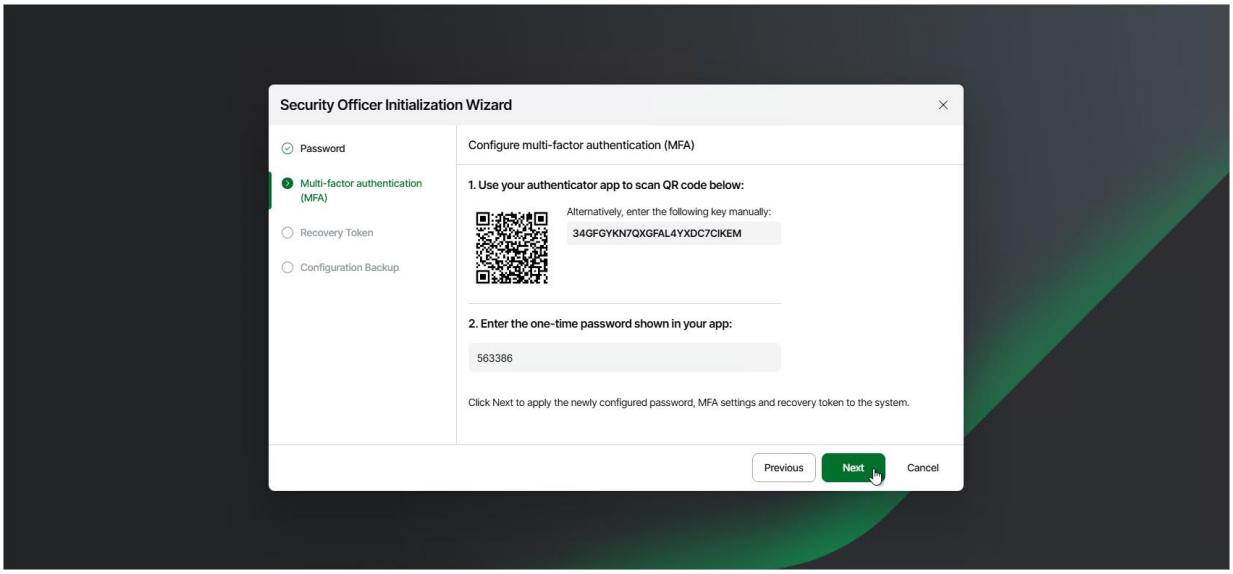
When you first log in to the Veeam Host Management as a Security Officer, perform the following steps:

1. Log in to the Veeam Host Management web UI.
2. Specify a new password that meets the following requirements:
   - 15 characters minimum.
   - 1 upper case character.
   - 1 lower case character.
   - 1 numeric character.
   - 1 special character.
   - No more than 4 characters of the same class in a row. For example, more than 4 lowercase or 4 numerical characters in sequence.
   - The new password must be different from the one specified in the Initial Configuration wizard.

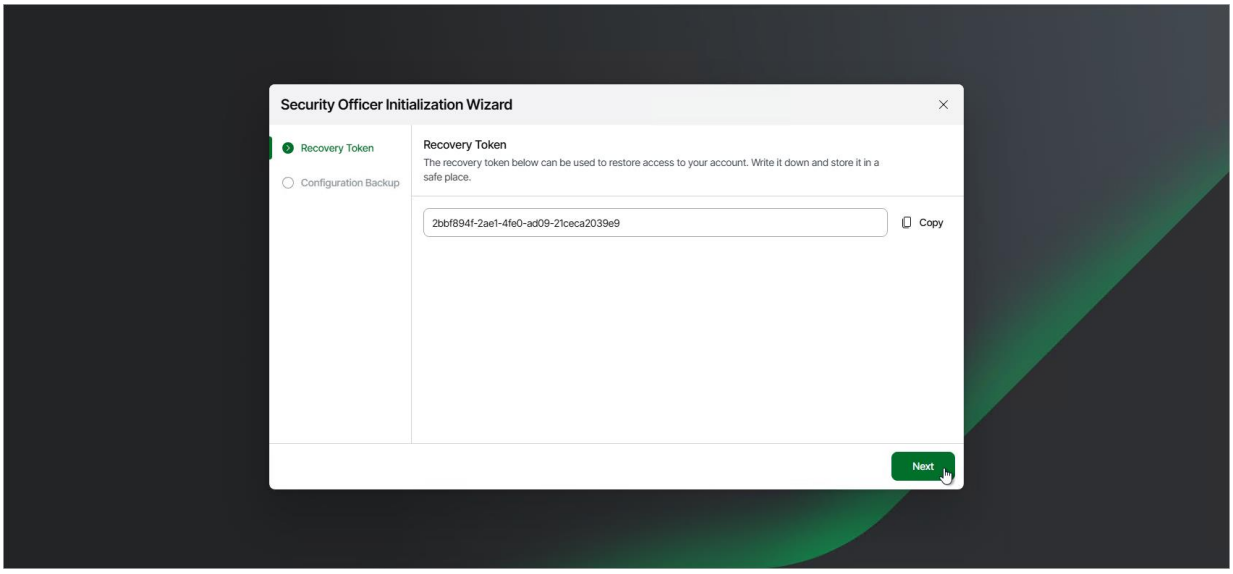


3. Click **Next**.
4. Configure multi-factor authentication:
   a. Open your authentication application. Enter the code or scan the QR code.
   b. Specify the one-time code provided by the application.

> **NOTE**
>
> If multi-factor authentication was disabled during initial configuration, this step is skipped.



5. Copy the recovery token and save it in a secure place.



6. Click **Finish**.

Managing User Authentication

Users with Host Administrator permissions can perform the following operations related to authentication of the local Veeam Software Appliance users:

- Configure password policies
- Unlock users
- Enable and disable multi-factor authentication
- Reset multi-factor authentication
- Reset user passwords
- Change own password

Users with Security Officer permissions can only approve authorization requests to reset user passwords. For more information, see Performing Security Officer Tasks.

> **NOTE**
>
> If you have multi-factor authentication enabled, you must enter a one-time password before you can perform the following operations on Host Administrator accounts:
>
> - Change a user password
> - Reset multi-factor authentication
> - Unlock users
>
> Authentication remains valid for 15 minutes.

Configuring Password Policies

A Host Administrator can define password policies that apply to all local users, except users with the Service Account role.

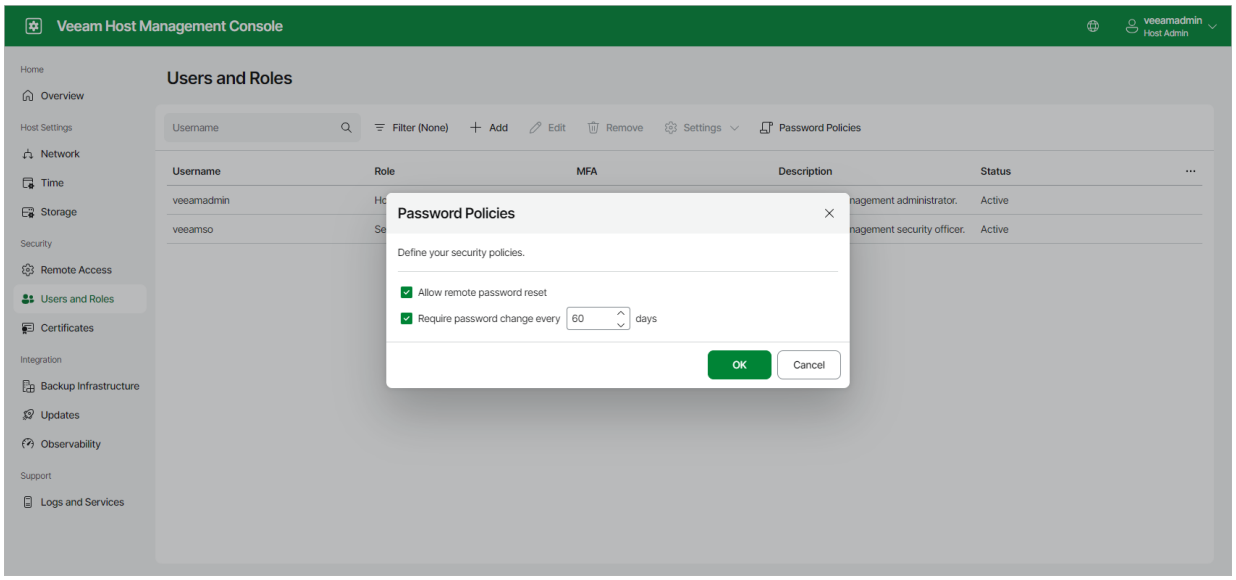
> **NOTE**
>
> Password policy settings are preserved during upgrades.

To configure password policies, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Click **Password Policies**.
4. Select or clear the **Allow remote password reset** check box. When enabled, users can request a password reset remotely from the sign-in page. A temporary password for the account must be set by a Security Officer.
5. Select or clear the **Require password change every N days** check box. When enabled, this specifies the number of days a password remains valid. The default is 60 days. You can specify a value from 1 to 365 days. To disable password expiration, clear the check box.

> **IMPORTANT**
>
> Disabling password expiration or setting the interval to more than 60 days violates the DISA STIG requirement V-258041.

6. Click **OK**.



Unlocking Users

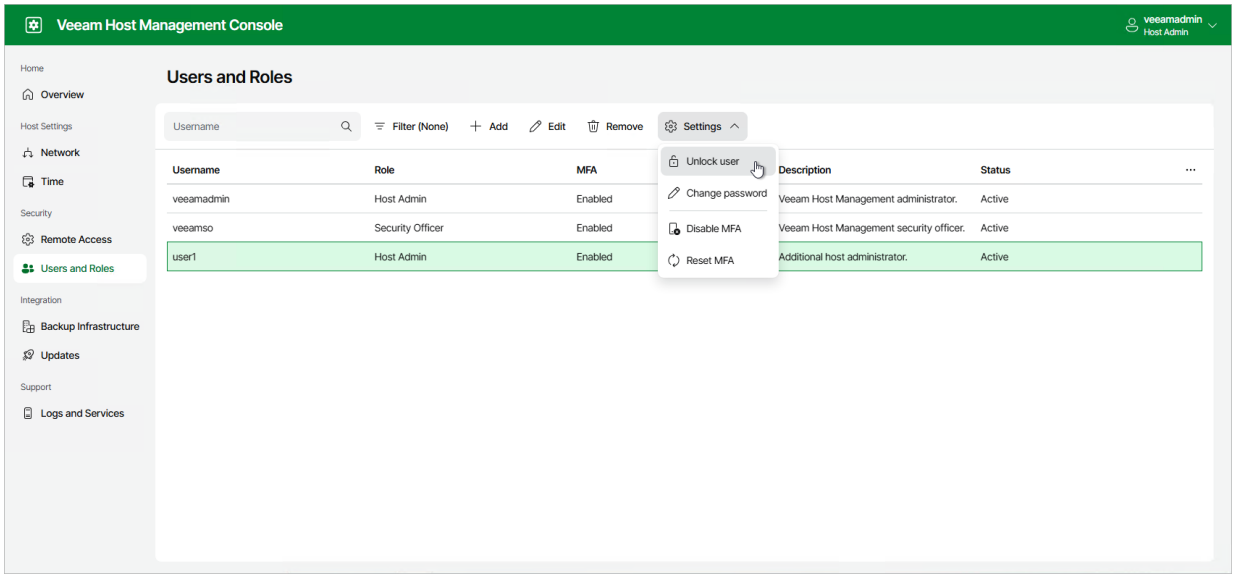
You can unlock users who were locked after three failed login attempts. Consider the following:

- If you did not configure the Security Officer account during the Veeam Software Appliance installation, the user will be automatically unlocked in 15 minutes. Alternatively, you can unlock the user manually.
- If you configure the Security Officer account, the user will not be automatically unlocked. You can unlock the user only manually.

To unlock the user manually, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Select the user.
4. Click **Settings** > **Unlock user**.

> **TIP**
>
> You can also unlock the user by resetting the password. For more information, see Resetting Passwords.

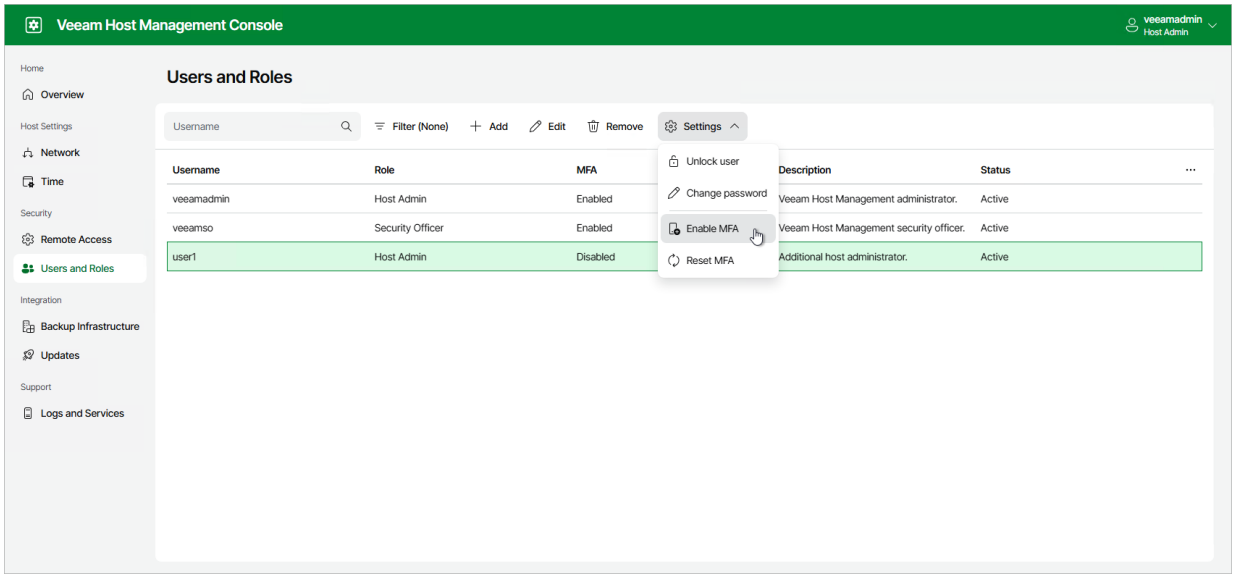


Enabling Multi-Factor Authentication

To enable multi-factor authentication for Host Administrator accounts, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Select the user.
4. Click **Settings** > **Enable MFA**.

For Security Officer accounts, multi-factor authentication is always enabled.



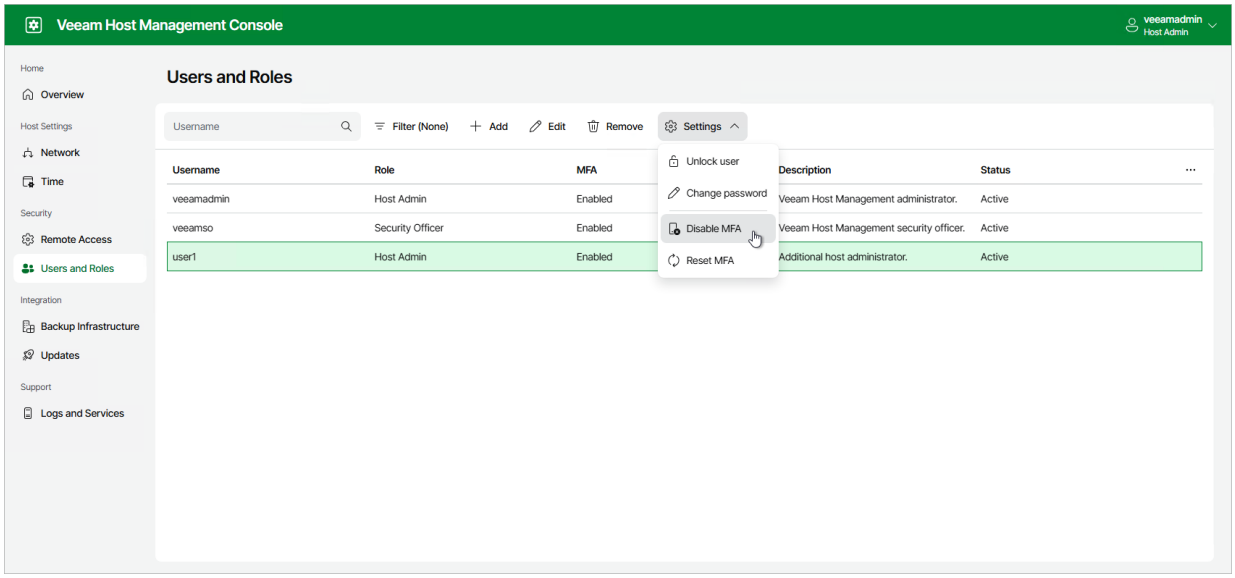
Disabling Multi-Factor Authentication

To disable multi-factor authentication for Host Administrator accounts, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.

3. Select the user.
4. Click **Settings** > **Disable MFA**.

For Security Officer accounts, multi-factor authentication cannot be disabled.



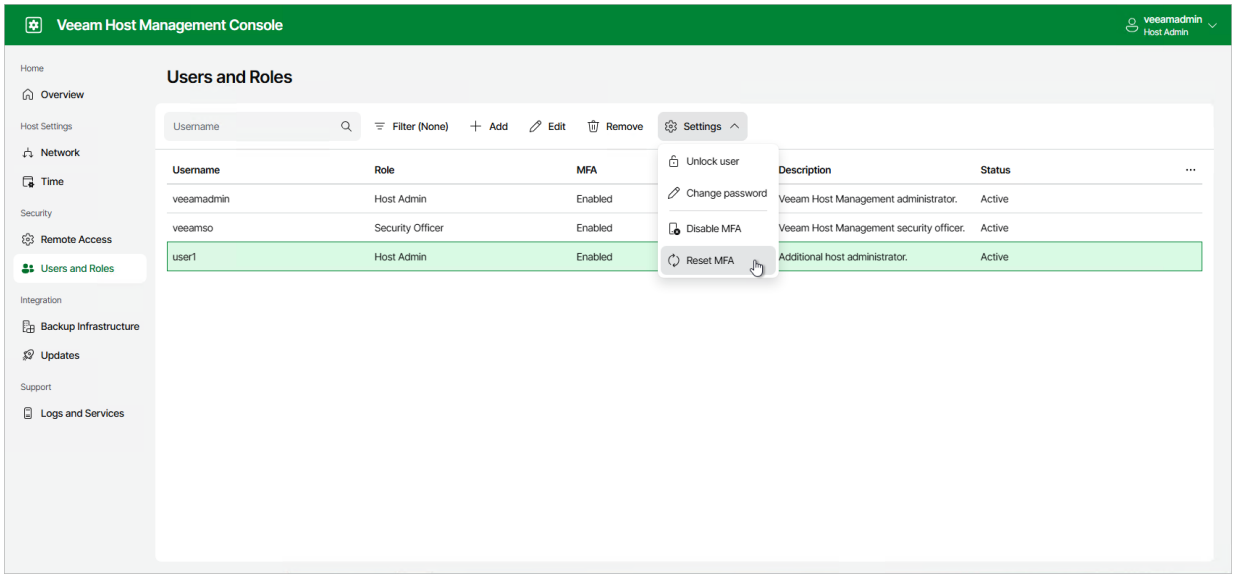
Resetting Multi-Factor Authentication

To reset multi-factor authentication for Host Administrator accounts, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Select the user.
4. Click **Settings** > **Reset MFA**.

Alternatively, you can reset multi-factor authentication through the password reset operation. For more information, see Resetting Passwords.

> **NOTE**
>
> A Host Administrator cannot reset multi-factor authentication for Security Officers. To do this, a Security Officer must use a recovery token. For more information, see Using Recovery Token.



Resetting Passwords

A Host Administrator can reset passwords for users including other Host Administrators to solve the following authentication issues:

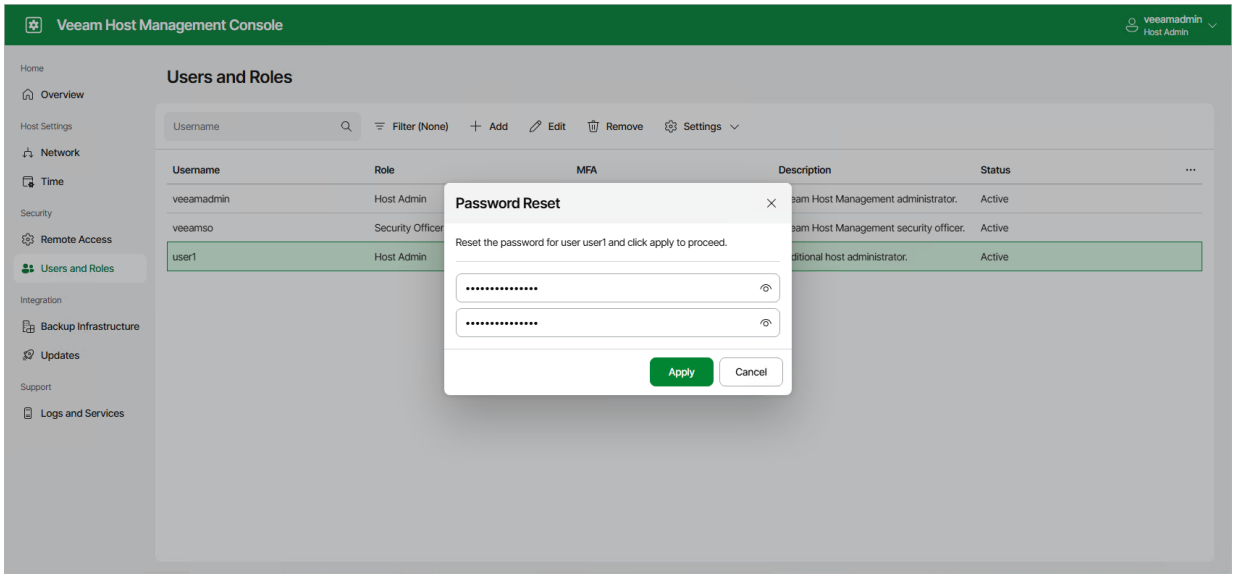
- A user account is locked after three failed login attempts.
- A user lost or forgot their password.
- A user lost or changed a mobile device with the mobile authentication application and does not have a code for multi-factor authentication.

> **NOTE**
>
> A Host Administrator cannot reset passwords for Security Officers. To do this, a Security Officer must use a recovery token. For more information, see Using Recovery Token.

To reset a user account password, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Users and Roles**.
3. Select the user.
4. Click **Settings** > **Change password**.

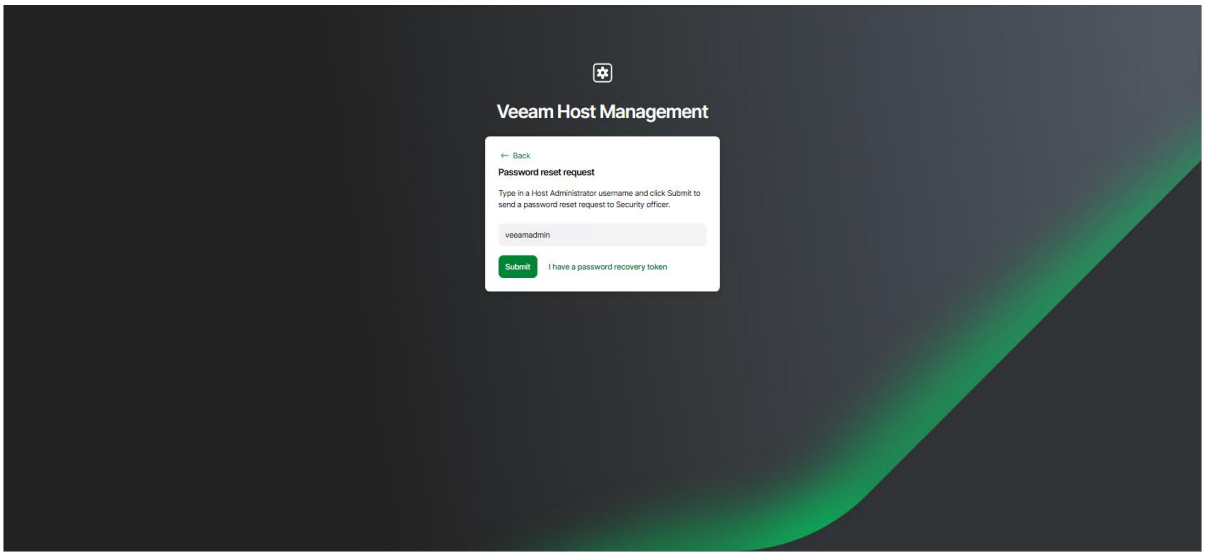
5. Specify a new password and click **Apply**. After password reset, the user will also need to set up multi-factor authentication.



If you are the only Host Administrator and you have authentication issues, you can reset your password in one of the following ways:

- If you did not configure the Security Officer account during the Veeam Software Appliance installation, you can only use Veeam LiveOS to restore access to the Veeam Host Management console. For more information, see this KB article.
- If you configured the Security Officer account, you can reset the Host Administrator password through the authorization request. To do this, perform one of the following operations:
  - On the Veeam Host Management web UI sign-in page, click **Forgot password?**, specify your user name and click **Submit**.
  - On the Veeam Host Management TUI logon screen, specify your user name and press [F2].

  After the Security Officer approves the request, the next time you log in you will also need to set up multi-factor authentication.



Managing Certificates

Users with Host Administrator permissions can manage the following certificates in the Veeam Host Management web UI:

- *Host management certificate* — secures the connection between the web browser and the Veeam Host Management web UI.
- *Trusted certificates* — allow the appliance to trust 3rd party servers and services, such as a syslog server that uses a custom TLS certificate.

> **NOTE**
>
> Before you manage certificates in the Veeam Host Management web UI, consider the following:
>
> - Changing the host management certificate or adding a trusted certificate requires Security Officer approval. For more information, see Performing Security Officer Tasks.
> - The file name of the certificate must be less than 255 characters.
> - The file name must contain only ASCII symbols.

Host Management Certificate

By default, the appliance uses a self-signed certificate. You can replace it with your own certificate or generate a new self-signed certificate to rotate the current one.

After the certificate is updated, the Veeam Host Management web UI restarts automatically and you are signed out.

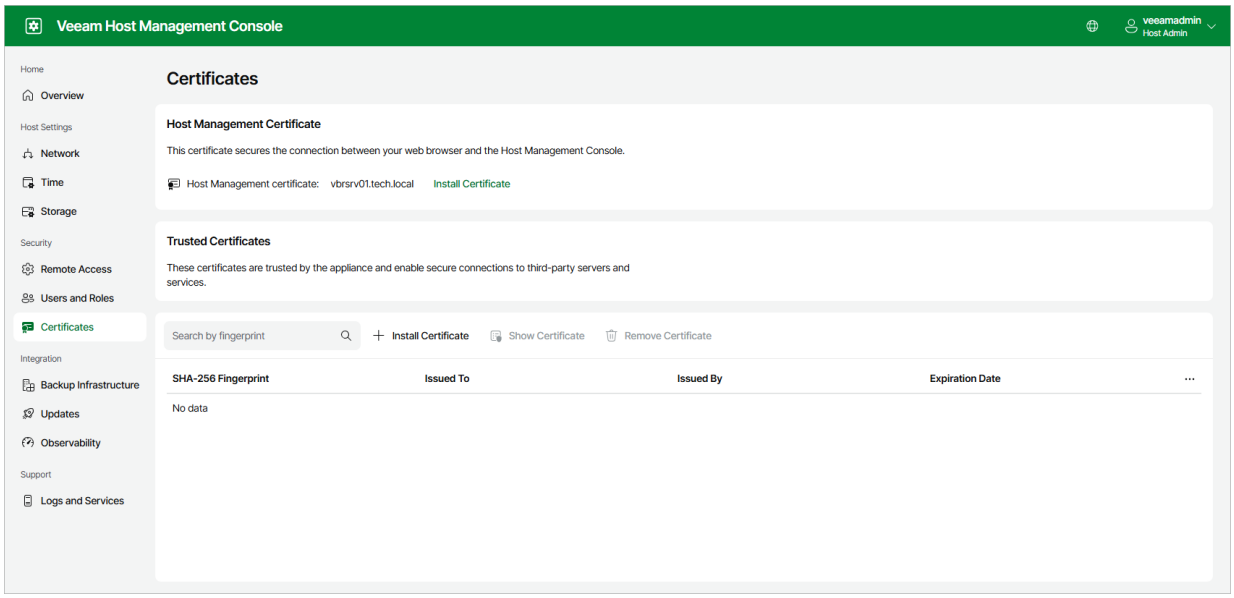
To install your own certificate, do the following:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Certificates**.
3. In the **Host Management Certificate** section, click **Install Certificate**.
4. At the **Certificate Source** step, select **Upload a new certificate** and click **Next**.
5. At the **Choose Certificate** step, select the certificate file in the `.crt`, `.cer`, `.pem`, or `.der` format. If the private key is in a separate file, also select the `.pem` key file and, if it is protected, enter its password. Click **Next**.
6. At the **Summary** step, review the certificate details and click **Finish**.

To generate a new self-signed certificate, do the following:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Certificates**.
3. In the **Host Management Certificate** section, click **Install Certificate**.
4. At the **Certificate Source** step, select **Generate a self-signed certificate** and click **Next**.
5. At the **Generate Certificate** step, enter a friendly name for the certificate and click **Next**.
6. At the **Summary** step, review the certificate details and click **Finish**.

> **IMPORTANT**
>
> A custom certificate is not regenerated if the host name changes or the appliance joins a domain. Make sure the certificate contains the correct fully qualified domain name (FQDN) of the appliance.



Trusted Certificates

If the appliance must connect to a 3rd party server or service that uses a certificate it does not already trust, you must add that certificate to the trusted store.

To do this, do the following:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Certificates**.
3. In the **Trusted Certificates** section, click **Install Certificate**.
4. At the **Choose Certificate** step, select the certificate file in the `.crt`, `.cer`, `.pem`, or `.der` format. Click **Next**.
5. At the **Summary** step, review the certificate details and click **Finish**.

To view or remove a trusted certificate, select it in the list and click **Show Certificate** or **Remove Certificate**.

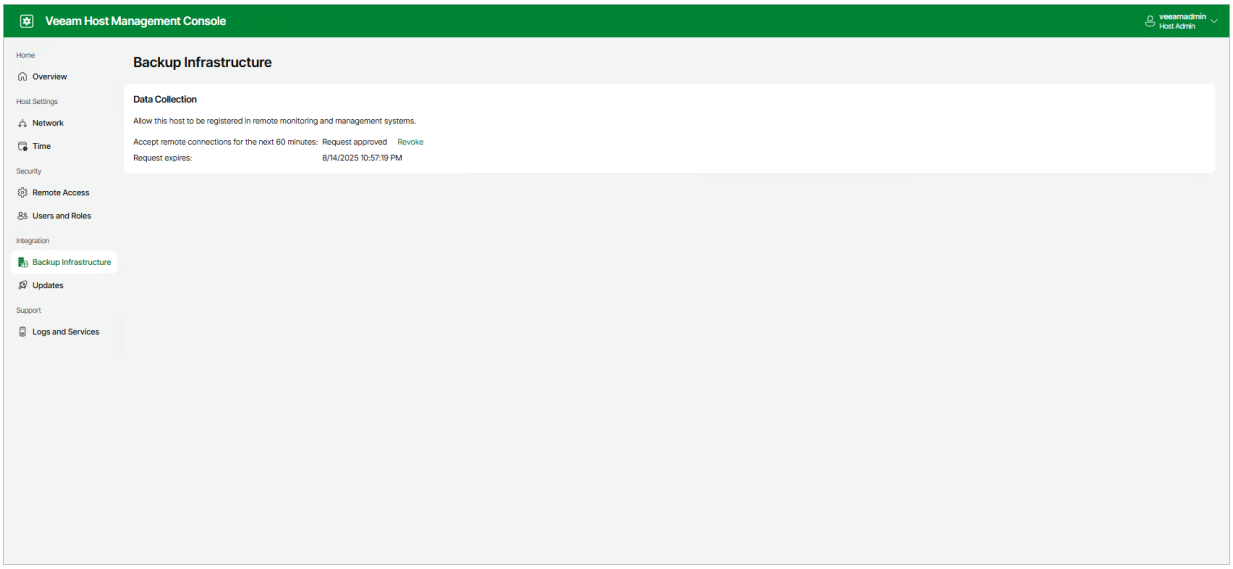
To find a certificate, enter its fingerprint in the search box.

Configuring Backup Infrastructure Settings

To collect data remotely, other Veeam monitoring and data management solutions including Veeam ONE, Veeam Recovery Orchestrator and Veeam Service Provider Console must install their agents on Veeam Software Appliance. By default, this operation is prohibited. To allow remote data collection, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator.
2. In the management pane, click **Backup Infrastructure**.
3. In the **Data Collection** section, click **Submit Request**:
   - If you did not configure the Security Officer account during the Veeam Software Appliance installation, remote connections for Veeam Agents will be allowed immediately for 60 minutes.
   - If you configured the Security Officer account, remote connections for Veeam Agents will be allowed for 60 minutes after the Security Officer approves the request.

If required, you can revoke permission before expiration. To do this, click **Revoke**.



Managing Updates

For more information on how to check for and install Veeam Software Appliance updates through Veeam Host Management console, see Veeam Software Appliance Update.

Performing Maintenance Tasks

Users with Host Administrator permissions can perform the following maintenance tasks:

- View system resource usage
- Start, stop and restart Veeam services
- Restart Veeam Software Appliance
- Import and export configuration files
- Manage Veeam components
- View and export Veeam Software Appliance events
- Download logs
- Change the logs directory
- Reset time shift protection on a Veeam Software Appliance

Viewing Resource Usage

You can monitor the CPU, memory, and storage usage of the appliance on the **Overview** page.

For detailed storage usage per volume, see Managing Storage.

Managing Veeam Services

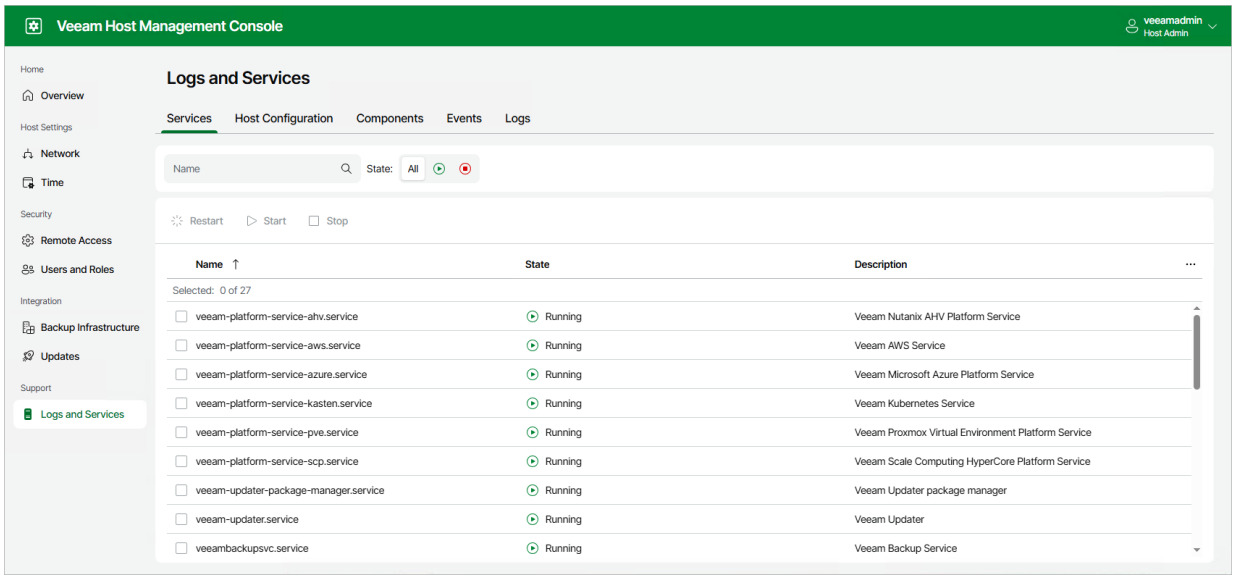
You can monitor and manage Veeam services in the Veeam Host Management web UI.

For more information, see Enterprise Manager Components.

To start, stop or restart a Veeam service, do the following:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Logs and Services**.
3. Open the **Services** tab.
4. Select the service in the list. To select several services, hold [Ctrl] and click each one.

5. Click **Start**, **Stop** or **Restart**.

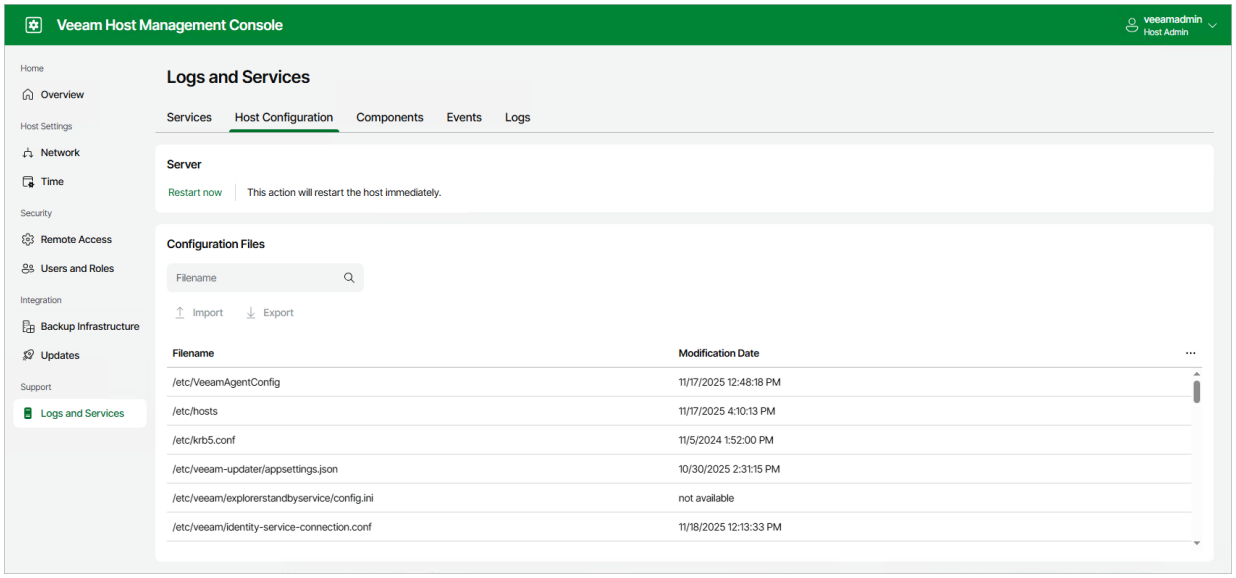


Restarting Appliance

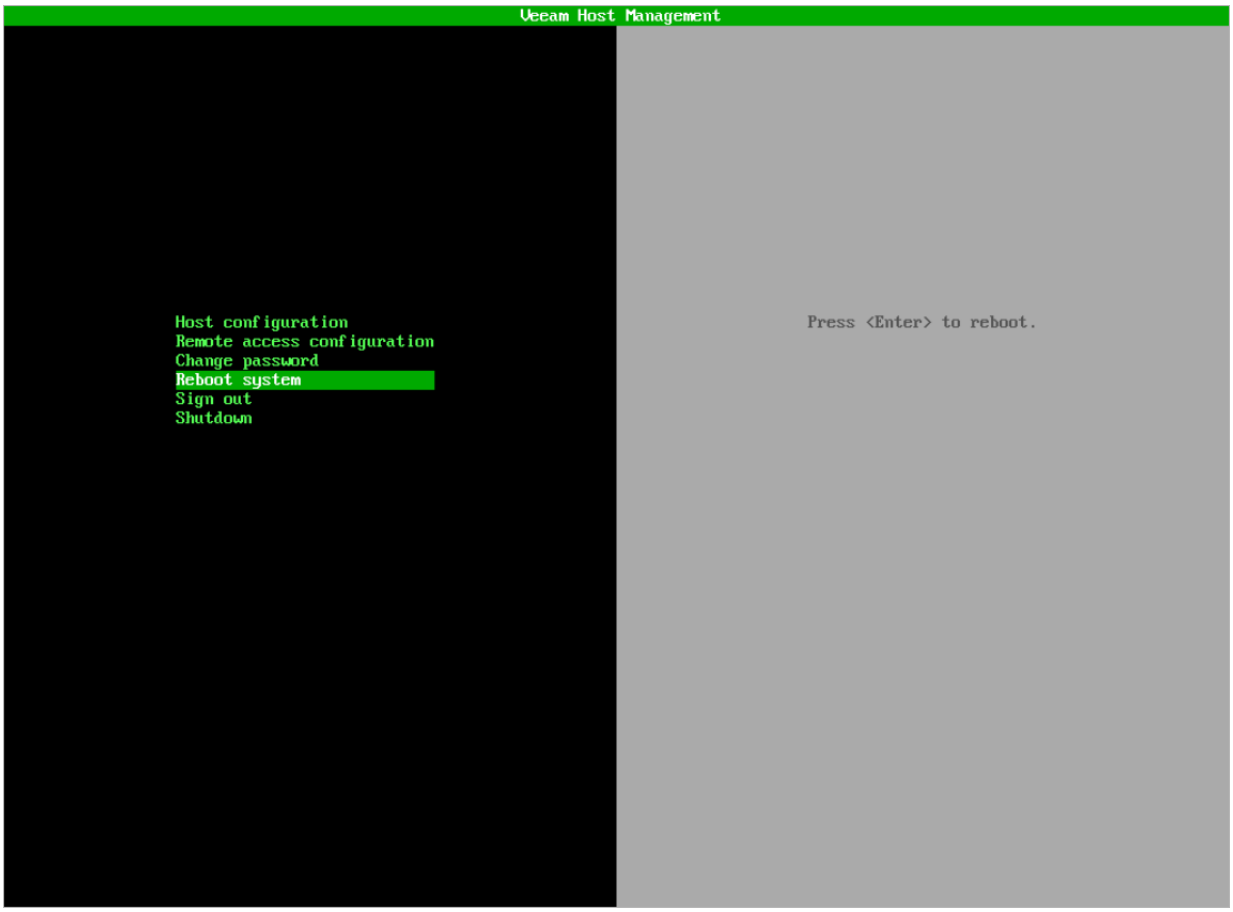
You can restart Veeam Software Appliance in the Veeam Host Management web UI or TUI.

If you use the Veeam Host Management web UI, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Logs and Services**.
3. On the **Host Configuration** tab, click **Restart now**.



If you use the Veeam Host Management TUI, in the main menu, select **Reboot system** and press [Enter].

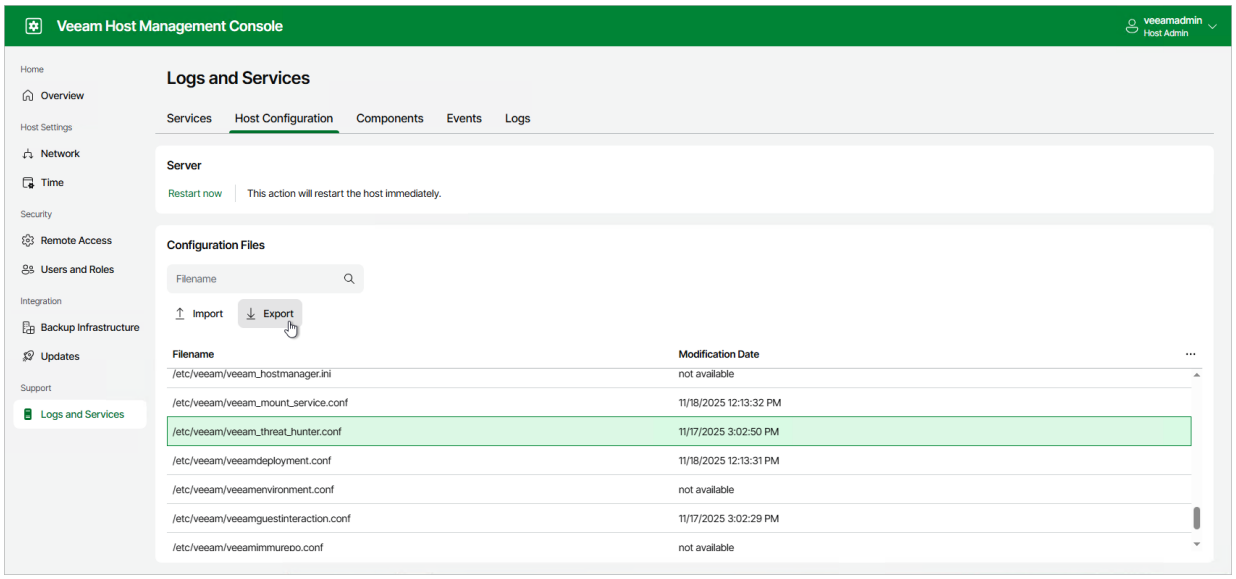


Managing Configuration Files

You can export and import required configuration files to customize Veeam Software Appliance configuration. To do this, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Logs and Services**.
3. On the **Host Configuration** tab, select the file in the **Configuration Files** section and click **Export**.
4. After you edit the file and update configuration parameters, click **Import** to upload the updated file.

It is strongly recommended that you restart the server after you apply a new configuration.

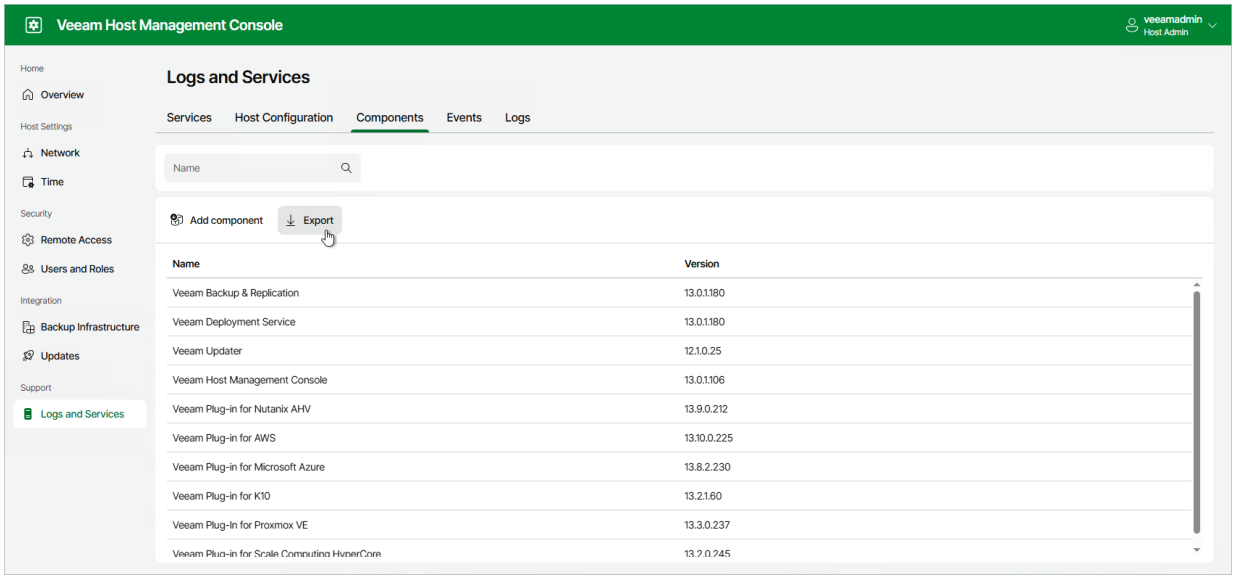


Managing Veeam Components

You can manage components installed on the Veeam Software Appliance. To view the list of components, log in to the Veeam Host Management web UI as a Host Administrator and click **Logs and Services** in the management pane. Then, click the **Components** tab.

Components and their versions are updated automatically when you add backup infrastructure components through the Veeam Backup & Replication console or install updates and hotfixes. You can also add a component manually. To do this, click **Add component**, select an installation package and click **Upload**.

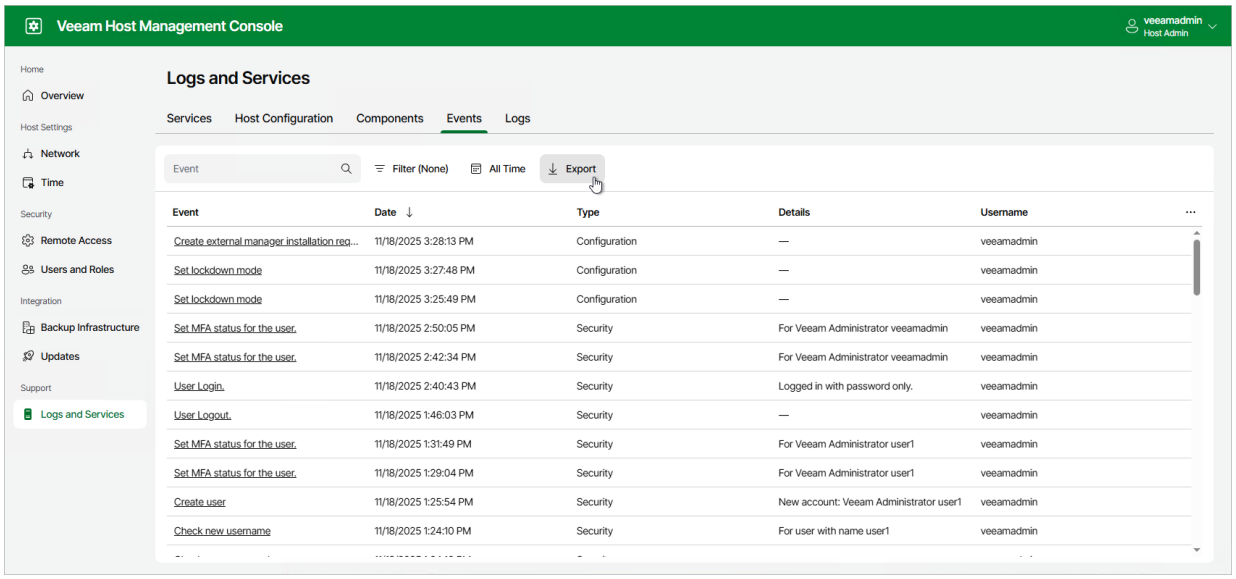
To export all components in the CSV format, click **Export**.



Viewing Appliance Events

You can monitor system, security, configuration and other types of events that occurred on the Veeam Software Appliance. To view the list of events, log in to the Veeam Host Management web UI as a Host Administrator and click **Logs and Services** in the management pane. Then, click the **Events** tab.

To export all events in the CSV format, click **Export**.

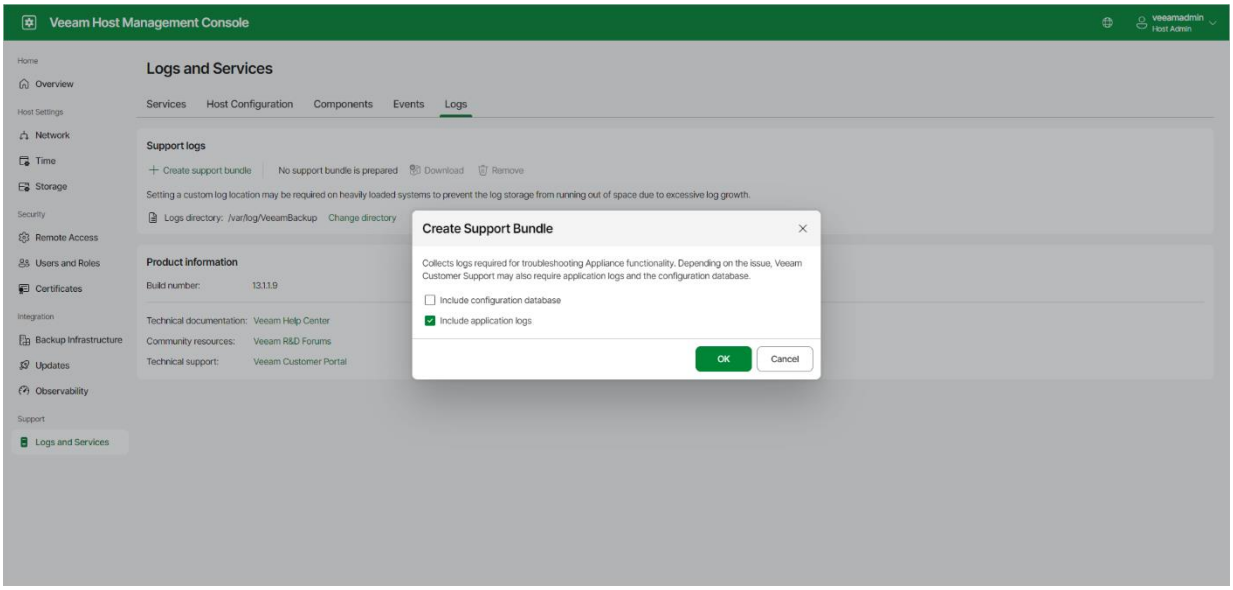


Downloading Logs

For troubleshooting, you can download all Veeam logs as an archive file. To do this, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Logs and Services**.
3. On the **Logs** tab, click **Create support logs bundle**.
4. To include operating system and Veeam logs in the archive, make sure that the **Include application logs** check box is selected. You can also select the **Include configuration database** check box to add a configuration database file to the archive.
5. Click **OK**.
6. When the archive is prepared, click **Download**.

> **TIP**
>
> Consider the following:
>
> - After you download the archive, you can delete it from the server. To do this, click **Remove**.
> - For more information on how to attach logs to a Veeam support case, see this KB article.



Changing Logs Directory

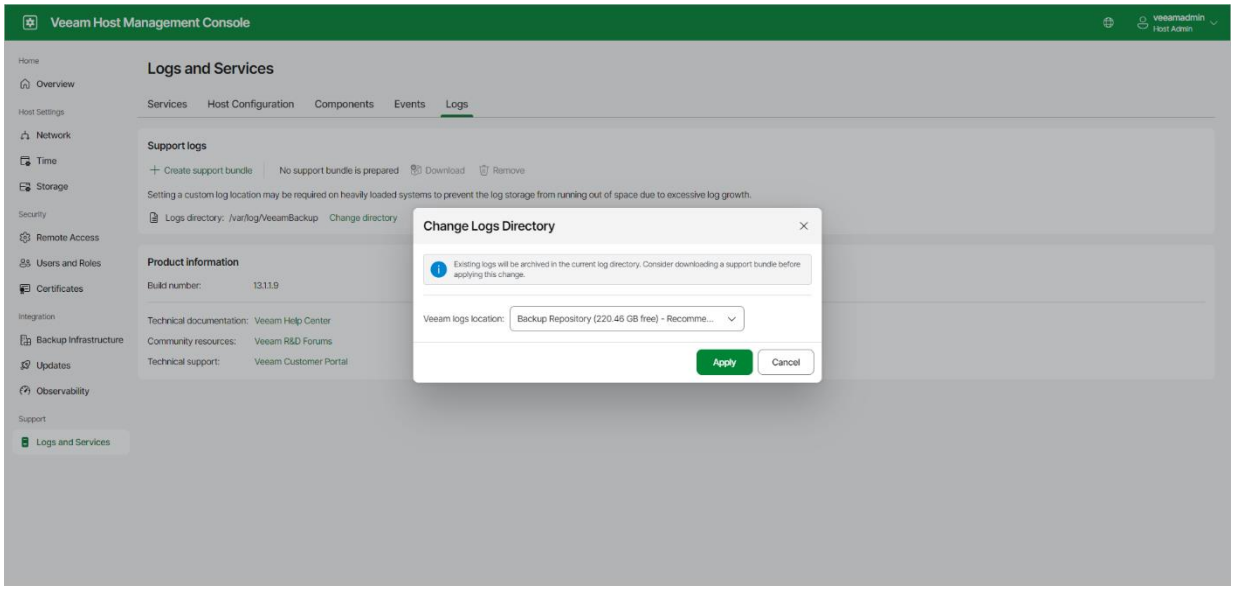
You can change the directory where Veeam logs are stored on the appliance.

> **IMPORTANT**
>
> Before you change the logs directory, consider the following:
>
> - Only new logs are written to the new directory. Existing logs are archived in the previous directory and remain on the previous volume.
> - Changing the logs directory restarts Veeam services, and running backup jobs may be interrupted.
> - It is recommended that you download a support bundle before you change the directory.

To change the logs directory, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the management pane, click **Logs and Services**.
3. On the **Logs** tab, click **Change directory**.
4. In the **Change Logs Directory** window, select the location where you want to store the logs. The list shows the locations available for Veeam logs and the free space on each.
5. Click **Apply**.

6. In the **Confirm Log Location Change** window, click **Apply**. The operation may take several minutes to complete.

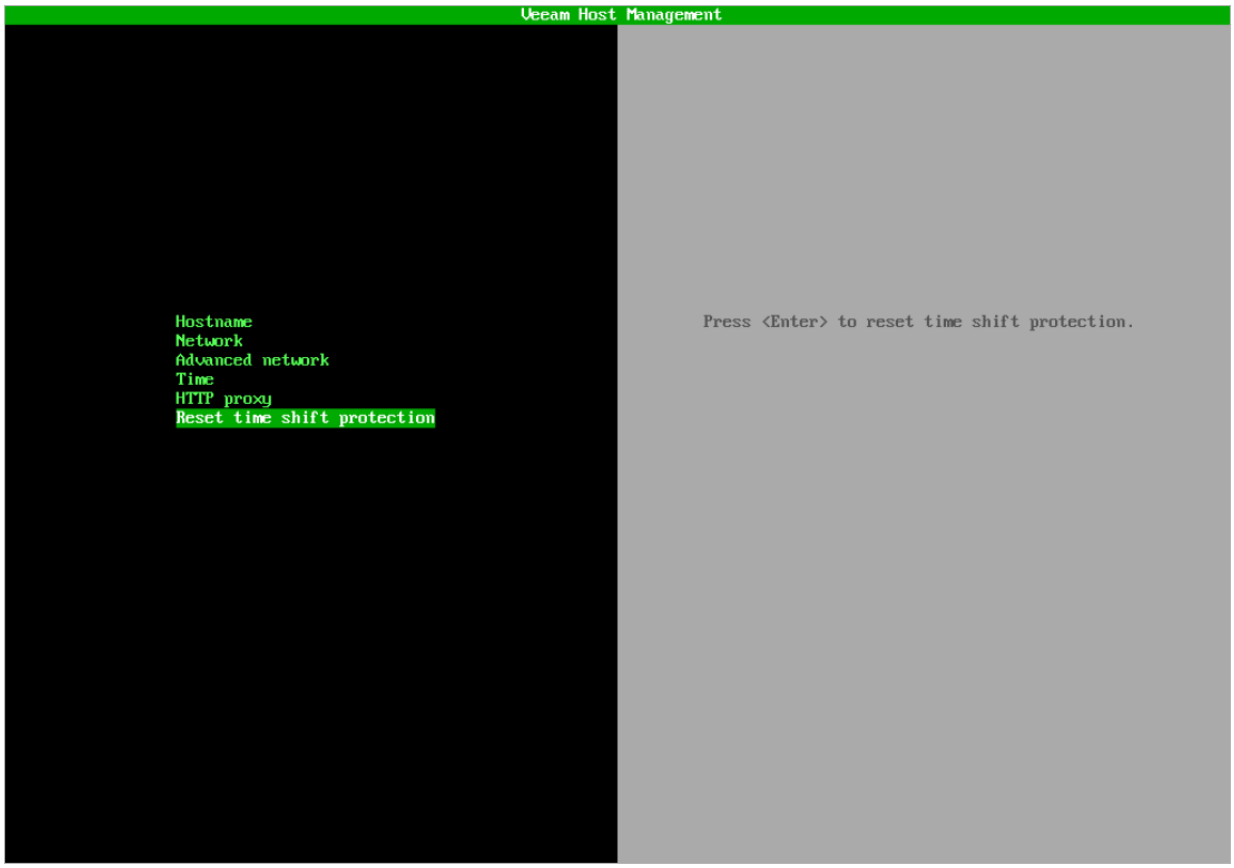


Resetting Time Shift Protection

In the Veeam Host Management TUI, you can reset the time shift protection on a Veeam Software Appliance. To do this, perform the following steps:

1. Log in to the Veeam Host Management TUI as a Host Administrator. For more information, see Accessing Veeam Host Management Console.
2. In the main menu, select **Host configuration**.
3. Select **Reset time shift protection**.

For more information on time shift protection, see How Immutability Works.



Performing Security Officer Tasks

Users with Security Officer permissions can perform the following tasks in the Veeam Host Management web UI:

- Approve or decline authorization requests
- View authorization request events
- Reset own password
- Reset MFA
- Reset password recovery token
- Approve or decline remote password reset
- Use password recovery token to resolve authentication issues
- View and export Veeam Software Appliance events

Managing Authorization Requests

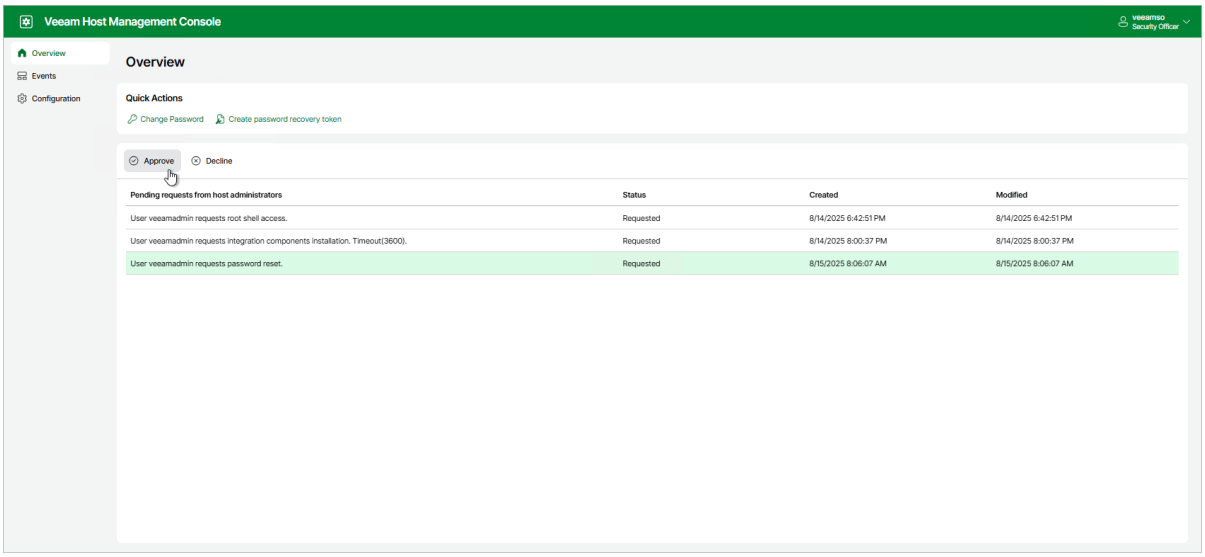
You can approve or decline the following requests from Host Administrators:

- Enable SSH
- Stop a Veeam service
- Grant temporary root access
- Reset password for the locked user
- Import configuration files
- Change a domain membership
- Add a Security Officer account
- Allow remote connections for Veeam Agents

To manage authorization requests, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Security Officer.
2. In the management pane, click **Overview**.

3. Select the request and click **Approve** or **Decline**.



Viewing Authorization Request Events

Events related to Security Officer authorization requests include information about:

- Approved and rejected requests
- Locked and unlocked Host Administrator accounts

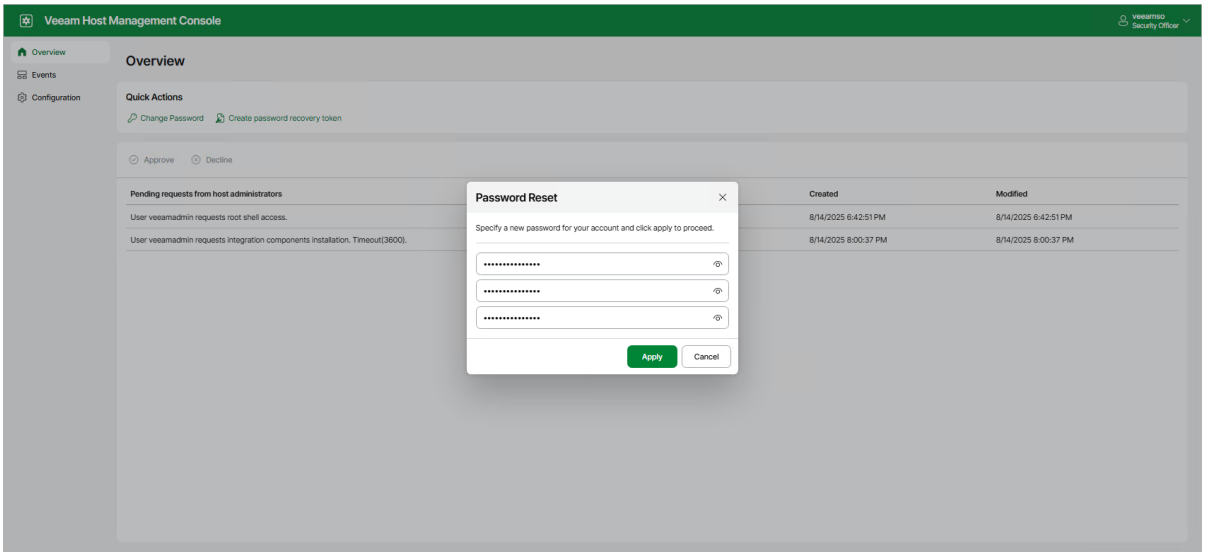
As a Security Officer, you can view these events in the Veeam Host Management web UI. For more information, see Viewing Appliance Events.

Resetting Own Password

As a Security Officer, you can reset your password in the Veeam Host Management web UI. To do this, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Security Officer.
2. In the management pane, click **Overview**.
3. Click **Change password**.
4. Specify the current password and a new password and click **Apply**.

> **NOTE**
>
> If you forgot or lost the password, or your Security Officer account is locked after three failed login attempts, you can use a recovery token to restore access to your account. For more information, see Using Recovery Token.



Resetting MFA

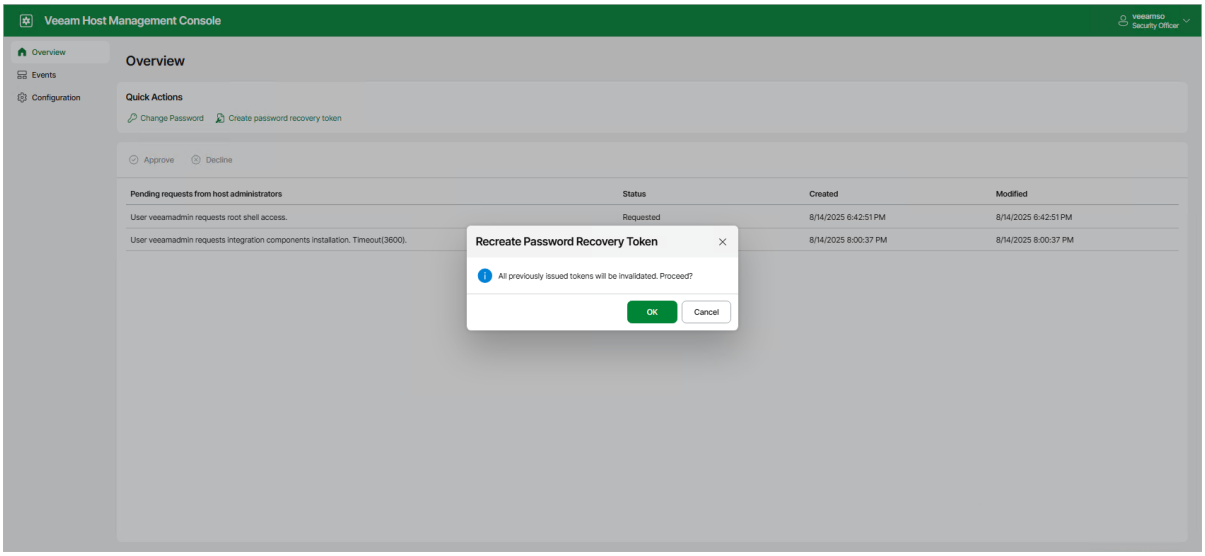
If you have multi-factor authentication issues, lose or change a mobile device with the mobile authentication application, you can use a recovery token to restore access to your account. For more information, see Using Recovery Token.

Resetting Password Recovery Token

You can reset your current password recovery token. To do this, perform the following steps:

1. Log in to the Veeam Host Management web UI as a Security Officer.
2. In the management pane, click **Overview**.
3. Click **Create password recovery token** and confirm the operation.
4. Enter a 6-digit confirmation code generated in the mobile authenticator application.
5. Copy the new recovery token and save it in a secure place.

> **NOTE**
>
> A new recovery token is also generated when you use your current recovery token to resolve authentication issues. For more information, see Using Recovery Token.



Approving or Declining Remote Password Reset

If remote password resets are enabled and a Host Administrator forgets their password or cannot log in to the Veeam Host Management web UI, they can request a password reset.

To approve or decline a password reset request, perform the following steps:

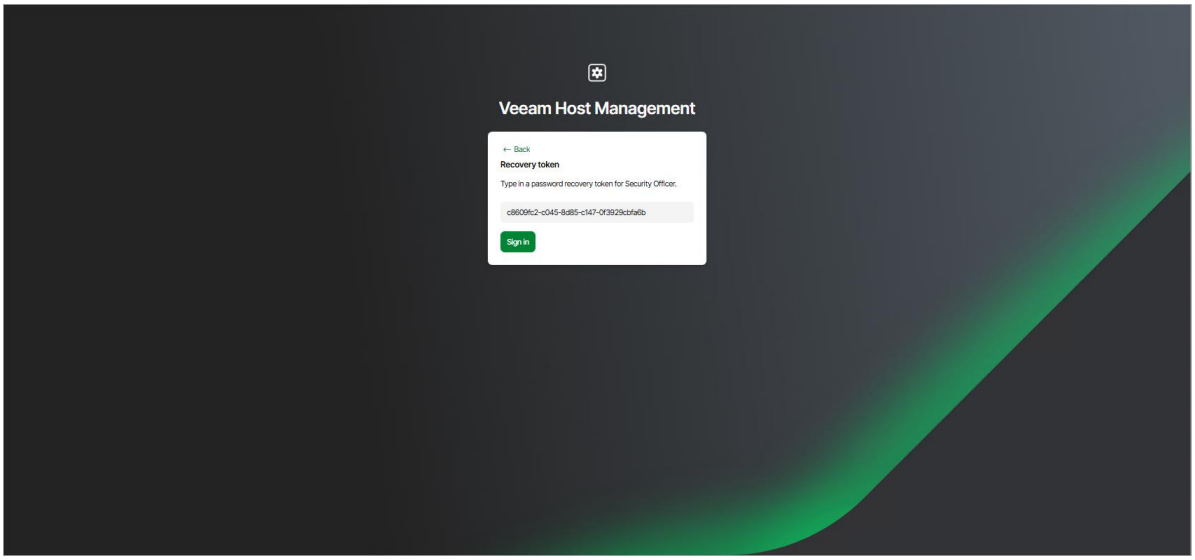
1. Log in to the Veeam Host Management web UI as a Security Officer.
2. In the management pane, click **Overview**.
3. In the list of pending requests, select the password reset request and click **Approve** or **Decline**.
4. If you approve the request, in the **Password Reset** window, specify a new password in the **New password** and **Repeat password** fields and click **Apply**.
5. Provide the new password to the Host Administrator. They will be prompted to specify a new password the next time they log in.

Using Recovery Token

If you forgot or lost the password, your Security Officer account is locked after three failed login attempts, or you have multi-factor authentication issues, you can restore access through the recovery token generated during the initial Security Officer logon. To do this, perform the following steps:

1. In the Veeam Host Management web UI sign-in page, click **Forgot password?**.
2. Click **I have a password recovery token**.
3. Specify your recovery token and click **Sign in**.
4. Complete the Security Officer Initialization wizard to enter a new password, set up multi-factor authentication and get a new recovery token.
5. Click **Finish**.

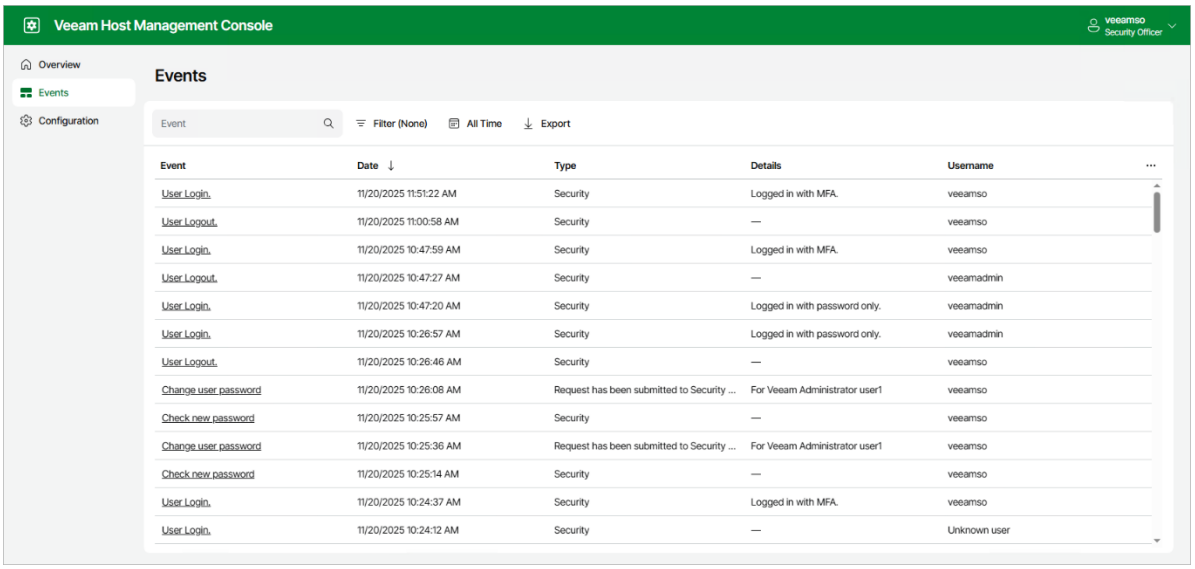
> **NOTE**
>
> If multi-factor authentication was disabled in the **Initial Configuration** wizard, the MFA setup step of the Security Officer Initialization wizard is skipped.



Viewing Appliance Events

You can monitor system, security, configuration and other types of events that occurred on the Veeam Software Appliance. To view the list of events, log in to the Veeam Host Management web UI as a Security Officer and click **Events** in the management pane.

To export all events in the CSV format, click **Export**.



Accessing Enterprise Manager

You can access Veeam Backup Enterprise Manager using Enterprise Manager credentials or single sign-on (SSO).

When you open Enterprise Manager for the first time, you must log in as a user with administrative privileges:

- For Microsoft Windows-based Enterprise Manager, enter credentials of a user account with local administrative rights or the account that was used to install Enterprise Manager.
- For Linux-based Enterprise Manager, log in using the *veeamadmin* account.

To access the Veeam Backup Enterprise Manager website, follow these steps:

1. Open your browser and enter the Enterprise Manager URL in one of the following formats:
   - For Microsoft Windows-based Enterprise Manager:

     ```
     https://<hostname>:9443
     ```

   - For Linux-based Enterprise Manager (the port number is optional):

     ```
     https://<hostname>:443
     ```

   If you cannot access the website over HTTPS, possible causes may include configuration or connectivity issues. For more information, see this Veeam KB article.
2. From the language drop-down list, select the desired display language. For details on adding new languages, see Managing Languages.
3. Log in to Enterprise Manager:
   - To log in with Enterprise Manager credentials:
     i. In the **Username** and **Password** fields, specify your Enterprise Manager credentials. To log in to a Microsoft Windows-based Enterprise Manager with a domain account, enter the user name in the *DOMAIN|Username* format. To log in to a Linux-based Enterprise Manager with a domain account, enter the user name in the UPN format.
     ii. To save the entered credentials for future access, select the **Remember me** option.
     iii. Click **Sign in**.
   - To log in with the credentials of the Microsoft Windows account that you are currently signed in on the machine where you are launching Enterprise Manager, click **Sign in as current user** option.
   - To log in with SSO, click **Sign in with SSO**. Enterprise Manager will redirect you to the login webpage of the single sign-on service. Complete the sign-in procedure on the login page. If the account is already authenticated in the single sign-on service, you will immediately access the Enterprise Manager website.

     The **Sign in with SSO** option is available if SAML authentication is configured for Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.

> **NOTE**
>
> If you log in under a user account that is not assigned an Enterprise Manager role, you will be automatically redirected to the Veeam Self-Service File Restore Portal. On this portal, you can browse and restore only machines on which your user account has local administrative rights. For more information on configuring Enterprise Manager security roles, see Configuring Accounts and Roles.

After you finish working with Enterprise Manager, or if you need to switch user accounts, click the user name in the upper-right corner of the main window and then click **Sign Out**.

Related Topics

- Exploring Enterprise Manager
- Configuring Accounts and Roles

Exploring Enterprise Manager

The user interface of Veeam Backup Enterprise Manager consists of two views.

- The **Home** view allows you to view on-going statistics on added backup servers, manage jobs and CDP policies, and perform recovery operations.
- The **Configuration** view allows you to add backup servers to Enterprise Manager, modify Enterprise Manager settings, and configure self-service restore portals.

> **TIP**
>
> To open online help, click the question mark at the top-right of the window. You will be redirected to the section of the user guide that explains the features and options available on the open tab.

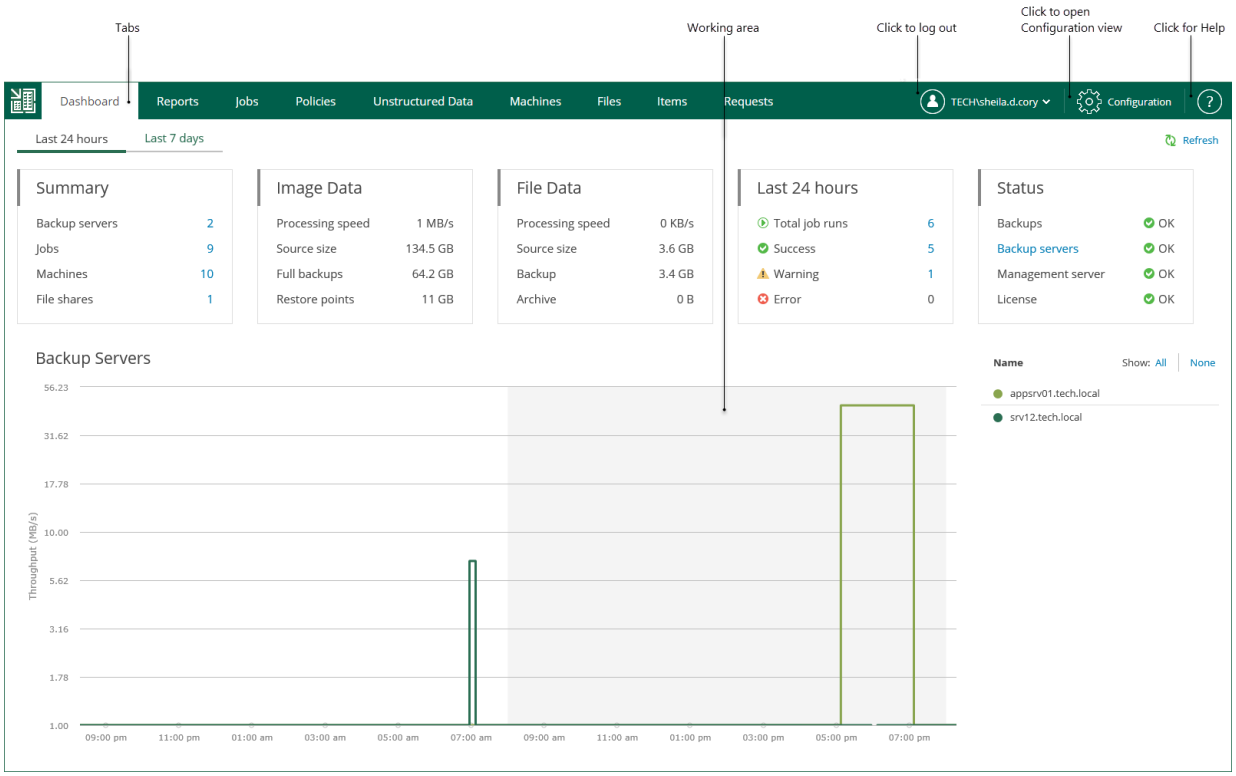
Home View

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 Configuring Accounts and Roles.

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

- View on-going statistics for your backup infrastructure using the **Dashboard** tab. For more information, see Viewing Dashboard.
- View detailed information about backup servers managed by Enterprise Manager using the **Reports** tab. For more information, see Reports on Backup Servers.
- Manage jobs on all managed backup servers using the **Jobs** tab. For more information, see Managing Jobs.
- Manage CDP policies on all managed backup servers using the **Policies** tab. For more information, see Managing CDP Policies.
- Browse for unstructured data backups, search for specific items, delete file shares and recover items from unstructured data backups using the **Unstructured Data** tab. For more information, see Working with Unstructured Data.
- Browse for machine backups, search for machines, delete machines and perform failover and replication operations with managed virtual or physical machines using the **Machines** tab. For more information, see Working with Machines.
- Browse the guest OS file system in a machine backup, search for guest OS files and restore necessary files using the **Files** tab. For more information, see Guest OS File Restore.

- Perform item-level recovery from application-aware backups created by Veeam Backup & Replication using the **Items** tab. For more information, see Application Item Restore.



Configuration View

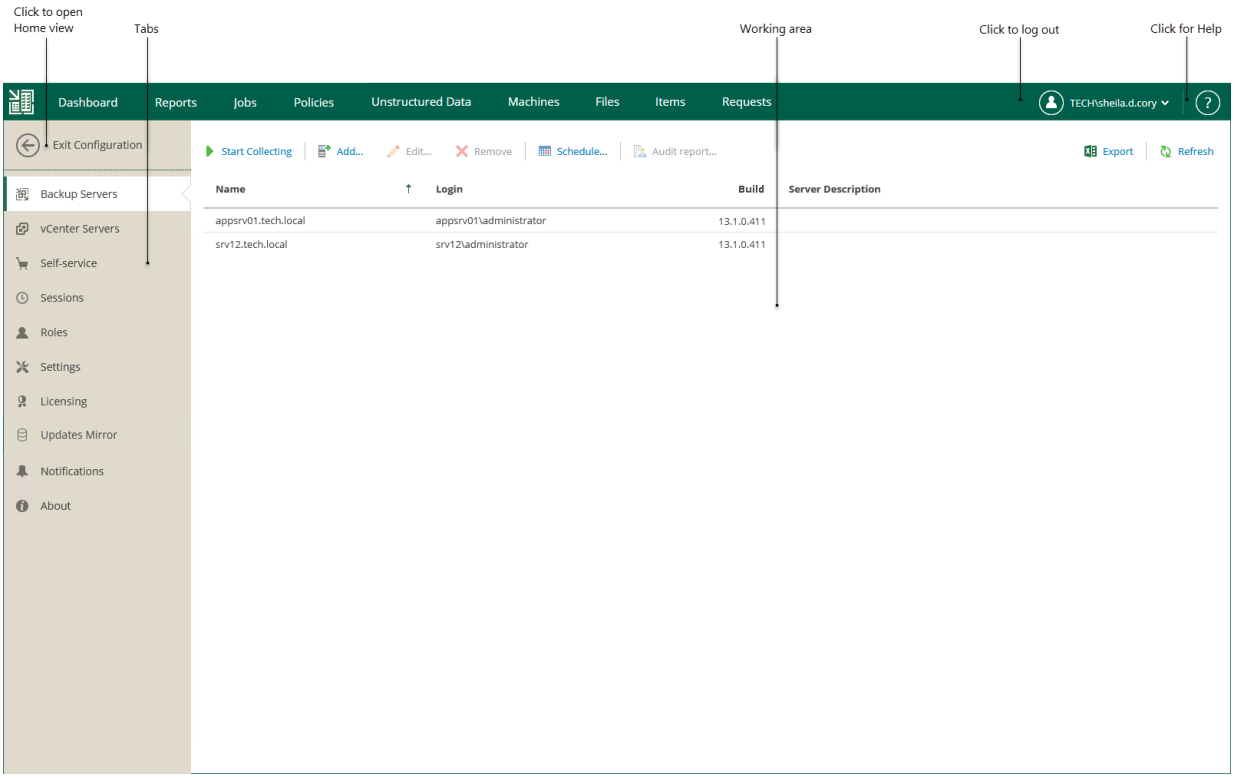
If you log in with an administrative account, you can click **Configuration** to open the **Configuration** view.

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

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

- Add, edit or remove Veeam Backup servers using the **Backup Servers** tab. For more information, see Managing Backup Servers.
- Work with vCenter Servers managed by Enterprise Manager using the **vCenter Servers** tab. For more information, see Viewing vCenter Servers.
- Manage VMware Cloud Director organizations and vSphere tenant accounts using the **Self-Service** tab. For more information, see Veeam Self-Service Backup Portal for Cloud Director and vSphere Self-Service Backup Portal.
- View and manage data collection job sessions using the **Sessions** tab. For more information, see Collecting Data from Backup Servers.
- Configure Enterprise Manager security roles using the **Roles** tab. For more information, see Configuring Accounts and Roles.
- Configure Enterprise Manager settings using the **Settings** tab. For more information, see Managing Encryption Keys, Configuring SAML Authentication Settings, Customizing Dashboard Chart and Configuring Retention Settings for Index and History.

- Manage licenses and view detailed reports on license consumption using the **Licensing** tab. For more information, see Licensing.
- Set email notifications using the **Notifications** tab. For more information, see Configuring Notification Settings.
- View product versions, URLs and log locations using the **About** tab. For more information, see Viewing Information About Enterprise Manager.



Viewing Dashboard

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

Backup Servers Statistics

Veeam Backup Enterprise Manager displays on-going statistics on backup servers, their jobs, processed machines and file shares as well as data size, processing speed and so on.

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

- Last 24 hours
- Last 7 days

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

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

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

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

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

The **File Data** widget contains the following information about unstructured data backups:

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

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

- *Total job runs* — total number of job runs.
- *Success* — number of jobs completed successfully.
- *Warning* — number of jobs completed with a warning.
- *Error* — number of failed jobs.

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

- *Backups* — status of backups that are verified by SureBackup jobs.
- *Backup servers* — status of the last collection job session.
- *Management server* — status of the Veeam Backup Enterprise Manager management server.
- *License* — status of licenses.
  - *OK* — current license is valid
  - *Warning* — working in grace period, or failed to update the license
  - *Error* — license is expired, and grace period is over

You can use the links in these blocks to drill down into detailed reports on specific aspects of the backup infrastructure.

Backup Servers Chart

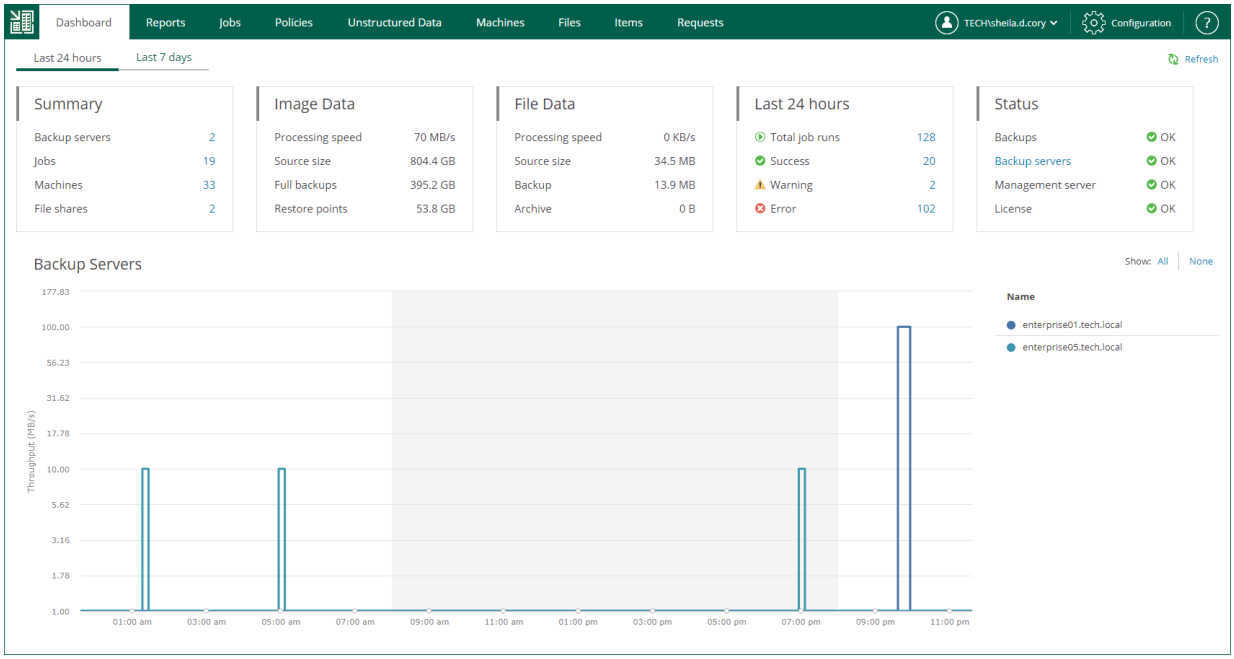
The **Backup Servers** chart shows date and time when backup jobs were performed, and the network throughput rate during the backup jobs. Jobs related to each backup server have their own color on the chart. The legend on the right interprets the color scheme used for all backup servers added to the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

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

- Last 24 hours
- Last 7 days

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

In the **Last 24 hours** view, the highlighted part of the chart represents the configured backup window. You can configure the backup window in the chart settings. For more information, see Customizing Dashboard Chart.



Configuring Enterprise Manager

As part of the Veeam Backup Enterprise Manager configuration process, you can perform the following tasks:

- Manage backup servers
- Collect data from backup servers
- View vCenter Servers and install Veeam plug-in for vSphere Client on necessary servers
- Configure retention settings for index and history
- Configure Enterprise Manager accounts and roles
- Configure SAML authentication settings
- Configure notification settings
- Install TLS Certificates
- Manage display languages

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

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

Initial Configuration

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

1. Log in to the Veeam Backup Enterprise Manager website. For more information, see Accessing Enterprise Manager.
2. Add backup servers you want to manage. For more information, see Adding Backup Servers.
3. Retrieve data from added backup servers. For more information, see Collecting Data from Backup Servers.
4. Assign the Portal Administrator, Restore Operator or Portal User roles to users who will work with Veeam Backup Enterprise Manager. For more information, see Configuring Accounts and Roles.
5. Provide email notification settings to be able to receive emails with summary on performed backup and replication jobs, lab request status changes and file restore operations. For more information, see Configuring Notification Settings.

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

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

Related Topics

- Configuring Retention Settings for Index and History
- Viewing Dashboard

Managing Backup Servers

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

In This Section

- Adding Backup Servers
- Editing Backup Servers
- Removing Backup Servers
- Collecting Data from Backup Servers
- Reports on Backup Servers
- Audit Reports

Adding Backup Servers

Veeam Backup Enterprise Manager allows you to manage jobs across multiple backup servers and perform recovery operations within a single application. To retrieve information about configured jobs and backup infrastructure of added backup servers, Enterprise Manager runs a data collection job. For more information, see Collecting Data from Backup Servers.

Before You Begin

Before you add backup servers, consider the following:

- You cannot add a backup server that is running a newer version than Enterprise Manager. The Enterprise Manager version must be equal to or later than the version of any backup server that you want to add. Before adding a backup server of a newer version, upgrade Enterprise Manager first. For details, see Veeam Software Appliance Update or Upgrading to Enterprise Manager 13.1.
- Enterprise Manager supports adding backup servers running Veeam Backup & Replication 12.3 or later. When Enterprise Manager and Veeam Backup & Replication run different major or minor versions, some Enterprise Manager features may not be available:
  - Enterprise Manager does not support editing jobs that are managed by backup servers of earlier major or minor versions. This includes Veeam Agent backup jobs, file backup jobs, object storage backup jobs, and backup copy jobs.
  - In Veeam Self-Service Backup Portal for Cloud Director and vSphere Self-Service Backup Portal, you cannot create and edit jobs managed by backup servers of earlier major or minor versions.
  - Data collection from backup servers of earlier major and minor versions takes more time, which can be critical if many backup servers are added to Enterprise Manager.
- Enterprise Manager on Linux uses Kerberos authentication to communicate with Microsof Windows backup servers. If you want to add a Microsoft Windows backup server, it must be joined to a domain; workgroup backup servers cannot be added bacause Kerberos authentication does not support local accounts. Linux backup servers do not have to be joined to a domain.

  Enterprise Manager on Microsoft Windows also uses Kerberos by default, but switches to NTLM authentication for workgroup backup servers or when Kerberos is not available. This allows you to add both domain-joined and workgroup backup servers in Enterprise Manager on Microsoft Windows.

  For details on Kerberos, see the Kerberos Authentication section of the Veeam Backup & Replication User Guide.
- If Enterprise Manager uses a proxy server, Enterprise Manager connects to backup servers through this proxy. Make sure that the backup server you want to add is either accessible through the proxy or added to the proxy bypass list. In the bypass list, specify the same DNS name or IP address that you use to add the backup server to Enterprise Manager. For details on configuring a proxy for Linux-based Enterprise Manager, see Configuring HTTPS Proxies.
- To add a backup server that is part of a High Availability (HA) cluster, add it using the cluster virtual IP address or cluster full DNS name. In this case, after a node switchover, Enterprise Manager will automatically collect the data from the active node.

  If a backup server that is already added to Enterprise Manager becomes part of an HA cluster, you must re-add it using the cluster virtual IP address or cluster full DNS name after assembling the cluster. If you do not re-add the backup server, Enterprise Manager will not be able to collect data from it after a node switchover. For more information on HA clusters, see the High Availability (HA) Cluster section of the Veeam Backup & Replication User Guide.

- Do not add the same backup server to multiple instances of Enterprise Manager, as well as a backup server cloned from an already added backup server.
- Do not add a backup server that holds the same configuration database as an already added backup server, even after you remove the original backup server from Enterprise Manager.

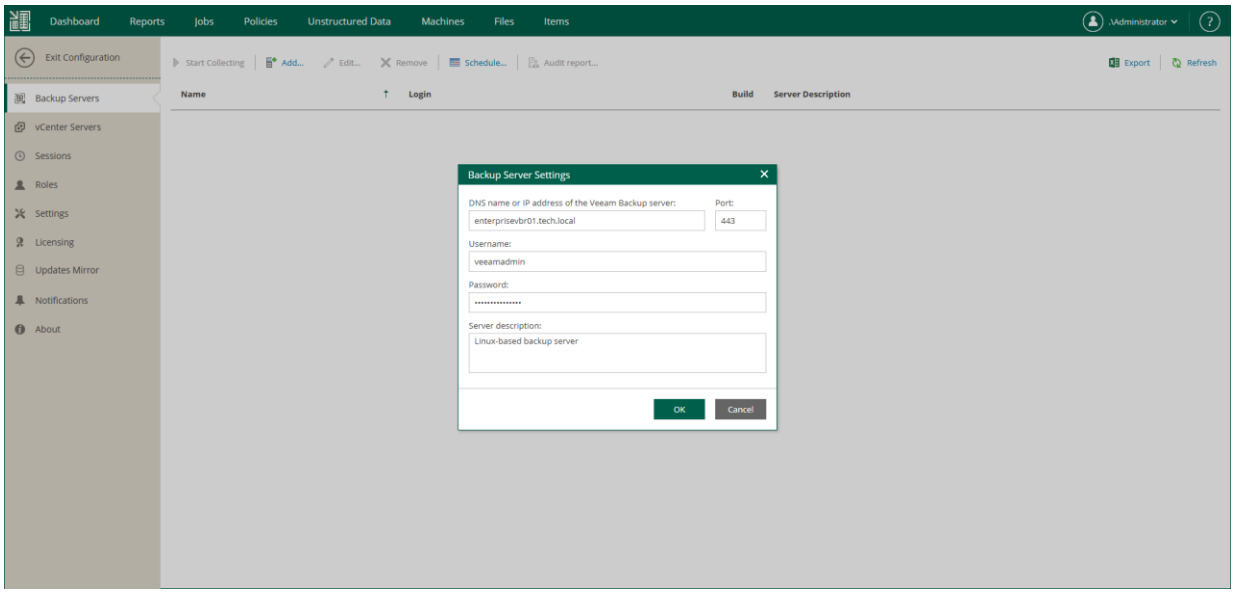
  Two backup servers may have the same configuration database if you migrate a configuration database from one backup server to another. To avoid conflicts when adding the server to Enterprise Manager, follow the steps in the Migrating Veeam Backup & Replication to Another Backup Server section of the Veeam Backup & Replication User Guide. During migration, the database will be restored with a new ID on the target backup server.

Adding Backup Server

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

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Backup Servers** section.
4. At the top of the **Backup Servers** section, click **Add**.
5. In the **DNS name or IP address of the Veeam backup server** field, enter the DNS name, IPv4 or IPv6 address of the server you want to add.
   - When specifying a DNS name, ensure that Enterprise Manager can resolve it.
   - If the backup server is part of a High Availability (HA) cluster, enter the cluster virtual IP address or cluster full DNS name. After a node switchover, Enterprise Manager will automatically collect the data from the active node. For more information on HA clusters, see the High Availability (HA) Cluster section of the Veeam Backup & Replication User Guide.
   - For more information on IPv6 support, see the IPv6 Support section of the Veeam Backup & Replication User Guide.
6. In the **Server description** field, specify a description for the backup server.
7. Enter the name and password of the backup server account.
   - The account must be assigned the Backup Administrator role. For more information, see Configuring Backup Server Roles.
   - When adding a Linux-based backup server, use the UPN format to specify a domain user.
   - [For Linux-based Enterprise Manager] If you are adding a backup server with Veeam Backup & Replication 12.3.x and you want to use an Active Directory account, specify the user name in the UPN format with a capitalized domain name (for example, *user@DOMAIN*).
8. Specify the port used by the Veeam Backup Service on the backup server.
9. Click **OK** to add the backup server.
10. In the certificate validation window, review the certificate thumbprint:
    - Click **Yes** if you trust the server.

- Click **No** if you do not trust the server. Enterprise Manager will display an error message, and the connection will not be established.



Configuring Backup Server Roles

Veeam Backup Enterprise Manager communicates with backup servers using TLS certificates that you specify when adding the backup servers. For more information, see Adding Backup Servers.

All operations on the backup server side are performed by Veeam Backup Service. The service verifies beforehand if Enterprise Manager has rights to accomplish the necessary actions. The account used by Enterprise Manager must have the Backup Administrator role assigned in Veeam Backup & Replication.

By default, when you install Veeam Backup & Replication on a backup server, the Backup Administrator role is assigned to the Windows Server Administrators group, so you can choose a user from the Administrators group as an account that will be used to communicate with the backup server. As soon as the group settings can be changed, it is recommended to explicitly assign the Backup Administrator role to the user account. For more information on assigning roles, see the Roles and Users section of the Veeam Backup & Replication User Guide.

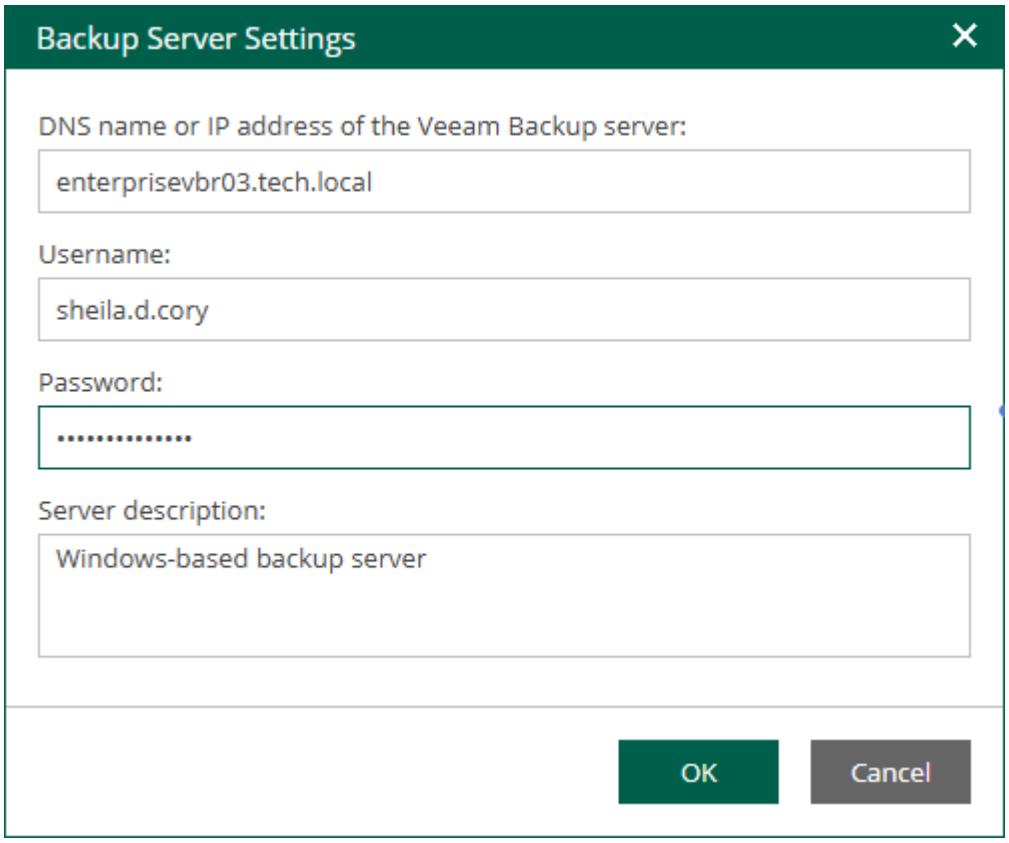
Editing Backup Servers

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

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

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Backup Servers** section.
4. Select a backup sever from the list and click **Edit** on the toolbar.

   Alternatively, you can right-click the selected backup server and select **Edit**.
5. Specify new connection settings and click **OK**.



Removing Backup Servers

To disconnect a backup server added to the Veeam Backup Enterprise Manager infrastructure, you must remove it from Enterprise Manager. After you remove a backup server, Enterprise Manager stops collecting data from the backup server and showing the backup server data such as jobs, backed up machines and so on.

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

To remove a backup server, do the following:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Backup Servers** section.
4. Select a backup sever from the list and click **Remove** on the toolbar.

   Alternatively, you can right-click the selected backup server and select **Remove**.
5. In the open window, click **Yes** to confirm the removal.

Collecting Data from Backup Servers

Veeam Backup Enterprise Manager retrieves data from added backup servers using a data collection job. The data collection job collects information from configuration databases of backup servers. The collected data is stored to the Veeam Backup Enterprise Manager configuration database and can be accessed by multiple users of Veeam Backup Enterprise Manager.

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 job session. For more information, see Data Collection Job Sessions.

NOTE

- Enterprise Manager automatically starts a data collection job right after you add a backup server.
- Data collection job collects data from all added backup servers at once.
- To ensure periodic update of the information available to Veeam Backup Enterprise Manager users, use periodic data collection.
- Data collection from backup servers of earlier versions takes more time, which can be critical if many backup servers are added to Enterprise Manager. If you notice a low performance of the data collection job, consider upgrading the backup servers.

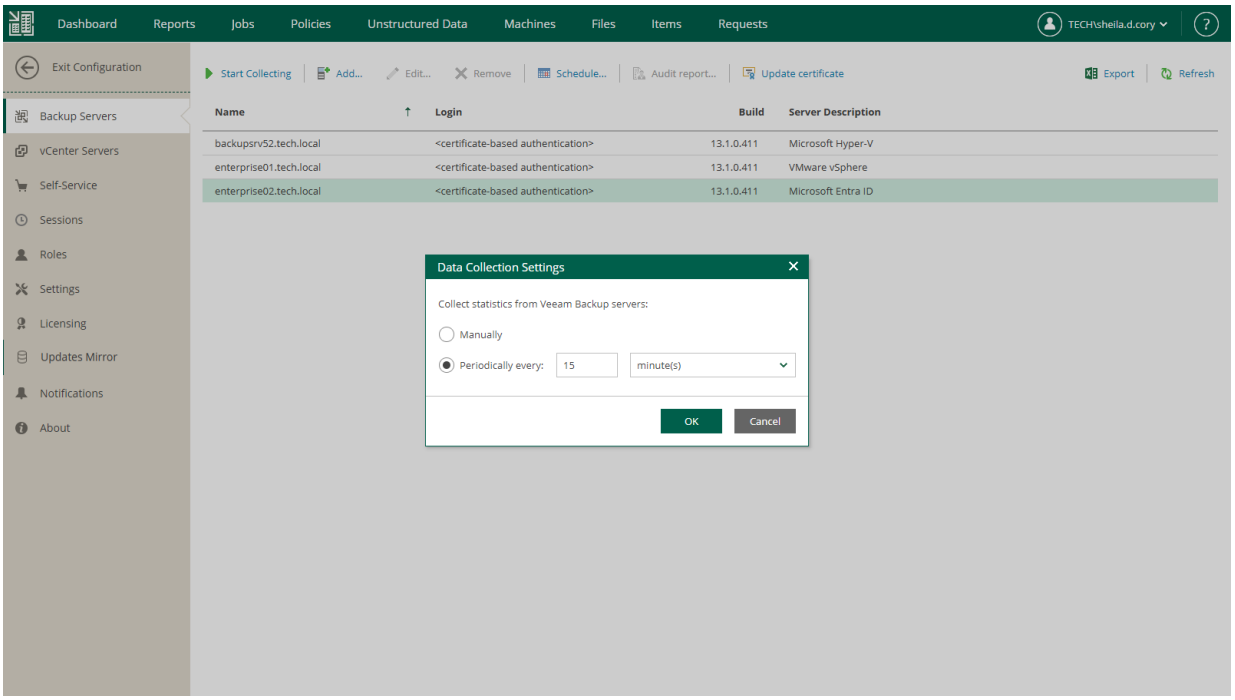
Periodic Data Collection

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. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Backup Servers** section.
4. Click **Schedule** on the toolbar.
5. In the **Data Collection Settings** window, specify the desired interval in the **Periodically every** option.

6. Click **OK**.



You can also disable periodic data collection. In this case, you can only start the data collection job manually.

To disable periodic data collection:

1. Select **Backup Servers** on the left of the **Configuration** view and click **Schedule** on the toolbar.
2. In the **Data Collection Settings** window, select the **Manually** option.
3. Click **OK**.

Manual Data Collection

You can start the data collection job manually at any time.

To start the data collection job manually:

1. Select **Backup Servers** on the left of the **Configuration** view.
2. Click **Start Collecting** on the toolbar.
3. To view the details on the started job session, click the **Sessions** link at the top or open the **Sessions** section of the **Configuration** view.

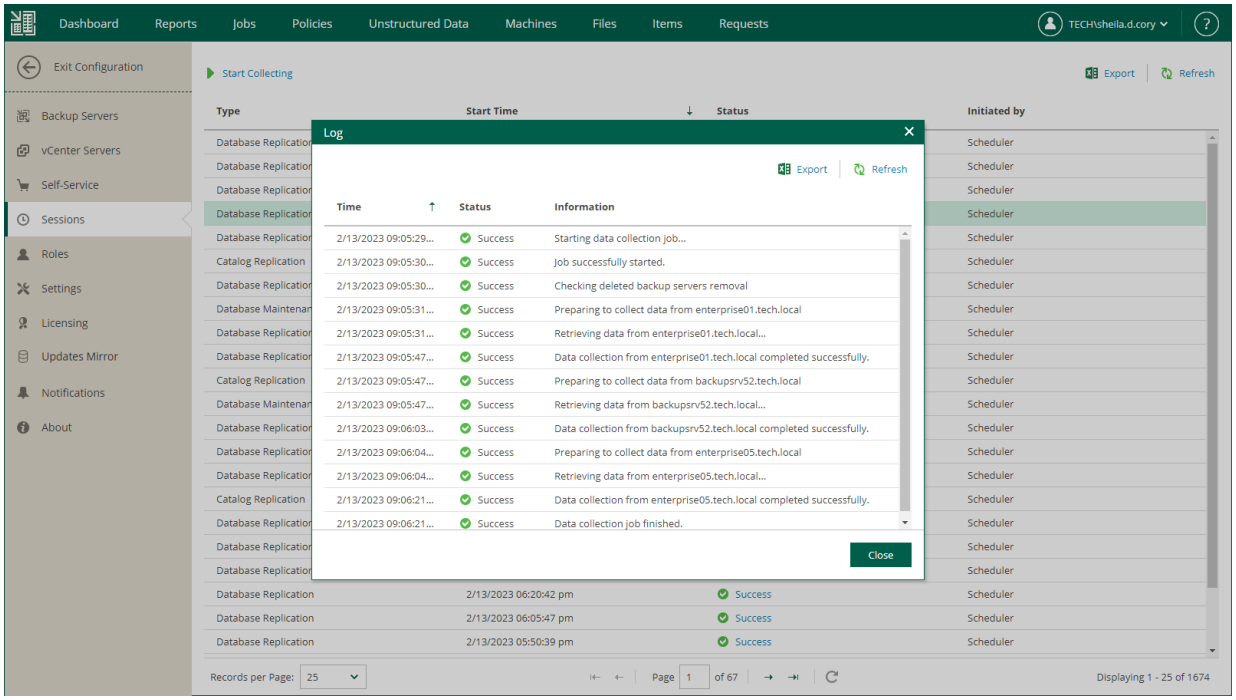
Data Collection Job Sessions

Every run of the data collection job initiates a new job session.

To view details on job sessions, to 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 link in the **Status** column.

3. In the displayed window, Veeam Backup Enterprise Manager shows the list of the job session events. For each job session event, Enterprise Manager shows the time of the event, its current status and information about the event.



Reports on Backup Servers

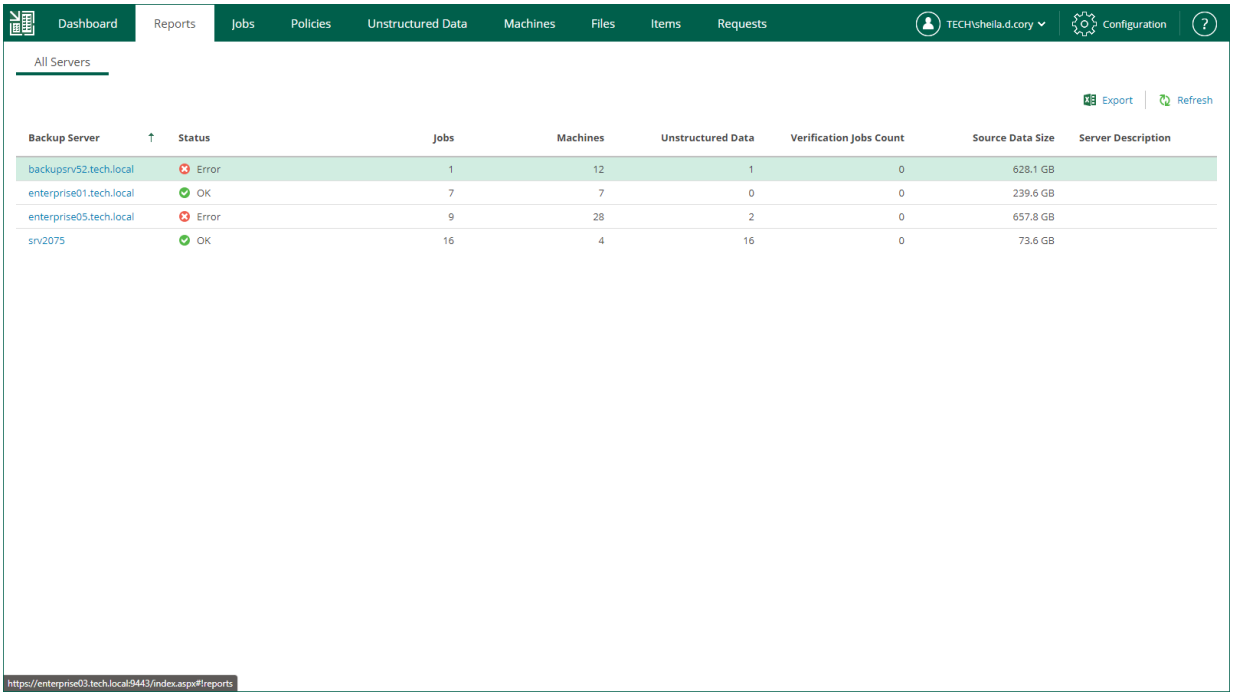
On the **Reports** tab, you can view statistical information about backup servers added to the Enterprise Manager infrastructure.

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

Parameter	Description
Backup Server	Name of the backup server.
Status	Status of the last data collection job session for the backup server. For more information on data collection, see Collecting Data from Backup Servers. Possible values: • *Never processed* — data collection has never been started for the backup server • *Processing* — data collection is in progress • *OK* — data was collected successfully • *Warning* — data collection completed with a warning • *Error* — data collection failed
Jobs	Number of jobs on the backup server.
Machines	Number of machines processed by the backup server, including the machines from imported or orphaned backups.
Unstructured Data	Number of object storage systems and file shares processed by the backup server, including the file shares from imported or orphaned backups.
Verification Jobs Count	Number of SureBackup jobs on the backup server.
Source Data Size	Size of source data processed by the backup server.
Server Description	Backup server description that was specified when adding the server to the Enterprise Manager infrastructure.

You can drill down into this data by clicking a link in the **Backup Server** column to move through the levels in the following succession: *Backup servers > Jobs > Job sessions > Session details*. Each level contains a list of entries with details for that particular level.

> **NOTE**
>
> You can export displayed information to a file using the **Export** link on the toolbar. To open the file on your machine, use the associated application.


Dashboard
Reports
Jobs
Policies
Unstructured Data
Machines
Files
Items
Requests
TECH\sheila.d.cory
Configuration
All Servers
Export
Refresh
Backup Server
Status
Jobs
Machines
Unstructured Data
Verification Jobs Count
Source Data Size
Server Description
backupsrv52.tech.local
Error
1
12
1
0
628.1 GB
enterprise01.tech.local
OK
7
7
0
0
239.6 GB
enterprise05.tech.local
Error
9
28
2
0
657.8 GB
srv2075
OK
16
4
16
0
73.6 GB
https://enterprise03.tech.local:9443/index.aspx#!reports

Audit Reports

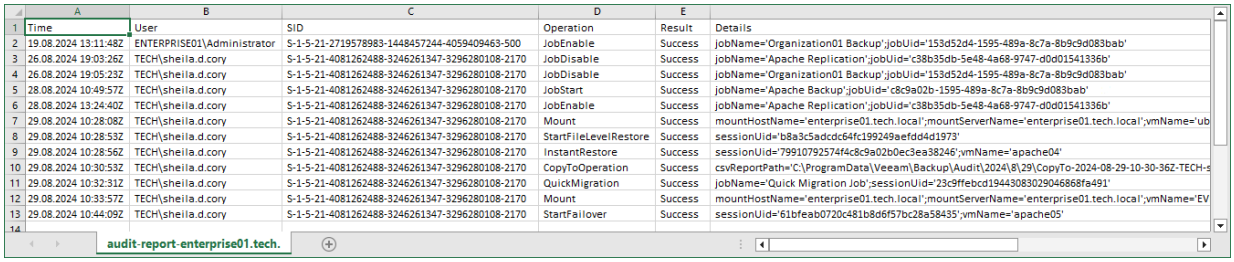
Audit reports contain records of user activity performed on the selected backup server for the specified period. Users with the Portal Administrator role can generate audit reports for backup servers added to the Veeam Backup Enterprise Manager infrastructure. For more information, see Generating Audit Report.

Audit Report Overview

Audit reports include the following details about user activity:

- Date and time when a user performed an operation
- User name
- User security identifier (SID)
- Name of the operation initiated by the user

  For more information on operations included in the report, see Audited Operations.
- Operation result
- Details on the performed operation



Time	User	SID	Operation	Result	Details
19.08.2024 13:11:48Z	ENTERPRISE01\Administrator	S-1-5-21-2719578983-1448457244-4059409463-500	JobEnable	Success	jobName='Organization01 Backup';jobUid='153d52d4-1595-489a-8c7a-8b9c9d083bab'
26.08.2024 19:03:26Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	JobDisable	Success	jobName='Apache Replication';jobUid='c38b35db-5e48-4a68-9747-d0d01541336b'
26.08.2024 19:05:23Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	JobDisable	Success	jobName='Organization01 Backup';jobUid='153d52d4-1595-489a-8c7a-8b9c9d083bab'
28.08.2024 10:49:57Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	JobStart	Success	jobName='Apache Backup';jobUid='c8c9a02b-1595-489a-8c7a-8b9c9d083bab'
28.08.2024 13:24:40Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	JobEnable	Success	jobName='Apache Replication';jobUid='c38b35db-5e48-4a68-9747-d0d01541336b'
29.08.2024 10:28:08Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	Mount	Success	mountHostName='enterprise01.tech.local';mountServerName='enterprise01.tech.local';vmName='ub
29.08.2024 10:28:53Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	StartFileLevelRestore	Success	sessionUid='b8a3c5adcdc64fc199249aefdd4d1973'
29.08.2024 10:28:56Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	InstantRestore	Success	sessionUid='79910792574f4c8c9a02b0ec3ea38246';vmName='apache04'
29.08.2024 10:30:53Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	CopyToOperation	Success	csvReportPath='C:\ProgramData\Veeam\Backup\Audit\2024\8\29\CopyTo-2024-08-29-10-30-36Z-TECH-s
29.08.2024 10:32:31Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	QuickMigration	Success	jobName='Quick Migration Job';sessionUid='23c9ffebcd19443083029046868fa491'
29.08.2024 10:33:57Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	Mount	Success	mountHostName='enterprise01.tech.local';mountServerName='enterprise01.tech.local';vmName='EV
29.08.2024 10:44:09Z	TECH\sheila.d.cory	S-1-5-21-4081262488-3246261347-3296280108-2170	StartFailover	Success	sessionUid='61bfeab0720c481b8d6f57bc28a58435';vmName='apache05'

audit-report-enterprise01.tech.

Generating Audit Report

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

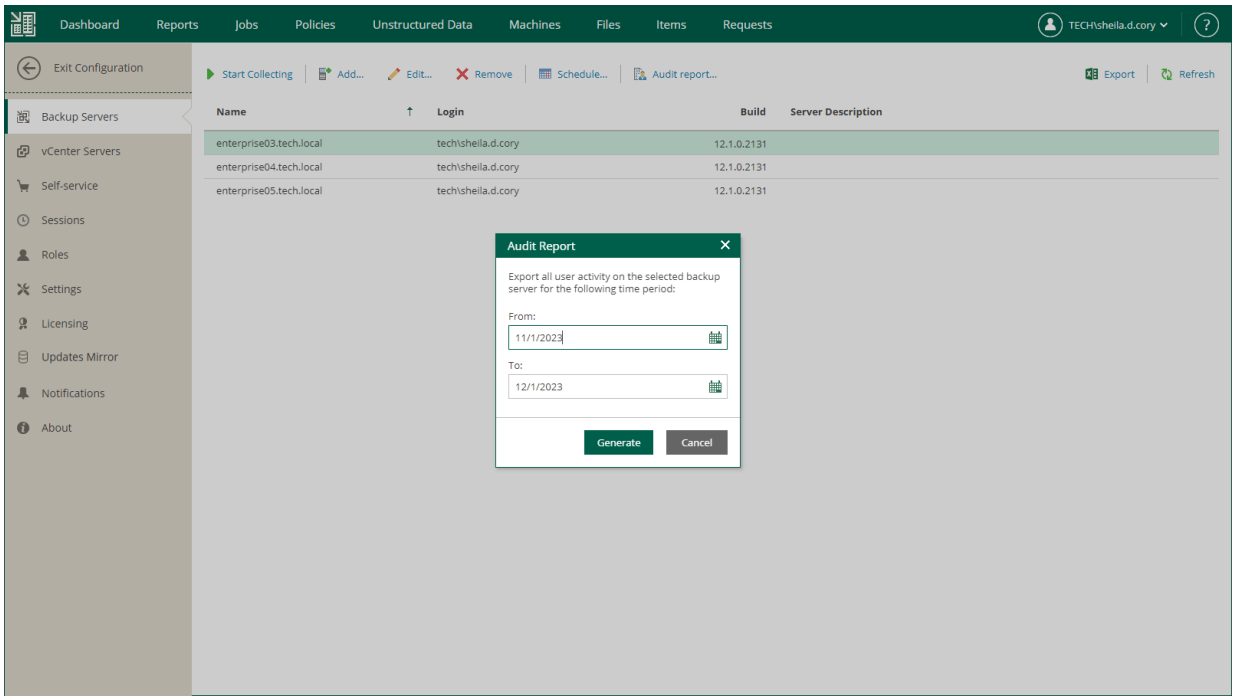
The generated file is also saved on the Enterprise Manager machine. Enterprise Manager does not clean up these files. You can find all reports in the following folder: `%ProgramData%\Veeam\Backup\WebRestore`.

To generate an audit report:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Backup Servers** section.
4. Select a backup server whose report you want to export.
5. Click **Audit report**.

6. In the **Audit Report** window, specify a time period covered by the report and click **Generate**.

   The report contains only the audit records whose retention period is not expired. The retention period is defined by the **Event history** setting of Enterprise Manager. For more information on retention settings, see Configuring Retention Settings for Index and History.



Audited Operations

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

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

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

Operation Type	Operation Name	Description
	Mount	Mounting backup content to a mount server

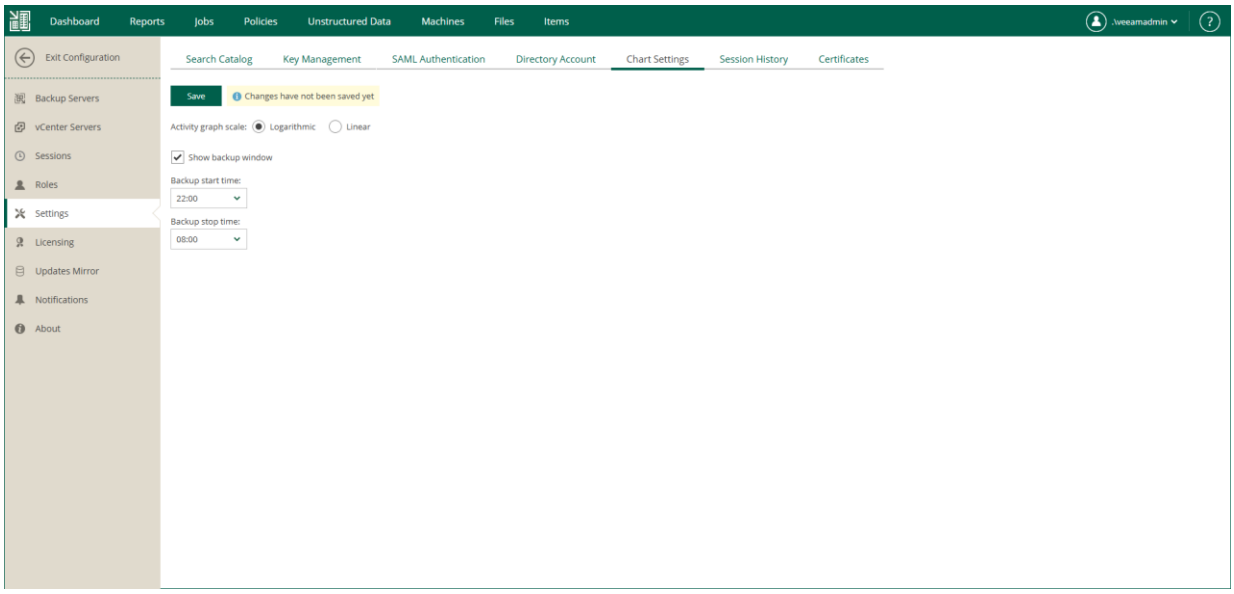
Customizing Dashboard Chart

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

> **IMPORTANT**
>
> Backup window interval that you specify here, effects the job settings that you configure for tenants that use the following portals:
>
> - vSphere Self-Service Backup Portal
> - Veeam Self-Service Backup Portal for Cloud Director

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

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



Viewing vCenter Servers

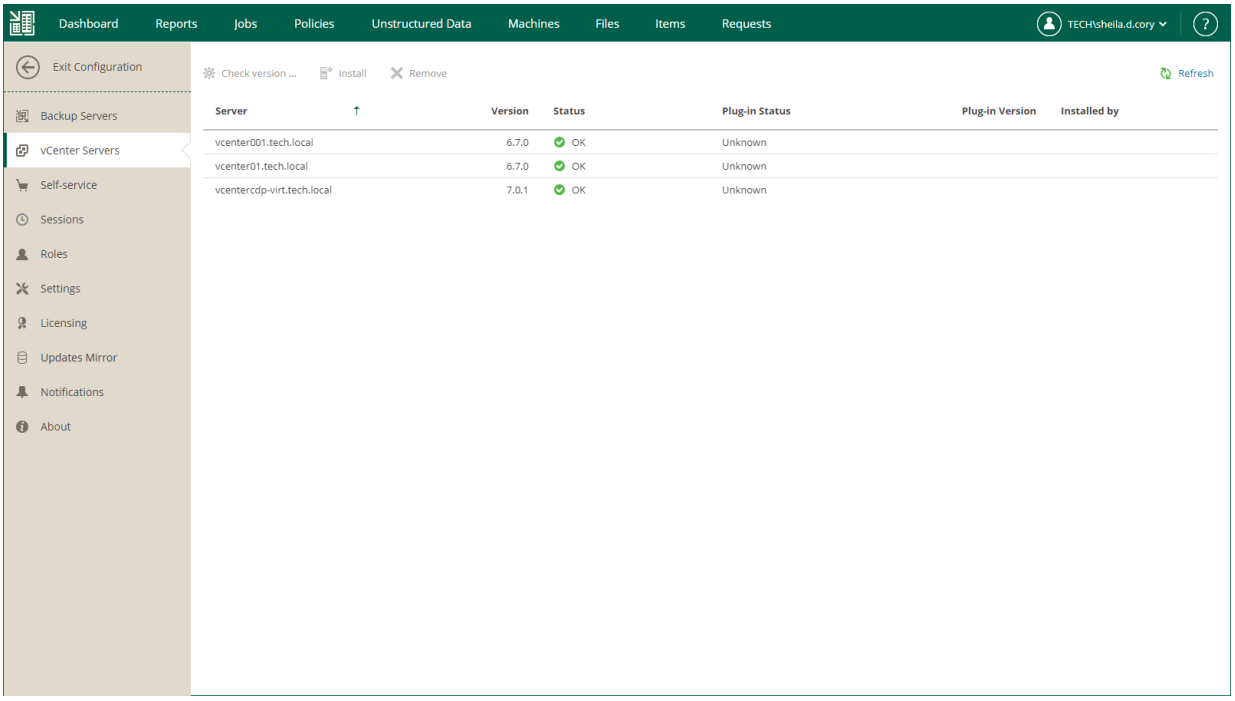
On the **vCenter Servers** tab of the **Configuration** view, you can view information on vCenter Servers added to your Veeam backup infrastructure.

You can perform the following operations with vCenter Servers:

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

For more information on the plug-in, see Veeam Plug-in for VMware vSphere Client.

> **IMPORTANT**
>
> To perform these operations, you should supply a user account with sufficient permissions to access vCenter Server. User account information is not imported from the Veeam Backup & Replication configuration database to the Enterprise Manager database for security reasons.



Managing Encryption Keys

Veeam Backup Enterprise Manager provides you with an alternative way for data encryption. It lets you decrypt the data if you have lost or forgotten the password used for data encryption or if a KMS server used for data encryption is not available. For more information on the concept, terms and procedures of data encryption, see the Data Encryption section of the Veeam Backup & Replication User Guide.

For encryption, Veeam Backup Enterprise Manager uses an Enterprise Manager keyset — a pair of matching keys:

- Public Enterprise Manager key encrypts storage keys on backup servers connected to Veeam Backup Enterprise Manager.
- Private Enterprise Manager key decrypts storage keys in case a password for encrypted backup or tape is lost.

To let Veeam Backup & Replication encrypt and decrypt data with Enterprise Manager keys, make sure Enterprise Manager keys are enabled in Veeam Backup Enterprise Manager.

To enable Enterprise Manager keys, do the following:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, select the **Enable encryption password loss protection** check box.
3. To save the changes, click **Save**.

During Veeam Backup Enterprise Manager installation, the setup automatically generates an Enterprise Manager keyset. You can perform the following operations with Enterprise Manager keysets using Enterprise Manager:

- Generate a new Enterprise Manager keyset
- Activate an Enterprise Manager keyset
- Specify retention settings for an Enterprise Manager keyset
- Export and import an Enterprise Manager keyset
- Delete an Enterprise Manager keyset

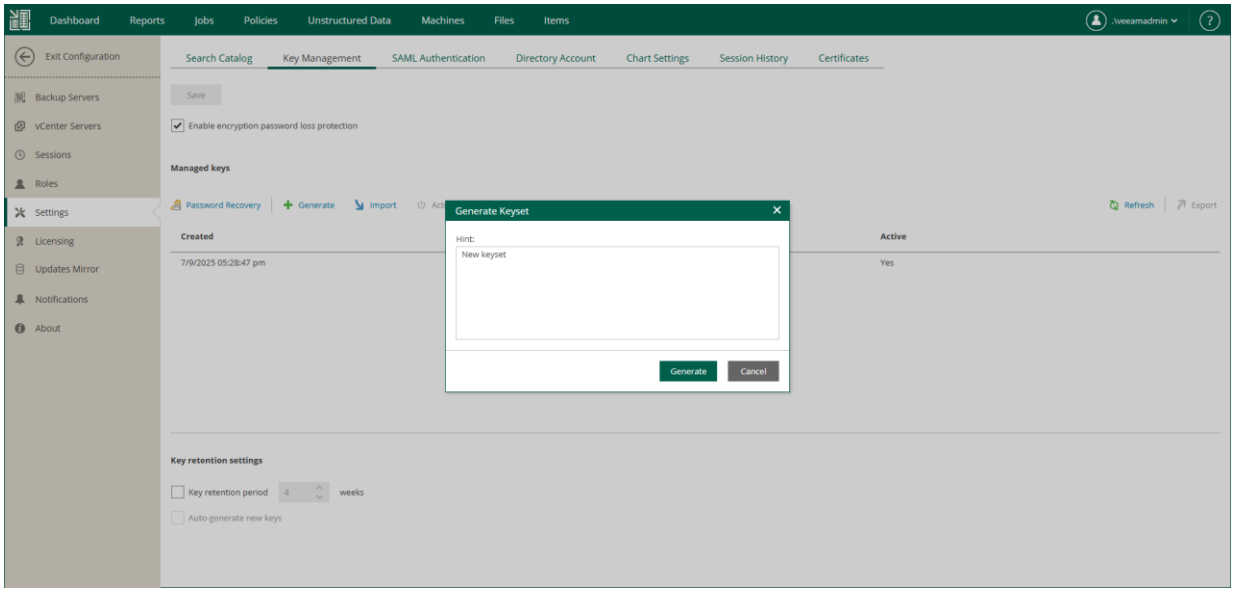
Generating Enterprise Manager Keyset

For safety's sake, periodically generate a new pair of Enterprise Manager keys. Regular change of encryption keys raises the encryption security level.

Enterprise Manager keys are created in the inactive state. To make the keys active and use them for encryption and decryption, you need to activate the keys. For details, see Activating Enterprise Manager Keyset.

To generate a new Enterprise Manager keyset:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, click **Generate**.
3. In the **Generate Keyset** window, enter a description for the created keyset. The keyset description will help you to distinguish the created keyset in the list.
4. Click **Generate**.



Activating Enterprise Manager Keyset

Active Enterprise Manager keys are the keys that are currently used in the encryption process. After you generate a new keyset, you need to activate it. As a result of activation, Veeam Backup Enterprise Manager performs the following actions:

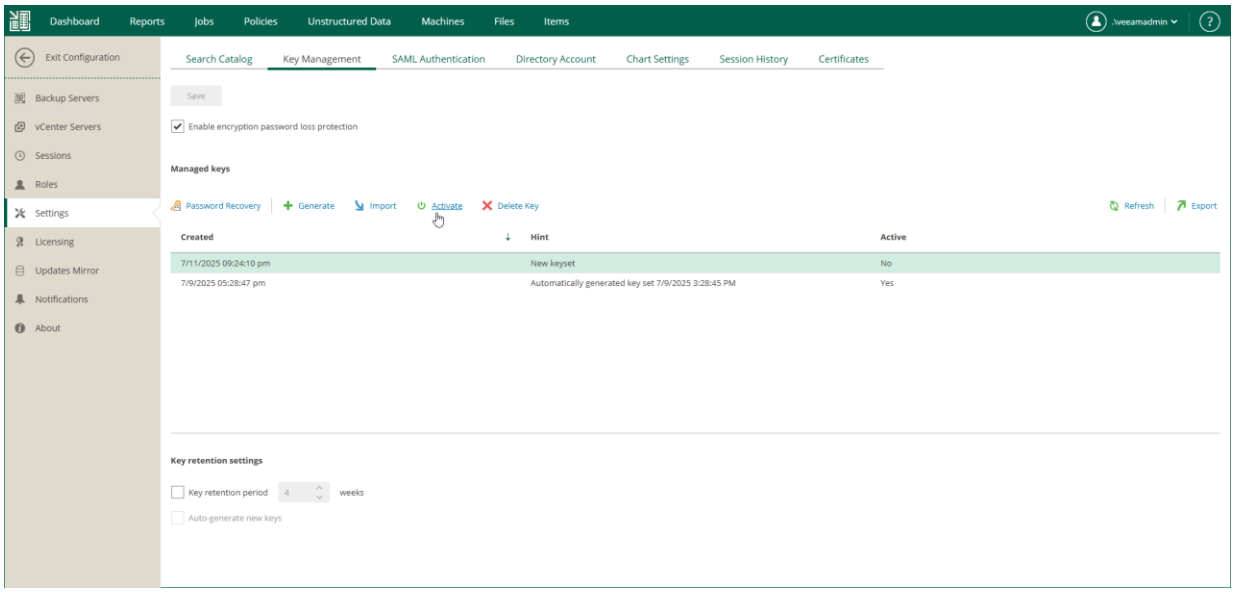
- Public Enterprise Manager key is propagated to all Veeam backup servers connected to Veeam Backup Enterprise Manager.
- Private Enterprise Manager key remains on Veeam Backup Enterprise Manager and marked as active.

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

You can perform manual activation for any keyset (generated manually or automatically). Manually generated keysets require manual activation.

To activate a keyset manually, do the following:

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



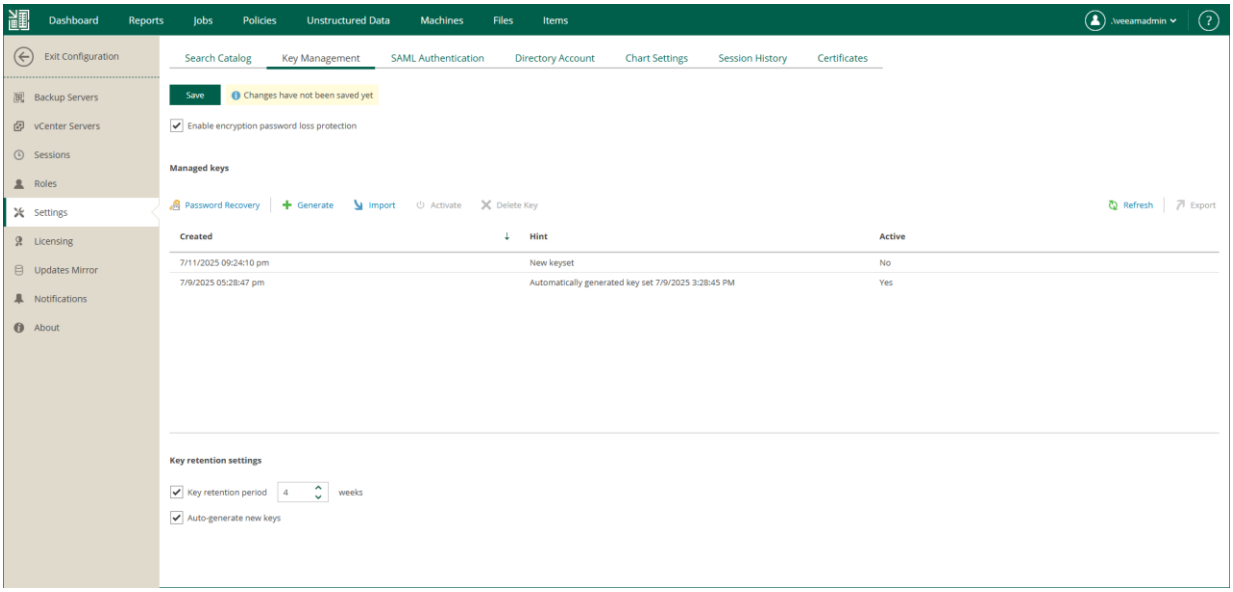
Specifying Retention Settings for Enterprise Manager Keyset

Government regulations and internal company policies may require you to regularly change encryption keys. The shorter the lifetime of an encryption key, the less data is encrypted with this key, which results in a higher level of encryption security.

The lifetime of Enterprise Manager keys is determined by the key retention period. The key retention period specifies how long the keys must remain active and be used for encryption and decryption operations.

You can configure the retention period for Enterprise Manager keysets as follows:

1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select the necessary options:
   - 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). When the retention period ends and key auto-generation is turned off, a user will receive a notification email and must manually create and activate a new keyset. After a new keyset is ready, the old keyset is marked as inactive.
   - To enable automatic generation of new keysets, select the **Auto-generate new keys** check box. When 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 propagates the new public Enterprise Manager key to all added backup servers. The private Enterprise Manager key remains on Veeam Backup Enterprise Manager and is used for data decryption.
3. Click **Save** to apply the settings.



Exporting and Importing Enterprise Manager Keyset

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

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

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

To export a keyset:

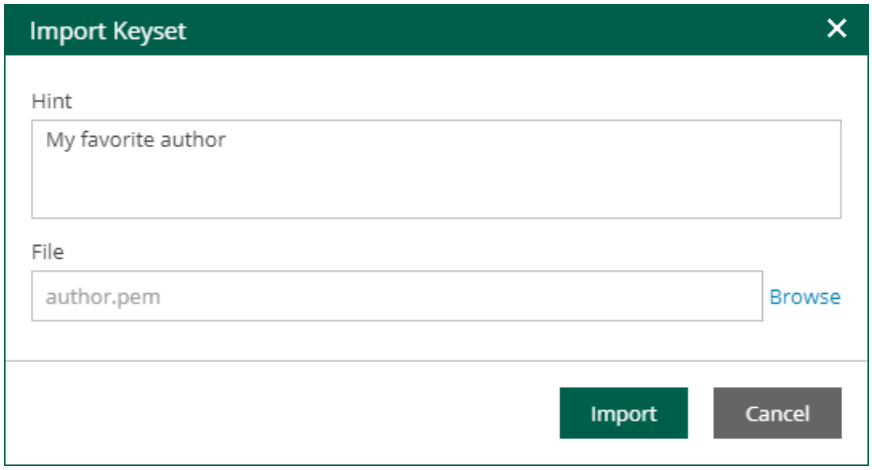
1. In Veeam Backup Enterprise Manager, open the **Settings** section of the **Configuration** view.
2. On the **Key Management** tab, in the **Managed keys** section, select a keyset you want to back up and click **Export**.
3. Save the resulting PEM file on the local disk or in a network shared folder.

To import a previously exported keyset:

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

When you import a keyset, it is saved to the Veeam Backup Enterprise Manager database and displayed in the keyset list in Veeam Backup Enterprise Manager.

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


Import Keyset
Hint
My favorite author
File
author.pem
Browse
Import
Cancel

Deleting Enterprise Manager Keyset

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

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

To delete a keyset:

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

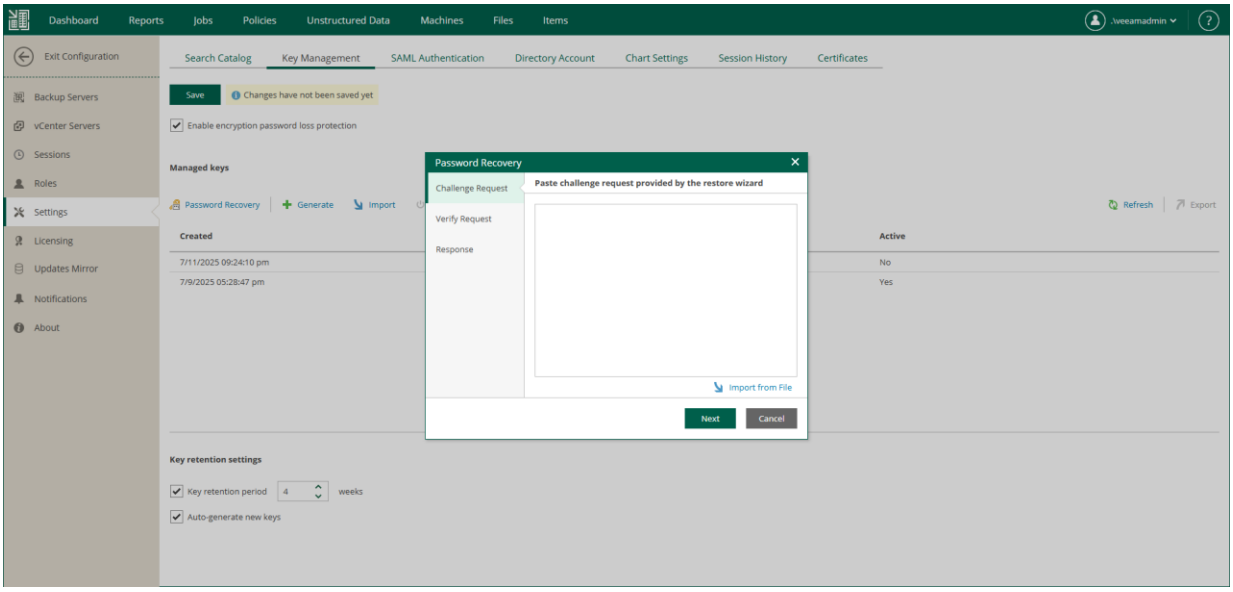
> **IMPORTANT**
>
> It is strongly recommended that you export a keyset before you delete it. If you delete a keyset and do not make its backup copy, you will not be able to restore data from a backup or tape encrypted with keys from this keyset in case a password is lost. For more information, see Exporting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

Handling Password Recovery Requests

When an encrypted backup file or tape media is imported on a backup server, a user key with password or a KMS server key is required to decrypt the data. However, the password can be lost or forgotten, or the KMS server may not be available. Veeam Backup Enterprise Manager lets decrypt such backups.

To decrypt your data, use the **Password Recovery** wizard within the following context:

1. In Veeam Backup & Replication, you generate a request message for password restore. For more information, see the Create Request for Data Restore section of the Veeam Backup & Replication User Guide.
2. In Veeam Backup Enterprise Manager, 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 backup server where the request was issued.
5. Then you can send the response back to requester, for example, by email. The requester will input this response to the Enterprise Keys Restore wizard on the Veeam backup server where the request was issued; Veeam Backup & Replication will process the response, retrieve the decrypted storage keys and use them to unlock encrypted backups or tapes and retrieve their content.

IMPORTANT

In case your organization encrypts configuration backups of a backup server, and you want to be able to serve password restore request for these backups, ensure the original 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 backup server is removed from Enterprise Manager, its public key will be deleted from the Enterprise Manager database.
- If a new configuration database is created on a backup server, then a new public key will be automatically generated for that 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 Explorers User Guide.

Configuring Accounts and Roles

Veeam Backup Enterprise Manager implements security based on user roles by limiting access to features and data. This empowers the administrator to delegate permissions in a granular way, on an as-needed basis. For example, the administrator can grant permissions to another user to recover files without being able to see the content of the files.

Administrators grant users and groups access to Enterprise Manager by adding accounts. When adding an account, administrators assign a role to the account to provide it with permissions.

Enterprise Manager offers the following roles:

- Portal Administrator
- Portal User
- Restore Operator

For the Portal User and Restore Operator roles, administrators can also configure restore scope and provide permissions for guest OS file restore and application item restore.

> **NOTE**
>
> This section describes management of user accounts and roles required to work with the main Enterprise Manager UI. If you plan to provide a user with access to vSphere Self-Service Backup Portal (and not to the main Enterprise Manager UI), you do not need to configure an account for this user on the **Roles** tab of the **Configuration** view. Such accounts are configured on the **Self-service** tab of the **Configuration** view. For more information, see Managing Tenant Accounts.

In This Section

- Accounts and Roles Overview
- Managing Accounts
- Configuring Restore Scope
- Configuring Permissions for File and Application Item Restore

Accounts and Roles Overview

Accounts

Administrators can add accounts to Veeam Backup Enterprise Manager to grant users access to the website. Enterprise Manager offers the following account types: User, Group, External User and External Group.

Type	Description	How to Sign In	Name Format
User	Local or AD user	By specifying a user name and password	• Windows-based Enterprise Manager: *DOMAIN\Username* (domain is optional) • Linux-based Enterprise Manager: *Username@DOMAIN* (domain is mandatory for AD users)
Group	Local or AD group	By specifying a user name and password	• Windows-based Enterprise Manager: *DOMAIN\Groupname* (domain is optional) • Linux-based Enterprise Manager: *Groupname@DOMAIN* (domain is mandatory for AD groups)
External User	IdP user	By using single sign-on*	*Username@Suffix*
External Group	IdP group	By using single sign-on*	Free-form string
vSphere Role	VMware vCenter Server role used to access the Veeam Plug-in for VMware vSphere Client	–	–

* For more information on the single sign-on capability, see SAML Authentication Support.

Roles

To provide an account with permissions, administrators assign one of the following roles to the account: Portal Administrator, Portal User or Restore Operator.

Role	How Is Assigned	Access to Configuration	Permissions
Portal Administrator	• Initially by default to the users listed in the local Administrators group and the user who installed Enterprise Manager • By Portal Administrator in **Configuration** > **Roles**	Yes	Full access to all available operations on all tabs of the web UI
Portal User	By Portal Administrator in **Configuration** > **Roles**	No	• Access objects from the restore scope on the **Machines** and **Files** tabs • Run Quick Backup for machines from the restore scope on the **Machines** tab • Perform restore operations as permitted by the delegation settings • View information about all backup servers and jobs on the **Dashboard**, **Reports**, **Jobs** and **Policies** tabs
Restore Operator	By Portal Administrator in **Configuration** > **Roles**	No	• Access objects from the restore scope on the **Machines** and **Files** tabs • Perform restore operations as permitted by the delegation settings

Users with the Portal User or Restore Operator role can access their *restore scope* — a list of objects that can be recovered by appropriate personnel. For example, the restore scope of database administrators is database servers (Microsoft SQL Server, Oracle or other), the restore scope of Exchange administrators is Exchange server machines, and so on. For more information on configuring restore scope, see Configuring Restore Scope.

IMPORTANT

You can customize the restore scope if you have the Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all objects and cannot be customized. However, you can delegate recovery of entire machines, guest files, or selected file types. For more information, see Configuring Permissions for File and Application Item Restore.

Managing Accounts

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

- Add account
- Edit account
- Remove account

When you add or edit an account, you can configure permissions for restore operations that the user can perform. The permissions are defined by restore scope and restore type. For more information, see the following sections:

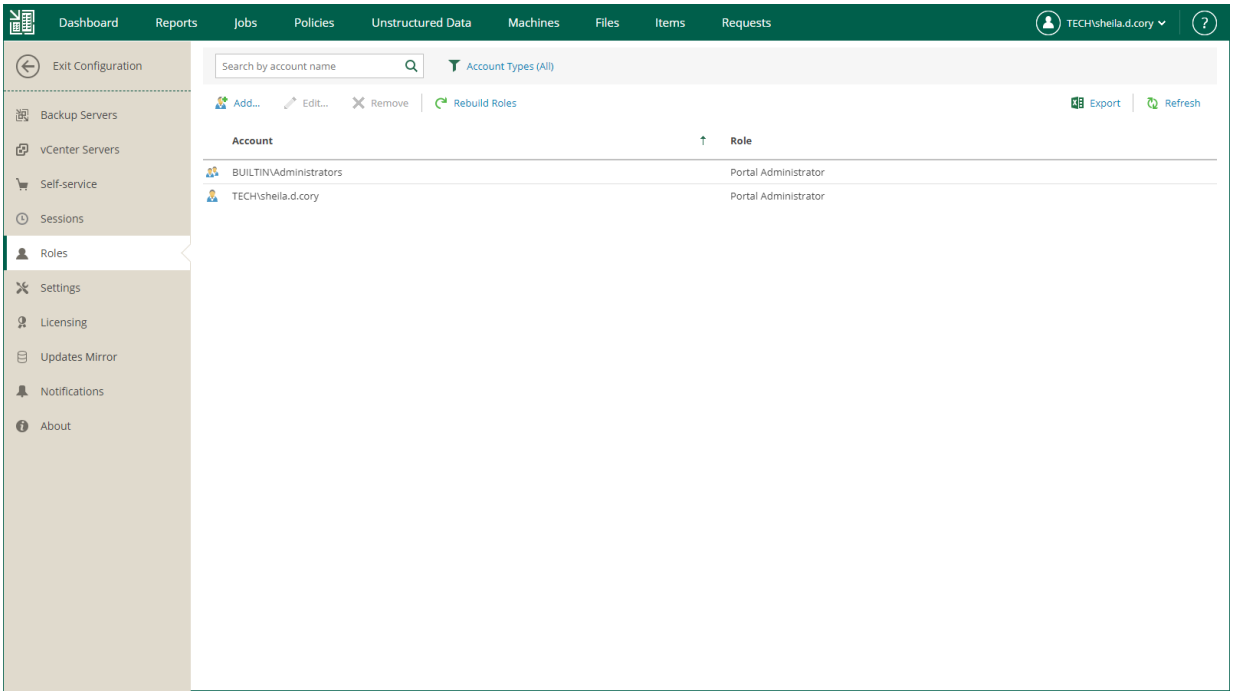
- Configuring Restore Scope
- Configuring Permissions for File and Application Item Restore

If you have Veeam ONE deployed in your backup infrastructure, you can view a report that lists Enterprise Manager users, their roles and restore permissions. For details, see the Delegated Restore Permissions Overview section of the Veeam ONE Reporting Guide.

Adding Account

To add an account, take the following steps:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Select the **Roles** section on the left of the **Configuration** view.



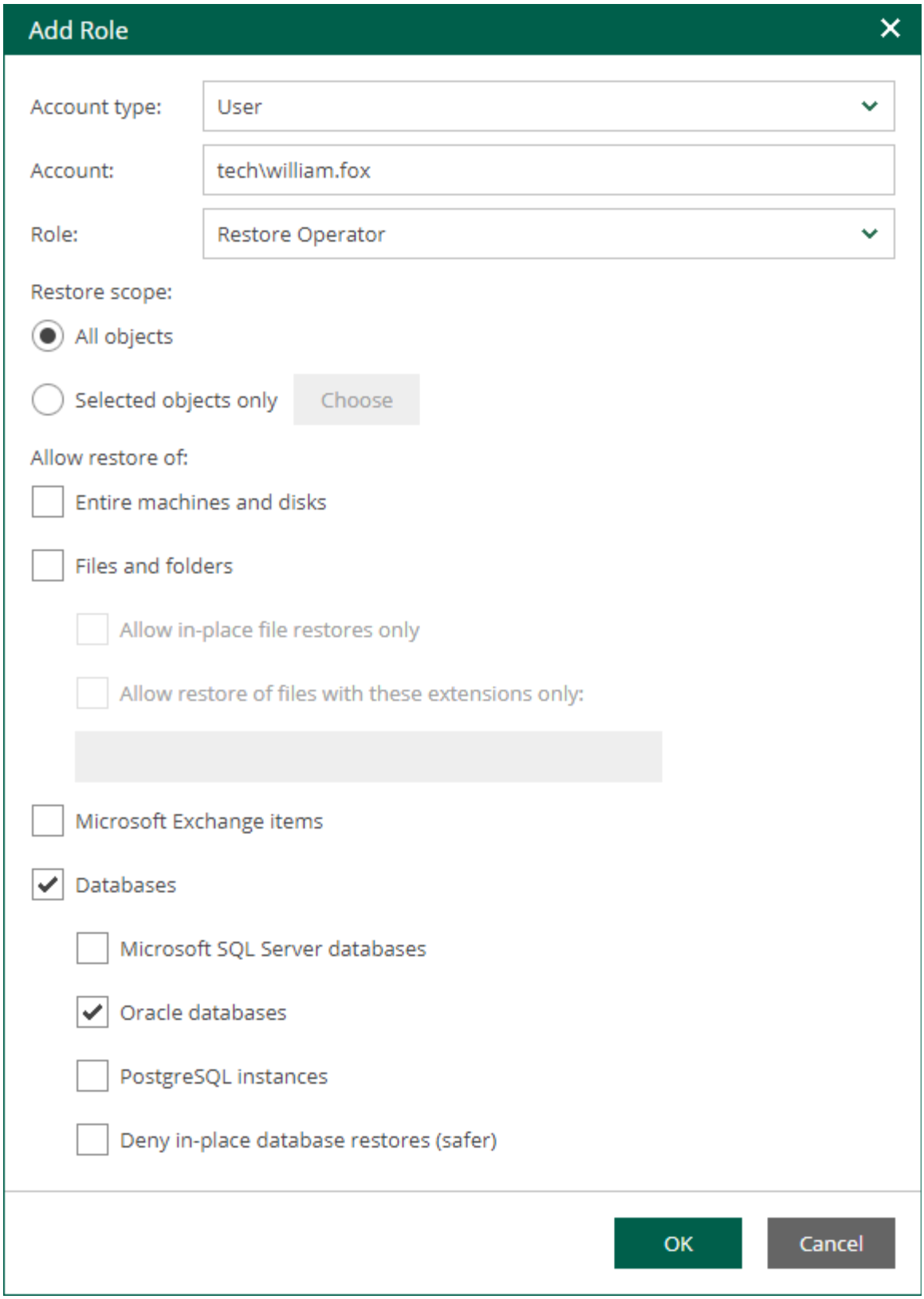
4. Click **Add** on the toolbar.
5. From the **Account type** list, select a type of the account: *User*, *Group*, *External User* or *External Group*. For more information, see Accounts and Roles Overview.

6. In the **Account** field, specify an account name in the *DOMAIN|Username* or *Username@Suffix* format depending on the account type. For more information, see Accounts and Roles Overview.
7. From the **Role** list, select a role you want to assign to the account: *Portal Administrator*, *Portal User* or *Restore Operator*. For more information, see Accounts and Roles Overview.

> **NOTE**
>
> To be able to assign any of portal roles to Active Directory domain users or groups, make sure that Veeam Backup Enterprise Manager service account has sufficient rights to enumerate Active Directory domains (by default, Active Directory users have enough rights to enumerate Active Directory domains).

8. [For Portal User or Restore Operator] In the **Restore scope** section, you can allow a user to restore all objects (machines and file shares) processed by managed backup servers or the selected objects only. For more information, see Configuring Restore Scope.

   In the **Allow restore of** section, you can configure additional restrictions for the restore scope. For more information, see Configuring Permissions for File and Application Item Restore.



Editing Account

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

Removing Account

To remove an added user or group, select it in the list and click **Remove** on the toolbar.

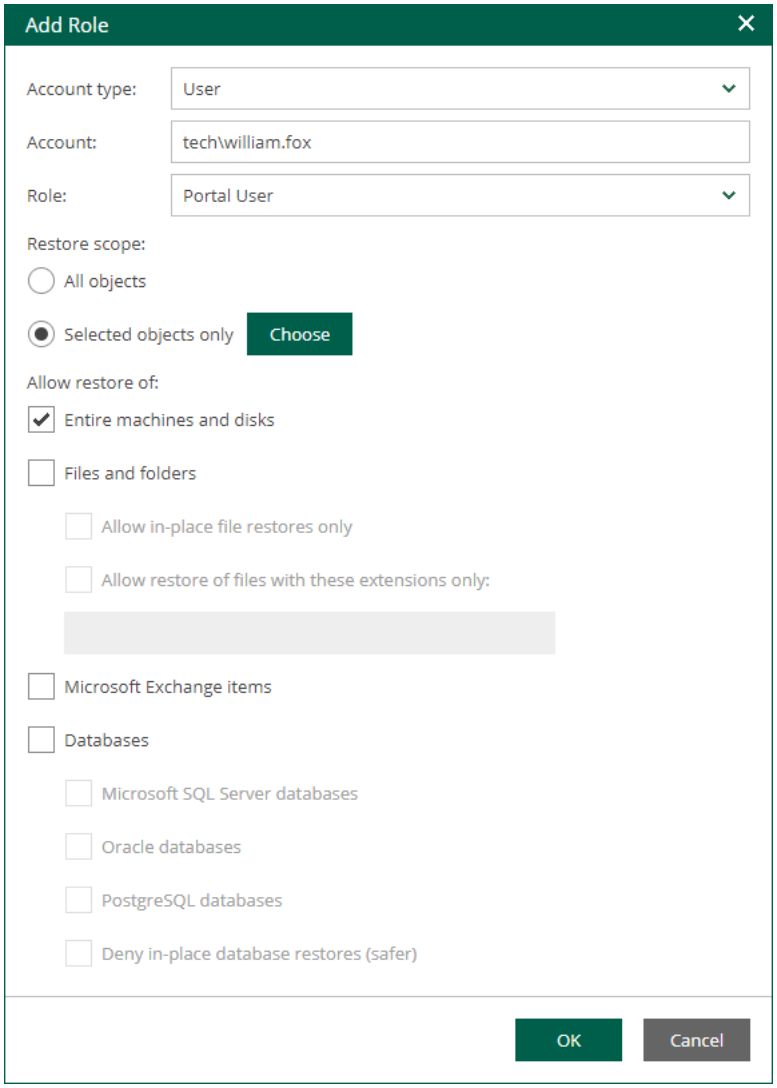
Configuring Restore Scope

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

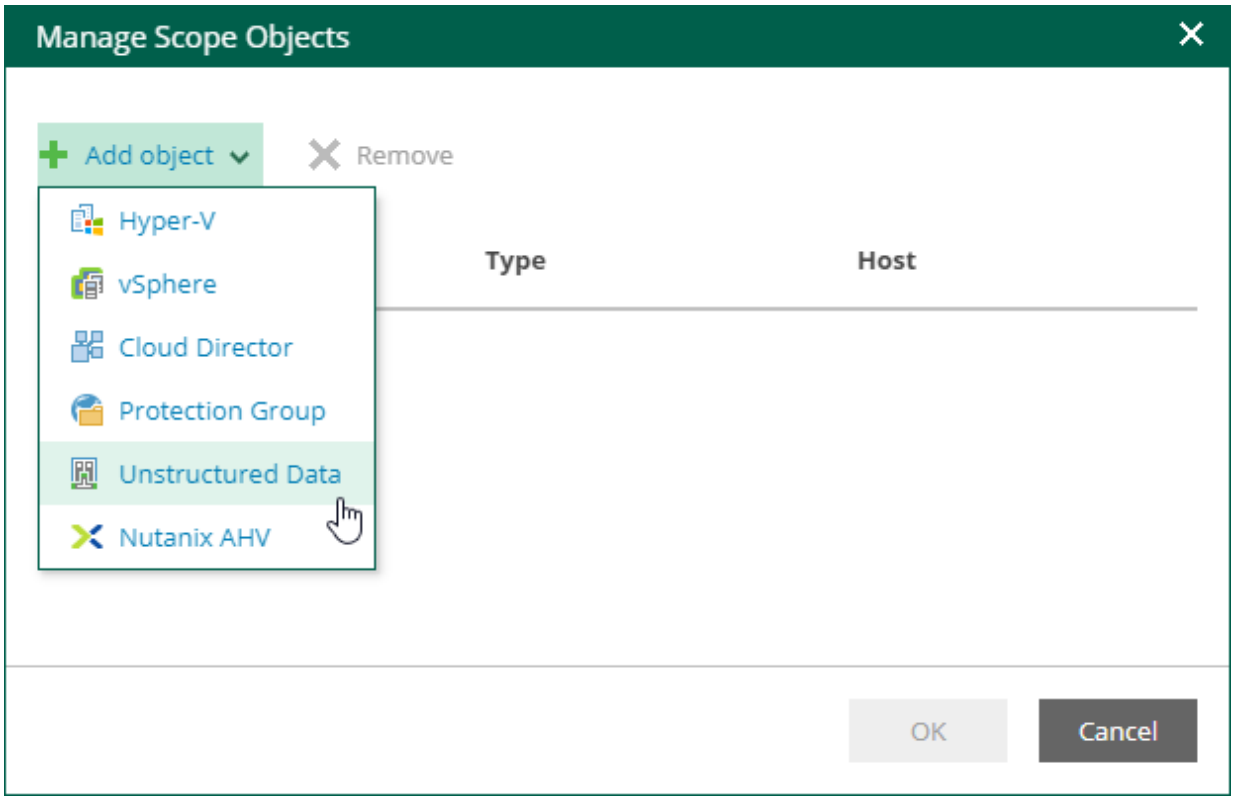
To customize the restore scope, perform the following steps when adding or editing a Portal User or Restore Operator account:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Select the **Roles** section on the left of the **Configuration** view.
4. Click **Add** to add an account, or select an existing account and click **Edit**.

5. In the **Restore scope** section, select the **Selected objects only** option and click **Choose**.



6. In the **Manage Scope Objects** window, click **Add object** and select what type of objects to display. You can select from the following types: *Hyper-V*, *vSphere*, *Cloud Director*, *Protection Group*, *Unstructured Data* or *Nutanix AHV*.



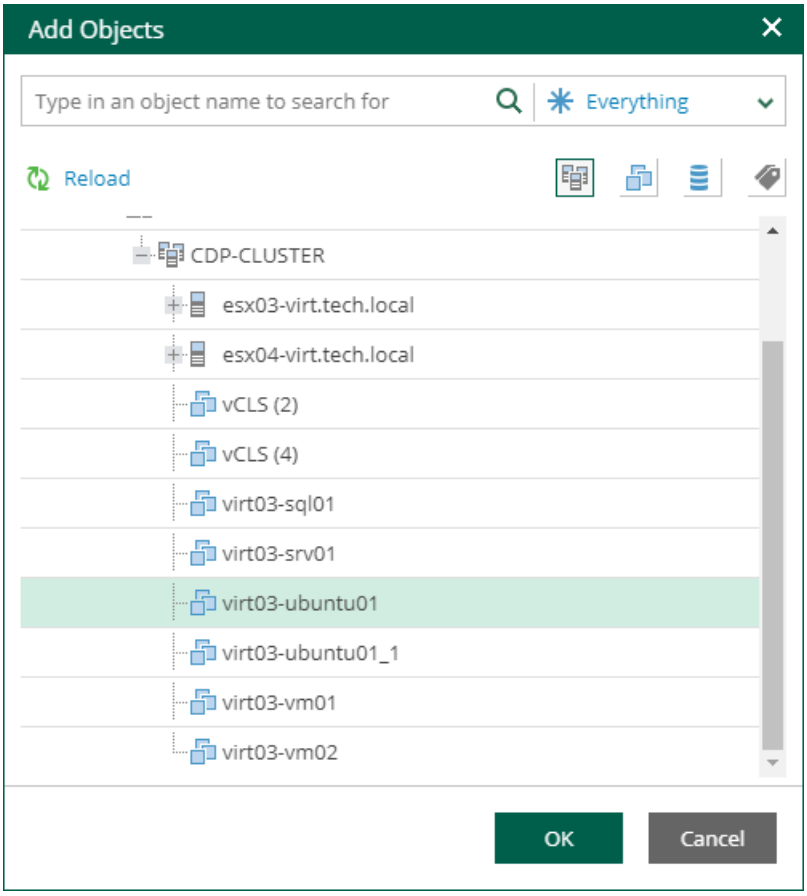
7. In the **Add Objects** window, select the objects you allow the user to restore. Consider that reverse DNS lookup on the Veeam Backup Enterprise Manager server must be functional. Otherwise, the **Add Objects** window may display incomplete infrastructure.

   To search for an object, type a name or its part in the search field. Specify the type of the object from the drop-down list next to the search field.

   You can also use the buttons in the upper-right corner to switch between virtual infrastructure views:

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

- For VMware Cloud Director, protection groups, unstructured data and Nutanix AHV, switching the views is not available.



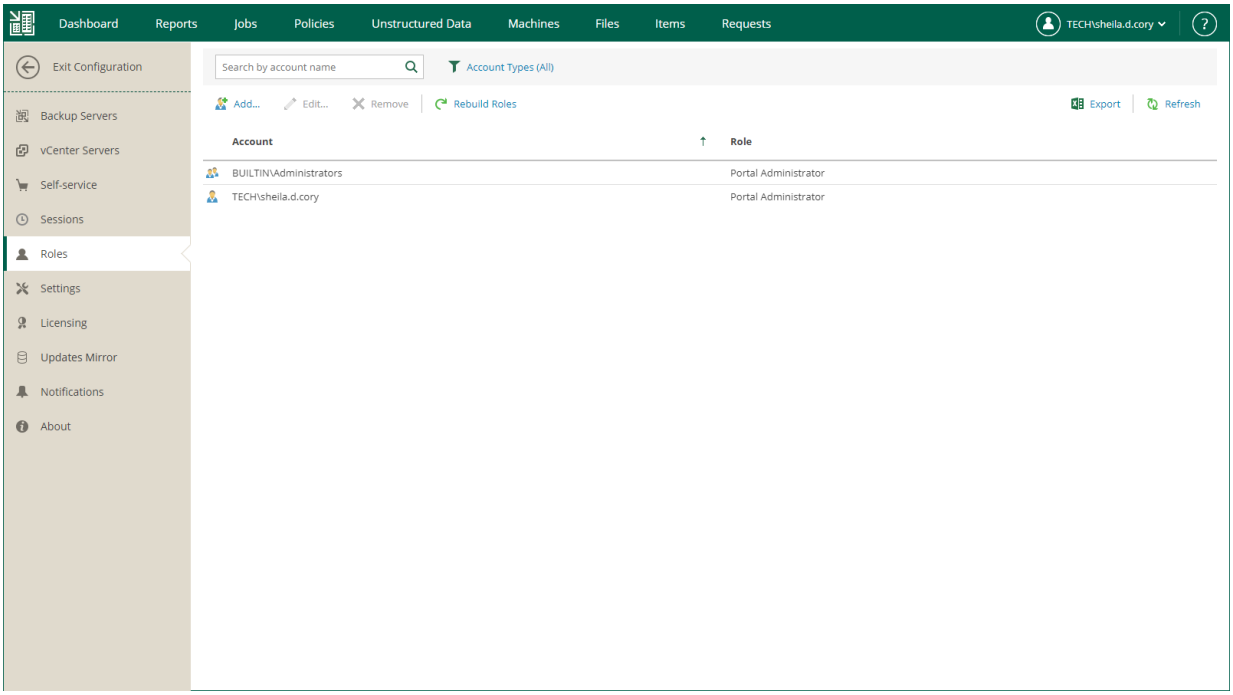
8. Click **OK** to save the settings.

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

> **NOTE**
>
> The **Machines** and **Unstructured Data** tabs display only machines and unstructured data (file shares and object storage systems) that have been backed up. The **Files** tab displays guest OS files only for machines that have been backed up with guest file indexing enabled. For more information on indexing, see Preparing for File Browsing and Searching.

Restore scope is automatically refreshed daily on built-in schedule and after any role modification. It may happen that some newly created machines, file shares and backups are not yet presented to users in the **Machines**, **Unstructured Data** or **Files** tabs right after the login to Enterprise Manager. If you cannot find an object after making a search query, click the **I don't see my VM** link to refresh the view. This link, however, is not visible until you get unsuccessful search results.

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



Configuring Permissions for File and Application Item Restore

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

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

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

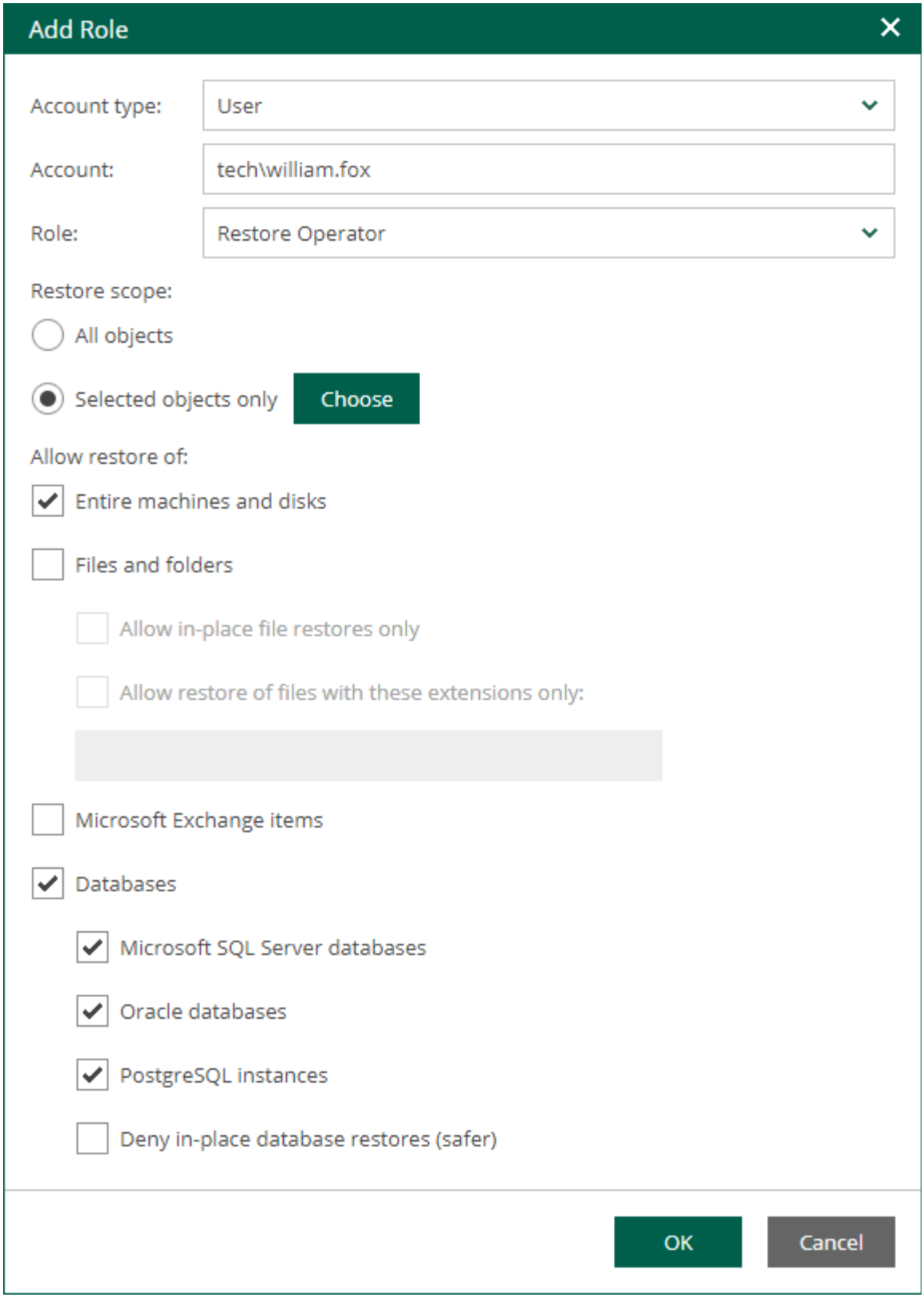
To configure permissions for file and application item restore, take the following steps:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Select the **Roles** section on the left of the **Configuration** view.
4. Click **Add** to add an account, or select an existing account and click **Edit**.
5. In the **Allow restore of** section, to allow restore of entire machines and VM disks of machines included in the restore scope, select the **Entire machines and disks** check box.
6. To allow restore of guest OS files, select the **Files and folders** check box. If you select this check box, you can also select the following options:
   - **Allow in-place file restores only** — select this option to allow file-level restore to the original location only. Consider that the restored files will be available only to accounts that have access to the original machine.

- **Allow restore of files with these extensions only** – select this option to define which file types are allowed for restore. In the text box, enter a list of extensions for allowed file types, separated by commas.

7. To allow restore of Microsoft Exchange items (mail, calendars, tasks), select the **Microsoft Exchange items** check box.
8. To allow restore of databases, select the **Databases** check box. If you select this check box, you can also select the following options:
   - Select **Microsoft SQL Server databases** to allow restore of Microsoft SQL databases on machines included in the user's restore scope.
   - Select **Oracle databases** to allow restore of Oracle databases on machines included in the user's restore scope.
   - Select **PostgreSQL instances** to allow restore of PostgreSQL instances on machines included in the user's restore scope.
   - Select **Deny in-place database restores** to restrict the user from overwriting the original databases during the database restore process.
9. Click **OK** to save the changes.

10. [For Microsoft Exchange items restore] Configure the settings of an Active Directory account that will be used to restore Microsoft Exchange items. For more information, see Configuring Active Directory Account.



Configuring Active Directory Account

You can either preconfigure an Active Directory account that will be used to restore Microsoft Exchange items or choose to specify an account every time you perform the restore operation.

To configure Active Directory account settings, take the following steps:

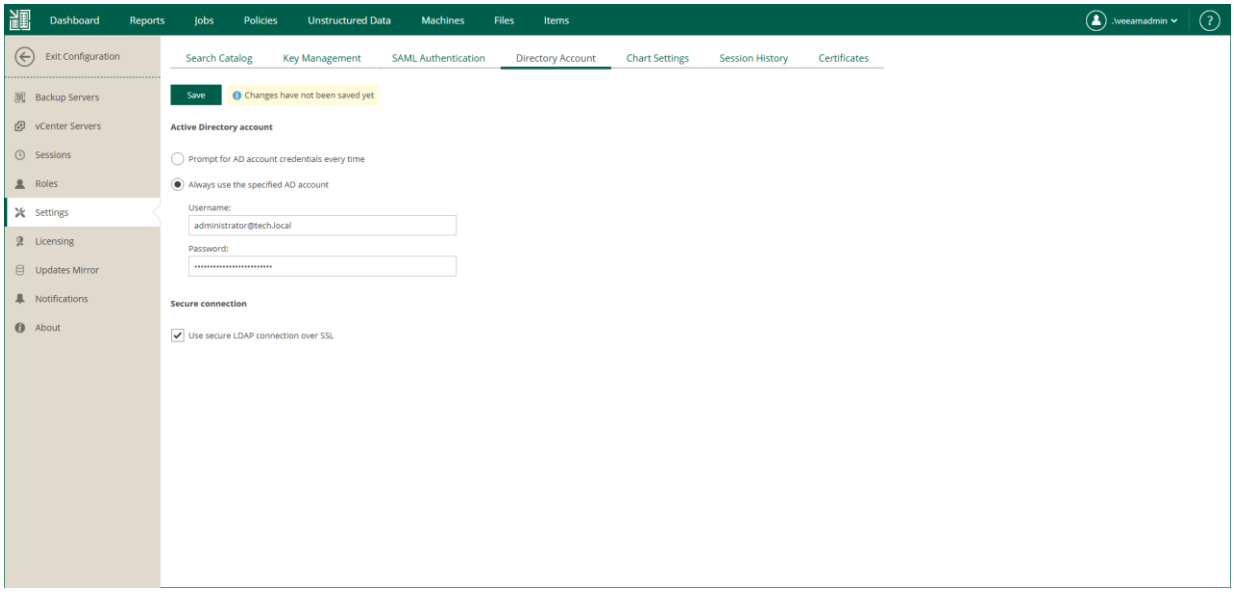
1. Open the **Settings** section of the **Configuration** view.
2. On the **Directory Account** tab, select one of the following options:
   - Select **Prompt for AD account credentials every time** to specify an account every time you perform the restore operation. This allows you to avoid storing account credentials in the Enterprise Manager configuration database.

     This option must be selected if you have Microsoft Exchange servers in different domains.
   - Select **Always use the specified AD account** to use a specific account every time you restore Microsoft Exchange items with Veeam Backup Enterprise Manager. This option is useful if you want to delegate restore operations to a non-administrative user.

     With this option selected, Microsoft Exchange servers must belong to the same Microsoft Active Directory forest.

     In this case, specify an Active Directory account name and password. Make sure the account meets the following requirements:

     - The account must be a member of the *Organization Management* group.
     - The account must have sufficient rights to access mailboxes. To assign these rights, you can use *Exchange Impersonation* or grant the *Full Access* permission to the account. For more information on Exchange Impersonation, see Microsoft Docs.
3. Select **Use secure LDAP connection over SSL** to set Enterprise Manager to connect to the domain controller over the SSL or TLS protocol.
4. Click **Save** to save the changes.



Configuring VMware vSphere Roles

Before you can use the Veeam Plug-in for VMware vSphere Client, you must map the VMware vSphere role that you will use to work with the plug-in with one of the Veeam Backup Enterprise Manager roles. For more information on the plug-in, see Veeam Plug-in for VMware vSphere Client.

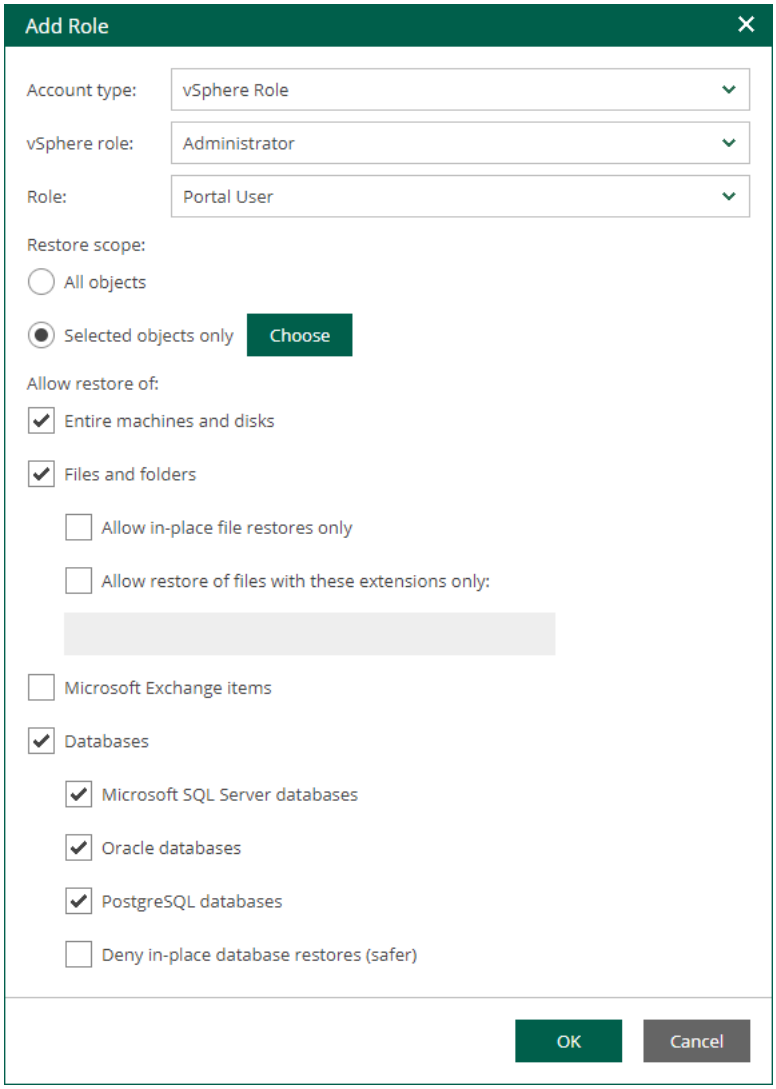
To map a VMware vSphere role, take the following steps:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Roles** section.
4. Click **Add** on the toolbar.
5. From the **Account type** list, select *vSphere Role*.
6. From the **vSphere role** list, select a vCenter Server role created in VMware vSphere that you will use to work with Veeam Plug-in for VMware vSphere Client.
7. From the **Role** list, select a role you want to assign to the account: *Portal Administrator*, *Portal User* or *Restore Operator*. For more information, see Roles.

> **NOTE**
>
> To be able to assign any of portal roles to Active Directory domain users or groups, make sure that Veeam Backup Enterprise Manager service account has sufficient rights to enumerate Active Directory domains (by default, Active Directory users have enough rights to enumerate Active Directory domains).

8. [For Portal User or Restore Operator] In the **Restore scope** section, you can allow a user to restore all objects (machines and file shares) processed by managed backup servers or the selected objects only. For more information, see Configuring Restore Scope.

   In the **Allow restore of** section, you can configure additional restrictions for the restore scope. For more information, see Configuring Permissions for File and Application Item Restore.



Configuring SAML Authentication Settings

Organizations that use single sign-on (SSO) in their infrastructure can allow users to access the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal using their SSO credentials. To enable this functionality, the Enterprise Manager administrator must configure SAML authentication settings.

> **NOTE**
>
> If SAML authentication is enabled, users can log in to vSphere Self-Service Backup Portal under SSO accounts only.

To configure SAML authentication settings:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Open the **Settings** section on the left of the **Configuration** view.
4. Click the **SAML Authentication** tab.
5. Select the **Enable SAML 2.0** option.
6. In the **Identity Provider Configuration** section, specify identity provider settings. For more information, see Specifying Identity Provider Settings.
7. [Optional] If you want to use a certificate to encrypt and sign service provider SAML requests, specify certificate settings. For more information, see Selecting Service Provider Certificate.
8. [Optional] Click the **Advanced Settings** link and specify advanced SAML authentication settings. For more information, see Specifying Advanced SAML Authentication Settings.
9. In the **Enterprise Manager Configuration** section, export or manually copy the service provider metadata for Veeam Backup Enterprise Manager. Use the metadata to register Enterprise Manager as a service provider on the identity provider side. This will enable SSO for both Enterprise Manager and vSphere Self-Service Backup Portal. For more information, see Obtaining Service Provider Settings.
10. Click **Save**.

After you configure SAML authentication settings, you can register user accounts that will be able to log in to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal using SSO. For more information, see Configuring Accounts and Roles and Managing Tenant Accounts.

Specifying Identity Provider Settings

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

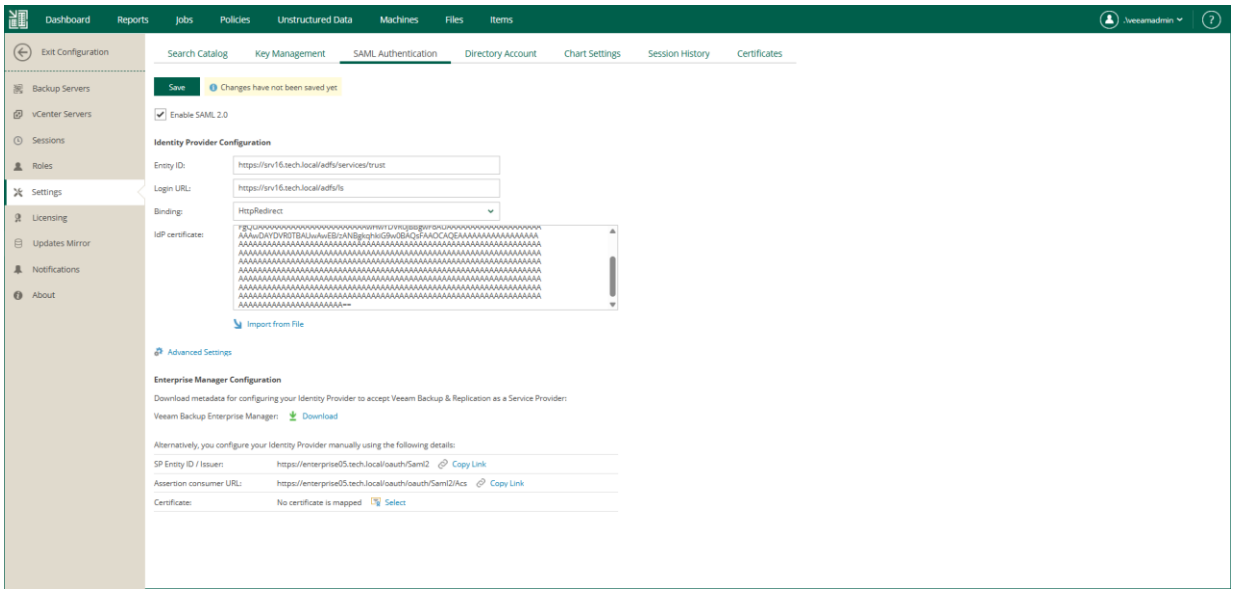
- Import identity provider settings from a SAML metadata file obtained from the identity provider.
- Specify identity provider settings manually.

To import identity provider settings from the SAML metadata file, in the **Identity Provider Configuration** section of the **SAML Authentication** view, click the **Import from File** link and browse to the metadata file. The metadata file structure must conform to the SAML 2.0 Metadata Schema.

Alternatively, you can specify identity provider settings manually:

1. In the **Identity Provider Configuration** section, in the **Entity ID** field, specify a unique ID of the identity provider.
2. In the **Login URL** field, specify the URL of the single sign-on login page provided by the identity provider.
3. From the **Binding** list, select a SAML binding used by the identity provider to send SAML responses: *HttpRedirect* or *HttpPost*.
4. In the **IdP certificate** field, specify a certificate that will be used to validate the signature of the signed authentication assertions and decrypt assertions sent by the identity provider.

> **NOTE**
>
> Veeam Backup Enterprise Manager does not support identity provider certificate rollover.



Selecting Service Provider Certificate

If you want to sign and encrypt authentication requests sent from Veeam Backup Enterprise Manager to the identity provider, you must select a certificate with a private key that will be used for encryption and signing. To select a certificate:

1. In the **Enterprise Manager Configuration** section of the **SAML Authentication** view, click the **Select** link next to the **Certificate** field.
2. In the **Select Service Provider Certificate** window, Veeam Backup Enterprise Manager will display certificates located in the certificate store on the Enterprise Manager server. Choose the necessary certificate from the list and click **Select**.

If you use a certificate to sign end encrypt SAML authentication requests, you must pass the public key certificate to the identity provider. The identity provider will use this certificate to encrypt requests and validate the request signature. For more information, see Obtaining Service Provider Settings.

TIP

Consider the following:

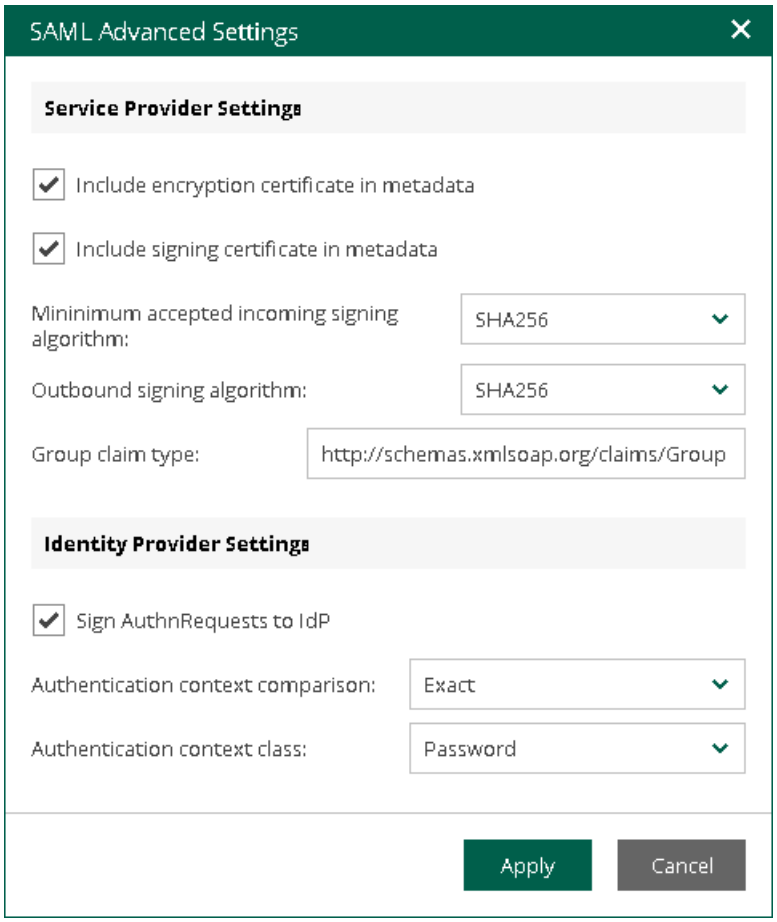
- To change the service provider certificate, click the **Remove** link next to the **Certificate** field. Then select another certificate from the certificate store.
- You can choose whether to include the certificate in the service provider metadata. For more information, see Specifying Advanced SAML Authentication Settings.

Specifying Advanced SAML Authentication Settings

In the **SAML Advanced Settings** window you can specify advanced settings for SAML authentication.

1. To include in the service provider SAML metadata a security certificate required to decrypt service provider authentication requests, select the **Include encryption certificate in metadata** check box.
2. To validate the signature of the signed requests, select the **Include signing certificate in metadata** check box.
3. From the **Minimum accepted incoming signing algorithm** and **Outbound sign algorithm** lists, select what type of signed requests and responses Enterprise Manager will be able to send and receive. By default, the *SHA256* option is selected. With this option selected, Enterprise Manager will send and receive requests and responses signed using the SHA256 or stronger algorithm.
4. By default, to provide for single sign-on authentication for groups of users, Veeam Backup Enterprise Manager accepts information about groups from the identity provider in statements of the *Group* type. If it is required to use for this purpose statements of a different type, in the **Group claim type** field, specify the necessary type.
5. If you want to sign authentication requests sent from Enterprise Manager to the identity provider with a digital certificate, in the **Identity Provider Settings** section, select the **Sign AuthnRequests to IdP** check box.
6. From the **Authentication context comparison** list, select a comparison method for authentication context: *Exact*, *Minimum*, *Maximum* or *Better*.
7. From the **Authentication context class** list, select one of the classes to specify an authentication method used by the Identity Provider. By default, the *Password* option is selected. For details on authentication context classes, see Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0.

8. Click **Apply**.



Obtaining Service Provider Settings

To set up SAML authentication for the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal, you need to register Enterprise Manager as a service provider on the identity provider side. To do this, obtain service provider settings and provide them to the identity provider.

You can obtain service provider settings in one of the following ways:

- Export service provider settings to an XML file
- Copy service provider settings

Exporting Service Provider Settings

You can export the service provider settings to a SAML metadata file, which is an XML file that conforms to the SAML 2.0 Metadata Schema. If you want to use a certificate to sign and encrypt SAML authentication requests, you must pass the public key certificate to the identity provider and include the certificate in the metadata file. For more information, see Specifying Advanced SAML Authentication Settings.

To export service provider settings for the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal, click the **Download** link next to the **Veeam Backup Enterprise Manager** field.

Copying Service Provider Settings

To copy service provider settings for the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal, do the following:

1. Copy the links next to the **SP Entity ID / Issuer** and **Assertion consumer URL** fields.
2. If you have selected a certificate that will be used to sign end encrypt SAML authentication requests, you must also pass the public key certificate to the identity provider. To copy the certificate, click the **Download** link next to the **Certificate** field.

Related Topics

SAML Authentication Support

SAML Authentication Support

Veeam Backup Enterprise Manager supports single sign-on authentication based on the SAML 2.0 protocol. Enterprise organizations who use a single sign-on (SSO) service in their IT infrastructure can extend single sign-on capabilities to Veeam Backup Enterprise Manager. Once a user of the organization is logged in to the single sign-on service, the user can access Veeam Backup Enterprise Manager without the need to provide their credentials.

You can enable SSO for the following Veeam Backup Enterprise Manager components:

- Veeam Backup Enterprise Manager website
- vSphere Self-Service Backup Portal

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

- User that logs in to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal.
- Service provider (SP) — an application accessed by the user. In the Veeam backup infrastructure, the service provider is the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal.
- Identity provider (IdP) — an external service (hosted on premises or in the public cloud) that facilitates SSO. The IdP keeps user identity data in a user store (or attribute store). Upon requests from the SP, the IdP issues SAML authentication assertions, that is, identifies the user and provides the SP with required information about the user.

  Veeam Backup Enterprise Manager supports identity providers that support the SAML 2.0 protocol, for example, Active Directory Federation Services (AD FS), Azure Active Directory (Azure AD), Okta, Auth0, Keycloak and so on.

The SP and IdP exchange information in the XML format in accordance with the SAML V2.0 Standard. The Enterprise Manager administrator can specify what information is required from the IdP to set up SAML authentication in Enterprise Manager and how SAML requests and responses are sent.

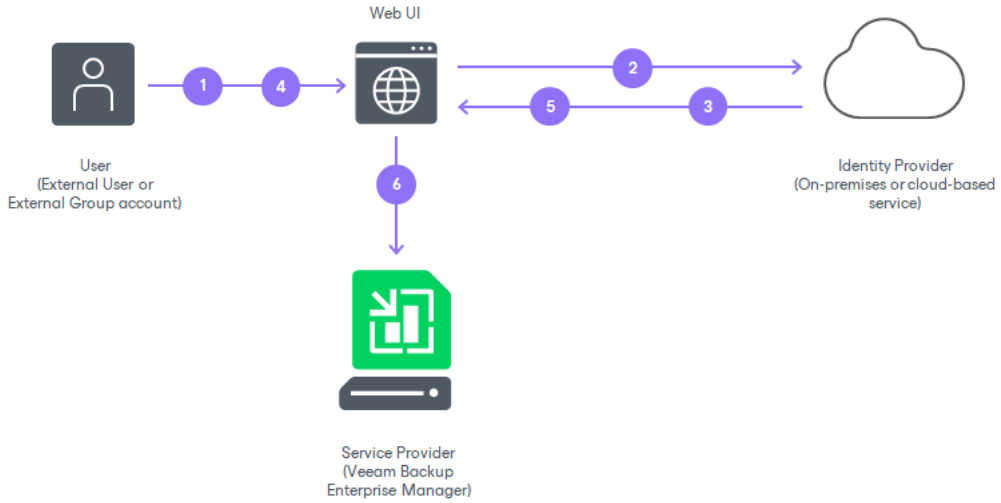
How It Works

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

1. The user accesses the website under an account of the *External* type. The account must be added in advance in Enterprise Manager by the Enterprise Manager administrator. For details on how to add an account, see Managing Accounts.
2. Veeam Backup Enterprise Manager redirects a SAML authentication request to the IdP.
3. If the user has not previously logged in with the single sign-on service of the IdP, the IdP redirects the user to the URL of the single sign-on webpage.

   Alternatively, if the user is already logged in with the single sign-on service, the user proceeds directly to the step 6.
4. If the user has not previously logged in with the single sign-on service, the user specifies the password of their account on the single sign-on webpage.
5. The IdP issues a SAML assertion and redirects it to Veeam Backup Enterprise Manager in the SAML response. The SAML assertion must meet the following requirements:
   - Contain a User Principal Name (UPN) of the user in the *<NameID>* element of the SAML response.
   - Specify that the UPN type is *Persistent*.

6. The user gains access to the website and can perform operations according to the role and restore scope specified for the user account.



Getting Started

To set up SAML authentication, the Enterprise Manager administrator must complete the following tasks in Enterprise Manager:

1. Obtain SAML metadata from the IdP and import this metadata to Veeam Backup Enterprise Manager. The IdP metadata includes the IdP entity ID, login URL, SAML binding and public key certificate that will be used to validate authentication assertions sent by the IdP. For more information, see Specifying Identity Provider Settings.
2. [Optional] If you want to use a digital certificate to encrypt and sign SP SAML requests, specify certificate settings. For more information, see Selecting SP Certificate.
3. [Optional] Specify advanced settings for SAML authentication. These settings define how the SP and IdP will exchange SAML information. You may want to adjust the settings to strengthen SAML information exchange between the SP and IdP. For more information, see Specifying Advanced SAML Authentication Settings.
4. Export SP SAML metadata in Veeam Backup Enterprise Manager and pass this metadata to the IdP. The SP metadata includes the SP entity ID, assertion consumer URL and public key certificate that will be used to encrypt SAML responses sent by the IdP. For more information, see Obtaining Service Provider Settings.
5. Create user accounts. To provide users of a SSO service with access to the Veeam Backup Enterprise Manager website or vSphere Self-Service Backup Portal, the administrator must create for these users accounts of the *External User* or *External Group* type. For more information, see Configuring Accounts and Roles and Managing Tenant Accounts.

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

Related Tasks

- Configuring SAML Authentication Settings
- Configuring Accounts and Roles

Configuring AD FS for SAML Authentication

Active Directory Federation Service (AD FS) is a hosted identity provider implemented as a feature in the Windows Server OS. It provides single sign-on capabilities for Active Directory (AD) users. If AD FS is used as the identity provider in the organization, to let AD users log in to the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal using the single sign-on service, an IT administrator must register the Veeam Backup Enterprise Manager website and vSphere Self-Service Backup Portal as service providers in AD FS.

To add a service provider in AD FS:

1. Obtain the service provider metadata exported from Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.
2. In AD FS, add a Relying Party Trust using the service provider metadata.
3. Edit the Claim Issuance Policy for the added Relying Party Trust to add an issuance transform rule with the following properties:
   - **Claim rule template** = *Transform an Incoming Claim*
   - **Incoming claim type** = *UPN*
   - **Outgoing claim type** = *NameID*
   - **Outgoing name ID format** = *Persistent Identifier*
4. [Optional] To provide single sign-on capabilities to AD groups, add to the Claim Issuance Policy an issuance transform rule with the following properties:
   - **Claim rule template** = *Send Group Membership as a Claim*
   - **User's group** = *<Name>*

     where *<Name>* is a name of the AD group that includes users that will access the service provider.

     When a user that belongs to the specified group attempts to access the service provider, the identity provider will issue an authentication assertion confirming that the user belongs to the group.
   - **Outgoing claim type** = *Group*

     Alternatively, if a different value is specified for the **Group claim type** option of advanced SAML settings in Enterprise Manager, the same value must be specified as the outgoing claim type in AD FS.
   - **Outgoing claim value** = *<Name>*

     where <Name> is a name of the group that will be returned to the service provider in authentication assertions.

     This value can be different from the **User's group** value, for example, if you do not want the service provider to display AD group names. This value must be the same as the name of the account of the External Group type added in Enterprise Manager. For more information, see Configuring Accounts and Roles and Adding Tenant Account.

   For example, you want to provide single sign-on capabilities to users that belong to the *Backup* AD group. In Enterprise Manager, you have the *EnterpriseUsers* account of the External Group type, and the default group claim type is specified in advanced SAML settings.

   To allow these users to log in to Enterprise Manager with the single sign-on service, you must create an issuance transform rule with the following properties:

   - **Claim rule template** = *Send Group Membership as a Claim*

- **User's group** = *Backup*
- **Outgoing claim type** = *Group*
- **Outgoing claim value** = *EnterpriseUsers*

Related Topics

- SAML Authentication Support
- Configuring SAML Authentication Settings

Configuring Retention Settings for Index and History

Veeam Backup Enterprise Manager allows you to configure retention settings for index files and event history. For details on data indexing, see Veeam Backup Catalog.

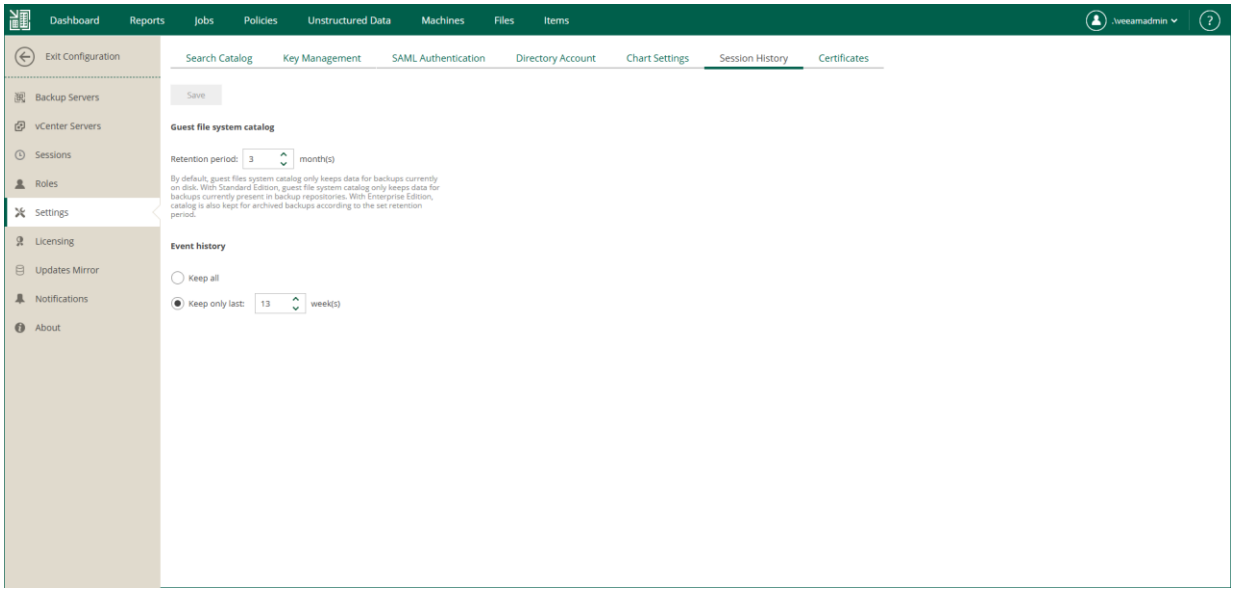
- If you use the Standard edition of Veeam Backup & Replication in your virtual environment, Veeam Backup Enterprise Manager keeps index files only for those backups that are currently stored on disk (that is, the backups are available on backup repositories).
- If you use the Enterprise or Enterprise Plus edition, 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 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.

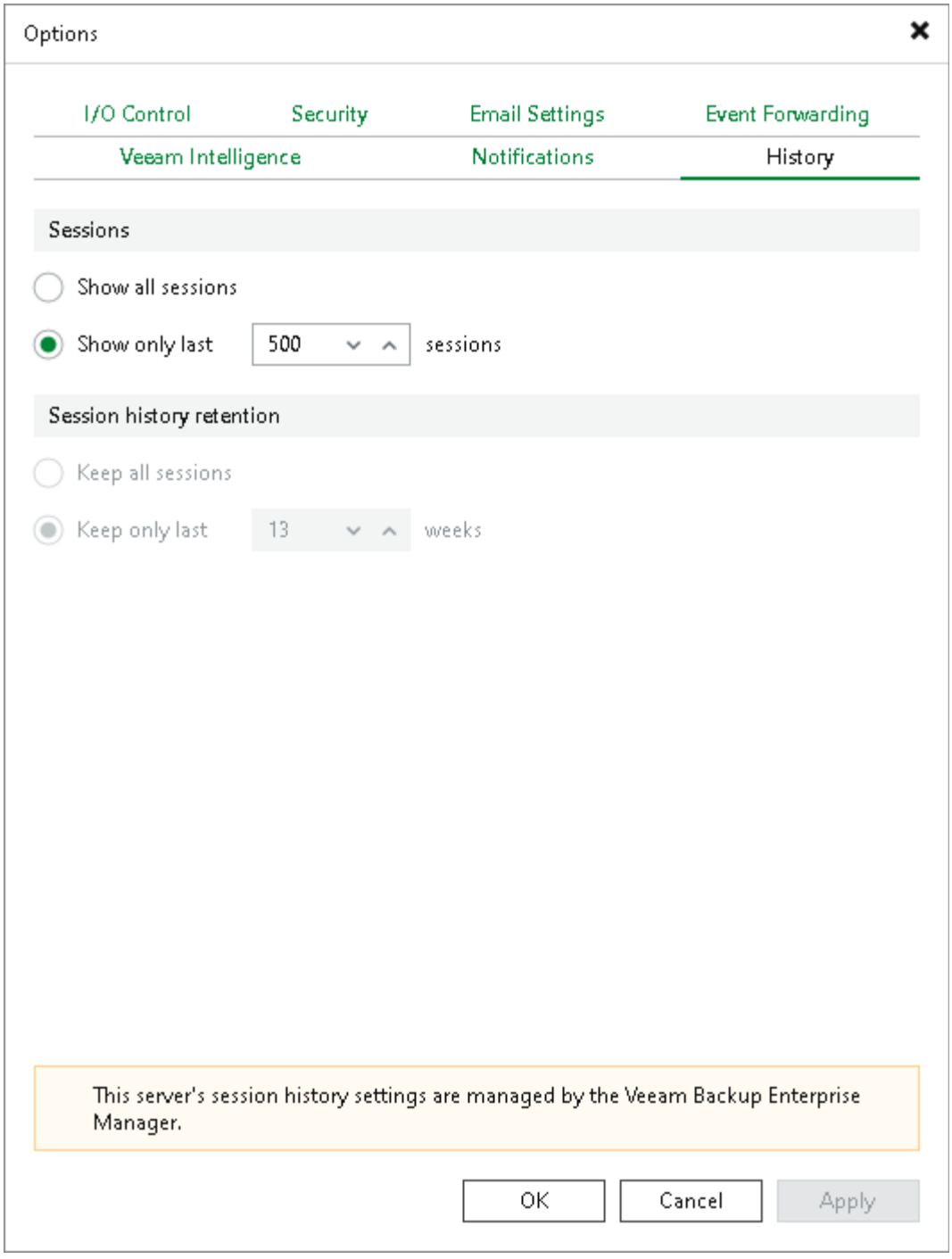
To configure retention settings, take the following steps:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. Open the **Settings** section on the left of the **Configuration** view.
4. On the **Session History** tab, in the **Guest file system catalog** section, specify how long index files must be stored on the Enterprise Manager server:
    a. Enter the desired number of months in the **Retention period, months** field. The default value is 3 months, the minimum allowed value is 1 month, and the maximum allowed value is 120 months, or 10 years.
    b. When finished, click the **Save** button under the **Event history** section. New retention settings will be saved in the Enterprise Manager database, and a message notifying you on the update will be displayed at the top of the window.
5. In the **Event history** section, specify the period for which Enterprise Manager should keep historical data available in the main working area of the Enterprise Manager website.
    a. Enter the desired number of weeks or select **Keep all**. By default, the retention period for session data is set to 13 weeks. The minimum allowed value is 1 week, and the maximum allowed value is 999 weeks.

b. When finished, click **Save**. New retention settings will be saved in the Enterprise Manager database, and a message notifying you on the update will be displayed at the top of the window.



Note that the retention settings you specify in Enterprise Manager are propagated to all backup servers connected to it. These settings override the **Session history retention** values specified in Veeam Backup & Replication. For example, if the retention option of a backup server is set to keep the session history for *15 weeks*, and in Enterprise Manager you select to *Keep only last 13 weeks*, the Enterprise Manager value will be propagated to the backup server; so the history will be kept for *13 weeks*.



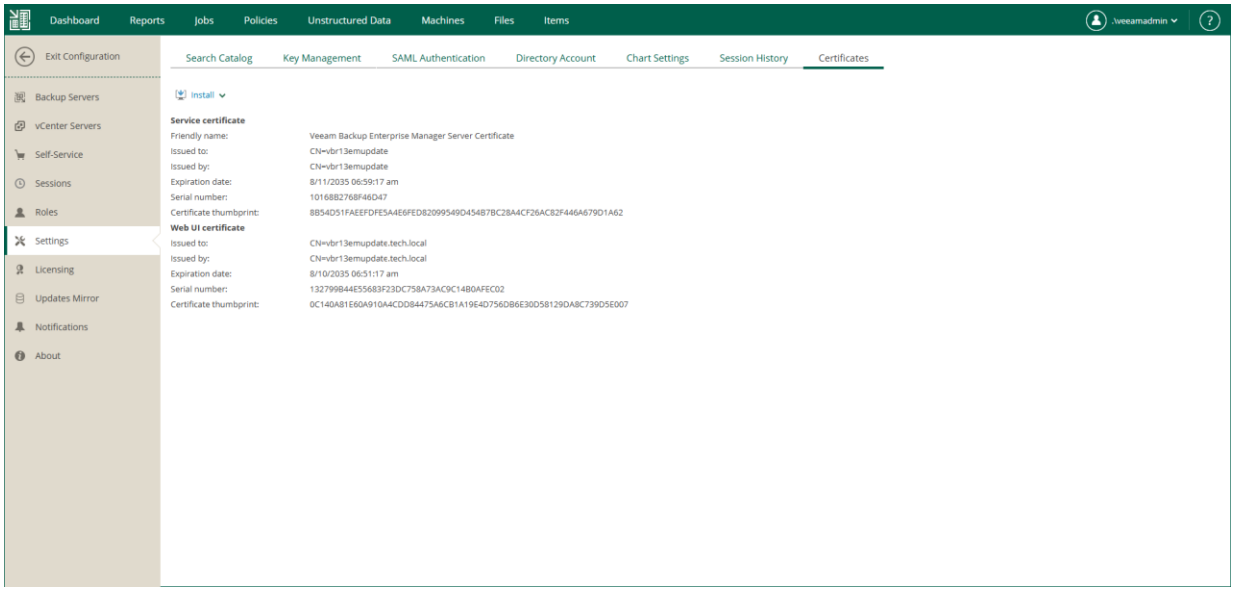
Managing TLS Certificates

TLS certificates ensure a secure connection with Veeam Backup Enterprise Manager over HTTPS. By default, Veeam Backup Enterprise Manager uses the same TLS certificate for all connections. If you want to use different certificates for different components, you can install new certificates. For more information, see Installing Certificates. The certificate is bound to Enterprise Manager, the REST API and their ports.

- During the Enterprise Manager installation on Linux, a self-signed certificate is generated.
- During the Enterprise Manager installation on Microsoft Windows, you can select an existing certificate or generate a new self-signed certificate.

Enterprise Manager use the following certificates:

- *Server certificate* is used by the Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service to communicate with backup servers added to the Enterprise Manager infrastructure. For more information, see How Enterprise Manager Authenticates to Backup Servers. The same certificate is used by the Veeam Backup Enterprise Manager REST API Service to communicate with REST API clients.
- *Web UI certificate* is used by the Veeam Backup Enterprise Manager web application, Veeam Plug-in for VMware vSphere Client, and Veeam Plug-in for VMware Cloud Director to communicate with the web browser.



How Enterprise Manager Authenticates to Backup Servers

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

Certificate-based connection works in the following way:

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

   For more information, see Adding Backup Servers.

2. Veeam Backup Enterprise Manager sends the credentials as well as the server certificate thumbprint that will be used by Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service for authentication.

3. Veeam Backup & Replication validates the credentials and saves Enterprise Manager data including the certificate thumbprint.

4. Veeam Backup & Replication sends its certificate thumbprint to Enterprise Manager.

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

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

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

6. The next time Enterprise Manager connects to Veeam Backup & Replication, the Enterprise Manager server certificate is used for authentication.

7. If a backup server certificate is updated, you will have to validate it from Enterprise Manager. Until you validate the certificate, Enterprise Manager cannot collect data from the backup server.

8. Thirty days before the Enterprise Manager certificate is expired, you are prompted to update it.

   For more information, see Installing Certificates.

Installing Certificates

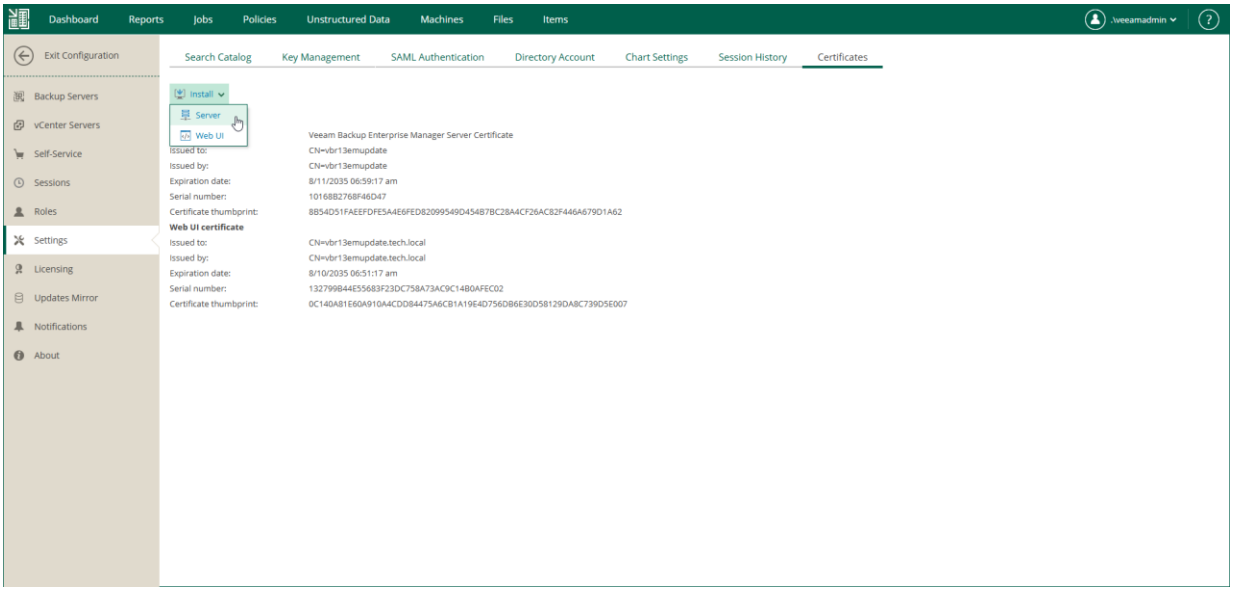
If an existing TLS certificate expires, or if you want to replace it (for example, with a certificate obtained from a Certificate Authority) you can install a new certificate. When using a certificate obtained from a CA, ensure that the Enterprise Manager IP address or fully qualified domain name is included in the certificate subject or subject alternative name.

If you plan to use a certificate signed by an internal Certificate Authority (CA), add the certificate to the certificate store before starting the installation. For details, see Using Certificate Signed by Internal CA.

> **NOTE**
>
> For Microsoft Windows-based Enterprise Manager, to update the certificate used by the Enterprise Manager web application and Veeam vSphere Client plug-in, you can also use Internet Information Services (IIS) Manager as an alternative method. For more information, see this Microsoft Docs article.

To install a new certificate, follow these steps:

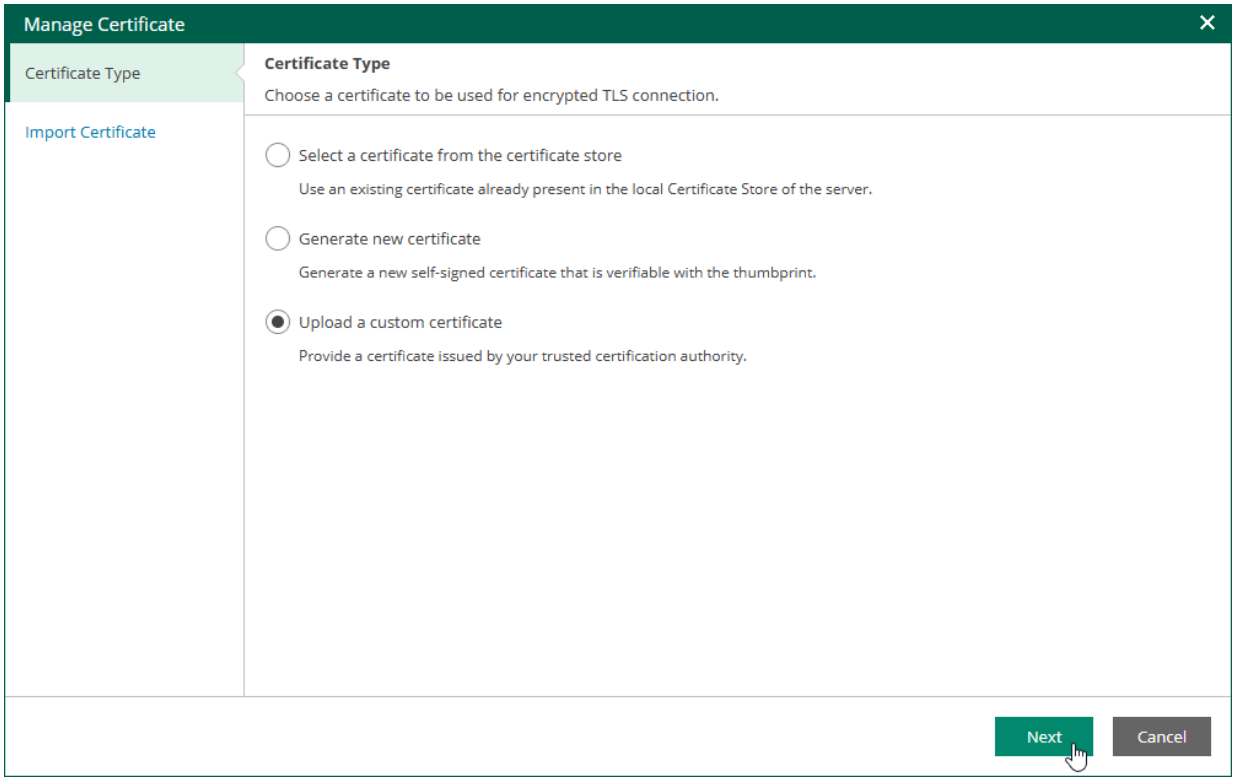
1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Open the **Settings** section.
4. On the **Certificates** tab, click **Install** and then choose the type of certificate to install:
   - Select **Server** to install the certificate that the Veeam Backup Enterprise Manager Service and Veeam Guest Catalog Service use to connect to backup servers. This certificate is also used by the Veeam Backup Enterprise Manager REST API.
   - Select **Web UI** to install the certificate that the Veeam Backup Enterprise Manager web app, Veeam Plug-in for VMware vSphere Client, and Veeam Plug-in for VMware Cloud Director use to connect to the web browser.



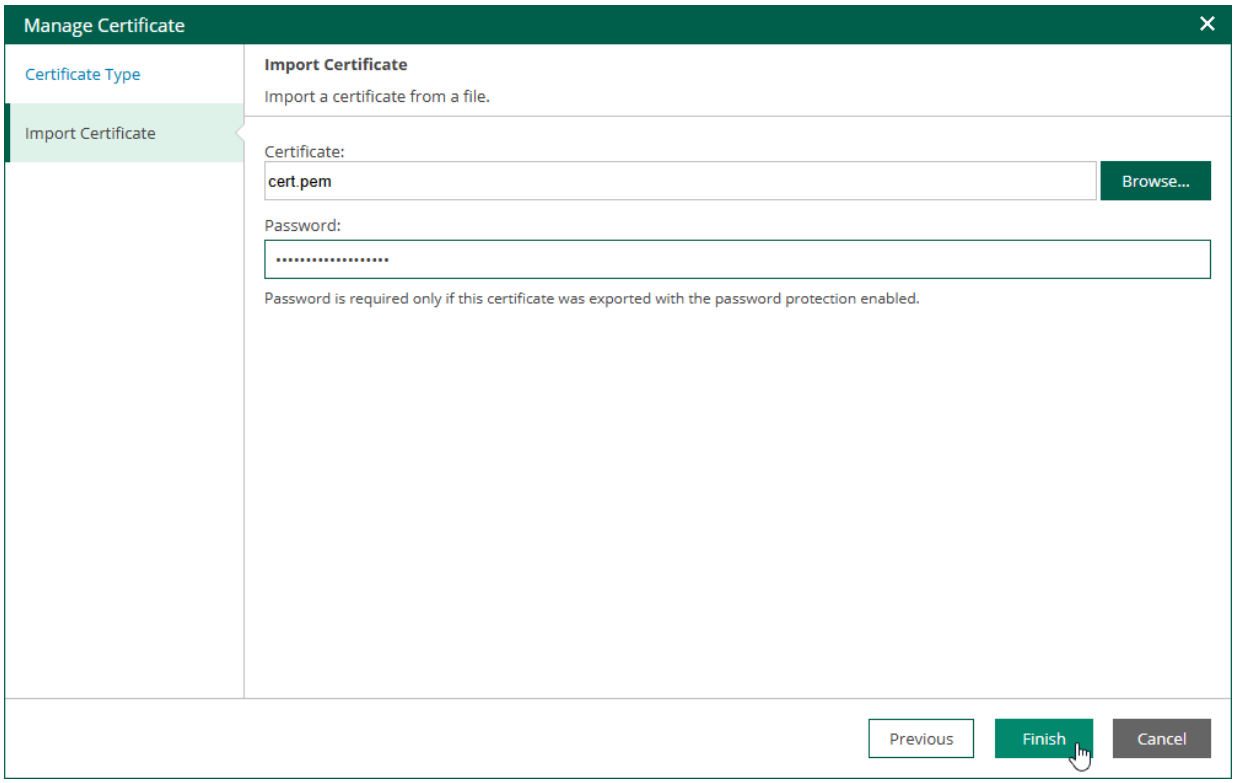
5. At the **Certificate Type** step of the **Manage Certificate** wizard, select one of the following options:
   - Select **Select a certificate from the certificate store** to use a certificate that is already uploaded to the local Certificate Store.
   - Select **Generate new certificate** if you want Enterprise Manager to generate a self-signed certificate.

- Select **Upload a custom certificate** to upload a certificate signed by your trusted Certificate Authority (CA). For more information on internal CA certificates, see Using Certificate Signed by Internal CA.

  Enterprise Manager accepts only PEM files that contain exactly two key sections: the private key and the server certificate. If the file contains multiple certificates, the upload fails with the following error: *PEM contains multiple public key sections*. In this case, keep only the private key and the server certificate in the PEM file, and remove all other certificates. Add intermediate certificates separately to the certificate store on the connected backup servers.



6. At the next step of the wizard, either provide a certificate friendly name for a self-signed certificate or choose an existing certificate that you want to install.



7. To install the certificate, click **Finish**.

Using Certificate Signed by Internal CA

You can use a certificate signed by an internal Certificate Authority (CA) as the server or web UI certificate to secure Enterprise Manager connections with other components and web browsers.

Before you install a certificate signed by an internal CA, add the certificate to the certificate store on the Enterprise Manager machine to ensure that Enterprise Manager trusts the CA.

Certificate Requirements

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

Requirement	Description
Subject	Set to the fully qualified domain name (FQDN) of the Enterprise Manager server.
Subject Alternative Name (SAN)	Include both the FQDN and the NetBIOS name. You can specify multiple DNS entries in the following format: *DNS:emserver.domain.local, DNS:emserver*
Key Size	Minimum 2048 bits.
Key Usage	For the server certificate, enable the following extensions: • *Digital Signature* • *Certificate Signing* • *Off-line CRL Signing* • *CRL Signing (86)* For the web UI certificate, enable the *Data Signature* extension.
Basic Constraints	Set **Path Length Constraint** to *0*.
Key Type	Set to *Exchange*.
	IMPORTANT The following certificates are not supported: • Elliptic Curve Signature (ECC) certificates • Cryptography API: Next Generation (CNG) certificates You cannot use certificates issued by public CAs as the server certificate, but you can use them as the web UI certificate.

CRL Requirements

Ensure that Certificate Revocation List (CRL) published by a CA and containing revoked certificates is accessible from the Enterprise Manager server to verify certificate status. The CRL must meet the following requirements:

- CRL is accessible from the Enterprise Manager server to verify certificate status.
- CRL must have an HTTP endpoint.
- CRL must be signed with a strong cryptographic algorithm such as RSA-SHA256.

Configuring Certificate Templates in Windows Server CA

If you use Windows Server Certification Authority for managing certificates, perform the following steps to configure a suitable certificate template:

1. Open the **Certificate Templates** Microsoft Management Console (MMC) snap-in.
2. Select a template based on the built-in **Subordinate Certification Authority** template or a similar template.
3. On the **Extensions** tab, enable the **Do not allow subject to issue certificates to other CAs** option.
4. Issue an Enterprise Manager certificate based on this template.

Adding Certificate to Certificate Store

If you want to use a certificate signed by an internal CA, ensure that Enterprise Manager trusts the CA. After you add the certificate to the certificate store, you can install the certificate. If you attempt to install a certificate without adding it to the store first, the installation will fail. For details on how to install an Enterprise Manager certificate, see Installing Certificates.

- For Microsoft Windows-based Enterprise Manager, add the certificate to the Trusted Root Certification Authority store.
- For Linux-based Enterprise Manager, copy the CA certificate to the `/etc/pki/ca-trust/source/anchors/` directory in the PEM format, and then run the following command as the root user.

```
update-ca-trust extract
```

Licensing

The Veeam Backup & Replication infrastructure requires a license to process backup and replication jobs. Using Enterprise Manager to manage Veeam Backup & Replication licenses reduces administration overhead. You can manage and activate licenses for the entire backup infrastructure from a single web console. Enterprise Manager allows you to view what workloads consume instances in the license, install a new license, and revoke the license from protected workloads.

Veeam Backup Enterprise Manager collects information about the type of license installed on added backup servers and the number of instances in the license. When Enterprise Manager collects data from backup servers, it also synchronizes license data by checking if the license installed on the backup server matches with the license installed on the Enterprise Manager server. If the licenses do not match, the license on the backup server is automatically updated to match the license of the Enterprise Manager server.

When you run a job, Enterprise Manager uses instances required for each type of protected workloads. If a workload is protected by multiple backup servers added to the Enterprise Manager infrastructure, the workload will consume the Enterprise Manager license only once.

Before You Begin

Before you install a new license, consider the following:

- Enterprise Manager on Linux supports the following instance-based licenses:
  - Subscription license
  - Rental license (Foundation, Advanced and Premium packages)
  - Perpetual license
  - Evaluation and NFR licenses

  Socket licenses are supported for Enterprise Manager on Windows only.
- You cannot use the same Enterprise Manager server to manage backup servers that require different licenses, for example, a backup server of a Veeam Cloud Connect service provider and a regular backup server used to process Veeam Backup & Replication jobs. For example, you add to Enterprise Manager a backup server with the Veeam Cloud Connect service provider license installed. Enterprise Manager will obtain information about the license and save it to its database. If you then add another backup server with a different type of license installed, Enterprise Manager will install the Veeam Cloud Connect service provider license on this backup server. As a result, you will be able to use the second backup server to configure the Veeam Cloud Connect infrastructure, and will not be able to use this server to run backup and replication jobs.
- You cannot install a license intended for version 13 on a backup server running Veeam Backup & Replication 12.
- If a backup server running an earlier version uses a different license type than Enterprise Manager, the backup server existing license will remain unchanged and the Enterprise Manager license will not be applied to the backup server. However, all workloads protected by the backup server will still be count toward the Enterprise Manager license.
- For information on Veeam Backup & Replication license types, see the Licensing section of the Veeam Backup & Replication User Guide.
- For information on Veeam Cloud Connect license types and license management tasks, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

- For more information on Veeam licensing, see Veeam Licensing Policy.

In This Section

- Installing License
- Viewing License Details
- Updating License
- Revoking License
- Removing License
- Managing Monthly Usage Reports

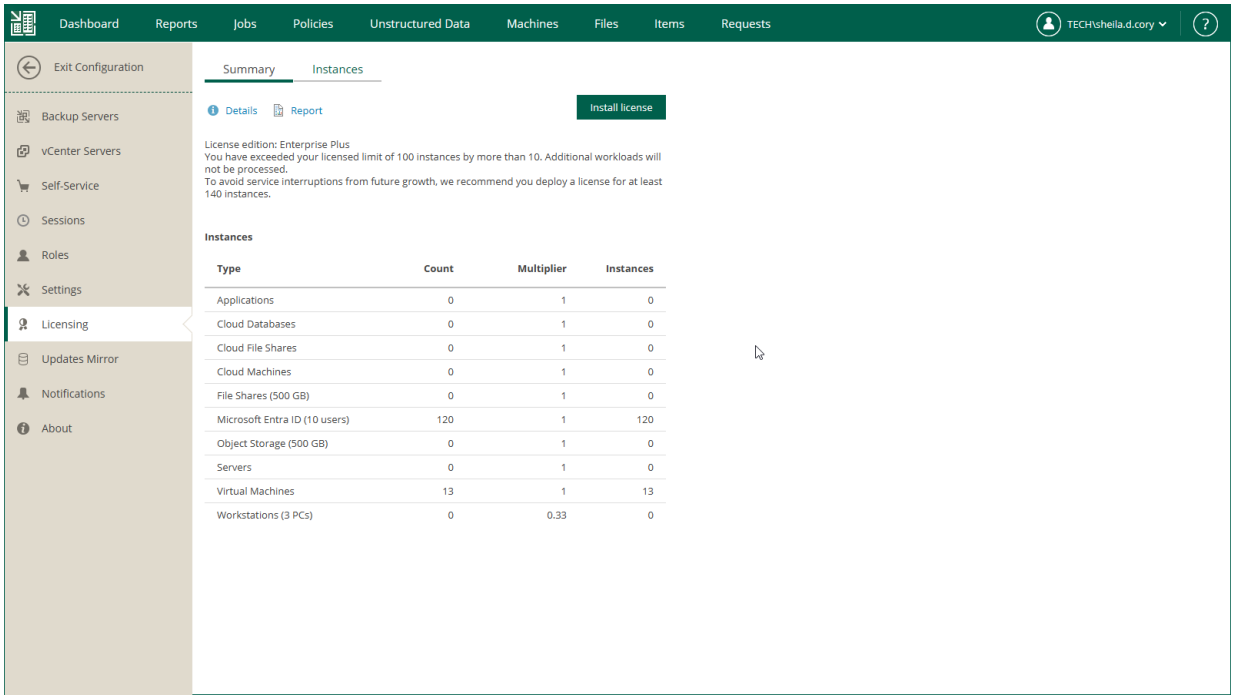
Installing License

When you first log in to Veeam Backup Enterprise Manager after the deployment, you must install a license. The license will be automatically applied to all backup servers added to Enterprise Manager. This approach simplifies tracking license usage and license updates across multiple backup servers.

Before you install a license, read the considerations and limitations.

To install a license, take the following steps:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Install license**.
5. Select the necessary LIC file and click **Open**.



Viewing License Details

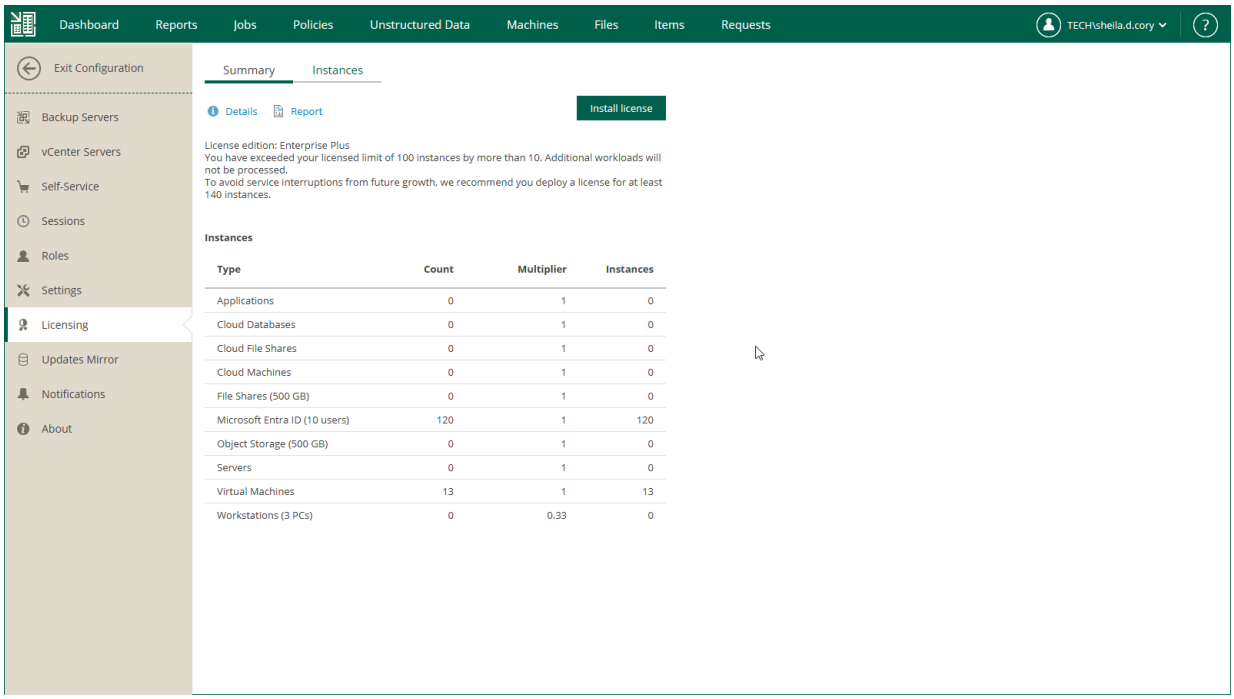
You can view information about the license edition, license state and a spreadsheet of the available and used instances per each type of protected workloads: Microsoft Entra tenants, virtual machines, physical servers and physical workstations, cloud machines, applications, file shares.

When you run a job, Enterprise Manager uses instances required for each type of protected workloads for per-instance licenses or applies a license to the protected hosts for per-socket licenses. If a workload is protected by multiple backup servers added to the Enterprise Manager infrastructure, the workload will consume the Enterprise Manager license only once.

For more information on Veeam licensing, see Veeam Licensing Policy.

To view license details:

1. Sign in to Veeam Backup Enterprise Manager under an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Licensing** section.



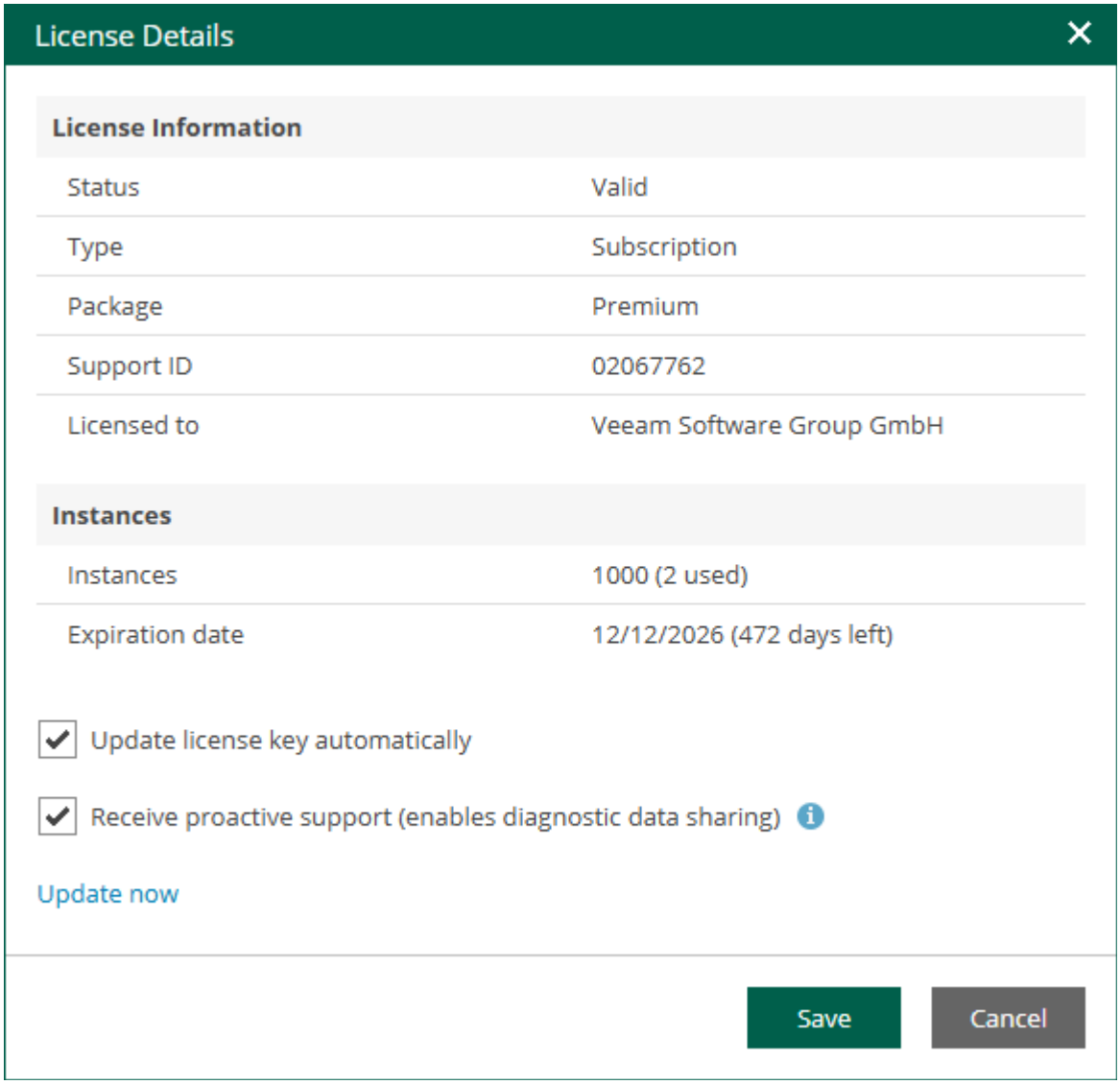
TIP

You can configure Veeam Backup Enterprise Manager to send notifications about expiring license. For more information on the Veeam Backup Enterprise Manager notification functionality, see Configuring Notification Settings.

NOTE

Veeam Backup Enterprise Manager does not display information about instances consumed in the Veeam Cloud Connect service provider license by tenant workloads. This information is available only on the backup server of the service provider. For more information, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

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



Updating License

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

You can use the following methods to update the license:

- Updating license manually
- Updating license automatically

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

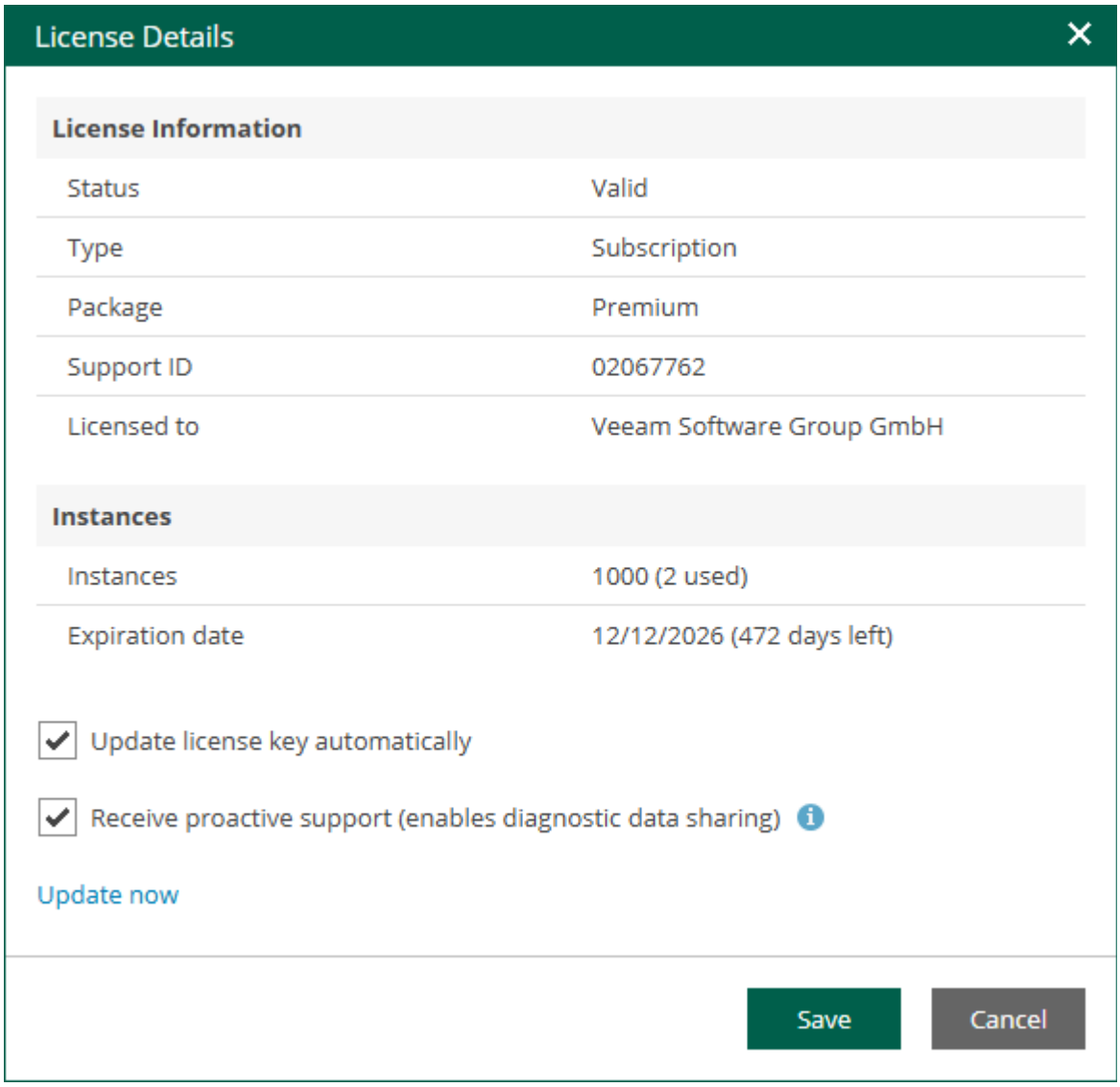
Updating License Manually

You can update the license manually on demand. When you update the license manually, Veeam Backup Enterprise Manager connects to the Veeam License Update Server, downloads a new license from it (if the license is available) and installs it.

To update the license, take the following steps:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Details**.

5. Click the **Update now** link.



Updating License Automatically

You can instruct Veeam Backup Enterprise Manager to schedule automatic connection with Veeam License Update Server and periodically send requests for a new license. When the automatic update is enabled, Enterprise Manager requests a new license weekly, and 7 days before current license expiration date — daily.

To enable automatic update, do the following:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Details**.
5. In the **Details** window, select the **Update license key automatically** check box. If this option is enabled in Enterprise Manager (even if it is disabled in the Veeam Backup & Replication console), automatic update will be performed anyway and Enterprise Manager will obtain a new key from Veeam licensing server and propagate it to all managed Veeam backup servers.

6. To receive proactive technical support services, select the **Receive proactive support** check box. Selecting this option also enables diagnostic data sharing. To learn how sensitive data is processed, see Processing of Sensitive Data in Veeam Technical Support.

NOTE

For information on license management in Veeam Backup & Replication, see the Licensing section of the Veeam Backup & Replication User Guide.

For information on license management for Veeam Cloud Connect Server Providers, see the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

Grace Period

Veeam Backup Enterprise Manager supports a grace period after the license expiration date. For Subscription license, it lasts for 30 days, for Rental license — 2 months. During this period the product will be running, but a warning about license expiration (grace period) will appear on the **Dashboard** tab and in the sessions information. You must update your license before the end of the grace period.

Messages that appear in the automatic license update session log are listed in the License Update Session Data section. Similar messages are received as pop-ups after you force the immediate update.

License Update Session Data

The table below lists the messages that can appear in the automatic license update session log. Similar messages are received as pop-ups after you force the immediate update. Recommendations for users (if applicable) are provided in the **Comment** field.

Message	Reason	Comment
"New license key has been received" "New license key has been installed" "License key has been auto-updated"	This sequence of messages means automatic license key update procedure has completed successfully.	You can open the License Information dialog in Veeam backup console or the Licensing section in Enterprise Manager to examine the details.
"License key type is not supported at the moment"	License key generation failed due to currently unsupported license type.	Currently, automatic update is supported only for licenses associated with *Hosting Rental* contract type.
"License key is invalid"	License signature (identifier) is invalid.	Contact your Veeam sales representative.
"Your existing license key is up to date"	License expiration date is more than 7 days from now.	This message could probably been issued due to an accidental attempt to update the license manually. Select to update the license key automatically, and the system will notify you on time.

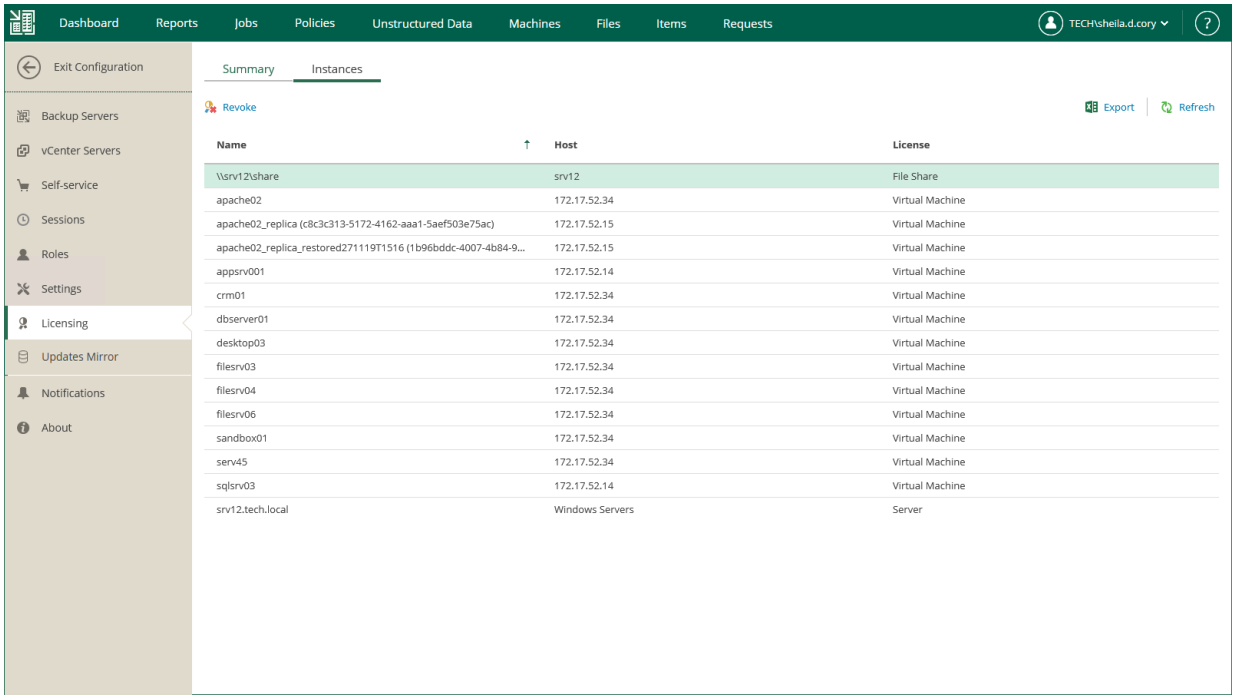
Message	Reason	Comment
"Your contract has expired, so the license key cannot be updated automatically. Please contact your Veeam sales representative to renew your contract."	Your contract has expired and needs to be renewed.	Contact your Veeam sales representative for contract renewal.
"General license key generation error has occurred"	Web licensing server did not return a new key upon request due to some other reason.	Wait for 24 hours (Veeam will re-try to update the key). Retries will take place for 1 month after key expiration date.

Revoking License

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

To revoke the license, take the following steps:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Licensing** section.
4. Select the **Instances** tab.
5. Select the required object in the list and click **Revoke**.



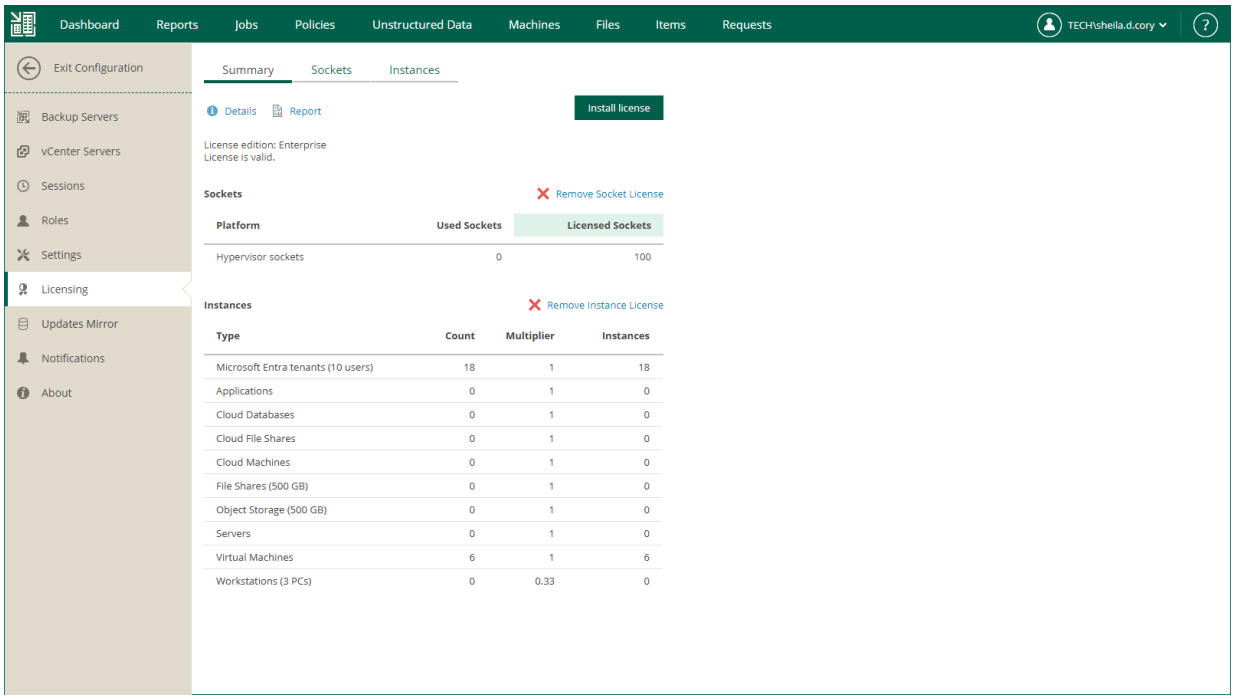
Removing License

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

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

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

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Licensing** section.
4. On the **Summary** tab, click **Remove Socket License** or **Remove Instance License**.
5. To confirm the removal, click **Yes**.



Managing Monthly Usage Reports

If you are a Service Provider that has a Rental license installed in Veeam Backup Enterprise Manager, you must submit a monthly license usage report.

You can submit a license usage report directly from Veeam Backup Enterprise Manager or from the VCSP Pulse Portal. Submitting a usage report from Enterprise Manager is only possible if automatic license update is enabled. Otherwise, you must fill out and submit the report in the VCSP Pulse Portal.

For more information about how license usage reporting works, see the License Usage Reporting section of the Veeam Cloud Connect Guide.

Veeam Backup Enterprise Manager generates a monthly usage report on the first day of the month. The report is based on the number of instances used for backup and replication in the previous month.

> **NOTE**
>
> Veeam Cloud Connect is supported only on Microsoft Windows-based Enterprise Manager.

In This Section

- Reviewing Monthly Usage Report
- Adjusting Monthly Usage Report
- Downloading Monthly Usage Report
- Submitting Monthly Usage Report

Reviewing Monthly Usage Report

You can review a monthly usage report before sending it to Veeam.

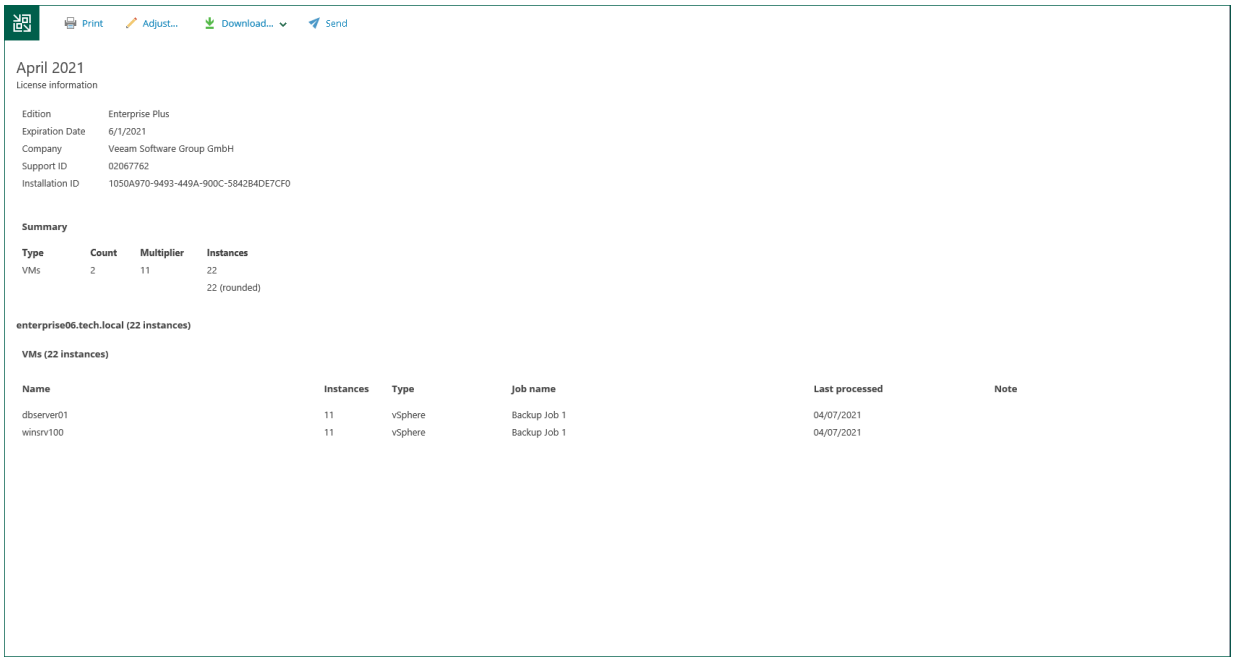
To review a report:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, click **Review**.
3. In the monthly usage report, check the number of reported instances. The report contains the following data:
    - License information: Veeam Backup & Replication edition, license expiration date, name of the company to which the license was issued and support ID.
    - The number of instances used by each type of protected workloads (VMs, workstations, servers and file shares) and the total number of used instances.
    - For each type of protected workloads, the report displays information about processed workloads and jobs that process these workloads.
    - For each type of protected workloads, the report also displays the number of new objects that are not included in the report.

On the report page, you can perform the following actions:

- Print the report

- Adjust the number of processed VMs in the report
- Download the report
- [For automatic reporting] Submit the report



Adjusting Monthly Usage Report

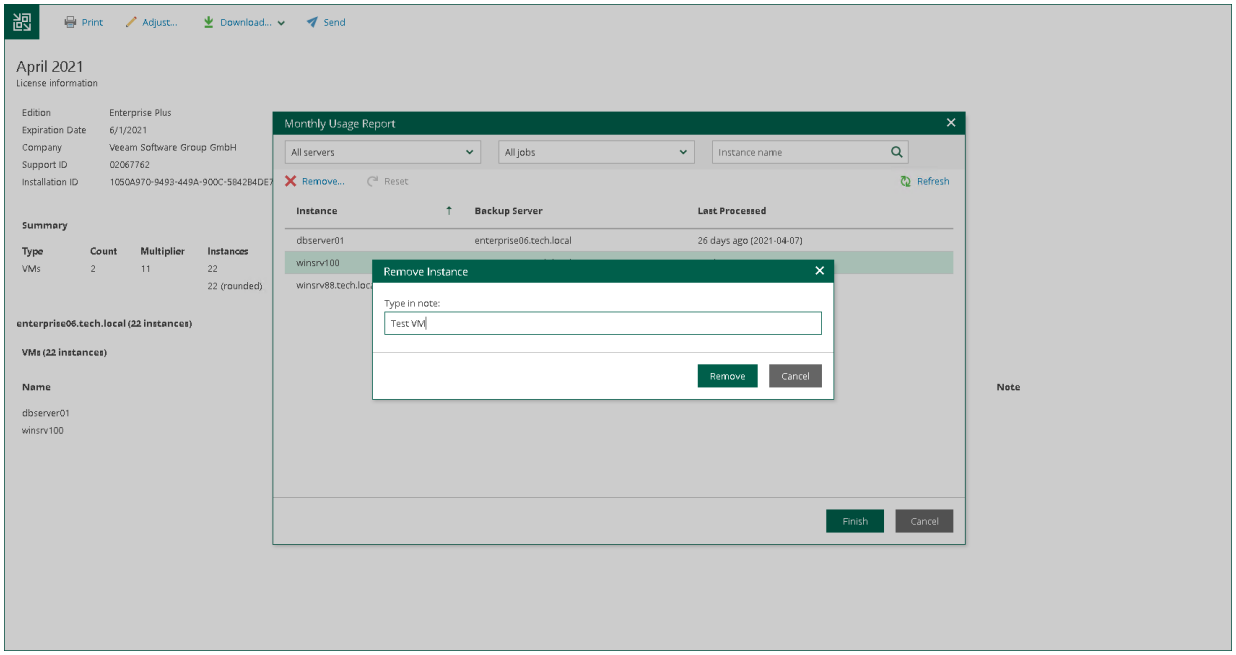
You can remove specific machines from a monthly usage report. For every removed machine, you must specify a reason.

To adjust a report:

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

   By default, the list of machines contains all managed machines included in the report. To quickly find the necessary machine, you can use the search field at the top of the window. You can also select a backup server and job from the drop-down lists to view a list of machines added to a specific job on a specific backup server.
5. In the **Remove Instance** window, in the **Type in note** field, provide a reason for removing the machine from the report.
6. Click **OK**, then click **Finish**. The change will be reflected in the report.

> **TIP**
>
> To reset changes introduced in the report, in the **Monthly Usage Report** window, click **Reset**.



Downloading Monthly Usage Report

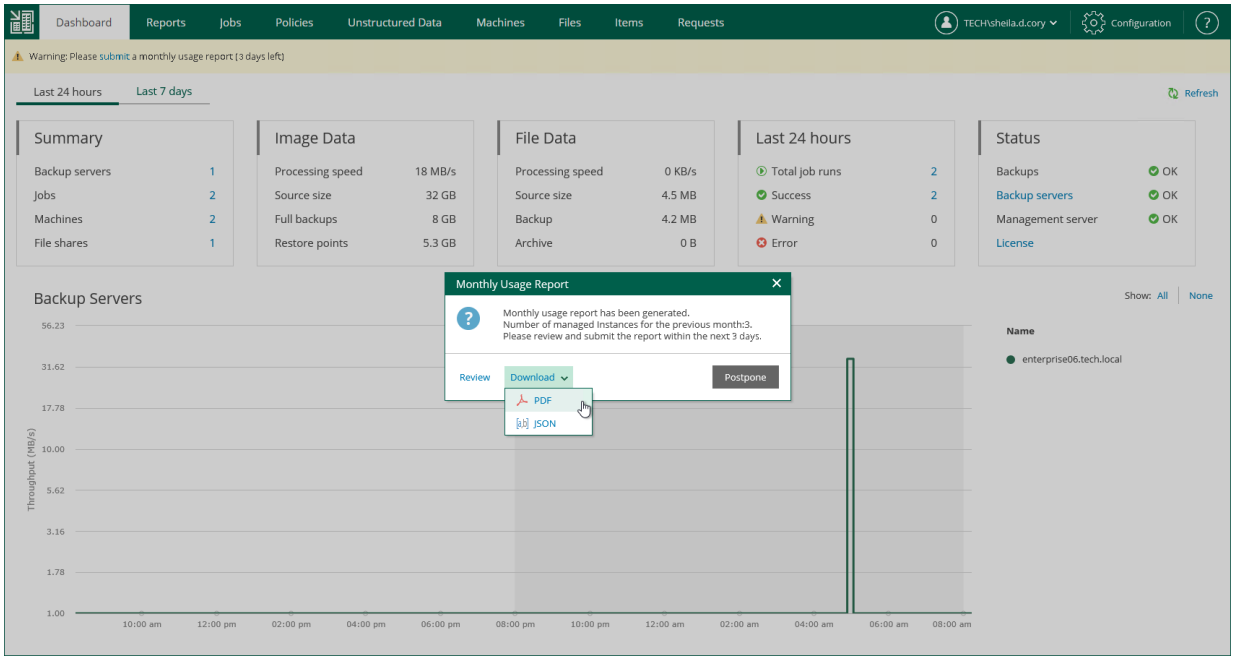
You can download a monthly usage report as a PDF or JSON file.

To download a monthly usage report:

1. In the monthly usage report notification, click the **submit** link.
2. Download the report. The procedure differs depending on the reporting method. For more information, see the License Usage Reporting section of the Veeam Cloud Connect Guide.
    - In case of automatic reporting, do the following:
        i. In the **Monthly Usage Report** window, click **Review**.
        ii. On the report page, click **Download** and select the report format: *PDF* or *JSON*.

- In case of manual reporting, in the **Monthly Usage Report** window, click **Download** and select the report format: *PDF* or *JSON*.

  You can also download the report after review. To do this, take the same steps as in case of automatic reporting.



Submitting Monthly Usage Report

On the first day of the month, Veeam Backup Enterprise Manager shows a warning on the **Dashboard** tab. The warning prompts you to submit a monthly usage report and informs you on the number of days within which the report must be submitted.

Depending on whether automatic license updating is enabled or disabled, you can submit a monthly usage report from Veeam Backup Enterprise Manager or the VCSP Pulse Portal.

For more information about how license usage reporting works, see the License Usage Reporting section of the Veeam Cloud Connect Guide.

Submitting Report from Veeam Backup Enterprise Manager

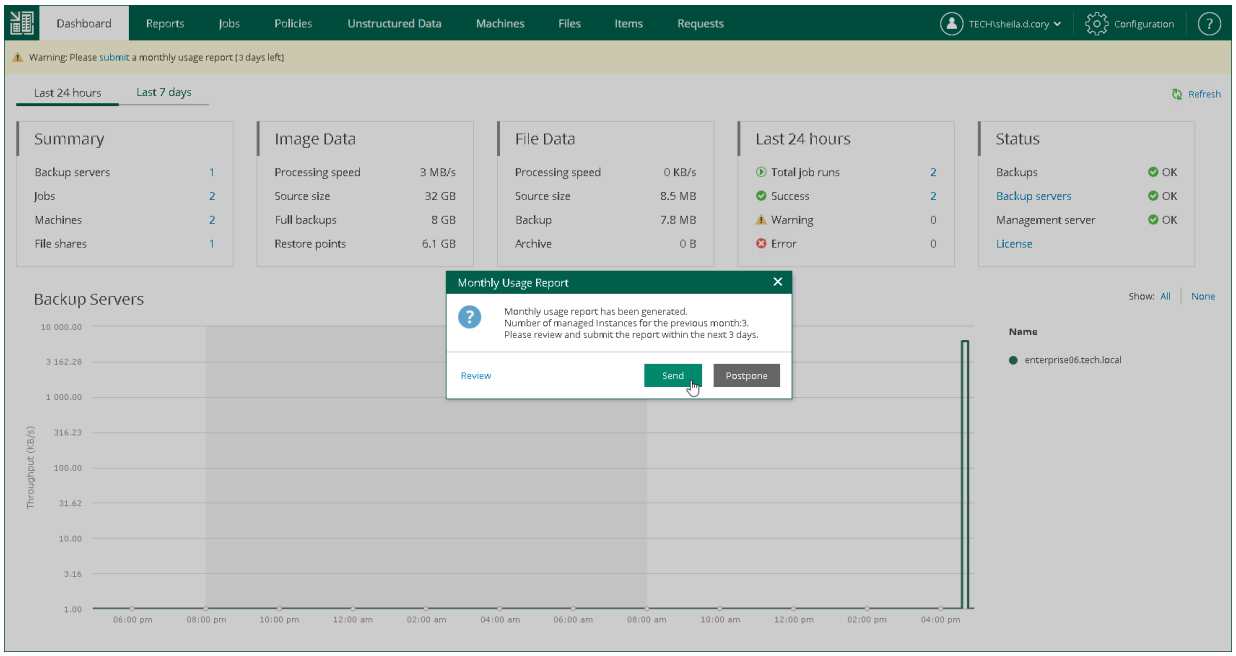
If automatic license update is enabled, you can send the monthly usage report directly from Veeam Backup Enterprise Manager. If you do not submit the report within 3 days, Veeam Backup Enterprise Manager sends the report automatically.

To submit a monthly usage report before the automatic submission, perform the following steps:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, to check or change the number of used instances, click **Review**.

   For more information, see Reviewing Monthly Usage Report and Adjusting Monthly Usage Report.
3. To submit the report, click **Send**.

   You can also postpone the report submission. To do this, click **Postpone**. In this case, Veeam Backup Enterprise Manager closes the **Monthly Usage Report** window. Until the report is sent to Veeam, on the **Dashboard** tab, Enterprise Manager keeps displaying a warning prompting to submit the report.



Submitting Report from VCSP Pulse Portal

If automatic license update is disabled, you must manually fill out and send the report in the VCSP Pulse Portal before the day defined by the agreement with Veeam or your Veeam Aggregator (if any is involved). The default day is the sixth day of the month.

To submit a monthly usage report from the VCSP Pulse Portal, perform the following steps:

1. In the monthly usage report notification, click the **submit** link.
2. In the **Monthly Usage Report** window, to check or change the number of used instances, click **Review**. For more information, see Reviewing Monthly Usage Report and Adjusting Monthly Usage Report.
3. To download the report, click **Download**.

   You can also postpone the report submission. To do this, click **Postpone**. In this case, Veeam Backup Enterprise Manager closes the **Monthly Usage Report** window. Until the report is sent to Veeam, on the **Dashboard** tab, Enterprise Manager keeps displaying a warning prompting to submit the report.
4. Fill out the report in the VCSP Pulse Portal with the used workloads and licenses and submit it, as described in the Using VCSP Pulse section of the Veeam Rental Licensing and Usage Reporting Reference Guide.

Configuring Updates Mirror

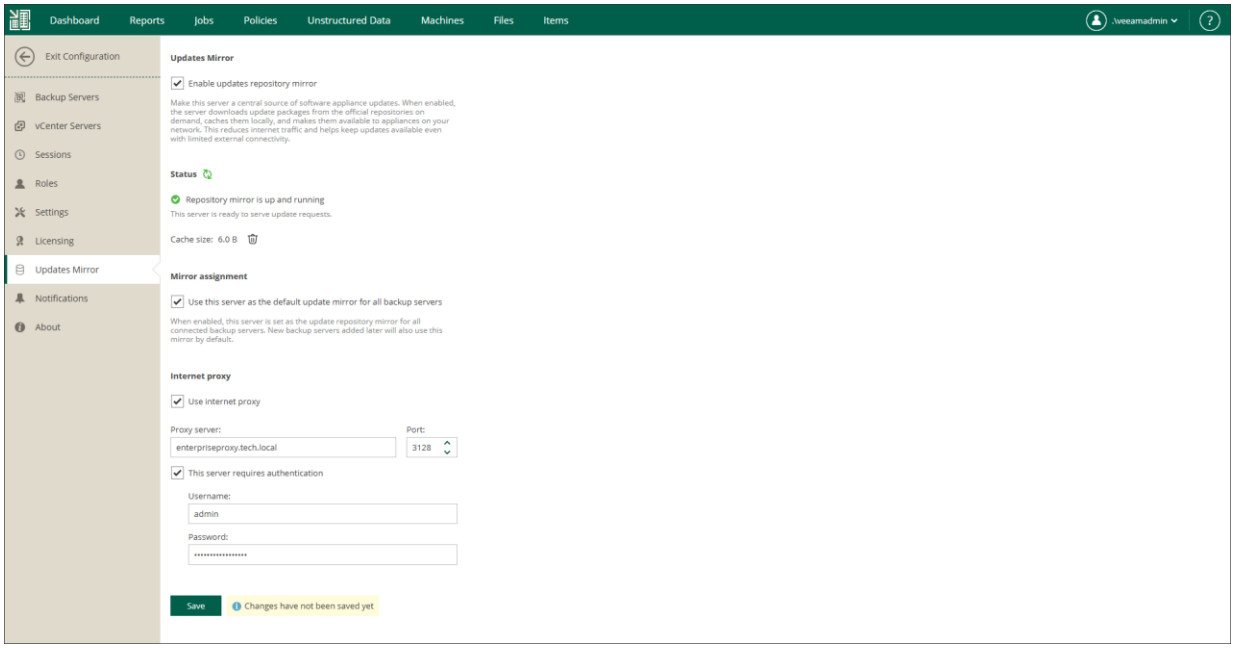
By default, Veeam Software Appliance updates for Enterprise Manager, backup servers and backup server components are installed from the Veeam Update Repository (`https://repository.veeam.com/vsa`). You can configure a local mirror of the Veeam Update Repository to reduce internet traffic or ensure that all components can be updated when internet connectivity is limited. In particular, you can set the Enterprise Manager machine as a mirror repository. For details about specifying another server as a local mirror, see Configuring Updates.

> **NOTE**
>
> You can configure Enterprise Manager as a mirror of the Veeam Update Repository only if Enterprise Manager is deployed as Veeam Software Appliance. In Microsoft Windows-based Enterprise Manager, the **Configuration** view does not include the **Updates Mirror** section, even if Enterprise Manager manages backup servers deployed as Veeam Software Appliance.

To configure Enterprise Manager as a mirror of the Veeam Update Repository, follow these steps:

1. Sign in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Updates Mirror** section.
4. To enable the mirror of the Veeam Update Repository on Enterprise Manager, select **Enable updates mirror**.
5. To use this mirror not only to install updates for Enterprise Manager but also for all added backup servers and their components, select **Use this server as the default update mirror for all backup servers**.
6. If Enterprise Manager does not have direct access to the internet, you can configure a dedicated internet proxy server. To specify an internet proxy, do the following:
   a. Select **Use internet proxy**.
   b. In the **Proxy server** field, specify a DNS name or IP address of the server that has access to the internet and that you want to use as your internet proxy.
   c. In the **Port** field, specify a port number over which to connect to the specified server.

d. To provide authentication credentials to access the internet proxy, select **This server requires authentication** and enter the username and password.



Configuring Notification Settings

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

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

After that, you can fine tune necessary notifications:

- Notifications on job results
- Notifications on restore operations
- Notifications on licensing
- Notifications on encryption keys operations

Mail Server Settings

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

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

- Connect Veeam Backup Enterprise Manager with a Google account
- Connect Veeam Backup Enterprise Manager with a Microsoft 365 account
- Use an SMTP server with basic authentication

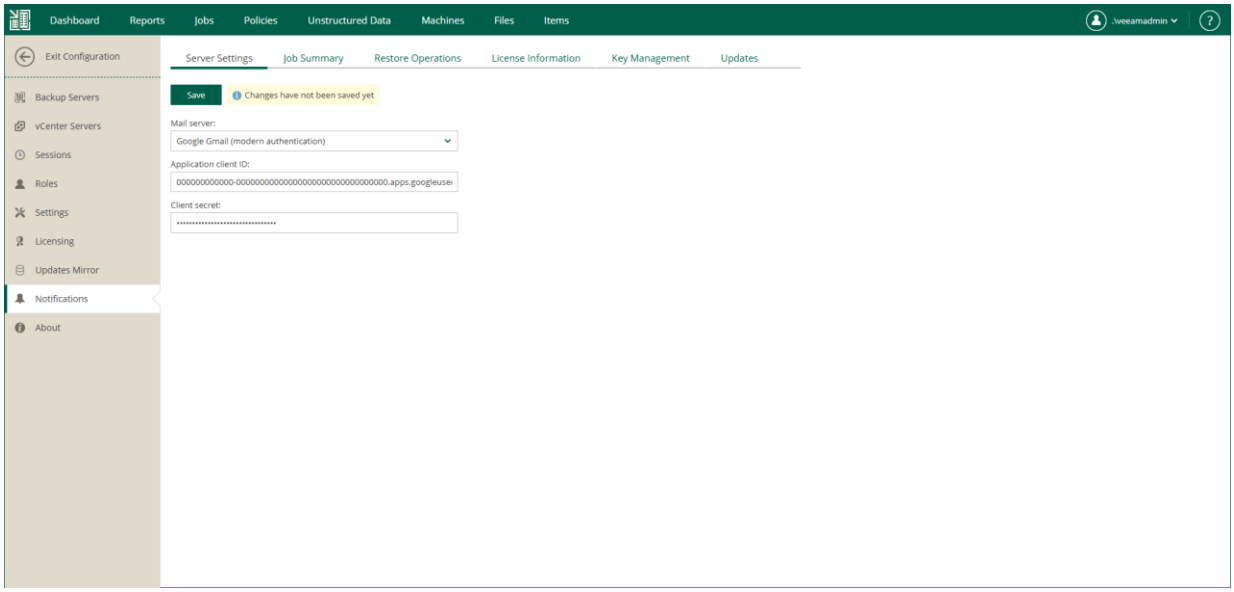
Google Account Settings

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

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

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. On the **Server Settings** tab, select *Google Gmail* from the **Mail server** list.
5. In the **Application client ID** field, specify the obtained client ID.
6. In the **Client secret** field, specify the client secret.
7. To save the credentials, click **Save**.
8. Click **Sign in with Google**.

9. Allow Veeam Backup Enterprise Manager to have access to your Google account and send email notifications on your behalf.



Registering Application in Google Cloud Console

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

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

1. Log in to the Google Cloud console under a Google account that you want to use for sending email notifications.
2. Create a new project and enable *Gmail API* for the project.

   You can do this with the Google setup tool.
3. Create the *OAuth client ID* credentials — a client ID and client secret for the Veeam Backup Enterprise Manager application.

   As an authorized redirect URI, specify the following:

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

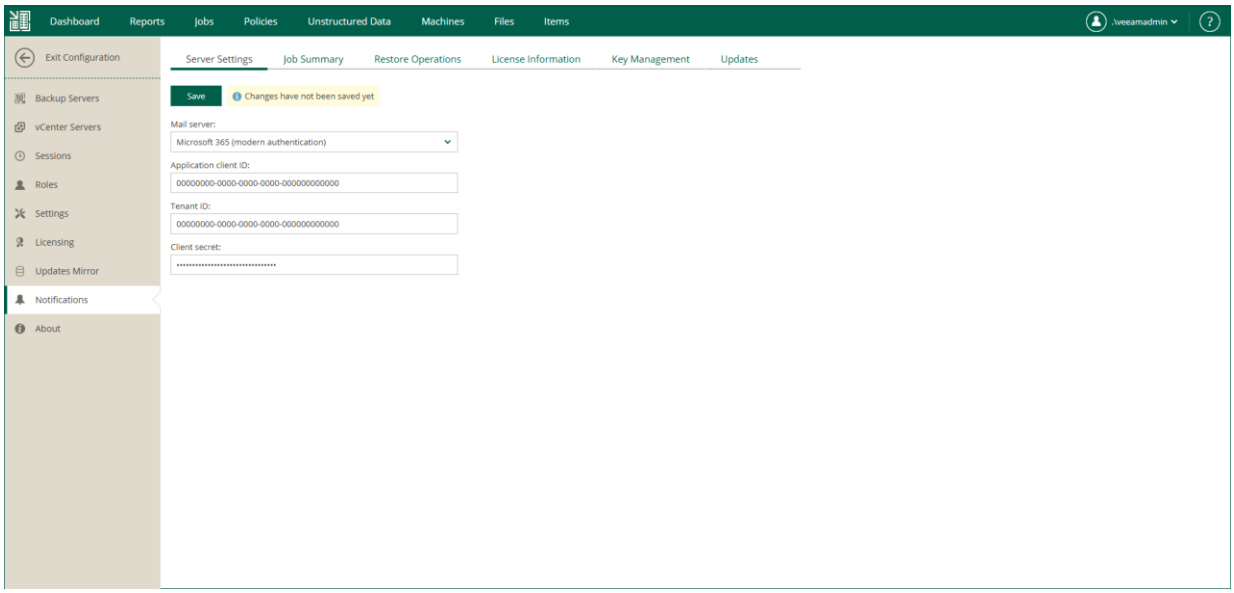
   where `<EnterpriseManagerServer>` is a host name of the host where the Enterprise Manager server resides.
4. Record the following data required for acquiring an access token:
   - Client ID
   - Client secret

Microsoft 365 Account Settings

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

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

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. On the **Server Settings** tab, select *Microsoft 365* from the **Mail server** list.
5. In the **Application client ID** field, specify the client ID assigned to your Microsoft Entra application.
6. In the **Tenant ID** field, specify the ID of your Microsoft Entra tenant.
7. In the **Client secret** field, specify the client secret assigned to your Microsoft Entra application.
8. To save the settings, click **Save**.
9. Click **Authorize now**.
10. Allow Veeam Backup Enterprise Manager to access your Microsoft 365 account and send email notifications on your behalf.



Registering Application in Microsoft Azure Portal

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

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

1. Log in to the Microsoft Azure portal under an account that you want to use for sending email notifications. The account must have an active subscription and the permissions to register Microsoft Entra applications.
2. Create a new app registration for Veeam Backup Enterprise Manager:
   a. In the **Name** field, specify a display name for your application.
   b. In the **Supported account types** section, select the **Accounts in this organizational directory only** option.
   c. In the **Redirect URI** section, select the **Web** option from the platform list and specify the following URI:

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

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

SMTP Server with Basic Authentication

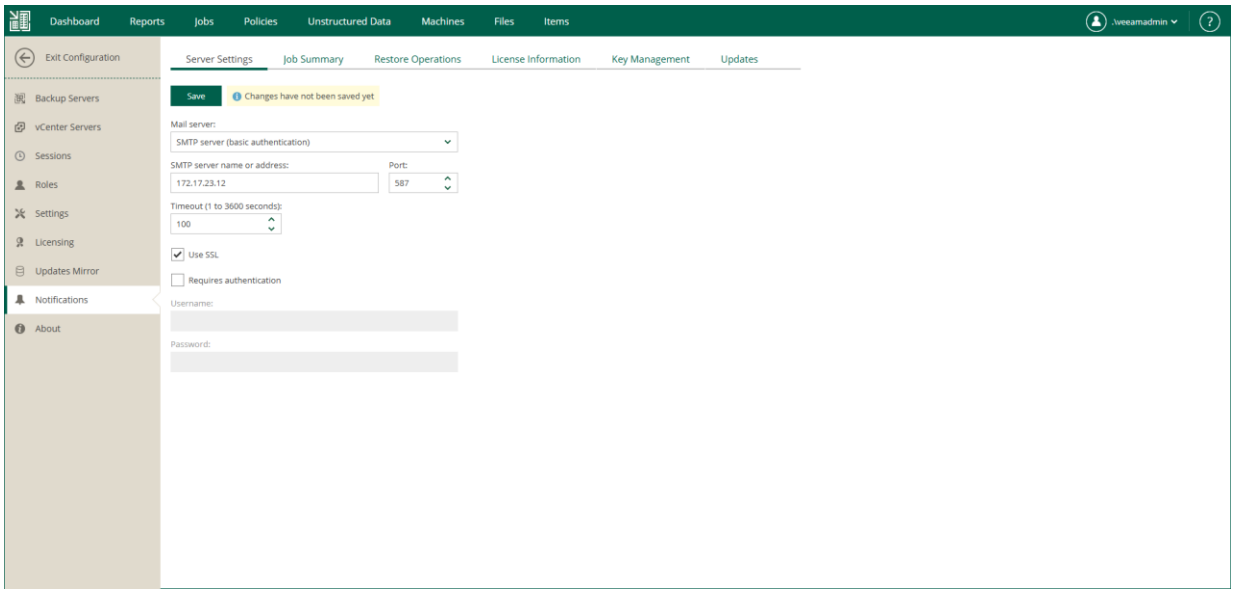
For sending email notifications, you can use a custom SMTP server with basic authentication.

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

To specify SMTP server settings, do the following:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. Open the **Notifications** section on the left of the **Configuration** view.
4. On the **Server Settings** tab, select *SMTP server* from the **Mail server** list.
5. 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**.

6. In the **Timeout** field, specify a timeout for email server — this should be a value from 1 to 3600 seconds. Default is **100** seconds.
7. If the SMTP server requires SSL connection, select the **Use SSL** check box.
8. If the SMTP server requires authentication, select the **Requires authentication** check box and specify authentication credentials.
9. Click **Save**.

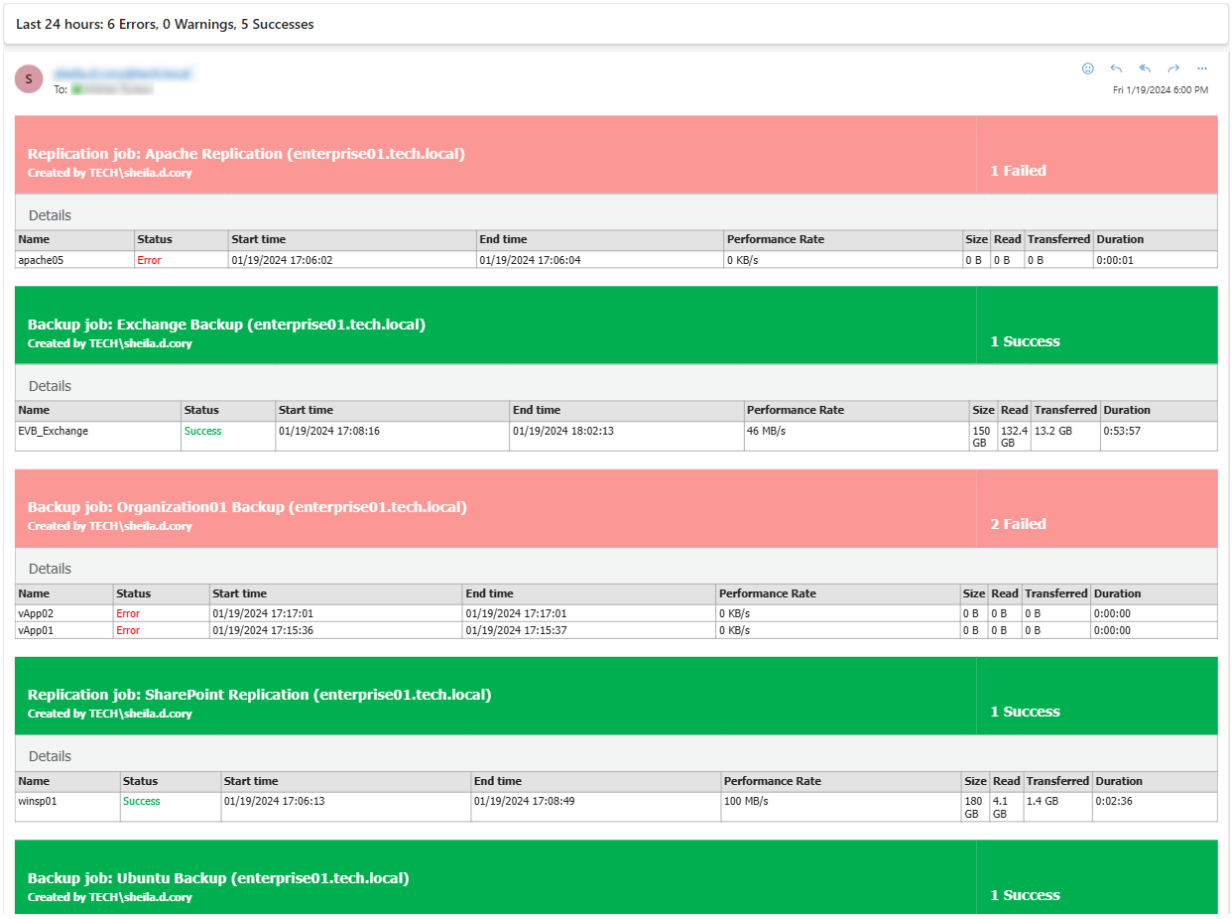


Notifications on Job Results

You can configure Veeam Backup Enterprise Manager to send daily email notifications with the results of finished jobs. The email message contains a detailed list of jobs performed with the *Error*, *Warning* and *Success* statuses. If you want to receive a notification after each job run, configure notification setting for this job in Veeam Backup & Replication. For details, see the Notification Settings section of the Veeam Backup & Replication User Guide.

The report includes the following job types:

- Backup jobs
- Replication jobs
- File backup jobs
- Object storage backup jobs
- Backup jobs of Veeam Agent for Linux and Veeam Agent for Microsoft Windows (both managed by Veeam Agent and by the backup server)



Last 24 hours: 6 Errors, 0 Warnings, 5 Successes

Fri 1/19/2024 6:00 PM

Replication job: Apache Replication (enterprise01.tech.local) — 1 Failed
Created by TECH\sheila.d.cory

Details

Name	Status	Start time	End time	Performance Rate	Size	Read	Transferred	Duration
apache05	Error	01/19/2024 17:06:02	01/19/2024 17:06:04	0 KB/s	0 B	0 B	0 B	0:00:01

Backup job: Exchange Backup (enterprise01.tech.local) — 1 Success
Created by TECH\sheila.d.cory

Details

Name	Status	Start time	End time	Performance Rate	Size	Read	Transferred	Duration
EVB_Exchange	Success	01/19/2024 17:08:16	01/19/2024 18:02:13	46 MB/s	150 GB	132.4 GB	13.2 GB	0:53:57

Backup job: Organization01 Backup (enterprise01.tech.local) — 2 Failed
Created by TECH\sheila.d.cory

Details

Name	Status	Start time	End time	Performance Rate	Size	Read	Transferred	Duration
vApp02	Error	01/19/2024 17:17:01	01/19/2024 17:17:01	0 KB/s	0 B	0 B	0 B	0:00:00
vApp01	Error	01/19/2024 17:15:36	01/19/2024 17:15:37	0 KB/s	0 B	0 B	0 B	0:00:00

Replication job: SharePoint Replication (enterprise01.tech.local) — 1 Success
Created by TECH\sheila.d.cory

Details

Name	Status	Start time	End time	Performance Rate	Size	Read	Transferred	Duration
winsp01	Success	01/19/2024 17:06:13	01/19/2024 17:08:49	100 MB/s	180 GB	4.1 GB	1.4 GB	0:02:36

Backup job: Ubuntu Backup (enterprise01.tech.local) — 1 Success
Created by TECH\sheila.d.cory

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

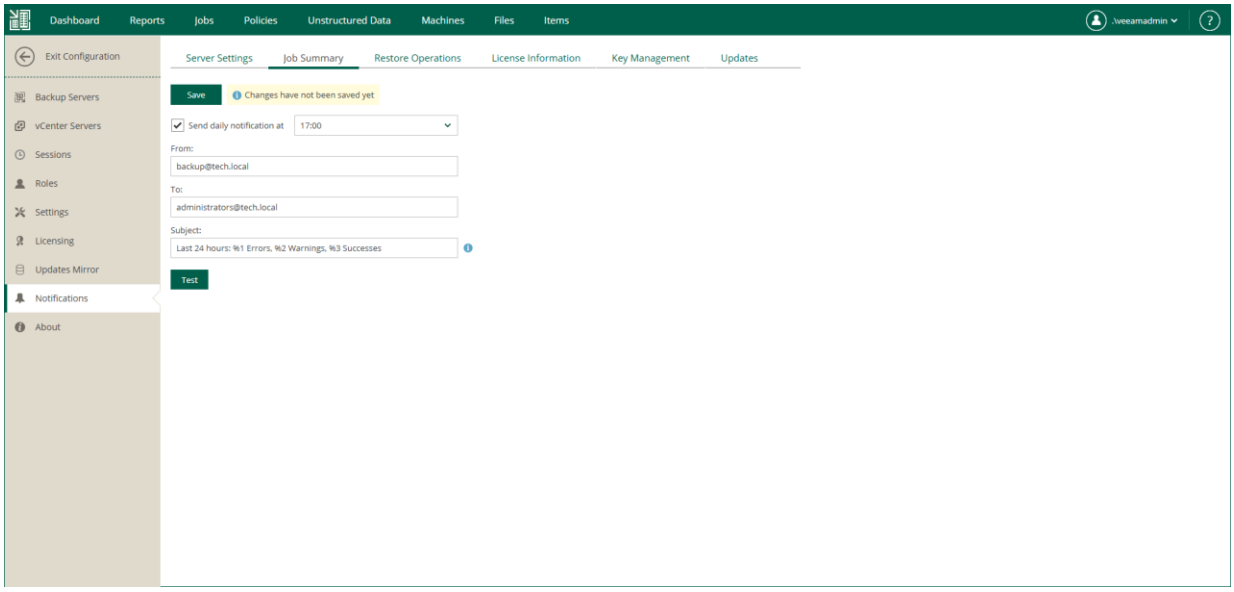
1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. Open the **Job Summary** tab.

5. Select the **Send daily notification at** check box and specify the time when you want a notification email to be sent.
6. In the **From** field, enter an email address of the notification sender.
7. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
8. In the **Subject** field, enter a subject of email notifications. You can use the following variables in the subject:
   - %1 — number of jobs that ended with errors for the last 24 hours
   - %2 — number of jobs that ended with warnings for the last 24 hours
   - %3 — number of jobs that ended successfully for the last 24 hours

     Job retries performed in the last 24 hours are also included in the report.
   - %4 — number of jobs whose last session ended with an error.
   - %5 — number of jobs whose last session ended with a warning.
   - %6 — number of jobs whose last session ended successfully.

     Jobs which were in *Disabled* state during the last session are also included in the report.
9. 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 Restore Operations

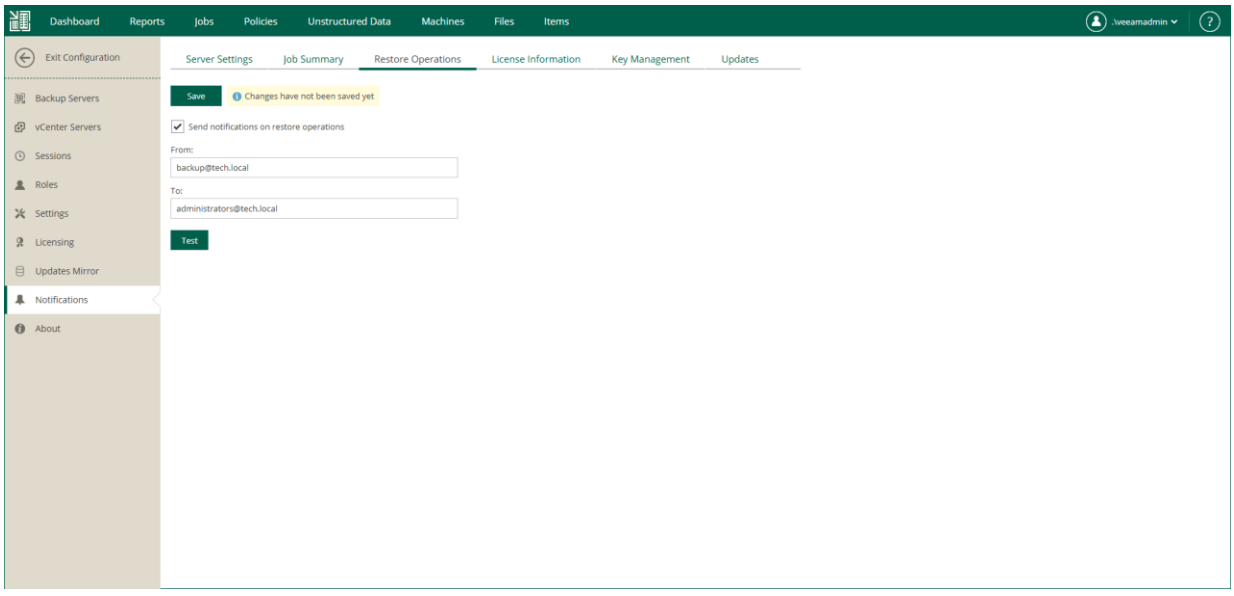
You can configure Veeam Backup Enterprise Manager to send email notifications about the following recovery operations:

- Instant Recovery
- Entire VM Restore
- Guest OS file restore
- Instant File Share Recovery
- Application Item Restore

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

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. Open the **Restore Operations** tab.
5. Select **Send notifications on restore operations**.
6. In the **From** field, enter an email address of the notification sender.
7. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
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.



Notifications on Licensing

You can configure Veeam Backup Enterprise Manager to send the following email notifications:

- [For Perpetual licenses] Notifications on support contract expiration
- [For Rental licenses] Notifications on license usage

Notifications on Support Contract Expiration

If you have a Perpetual license installed and your support contract is expired, Veeam Backup Enterprise Manager adds the *SUPPORT EXPIRED* prefix to the subject of all its email messages. You can configure Enterprise Manager to remove the prefix.

To remove the *SUPPORT EXPIRED* prefix from the message subject:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. Open the **License Information** tab.
5. Select the **Disable support contract expiration notifications** check box.

Notifications on License Usage

If you have a Rental license installed, you can configure Veeam Backup Enterprise Manager to send email notifications on license usage. Every notification contains a monthly usage report about instances used for backup and replication in the previous month. For more information on the reports, see Managing Monthly Usage Reports.

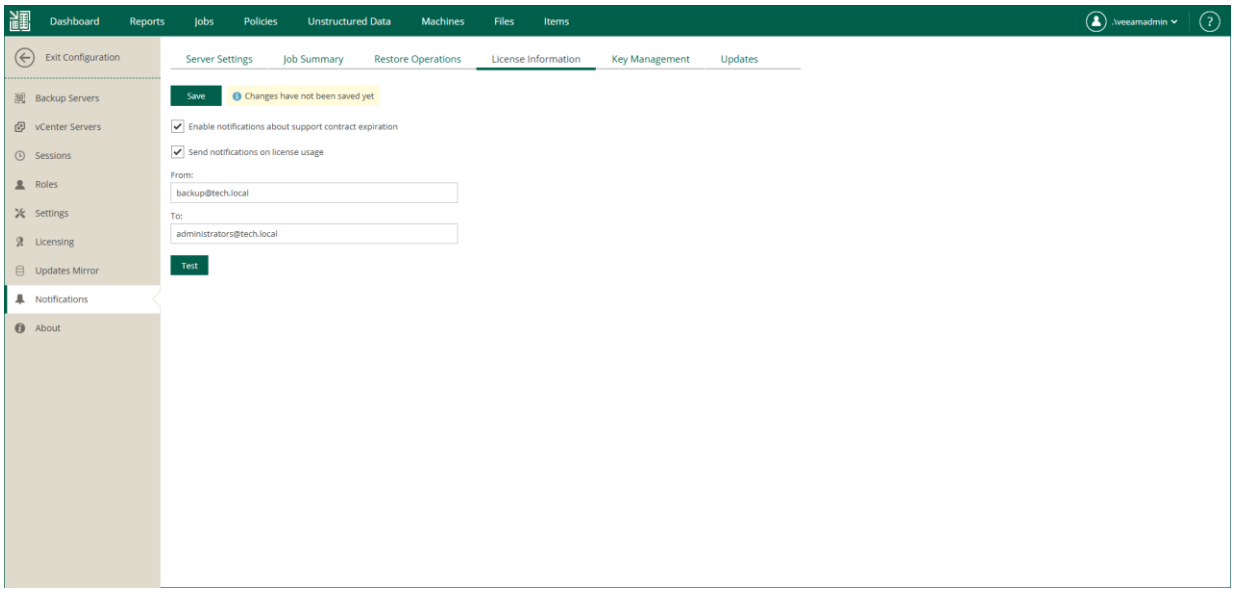
Enterprise Manager sends notifications on license usage on the first day of the month. If Veeam Backup & Replication does not perform any backup and replication jobs for the whole month, Enterprise Manager does not send the notifications.

To enable email notifications on license usage:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. Open the **Notifications** section on the left of the **Configuration** view.
4. Open the **License Information** tab.
5. Select the **Send notifications on license usage** check box.
6. In the **From** field, enter an email address of the notification sender.
7. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
8. Click **Save**.

TIP

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



Notifications on Key Management

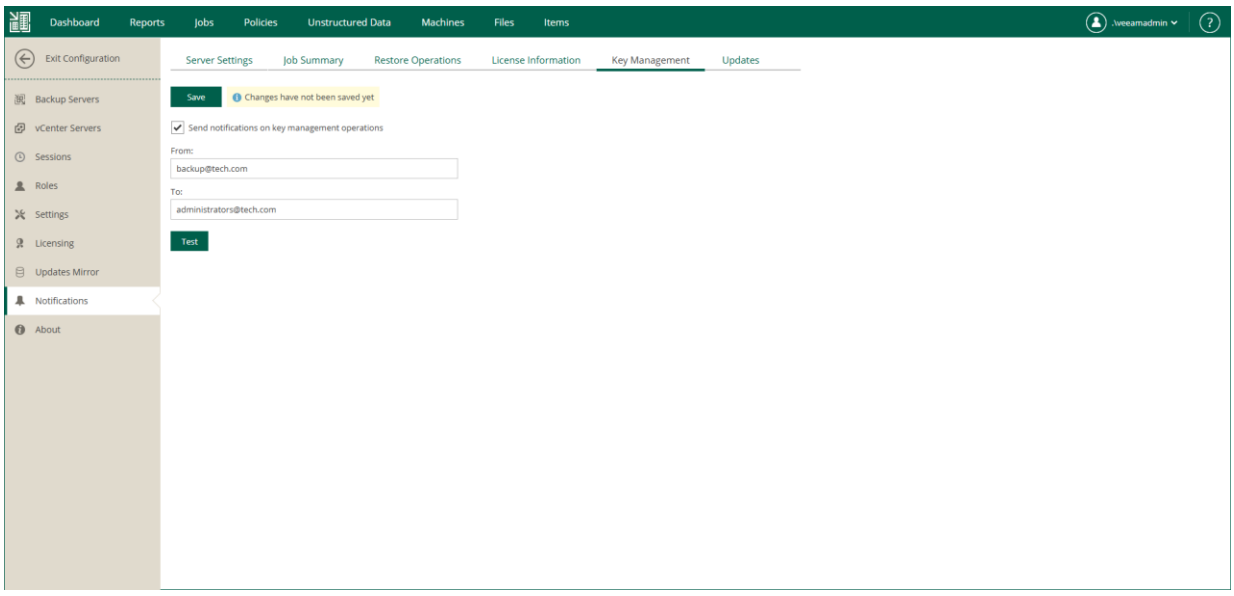
Veeam Backup Enterprise Manager allows you to perform operations with encryption keys. For more information, see Managing Encryption Keys.

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

To receive key management notifications, do the following:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. Open the **Key Management** tab.
5. Select the **Send notifications on key management operations** check box.
6. In the **From** field, enter an email address of the notification sender.
7. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
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.



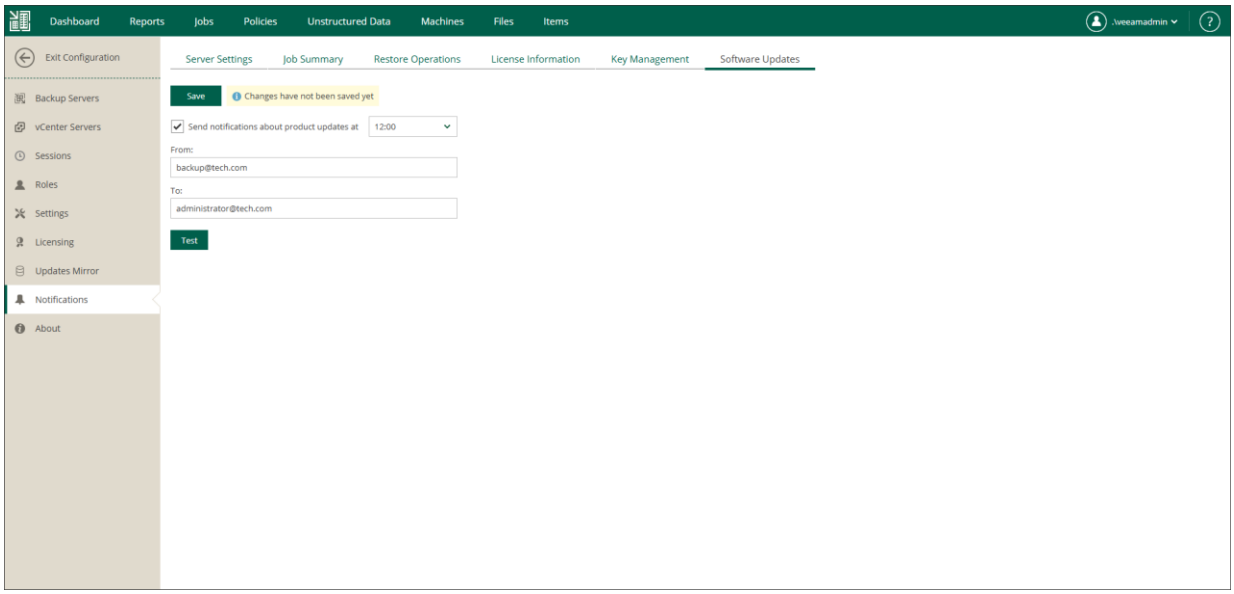
Notifications on Updates

If you use Veeam Backup Enterprise Manager on Linux, you can configure Enterprise Manager to send email notifications when product updates become available.

To enable email notifications for Enterprise Manager updates, follow these steps:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **Notifications** section.
4. Open the **Software Updates** tab.
5. Select the **Send notifications about product updates at** check box and specify the time when you want a notification email to be sent.
6. In the **From** field, enter an email address of the notification sender.
7. In the **To** field, enter an email address of the notification recipient. Use a comma to specify multiple addresses.
8. Click **Save**.

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

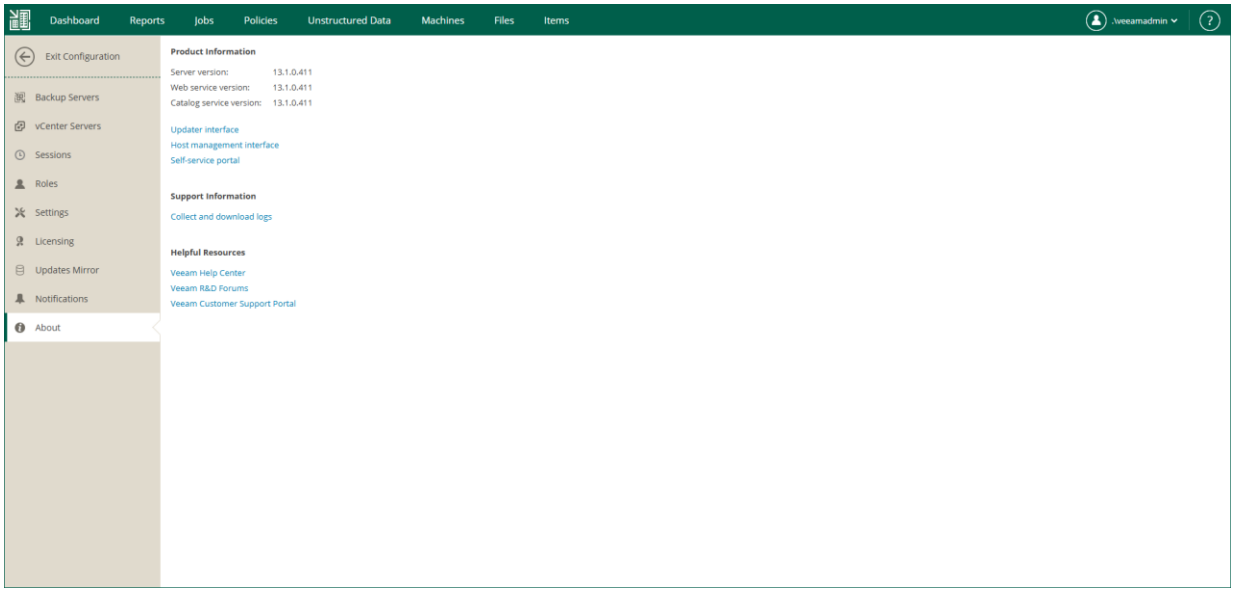


Viewing Information About Enterprise Manager

In the **About** section, you can check the product version and find links to Veeam Updater, Veeam Host Management, Veeam Self-Service File Restore Portal, and resources that can help you resolve issues with Enterprise Manager. You can also download Enterprise Manager logs for Veeam Customer Support. For more information, see Enterprise Manager Logs.

To view information about Enterprise Manager, do the following:

1. Log in to Enterprise Manager using an account with the Portal Administrator role.
2. In the upper-right corner, click **Configuration**.
3. In the **Configuration** view, open the **About** section.



Managing Languages

Veeam Backup Enterprise Manager interface is available in several languages. You can select a language for the following Veeam Backup Enterprise Manager components:

- Veeam Backup Enterprise Manager website
- Veeam Self-Service Backup Portal for Cloud Director
- vSphere Self-Service Backup Portal

Available Languages

Veeam Backup Enterprise Manager is available in the following languages:

- Chinese (Simplified, PRC)
- English
- French
- German
- Italian
- Japanese
- Spanish

Selecting Language

The first time you visit one of the Veeam Backup Enterprise Manager components, the content is displayed in the language of your browser. If the website does not support the browser language, the interface is displayed in English.

You can select a preferred language from the drop-down list on the login page. If the language you need is not available, you can add it. For more information, see Adding Languages.

In This Section

- Language Files Overview
- Adding Languages

Language Files Overview

To support multiple languages, Veeam Backup Enterprise Manager uses the GNU gettext tools. Veeam Backup Enterprise Manager languages are stored in POT, JSON and PO files. The files are located in the `lang` folder on the Enterprise Manager server. By default, the path to the folder is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

All files names must follow the naming conventions. For more information, see File Names.

File Formats

Enterprise Manager languages are stored in text files of the following formats:

- POT files that contain UI texts in the source language. The source language of Enterprise Manager is English.
- [Optional] PO files that contain UI texts as pairs of strings: source string and its translation. Each language is stored in a separate file. You can create PO files from the POT files and use them in the translation process. After you finish the translation, you must convert PO files to the JSON format.
- JSON files that contain UI texts as pairs of strings: source string and its translation. Enterprise Manager uses these files to display the interface in a language other than English.

File Names

In order for Veeam Backup Enterprise Manager to recognize files within the `lang` folder as language files, their names must follow the naming conventions.

POT files must have the following names:

- `messages.pot` — file used for the Veeam Backup Enterprise Manager website
- `vcloud_messages.pot` — file used for Veeam Self-Service Backup Portal
- `vsphere_messages.pot` — file used for vSphere Self-Service Backup Portal

JSON files must have the following names:

- `messages.<code>.json` — file used for the Veeam Backup Enterprise Manager website
- `vcloud_messages.<code>.json` — file used for Veeam Self-Service Backup Portal
- `vsphere_messages.<code>.json` — file used for vSphere Self-Service Backup Portal

where `<code>` is an ISO 639-1 code that represents the language. The code consists of a two-letter lowercase culture code and optional two-letter uppercase region code. For example: `en`, `fr-CA`, `fr-FR`, `pt-BR` or `pt-PT`.

Adding Languages

Veeam Backup Enterprise Manager is available in several languages. If the language you need is not available, you can add it. Before you start adding new languages, check whether the languages are supported by the server where Veeam Backup Enterprise Manager is deployed.

To check whether a language is supported, run the following command:

```
New-Object -TypeName 'System.Globalization.CultureInfo' -ArgumentList "<code>"
```

where `<code>` is an ISO 639-1 code that represents the language. The code consists of a two-letter lowercase culture code and optional two-letter uppercase region code. For example: `en`, `fr-CA`, `fr-FR`, `pt-BR` or `pt-PT`.

To add new languages:

1. Translate source UI texts to the new languages.

   For more information, see Translating Source Texts.

2. Convert the translation files.

   For more information, see Converting PO to JSON.

3. Save the translation files to the `lang` folder. The default path is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

   > **IMPORTANT**
   >
   > Make sure the JSON translation files are named as follows: `messages.xx.json`, `vcloud_messages.xx.json`, `vsphere_messages.xx.json`. For more information on file naming, see Language Files Overview.

4. In IIS Manager, restart the VeeamBackup website and recycle the VeeamBackup application pool. For more information, see the Site <site> and Recycling Settings for an Application Pool <recycling> sections of Microsoft Docs.

Translating Source Texts

Source texts are stored in POT files. The files are located in the `lang` folder on the Enterprise Manager server. By default, the path to the folder is the following: `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager\WebApp\scripts\build\production\resources\lang`.

To translate source texts:

1. Get the source files from the `lang` folder:

   - `messages.pot`
   - `vcloud_messages.pot`
   - `vsphere_messages.pot`

   For more information on file names and formats, see Language Files Overview.

2. For each language, create PO files using the POT files as templates.

   For more information, see this GNU gettext article.

3. Name the PO files as follows:

   - `messages.<code>.po`
   - `vcloud_messages.<code>.po`
   - `vsphere_messages.<code>.po`

   For more information, see Language Files Overview.

4. Translate PO files in a text editor or a CAT tool.

   For more information on PO files, see PO File Structure.

   > **TIP**
   >
   > Although PO files are not used by Veeam Backup Enterprise Manager, you can save them in the `lang` folder to keep them together with other language files.

PO File Structure

Each PO file contains the following elements:

- Header
- Translation entries

Header

Header contains meta data of the PO file: language code in the ISO 639-1 format, content type and encoding, and plural form information.

Parameter	Description
Language	ISO 639-1 code of the translation language.
MIME-Version	MIME version. Set it to *1.0*.
Content-Type	Content type and character encoding used for the translation language. Set the type value to *text/plain*.You can use the UTF-8 encoding for any language.
Content-Transfer-Encoding:	Content transfer encoding. Set the value to *8bit*.
Plural-Forms	Number of plural forms and the plural form formula of the translation language.

For example:

```
"Project-Id-Version: \n"
"POT-Creation-Date: \n"
"PO-Revision-Date: \n"
"Language-Team: \n"
"Language: de\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=UTF-8\n"
"Content-Transfer-Encoding: 8bit\n"
"Plural-Forms: nplurals=2; plural=(n != 1);\n"
"X-Generator: \n"
```

For more information on the PO header, see this GNU gettext article.

Translation entries

In a PO file, translation entries are separated with a blank string. Each entry consists of the following elements:

- `msgid` — string in the source language
- [Optional] `msgid_plural` — plural form of the `msgid` string
- `msgstr` — string in the translation language

Before you begin translating, consider the following:

- Do not modify `msgid` strings. They are references to the source code. Veeam Backup Enterprise Manager uses them to find their translation.
- If an `msgid` string contains variables, do not translate them.

  Variables are placed inside braces. For example, the following entry contains the `restoreItemsCount` variable:

  ```
  msgid "Pending restore ({restoreItemsCount} items)"
  msgstr "Ausstehende Wiederherstellung ({restoreItemsCount} Elemente)"
  ```

- If an `msgid` string is followed by its plural form `msgid_plural`, provide translation for each form.

  For example:

  ```
  msgid "${ pointsCount } point"
  msgid_plural "${ pointsCount } points"
  msgstr[0] "${ pointsCount } Punkt"
  msgstr[1] "${ pointsCount } Punkte"
  ```

  For more information on translating plural forms, see this GNU gettext article.

Converting PO to JSON

Veeam Backup Enterprise Manager loads translated strings from JSON files. After you finish translating PO files, convert them to the JSON format.

To convert a file from the PO format to the JSON format, use the `Veeam.Backup.Localization.PoConverter.exe` utility.

1. To locate the utility, use the `cd` command. By default, the utility is located in the Enterprise Manager folder.

   ```
   cd '<path>'
   ```

   where `<path>` is a path to the utility file.

   For example:

   ```
   cd 'C:\Program Files\Veeam\Backup and Replication\Enterprise Manager'
   ```

2. Run the utility with the following command:

   ```
   .\Veeam.Backup.Localization.PoConverter.exe '<po_file>'
   ```

   where `<po_file>` is a path to the PO file.

   For example:

   ```
   .\Veeam.Backup.Localization.PoConverter.exe 'C:\Program Files\Veeam\Backup
   and Replication\Enterprise Manager\WebApp\scripts\build\production\resourc
   es\lang\messages.zh_CN.po'
   ```

The JSON file will be created in the folder of the PO file.

> **TIP**
>
> To view help for the Veeam.Backup.Localization.PoConverter.exe utility, run the utility with the `/help` parameter.

Managing Jobs

Veeam Backup Enterprise Manager acts as a single point for managing jobs from all added backup servers. Users with the Portal Administrator role can centrally manage jobs that have been previously configured on added backup servers: start, stop, retry, clone, delete jobs and edit selective job settings.

Consider the following limitations:

- For the following workloads, Enterprise Manager displays only backup copy jobs and SureBackup jobs running in the **Backup verification and content scan only** mode:
  - AWS
  - Google Cloud
  - Microsoft Azure
  - Nutanix AHV
  - Oracle Linux Virtualization Manager and Red Hat Virtualization
  - Proxmox VE
  - Scale Computing HyperCore
- For physical machines, Enterprise Manager displays the following job types:
  - Both Veeam Agent backup jobs managed by Veeam Agent and Veeam Agent backup jobs managed by the backup server. For more information, see Veeam Agents Support.
  - Backup copy jobs

In This Section

- Viewing Jobs
- Starting, Stopping and Retrying Jobs
- Enabling and Disabling Jobs
- Editing Jobs
- Creating Active Full Backups
- Cloning Jobs
- Deleting Jobs

Viewing Jobs

From Veeam Backup Enterprise Manager, you can view information about jobs configured on all backup servers added to Enterprise Manager. To view the jobs, open the **Jobs** tab. Every job in the list is described with the following data: job name, type, platform of the objects it processes, backup server on which the job was created, current job status, date of the latest run, date of the next run (if the job is scheduled) and job description.

To quickly find a job, you can use filters and the search field.

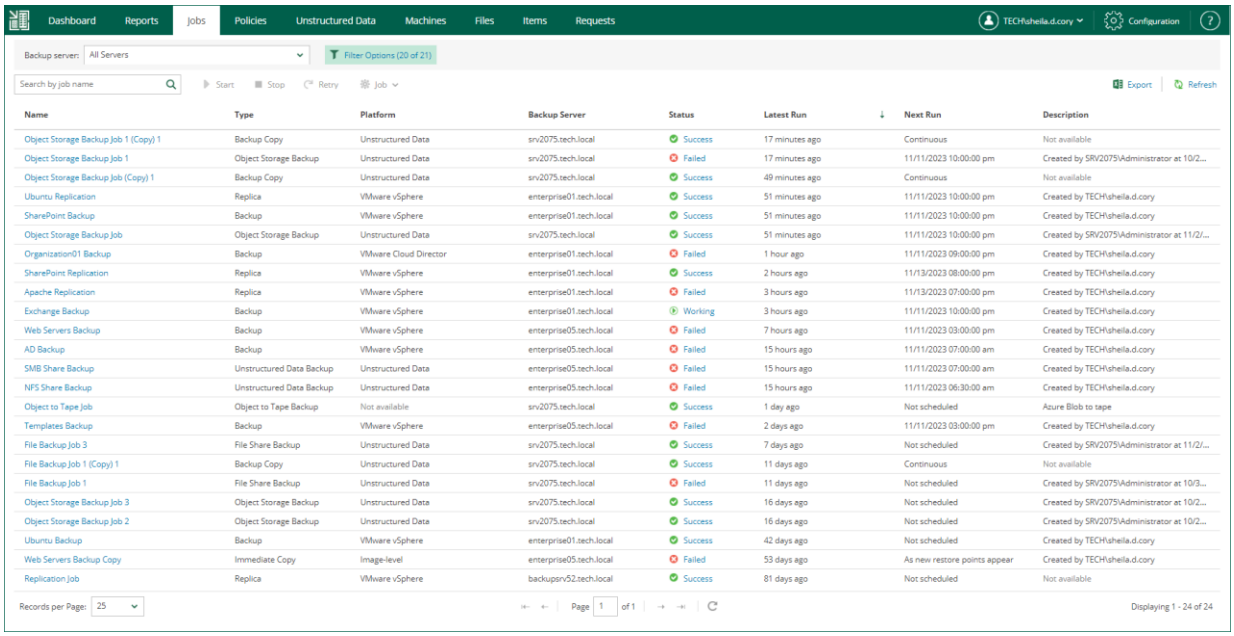
- To view jobs of a specific backup server, select the server from the **Backup server** drop-down list.
- To filter job by job types or job statuses, use the **Filter Options** filter.

  Once you have selected necessary job types and statuses, click **Apply** to apply the filter.
- To find a job by its name, use the search field.

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

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

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



Starting, Stopping and Retrying Jobs

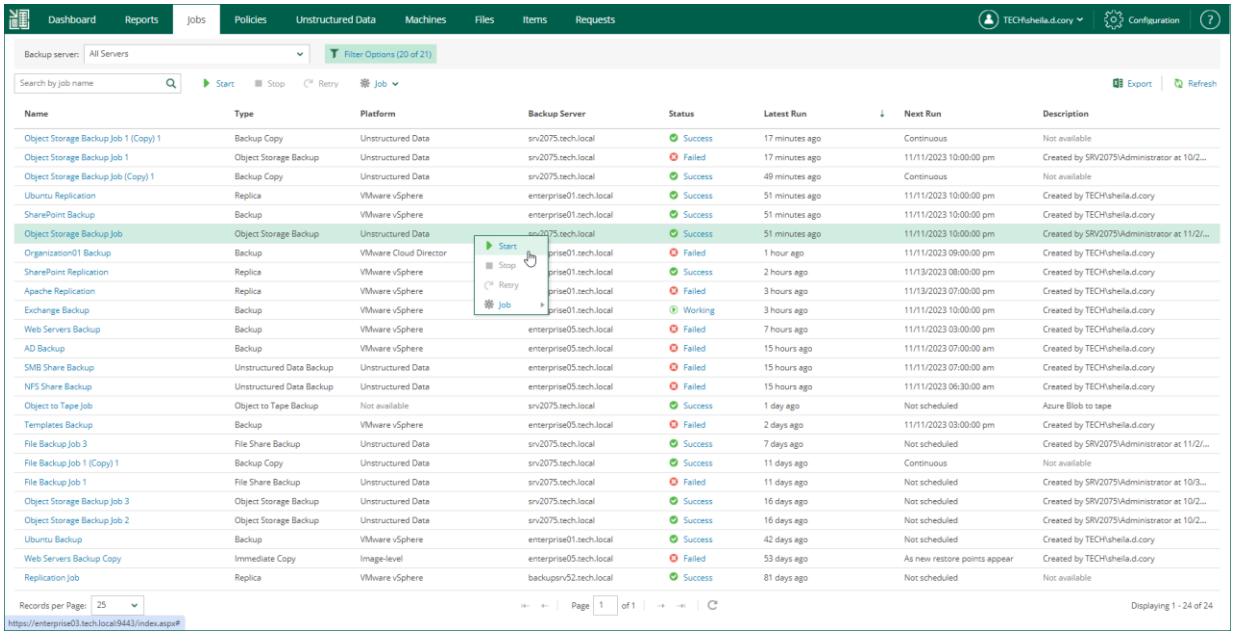
Users with the Portal Administrator role can control backup and replication jobs without the need to access the Veeam Backup & Replication console on the backup server.

On the **Jobs** tab, you can start, stop or retry a job.

- To start a job, select the job from the list and click **Start**.
- To stop a job, select the job from the list and click **Stop**.
- To retry a failed job, select the job from the list and click **Retry**.

NOTE

- For more information on starting a backup copy job, see the Starting and Stopping Backup Copy Jobs section of the Veeam Backup & Replication User Guide.
- For more information on starting and stopping a Microsoft SQL Server, Oracle or PostgreSQL backup job with transaction log processing enabled, see the Starting and Stopping Transaction Log Backup Jobs section of the Veeam Backup & Replication User Guide.



Enabling and Disabling Jobs

Veeam Backup Enterprise Manager allows you to enable and disable jobs of the following types:

- Scheduled backup jobs

  Disabled backup jobs do not start by the specified schedule. When you disable a job that backs up Microsoft SQL Server, Oracle or PostgreSQL machines, transaction log processing (if enabled for that job) will be also disabled.

- Scheduled replication jobs

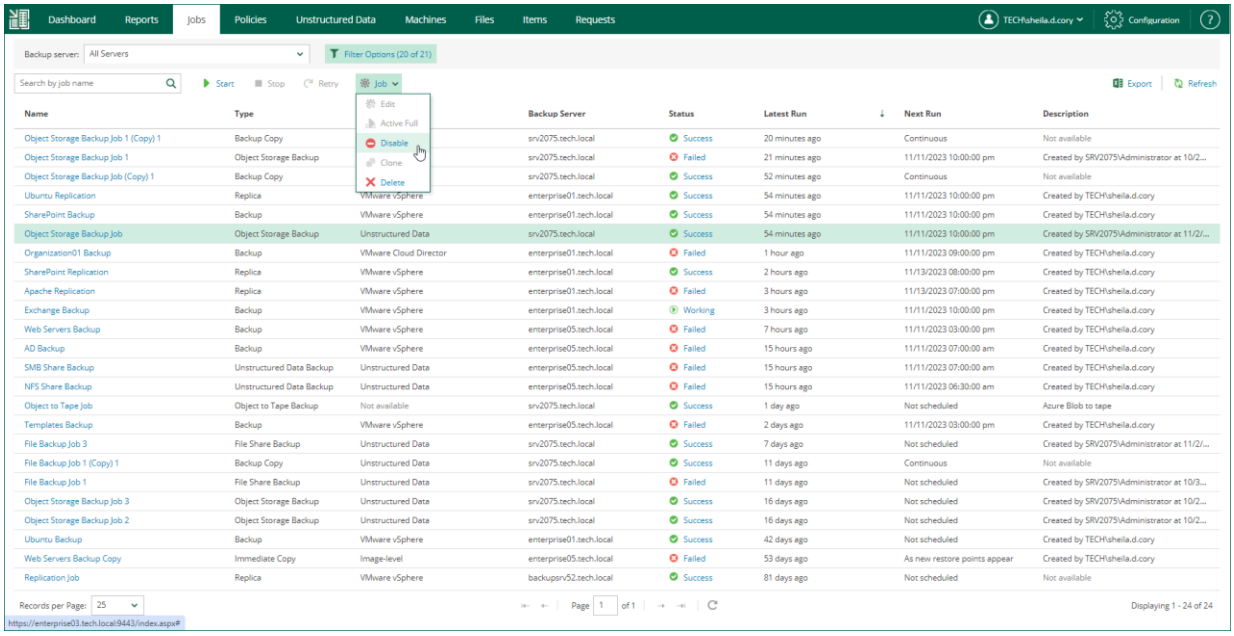
  Disabled replication jobs are not started by the specified schedule.

- Backup copy jobs

  Disabled backup copy jobs do not monitor source backup repositories and do not copy restore points to the target backup repository.

To enable or disable a job:

1. On the **Jobs** tab, select a job from the list.
2. On the toolbar, click **Job**.
3. Select **Enable** or **Disable** from the list of commands.



Editing Jobs

Users with the Portal Administrator role can modify settings of VMware and Hyper-V backup and replication jobs that have been previously configured on backup servers connected to Veeam Backup Enterprise Manager. In Enterprise Manager, you can change only a subset of the job settings. To edit other job settings, use the Veeam Backup & Replication console.

IMPORTANT

- You can edit jobs if you have an Enterprise or Enterprise Plus license installed.
- In Enterprise Manager, you cannot edit jobs that are managed by backup servers of earlier versions as well as Veeam Agent backup jobs, file backup jobs, object storage backup jobs, and backup copy jobs. To edit settings of such jobs, use the Veeam Backup & Replication console.

In Veeam Backup Enterprise Manager, you can change the following job settings:

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

The changes take effect with the next job run.

NOTE

If the *Location* properties of the source object and target object do not match, you will receive a warning message after you finish editing. For example, you may have a backup job targeted at repository located in Sydney, and source machines located in London.

To edit a job, use the **Edit Backup Job** (or **Edit Replication Job**) wizard.

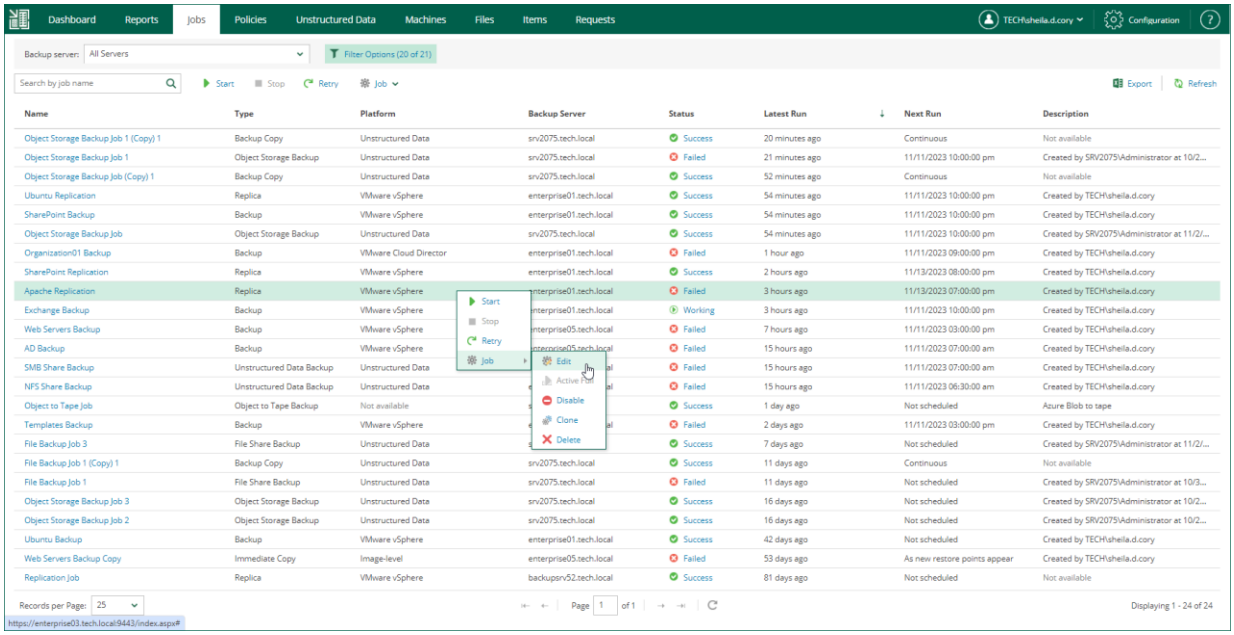
1. Launch the wizard for job editing.
2. Edit job name and retention settings.
3. Edit the list of VMs.
4. Change the VM processing order.
5. Configure guest processing settings.
6. Edit job scheduling settings.

Step 1. Launch Wizard

To launch the wizard for job editing:

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

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



Step 2. Edit Job Name and Retention Settings

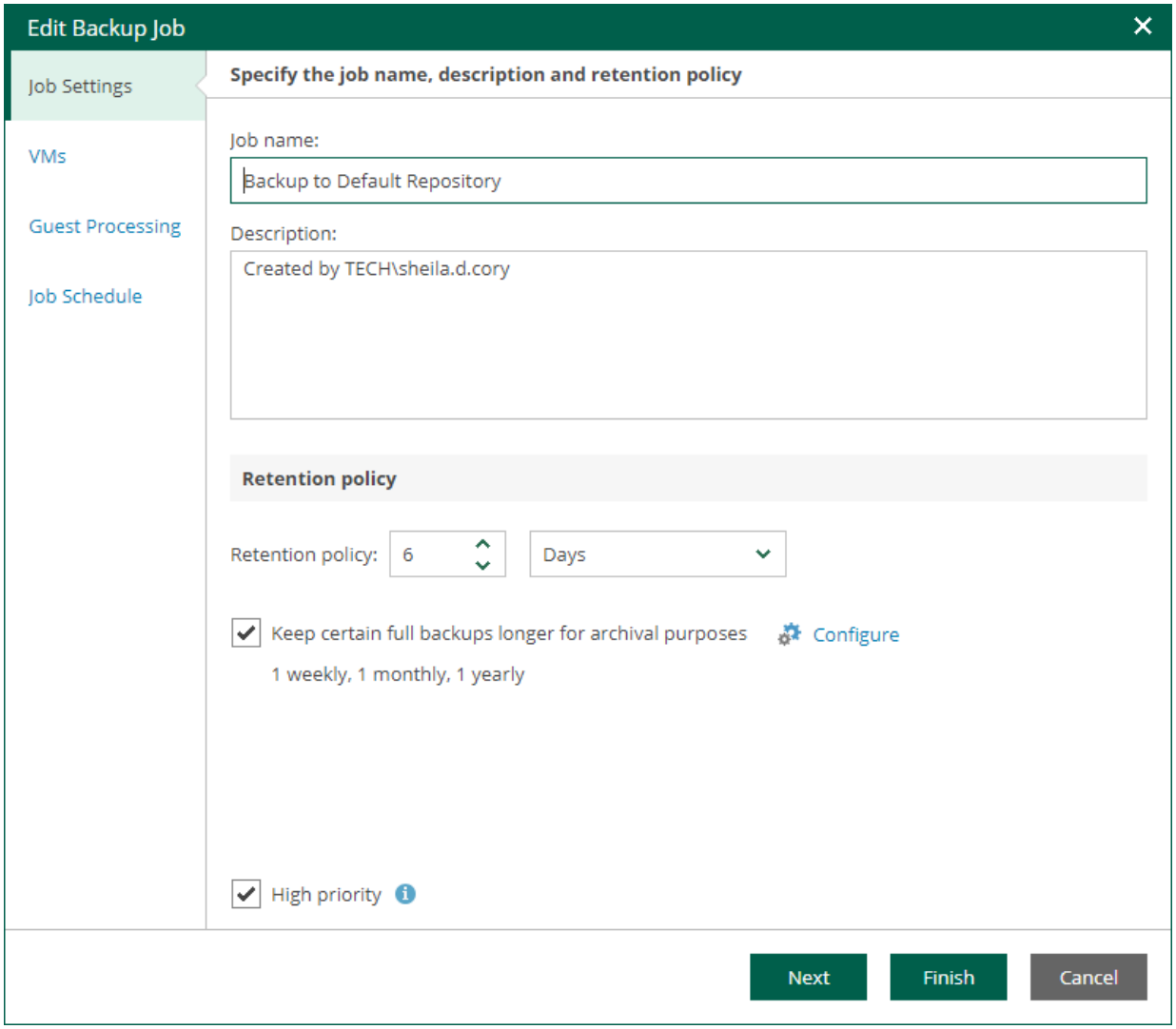
At the **Job Settings** step of the wizard, you can modify name and description for the selected job, as well as its retention policy.

1. In the **Job name** field, enter a name for the job.
2. In the **Description** field, provide an optional description for future reference. The default description contains information about the user who created the job, date and time when the job was created.
3. To change retention policy settings, in the **Retention policy** section, specify the number of days that you want to keep restore points in the backup repository. After this period, restore points will be removed from the backup chain.

   Jobs created in previous versions of Veeam Backup & Replication may have the retention policy defined by the number of restore points rather than by days. For such jobs, you can change the retention unit to days.

   For more information on retention, see the Short-Term Retention Policy section of the Veeam Backup & Replication User Guide. You can also refer to this Veeam KB article.
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how often full backups are retained. For more information, see the Long-Term Retention Policy (GFS) section of the Veeam Backup & Replication User Guide.

5. Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. For more information on job priorities, see the Job Priorities section of the Veeam Backup & Replication User Guide.



Step 3. Edit List of VMs

At the **Virtual Machines** step of the wizard, you can add or remove individual VMs or VM containers, for example, entire hosts or clusters. Jobs with VM containers are dynamic in their nature: if a new machine is added to the container after the job is created, the job is automatically updated to include the added machine.

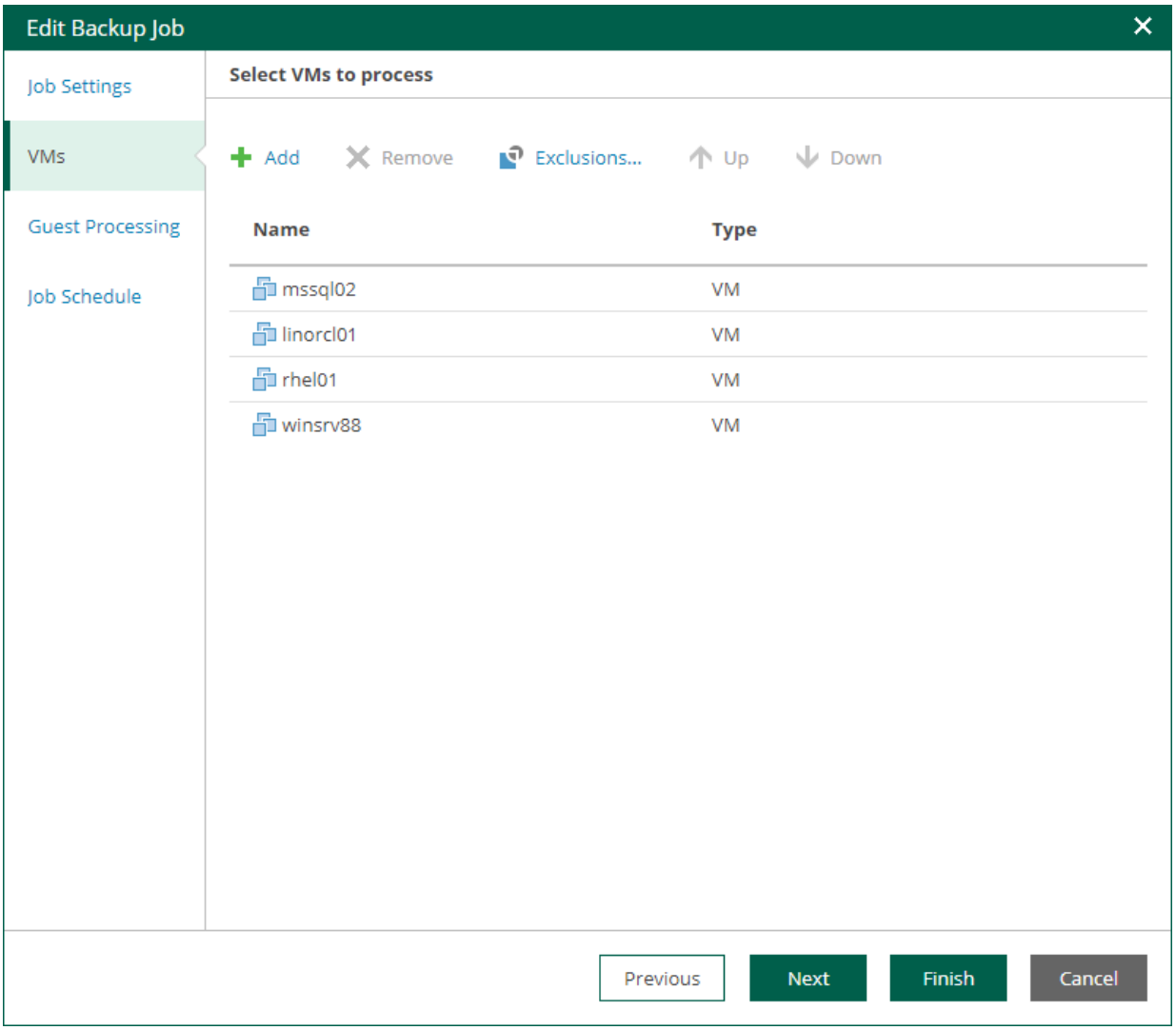
NOTE

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

Adding VMs and VM containers

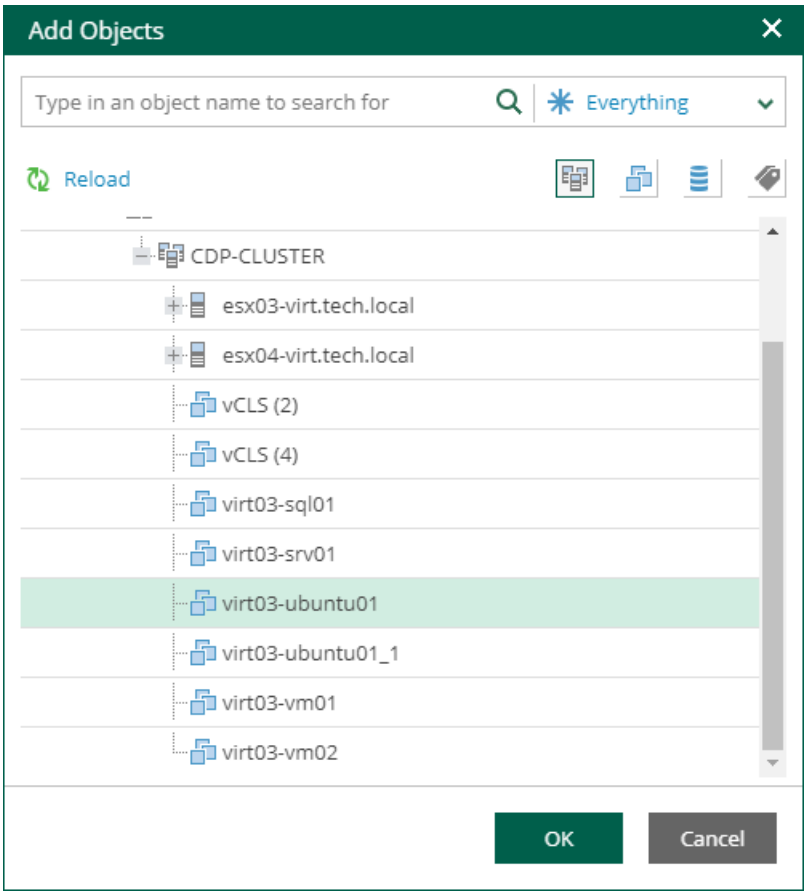
To add a VM or a VM container:

1. Click the **Add**.



2. In the virtual infrastructure tree, select the necessary VMs or VM containers.

   If you select a VM container and later add a new VM to the container, Veeam Backup & Replication will update job settings automatically to include the VM.



> **TIP**
>
> To quickly find the necessary objects, you can do the following:
>
> - Search for objects: type a name or part of a name in the search field. Specify the type of the object from a scroll list next to the search field.
> - Use the buttons in the upper-right corner to switch between virtual infrastructure views:
>   - For Microsoft Hyper-V objects, you can switch between the *Hosts and VMs*, *Hosts and Volumes*, and *Hosts and VM Groups* views.
>   - For VMware vSphere objects, you can switch between the *Hosts and Clusters*, *VMs and Templates*, *Datastores and VMs* and *Tags and VMs* views.
>   - For VMware Cloud Director, protection groups, unstructured data and Nutanix AHV, switching the views is not available.

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

Removing VMs and VM containers

To remove a VM or VM container, select it in the list and click **Remove**.

Excluding VMs

You can also exclude individual VMs from VM containers (for example, if you need to back up the whole VMware or Hyper-V server except several machines running on this server).

To exclude VMs from a VM container:

1. Select a VM container in the list and click **Exclusions**.
2. In the **Exclusions** window, click **Add** and select machines that you want to exclude.

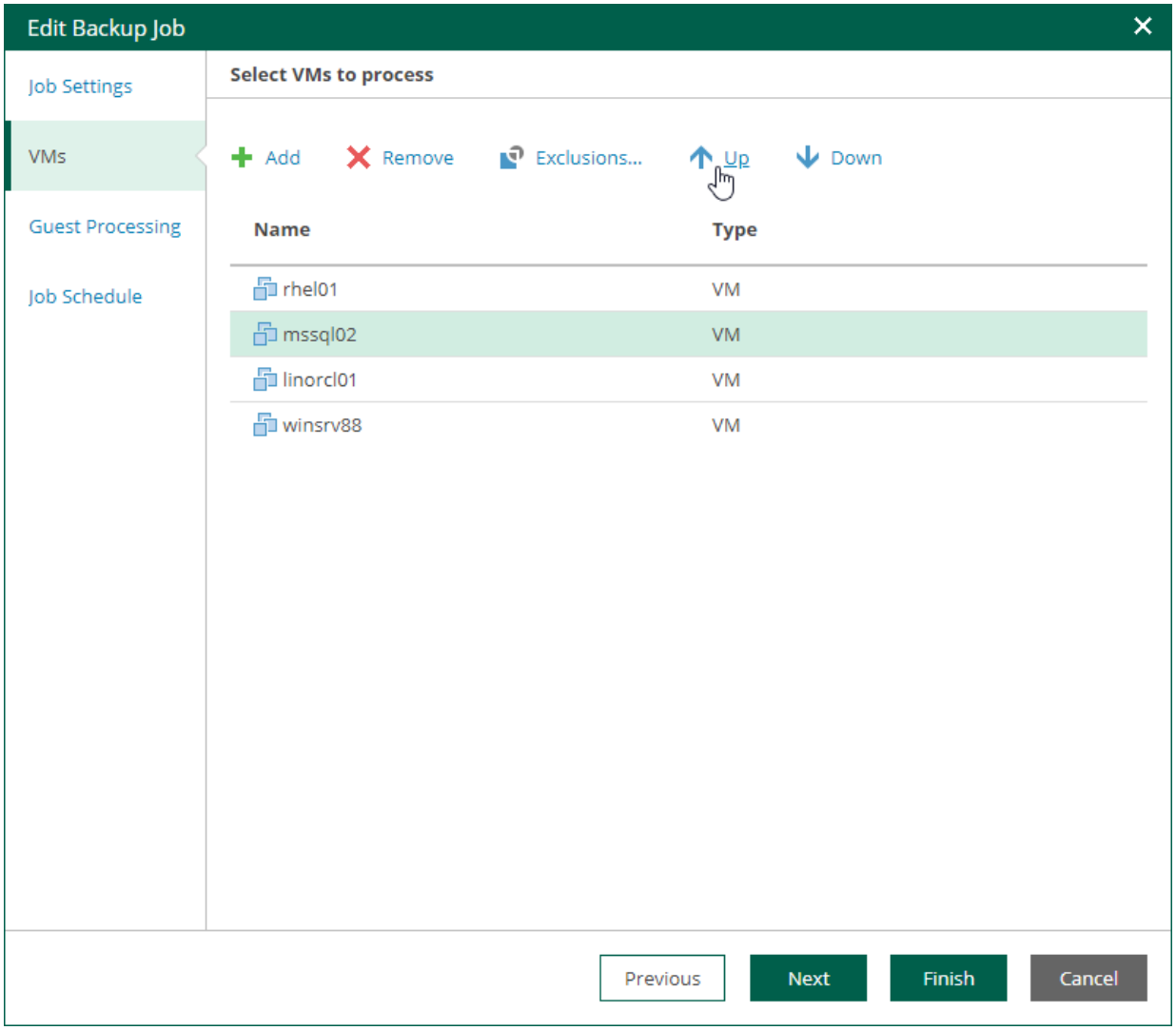
Step 4. Change VM Processing Order

At the **Virtual Machines** step of the wizard, you can change the VM processing order. It can be helpful if specific VMs must be processed first, if you want to ensure that processing of a MV does not overlap with other scheduled activities, or that VM processing is completed before the certain time.

To change the VM processing order, select the necessary machines and move them up or down the list using the **Up** and **Down** buttons on the right. In the same manner, you can set the backup order for containers in the backup list.

NOTE

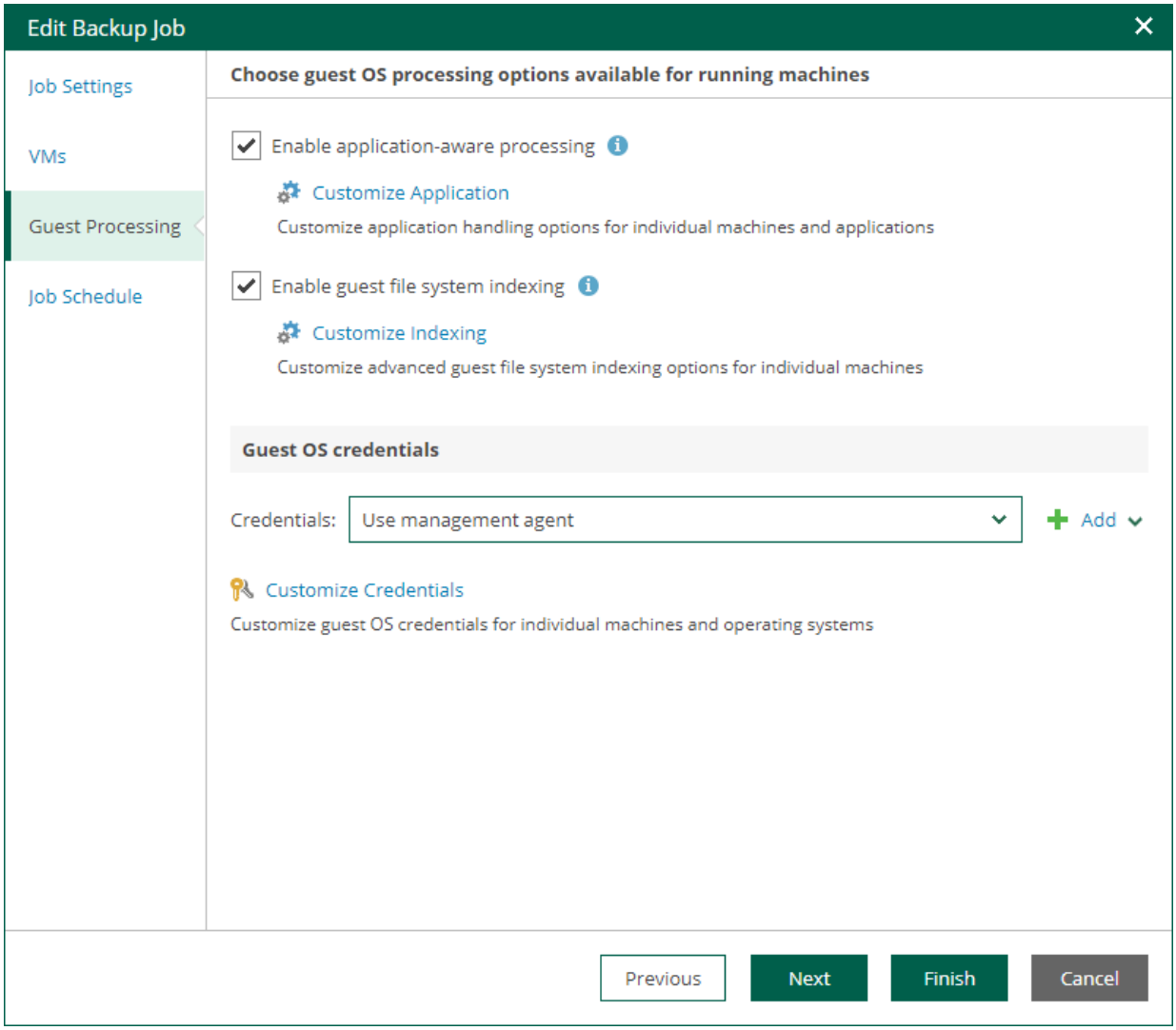
- VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, add them as standalone VMs, not as a part of containers.
- The processing order may differ from the order that you have defined. For example, if resources of a VM that is higher in the priority are not available, and resources of a VM that is lower in the priority are available, the VM with the lower priority will be processed first.
- For VMware Cloud Director backup jobs, you can change the order of the following Cloud Director objects: VMs, vApps, organization VDCs, organizations and the Cloud Director instance. The scope depends on your Cloud Director access rights.
- For VMware Cloud Director replication jobs, you cannot change the VM processing order. You can manage only vApps and other Cloud Director containers.



Step 5. Configure Guest Processing Settings

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

- Application-Aware Processing
- Guest OS File Indexing
- Guest OS Credentials



Application-Aware Processing

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

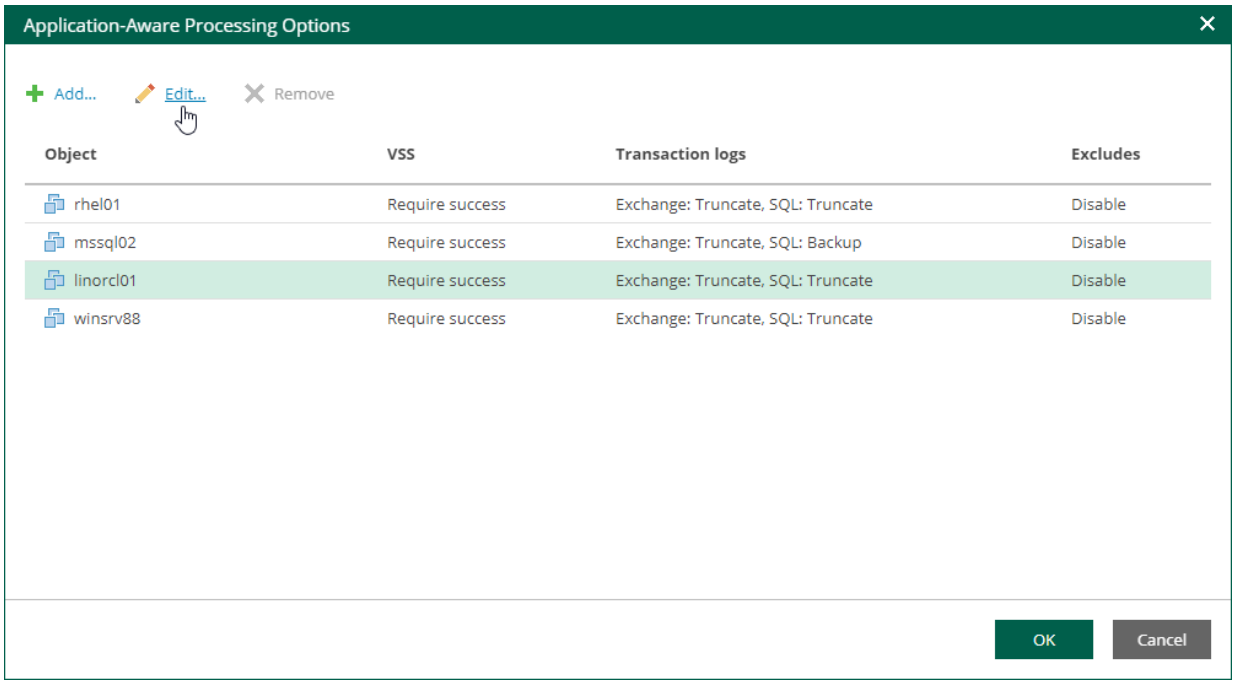
To configure application-aware processing, take the following steps:

1. Select the **Enable application-aware processing** check box.

2. Click the **Customize Application** link.
3. To define custom settings for a machine, select it and click **Edit**.

   To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.

   To discard custom settings of a machine, select the machine in the list and click **Remove**.
4. Configure the necessary settings for the selected application server:
   - General Settings
   - Microsoft SQL Server Transaction Log Settings
   - Oracle Archived Redo Log Settings
   - PostgreSQL Archive Log Settings
   - VM Guest OS File Exclusion



General Settings

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

1. In the **Applications** section, select the option that corresponds to your transactionally-consistent backup creation scenario.
   - Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the backup job if an error occurs.
   - Select **Try application processing, but ignore failures** if you want to continue the backup process even if an error occurs. This option guarantees completion of the job. The created backup image will not be transactionally consistent, but rather crash-consistent.
   - Select **Disable application processing** if you do not want to enable application-aware processing for the VM. This option makes the **Transaction Logs Processing** section unavailable.

2. If you want Veeam Backup & Replication to process application logs or create copy-only backups, do one of the following:
   - [For Microsoft Exchange and Microsoft SQL VMs] If you want Veeam Backup & Replication to process application logs, select **Process transaction logs with this job** and specify settings on the **SQL** tab. For more information, see Microsoft SQL Server Transaction Log Settings.

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

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

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

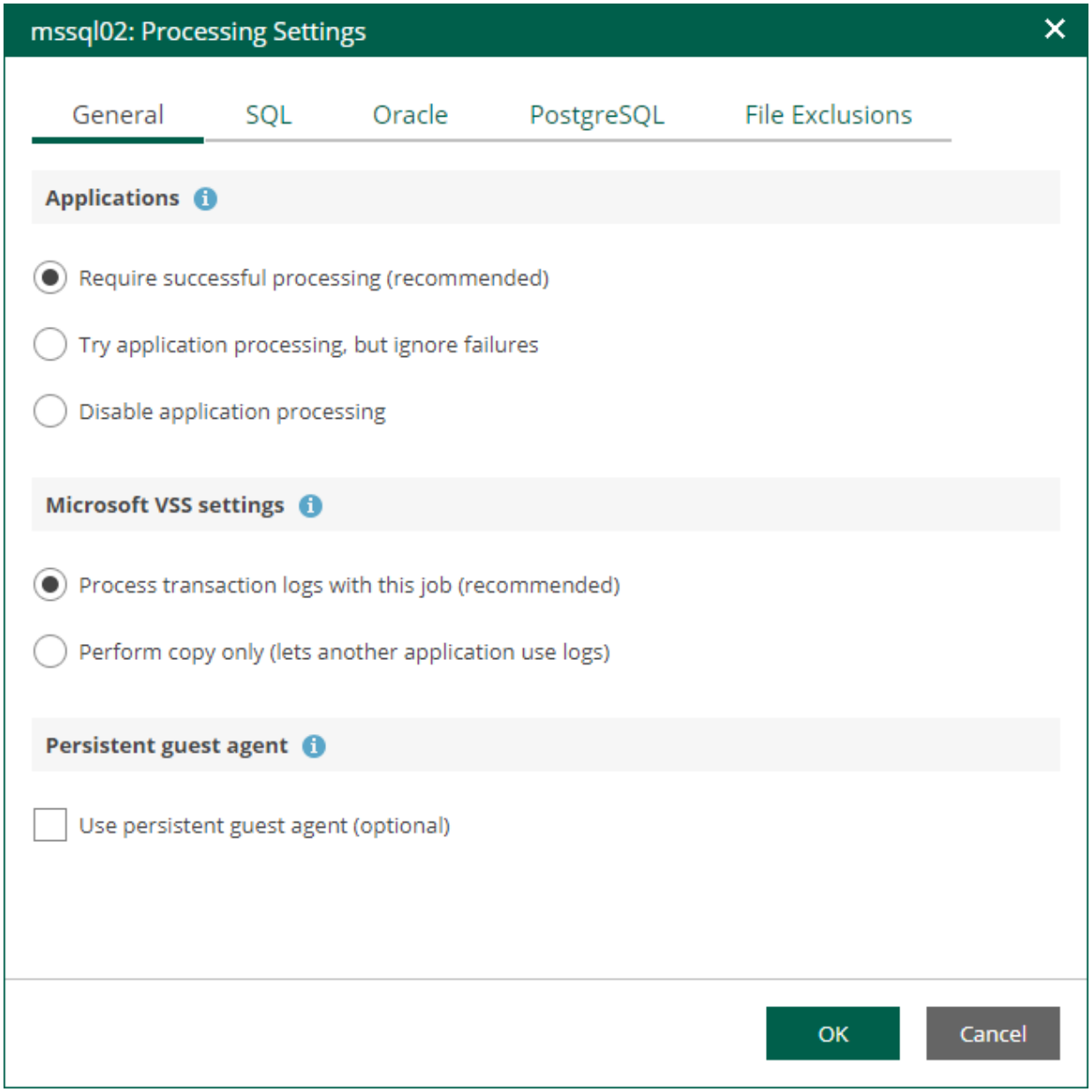
- [For Oracle VMs and PostgreSQL VMs] You must specify settings for application log handling on the **Oracle** and **PostgreSQL** tabs of the **VM Processing Settings** window. For more information, see Oracle Archived Redo Log Settings and PostgreSQL Archive Log Settings.

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

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

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

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

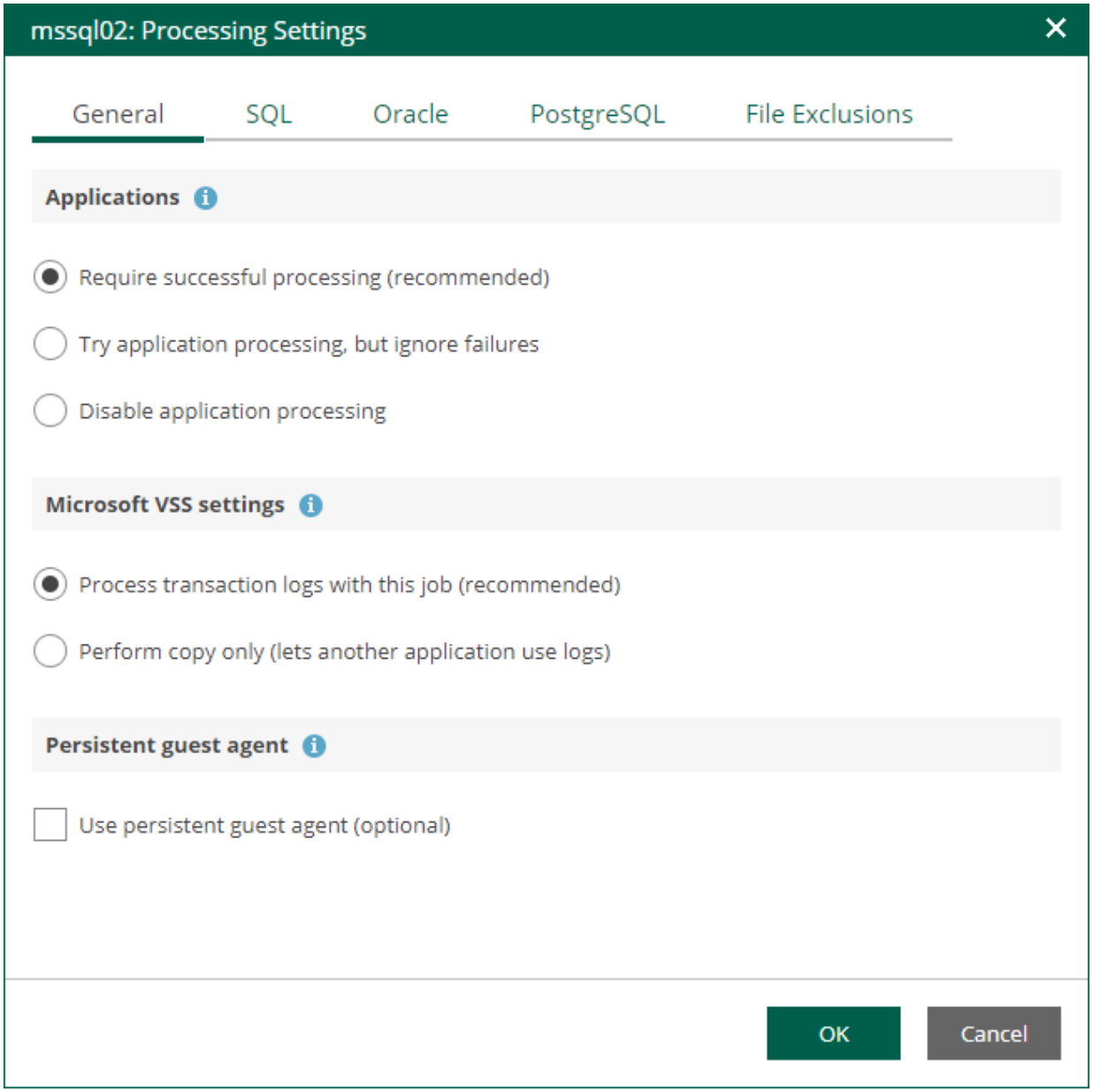


Microsoft SQL Server Transaction Log Settings

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

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

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



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

     > **NOTE**
     >
     > If the account specified at the Guest Processing step does not have enough rights, Veeam Backup & Replication tries to truncate logs using the *NT AUTHORITY|SYSTEM* account. Make sure that the account has permissions listed in the Permissions section of the Veeam Explorers User Guide.

- Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Backup & Replication will not truncate transaction logs on the Microsoft SQL Server VM.

  Select this option for databases that use the Simple recovery model. If you enable this option for databases that use the Full or Bulk-logged recovery model, transaction logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrators must take care of transaction logs themselves.

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

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

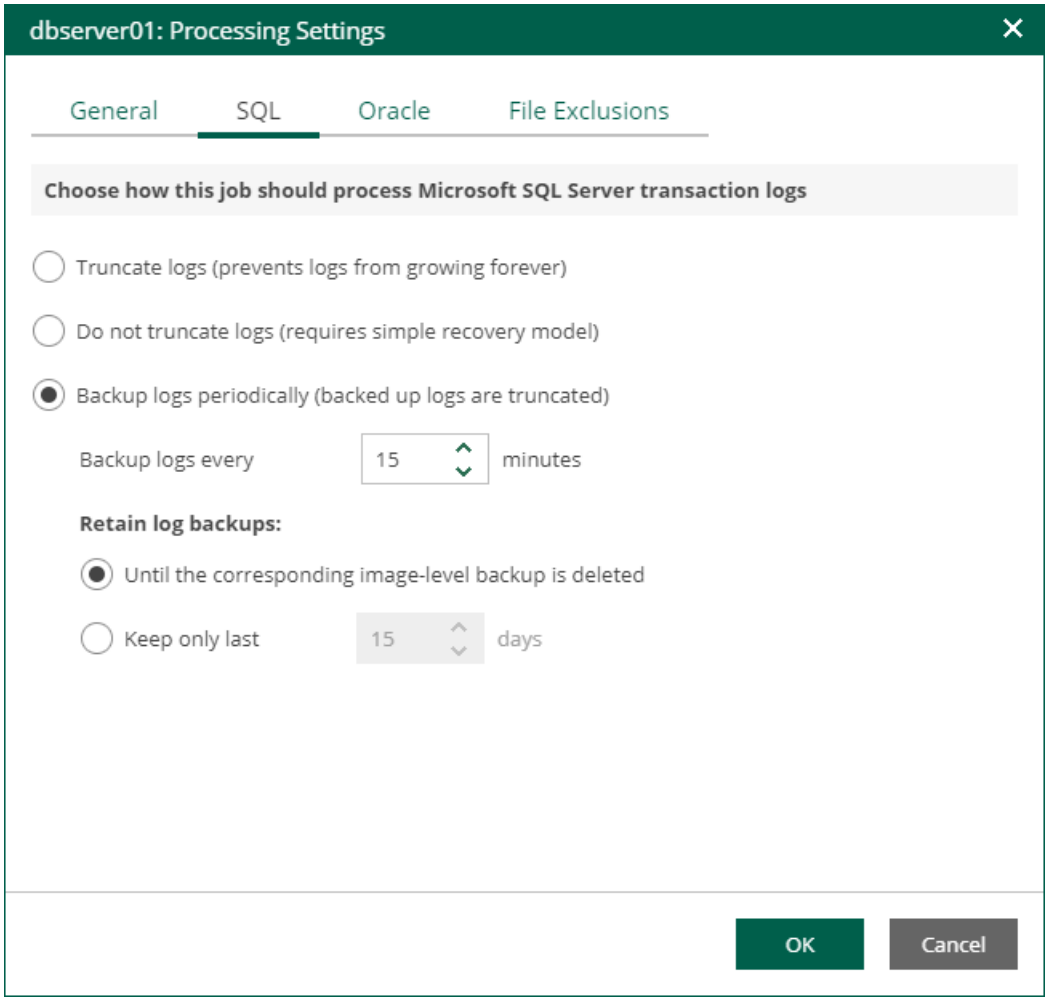
7. If you have selected the **Backup logs periodically** option, specify settings for transaction log backup:

   a. In the **Backup logs every <N> minutes** field, specify the frequency for transaction log backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

   b. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup repository.

      - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
      - Select **Keep only last <N> days** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backups. For more information, see Retention for Transaction Log Backups section of the Veeam Backup & Replication User Guide.

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

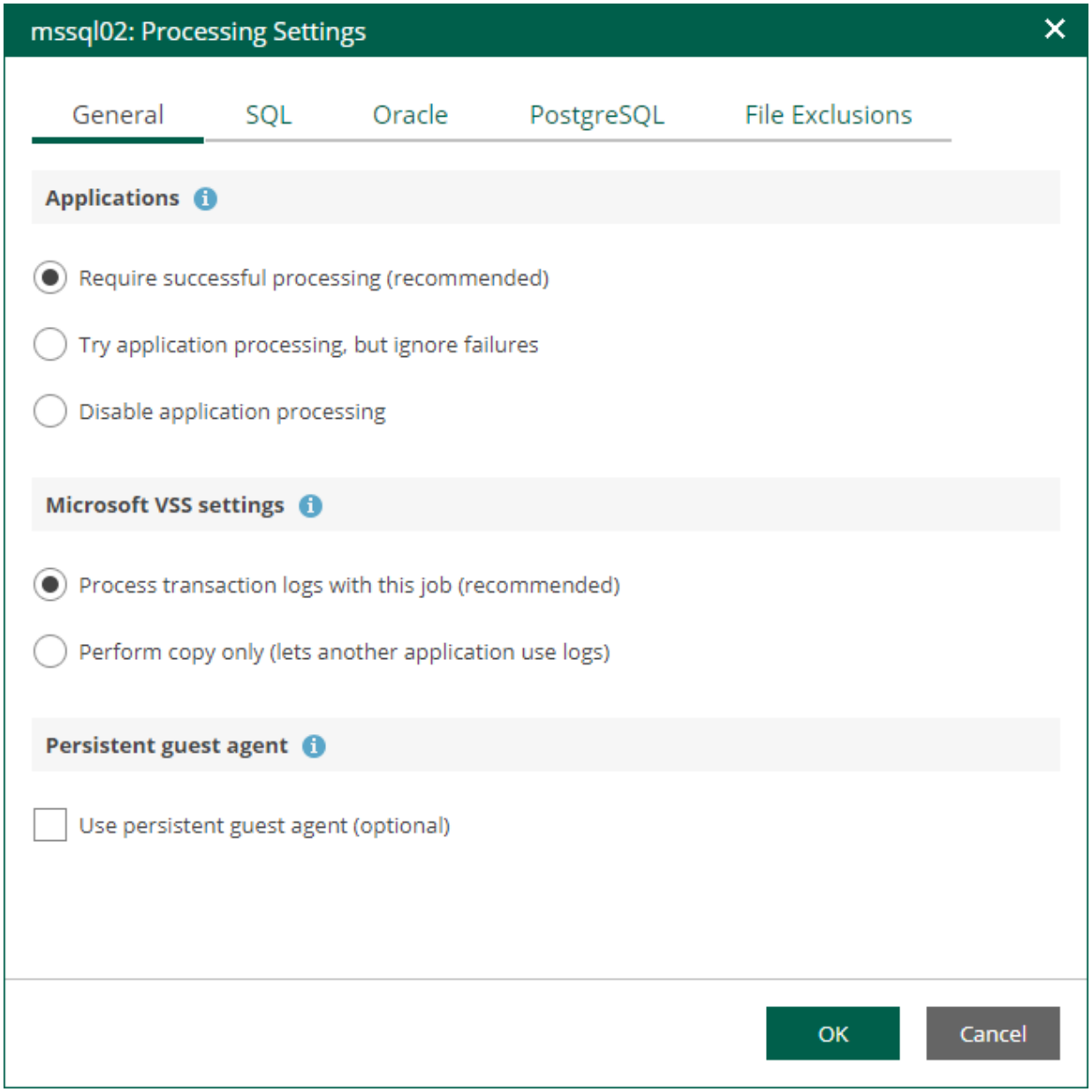


Oracle Archived Redo Log Settings

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

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

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



5. On the **Oracle** tab of the **VM Processing Settings** window, specify log processing settings.

   a. Specify a user account that will connect to the Oracle database and perform Oracle archived logs backup and deletion.

      - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.
      - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

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

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

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

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

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

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

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

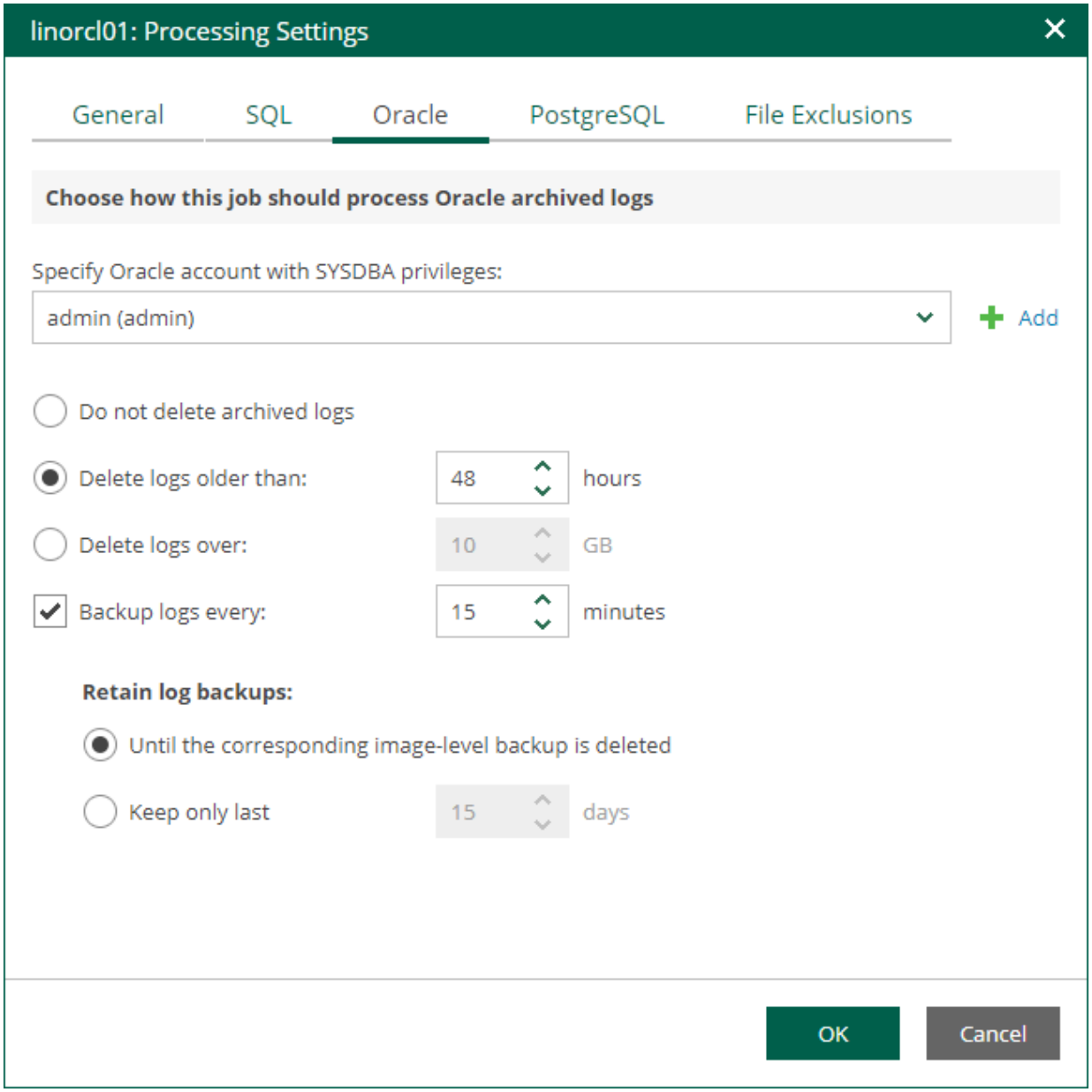
c. To back up Oracle archived logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archived log backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

> **IMPORTANT**
>
> If you plan to use this option together with archived logs deletion from Oracle machine guest, make sure that these settings are consistent: logs should be deleted after they are backed up to repository. Thus, you need to set up backup schedule and log removal conditions appropriately.

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

   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
   - Select **Keep only last <N> days** to keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the image-level backups. For more information, see the Retention for Archived Log Backups section of the Veeam Backup & Replication User Guide.

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

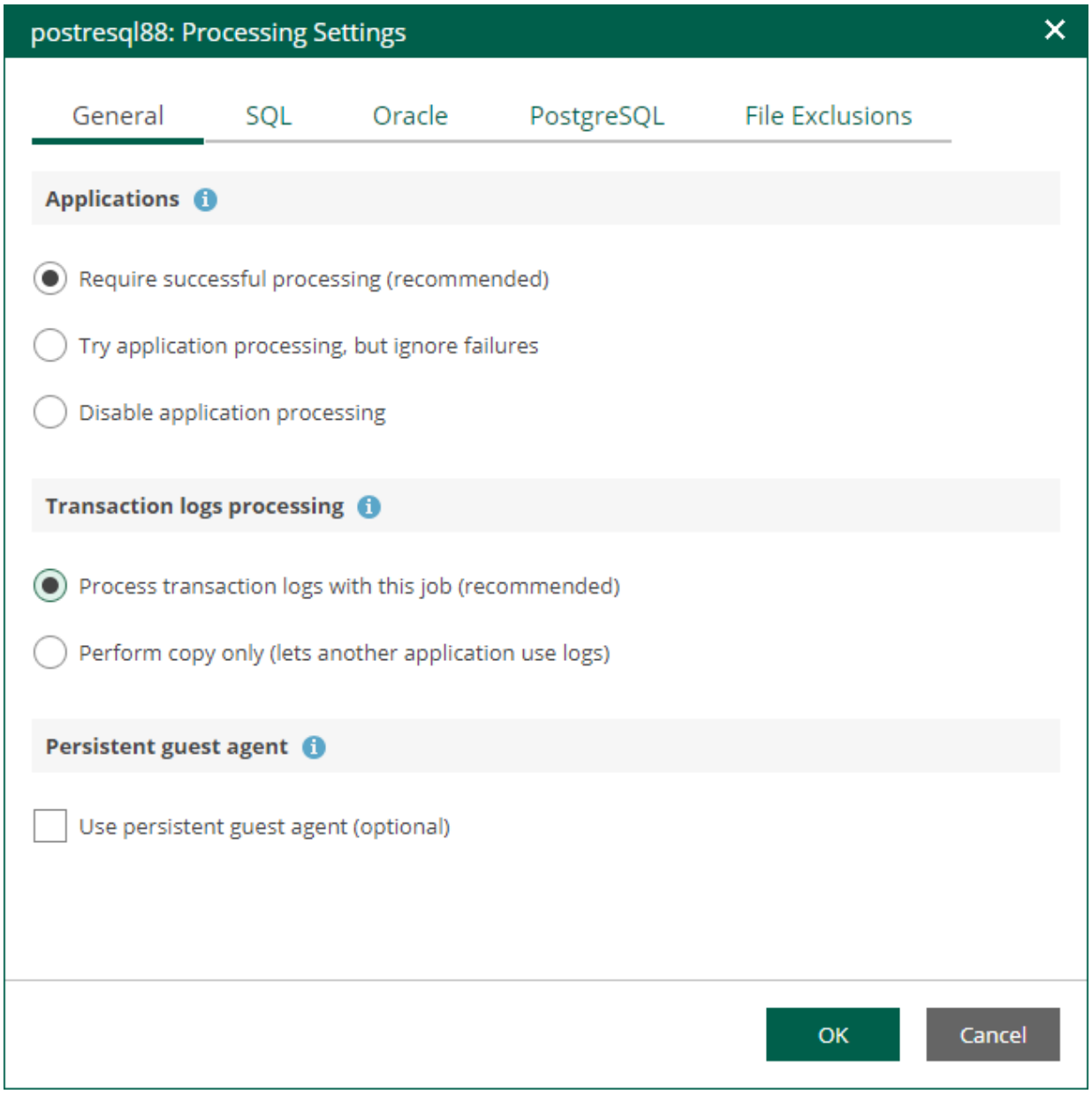


PostgreSQL Archive Log Settings

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

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

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



5. On the **PostgreSQL** tab of the **VM Processing Settings** window, specify settings for PostgreSQL logs processing.

   a. Specify an account that will connect to the PostgreSQL instance and perform PostgreSQL archive logs backup and deletion. The `pg_hba.conf` configuration file of the PostgreSQL instance must contain a record with the account.

      - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the PostgreSQL instance.
      - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

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

   b. Specify an authentication method for the selected user account.

- Select **Database user with password** if you have specified an account with password-based authentication. In this case, you must provide Veeam Backup & Replication with the account password that will be stored in the Veeam Backup & Replication database.
- Select **Database user with password file (.pgpass)** if you have specified an account with password-based authentication. In this case, you do not have to specify the account password when adding the account in Veeam Backup & Replication. Instead, the account password must be specified in the PGPASS password file stored in the user's home directory.
- Select **System user without password (peer)** if you have specified a local system account with peer authentication.

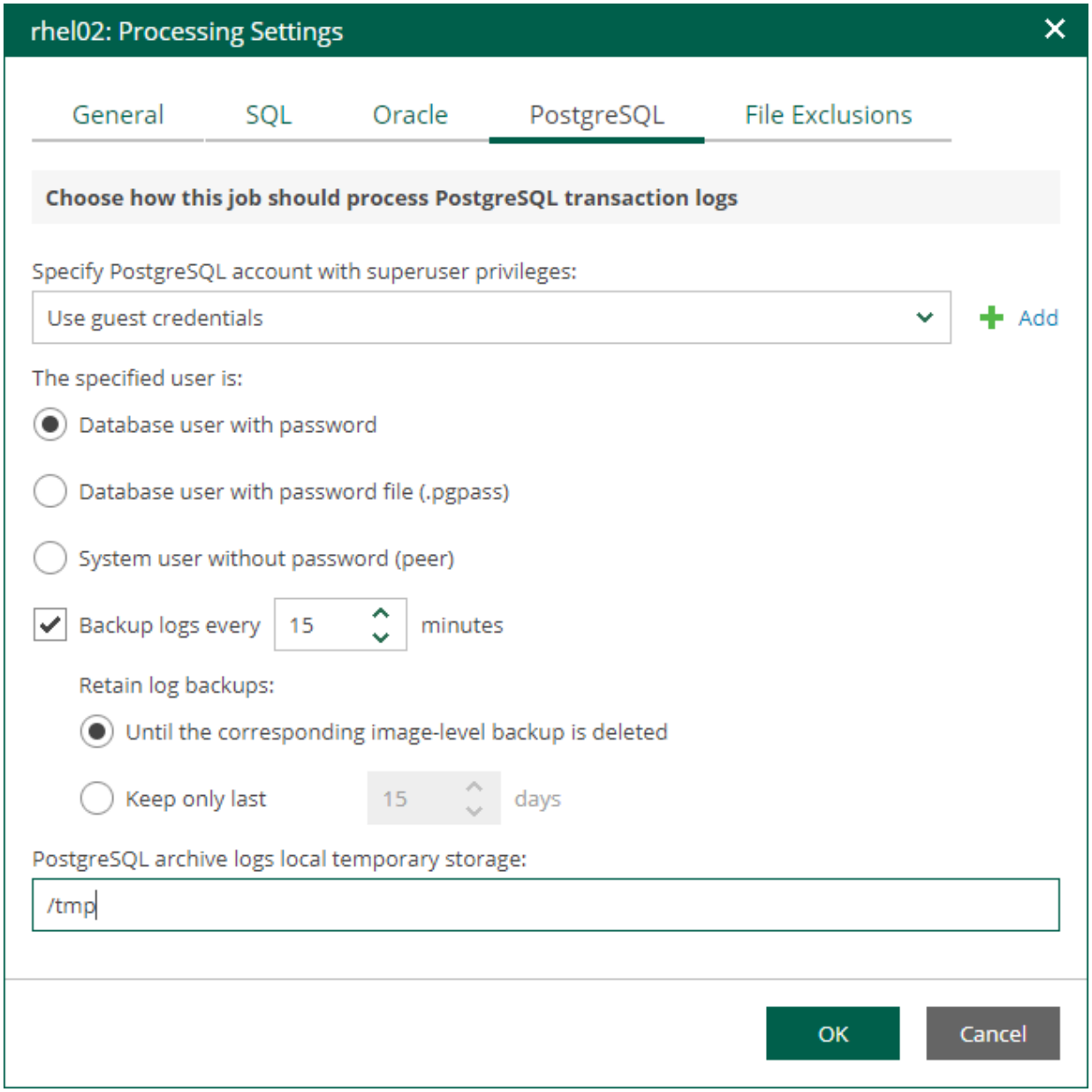
c. To back up PostgreSQL archive logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archive log backup. By default, archive logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

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

- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
- Select **Keep only last <N> days** to keep archive logs for a specific number of days. By default, archive logs are kept for 15 days. If you select this option, you must make sure that retention for archive logs is not greater than retention for the image-level backups. For more information, see the Retention for PostgreSQL WAL Files section of the Veeam Backup & Replication User Guide.

e. In the **PostgreSQL archive logs local temporary storage** field, specify a path on the PostgreSQL machine that Veeam Backup & Replication will use to temporarily store PostgreSQL archive logs until they are backed up. Veeam Backup & Replication does not create the temporary storage folder so the folder must exist on the machine. Make sure the temporary location has enough free space for storing the log files.

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



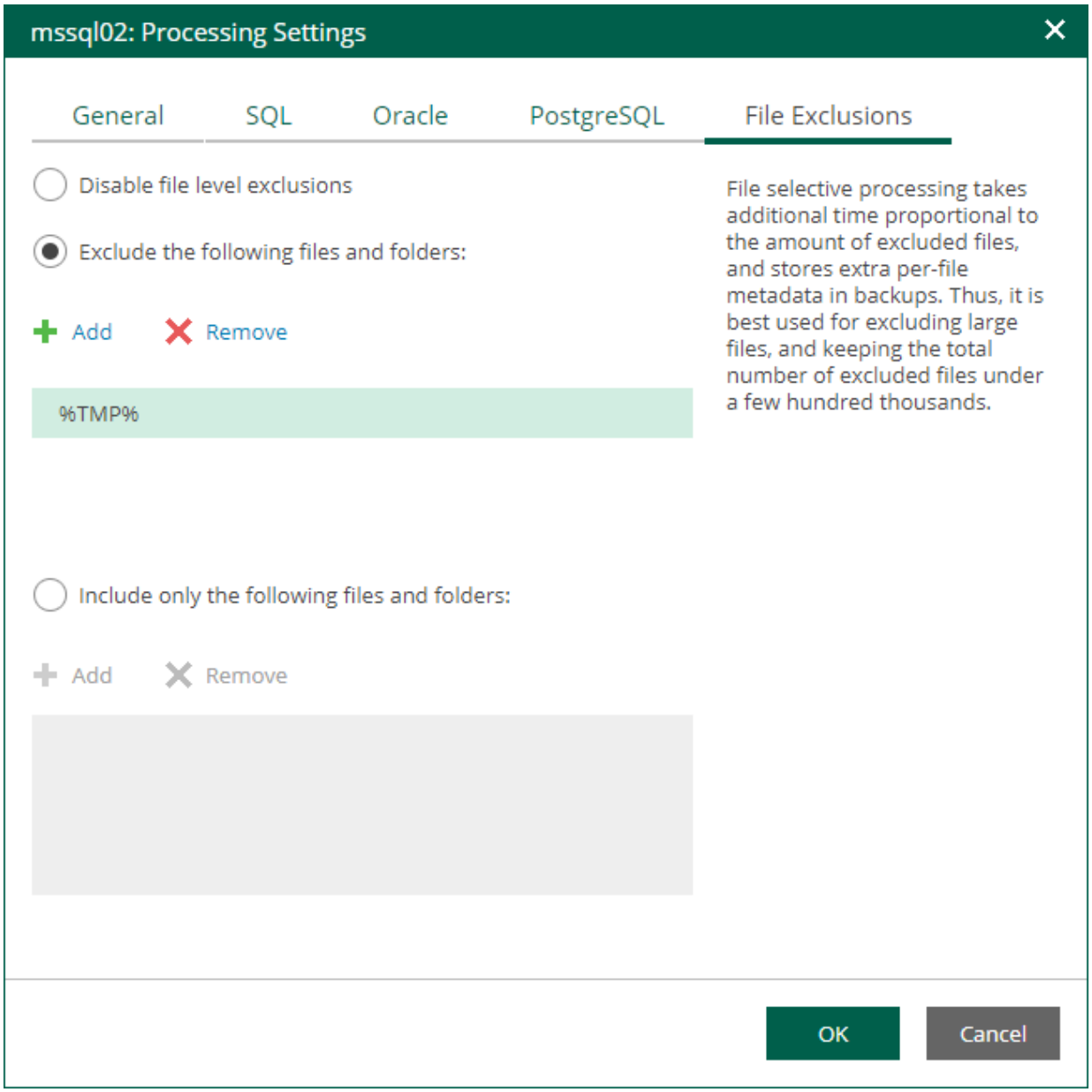
VM Guest OS File Exclusion

If you do not want to back up specific files and folders on the VM guest OS, you can exclude them from the backup. Exclusions can help decrease the backup file size. However, selective processing takes additional time that depends on the number of excluded files. It also requires obtaining per-file metadata (stored in backups). Thus, it is recommended to use this option for excluding large files. By default, exclusions are disabled.

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

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

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



Guest OS File Indexing

To quickly find the necessary guest OS files in backups, select the **Enable guest file system indexing** check box. This setting provides, in particular, advanced search capabilities when viewing guest OS files and performing 1-Click file restore using Enterprise Manager web UI. If indexing is disabled, you can only use quick search within the selected restore point.

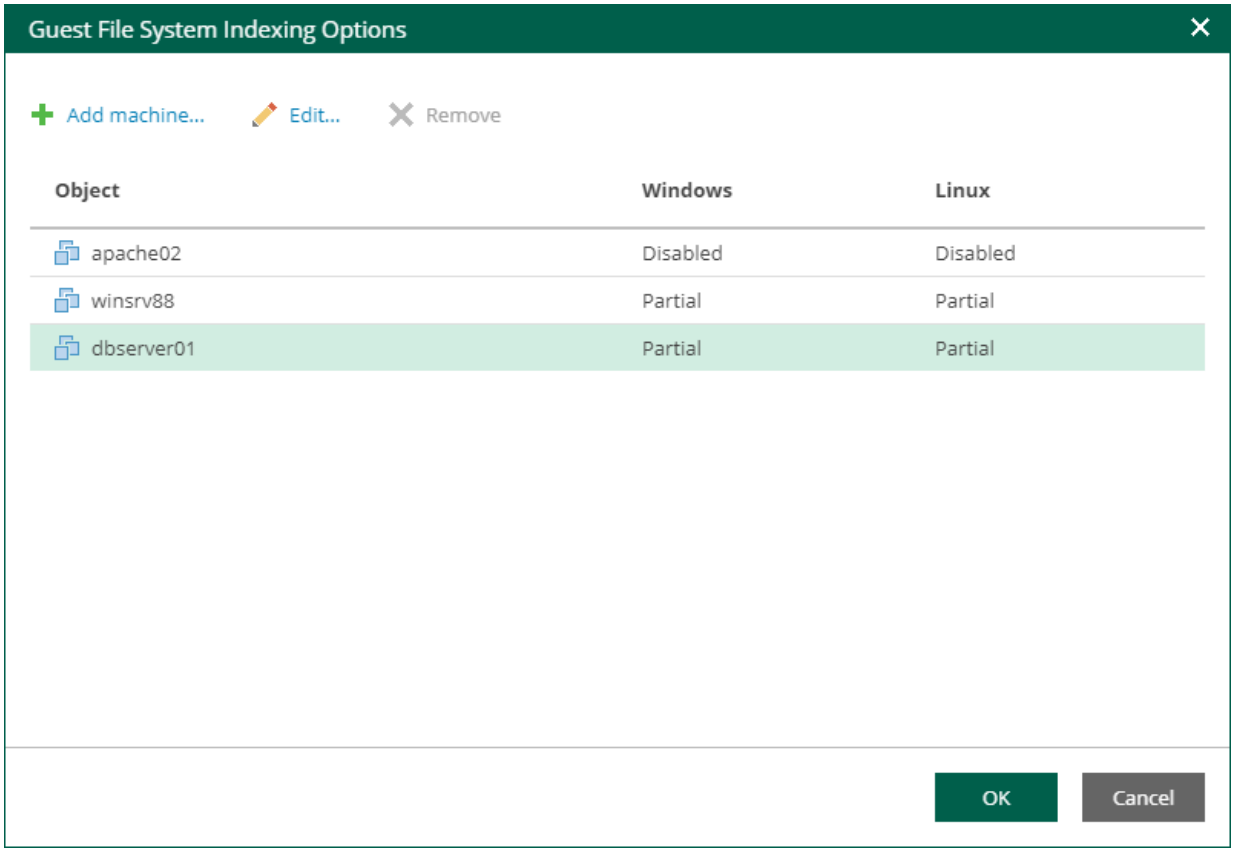
> **NOTE**
>
> For proper file indexing of Linux machines, Veeam Backup & Replication requires several utilities to be installed on the machines: `mlocate`, `gzip`, and `tar`. If these utilities are not found, you are prompted to deploy them to support index creation.

To provide granular indexing options for individual machines:

1. Click the **Customize Indexing** link.
2. In the **Guest File System Indexing Options** window, select a machine from the list and click **Edit**.

   Consider the following:

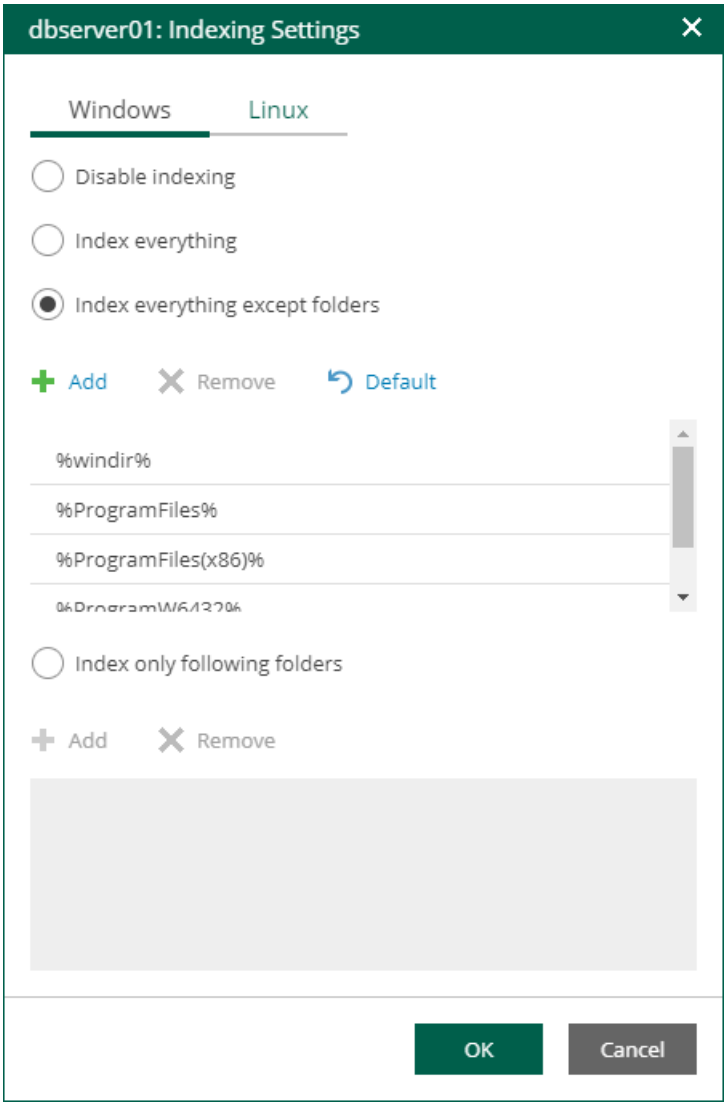
   - To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add Machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
   - To discard custom settings of a machine, select it from the list and click **Remove**.



3. In the **Indexing Settings** window displayed for the selected machine, go to the **Windows** or **Linux** tab and specify what files should be indexed:

   - Select **Disable indexing** if you do not want to index guest OS files of the machine.
   - Select **Index everything** if you want to index all guest OS files inside the machine.
   - Select **Index everything except folders** if you want to index all guest OS files except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders to exclude using the **Add** and **Remove** buttons.

- Select **Index only following folders** to select specific folders that you want to index. To form the list of folders, use the **Add** and **Remove** buttons.

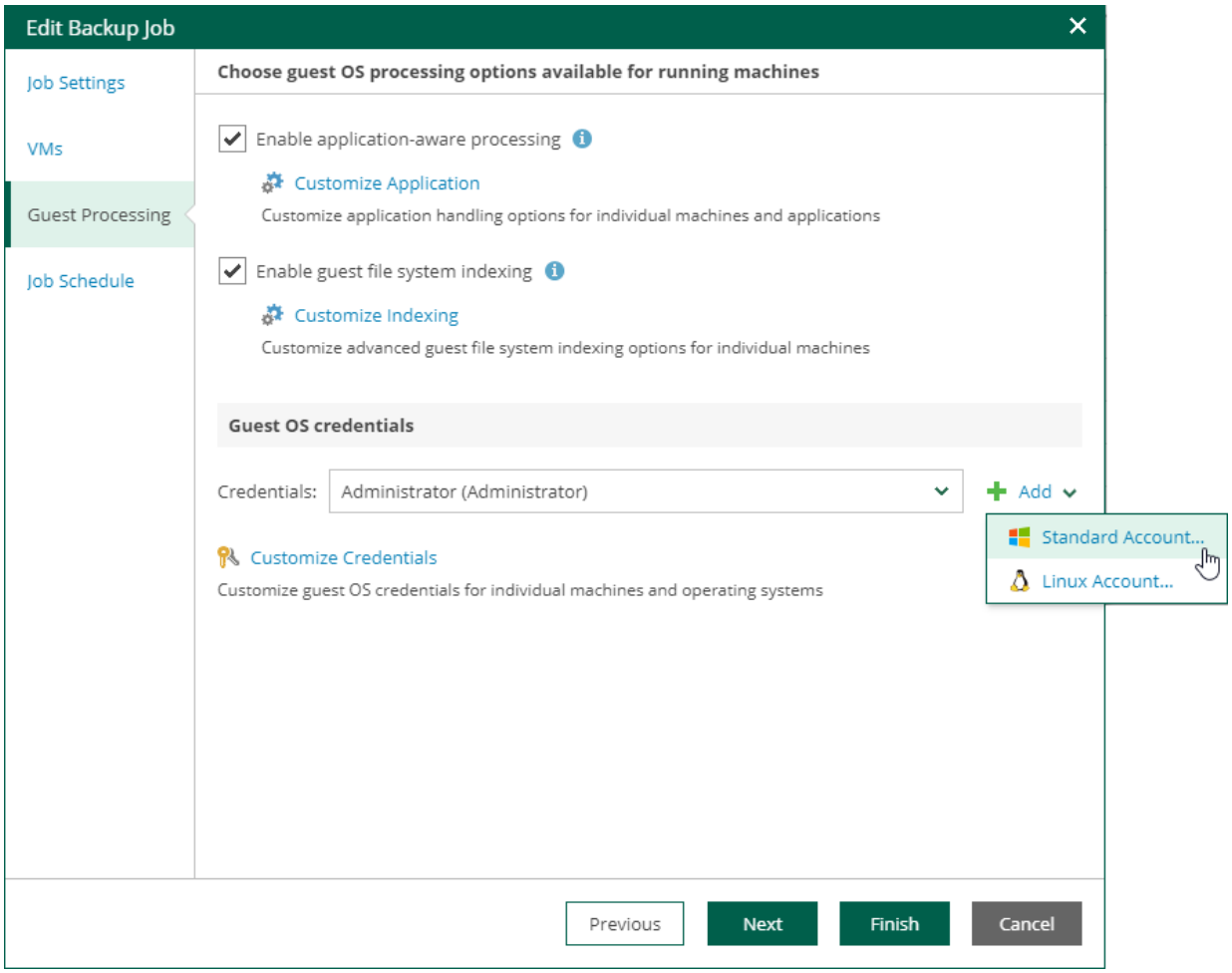


4. Click **OK** to save the settings and close the window.

Guest OS Credentials

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

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



In the **Guest OS credentials** section, you can select credentials from the list, or click the **Add** button to add new credentials.

- For Windows guest OS, specify a user account (name and password) with local administrative rights on target machine, and optional description. Credentials must be specified in the following format:
  - For Active Directory accounts: *DOMAIN|Username*
  - For local accounts: Username or *HOST|Username*
- For Linux guest OS, you can choose one of the following options:
  - If Management Agent is installed on the VM, you can select the **Use management agent** option.
  - If Management Agent is not installed on the VM, specify a user name, password, and SSH port (by default, port 22 is used).

    If you specify data for a non-root account that does not have root privileges on a Linux server, you can use the **Non-root account** section to grant this account elevated permissions as follows:

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

ii. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the root account password.

If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

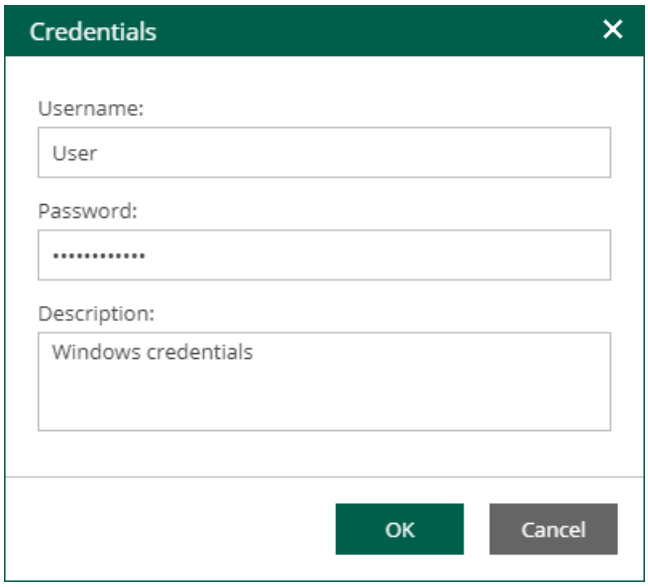
iii. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the root account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

Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

IMPORTANT

For machine guest OS indexing of Linux-based machines, a user account with root privileges on the machine is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based machine, grant root privileges to this account and specify settings of this account in the **Guest OS credentials** section.

It is also recommended to avoid additional commands output for the specified user (like messages echoed from within `~/.bashrc` or command traces before execution), because they may affect Linux machine processing.



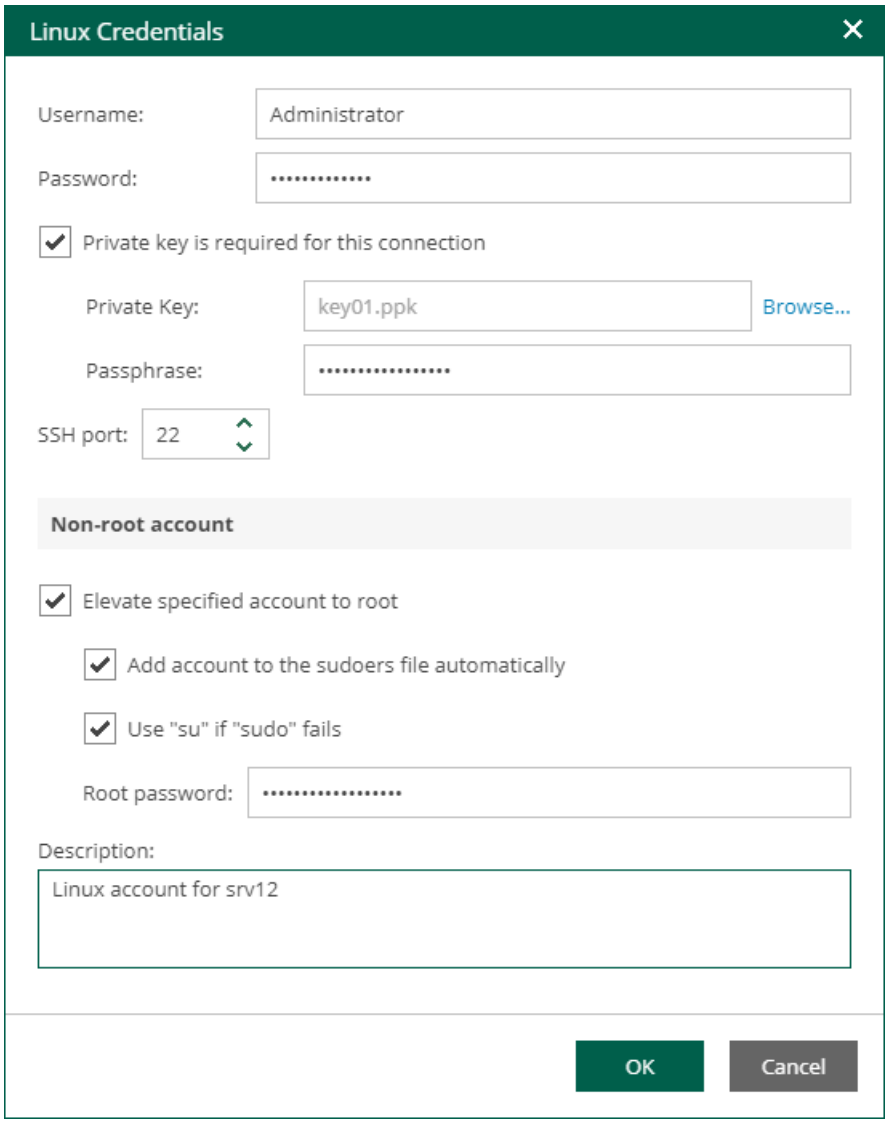
Linux Private Key

Another option is to use Linux private key. This method eliminates the need to supply password at each login, helps to protect against malicious applications like keyloggers, thus strengthening security, and simplifies launch of automated tasks, decreasing administrative load in Linux environments. For this method, a user must create a pair of keys:

- *Private key* is stored on the client (user's) machine — that is, on the machine where Veeam Backup & Replication runs. The key is usually stored in the encrypted form. To decrypt a private key, you need to supply a passphrase specified at key creation.
- *Public key* is stored on the server (Linux machine) in a special `authorized_keys` file that contains a list of public keys.

If you plan to use Linux private key for authentication, make sure you have created private and public keys and stored them appropriately: private key on the client side (Veeam backup server) and public key on the server side (Linux machine). You should also have the passphrase for the private key if it is encrypted. If you select to use Linux private key credentials, you should specify the following:

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



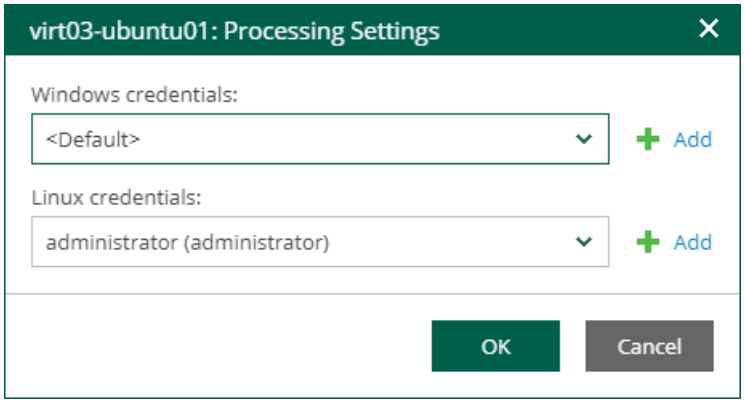
Special Credentials for Machine

By default, for all machines in the list, Veeam Backup & Replication uses common credentials you provided in the **Guest OS credentials** section. To use a different account for deploying the agent inside a specific machine, you can customize credentials for the machine.

To customize credentials:

1. In the **Guest OS credentials** section, select **Customize Credentials**.

2. Select the necessary machine from the list and click **Set User**.
3. Specify custom guest OS credentials and click **OK**.



To remove custom credentials for a machine:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Remove**.

> **NOTE**
>
> To customize settings of a machine added as part of a container, the machine should be included in the list as a standalone instance. For that, click **Add machine** and choose a machine whose settings you want to customize.

Step 6. Edit Job Schedule

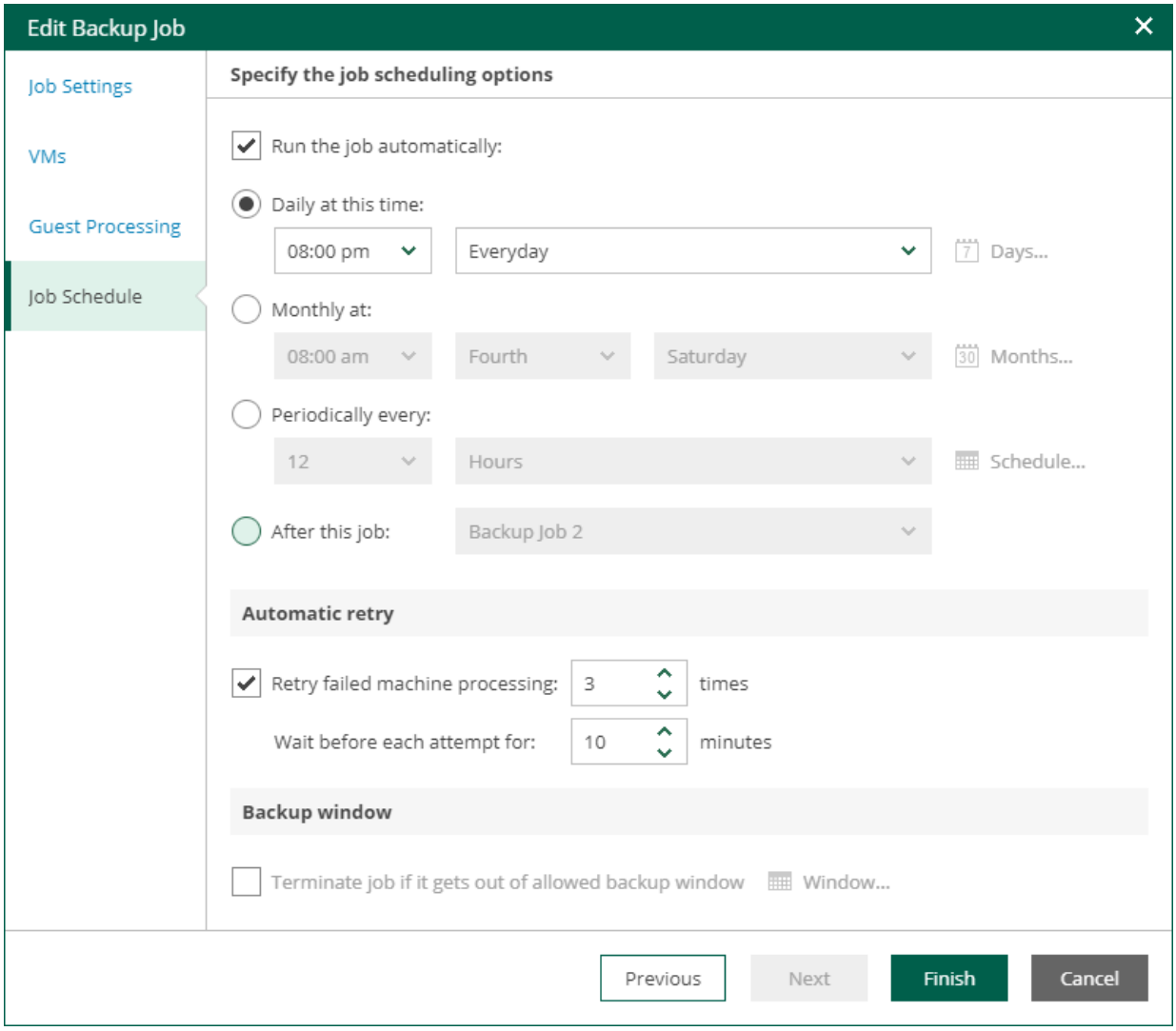
At the **Job Schedule** step of the wizard, you can select to run the job manually or schedule the job to run on a regular basis.

To edit the job schedule:

1. Select the **Run the job automatically** check box. If the check box is not selected, you will need to start the job manually.
2. Edit the scheduling settings. You can select to run the job daily, monthly, periodically with a specific time interval, continuously or after a specific job.

   For more information, see Schedule Settings.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication must attempt to run the backup job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed machines only. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job runs.
4. In the **Backup window** section, edit the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not provide unwanted overhead on the production environment. To set up a backup window for the job:
   a. Select the **Terminate job if it gets out of allowed backup window** check box and click **Window**.

b. Define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.



NOTE

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

Schedule Settings

If you have selected to run the job automatically, you can select one of the following options:

- To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
- To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

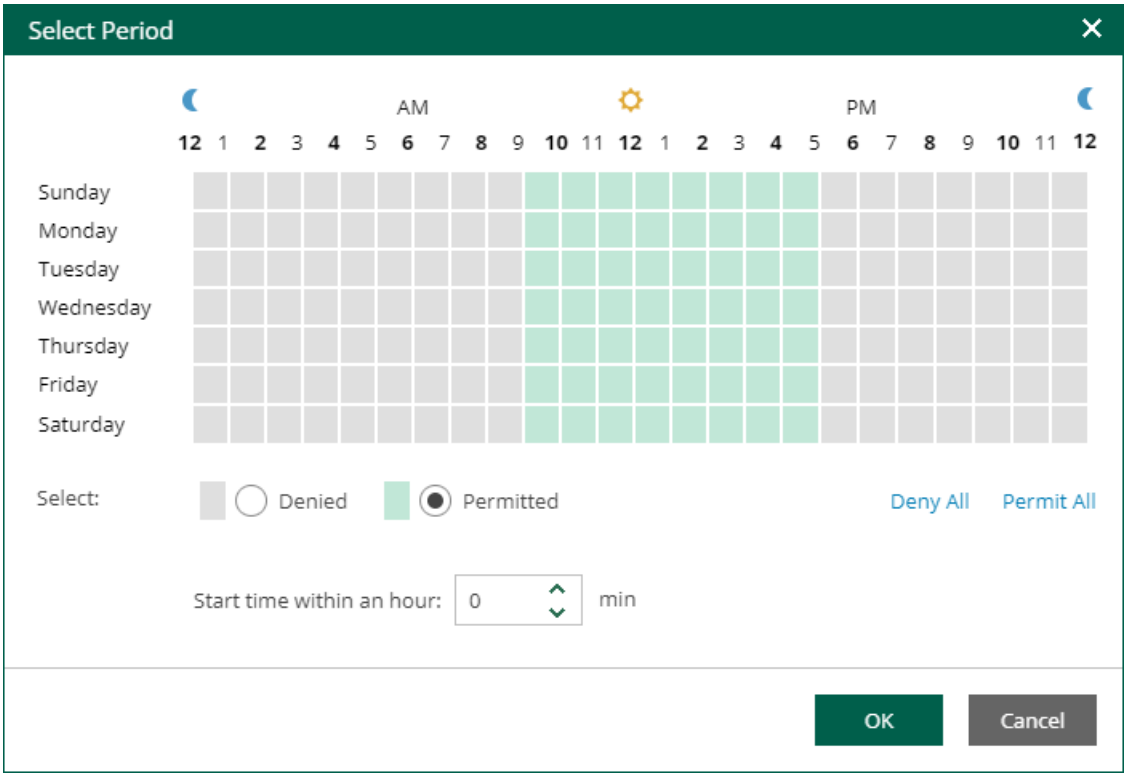
> **NOTE**
>
> When you configure the job schedule, keep in mind possible date and time changes (for example, related to daylight saving time transition).

- To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

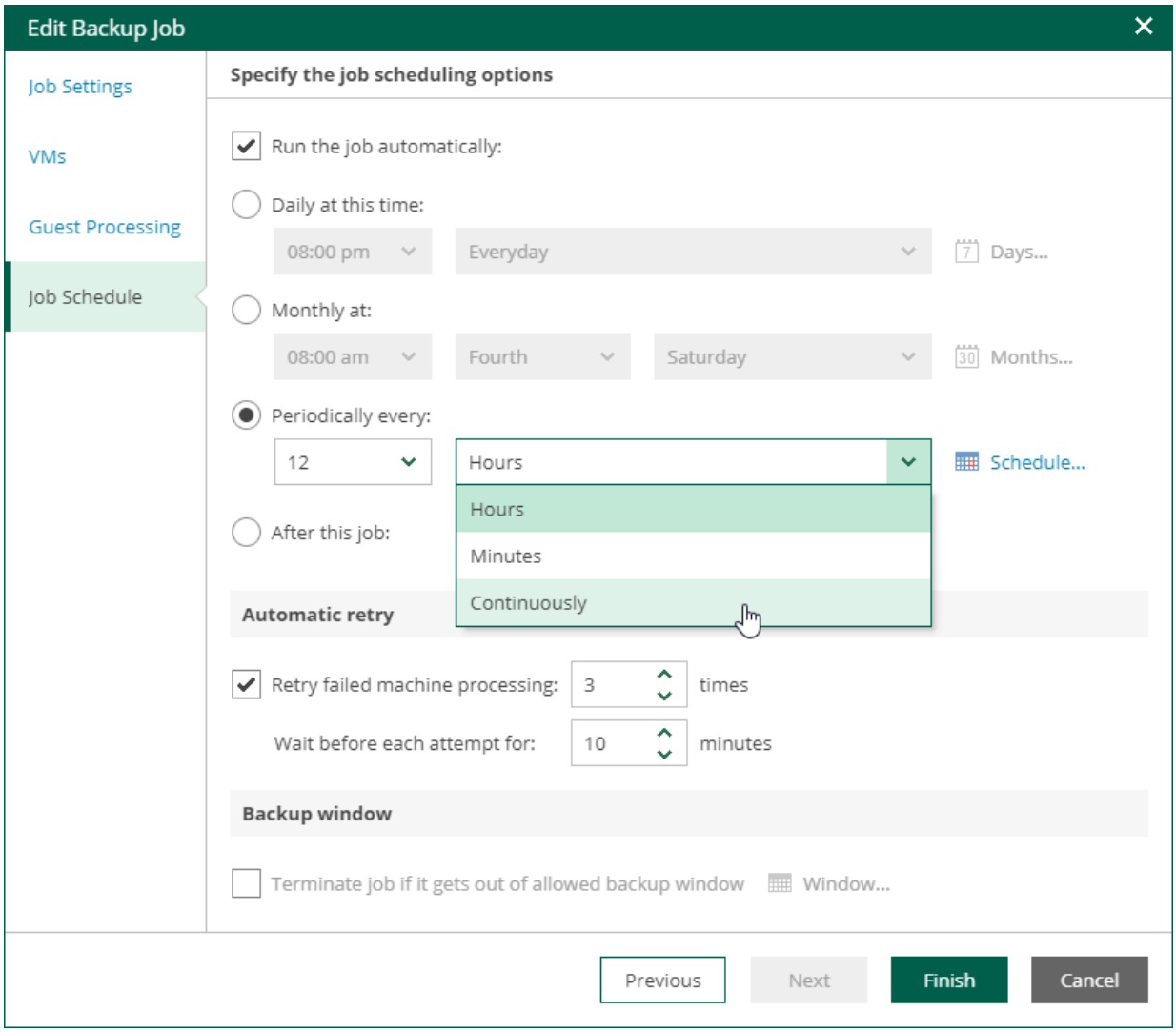
  A repeatedly run job is started by the following rules:

  - Veeam Backup & Replication always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
  - If you define permitted hours for the job, after the denied interval is over, Veeam Backup & Replication will immediately start the job and then run the job by the defined schedule.

  For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.



- To run the job continuously, select the **Periodically every** option and choose **Continuously** from the drop-down list on the right. A new backup job session will start as soon as the previous backup job session finishes.



- To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list. If you start the first job manually, Veeam Backup Enterprise Manager will display a notification. You will be able to choose whether to start the chained job as well.

> **NOTE**
>
> You can chain jobs that are processed on the same backup server only.

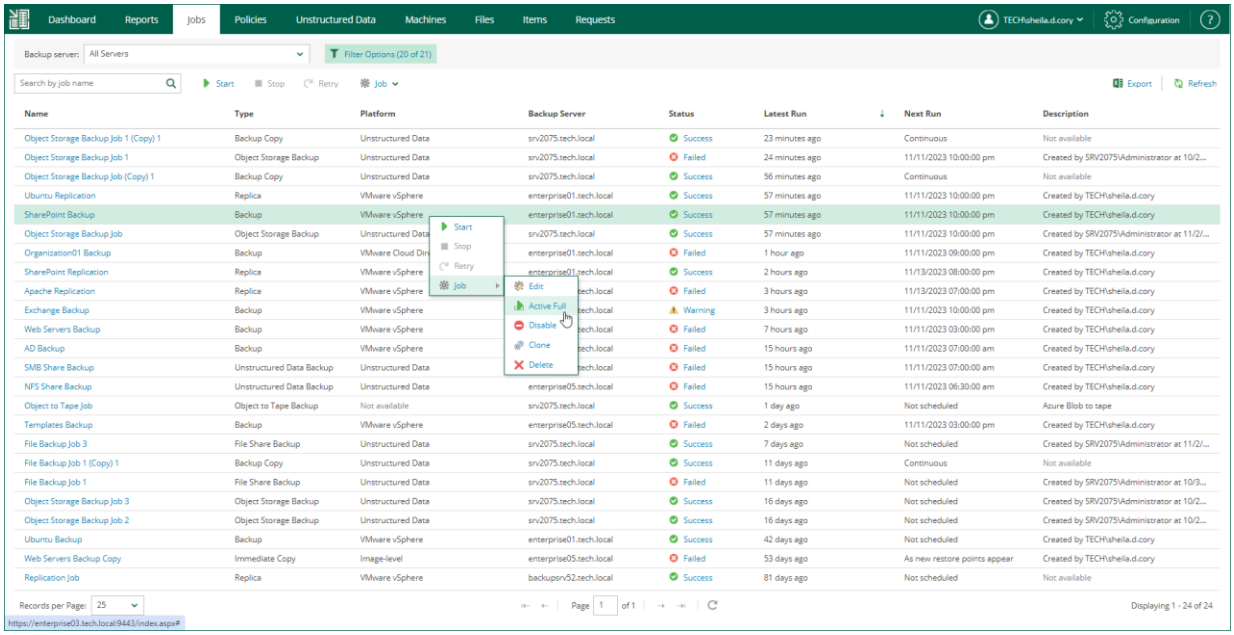
Creating Active Full Backups

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

> **NOTE**
>
> Creating active full backups is unavailable for backup copy jobs, file backup jobs and object storage backup jobs.

To perform an active full backup:

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



Cloning Jobs

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

> **NOTE**
>
> Job cloning is not available for file backup jobs and object storage backup jobs.

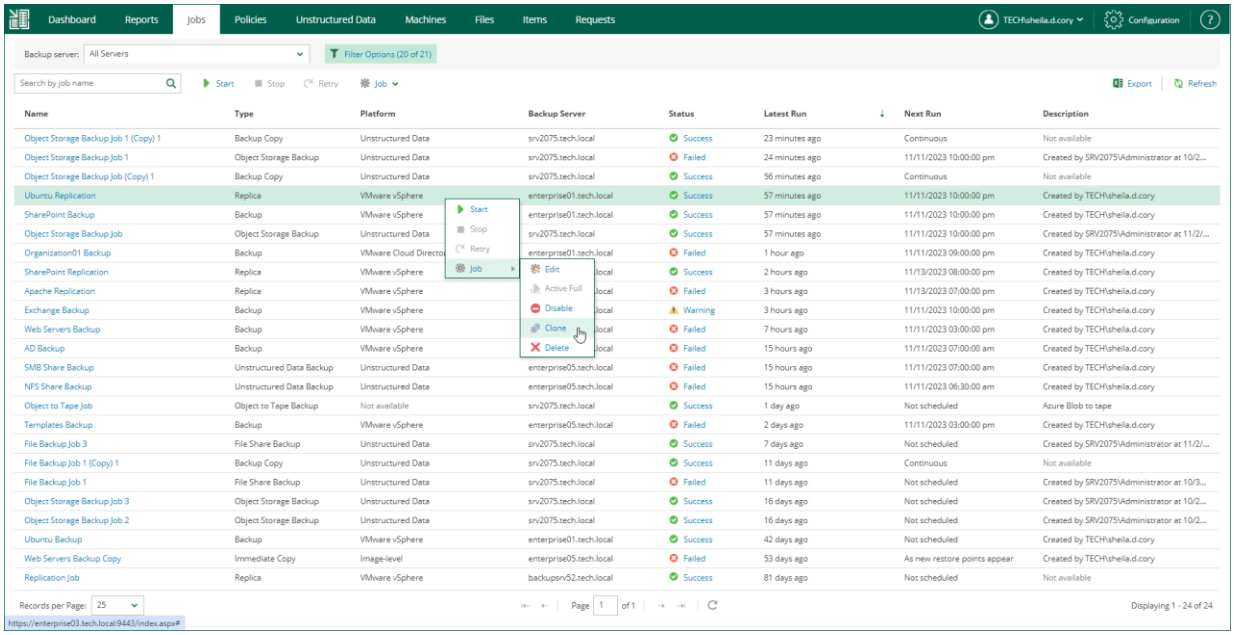
To clone an existing job, do the following:

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

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

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

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



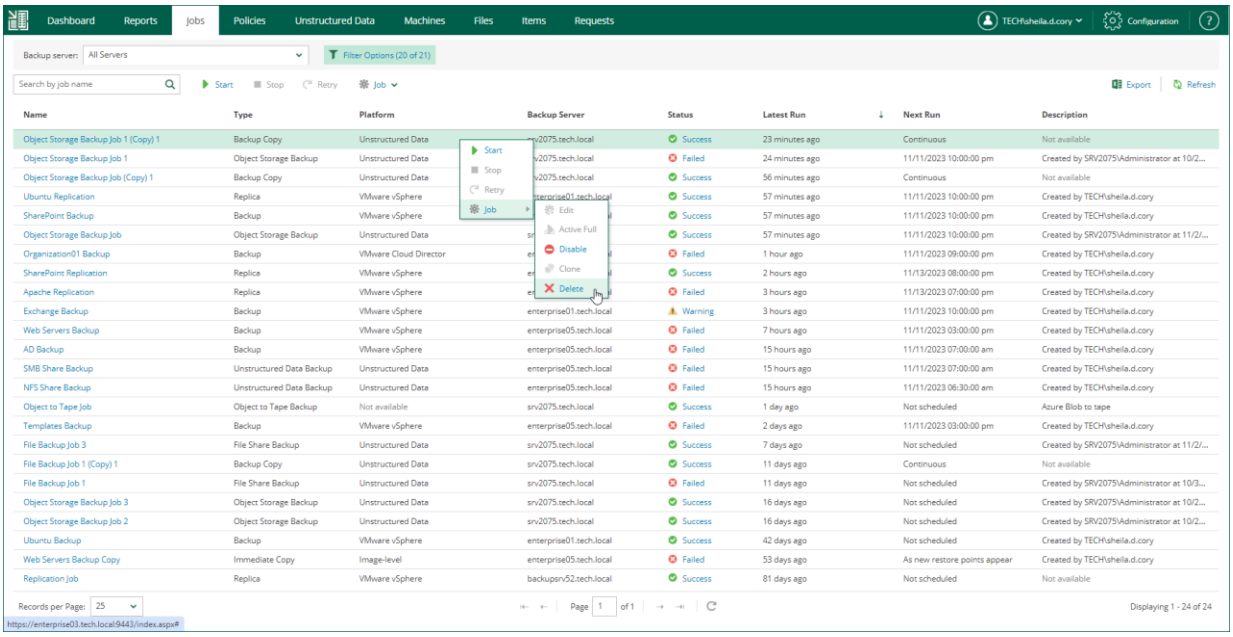
Deleting Jobs

Users with the Portal Administrator role can delete a job and also instruct Veeam Backup Enterprise Manager to delete backup files created by this job in the backup repository. Deleted jobs will no longer appear in the UI. They will be removed from the Enterprise Manager database and from the Veeam Backup configuration database on the backup server. If you select to delete backup files, they will be removed from backup repository.

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

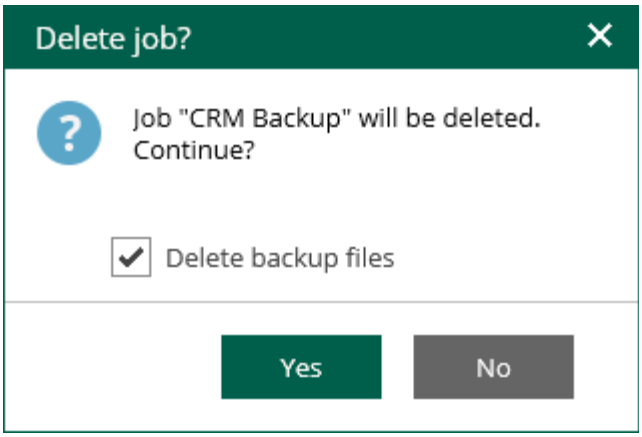
To delete a job, take the following steps:

1. On the **Jobs** tab, select the required job in the list.
2. Expand the menu commands by clicking **Job**, then select **Delete**.



3. You will be prompted to delete backup files. To delete backup files, select the **Delete backup files** check box and click **Yes** to confirm the operation.

   If four-eyes authorization is enabled on the backup server, backup files will remain in the backup repository and become orphaned.



Managing CDP Policies

Veeam Backup Enterprise Manager allows you to manage CDP policies that were previously created on added backup servers. Veeam Backup Enterprise Manager displays CDP policies that process VMware vSphere or VMware Cloud Director objects.

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

For more information on CDP, see the Continuous Data Protection (CDP) section of the Veeam Backup & Replication User Guide.

In This Section

- Viewing Policies
- Enabling and Disabling Policies
- Editing Policies
- Deleting Policies

Viewing Policies

From Veeam Backup Enterprise Manager, you can view information about all CDP policies from all backup servers added to Enterprise Manager. To view CDP policies, open the **Policies** tab.

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

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

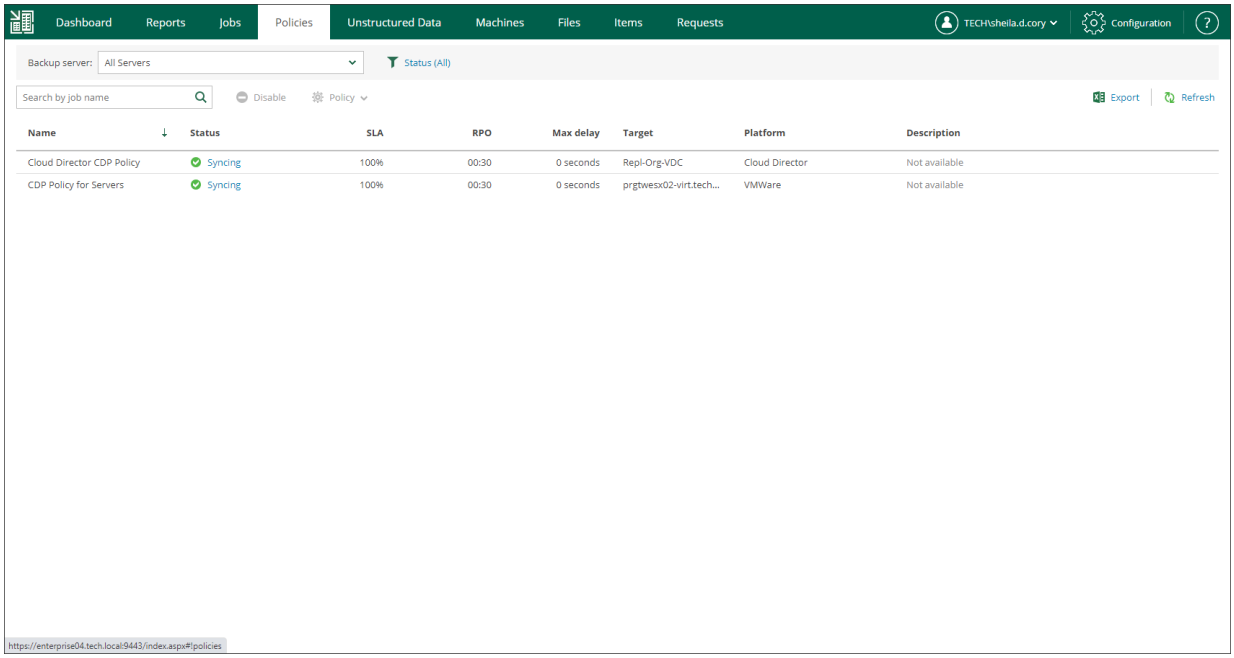
To quickly find a CDP policy, you can use filters and the search field.

- To filter the list of policies:
  - Use the **Backup server** list to view the policies of the selected backup server only.
  - Use the **Status** filter to view the policies with the selected statuses only.

    Once you have selected necessary statuses, click the **Apply** button to apply the filter.
- To find a policy by its name, use the search field.

In addition to the information presented in the list of policies, the **Policies** tab allows you to view advanced policy data. To see detailed policy statistics, click the state link in the **Status** column.

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

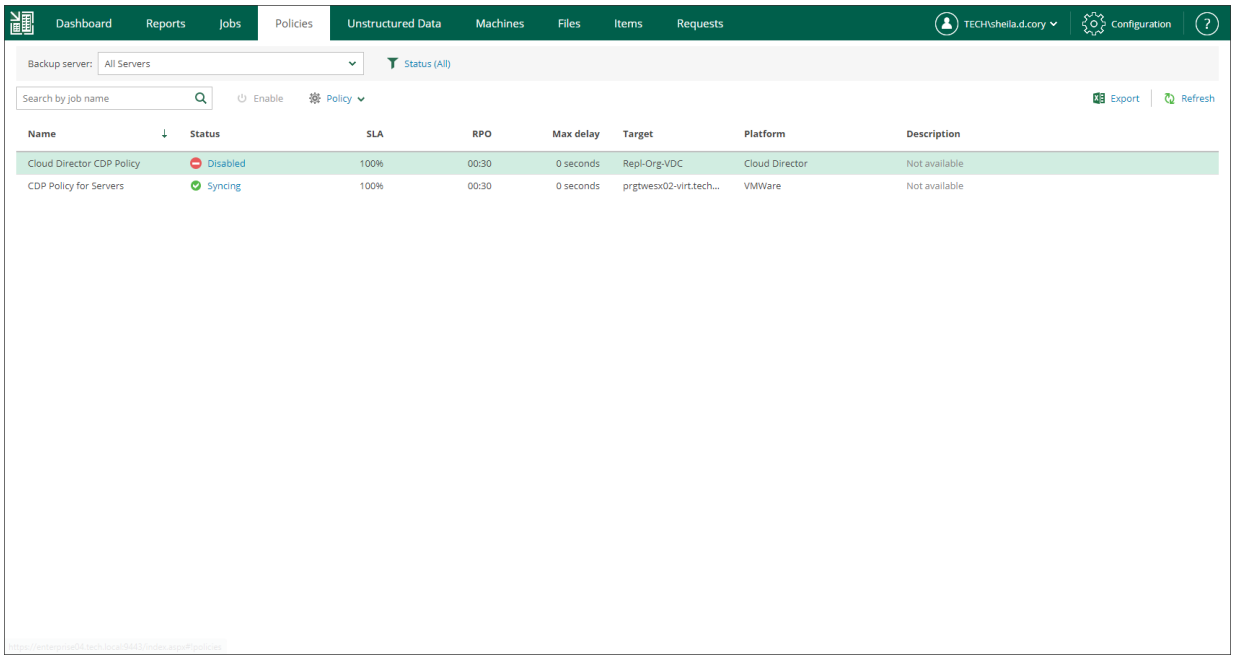

Dashboard
Reports
Jobs
Policies
Unstructured Data
Machines
Files
Items
Requests
TECH\sheila.d.cory
Configuration
Backup server:
All Servers
Status (All)
Search by job name
Disable
Policy
Export
Refresh
Name
Status
SLA
RPO
Max delay
Target
Platform
Description
Cloud Director CDP Policy
Syncing
100%
00:30
0 seconds
Repl-Org-VDC
Cloud Director
Not available
CDP Policy for Servers
Syncing
100%
00:30
0 seconds
prgtwesx02-virt.tech...
VMWare
Not available
https://enterprise04.tech.local:9443/index.aspx#!policies

Enabling and Disabling Policies

Users with the Portal Administrator role can enable and disable CDP policies. Disabled CDP policies are temporary paused.

To enable or disable a policy:

1. On the **Policies** tab, select a policy from the list.
2. On the toolbar, click **Enable** or **Disable**.



Editing Policies

If Veeam Backup Enterprise Manager has an Enterprise or Enterprise Plus license installed, users with the Portal Administrator role can modify settings of CDP policies that have been previously configured on added backup servers . In Veeam Backup Enterprise Manager, you can change only a subset of the CDP policy settings. You can configure other policy settings with the Veeam Backup & Replication console only.

You can edit the following CDP policy settings:

- Policy name and description
- List of VMs that the policy processes
- Policy schedule
- Guest processing settings

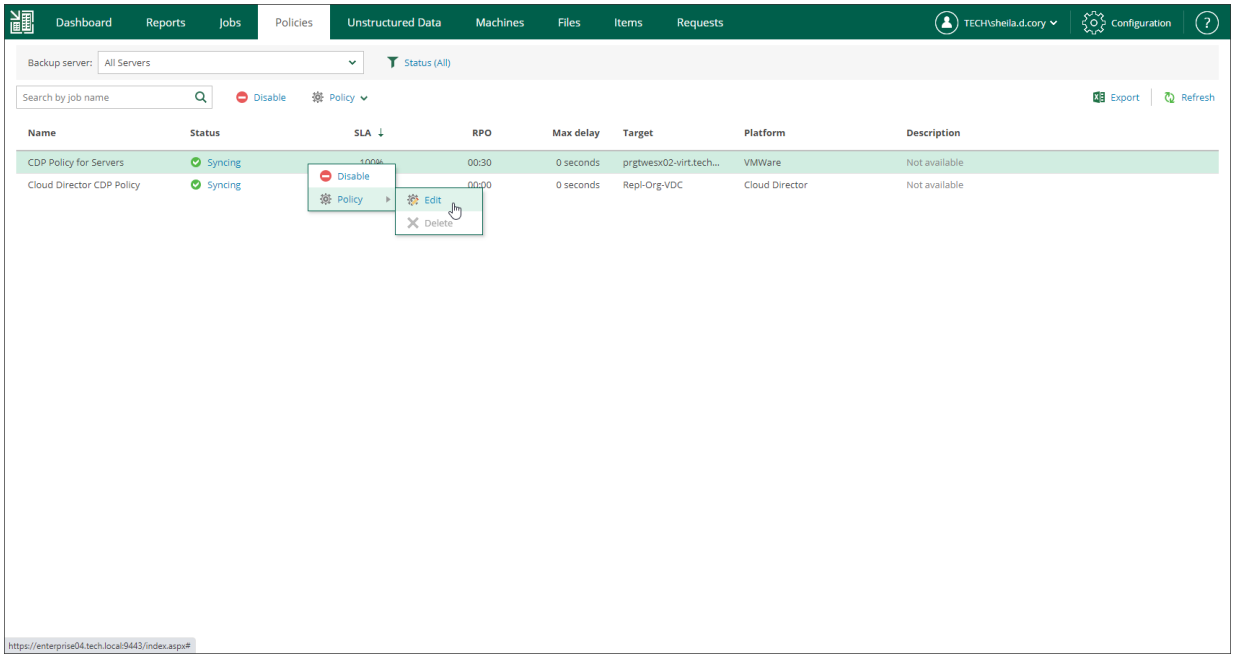
To edit a CDP policy, use the **Edit Policy** wizard.

1. Launch the Edit Policy wizard.
2. Edit the policy name and description.
3. Edit the list of VMs.
4. Configure RPO and retention settings.
5. Configure guest processing settings.

Step 1. Launch Edit Policy Wizard

To launch the **Edit Policy** wizard:

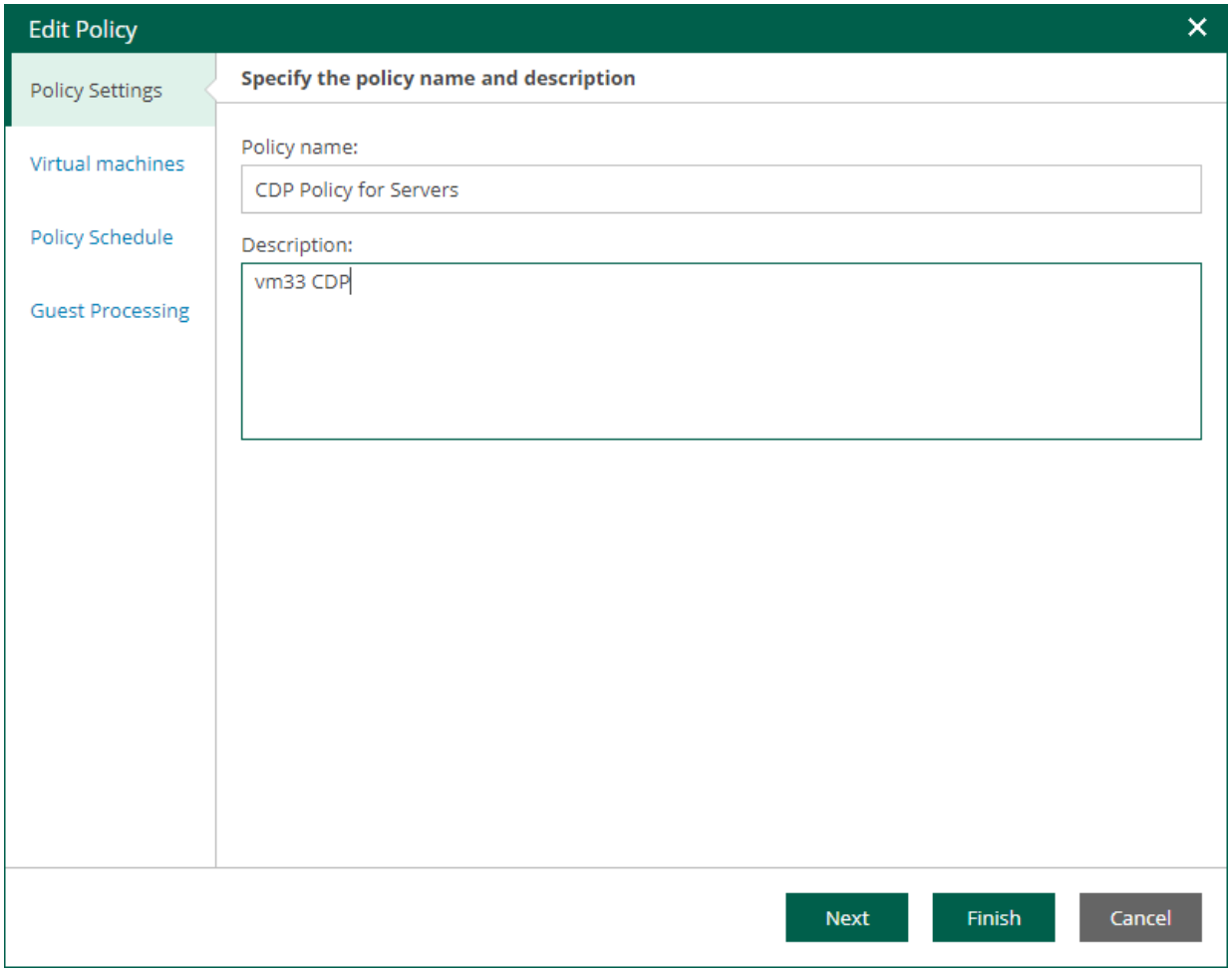
1. Open the **Policies** tab and select the necessary policy from the list.
2. On the toolbar, click **Policy** and select **Edit**.



Step 2. Edit Policy Name and Description

At the **Policy Settings** step of the wizard, you can modify the name and description of the selected CDP policy:

1. In the **Policy name** field, specify a name for the policy.
2. In the **Description** field, provide an optional description for future reference.



Step 3. Edit List of VMs

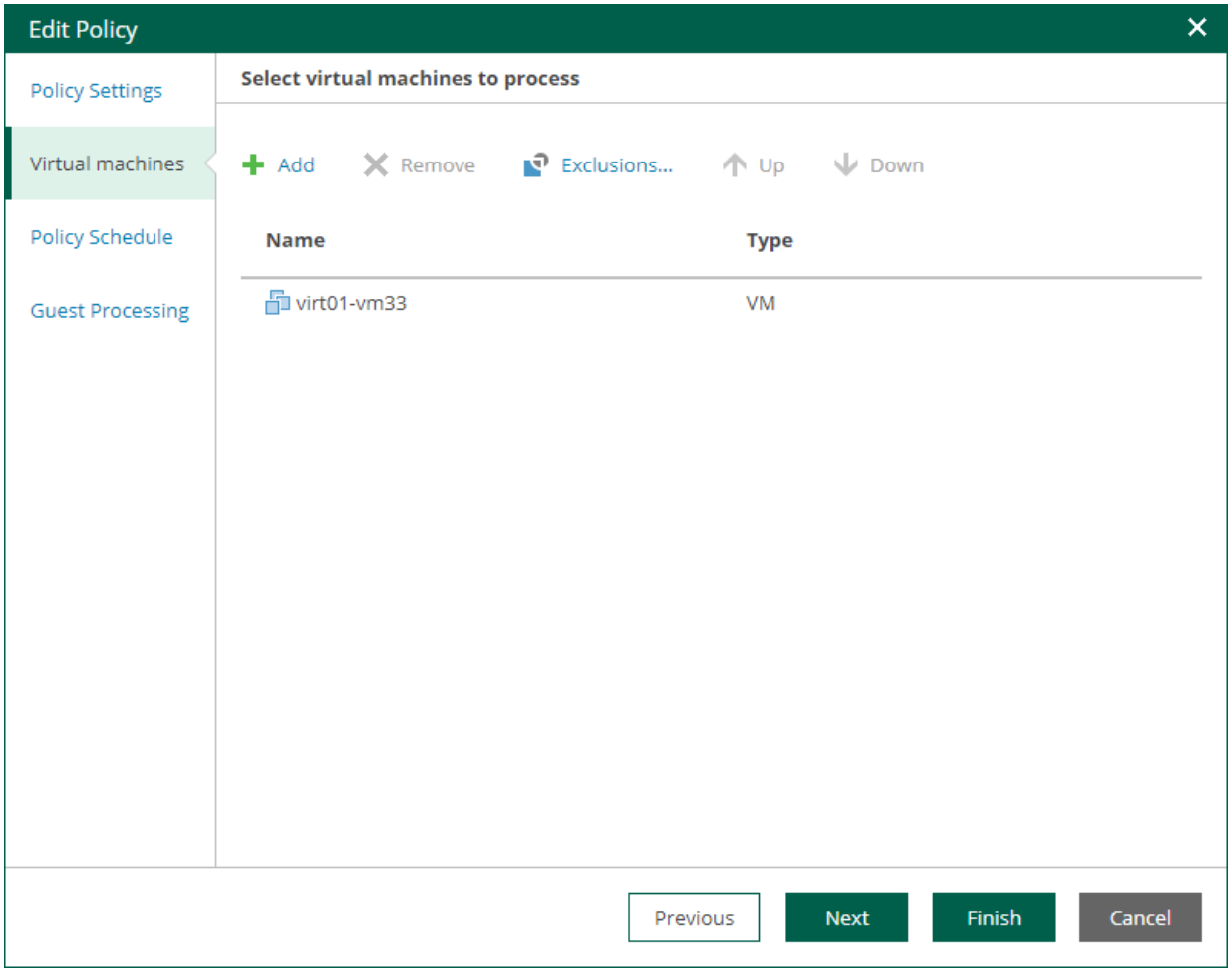
At the **Virtual Machines** step of the wizard, you can add or remove individual VMs or VM containers (for example, hosts or folders). You can also exclude individual VMs from VM containers, for example, if you need to replicate an entire VMware vSphere server except some machines running on this server.

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

Adding VMs and VM containers

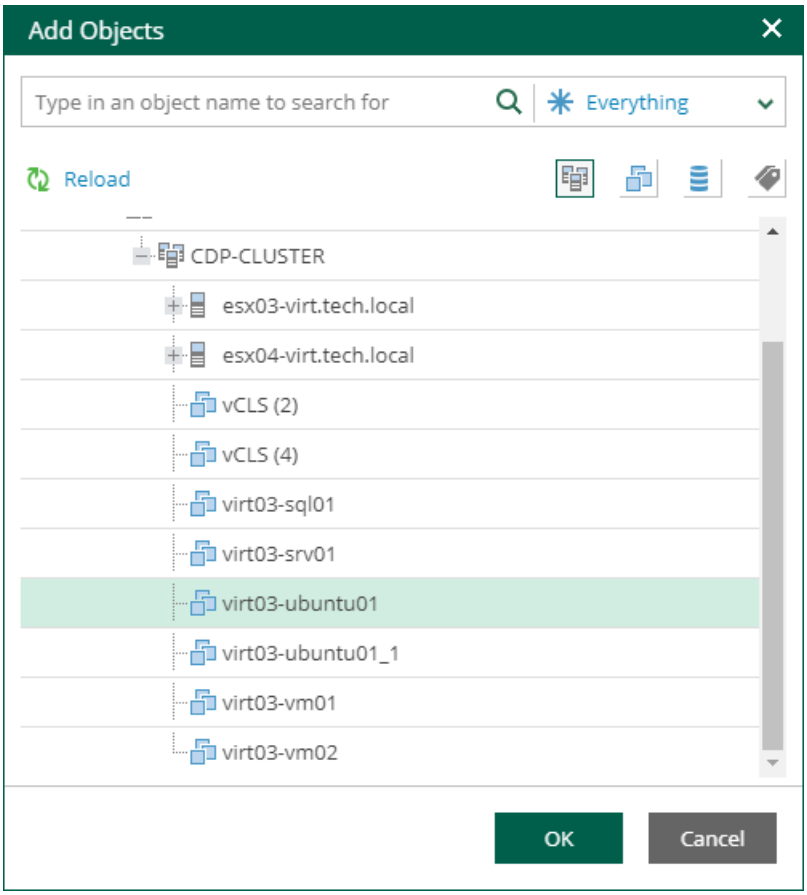
To add a VM or VM container:

1. Click **Add**.



2. In the virtual infrastructure tree, select the necessary VMs or VM containers.

   If you select a VM container and later add a new VM to the container, Veeam Backup & Replication will update policy settings automatically to include the VM.



> **TIP**
>
> To quickly find the necessary objects, you can do the following:
>
> - Search for objects: type a name or part of a name in the search field. Specify the type of the object from a scroll list next to the search field.
> - Switch between virtual infrastructure views using the buttons in the upper-right corner: **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** and **Tags and VMs**.

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

Removing VMs and VM containers

To remove a VM or VM container, select it in the list and click **Remove**.

Excluding VMs from VM containers

To exclude VMs from a VM container:

1. Select a VM container in the list and click **Exclusions**.
2. In the **Exclusions** window, click **Add** and select machines that you want to exclude.

Changing Object Processing Order

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

To change the processing order, select the necessary objects and move them up or down the list using the **Up** and **Down** buttons on the right.

NOTE

- VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, add them as standalone VMs, not as a part of containers.
- The processing order may differ from the order that you have defined. For example, if resources of a VM that is higher in the priority are not available, and resources of a VM that is lower in the priority are available, the VM with the lower priority will be processed first.

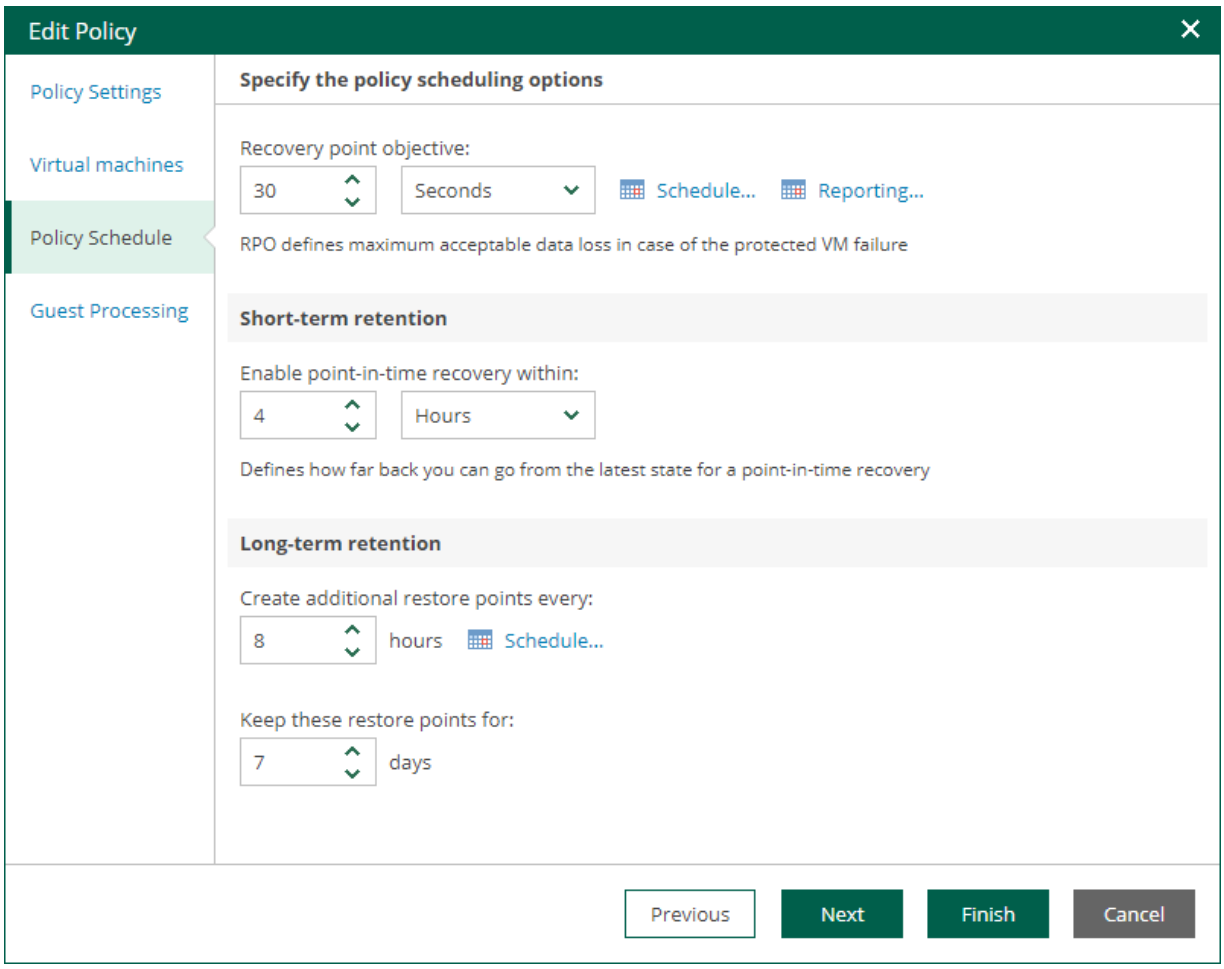
Step 4. Edit Policy Schedule

At the **Policy Schedule** step of the wizard, you can edit schedule and retention settings:

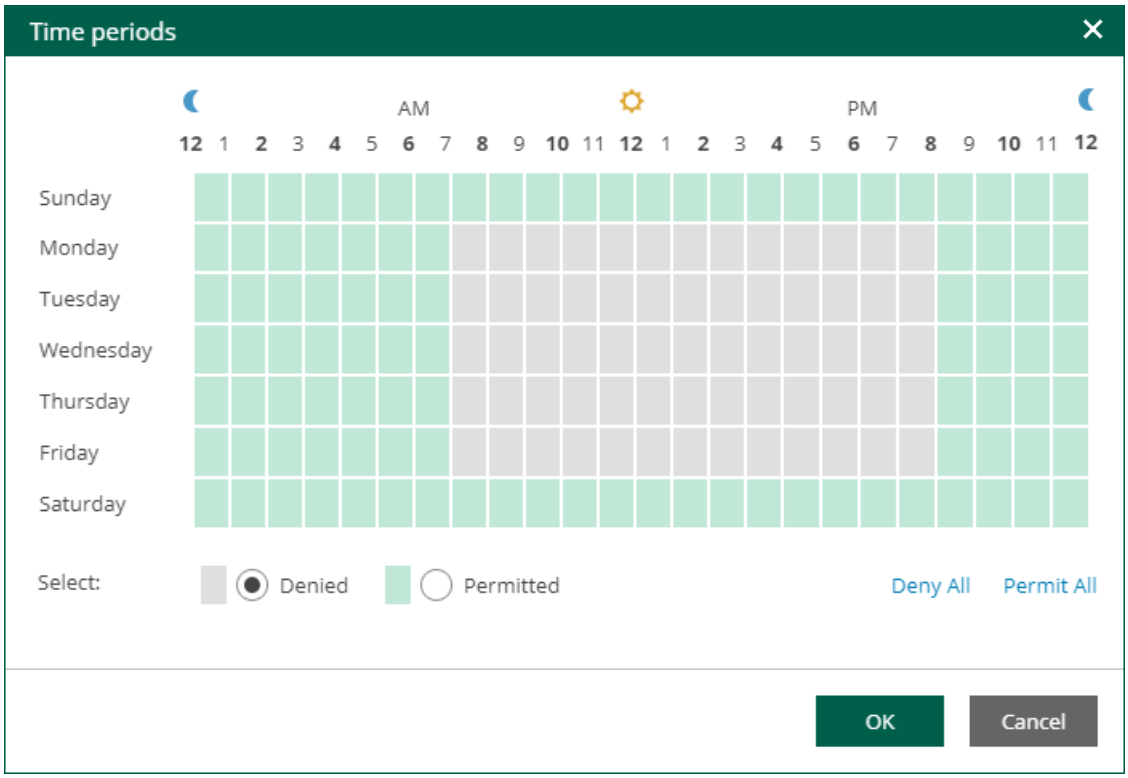
1. Configure scheduling settings:

   a. In the **Recovery point objective** section, specify an RPO in seconds or minutes. You can select the period from 2 seconds to 60 minutes.

   During every specified period, Veeam Backup & Replication will create short-term restore points for VM replicas and send these restore points to the target destination. Note that short-term restore points are crash-consistent.



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



2. To instruct the CDP policy to display a warning or error if a newly created replicated states are not transferred to the target within the set RPO, click **Reporting**. Then specify when the policy must display errors and warnings.

   If you have configured email notification settings, Veeam Backup & Replication will mark the policy with the *Warning* or *Error* status and will also send email notifications.

3. In the **Short-term retention** section, specify how long you want to store a short-term restore point. The maximum value is 7 days. Note that the total size of the log files that store incremental changes is a maximum of 2 TB per VM disk.

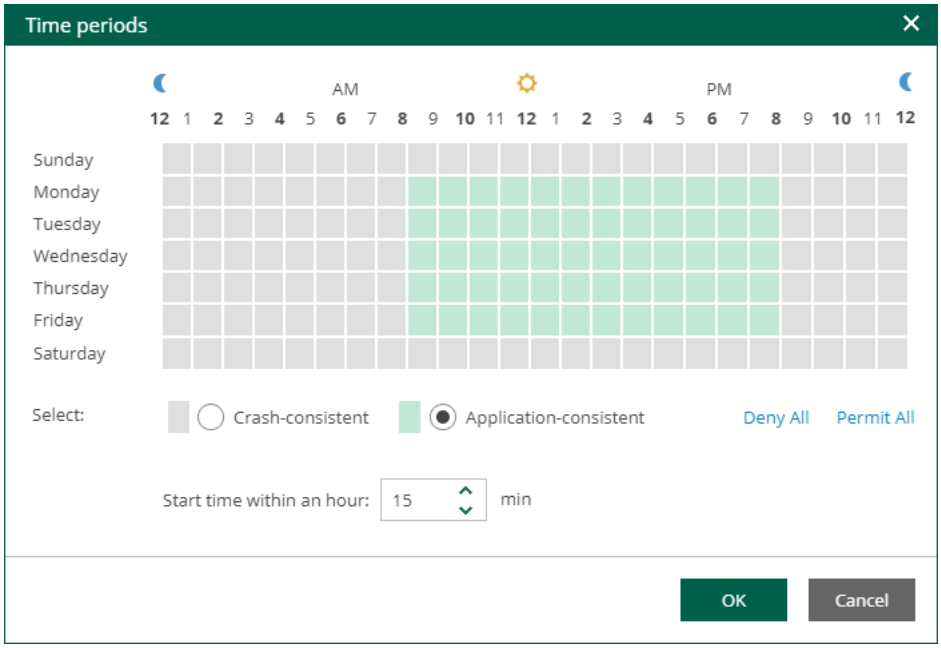
4. In the **Long-term retention** section, configure when to create long-term restore points and for how long to store them:

   a. In the **Create additional restore points every** field, specify how often you want to create long-term restore points.

   b. In the **Keep restore points for** field, specify for how long to store these long-term restore points.

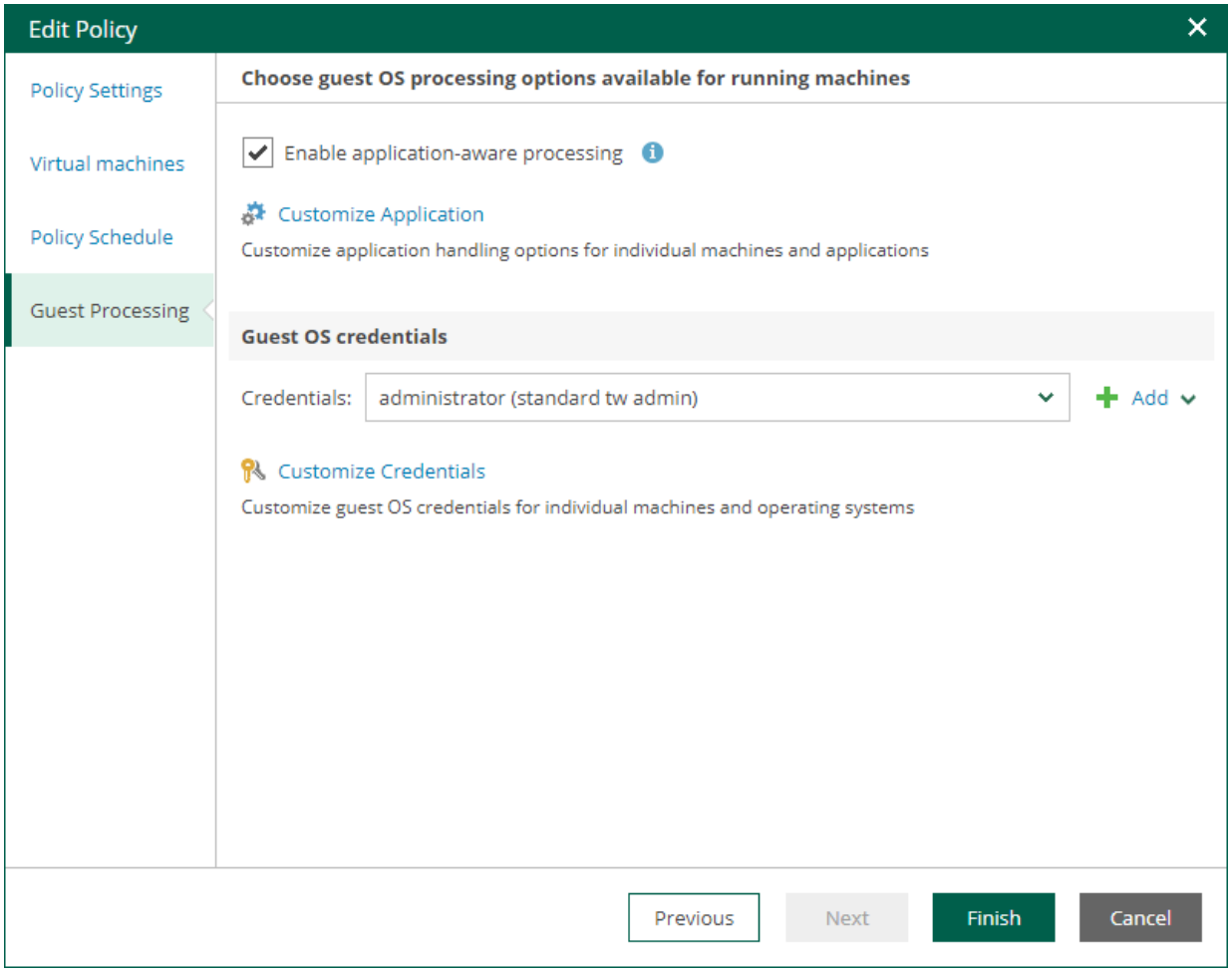
c. To specify time periods when Veeam Backup & Replication must create application-consistent and crash-consistent long-term restore points, click **VSS**. In the **Time periods** window, select the necessary time area and click **Crash-consistent** or **Application-consistent**. By default, Veeam Backup & Replication creates application-consistent backups if you enable application-aware processing. If you do not enable application-aware processing, Veeam Backup & Replication will create crash-consistent long-term restore points.

   To shift the schedule, specify the offset in the **Start time within an hour** field. For example, you schedule creation of crash-consistent restore points from 00:00 to 01:00, and set the offset value to 25. The schedule will be shifted forward, and the crash-consistent restore points will be created from 0:25 and to 01:25.



Step 5. Configure Guest Processing Settings

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



In This Section

- Application-Aware Processing
- Guest OS Credentials

Application-Aware Processing

If VMs run Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, or Oracle, you can enable application-aware processing to create transactionally consistent replicas. The transactionally consistent replicas guarantee proper recovery of applications without data loss.

To configure application-aware processing:

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

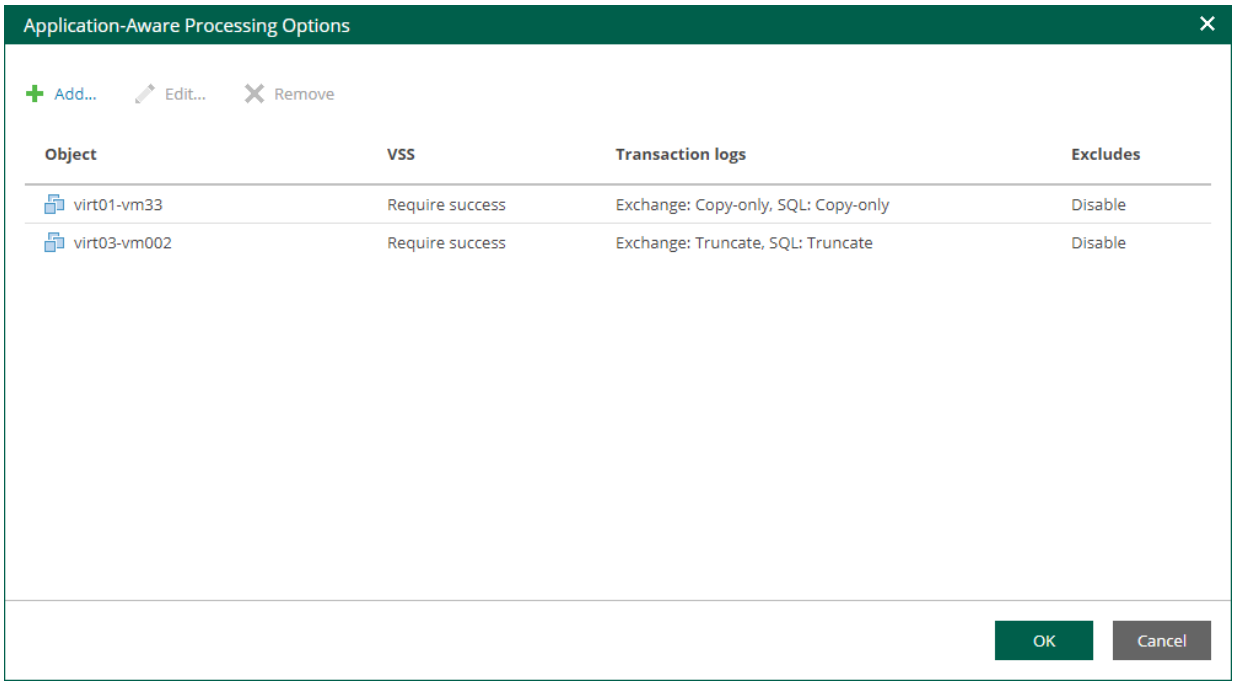
3. To define custom settings for a machine in the list, select it and click **Edit**.

   Consider the following:

   - To customize settings of a machine added as part of a container, add the machine as a standalone instance. For that, click **Add machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
   - To discard custom settings of a machine, select the machine in the list and click **Remove**.

4. Configure the necessary settings for the selected application server:

   - General Settings
   - Microsoft SQL Server Transaction Log Settings
   - Oracle Archived Log Settings



General Settings

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

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

   - Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the CDP replication if an error occurs.
   - Select **Try application processing, but ignore failures** if you want to continue the CDP replication even if an error occurs. This option guarantees the CDP policy will continue working. The created replica will not be transactionally consistent, but rather crash consistent.
   - Select **Disable application processing** if you do not want to enable application-aware processing for the VM. This option makes the **Transaction Logs Processing** section unavailable.

2. [For Microsoft Exchange, Microsoft SQL Server, and Oracle] In the **Microsoft VSS** section, specify whether this CDP policy should process transaction logs or create copy-only replicas.

   - Select **Process transaction logs with this job** if you want Veeam Backup & Replication to process transaction logs.

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

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

     - For Microsoft SQL Server transaction log processing — on the **SQL** tab. For more information, see Microsoft SQL Server Transaction Log Settings.
     - For Oracle database archived logs processing — on the **Oracle** tab. For more information, see Oracle Archived Log Settings.

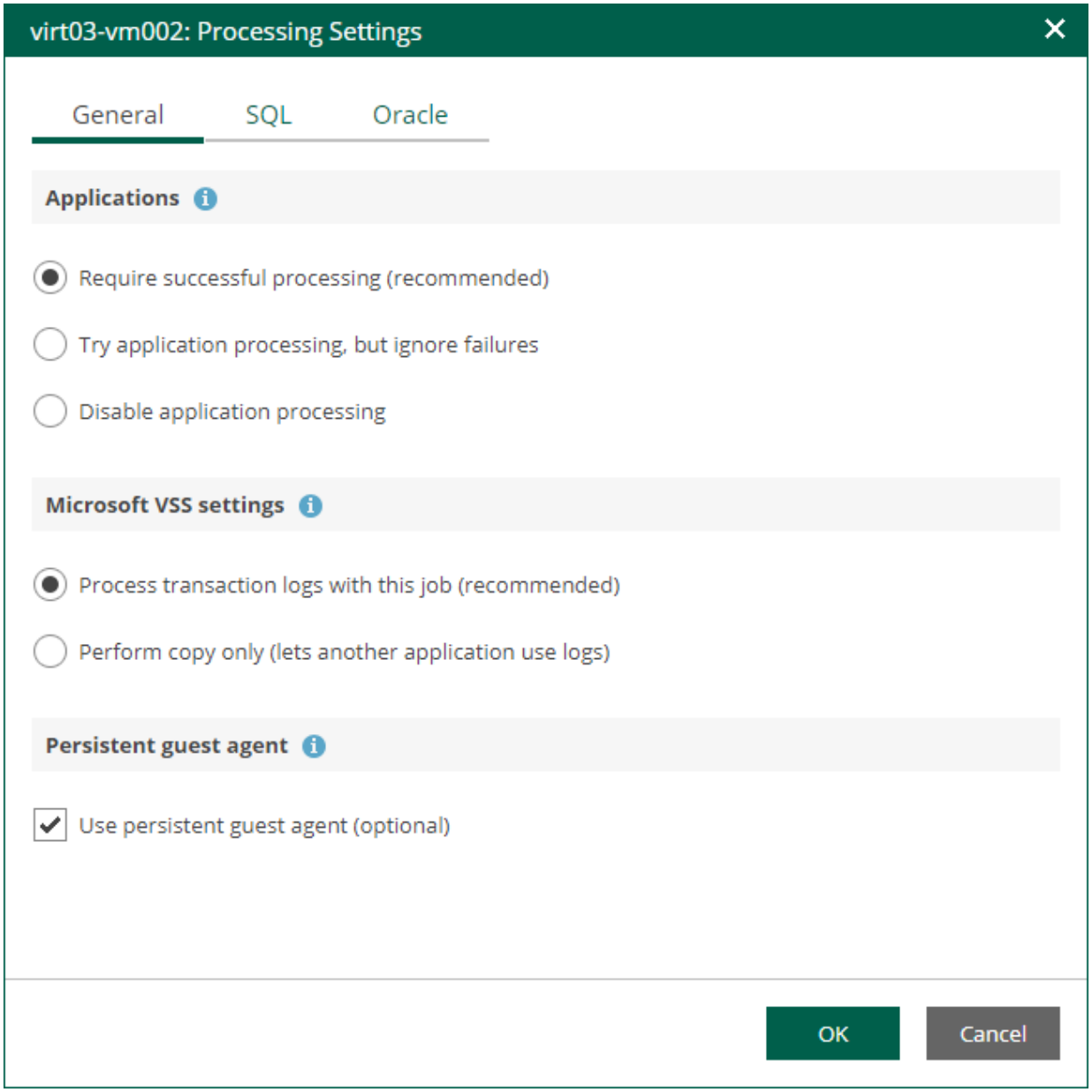
   - Select **Perform copy only** if you use another replication tool to perform guest level replication, and this tool maintains consistency of the database state. Veeam Backup & Replication will create a copy-only replica for the selected VM. The copy-only replica preserves the chain of full and differential backup files and transaction logs on the VM. For more information, see Microsoft Docs.

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

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

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

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

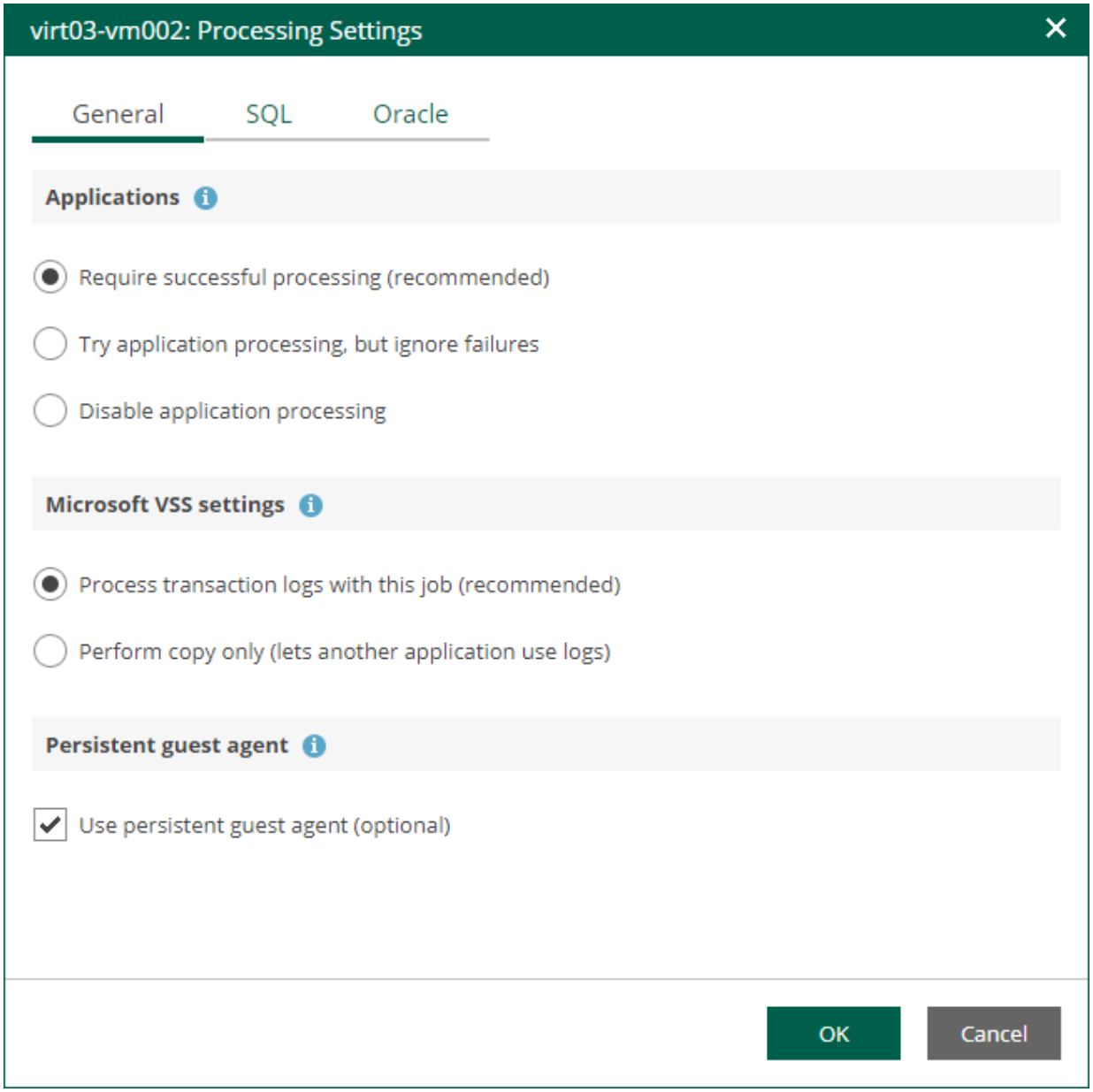


Microsoft SQL Server Transaction Log Settings

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

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

- In the **Transaction logs processing** section, the **Process transaction logs with this job** option must be selected.

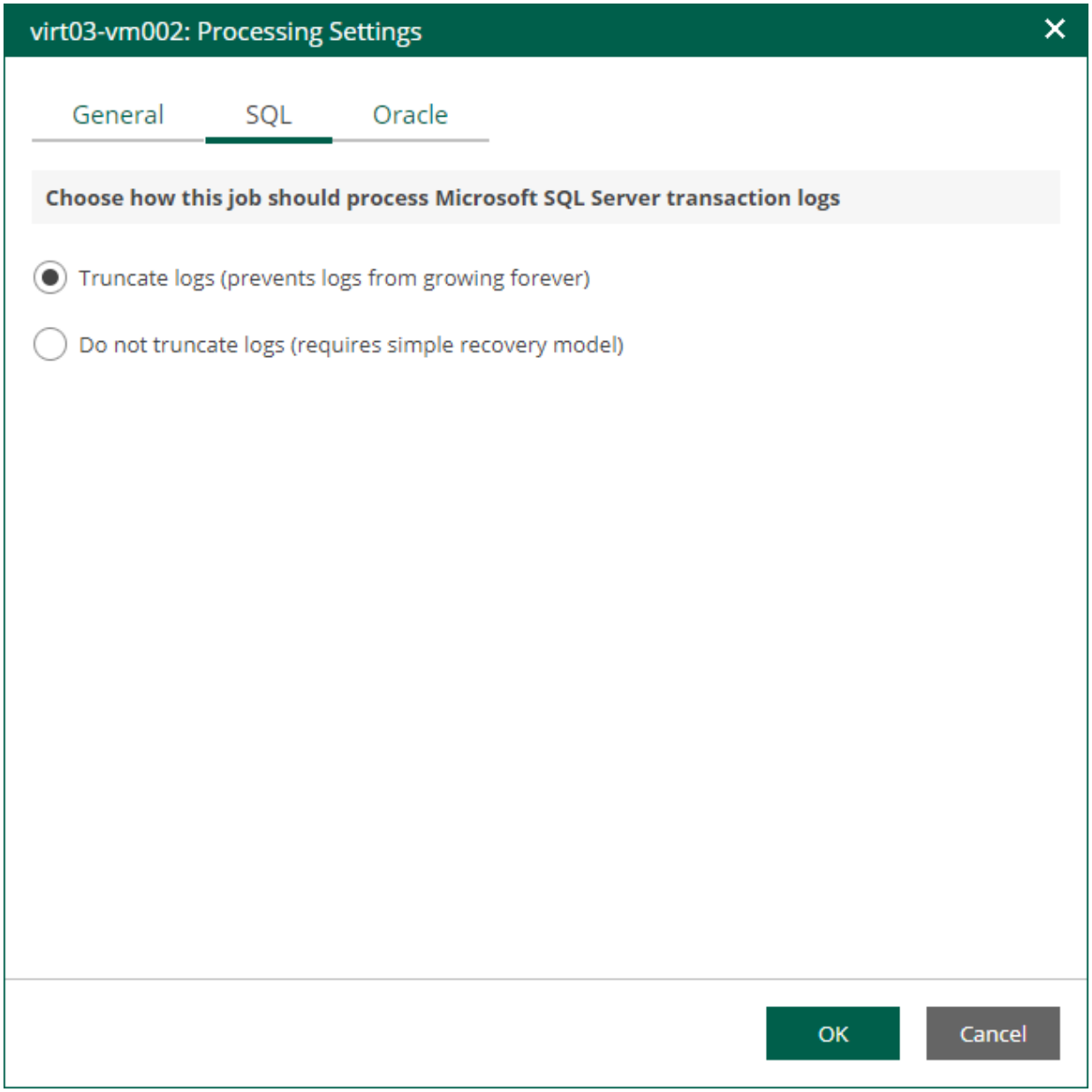


5. Open the **SQL** tab of the **VM Processing Settings** window.
6. Specify how Veeam Backup & Replication will process Microsoft SQL Server transaction logs.
   - Select **Truncate logs** to truncate transaction logs after the CDP policy creates a long-term restore point.

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

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

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

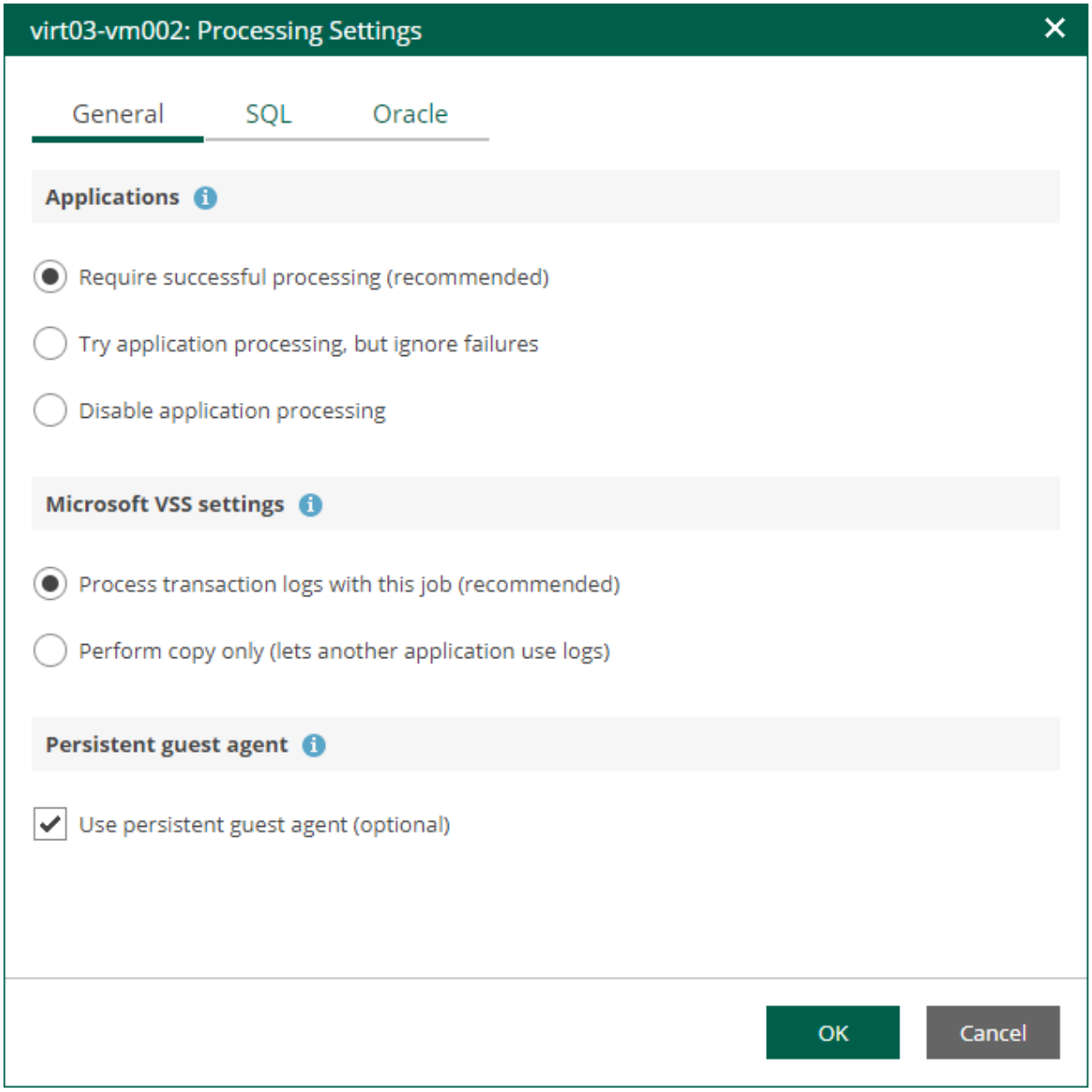


Oracle Archived Log Settings

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

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

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



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

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

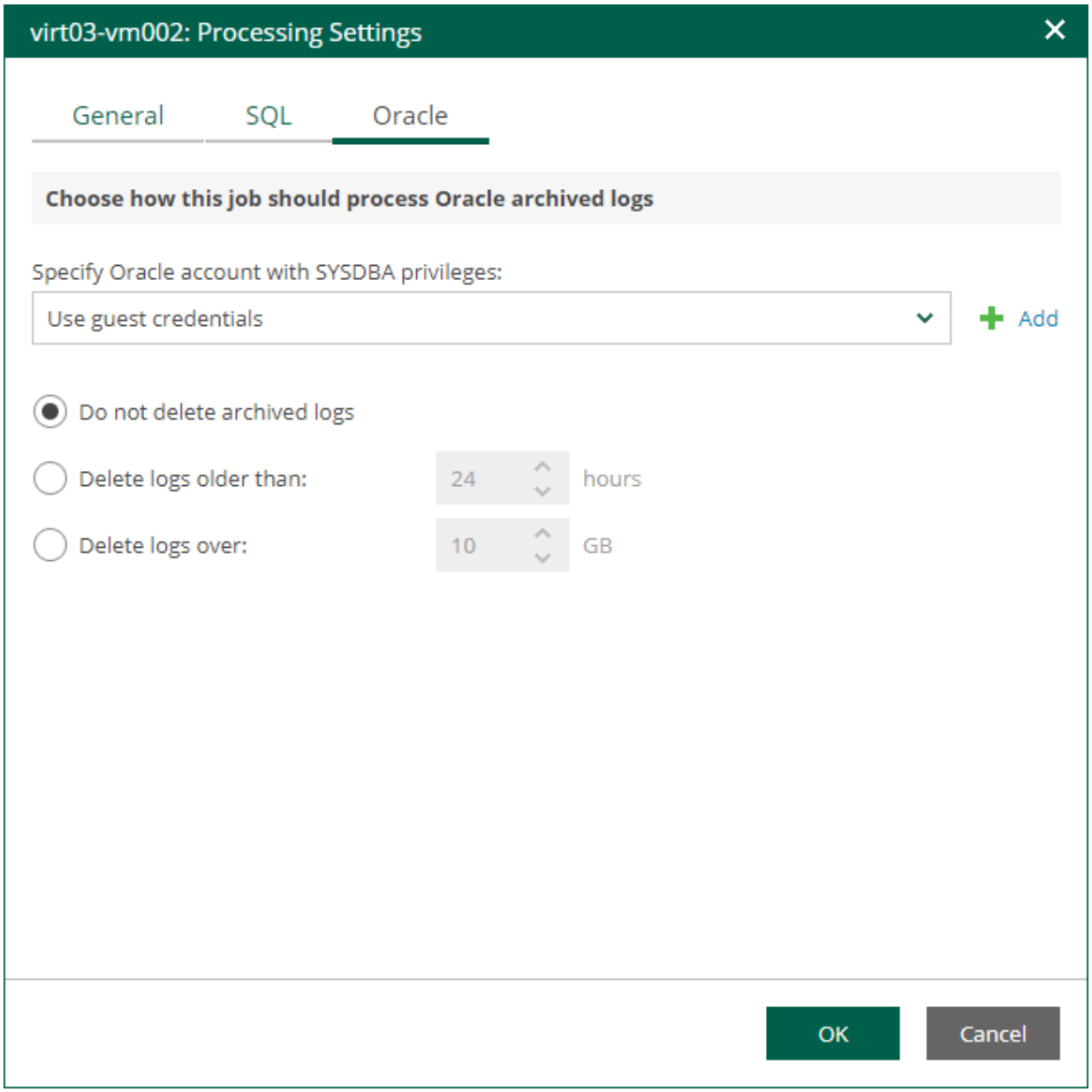
b. Specify how Veeam Backup & Replication must process archived redo logs on the Oracle VM.

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

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

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

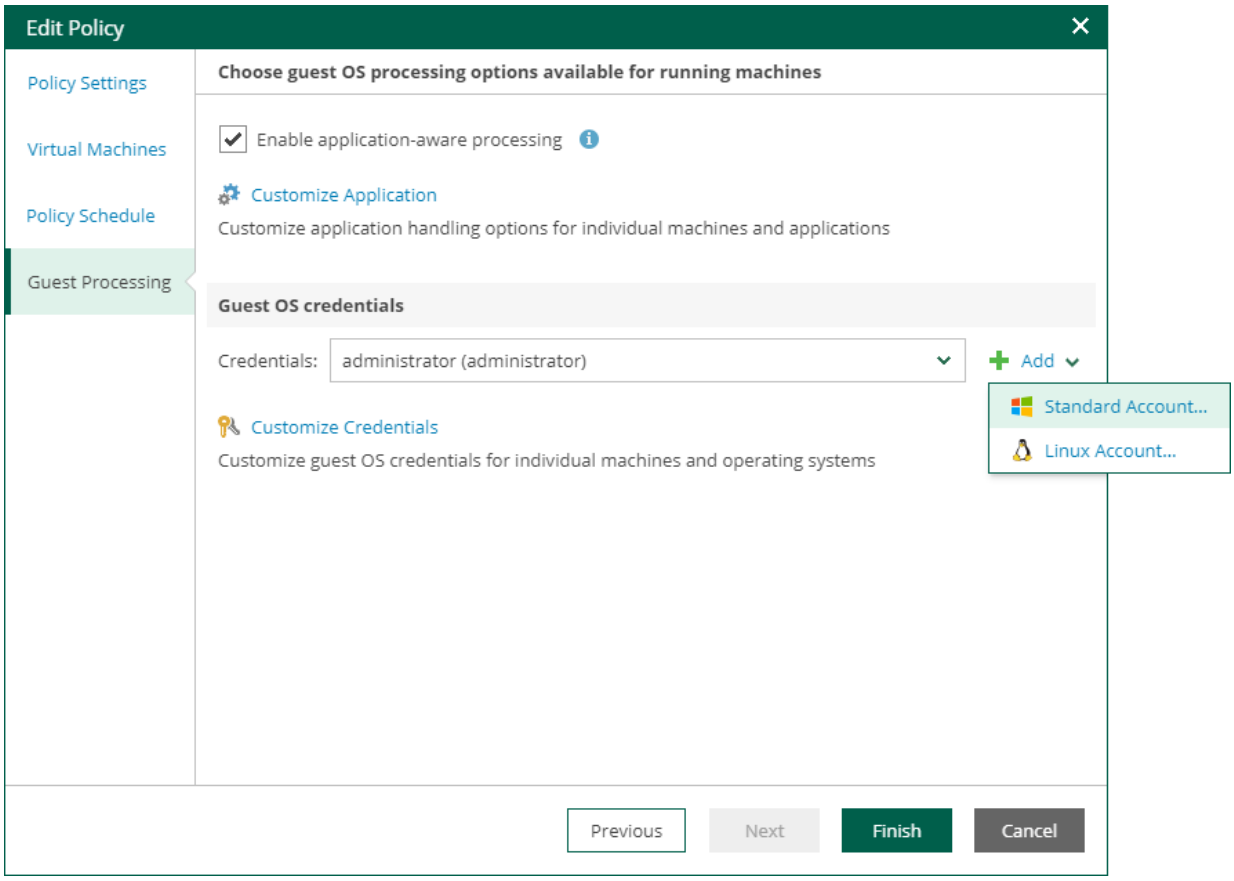
Transaction logs will be deleted using Oracle Call Interface after the CDP policy creates a long-term restore point. If the creation fails, the logs will remain untouched until the next start of the long-term restore point creation.



Guest OS Credentials

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

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



In the **Guest OS credentials** section, you can select credentials from the list, or click the **Add** button to add new credentials.

- For Windows guest OS, specify a user account (name and password) with local administrative rights on target machine, and optional description. Credentials must be specified in the following format:
  - For Active Directory accounts: *DOMAIN|Username*
  - For local accounts: Username or *HOST|Username*
- For Linux guest OS, you can choose one of the following options:
  - If Management Agent is installed on the VM, you can select the **Use management agent** option.
  - If Management Agent is not installed on the VM, specify a user name, password, and SSH port (by default, port 22 is used).

    If you specify data for a non-root account that does not have root privileges on a Linux server, you can use the **Non-root account** section to grant this account elevated permissions as follows:

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

ii. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the root account password.

If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

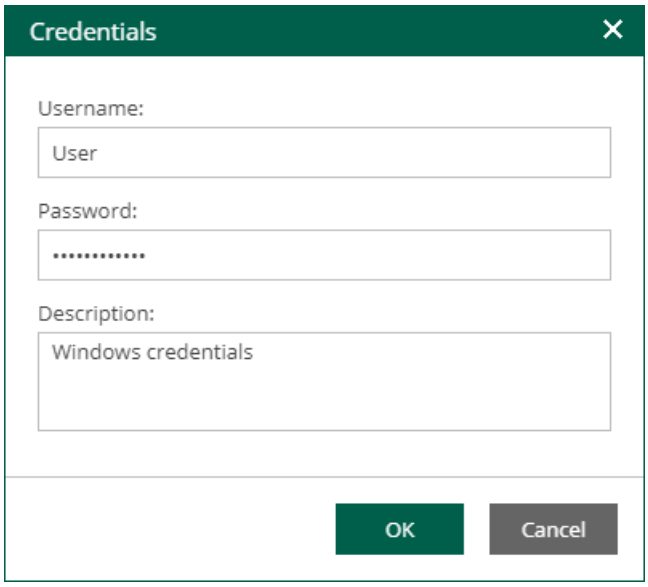
iii. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the root account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

Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

IMPORTANT

For machine guest OS indexing of Linux-based machines, a user account with root privileges on the machine is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based machine, grant root privileges to this account and specify settings of this account in the **Guest OS credentials** section.

It is also recommended to avoid additional commands output for the specified user (like messages echoed from within `~/.bashrc` or command traces before execution), because they may affect Linux machine processing.



Linux Private Key

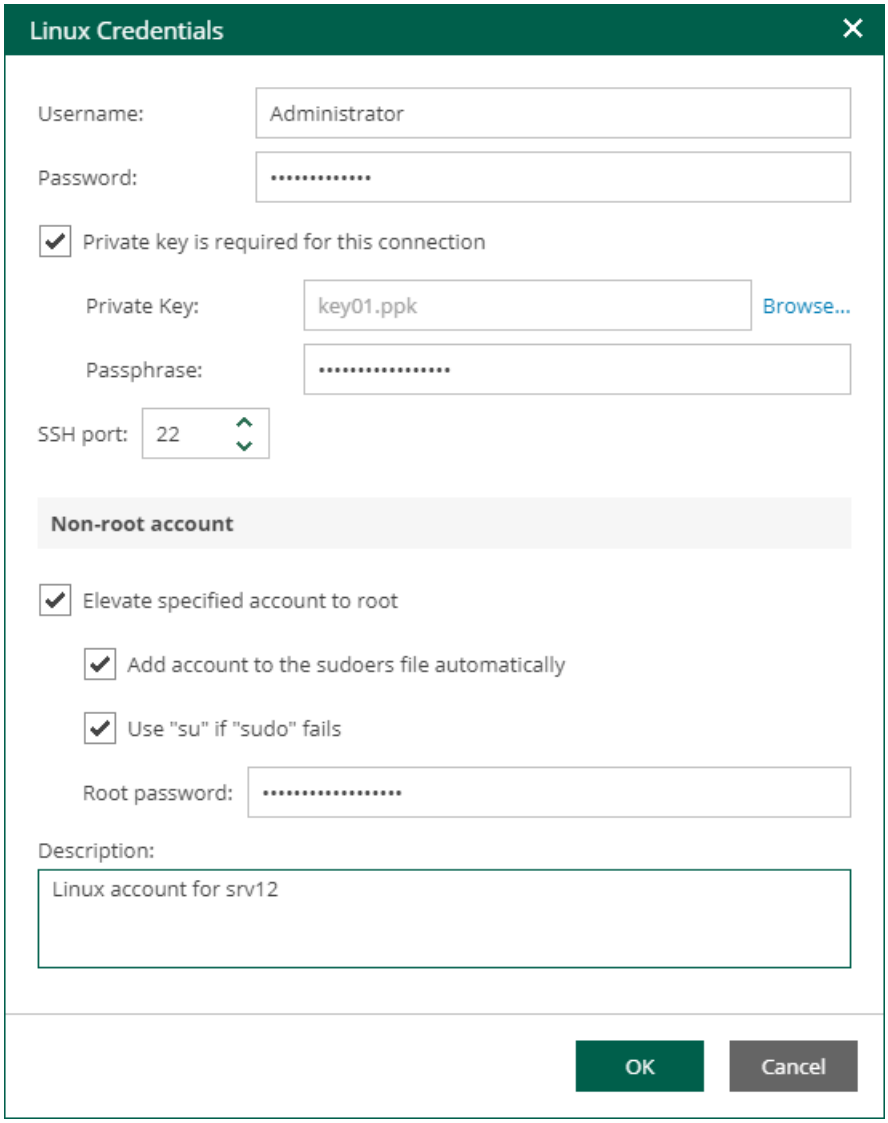
Another option is to use Linux private key. This method eliminates the need to supply password at each login, helps to protect against malicious applications like keyloggers, thus strengthening security, and simplifies launch of automated tasks, decreasing administrative load in Linux environments. For this method, a user must create a pair of keys:

- *Private key* is stored on the client (user's) machine — that is, on the machine where Veeam Backup & Replication runs. The key is usually stored in the encrypted form. To decrypt a private key, you need to supply a passphrase specified at key creation.

- *Public key* is stored on the server (Linux machine) in a special `authorized_keys` file that contains a list of public keys.

If you plan to use Linux private key for authentication, make sure you have created private and public keys and stored them appropriately: private key on the client side (Veeam backup server) and public key on the server side (Linux machine). You should also have the passphrase for the private key if it is encrypted. If you select to use Linux private key credentials, you should specify the following:

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

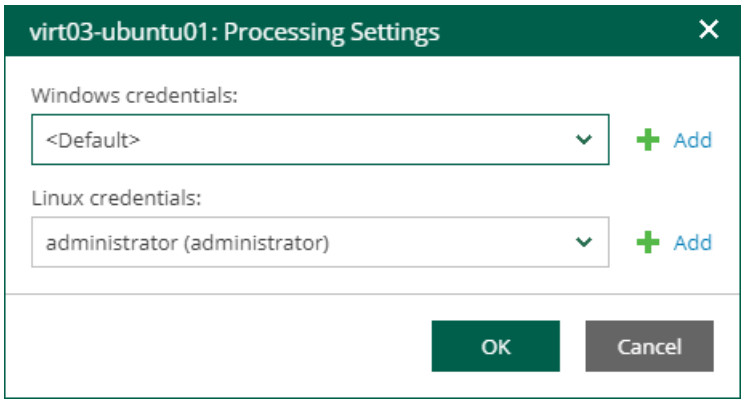


Special Credentials for Machine

By default, for all machines in the list, Veeam Backup & Replication uses common credentials you provided in the **Guest OS credentials** section. To use a different account for deploying the agent inside a specific machine, you can customize credentials for the machine.

To customize credentials:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Set User**.
3. Specify custom guest OS credentials and click **OK**.



To remove custom credentials for a machine:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Remove**.

> **NOTE**
>
> To customize settings of a machine added as part of a container, the machine should be included in the list as a standalone instance. For that, click **Add machine** and choose a machine whose settings you want to customize.

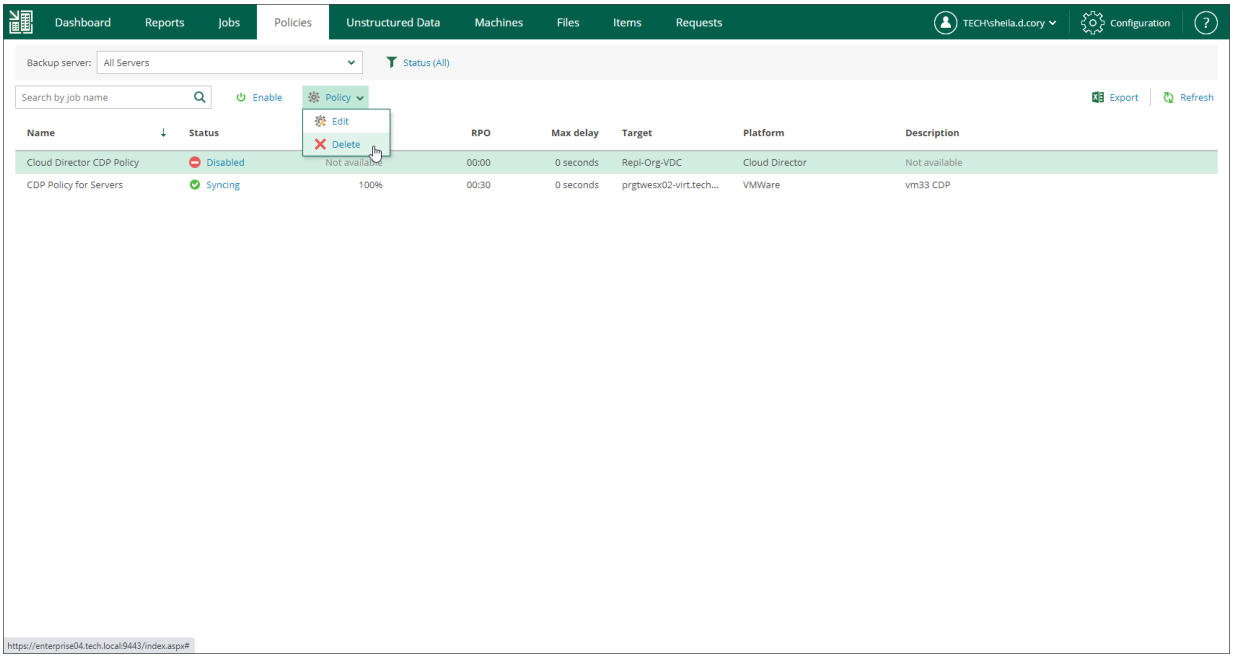
Deleting Policies

Users with the Portal Administrator role can permanently delete CDP policies. The deleted policies will no longer appear in the UI. They are removed from the Enterprise Manager database and from the Veeam Backup configuration database on the backup server.

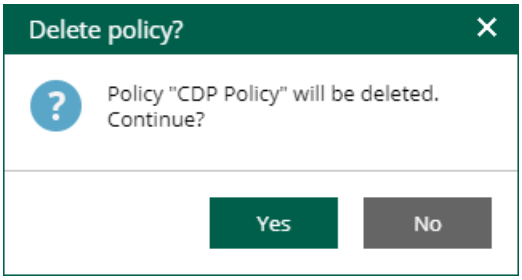
Before you delete a CDP policy, you must disable it.

To delete a policy:

1. On the **Policies** tab, select the required policy in the list.
2. On the toolbar, click **Policy** and select **Delete**.



3. In the displayed window, click **Yes** to confirm the operation.



Working with Unstructured Data

With Veeam Backup Enterprise Manager, authorized users can perform the following operations with unstructured data (file shares and object storage systems) processed by Veeam Backup & Replication:

- View unstructured data backups
- Browse unstructured data backups for specific items
- Search unstructured data backups for specific items
- Recover items from backups
- Delete backups

NOTE

- In the Enterprise Plus edition of Veeam Backup & Replication, users with the Portal Administrator role can customize the restore scope of other users (list of objects the user can recover). In other editions, the restore scope includes all objects and cannot be customized. However, you can delegate recovery of an entire file share, object storage or selected file type. Possible delegation options are described in the Configuring Permissions for File and Application Item Restore section.
- Veeam Backup Enterprise Manager does not display objects from the unstructured data to tape backups.

Viewing Unstructured Data Backups

From Veeam Backup Enterprise Manager, you can view information about unstructured data (file shares and object storage systems) processed by backup jobs configured on added backup servers. You can view backed up unstructured data on the **Unstructured Data** tab.

Each entry in the unstructured data list contains the following information:

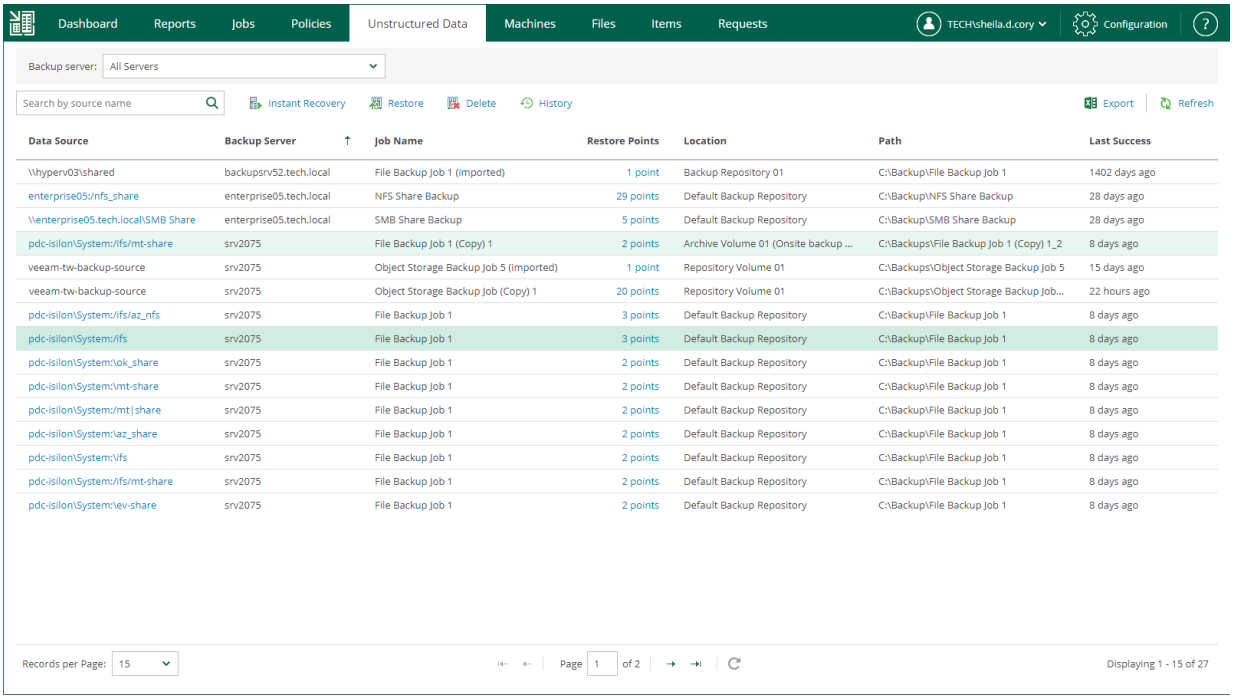
- *Data Source* — file share or object storage
- *Backup Server* — backup server that processes the data source
- *Job Name* — backup job that backs up the data source
- *Restore Points* — number of created restore points
- *Location* — name of the backup repository where the restore points are stored
- *Path* — path to the backup files
- *Last success* — time the job last ran successfully

To quickly find a data source (file share or object storage), you can filter the list of data sources by backup server or data source.

- To filter data sources by backup server name, from the **Backup server** list, select the necessary backup server. Veeam Backup Enterprise Manager will display backups of only those file data sources that are processed by the selected backup server.

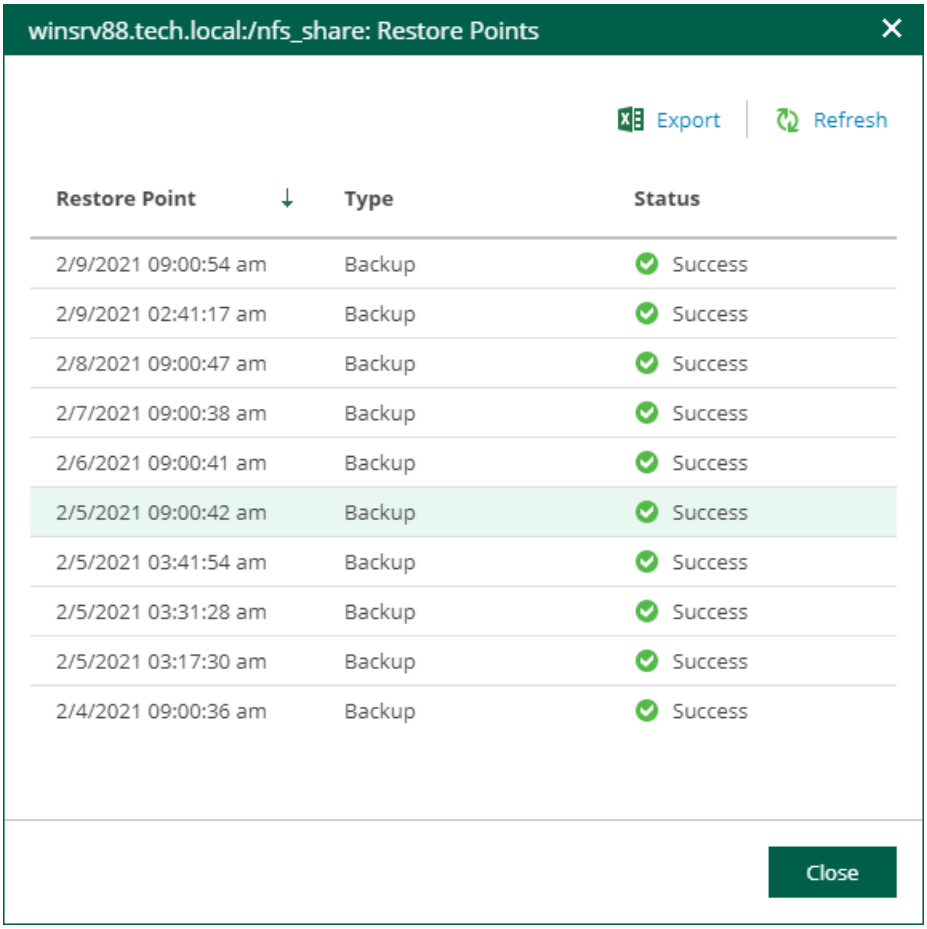
  The **Backup server** filter is only available for users with the Portal Administrator or Portal User role.
- To filter data sources by source name, enter the name or a part of the name in the search field. Veeam Backup Enterprise Manager will display backups of only those data sources whose names match the text that you entered.

> **NOTE**
>
> To export displayed information to a file, use the **Export** link on the toolbar.



You can also view additional data about each data source:

- To see detailed information about a data source, click its name in the **Data Source** column.
- To see detailed information about restore points, click a link in the **Restore Points** column.



Browsing for Items in Unstructured Data Backups

You can browse the content of file shares and object storage systems for specific items in the selected backup.

To browse the content of a data source, do the following:

1. On the **Unstructured Data** tab, select a data source and click **Restore**.

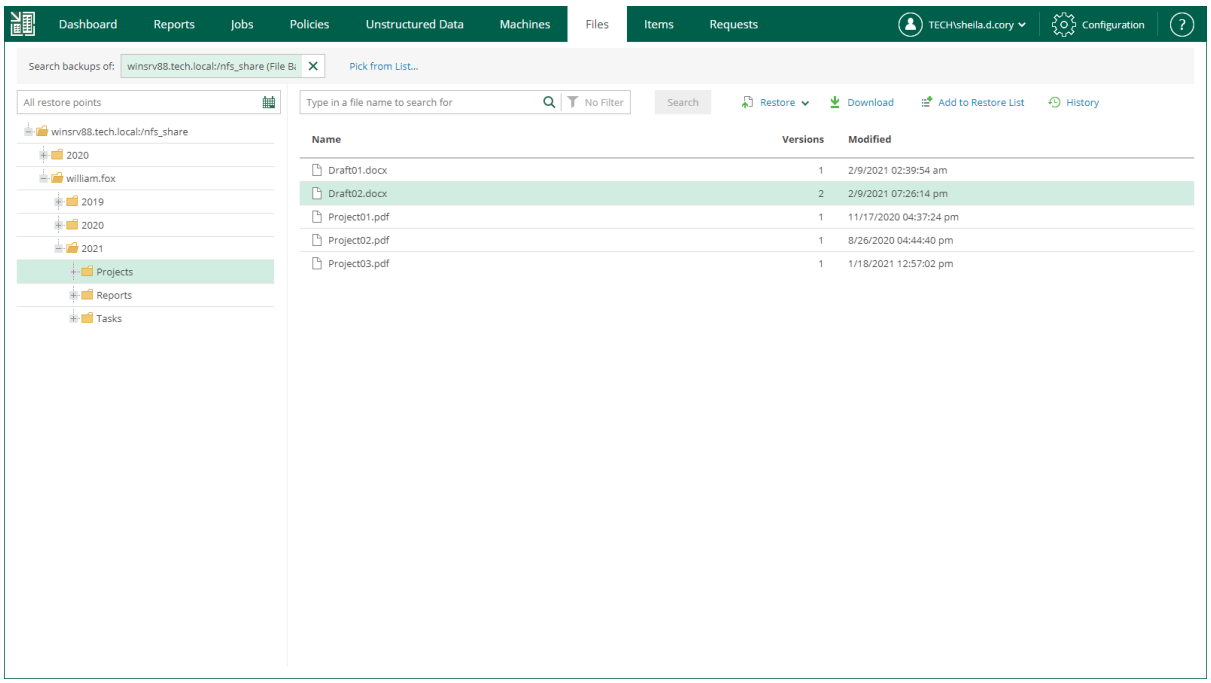
   Alternatively, on the **Files** tab, in the **Search backups of** field, enter the name of a data source whose items you want to browse or click the **Pick from List** link and select a data source in the **Select Object** window. Then click **Mount**.

2. Wait while Veeam Backup & Replication mounts the content from backup to a backup server. When the process is completed, Veeam Backup Enterprise Manager displays the content of the data source.

3. You can browse files contained in all restore points created by the backup job or in a specific restore point.

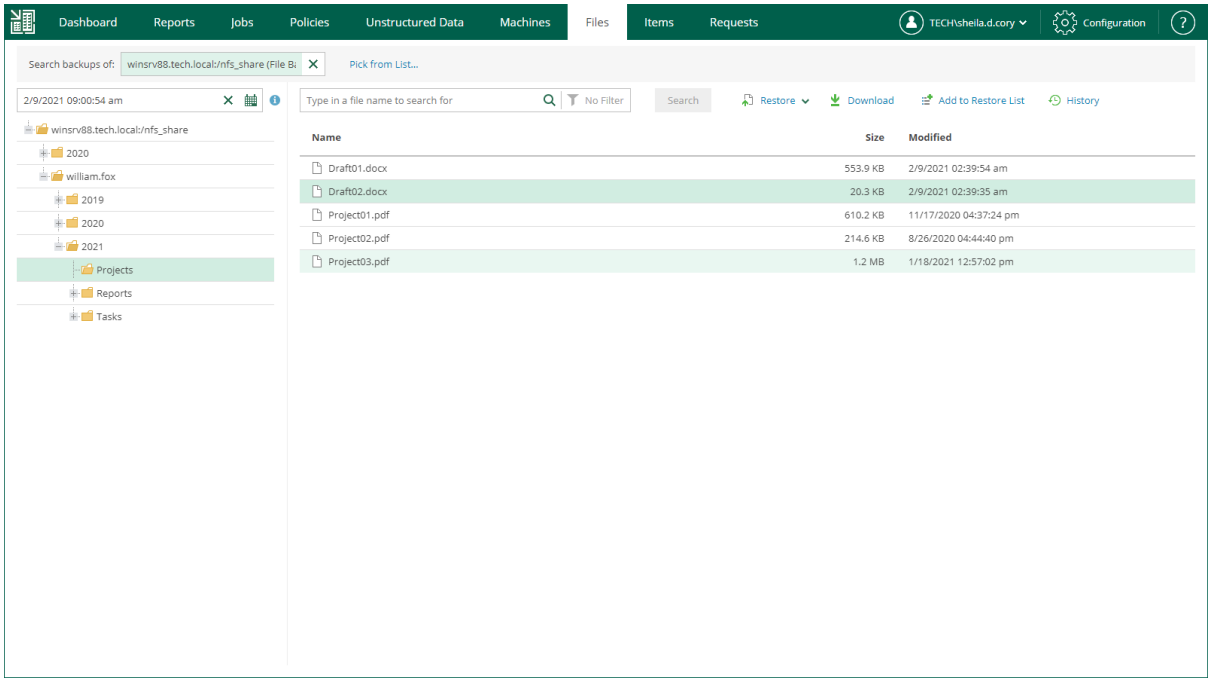
   - By default, the **All restore points** option is selected. With this option selected, you can browse the content in all restore points created by the backup job.

     For each object in the backup, Enterprise Manager displays the number of object versions and the date when the latest version was created. If an object has more than one version, you can select a necessary version during the restore process. For more information, see Restoring Specific Files.



- To select a specific restore point, click the calendar icon in the restore point field and select the necessary backup date and a restore point created on that date. Note that you cannot select a date on which the backup was not performed.

  For each file in the backup, Enterprise Manager displays file size and the date when the file version is created. Enterprise Manager displays only the file version contained in the selected restore point. For more information on file restore, see Restoring Specific Files.



TIP

You can use the search field at the top of the working area to search for specific files and folders. Depending on the number of files in the file share, the search process may take some time. For more information, see Searching for Items in Unstructured Data Backups.

Searching for Items in Unstructured Data Backups

Veeam Backup Enterprise Manager allows you to search unstructured data (file shares and object storage systems) for specific items. After you find necessary files, you can select them to perform file restore.

> **IMPORTANT**
>
> When you back up unstructured data, file system indexing is not created. Therefore, advanced search capabilities using filters are not available.

To perform simple search, do the following:

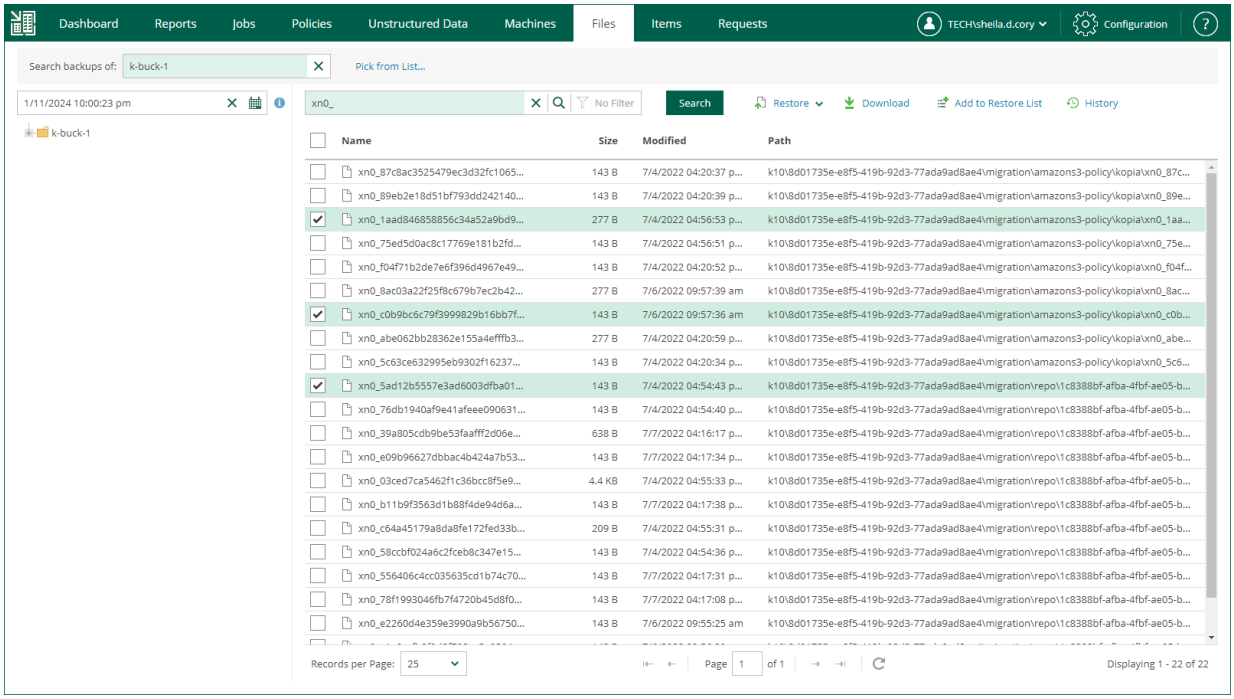
1. On the **Unstructured Data** tab, select a data source and click **Restore**.

   Alternatively, on the **Files** tab, in the **Search backups of** field, enter the name of a data source whose items you want to browse or click the **Pick from List** link and select a data source in the **Select Object** window. Then click **Mount**.

2. In the **Search backups of** field, enter the name of a data source whose items you want to restore or click the **Pick from List** link and select the necessary data source in the **Select Object** window.

3. In the search field, enter the name of the necessary item or a part of it.

4. To view the search results, press [Enter] or click **Search**.



Data Recovery

With Veeam Backup Enterprise Manager, you can restore unstructured data previously backed up with file backup jobs or object storage backup jobs. You can restore the following data:

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

Enterprise Manager offers the following recovery options:

- Instant file share recovery allows you to recover a point-in-time file share state.
- Restore of files and folders allows you to restore specific items located on a file share or object storage.

Instant File Share Recovery

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

- SMB file shares

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

- NFS file shares

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

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

Performing Instant File Share Recovery

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

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

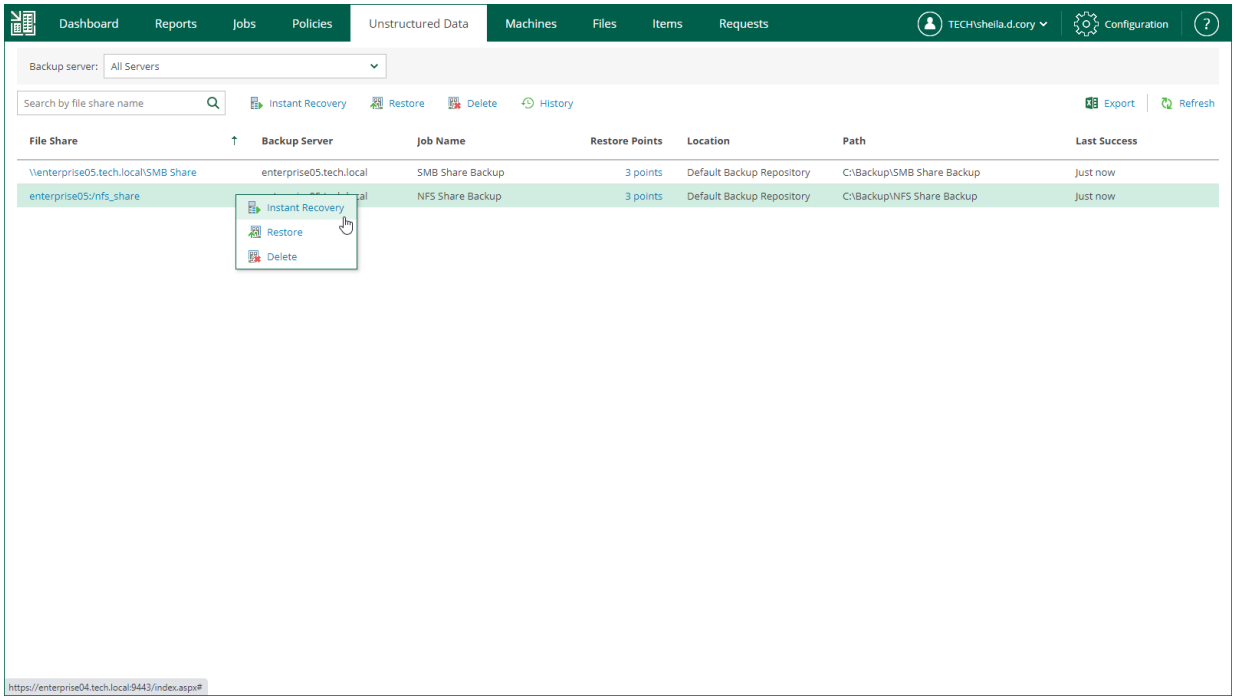
1. Launch the Instant File Share Recovery wizard.
2. Select a restore point.
3. Specify access permissions.
4. Review the recovery settings.

Step 1. Launch Instant File Share Recovery Wizard

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

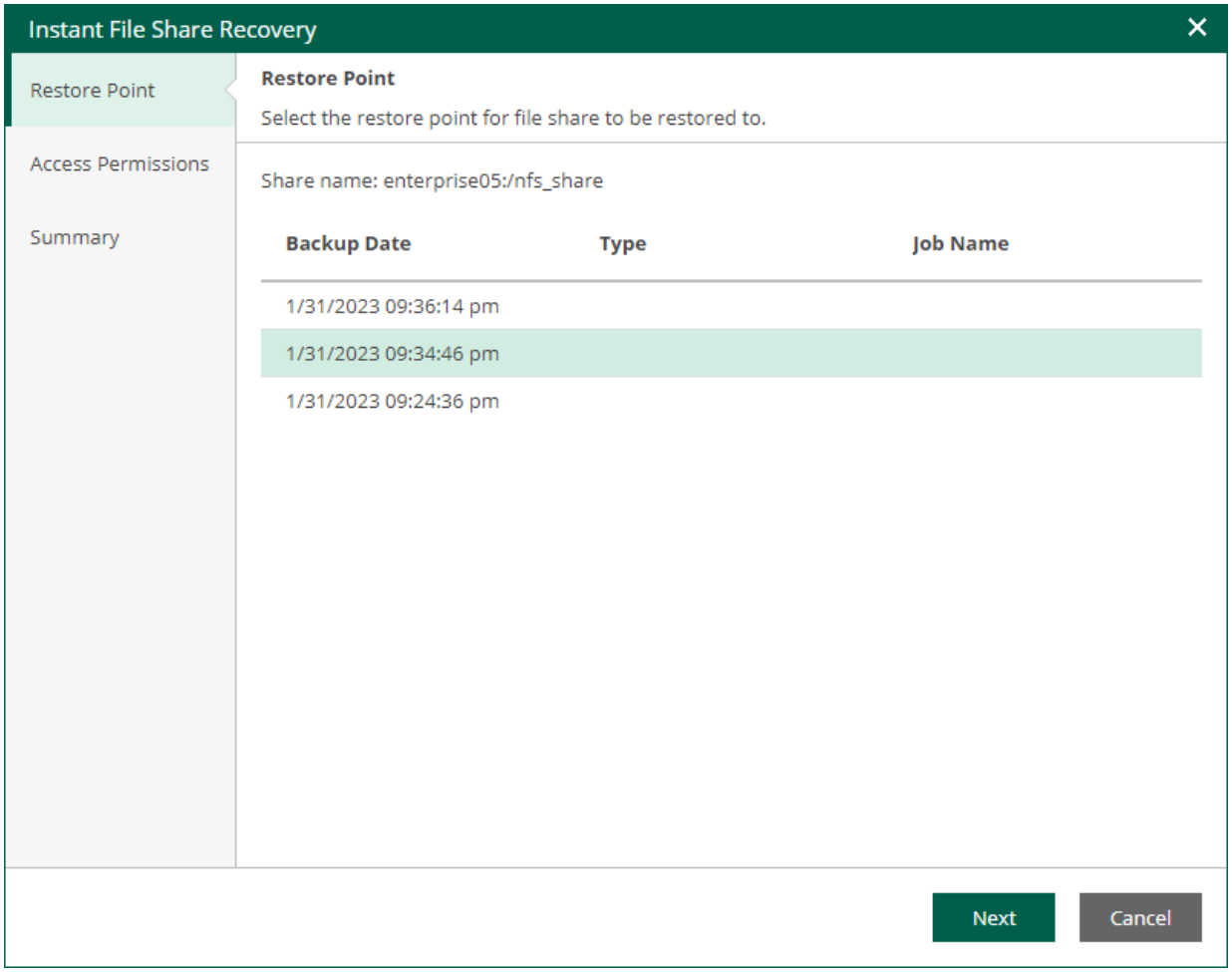
1. Open the **Unstructured Data** tab and select a file share from the list.
2. On the toolbar, click **Instant Recovery**.

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



Step 2. Select Restore Point

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



Step 3. Specify Access Permissions

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

1. Configure access permissions for the file share. The following options are available:
   - **Allow to everyone**
   - **Deny to everyone**
   - **Allow to the following accounts or groups only**

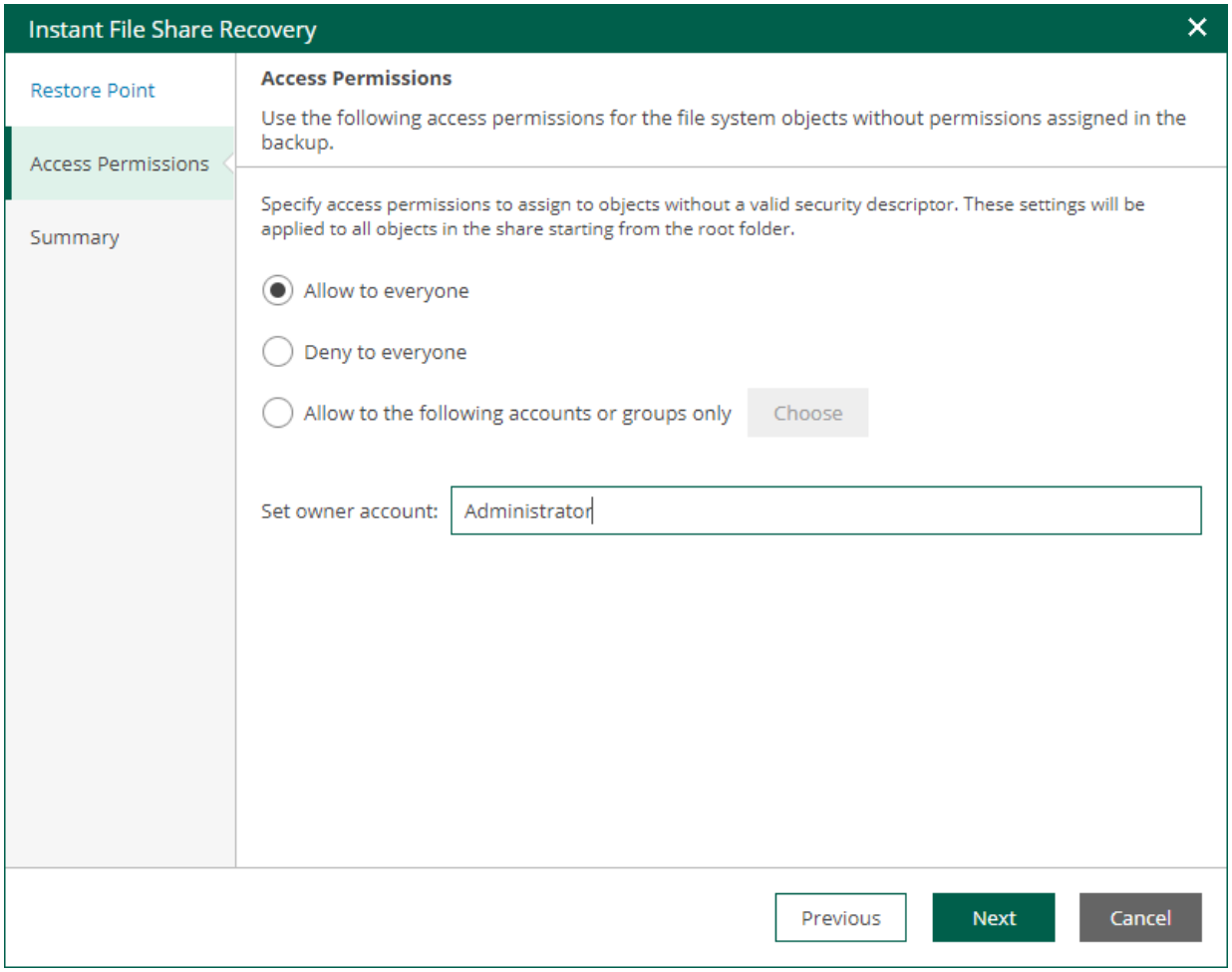
     If you select this option, configure accounts and groups to which you want to grant permissions for accessing the file share:

     i. Next to the **Allow to the following accounts or groups only** option, click **Choose**.

     ii. In the **Accounts and Groups** window, click **Add** to add an account or group.

     iii. Specify a name of the account or group and click **OK**.

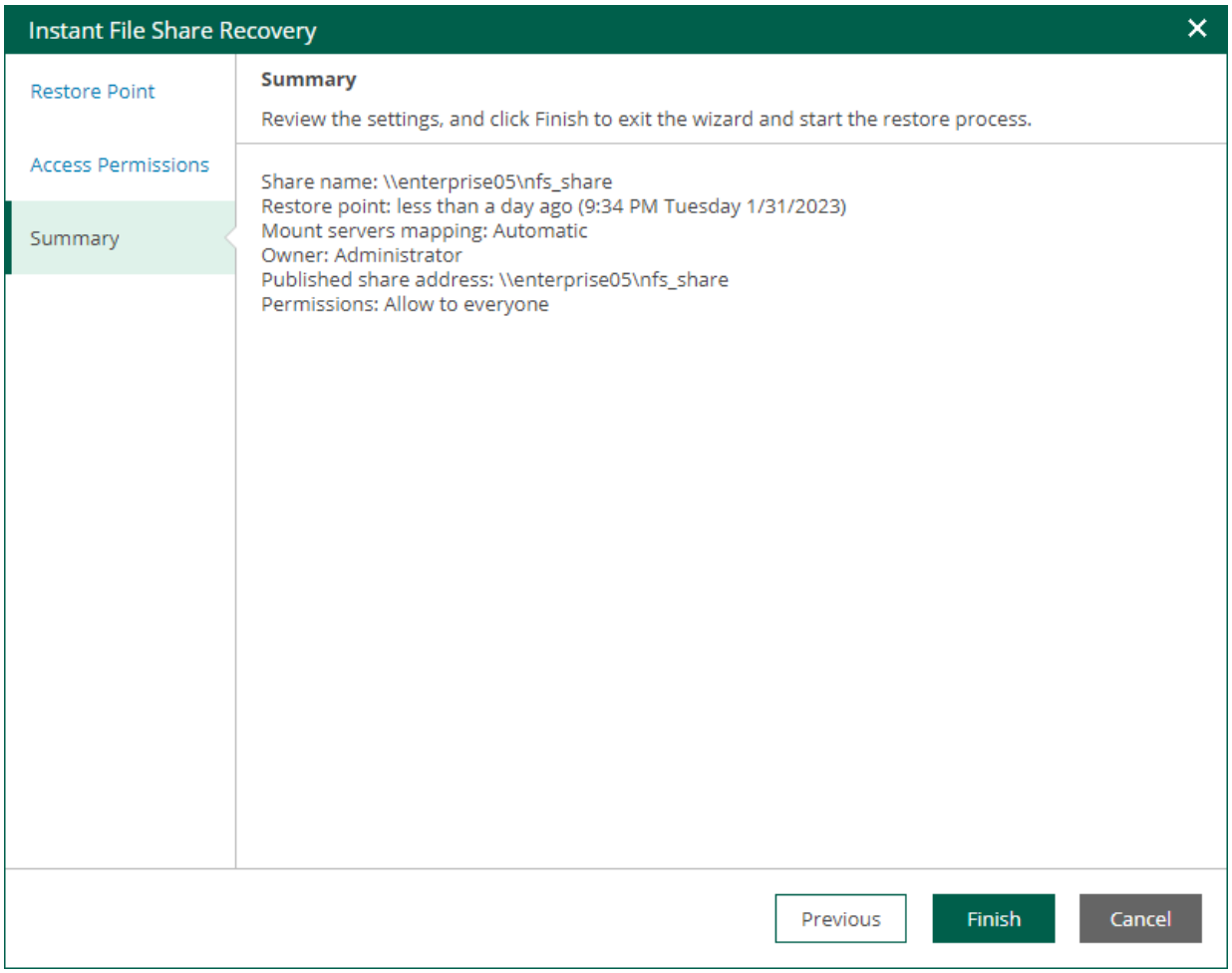
     iv. Add other accounts or groups if necessary. Use the **Remove** button to remove an account or group.
2. In the **Set owner account field**, specify the owner account for the file share.



Step 4. Review Recovery Settings

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Unstructured Data Restore History** view. Note that the **Unstructured Data Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.



What You Do Next

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

Finalizing Instant File Share Recovery

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

- [For NFS file shares] When you perform instant recovery of an NFS file share, the file share is published as a read-only SMB file share that lets you instantly access all recovered files. After you finish working with the files, you must stop publishing the recovered file share.

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

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

Migrating Recovered File Shares

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

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

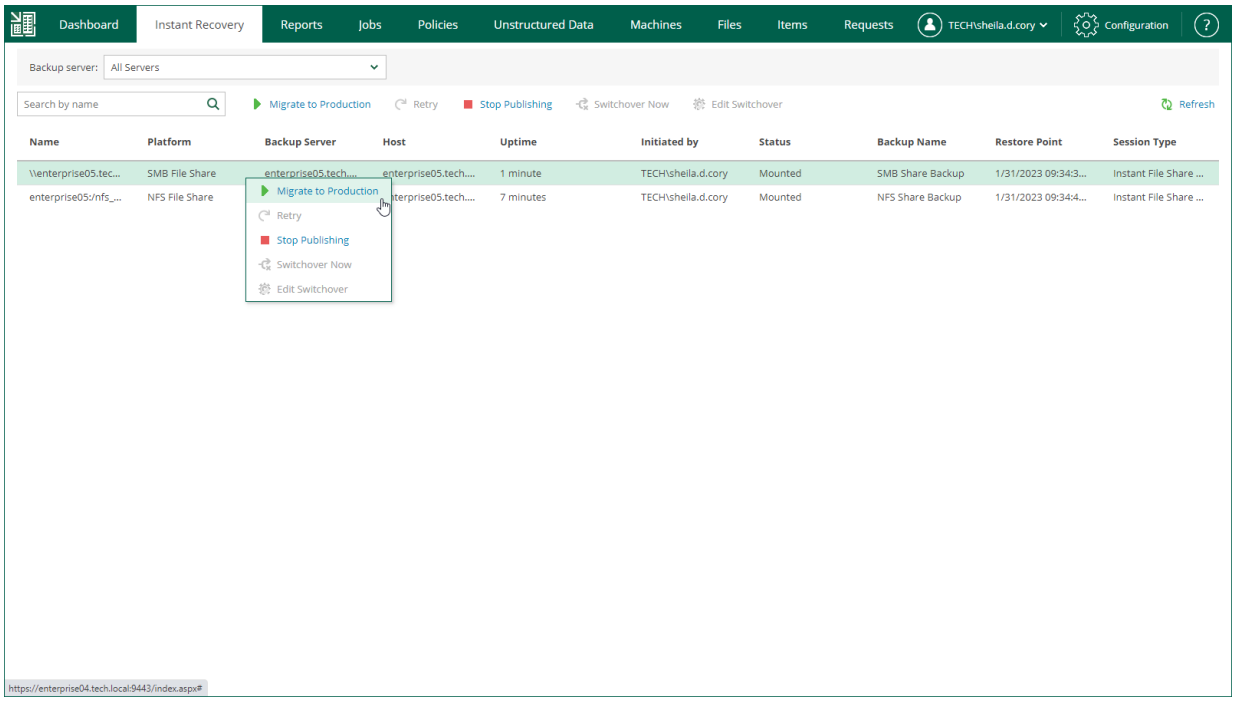
1. Launch the Migrate to Production wizard.
2. Specify file share destination.
3. Specify restore options.
4. Configure switchover.
5. Review the migration settings.

Step 1. Launch Migrate to Production Wizard

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

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

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



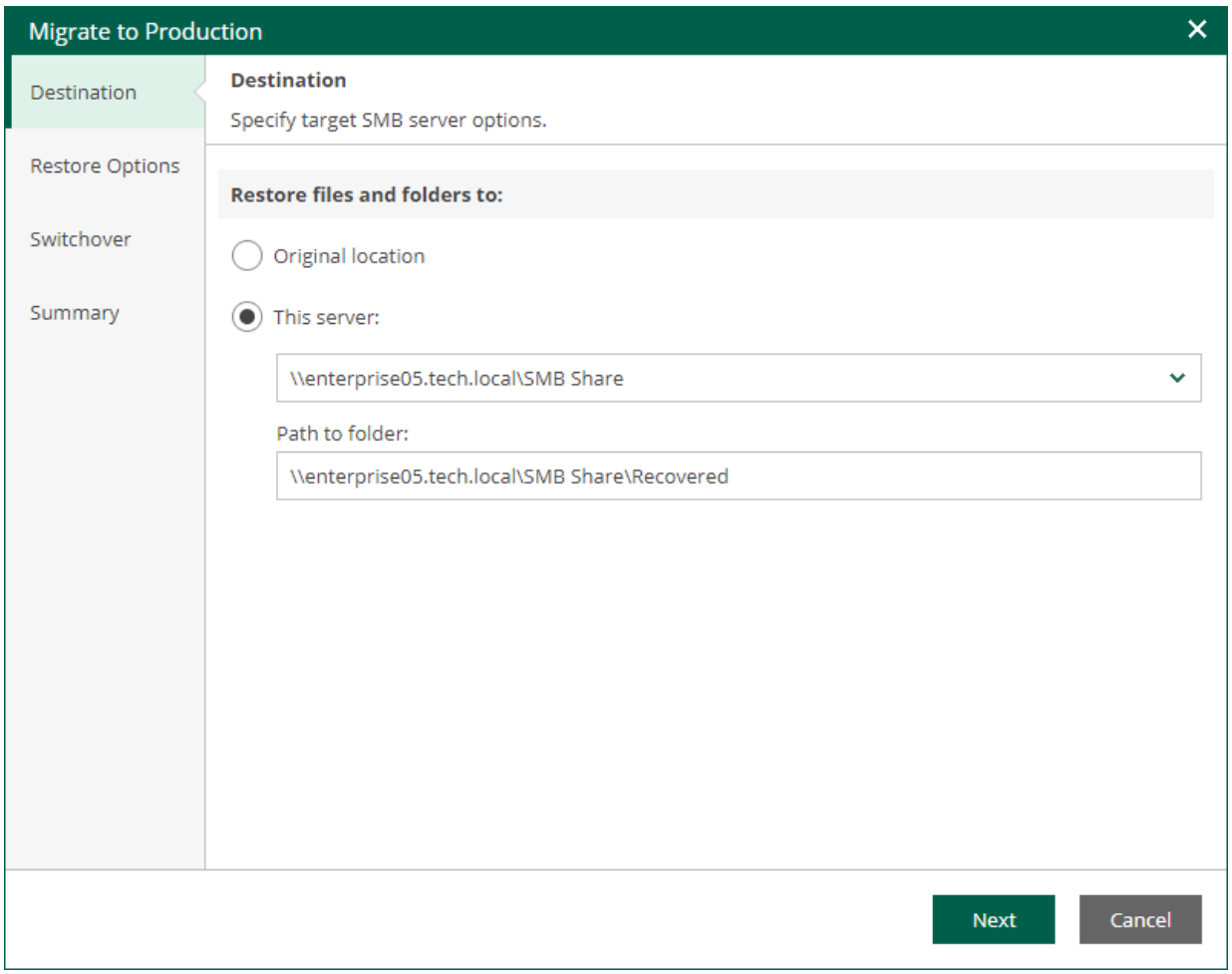
Step 2. Specify Destination

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

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

     You can select any file share added to the backup inventory. If the required file share is missing in the drop-down list, add a new file share to the backup server infrastructure. For more information on how to add a new file share, see the Adding File Share section of the Veeam Backup & Replication User Guide.

  b. In the **Path to file** field, specify a path to the folder on the selected file share where the files must be restored.



Step 3. Specify Restore Options

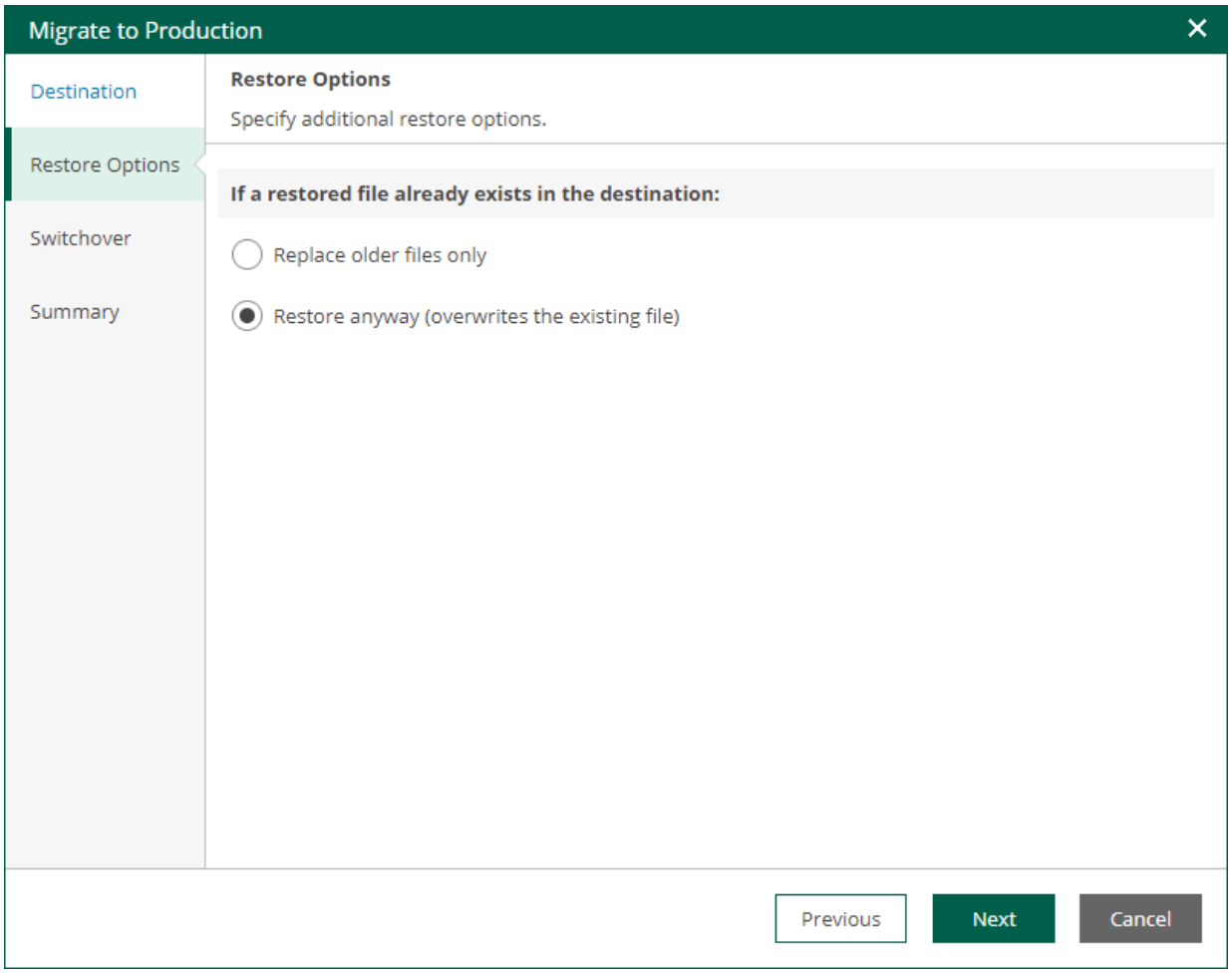
At the **Restore Options** step of the wizard, specify overwrite options in case the file with the same name already exists in the target folder.

- **Replace older files only**

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

- **Restore anyway**

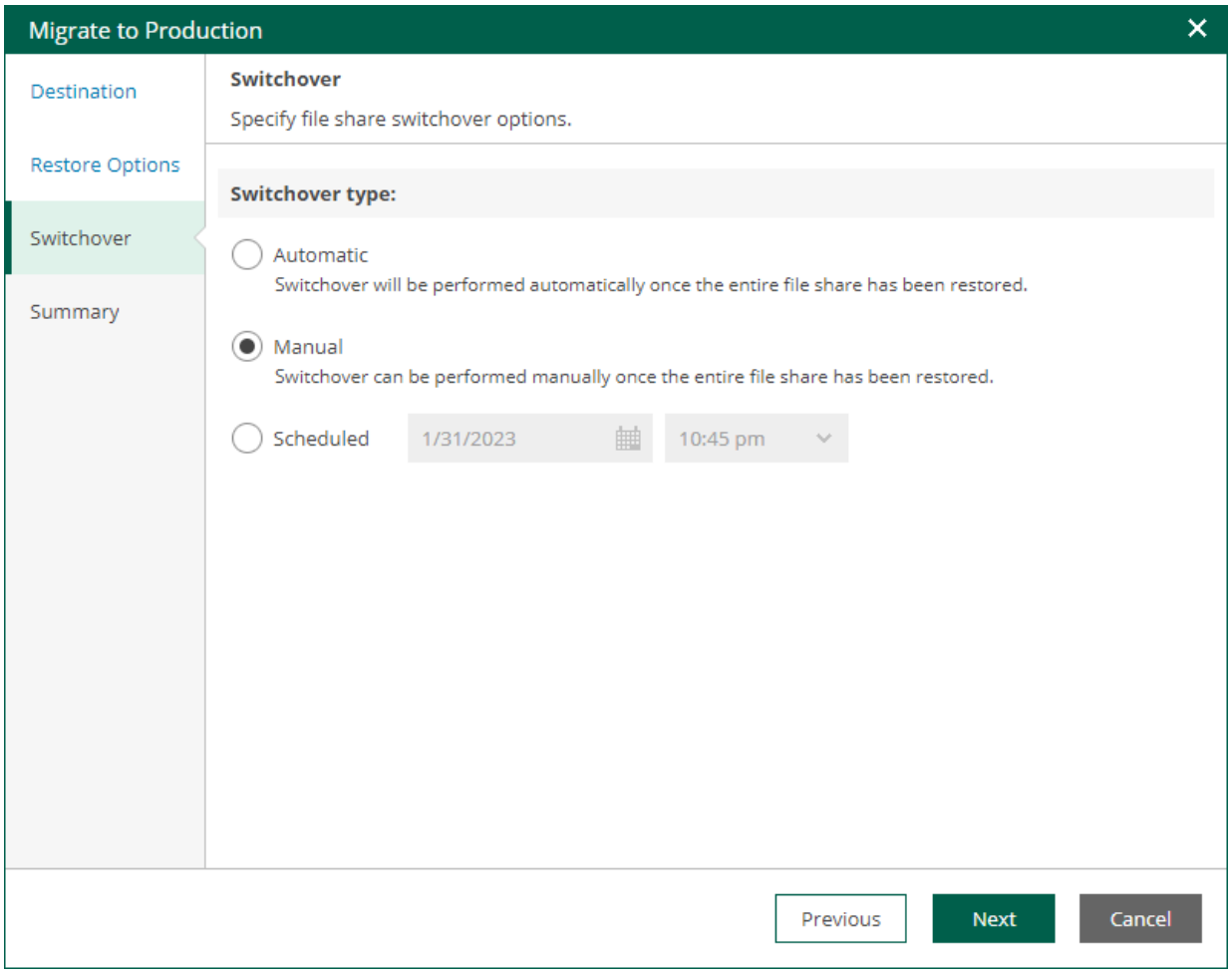
  Select this option if you want to overwrite the existing file with the restored file in all cases.



Step 4. Configure Switchover

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

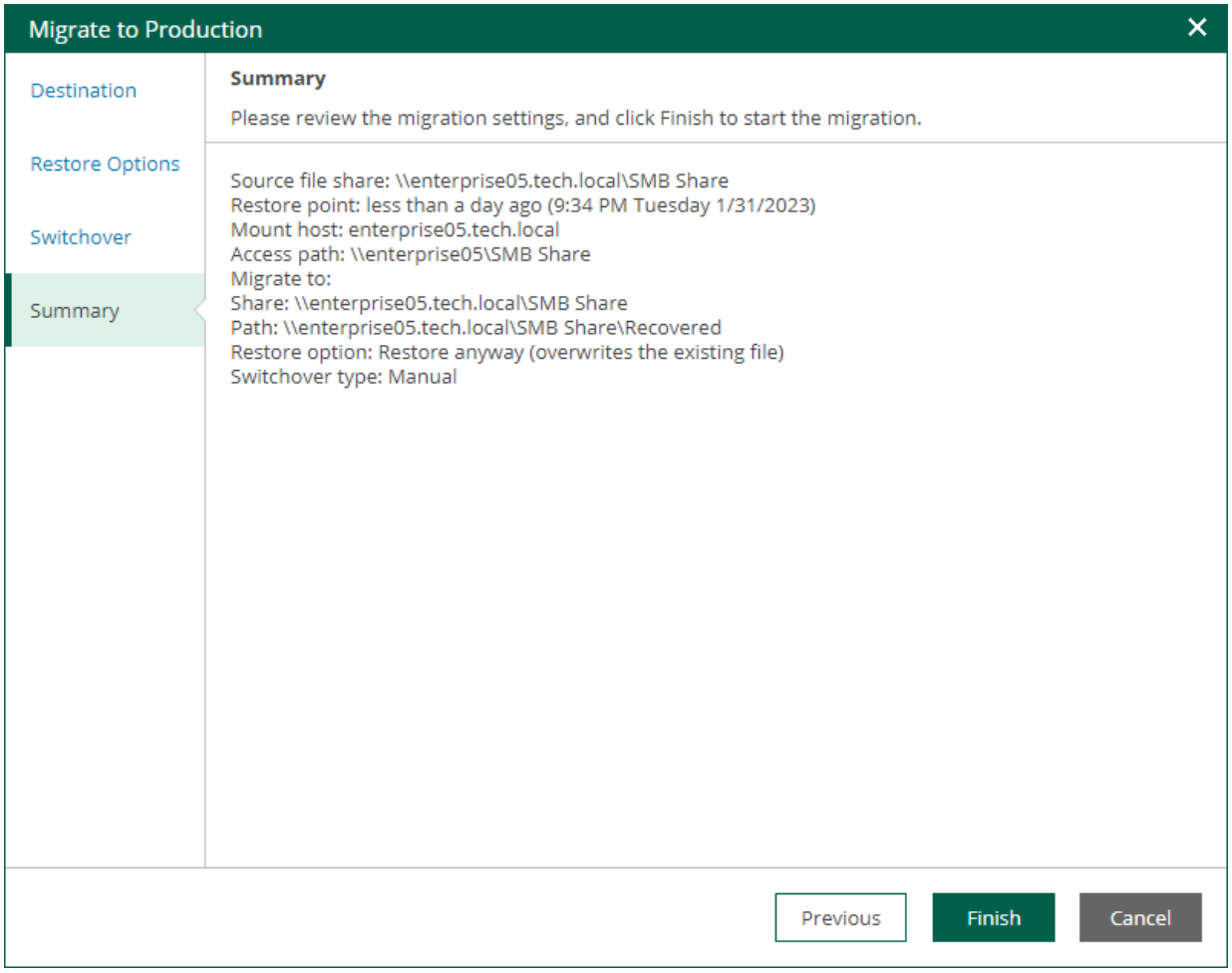
- **Automatic** – select this option if you want Veeam Backup & Replication to perform the switch automatically right after the entire file share will be restored.
- **Manual** – select this option if you want to perform the switch manually.
- **Scheduled** – select this option if you want Veeam Backup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



Step 5. Review Migration Settings

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Unstructured Data Restore History** view. Note that the **Unstructured Data Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.



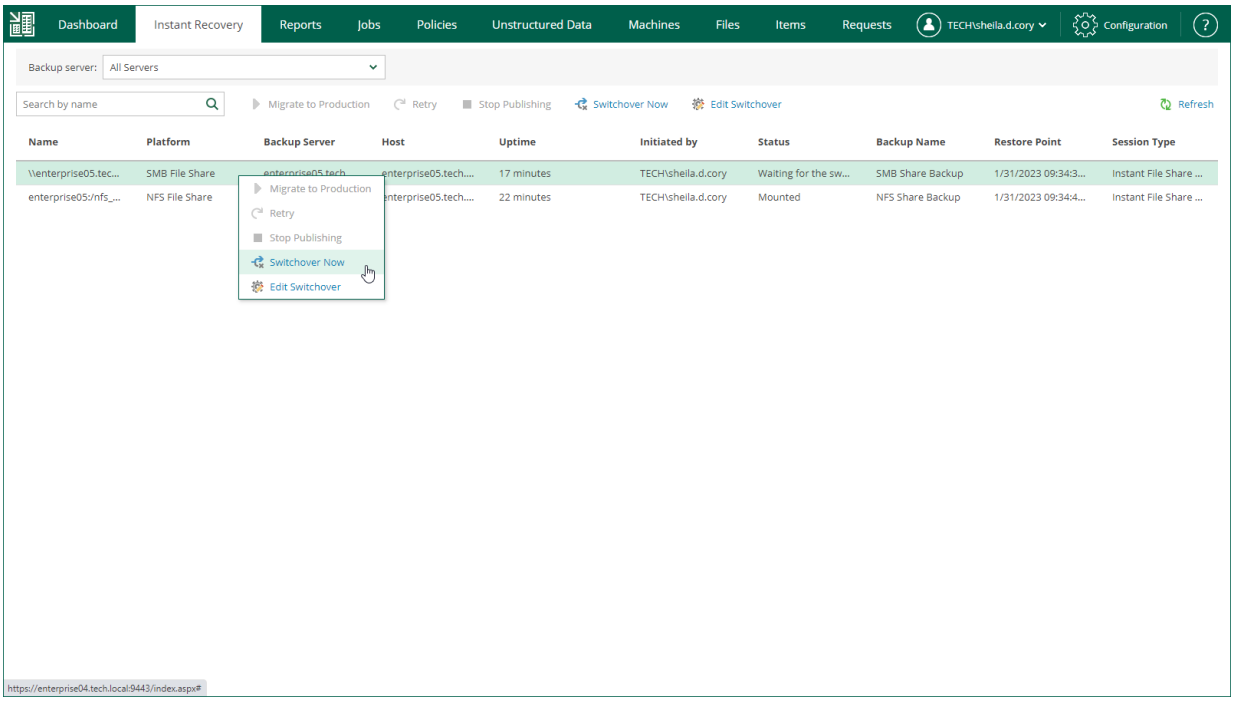
Switching to Production File Share Manually

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

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

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

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



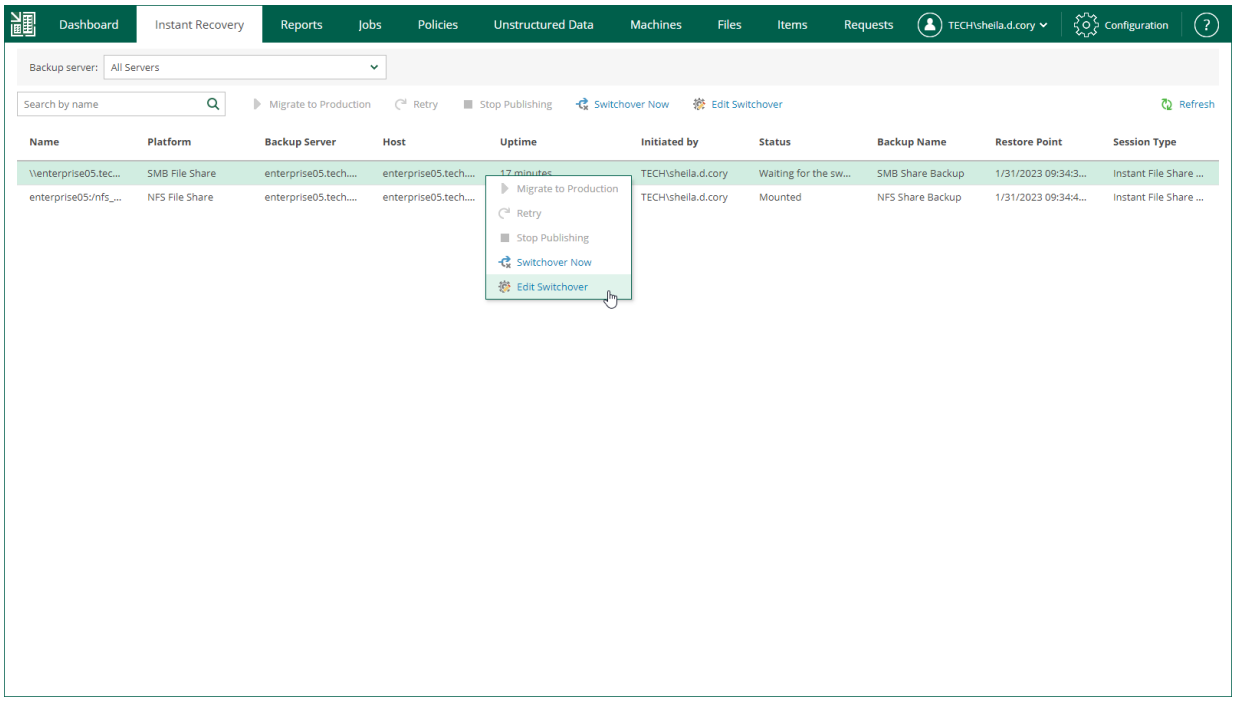
Changing Switchover Time

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

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

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

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



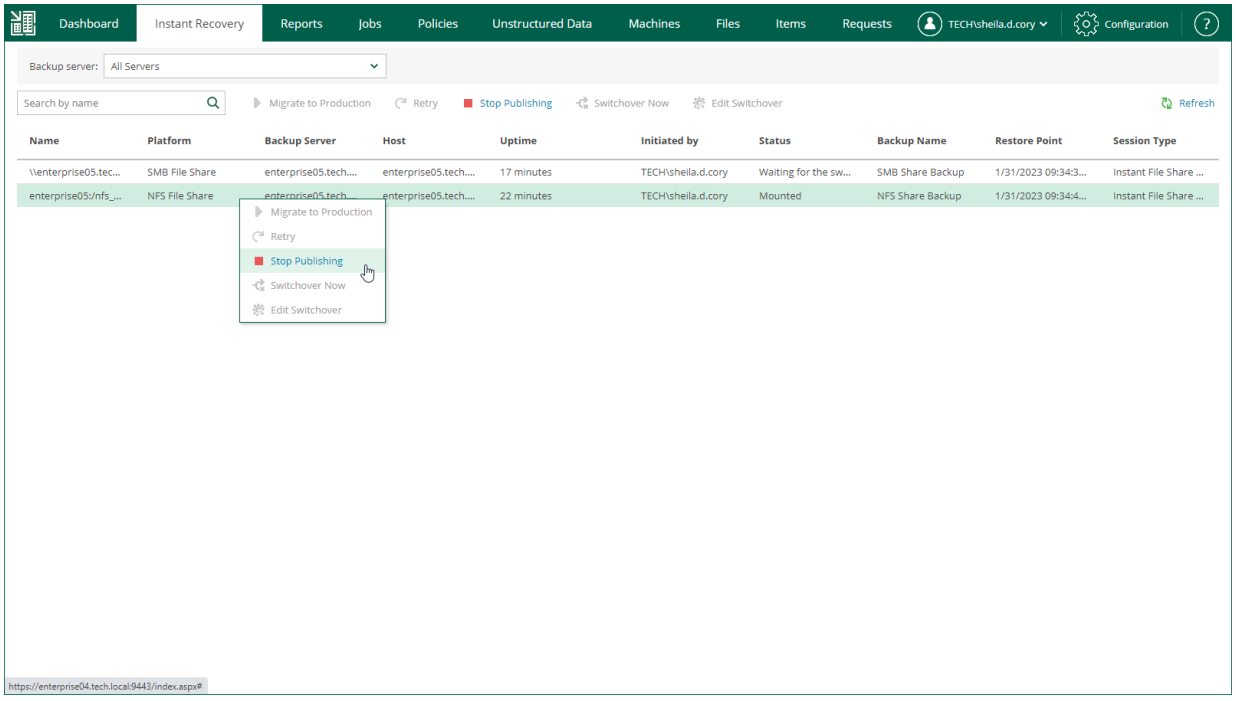
Unpublishing Recovered File Shares

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

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

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

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



Restoring Specific Files

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

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

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

In This Section

- Restoring Files to Original Location
- Downloading Files
- Restoring Multiple Files

Restoring Files to Original Location

In this restore scenario, Veeam Backup Enterprise Manager will extract a file from the backup and restore it to the original location in the file share or object storage. Restoring files to the original location is the most secure recovery method, as the user who initiates the restore operation in the Enterprise Manager UI cannot access the file itself.

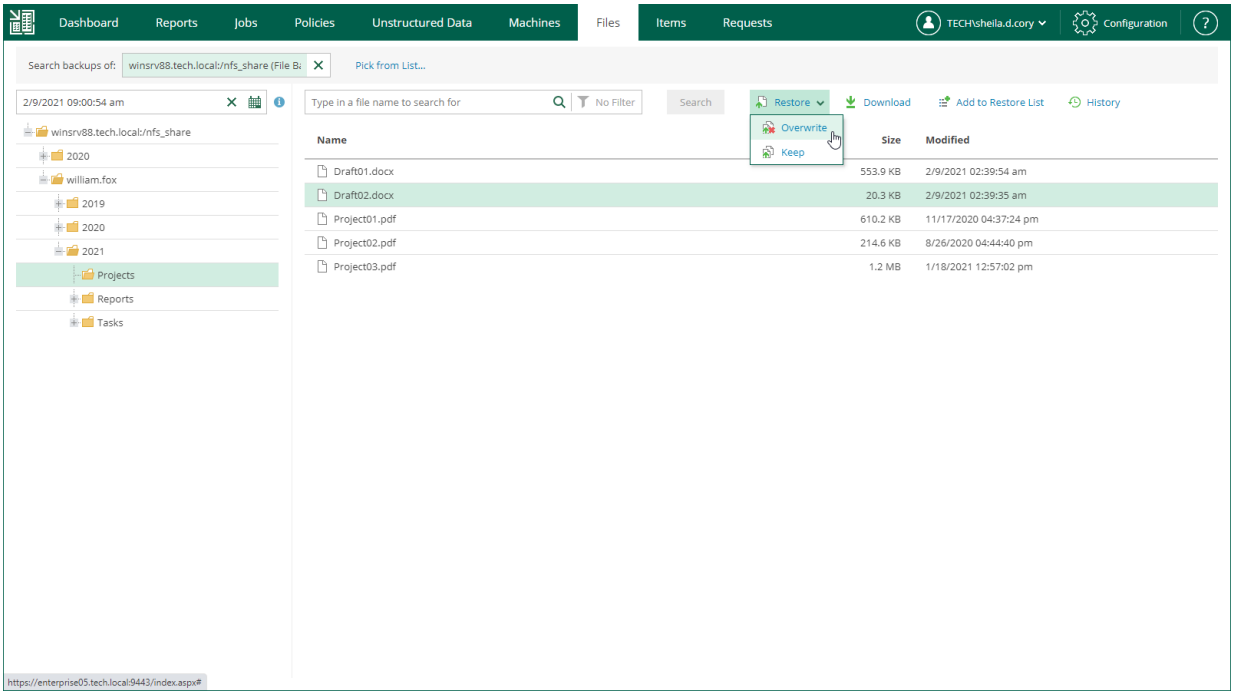
To restore a file to the original location, do the following:

1. Locate the necessary file using browse or search possibilities of Veeam Backup Enterprise Manager. For details, see Viewing Unstructured Data Backups and Browsing for Items in Unstructured Data Backups.

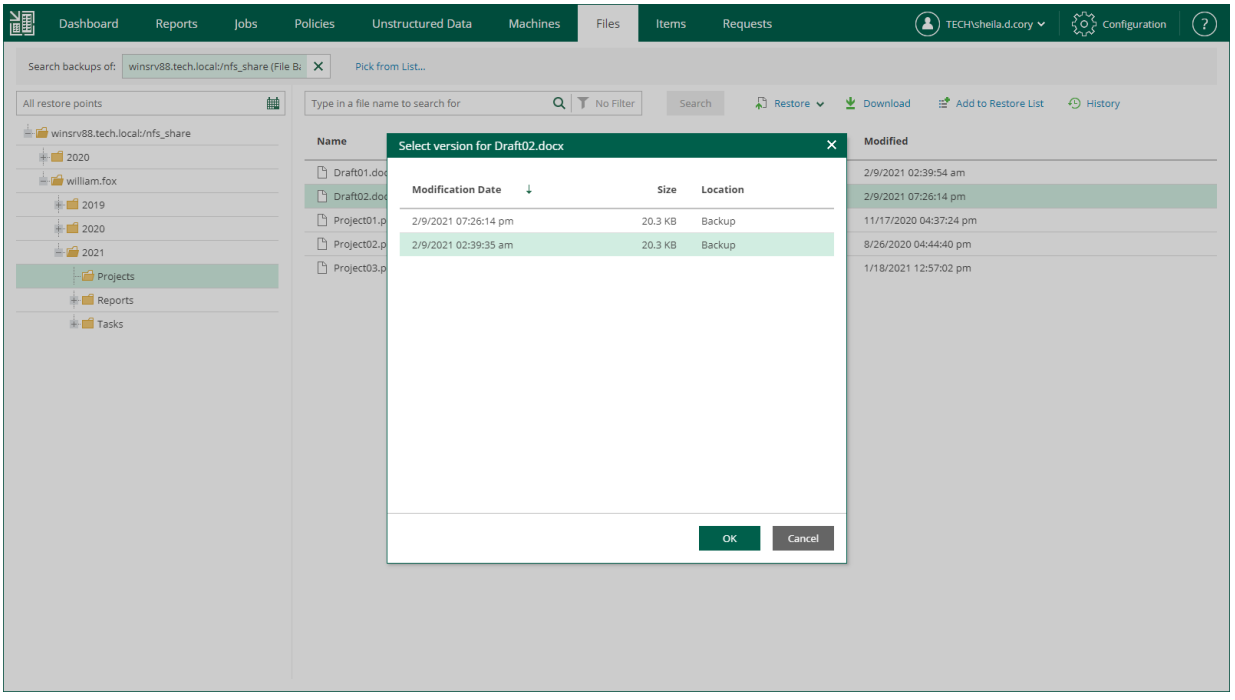
   You can select multiple files in file shares. Selection of multiple object storage items is not available.

2. Click **Restore** and select how to restore the selected items:
   - If you select **Overwrite**, the item from the backup will replace the original item in the data source.

- If you select **Keep**, the item from the backup will be restored next to the original item in the data source. The restored item will have the *_RESTORED_<date>_<time>* suffix in its file name.



3. If you browse items in all restore points created for the data source, and the restore points contain multiple versions of the item, Enterprise Manager will prompt you to select the item version. In the **Select version** window, select the restore point that contains the necessary item version and click **OK**.



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

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

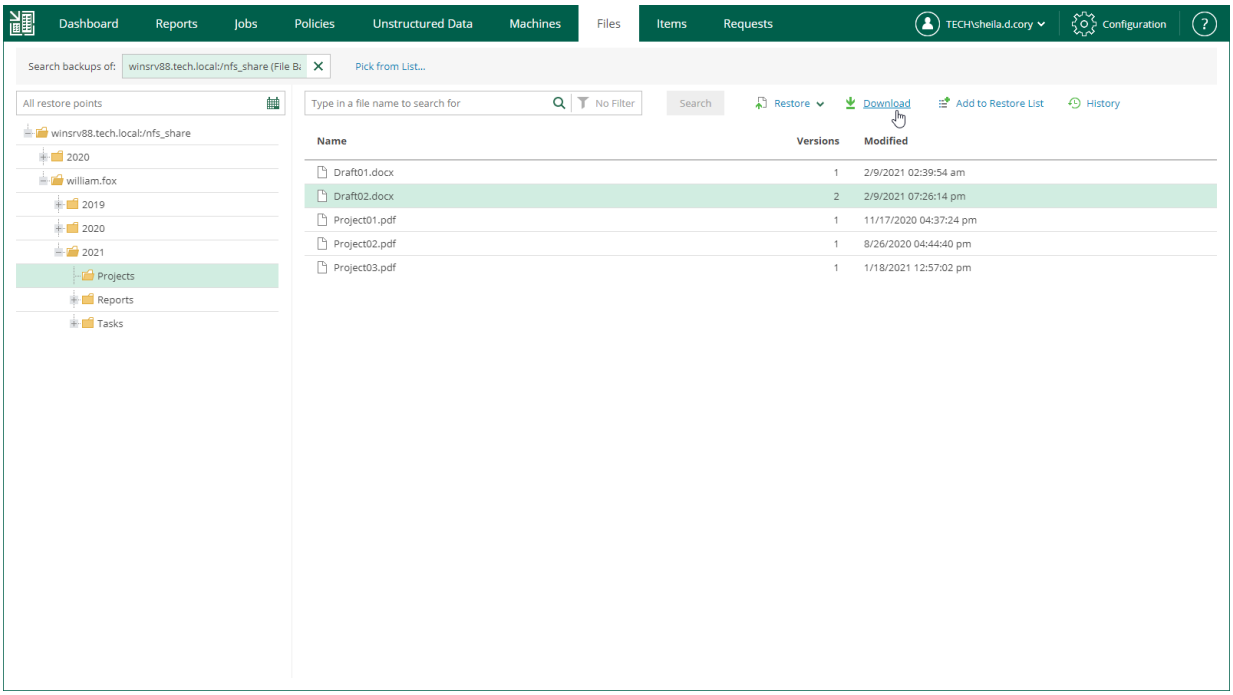
Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **File Restore History** view. Note that the **File Restore History** view displays only the restore operations initiated from Enterprise Manager; restore operations initiated from Veeam Backup & Replication are not displayed.

Downloading Files

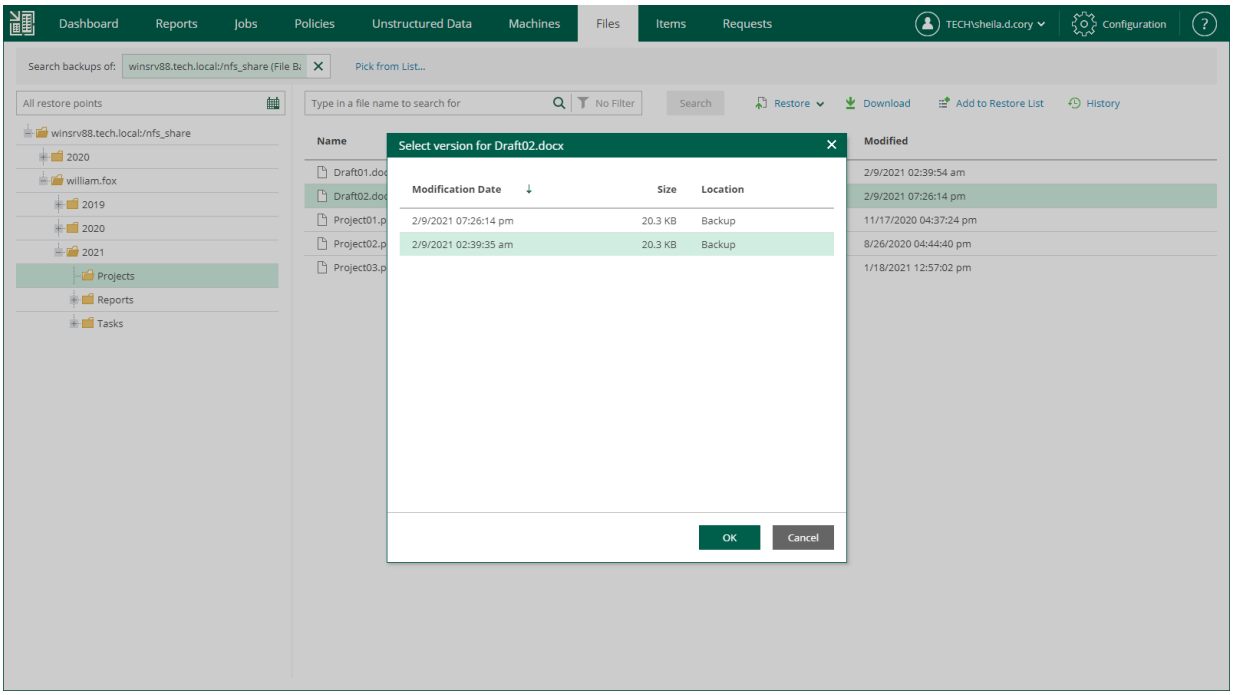
If you choose to download a file, Veeam Backup Enterprise Manager interacts with the backup server to extract the necessary file from the backup. The user who initiated the restore will be able to download the file to the local machine, that is, the Enterprise Manager server.

To download a file, do the following:

1. Locate the necessary file using browse or search possibilities of Enterprise Manager. For details, see Viewing Unstructured Data Backups and Browsing for Items in Unstructured Data Backups.
2. Click **Download**.



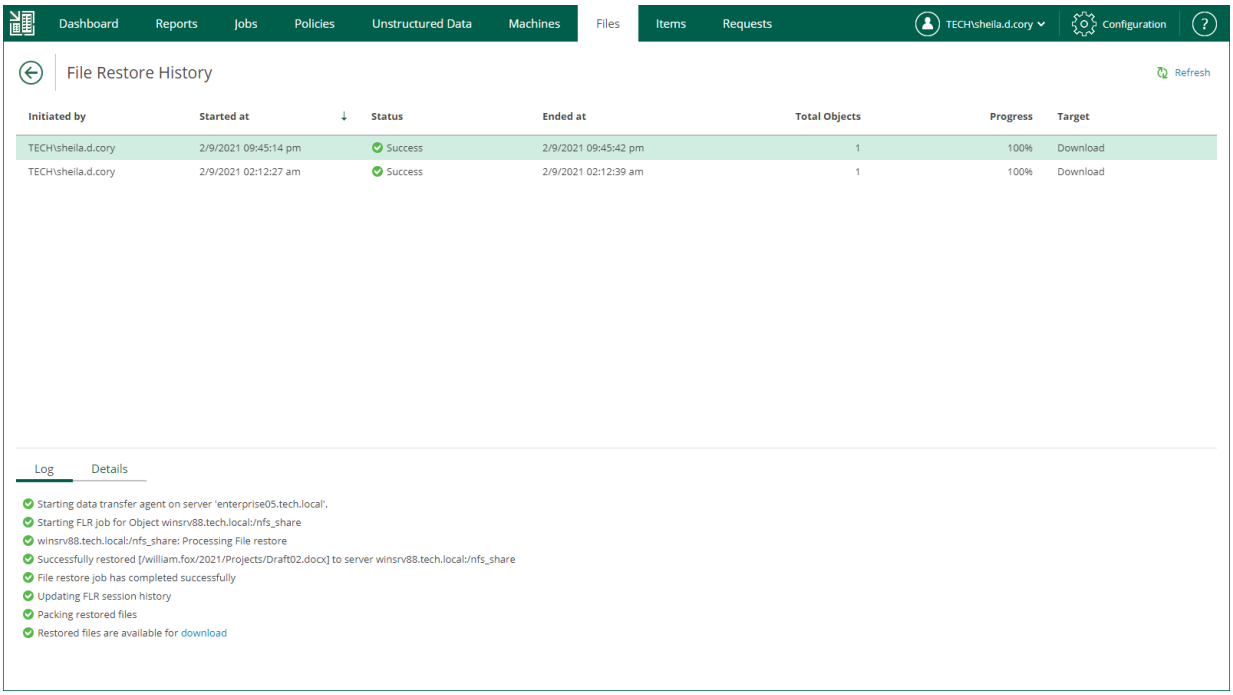
3. If you browse items in all restore points created for the data source, and the restore points contain multiple versions of the item, Enterprise Manager will prompt you to select the item version. In the **Select version** window, select the restore point that contains the necessary item version and click **OK**.



4. In the displayed window, click **Yes**.
5. Wait for restore session to complete and the item to be retrieved from the backup.
6. Select the item from the list.
7. On the **Log** tab of the **File Restore History** view, click the **download** link in the *Restored files are available for download* record of the session log.

   The file is saved to the default download folder on your local machine.

If you download a single file, it is also saved in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Multiple files are packed in a ZIP file named `FLR_<date>_<time>.zip` and stored in the same folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.



Restoring Multiple Files

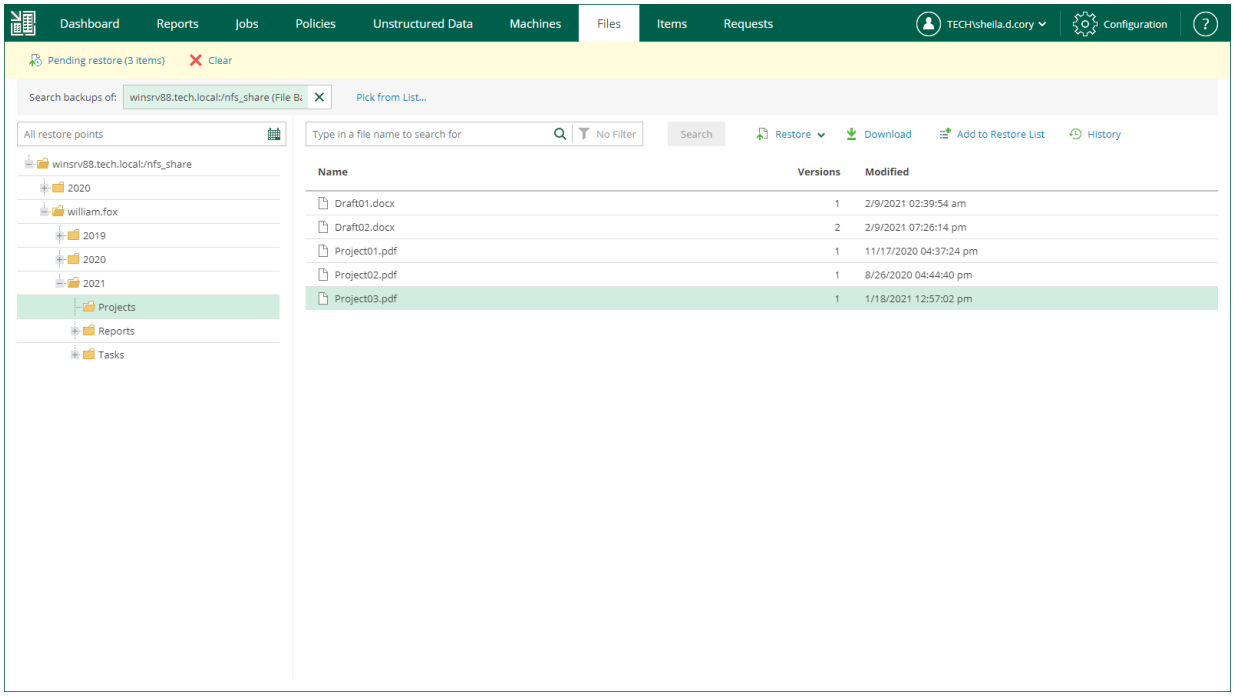
In addition to restoring single files from selected restore points, Veeam Backup Enterprise Manager supports bulk restore. If you need to restore multiple files at once, you can select more than one file in the preview pane when browsing, and then use the **Restore** command, or add the necessary files to the restore list and then restore all files at once. Unlike the **Restore** command, using the restore list helps you to prepare for restore files from different data sources 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 details, see Viewing Unstructured Data Backups and Browsing for Items in Unstructured Data Backups.
2. Click **Add to Restore List**.
3. If you browse items in all restore points created for the data source, and the restore points contain multiple versions of the item, Enterprise Manager will prompt you to select the item version. In the **Select version** window, select the restore point that contains the necessary item version and click **OK**.

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

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



To restore files added to the restore list:

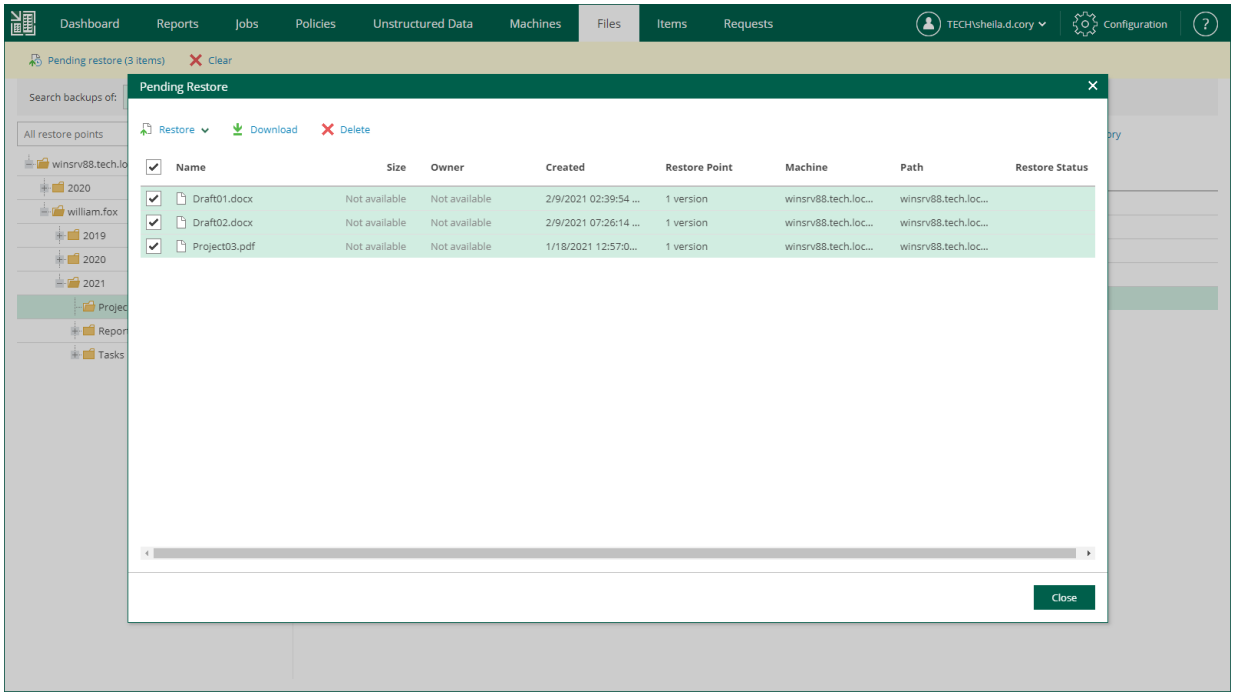
1. In the restore list notification, click **Pending restore**.
2. In the **Pending Restore** window, select check boxes next to the files that you want to restore. Use the check box next to the header of the **Name** column to select all files in the list at once.

   If you want to remove a file from the restore list, select the file and click **Delete**.
3. Click the **Restore** or **Download** link to perform the necessary restore operation for the selected files.
4. In the displayed window, click **Yes**.
5. [For the download operation] Wait for restore session to complete. On the **Log** tab of the **File Restore History** view, click the **download** link.

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

   Multiple files are also saved in a ZIP file named `FLR_<date>_<time>.zip` in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.

> **TIP**
>
> Veeam Backup Enterprise Manager keeps links for downloaded files in the history for one day. To download a file that was previously restored:
>
> 1. On the **Files** tab, click **History**.
> 2. In the **File Restore History** view, select the necessary restore session.
> 3. On the **Log** tab, click the **download** link.


Dashboard
Reports
Jobs
Policies
Unstructured Data
Machines
Files
Items
Requests
TECH\sheila.d.cory
Configuration
Pending restore (3 items)
Clear
Search backups of:
All restore points
winsrv88.tech.lo
2020
william.fox
2019
2020
2021
Projec
Repor
Tasks
Pending Restore
Restore
Download
Delete
Name
Size
Owner
Created
Restore Point
Machine
Path
Restore Status
Draft01.docx
Not available
Not available
2/9/2021 02:39:54 ...
1 version
winsrv88.tech.loc...
winsrv88.tech.loc...
Draft02.docx
Not available
Not available
2/9/2021 07:26:14 ...
1 version
winsrv88.tech.loc...
winsrv88.tech.loc...
Project03.pdf
Not available
Not available
1/18/2021 12:57:0...
1 version
winsrv88.tech.loc...
winsrv88.tech.loc...
Close

Deleting Backups

You can delete the data of a file share or object storage from a backup repository. The deleted data source is not removed from the list immediately. It will be removed from the list after the records about the data source are removed from the configuration database of the backup server. Once this operation completes, a notification will appear at the top of the Enterprise Manager window.

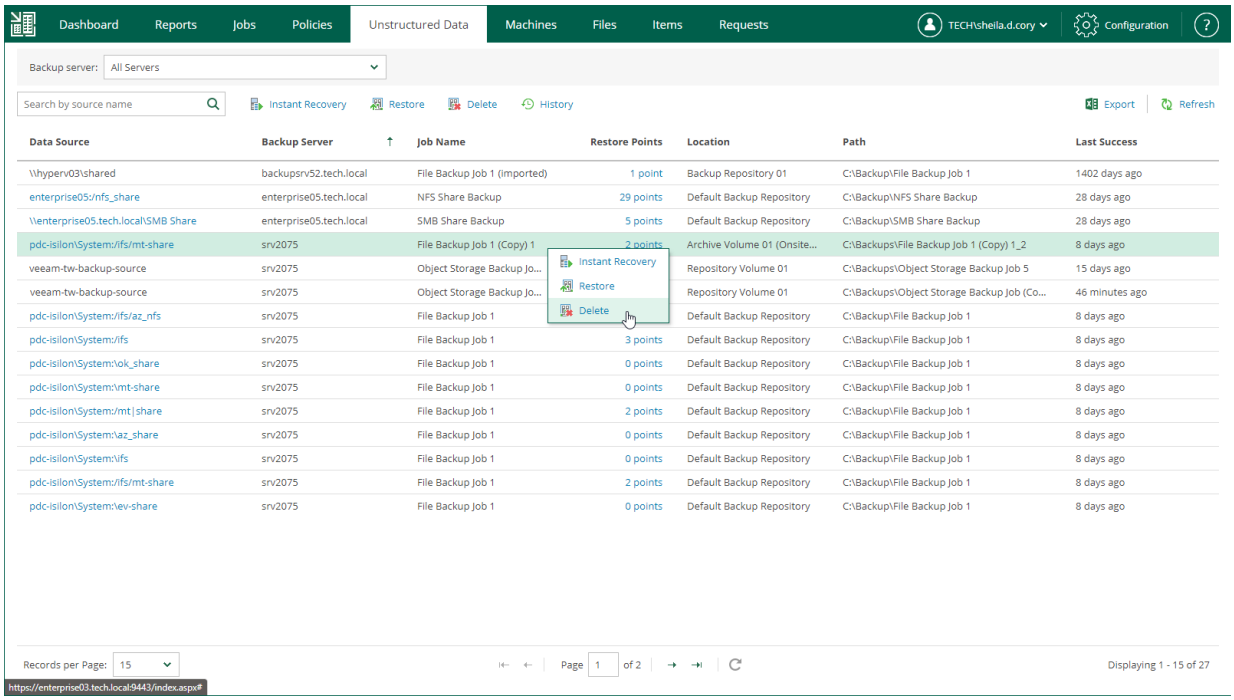
If four-eyes authorization is enabled on the backup server, backup files will remain in the backup repository and become orphaned.

To delete a backup, do the following:

1. Open the **Unstructured Data** tab.
2. In the list of backups, select the necessary backup and click **Delete**.

   To locate the necessary backup, you can filter backups by backup server name or search by data source name.
3. In the displayed window, click **Yes**.

> **NOTE**
>
> If several data sources are processed by the same backup job, deletion of the selected data source backup will not affect other data sources in the job.



Working with Machines

Authorized users can restore VMs included in their restore scope. Users with the Portal Administrator role have no scope limitations. The restore scope can be customized if you have the Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all machines and cannot be customized. However, you can delegate recovery of entire machines, guest files, or selected file types. Possible delegation options are described in the Configuring Permissions for File and Application Item Restore section.

With Veeam Backup Enterprise Manager, you can perform the following operations with machines:

- View machines and delete them from backups
- Create on-demand incremental backups (quick backups) for machines
- Restore machines and VM disks from backups
- Failover to VM replicas and VMware Cloud Director vApps
- Run failover plans for VMware vSphere and Microsoft Hyper-V VMs

NOTE

Veeam Backup Enterprise Manager does not display Nutanix AHV VMs, and recovery of Nutanix AHV VMs is not available. However, you can browse and restore guest OS files of Nutanix AHV VMs. For more information, see Guest OS File Restore.

In This Section

- Viewing Machines
- Deleting Machine from Backup
- Quick Backup
- VM Recovery

Viewing Machines

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

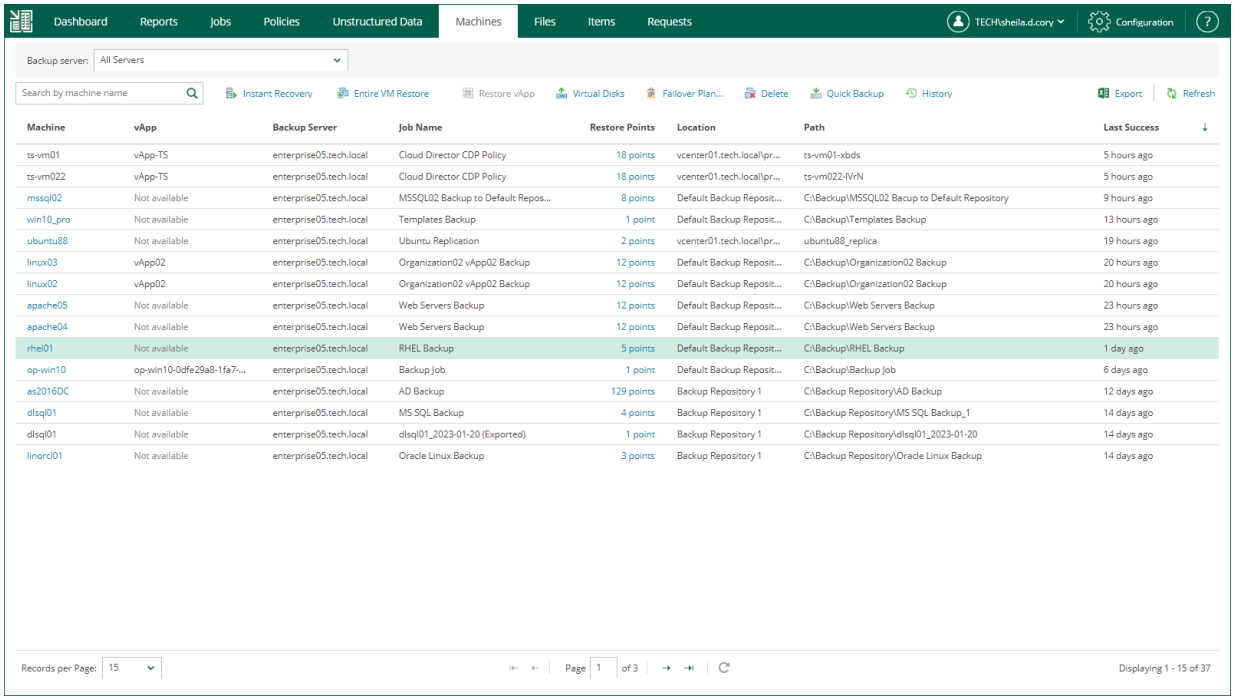
> **NOTE**
>
> Veeam Backup Enterprise Manager does not display Nutanix AHV VMs, and recovery of Nutanix AHV VMs is not available. However, you can browse and restore guest OS files of Nutanix AHV VMs. For more information, see Guest OS File Restore.

Entries in the list contain the following data:

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

You can filter machines in the list by a backup server or search for specific machines by a machine name. To search for a machine, enter its name or part of the name in the **Search** field.

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

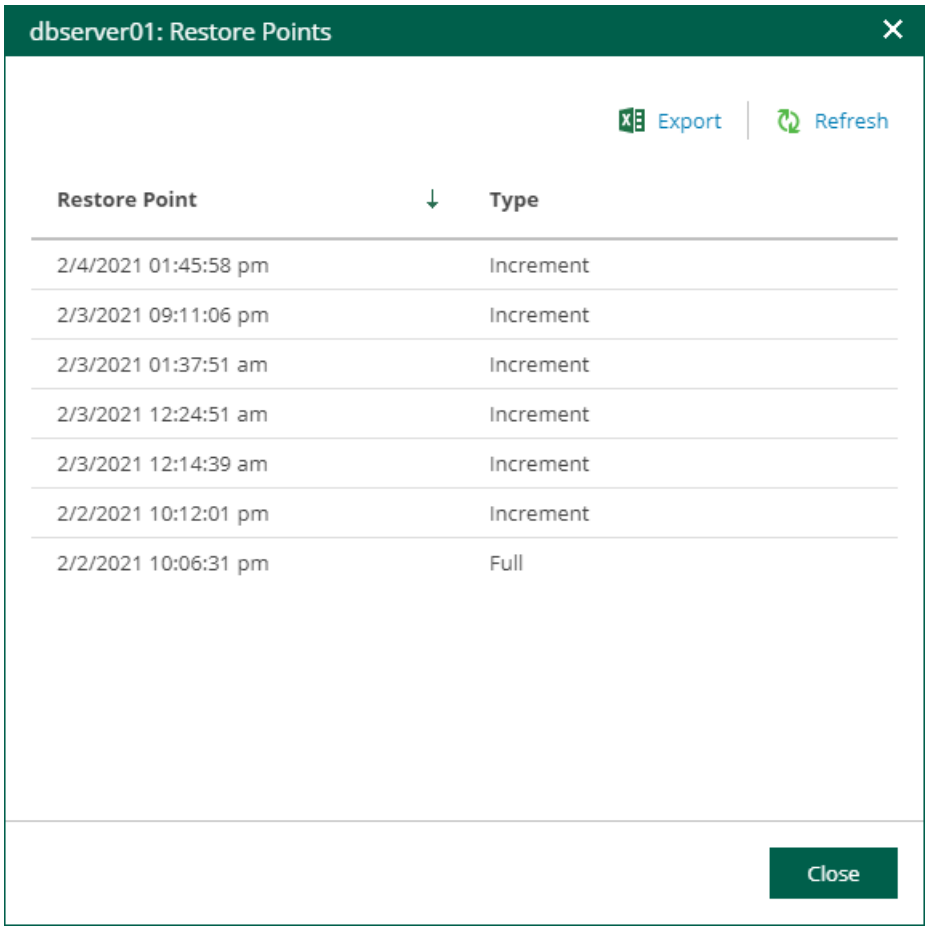


Besides the information presented in the list of machines, the **Machines** tab allows you to view advanced data about each machine:

- To check a report containing a list of job runs for a specific machine, click the machine name in the **Machine** column.

  Note, you cannot open a report for machines processed by backup copy jobs and machines from imported or orphaned backups.

- To open a list of machine restore points, click a link in the **Restore Points** column.



Deleting Machine from Backup

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

Before You Begin

Before you delete a machine from a backup, consider the following considerations and limitations:

- If four-eyes authorization is enabled on the backup server, you cannot delete a machine from backup using Enterprise Manager.
- If multiple machines are processed by the same backup job, deletion of a 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.

Deleting Machine

To delete a machine from a backup, do the following:

1. On the **Machines** tab, select the necessary machine backup from the list of machines.

   To quickly find a machine, you can filter machines in the list by a backup server or search for specific machines by machine name.
2. Click **Delete**.
3. To remove backups marked with weekly, monthly and yearly GFS flags, select the **Remove GFS full backups** check box.

   The check box is displayed if the machine has GFS backups.
4. Click **Yes** to confirm deletion.

Quick Backup

Quick backup is an ad-hoc incremental backup for a machine added to a backup job. To create a new incremental restore point, Veeam Backup & Replication triggers an existing backup job that processes the selected machine. This restore point will be added to the backup chain in the backup repository. Quick backup can be helpful if you want to produce an additional restore point for a machine in the backup job and do not want to configure a new job or modify the existing one. For more information on quick backup, see the Quick Backup section of the Veeam Backup & Replication User Guide.

Before You Begin

Before you perform quick backup for a machine, consider the following considerations and limitations:

- The machine (physical or virtual) must be processed by a regular backup job or Veeam Agent backup job managed by the backup server.

  Quick backup is not available for VMware Cloud Director VMs processed with VMware Cloud Director jobs.
- A backup job processing the machine must exist on the backup server.
- A full backup file for the machine must exist in the backup repository.
- You cannot perform quick backup for multiple machines simultaneously if the machines are processed by the same backup job.

Performing Quick Backup

To perform quick backup, do the following:

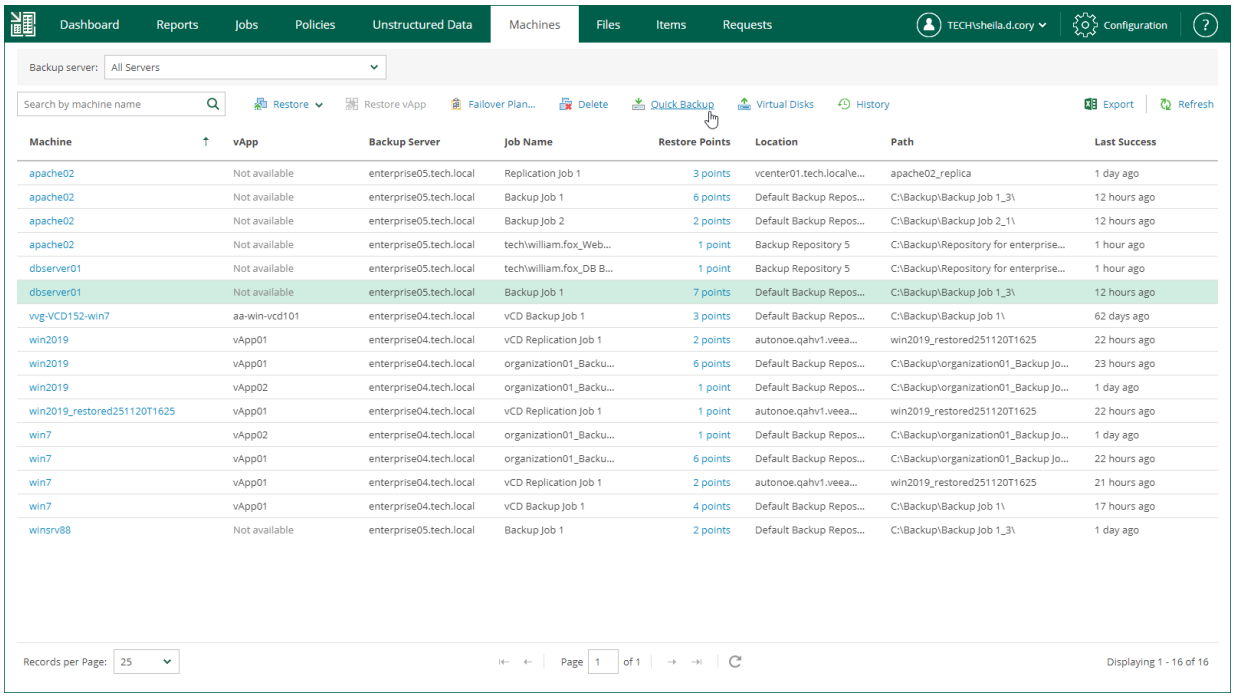
1. On the **Machines** tab, select the necessary machine.
2. On the toolbar, click **Quick Backup**.

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

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

1. On **Jobs** tab, select the backup job that processes the machine.
2. Click the job status link in the **Status** column.

3. To view the session log, on the opened **Reports** tab, select the machine.



VM Recovery

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

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

- Instant Recovery
- Entire VM Restore
- Virtual Disk Restore
- VM Failover
- Failover Plans

Instant Recovery

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

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

- Instant recovery of VMware vSphere VMs to VMware vSphere
- Instant recovery of VMware Cloud Director VMs to VMware Cloud Director
- Instant recovery of Microsoft Hyper-V VMs to Microsoft Hyper-V

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

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

Supported Backup Types

You can recover workloads from the following types of backups:

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

Instant Recovery to VMware vSphere

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

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

Performing Instant Recovery to VMware vSphere

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

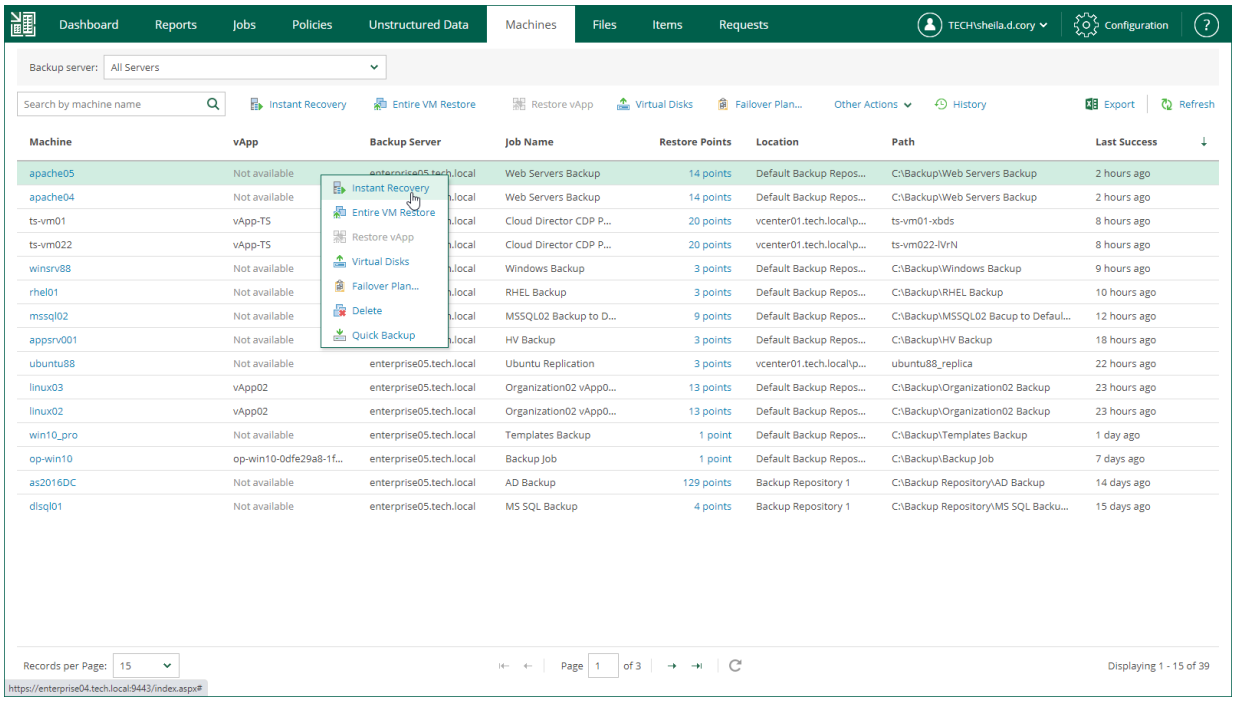
1. Launch the Instant Recovery wizard.
2. Select a restore point.
3. Select a recovery mode.
4. Specify destination settings for the recovered VM.
5. Specify target datastore.
6. Review the recovery settings.

Step 1. Launch Instant Recovery Wizard

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

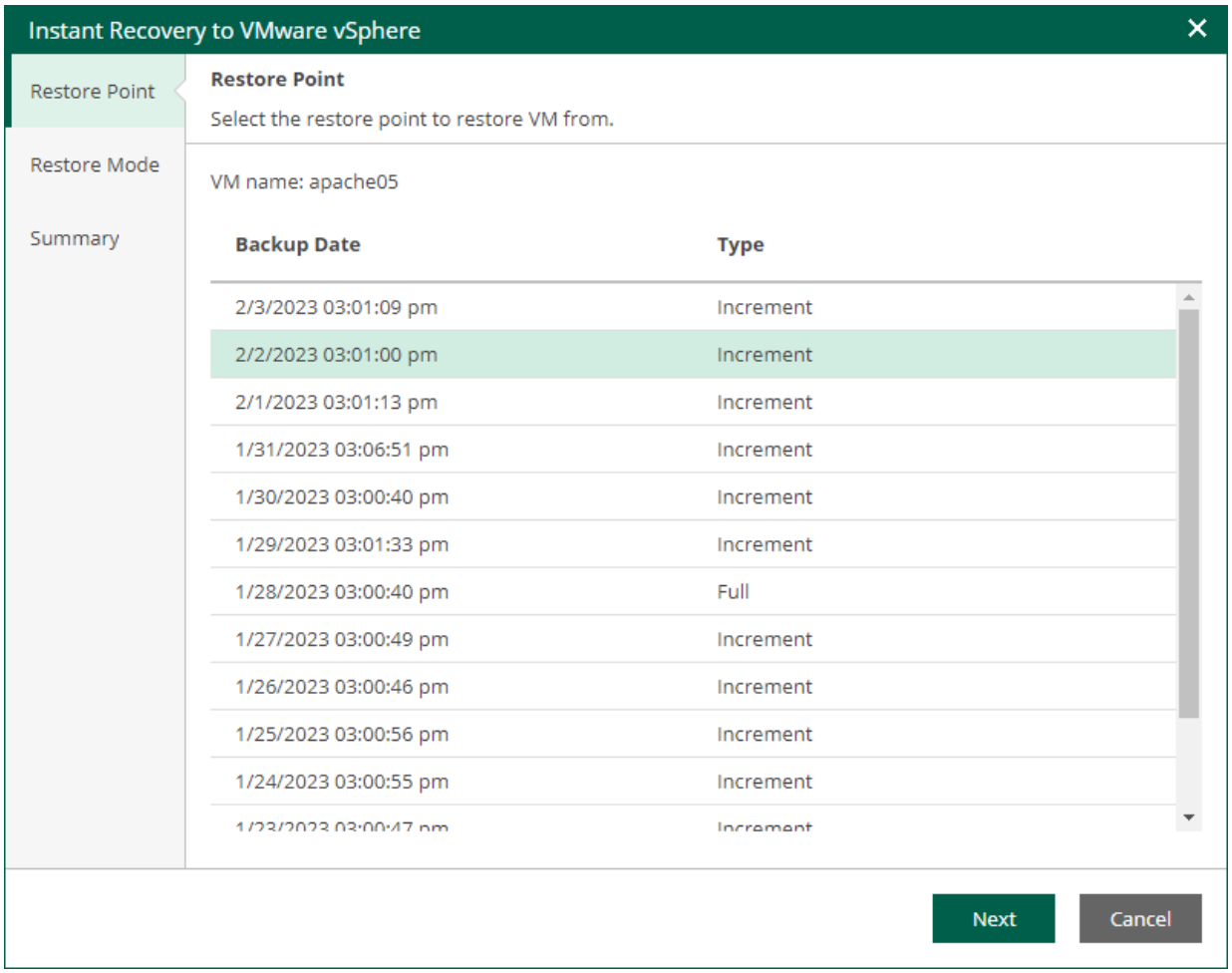
1. On the **Machines** tab, select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Instant Recovery**.

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



Step 2. Select Restore Point

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



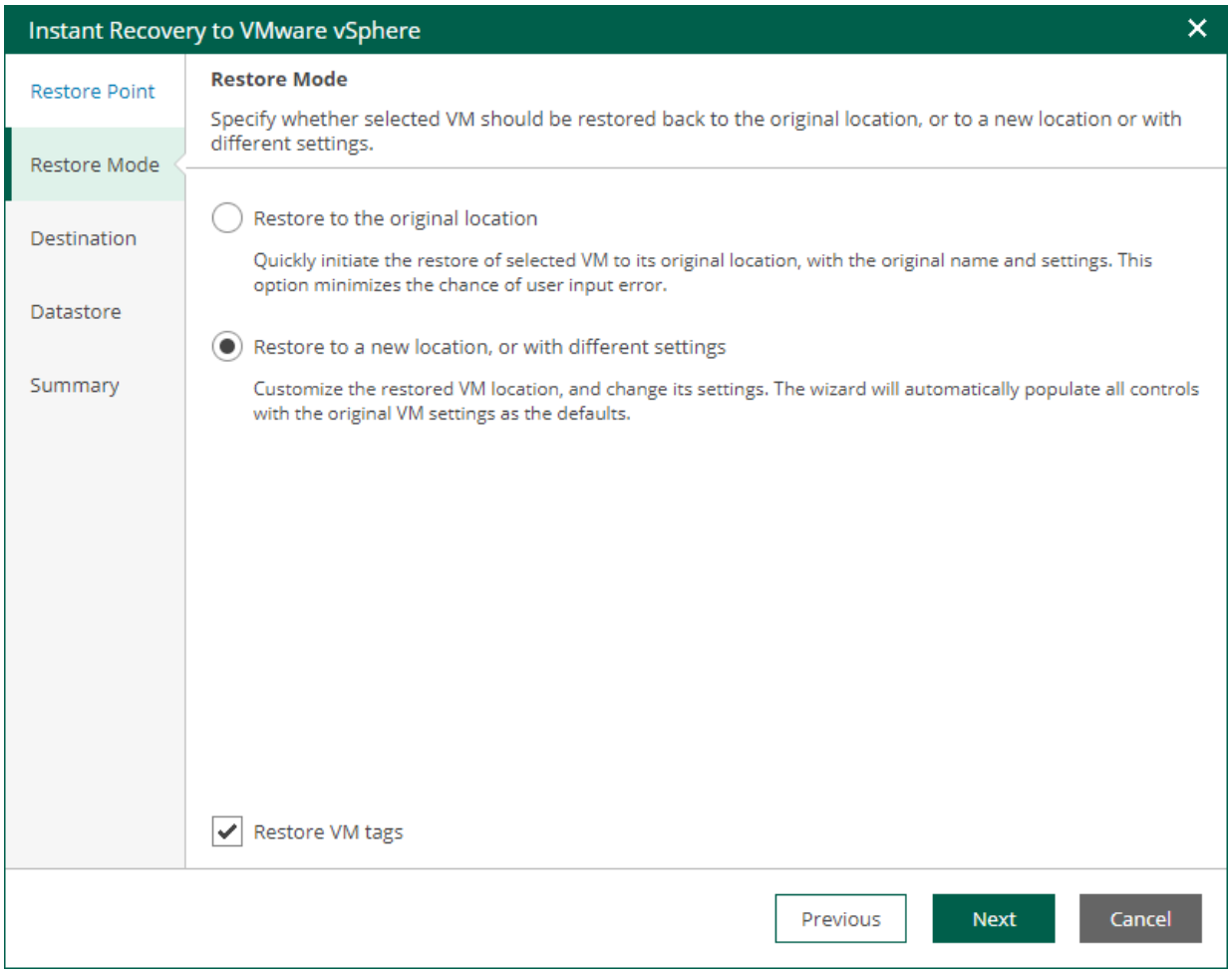
Step 3. Select Recovery Mode

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

1. Select a destination for recovery:
   - Select **Restore to the original location** to recover the VM with initial settings to the original location. If this option is selected, you will pass directly to the Summary step of the wizard.

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

   - Select **Restore to a new location or with different settings** to recover the VM to a new location, or to any location but with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.
2. If you want to recover tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will recover the VM with original tags if the following conditions are met:
   - You recover a VM to the original location.
   - The original VM tags are available on the source vCenter Server.



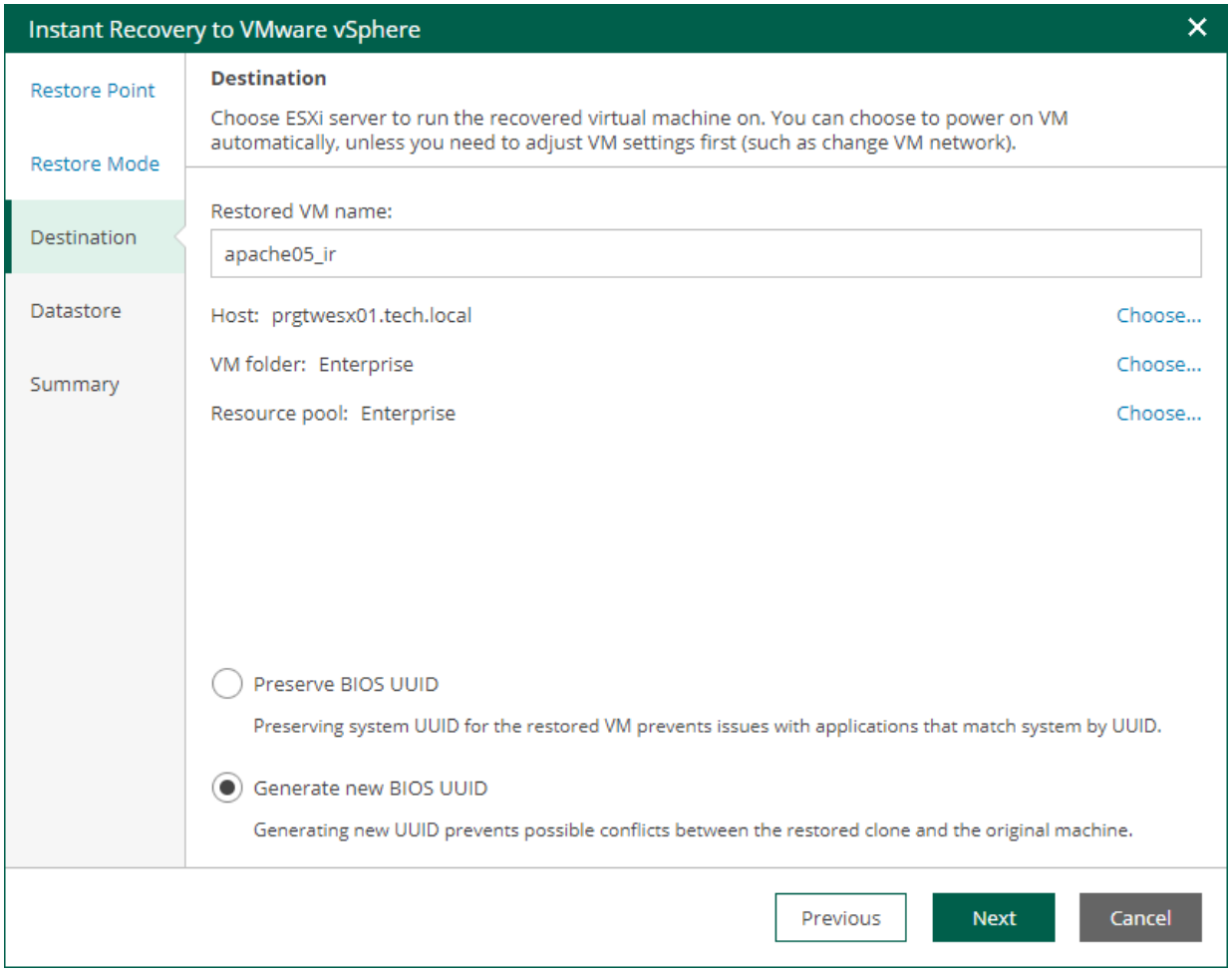
Step 4. Specify Destination Settings

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

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

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

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



Step 5. Specify Datastore

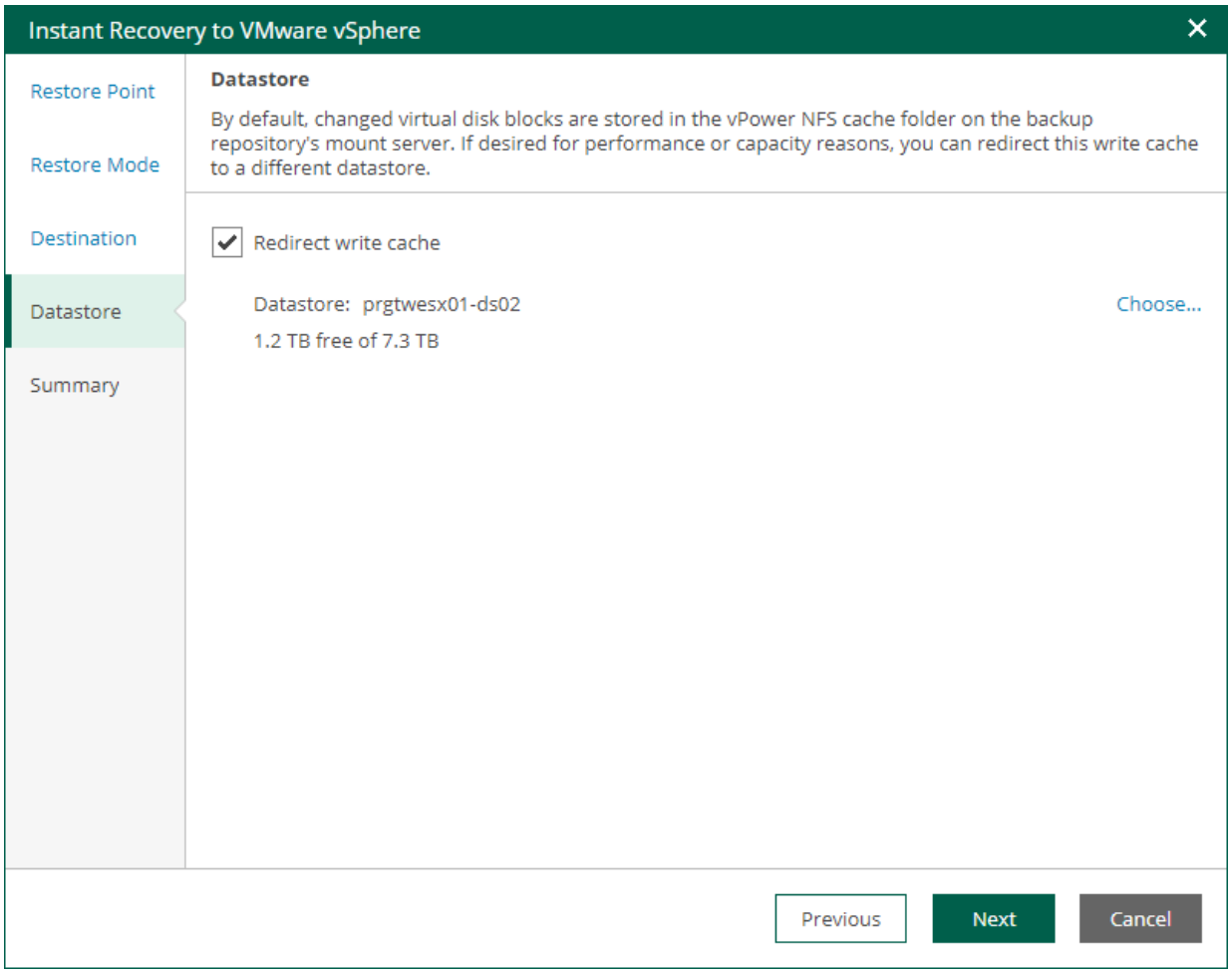
The **Datastore** step of the wizard is available if you recover a VM to a new location or with different settings.

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

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

To redirect redo logs, do the following:

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



Step 6. Review Recovery Settings

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

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

   If you recover a VM for testing disaster recovery while the original VM is still running, leave this check box unselected. Before you power on the recovered VM, you must disconnect it from the production network and connect to a non-production network to avoid conflicts.

2. To start the VM right after recovery, select the **Power on target VM after restoring** check box. If you recover the workloads to the production network, make sure that the original VM is powered off.

3. Review the settings that you have specified for Instant Recovery and click **Finish**.

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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

After you have performed instant file share recovery, you have to finalize it. For more information, see Finalizing Instant Recovery to VMware vSphere.

What You Do Next

After you have performed instant file share recovery, you have to finalize it. For more information, see Finalizing Instant Recovery to VMware vSphere.

Finalizing Instant Recovery to VMware vSphere

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

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

Testing Recovered VM

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

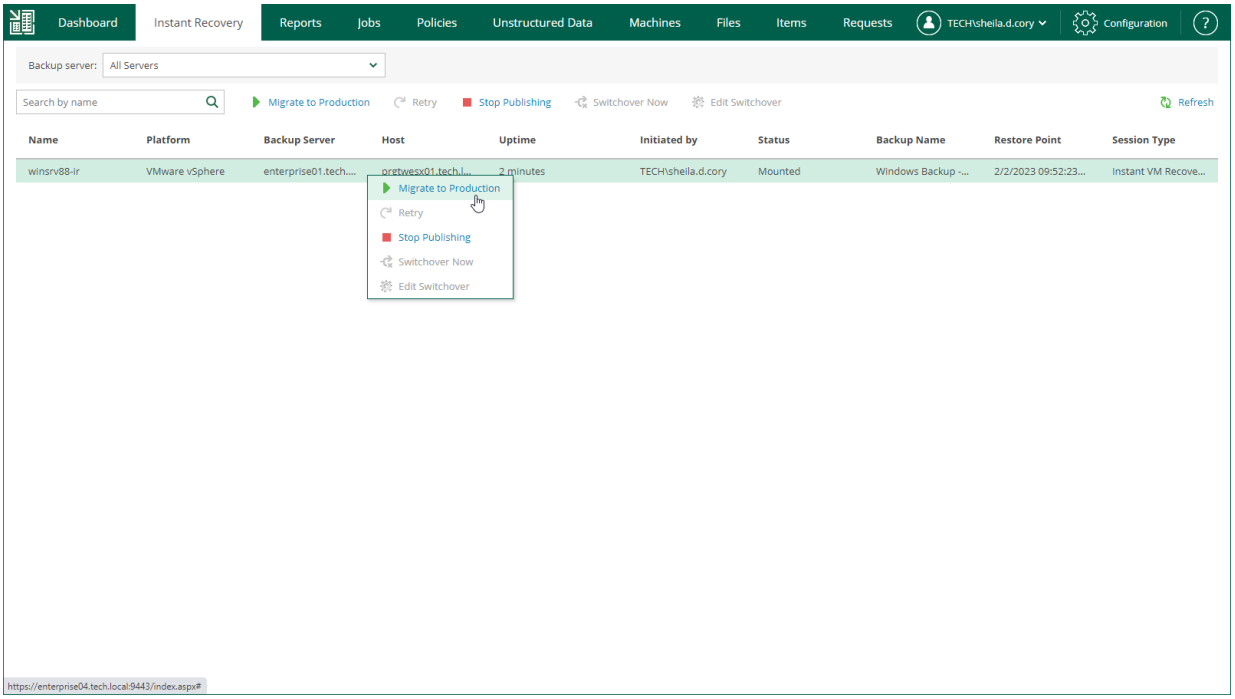
Migrating Recovered VM

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

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

1. Open the **Instant Recovery** tab and select the necessary VMware vSphere VM from the list.

2. On the toolbar, click **Migrate to production**.



3. At the **Destination** step of the **VMware Cloud Director Quick Migration** wizard, specify destination where you want to migrate the VM.

   a. Click **Choose** next to the **Host** field and select an ESXi host or cluster where the relocated VM must be registered.

   b. Click **Choose** next to the **VM folder** field and select the target VM folder.

   c. Click **Choose** next to the **Resource pool** field and select the target resource pool.

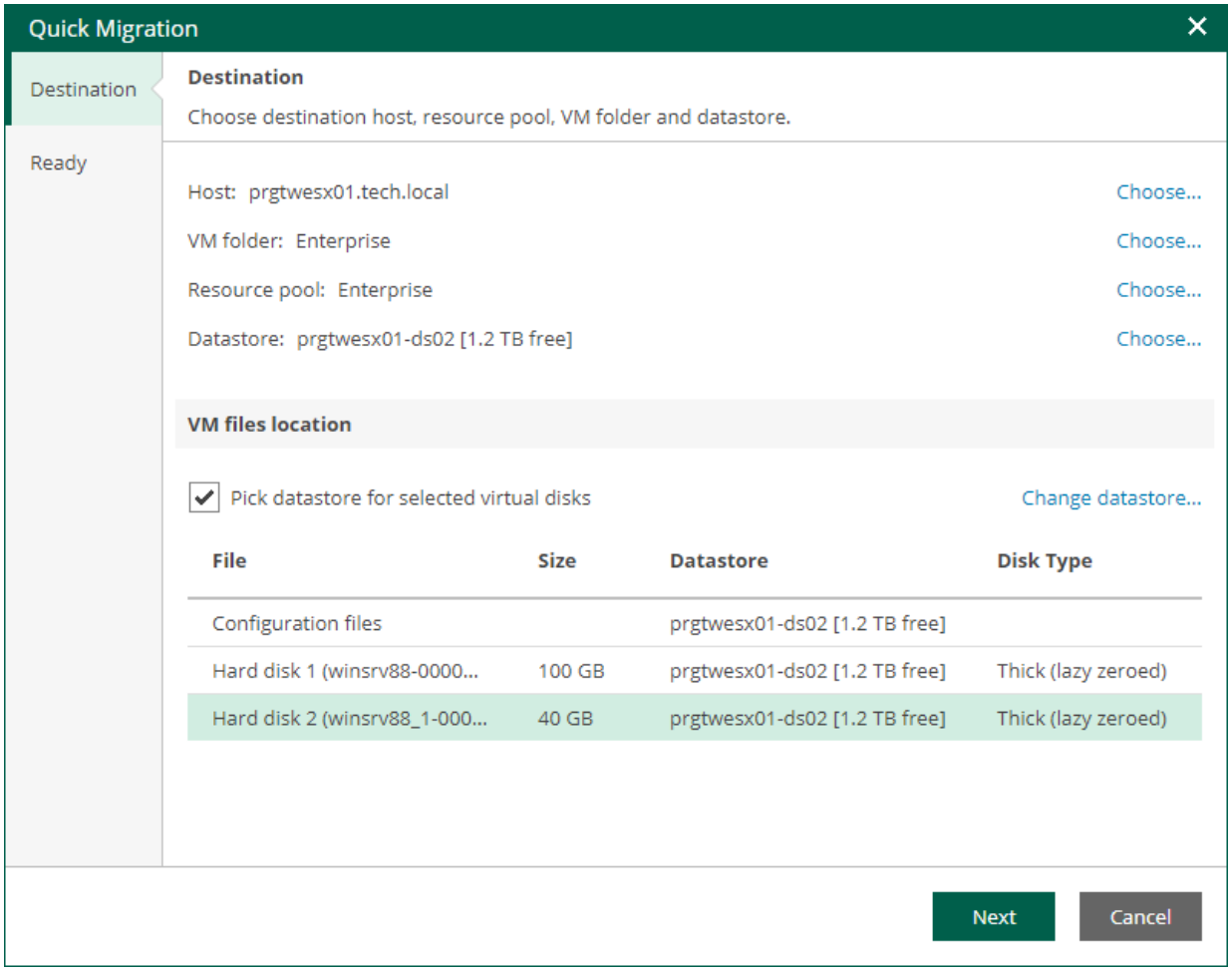
   d. Click **Choose** next to the **Datastore** field and select the target datastore.

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

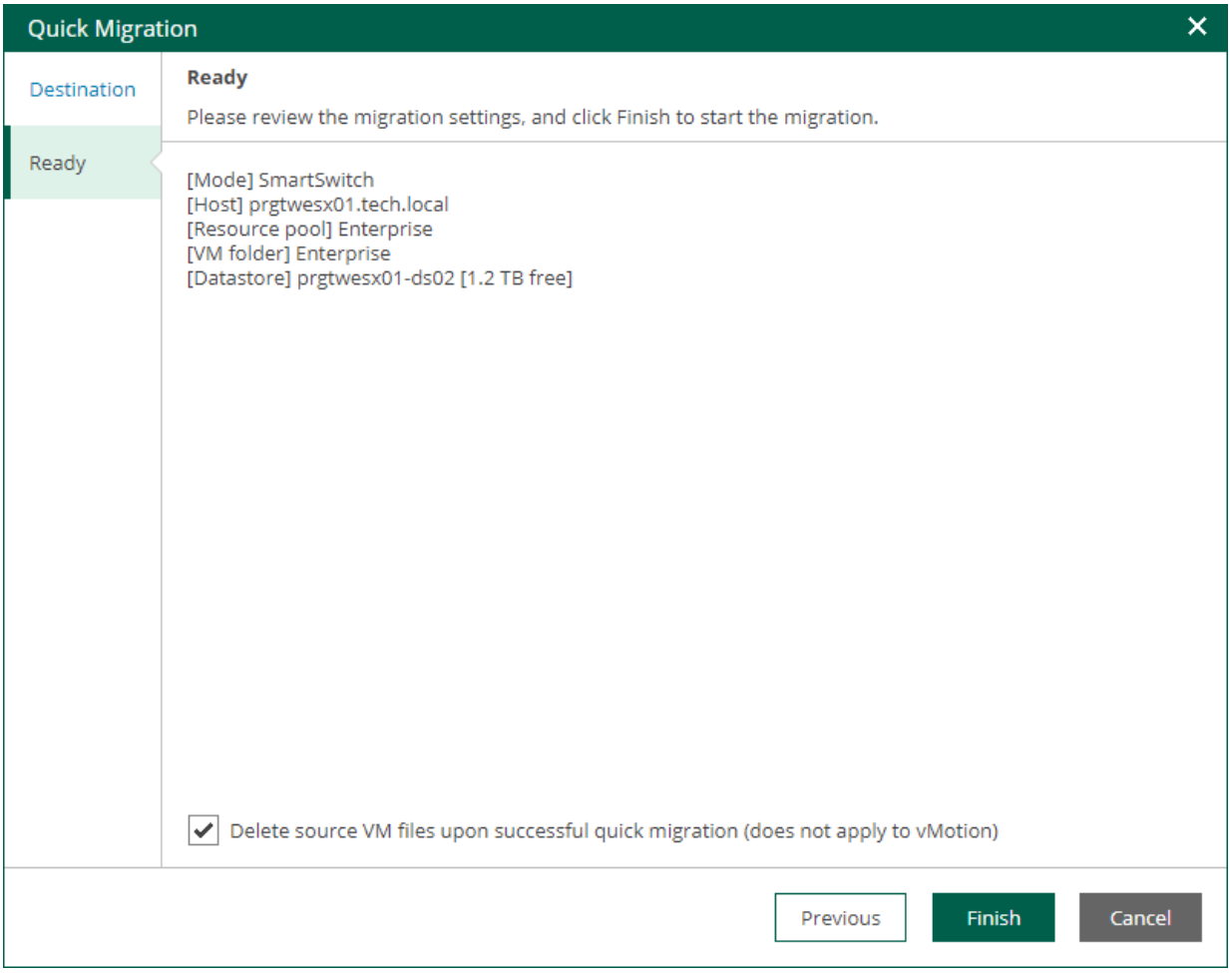
      i. Select the **Pick datastore for selected virtual disks** check box.

      ii. Select the configuration files or one of the hard disks and click **Change datastore**.

iii. In the **Add objects** window, choose the necessary datastore and click **OK**.



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



Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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

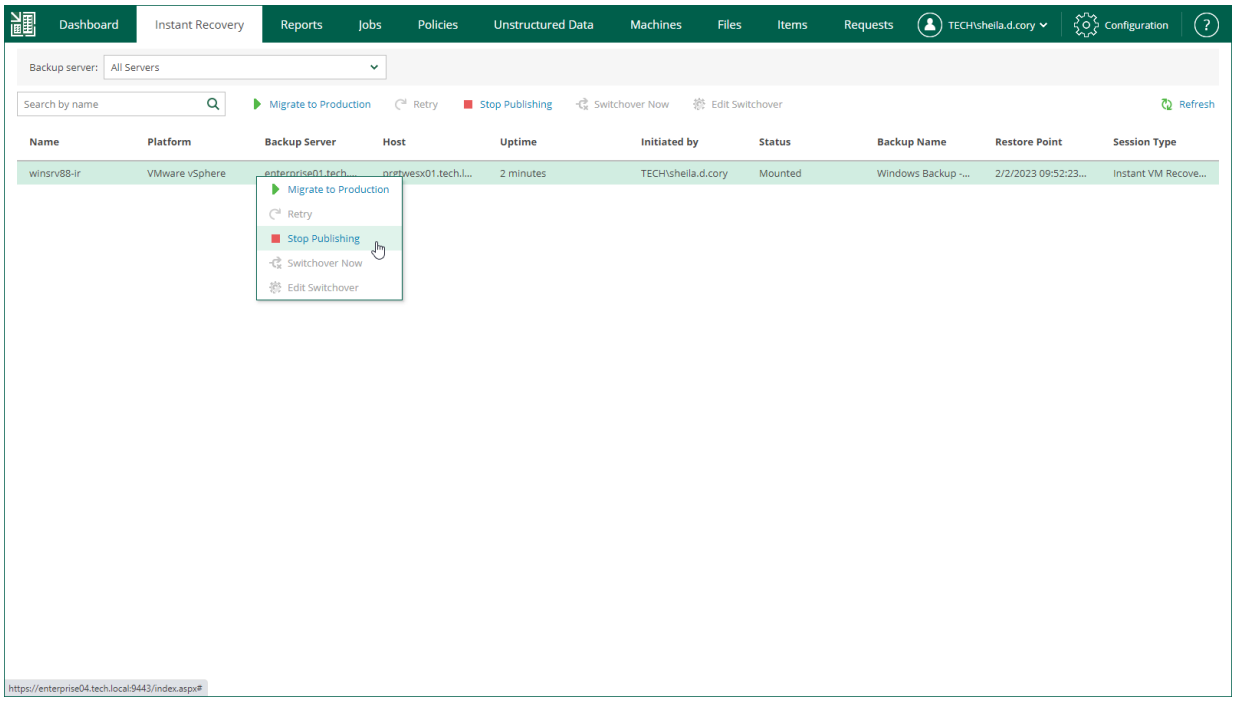
Unpublishing Recovered VM

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

To remove a recovered VM, do the following:

1. Open the **Instant Recovery** tab and select the necessary VMware vSphere VM from the list.

2. On the toolbar, click **Stop Publishing**.



Instant Recovery to VMware Cloud Director

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

For more information on Instant Recovery, see the Performing Instant Recovery to Cloud Director vApp section of the Veeam Backup & Replication User Guide.

Performing Instant Recovery to VMware Cloud Director

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

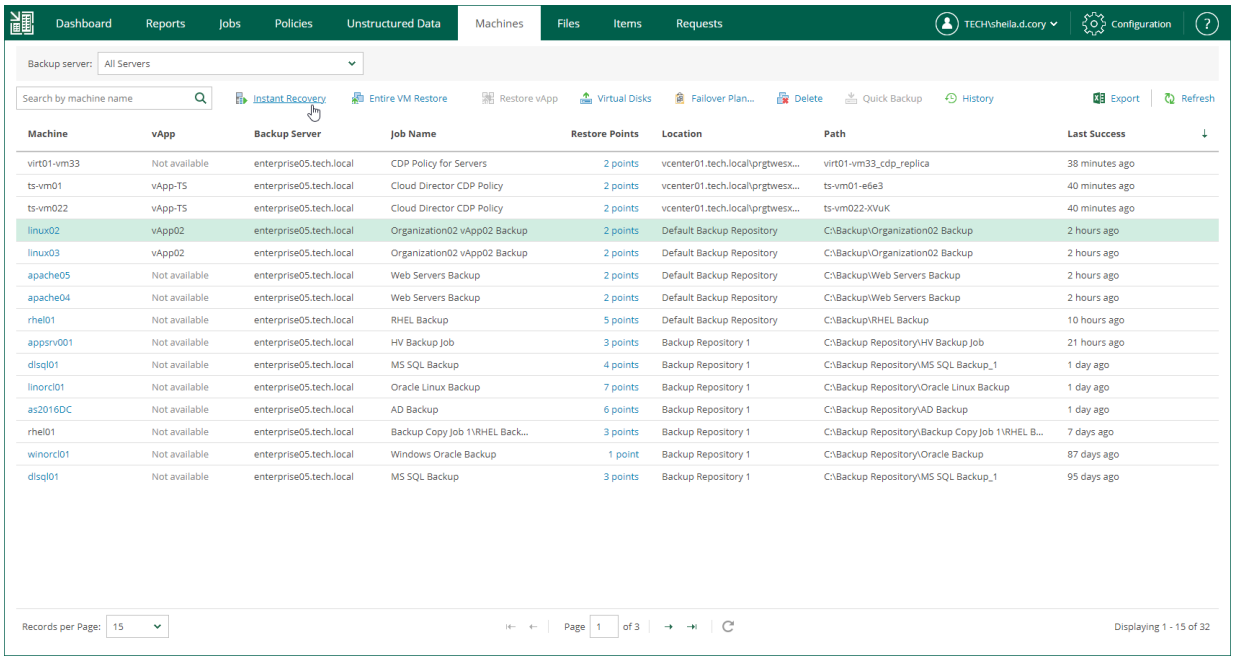
1. Launch the Instant Recovery to VMware Cloud Director wizard.
2. Select a restore point.
3. Select a recovery mode.
4. Specify destination settings for the recovered VM.
5. Specify target datastore.
6. Configure network mapping.
7. Review the recovery settings.

Step 1. Launch Instant Recovery Wizard

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

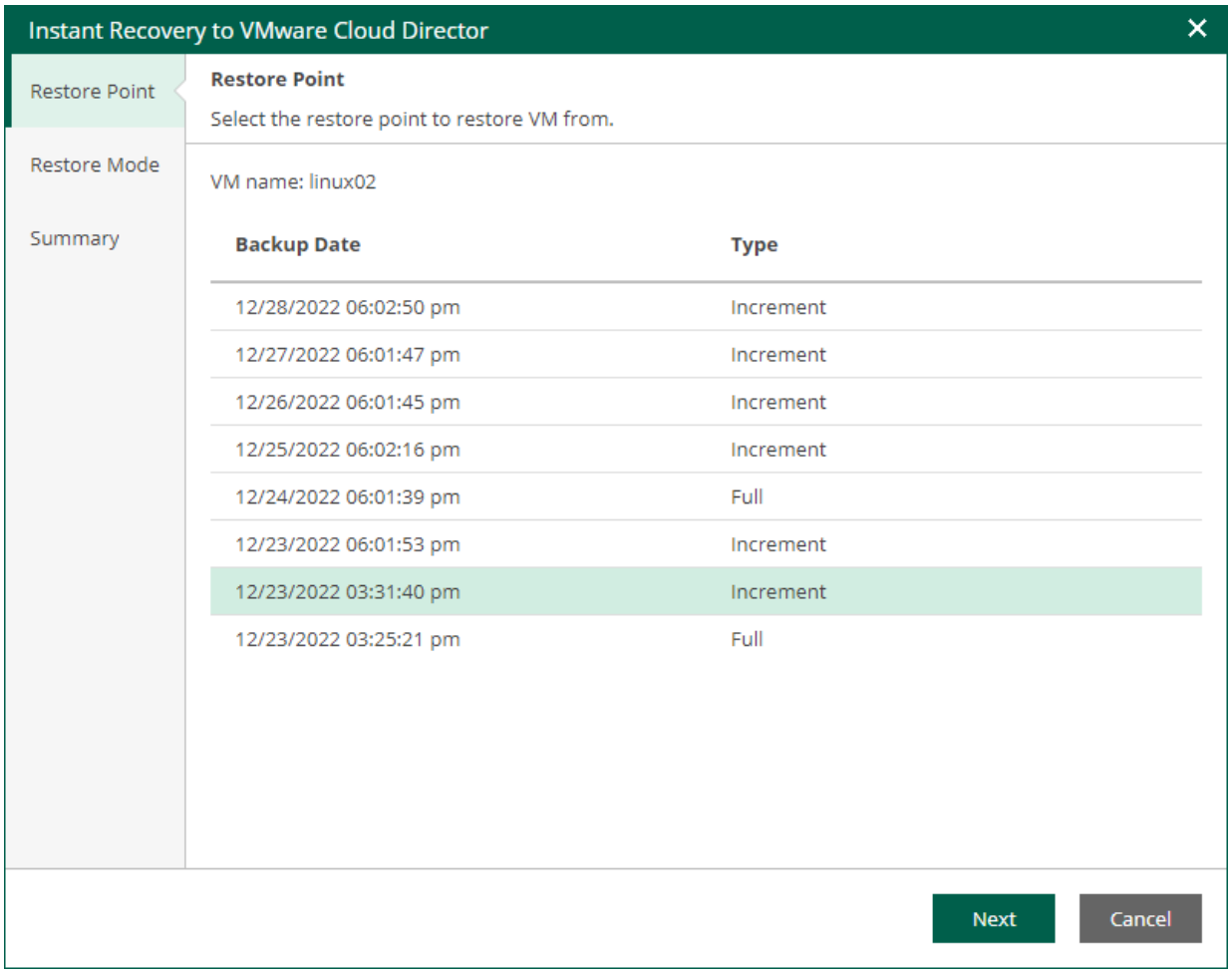
1. On the **Machines** tab, select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Instant Recovery**.

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



Step 2. Select Restore Point

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



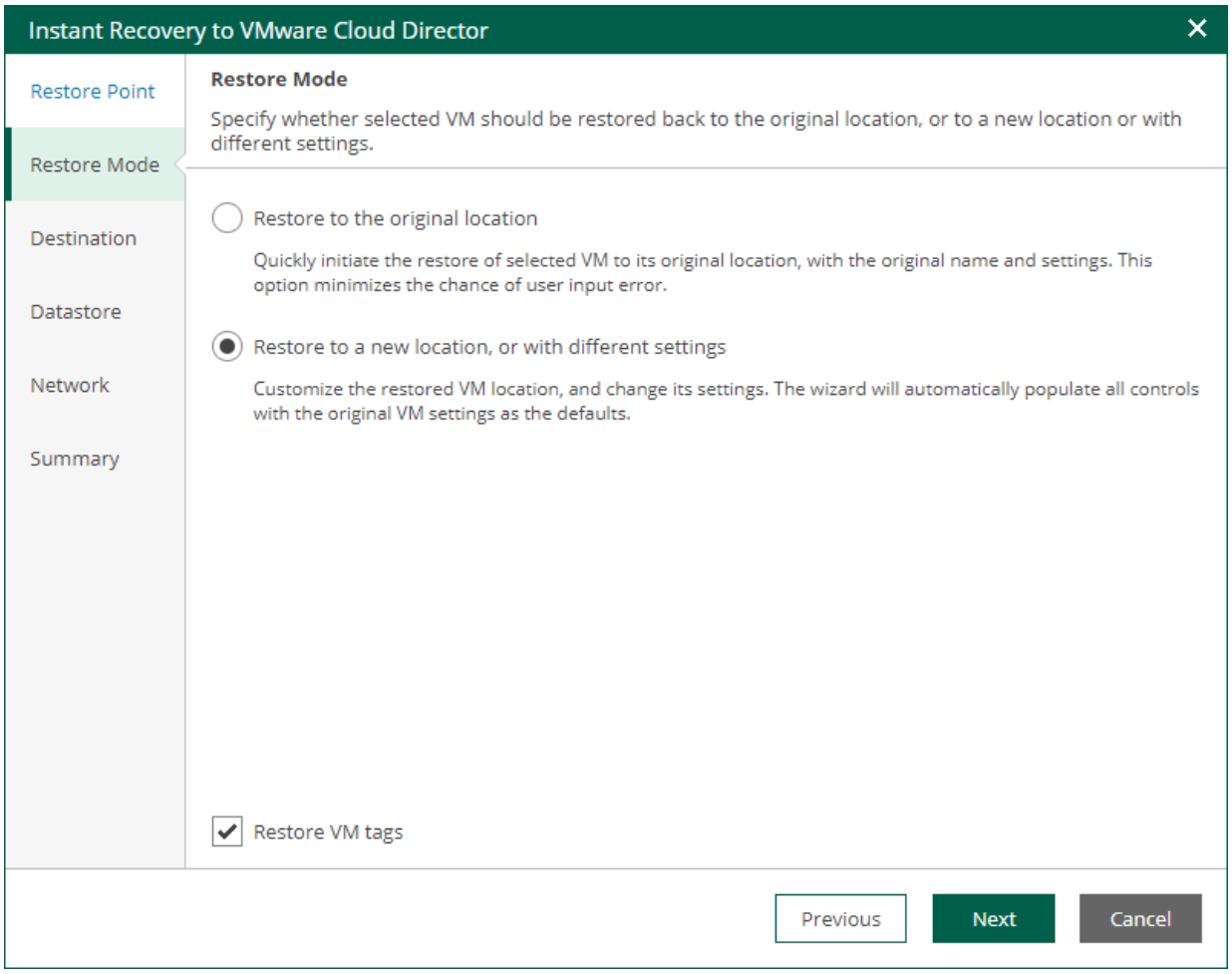
Step 3. Select Recovery Mode

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

1. Select a destination for recovery:
   - Select **Restore to the original location** to recover the VM with initial settings and to the original location. If this option is selected, you will pass directly to the Summary step of the wizard.

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

   - Select **Restore to a new location or with different settings** to recover the VM to a new location, or to any location but with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.
2. If you want to recover tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will recover the VM with original tags if the following conditions are met:
   - You recover a VM to the original location.
   - The original VM tags are available on the source vCenter Server.

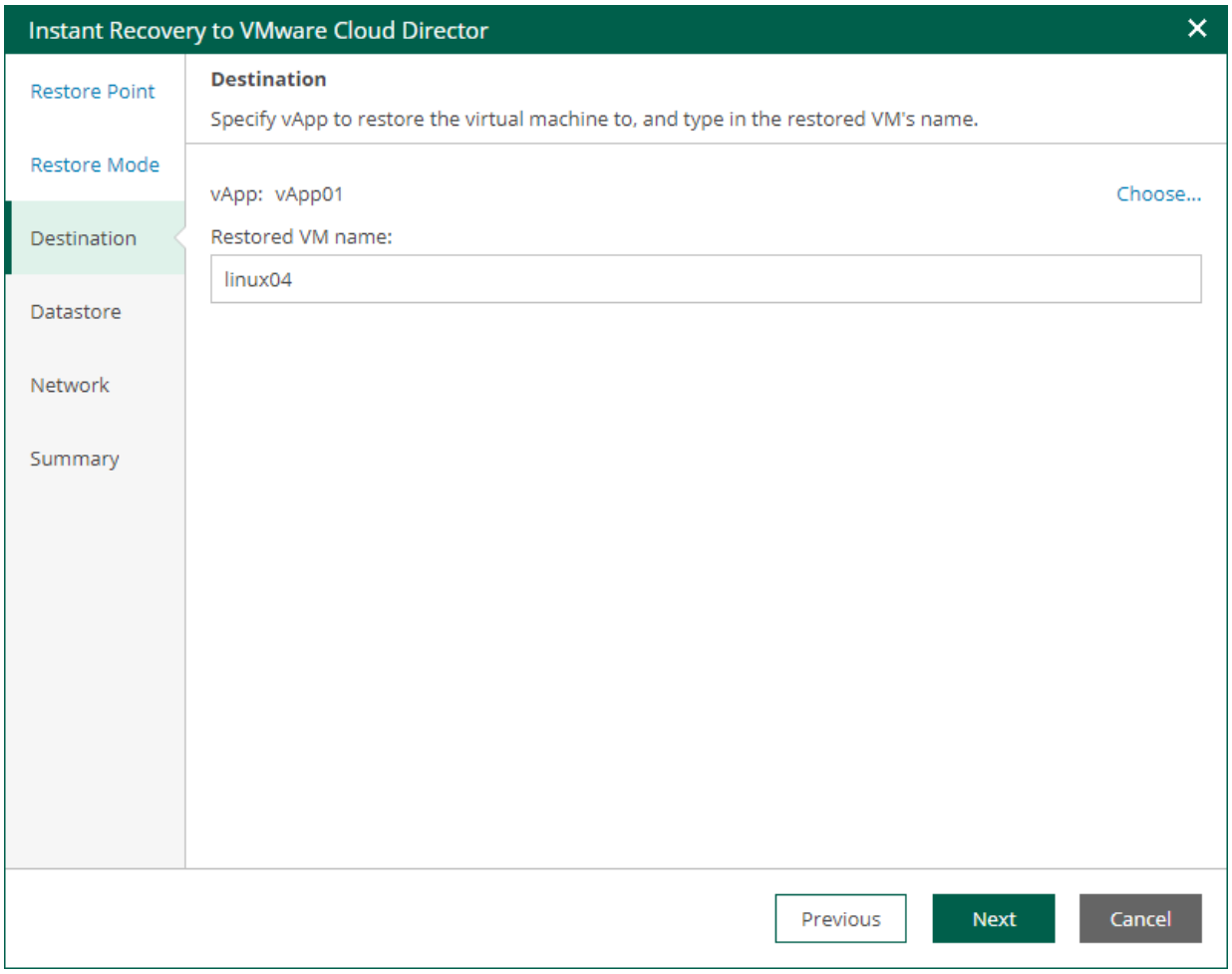


Step 4. Specify Destination Settings

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

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

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



Step 5. Specify Datastore

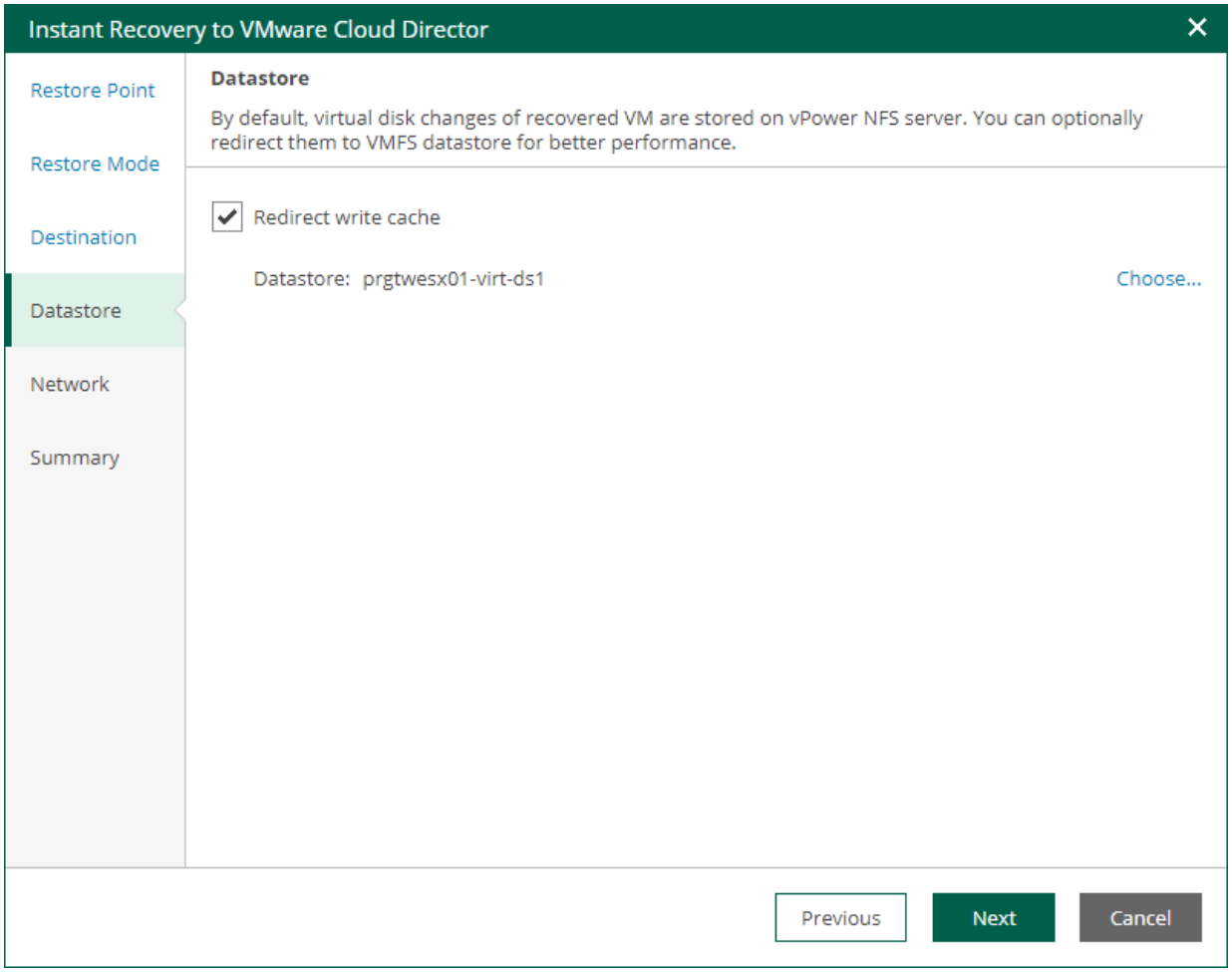
The **Datastore** step of the wizard is available if you recover a VM to a new location or with different settings.

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

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

To redirect redo logs, do the following:

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



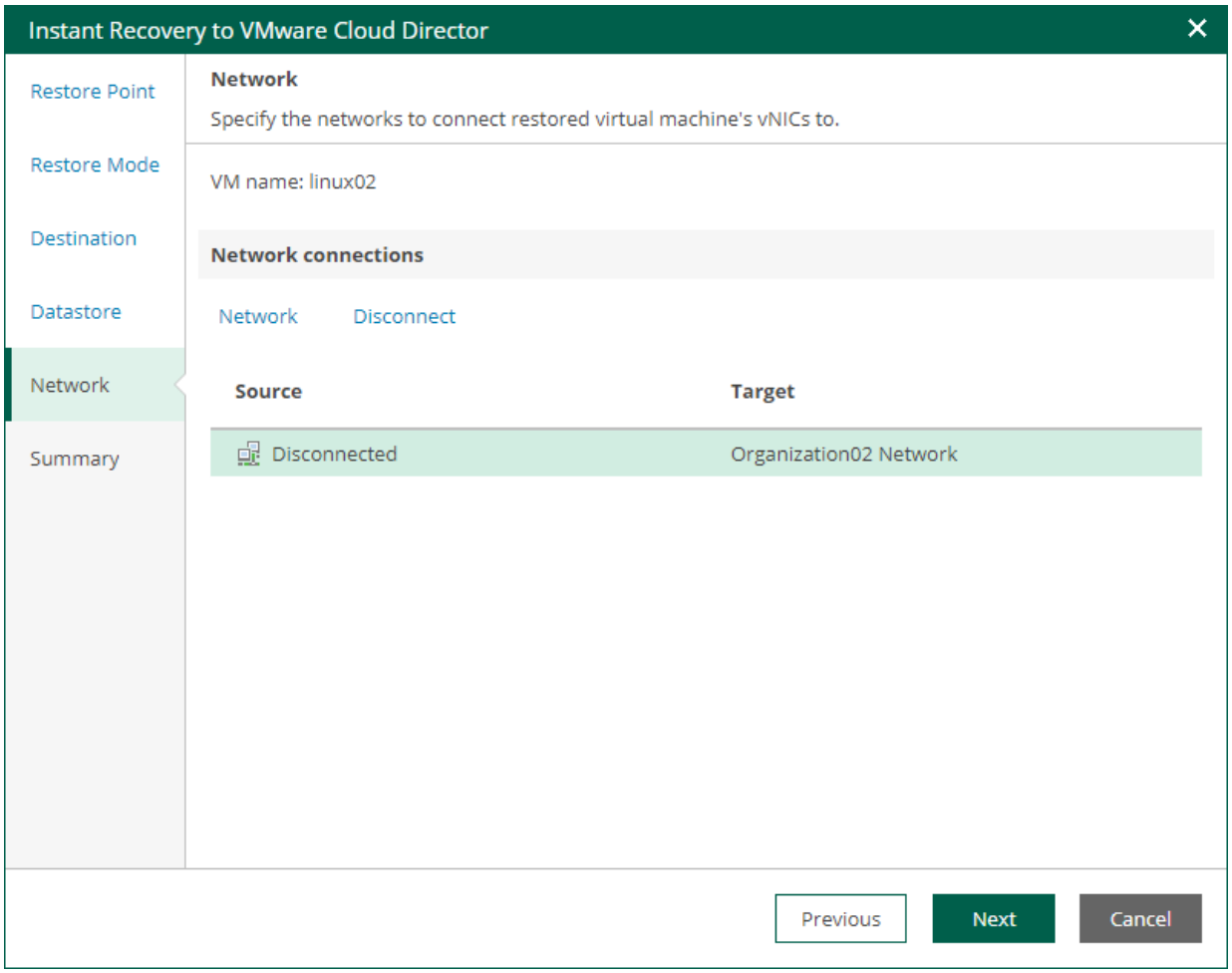
Step 6. Configure Network Mapping

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

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

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

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



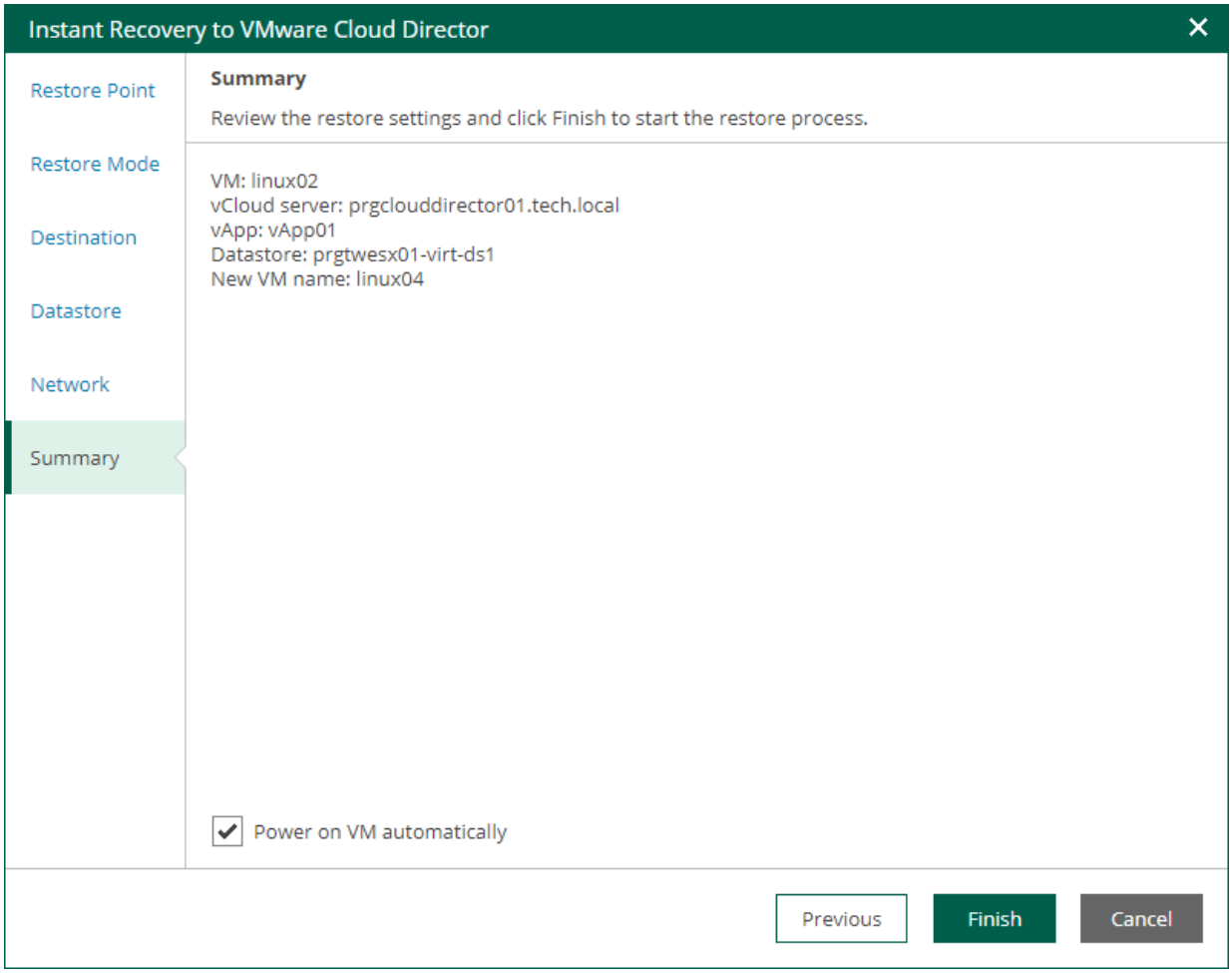
Step 7. Review Recovery Settings

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

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



What You Do Next

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

Finalizing Instant Recovery to VMware Cloud Director

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

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

Testing Recovered VM

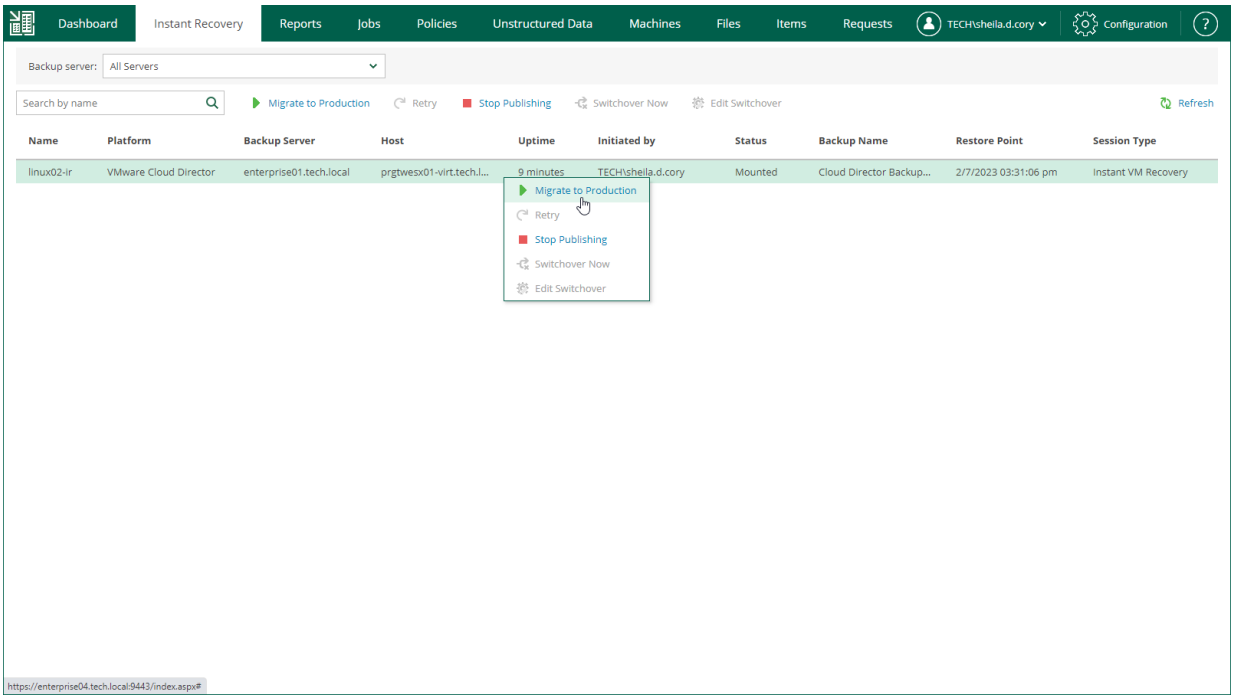
To test a recovered VM before you migrate it to production, you can launch the VMware Remote Console software from the Veeam Backup & Replication console. For more information, see the Finalizing Instant Recovery to VMware vSphere section of the Veeam Backup & Replication User Guide.

Migrating Recovered VM

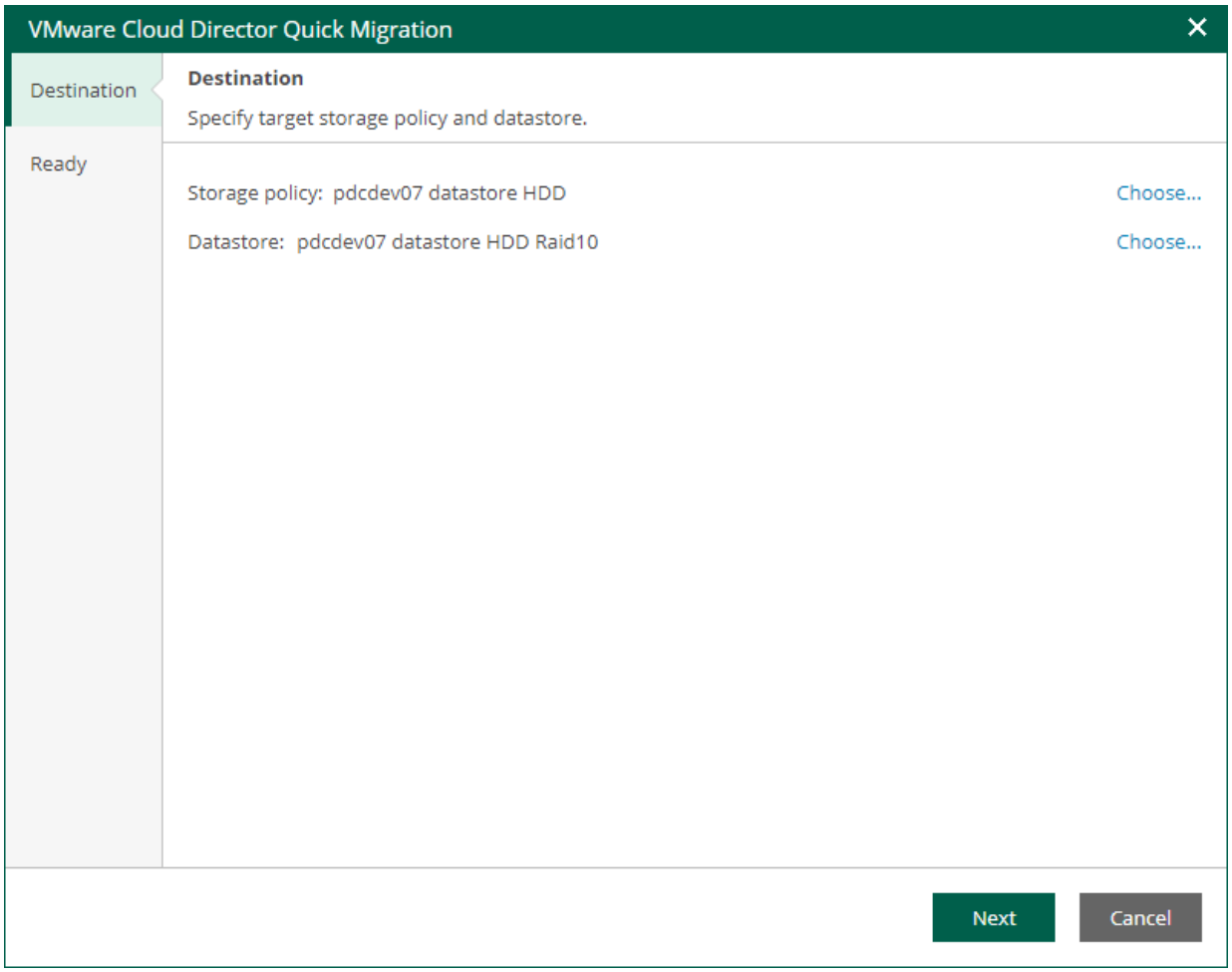
If a VM is recovered successfully, you can migrate it to the production environment.

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

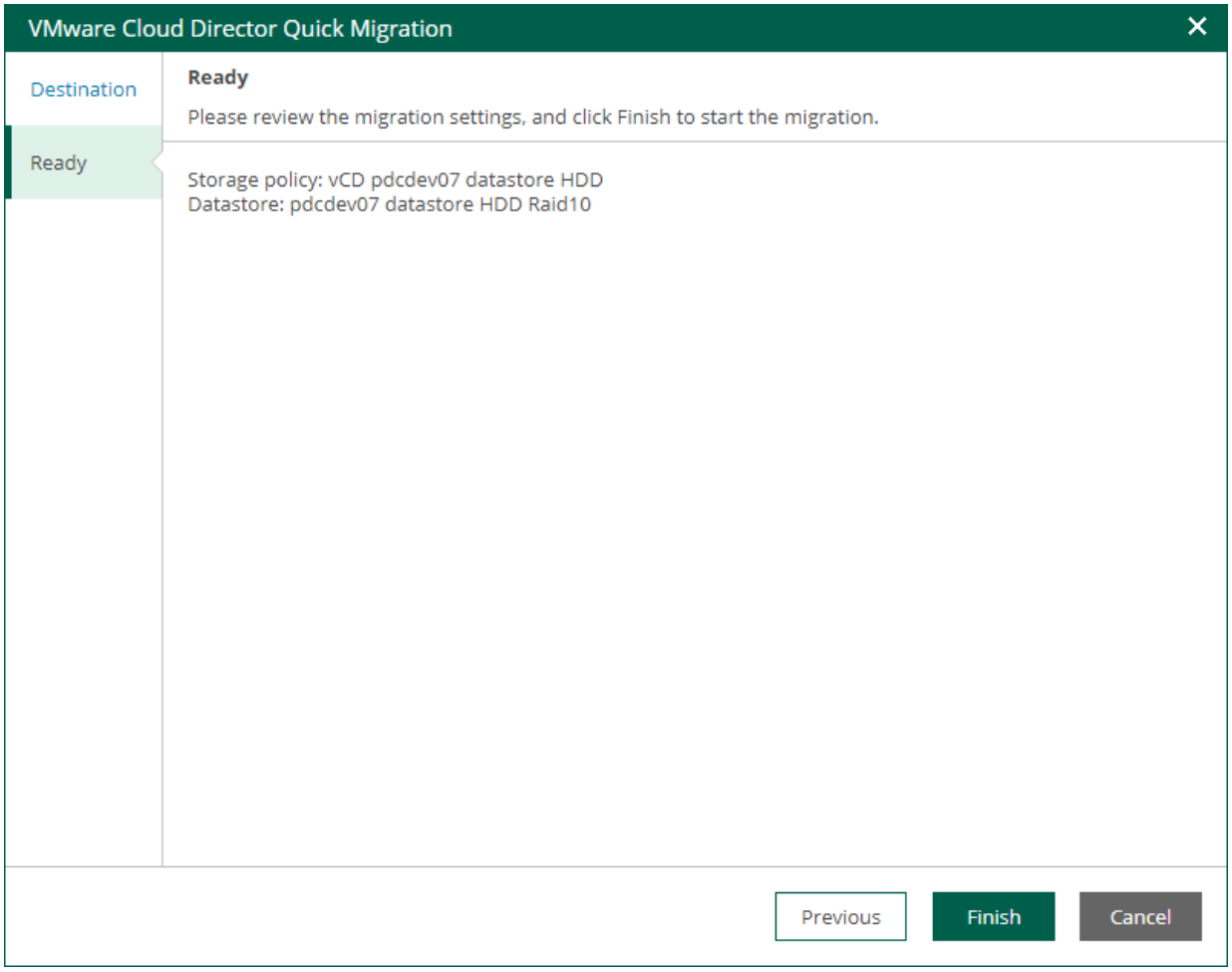
1. Open the **Instant Recovery** tab and select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Migrate to production**.



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



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



Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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

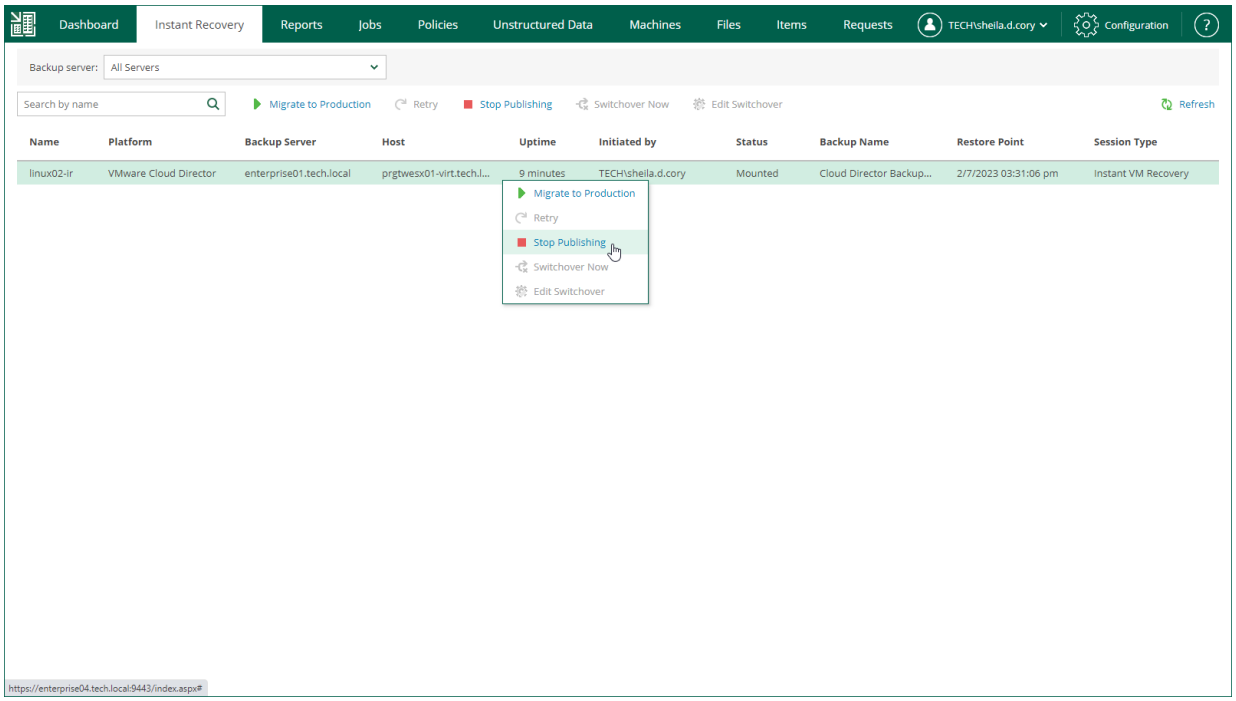
Unpublishing Recovered VM

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

To remove a recovered VM, do the following:

1. Open the **Instant Recovery** tab and select the necessary VMware Cloud Director VM from the list.

2. On the toolbar, click **Stop Publishing**.



Instant Recovery to Microsoft Hyper-V

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

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

Performing Instant Recovery to Microsoft Hyper-V

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

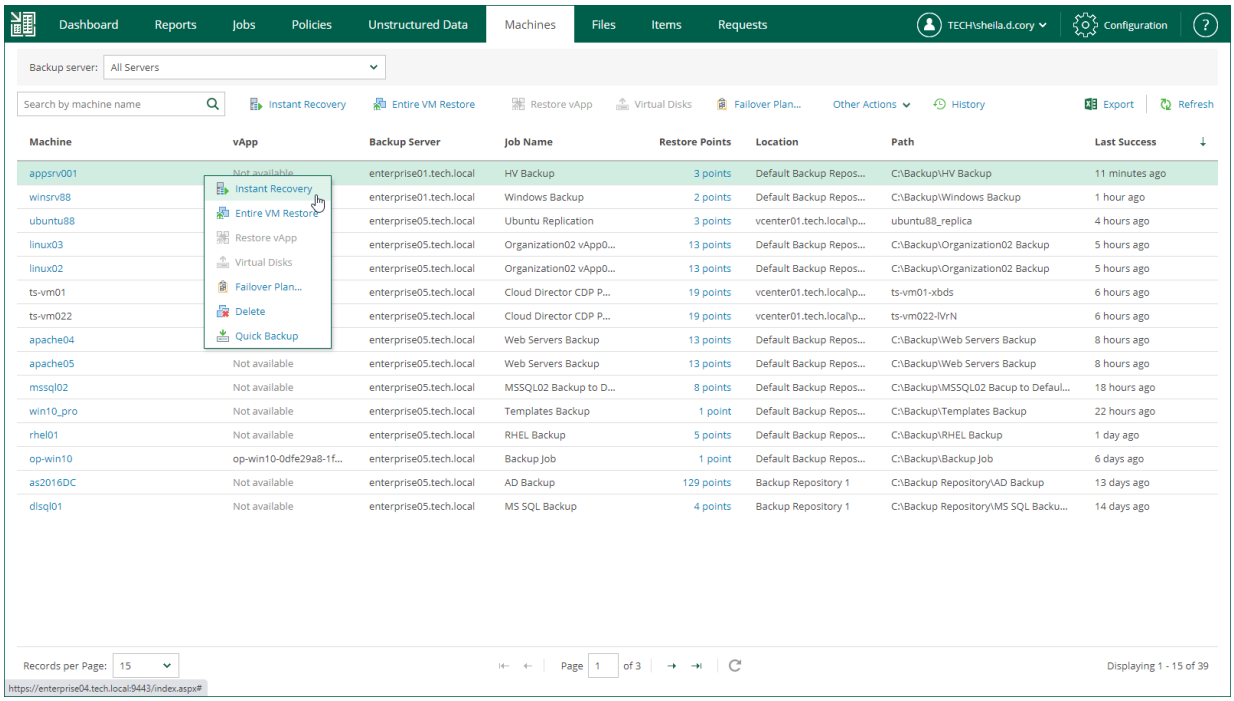
1. Launch the Instant Recovery wizard.
2. Select a restore point.
3. Select a recovery mode.
4. Specify destination settings for the recovered VM.
5. Specify a target datastore.
6. Configure network mapping.
7. Review the recovery settings.

Step 1. Launch Instant Recovery Wizard

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

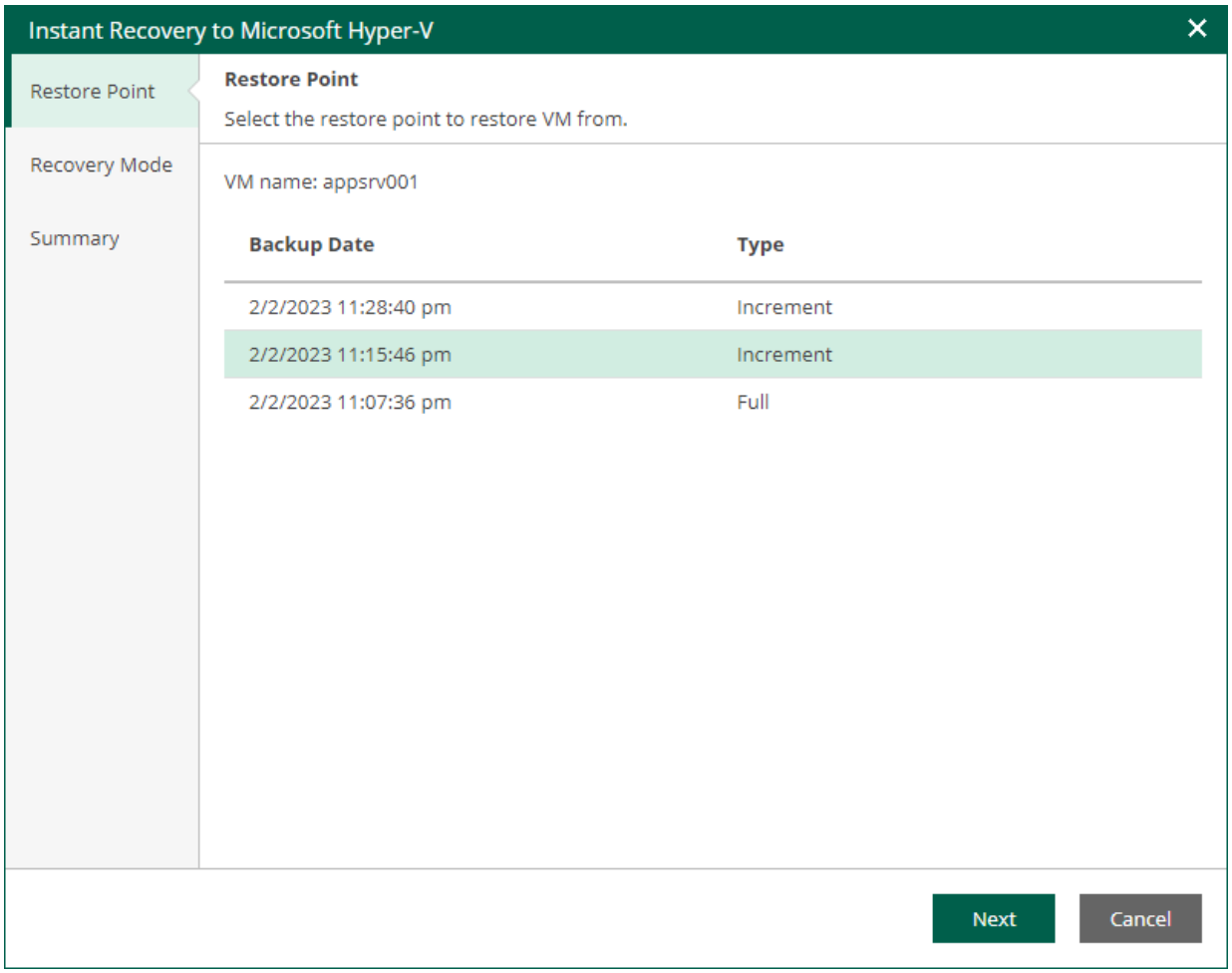
1. On the **Machines** tab, select the necessary Hyper-V VM from the list.
2. On the toolbar, click **Instant Recovery**.

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



Step 2. Select Restore Point

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



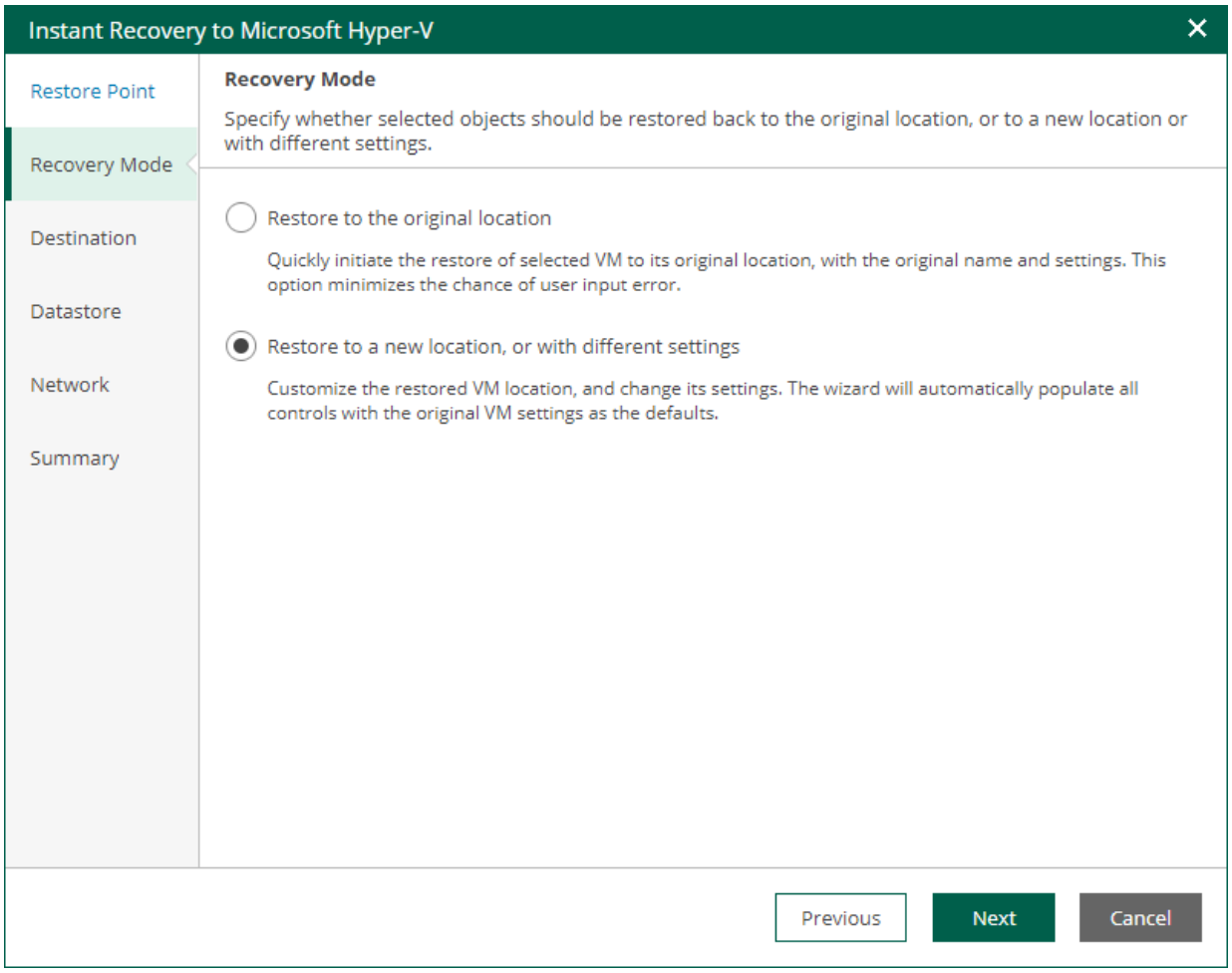
Step 3. Select Recovery Mode

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

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

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

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



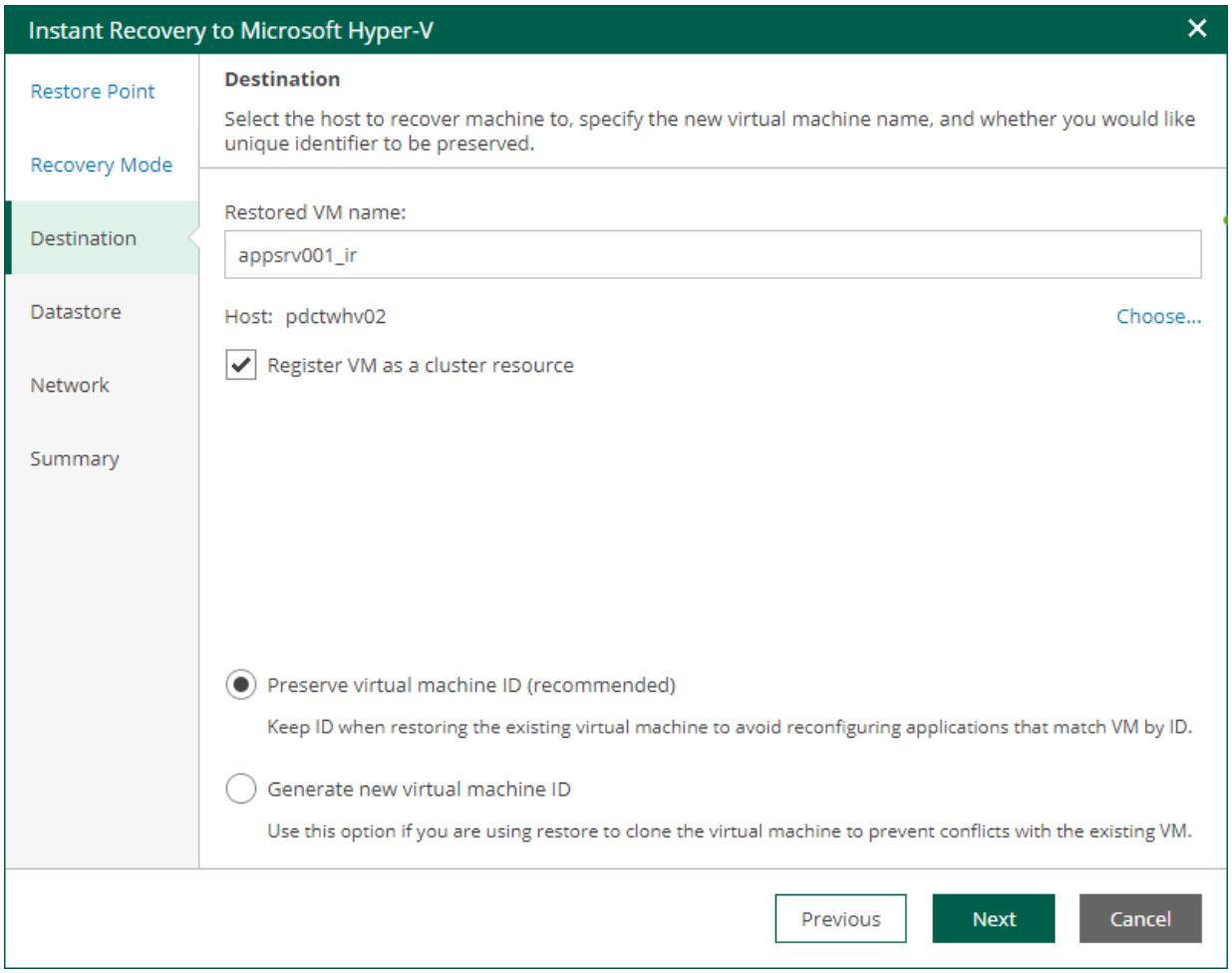
Step 4. Specify Destination Settings

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

To configure destination settings, do the following:

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

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



Step 5. Specify Datastore

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

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

To change a default path, do the following:

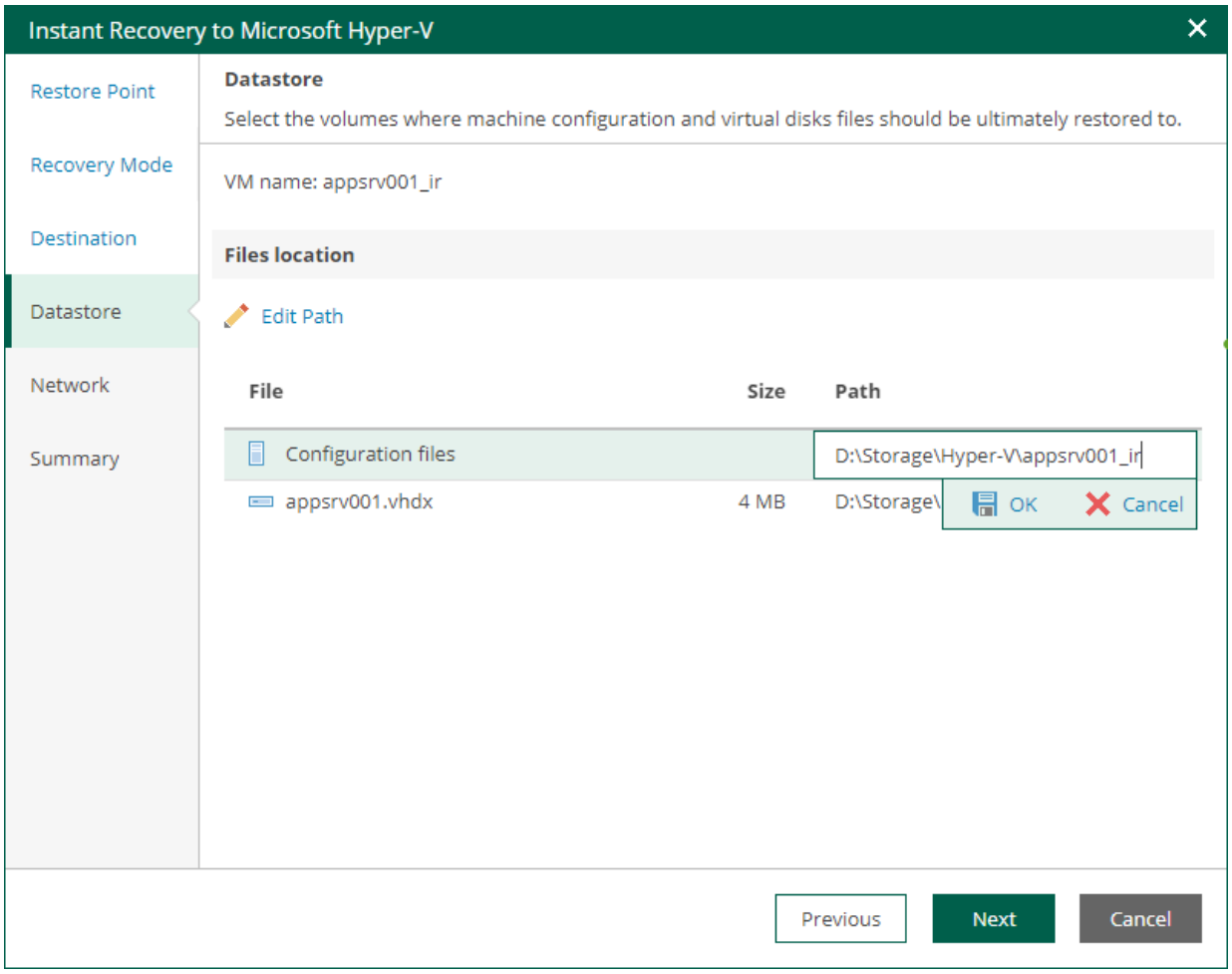
1. Select the configuration files or one of the disk files and click **Edit Path**.

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

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

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

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



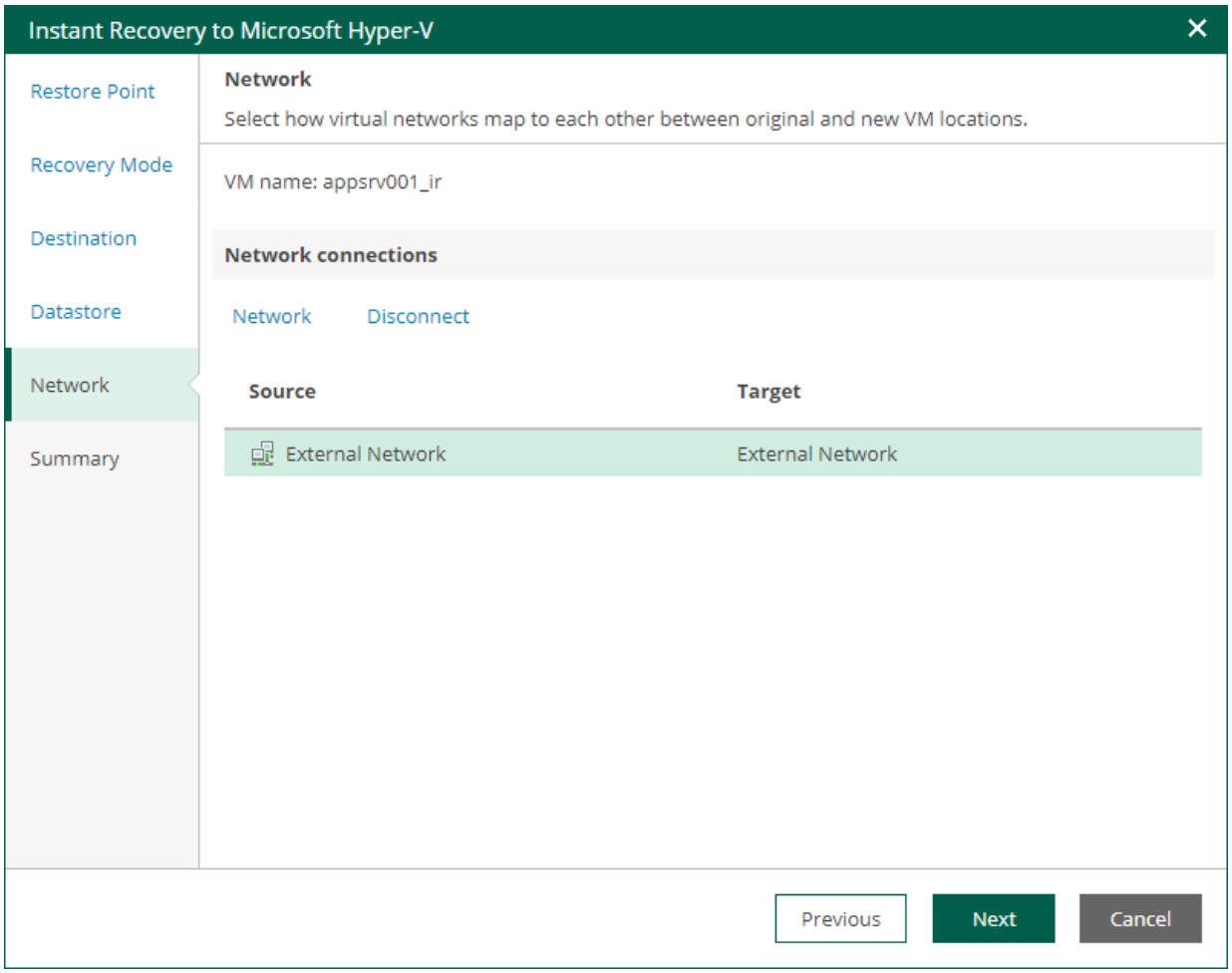
Step 6. Configure Network Mapping

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

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

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

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



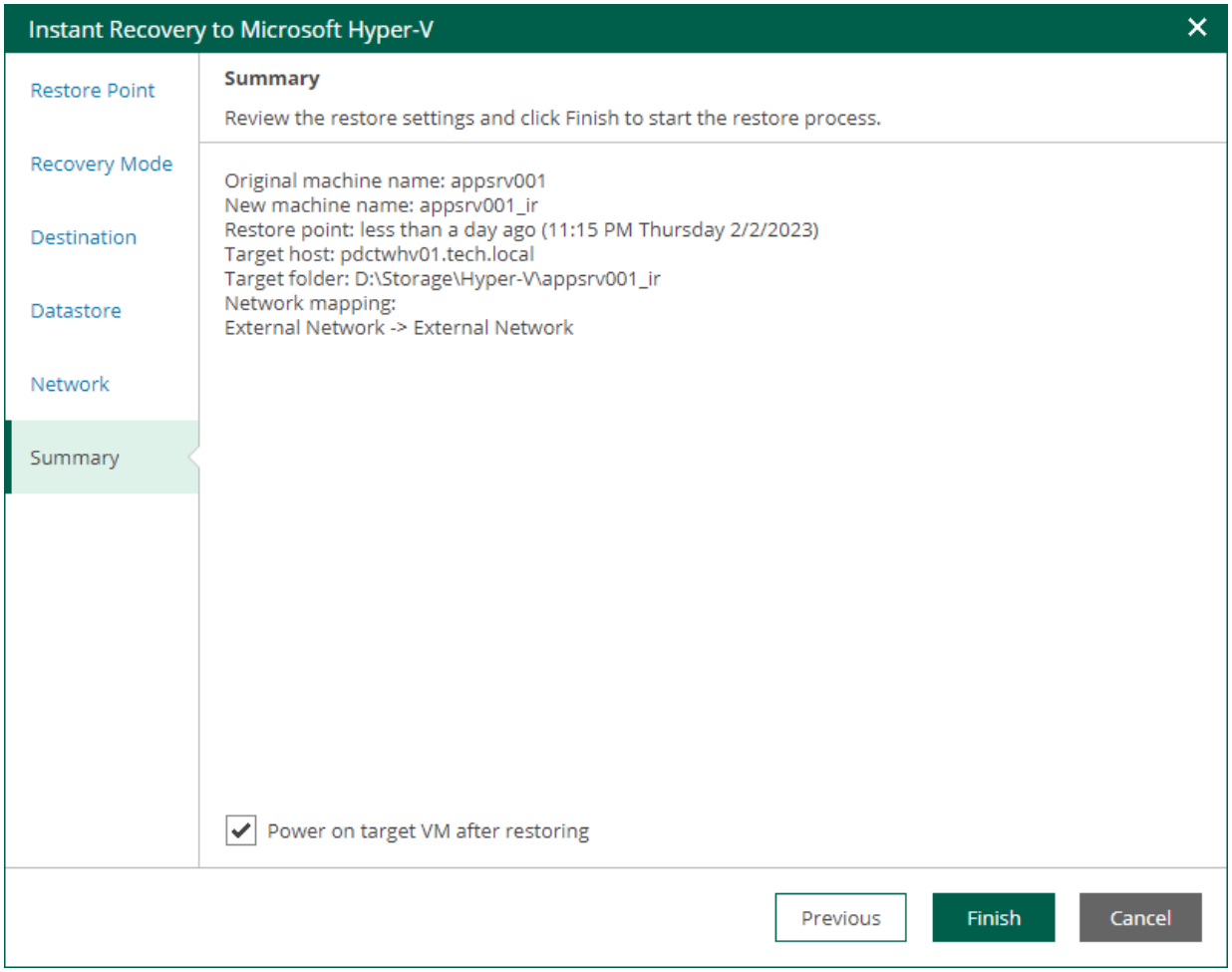
Step 7. Review Recovery Settings

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

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



What You Do Next

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

Finalizing Instant Recovery to Microsoft Hyper-V

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

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

Testing Recovered VM

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

Migrating Recovered VM

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

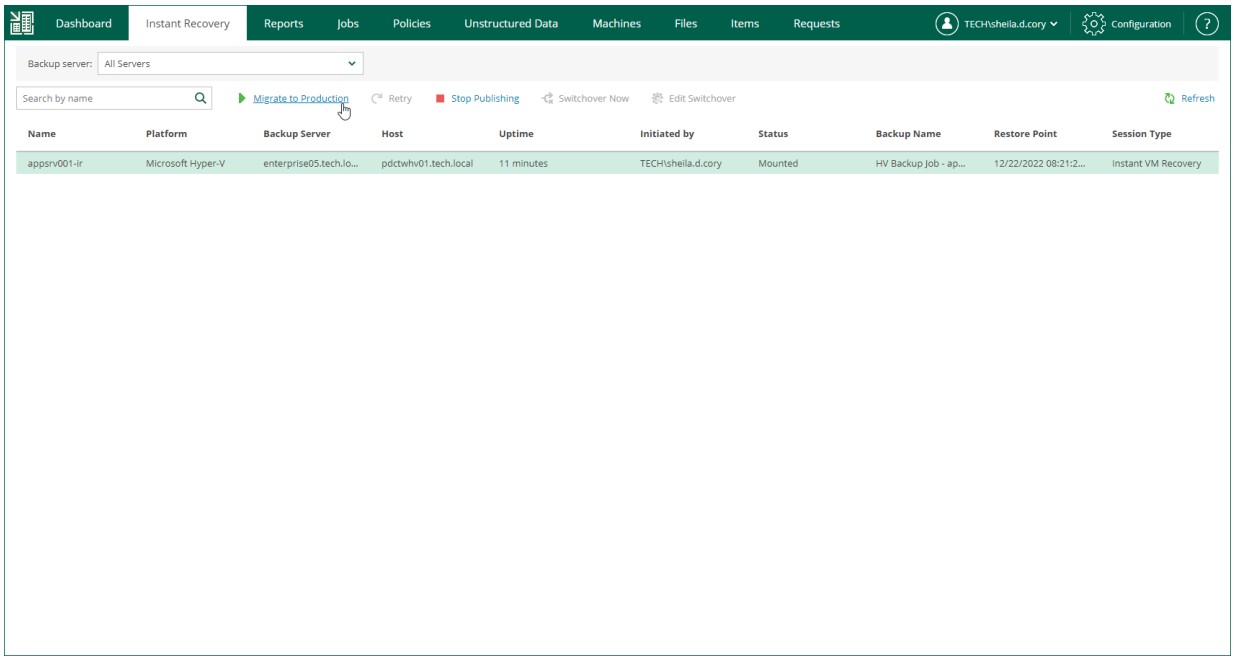
> **NOTE**
>
> After the migration is finished, the original VM still remains if the destination differs from the original location. If you do not need the VM, you have to manually remove it using the Hyper-V client.

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

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



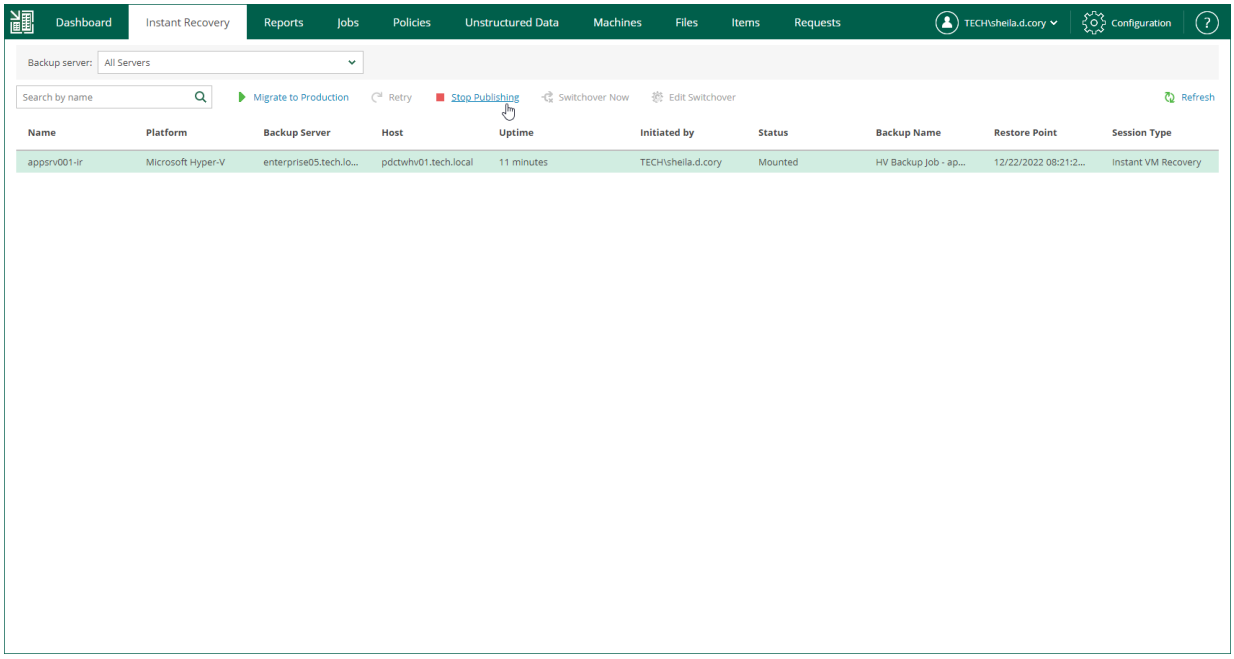
Unpublishing Recovered VM

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

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

To remove a recovered VM, do the following:

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



Entire VM Restore

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

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

- Restoring a VMware vSphere VM to VMware vSphere
- Restoring a VMware Cloud Director VM to VMware Cloud Director
- Restoring a Microsoft Hyper-V VM to Microsoft Hyper-V

Before You Begin

Before you perform entire VM restore, consider the following:

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

Restoring Entire VM to VMware vSphere

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

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

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

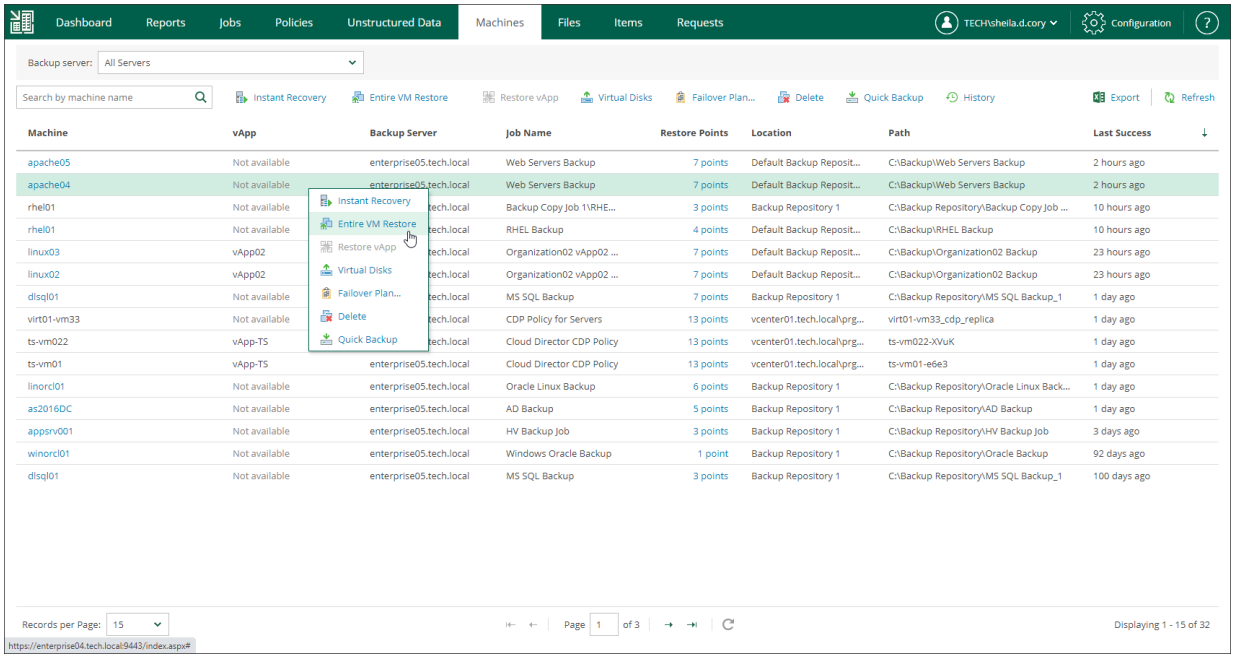
1. Launch the Entire VM Restore wizard.
2. Select a restore point.
3. Select a restore mode.
4. Specify destination settings for the recovered VM.
5. Specify a target datastore.
6. Configure network mapping.
7. Review the recovery settings.

Step 1. Launch Entire VM Restore Wizard

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

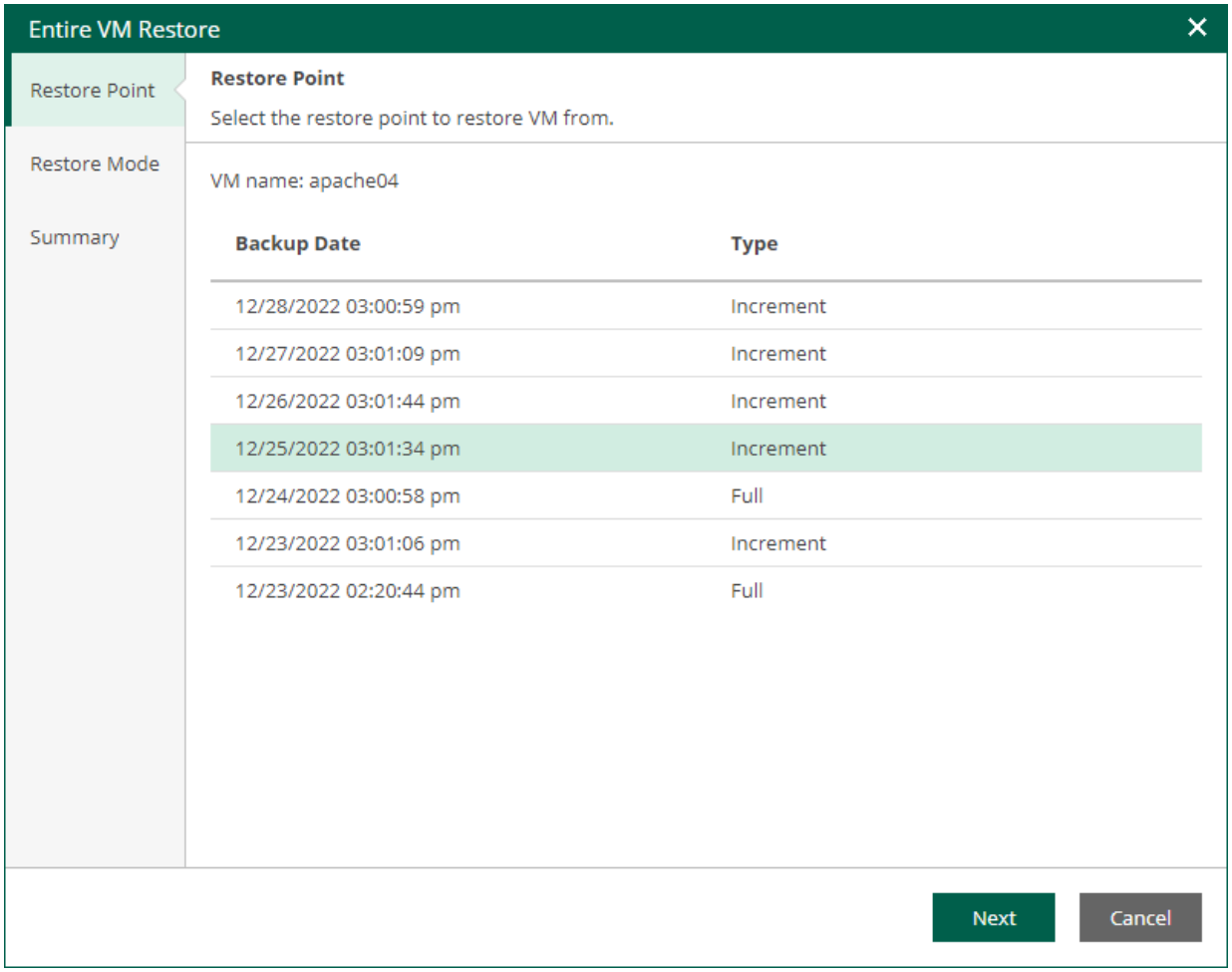
1. Open the **Machines** tab and select the necessary VMware vSphere VM from the list.
2. On the toolbar, click **Restore**.

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



Step 2. Select Restore Point

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



Step 3. Select Restore Mode

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

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

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

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

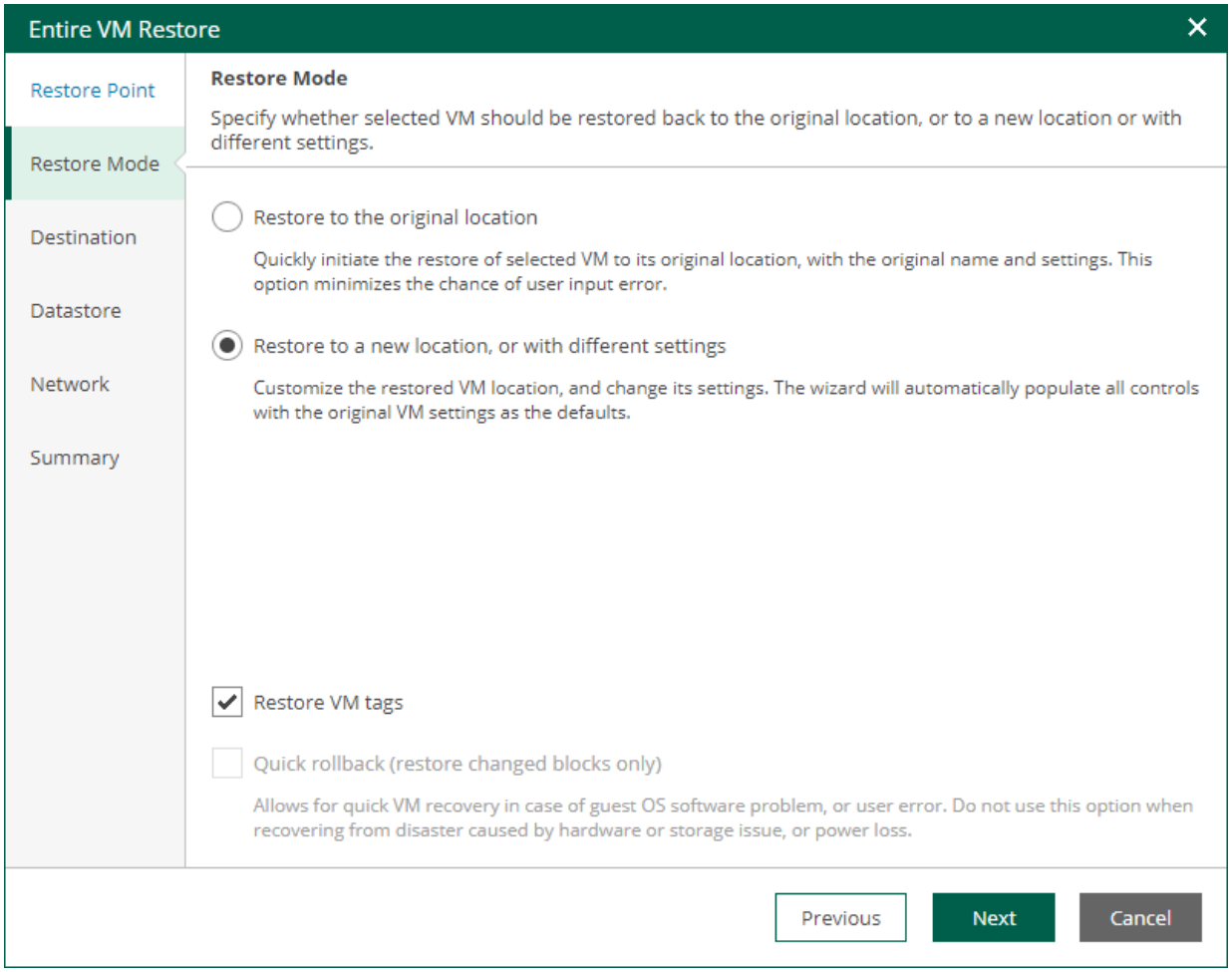
     During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication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

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

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

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

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

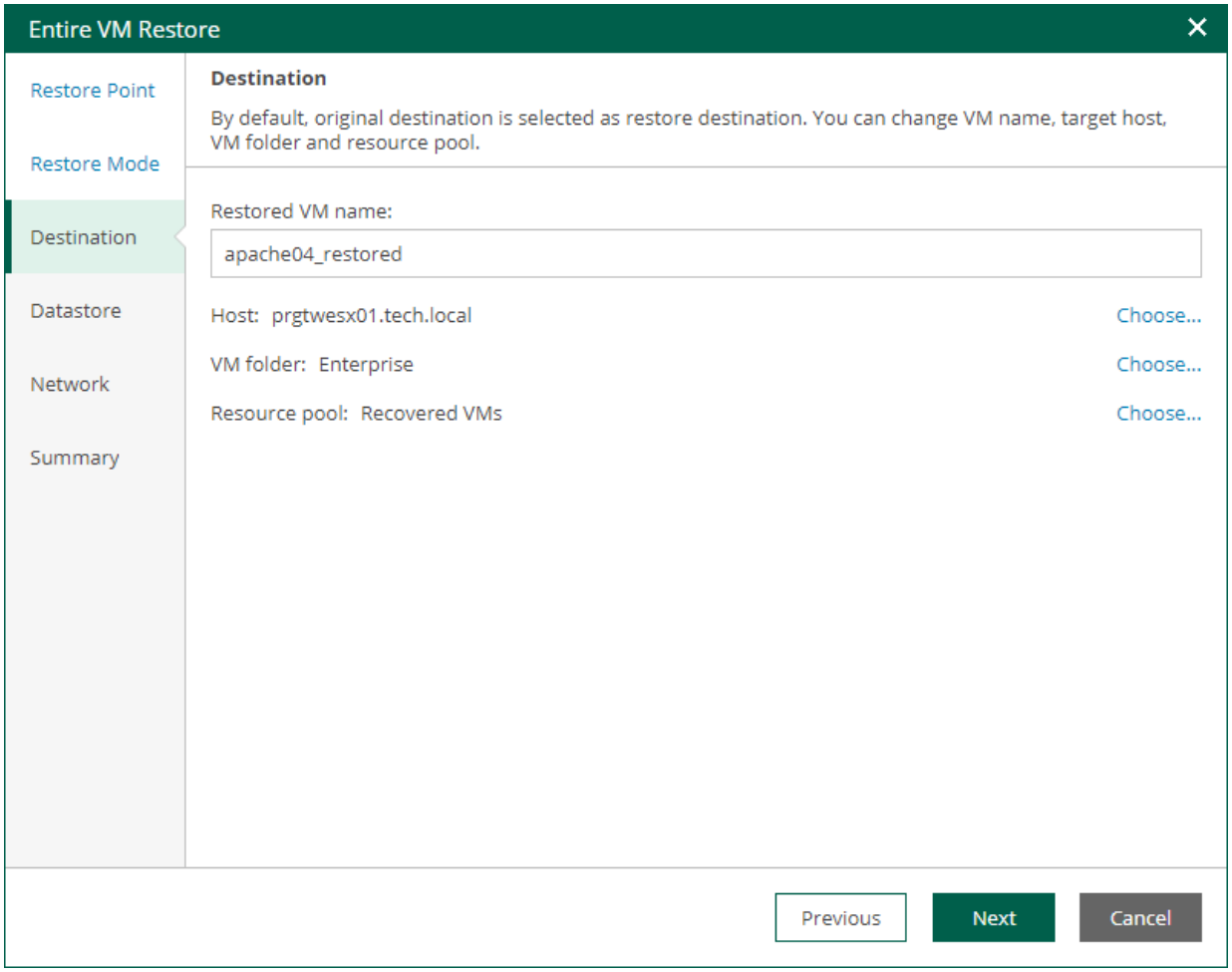


Step 4. Specify Destination Settings

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

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

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



Step 5. Specify Datastore and Disk Type

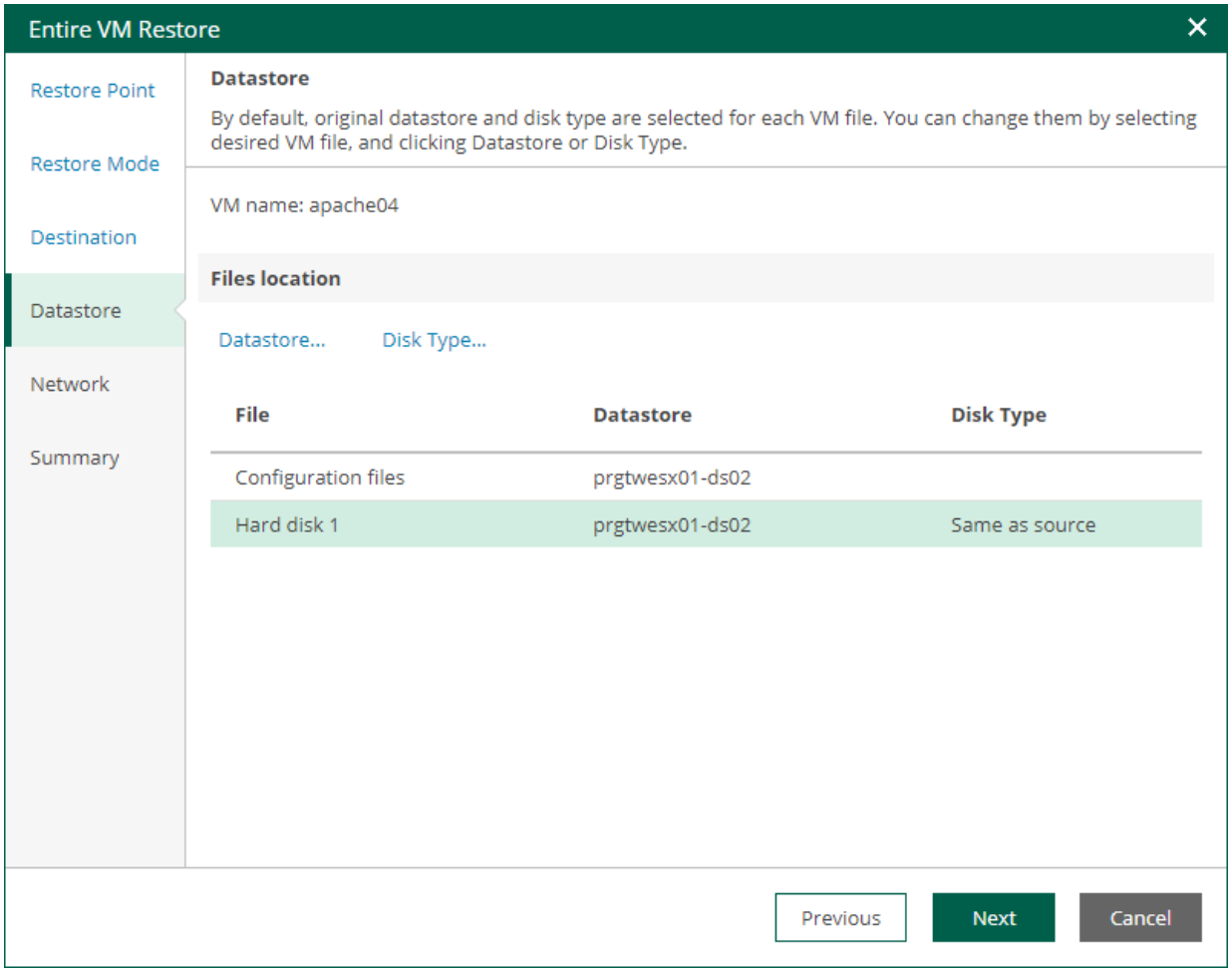
The **Datastore** step of the wizard is available if you restore a VM to a new location or with different settings.

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

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

1. To change the target datastore for VM configuration files or disk files, do the following:
   a. Select the configuration files or one of the hard disks and click **Datastore**.
   b. In the **Select Datastore** window, choose the necessary datastore and click **OK**.
2. By default, hard disks of the restored VM have the same type as disks of the original VM. To change the disk type, do the following:
   a. Select a hard disk and click **Disk Type**.
   b. In the **Restored VM Disk Type** window, select a disk format and click **OK**. For more information about disk formats, see the Virtual Disk Options section of the VMware vSphere documentation.

> **NOTE**
>
> You can only change disk format for VMs with Virtual Hardware version 7 or later.



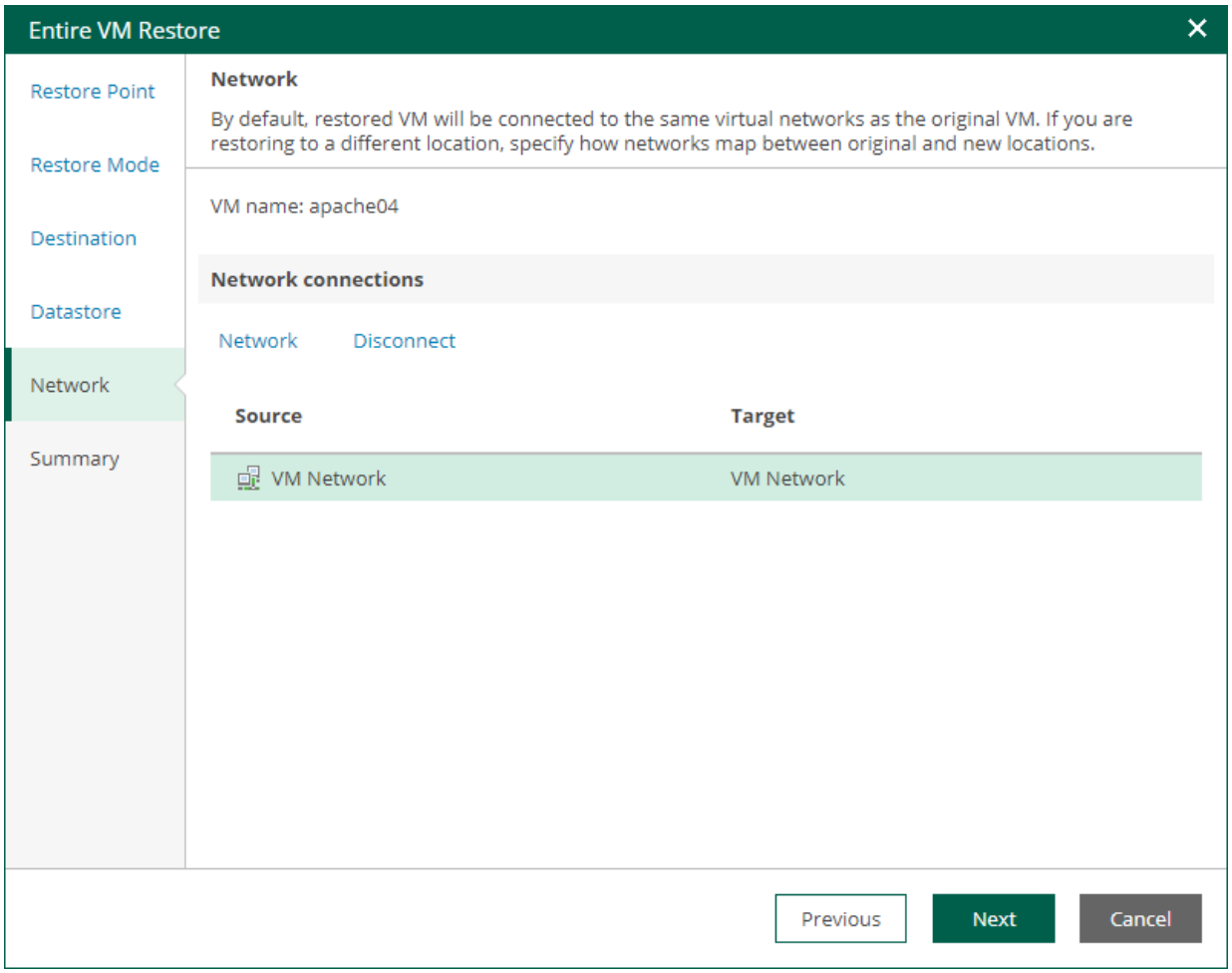
Step 6. Configure Network Mapping

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

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

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

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

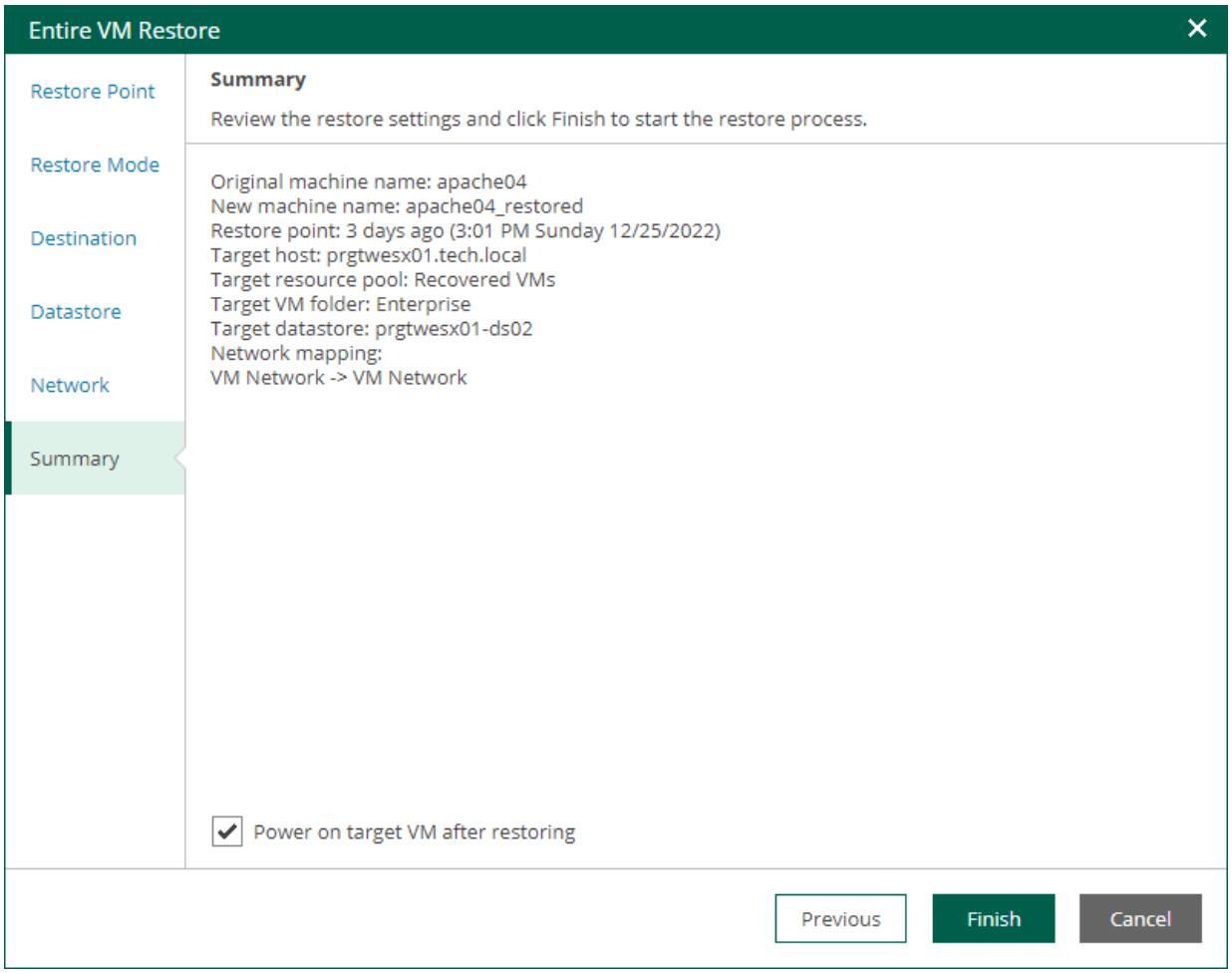


Step 7. Review Restore Settings

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



Restoring Entire VM to VMware Cloud Director

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

For more information on entire VM restore of VMware Cloud Director VMs, see the Restoring VMs to Cloud Director vApp section of the Veeam Backup & Replication User Guide.

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

1. Launch the Entire VM Restore wizard.
2. Select a restore point.
3. Select a restore mode.

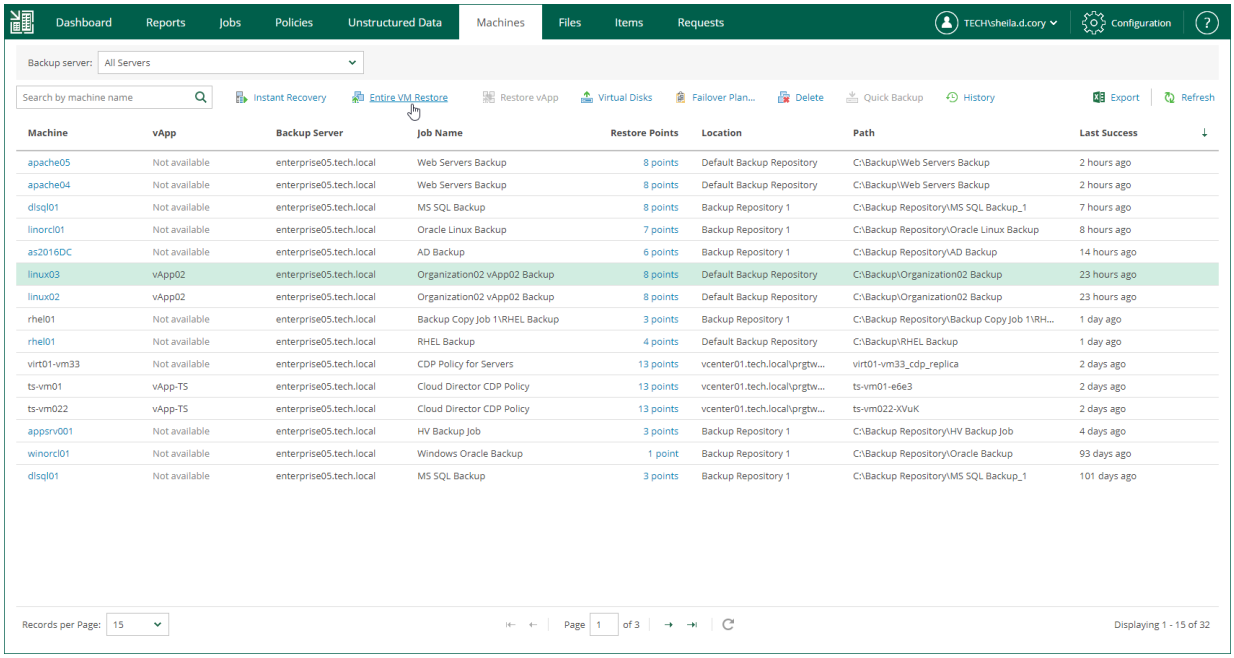
4. Specify destination settings for the recovered VM.
5. Specify a target datastore.
6. Configure network mapping.
7. Configure fast provisioning.
8. Review the recovery settings.

Step 1. Launch Entire VM Restore Wizard

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

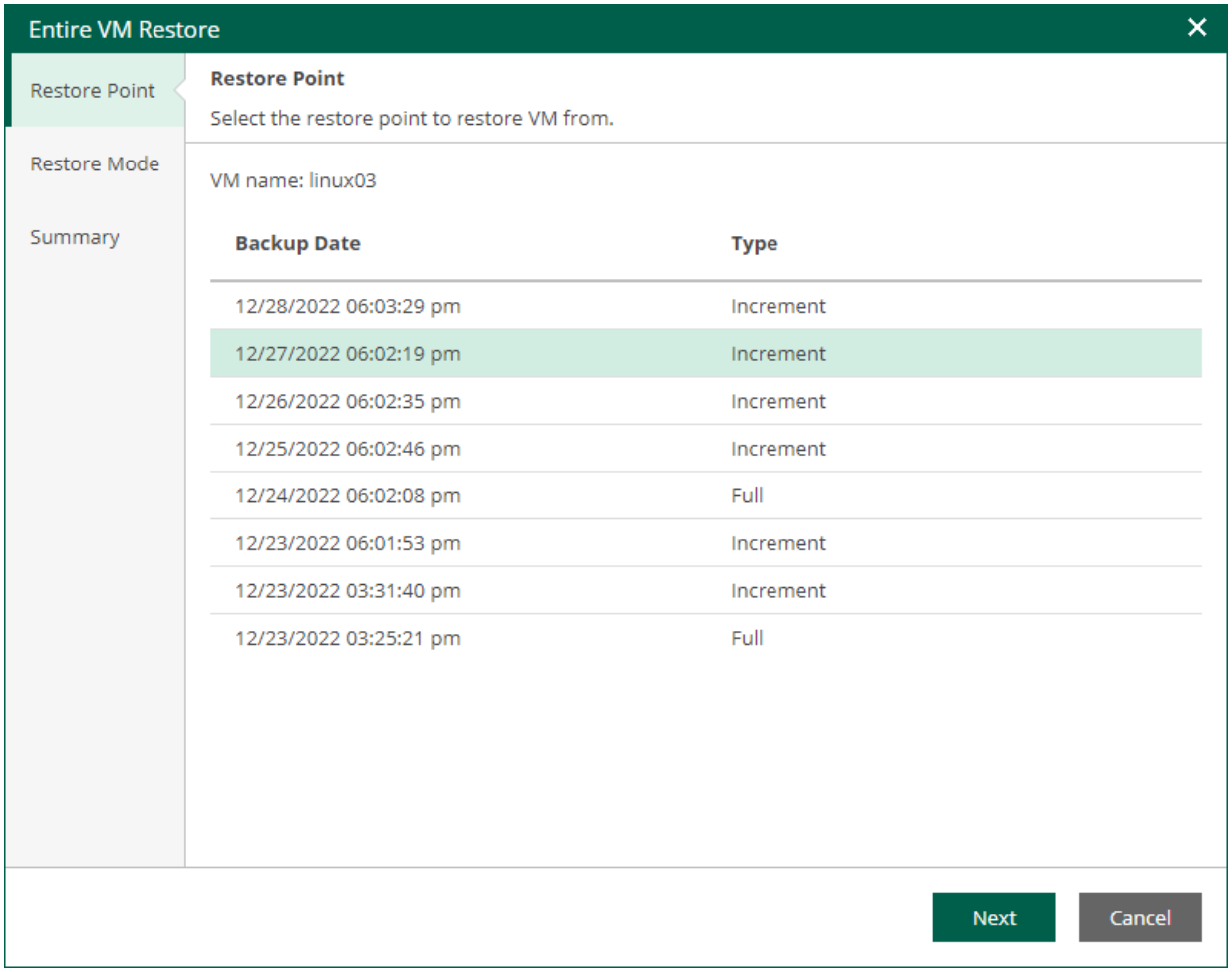
1. Open the **Machines** tab and select the necessary VMware Cloud Director VM from the list.
2. On the toolbar, click **Entire VM Restore**.

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



Step 2. Select Restore Point

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



Step 3. Select Restore Mode

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

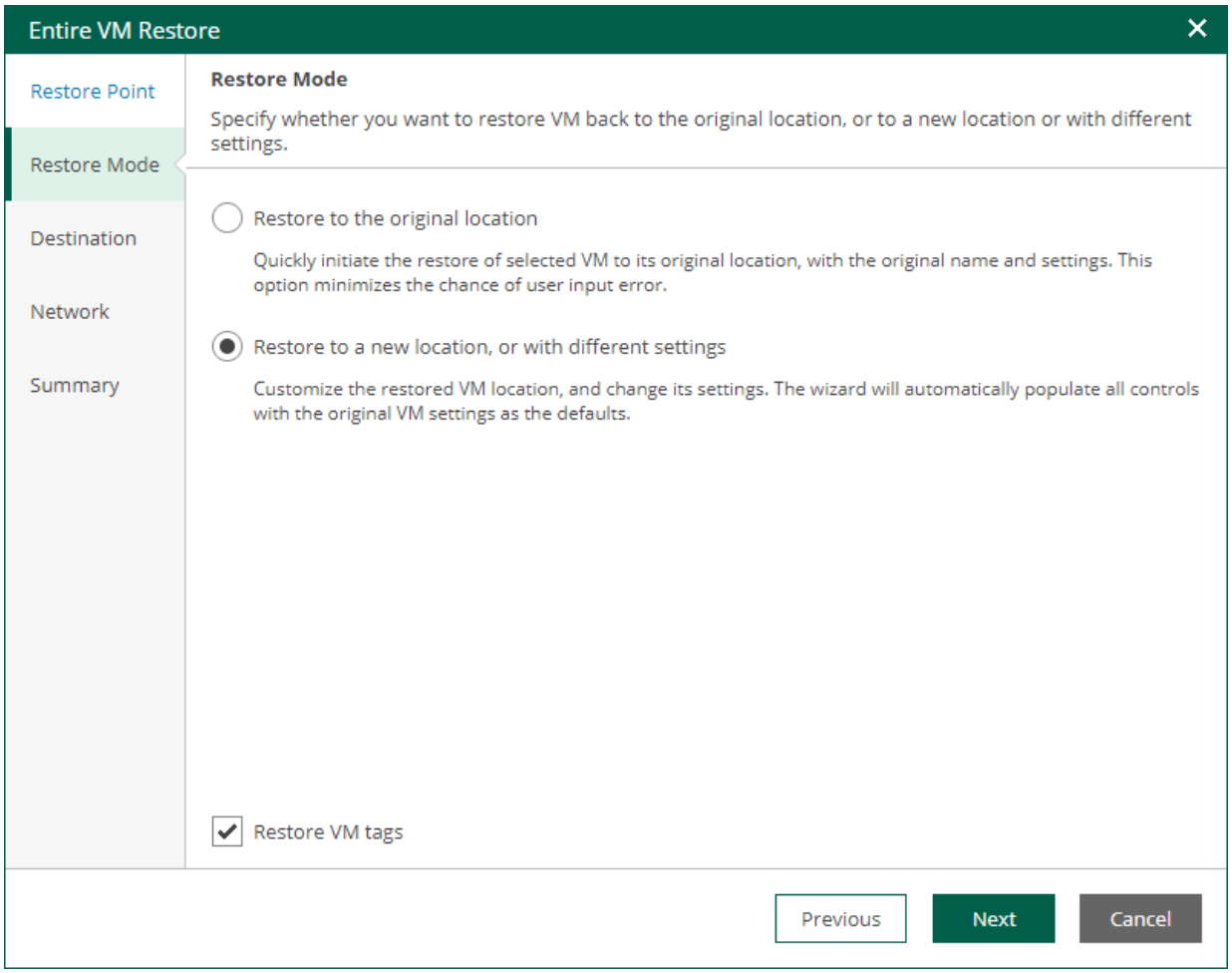
When you perform entire VM restore using Veeam Backup Enterprise Manager, Veeam Backup & Replication automatically selects a backup proxy over which VM data must be transported to the source datastore. You can select a backup proxy manually from the **Entire VM Restore** wizard in the Veeam Backup &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

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

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

     During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication deletes the original VMs. In this case, you must edit existing jobs to exclude original VMs from them.
2. If you want to restore tags that were assigned to the original VM and assign them to the recovered VM, select the **Restore VM tags** check box. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
   - You restore a VM to the original location.

- The original VM tags are available on the source vCenter Server.

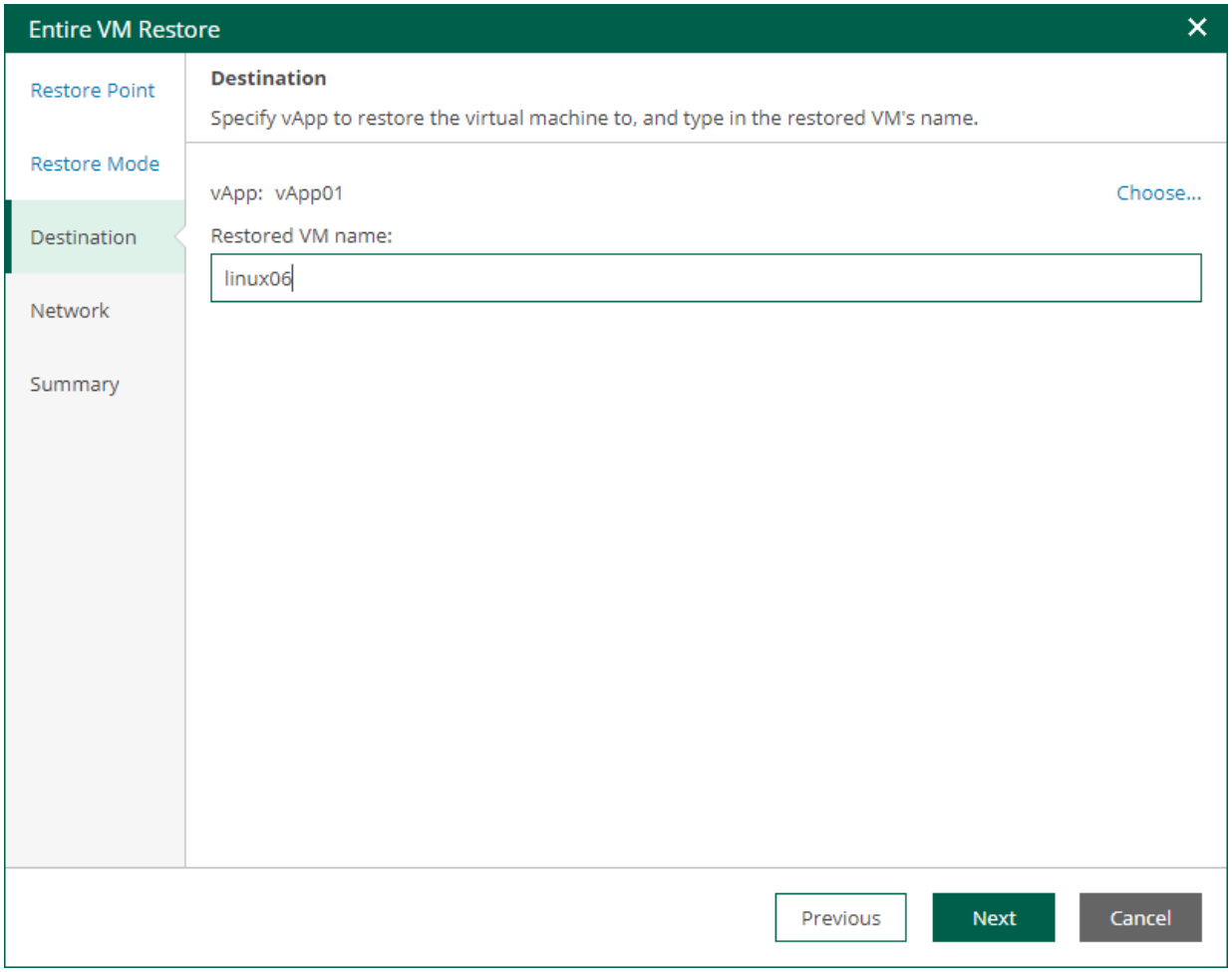


Step 4. Specify Destination Settings

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

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

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



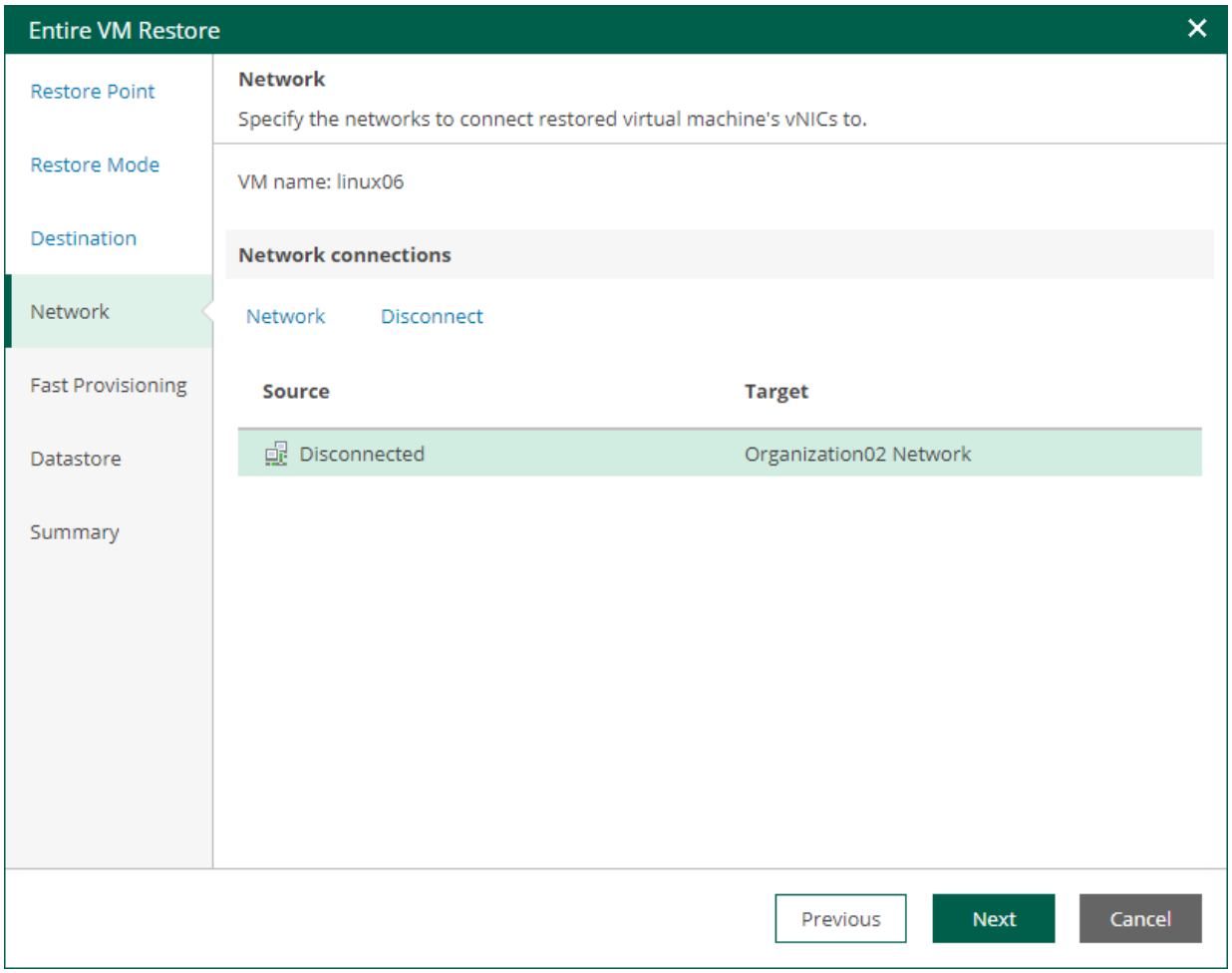
Step 5. Configure Network Mapping

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

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

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

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

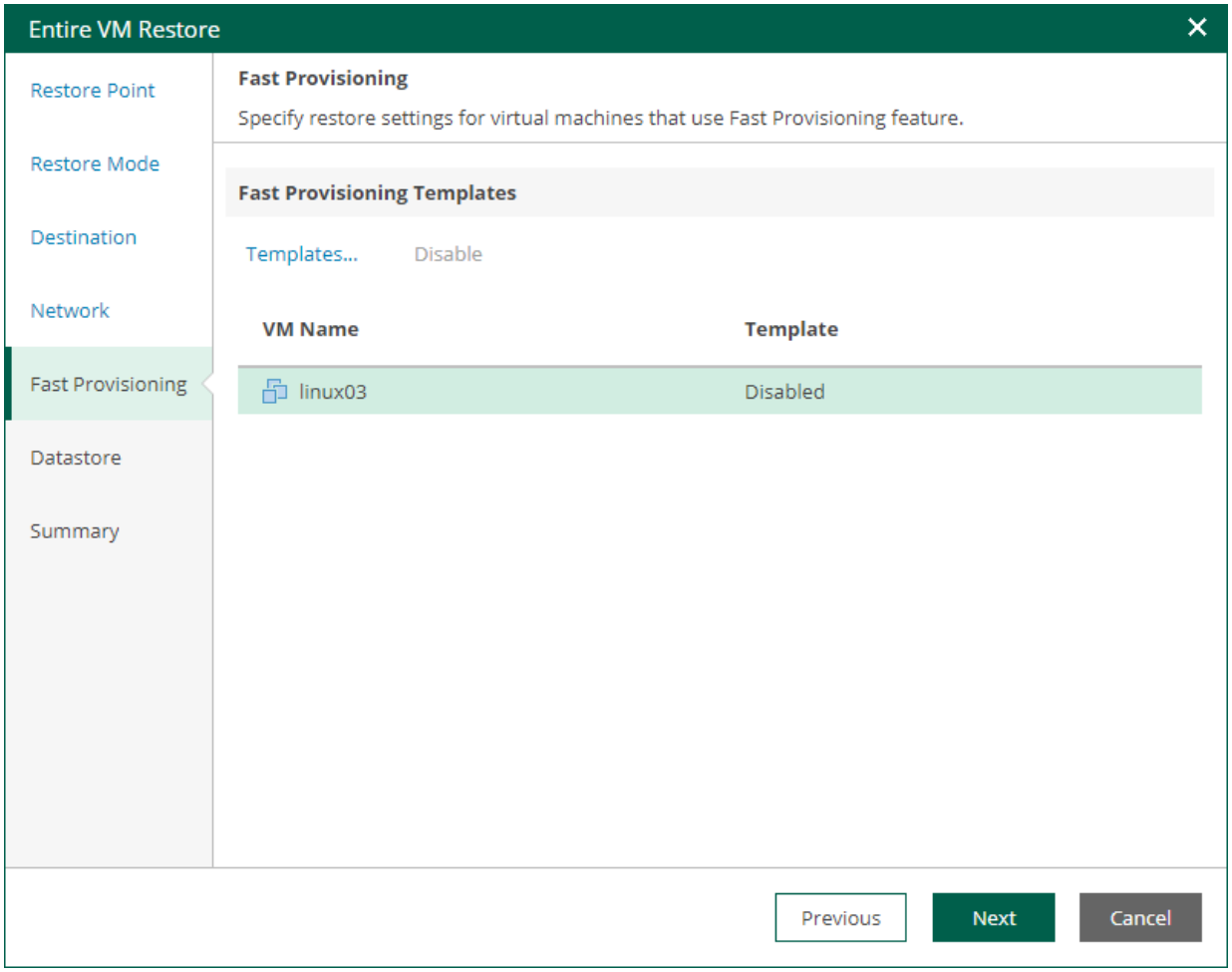


Step 6. Configure Fast Provisioning

The **Fast Provisioning** step of the wizard is available if you restore a VM to a new location or with different settings, and if fast provisioning is enabled on the target organization VDC.

At this step of the wizard, you can configure fast provisioning for the restored VM.

- To specify a fast provisioning template for the VM, select the VM in the list, click **Templates**, and choose a template to which the restored VM must be linked.
- To disable fast provisioning for the VM and restore it as a regular VM, select the VM in the list and click **Disable**.

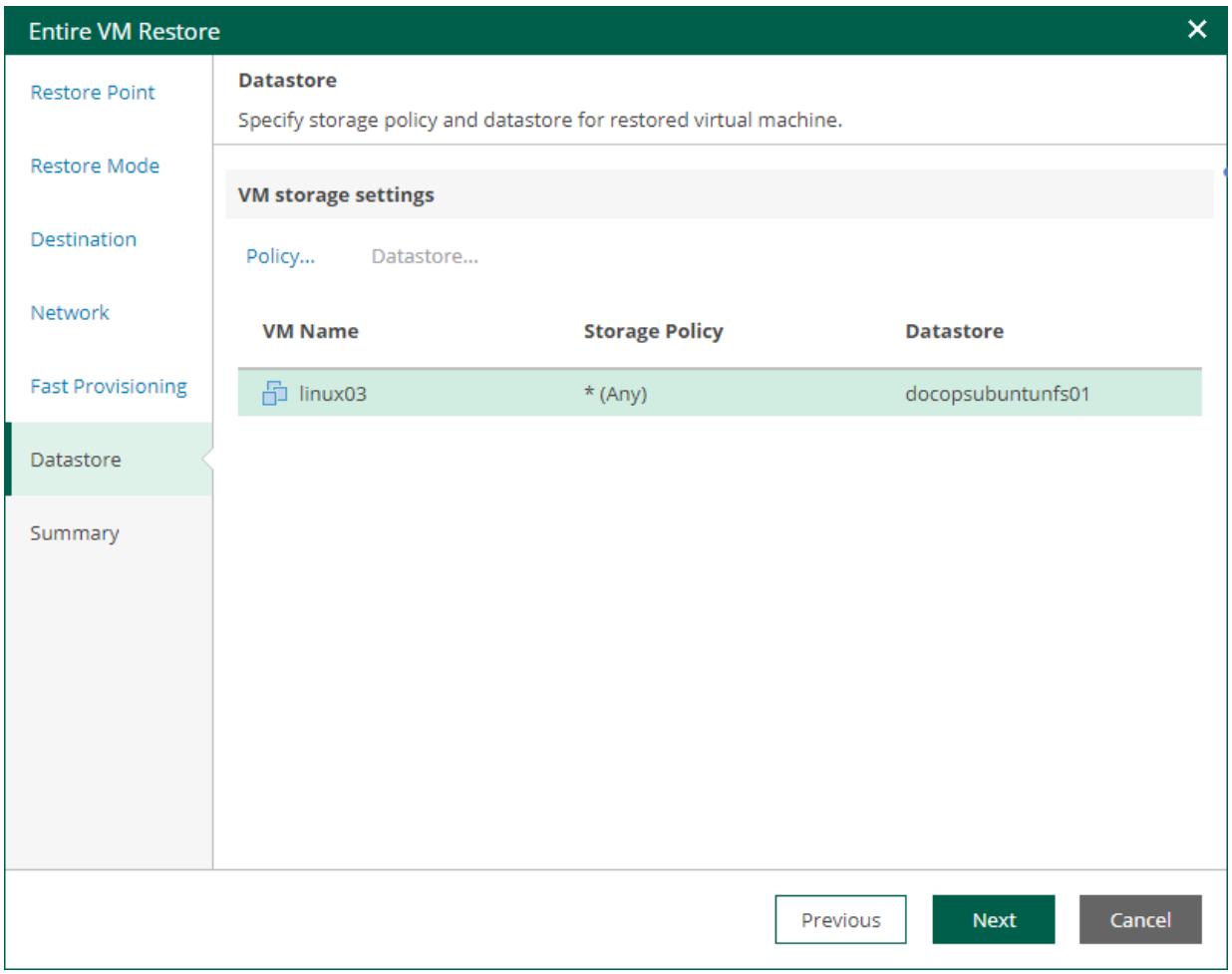


Step 7. Specify Storage Policy and Datastore

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

At this step of the wizard, you can specify a storage policy and datastore for the restored VM.

1. To change the target storage policy, do the following:
   a. Select a VM and click **Policy**.
   b. In the **Select Storage Policy** window, select a storage policy and click **OK**.
2. To change the target datastore, do the following:
   a. Select a VM and click **Datastore**.
   b. In the **Select Datastore** window, select a datastore and click **OK**.

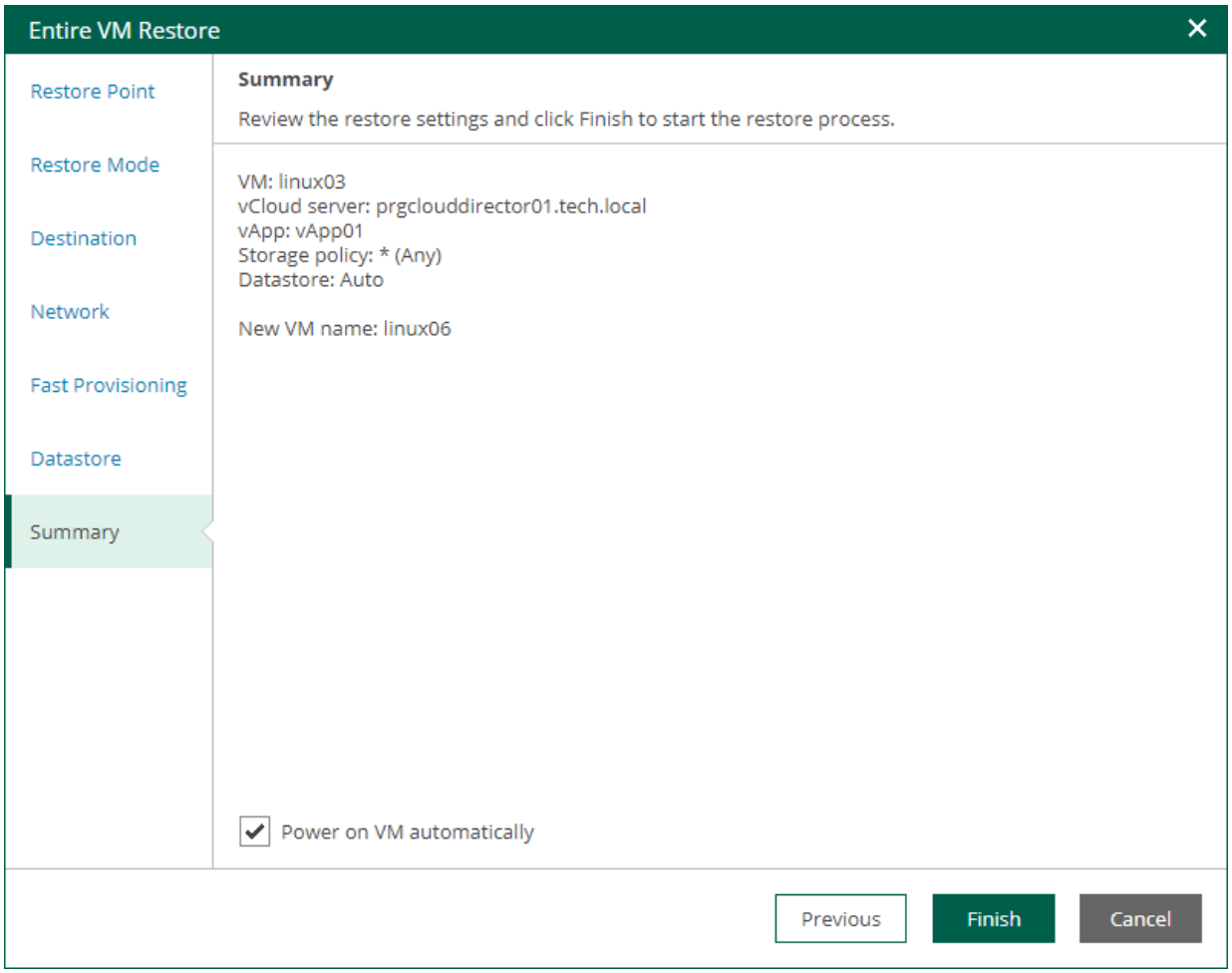


Step 8. Review Restore Settings

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



Restoring Entire VM to Microsoft Hyper-V

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

For more information on entire VM restore of Microsoft Hyper-V VMs, see the Entire VM Restore section of the Veeam Backup & Replication User Guide.

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

1. Launch the Entire VM Restore wizard.
2. Select a restore point.
3. Select a recovery mode.
4. Specify destination settings for the recovered VM.

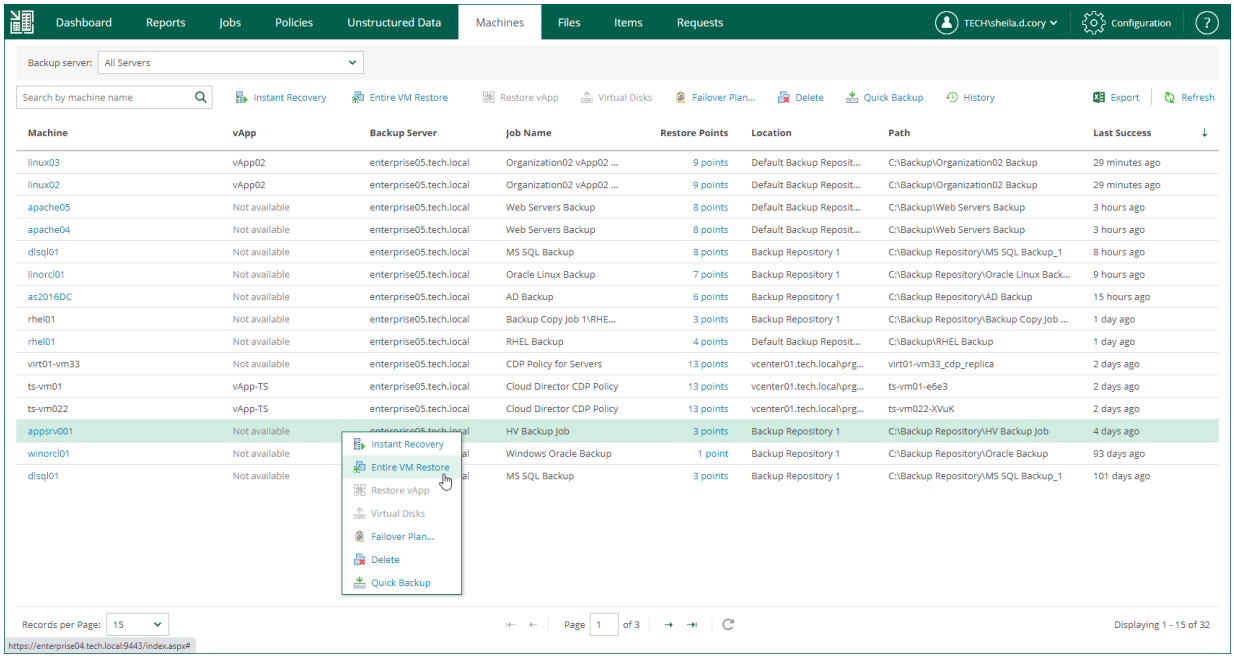
5. Specify a target datastore.
6. Configure network mapping.
7. Review the recovery settings.

Step 1. Launch Entire VM Restore Wizard

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

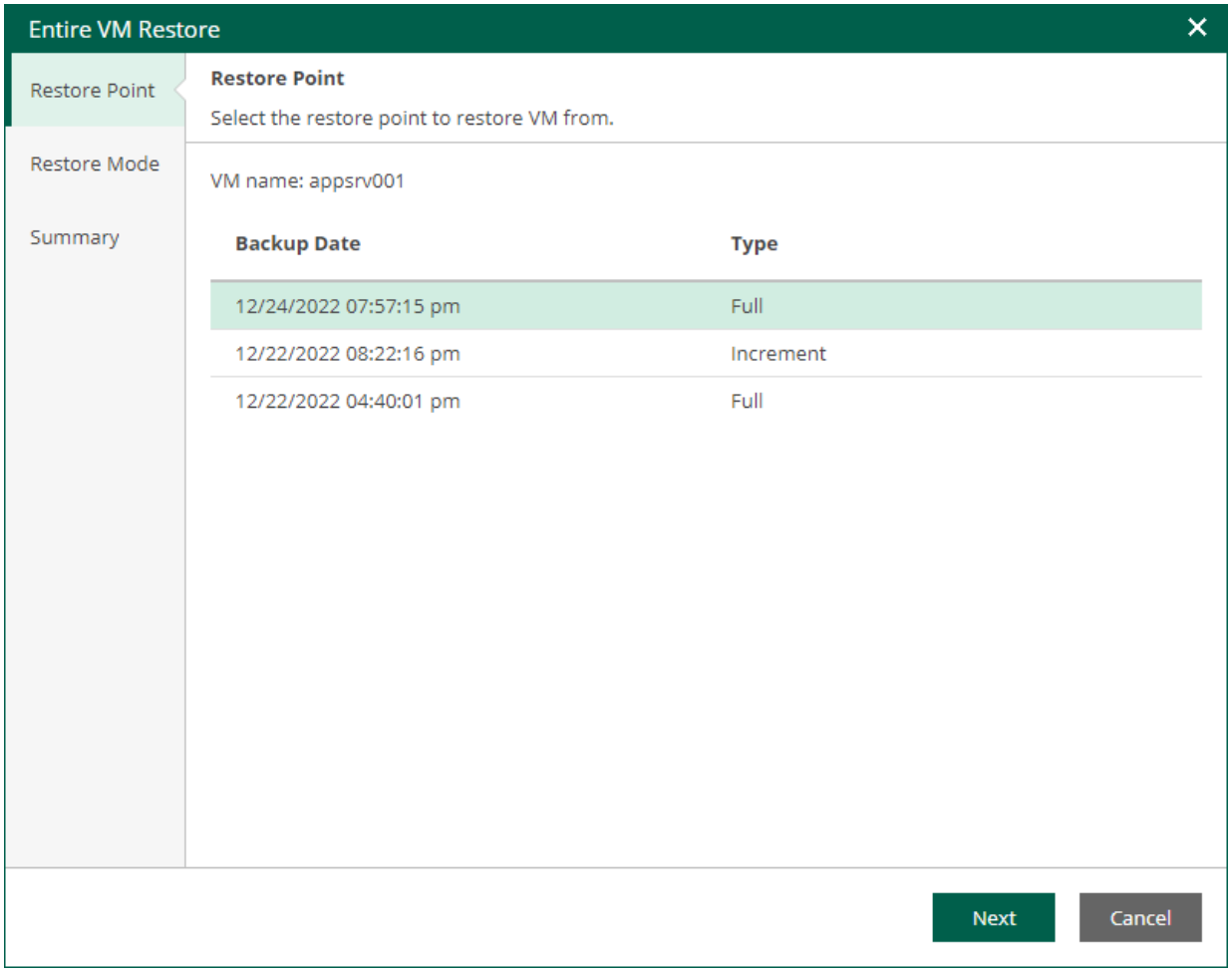
1. Open the **Machines** tab and select the necessary Microsoft Hyper-V VM from the list.
2. On the toolbar, click **Restore**.

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



Step 2. Select Restore Point

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



Step 3. Select Restore Mode

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

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

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

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

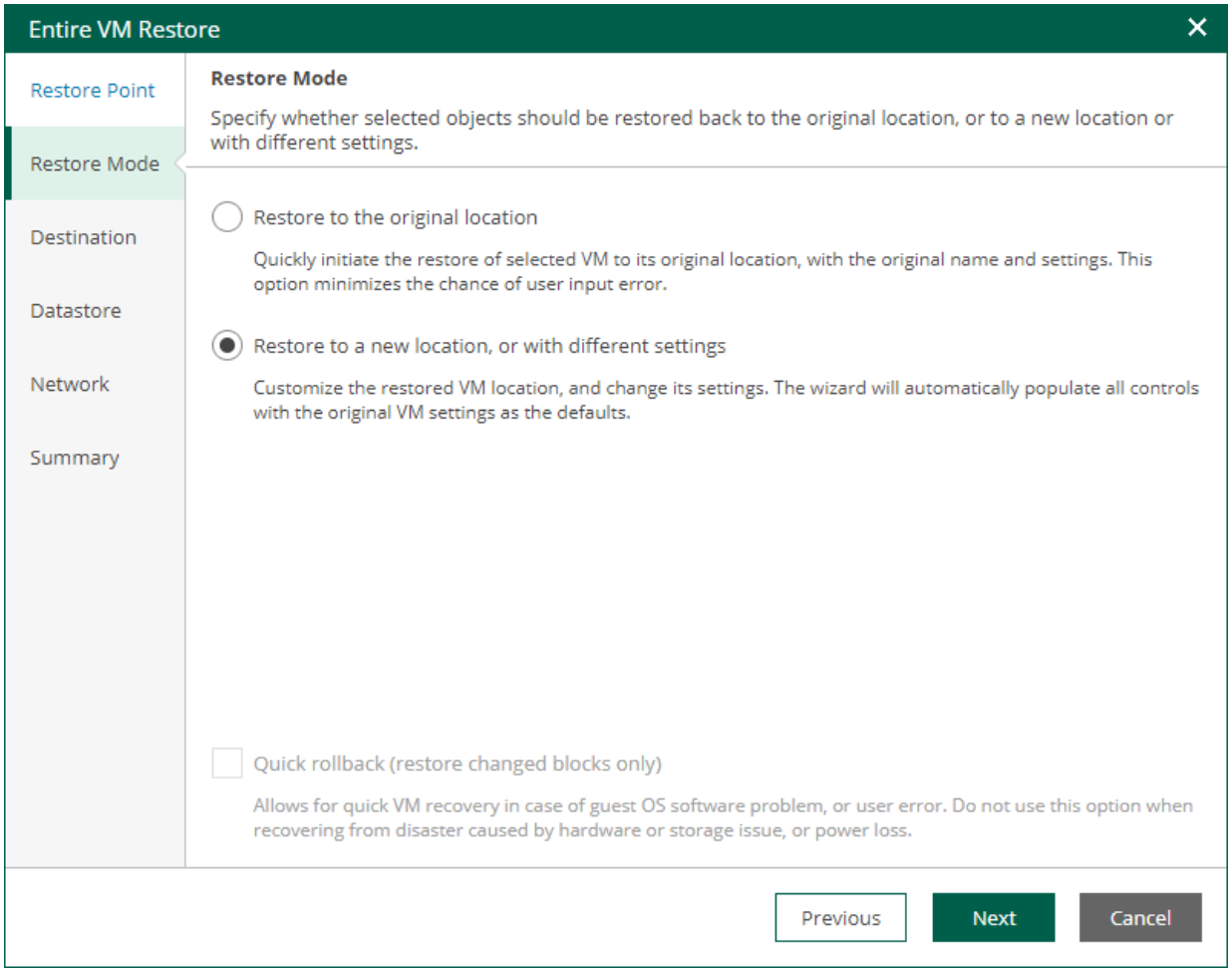
     During restore to a new location, Veeam Backup & Replication creates new VMs. If you want to process the restored VMs, you must edit existing jobs or create new jobs to process the restored VMs. If you restore VMs with the same name and to the same folder as the original VMs, Veeam Backup & Replication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

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

2. [For VM restore to the original location] Select the **Quick rollback** check box to perform incremental restore for the VM. Veeam Backup & Replication will query Changed Block Tracking to get data blocks that are required to revert the VM to the restore point, and will restore only these data blocks. Quick rollback significantly reduces the restore time and has little impact on the production environment.

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

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



Step 4. Specify Destination Settings

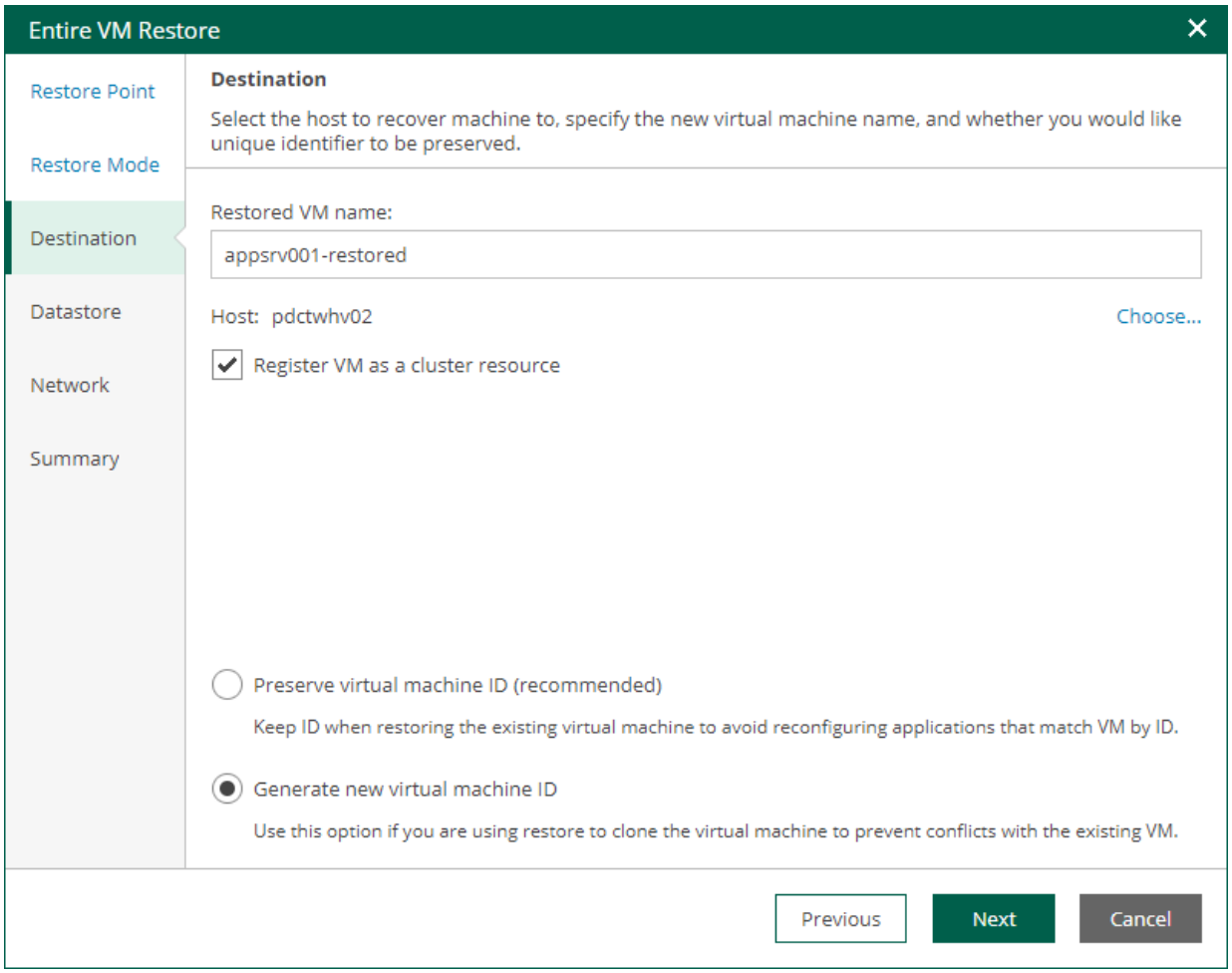
The **Destination** step of the wizard is available if you restore a VM to a new location or with different settings.

At this step of the wizard, you can specify a name of the restored VM and target host, register the VM as a cluster resource, and generate a new BIOS UUID.

To configure destination settings, do the following:

1. In the **Restored VM name** field, specify a name under which the workload will be restored.
2. In the **Host** field, specify a target host.
3. If the specified host is a part of a Hyper-V failover cluster, you can register the restored VM as a cluster resource. In this case, if the target host is brought offline or fails for any reason, the VM will fail over to another node in the cluster. To do this, select the **Register VM as a cluster resource** check box.
4. Choose whether to preserve the BIOS UUID or generate a new BIOS UUID.

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



Step 5. Specify Datastore

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

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

To change a default path, do the following:

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

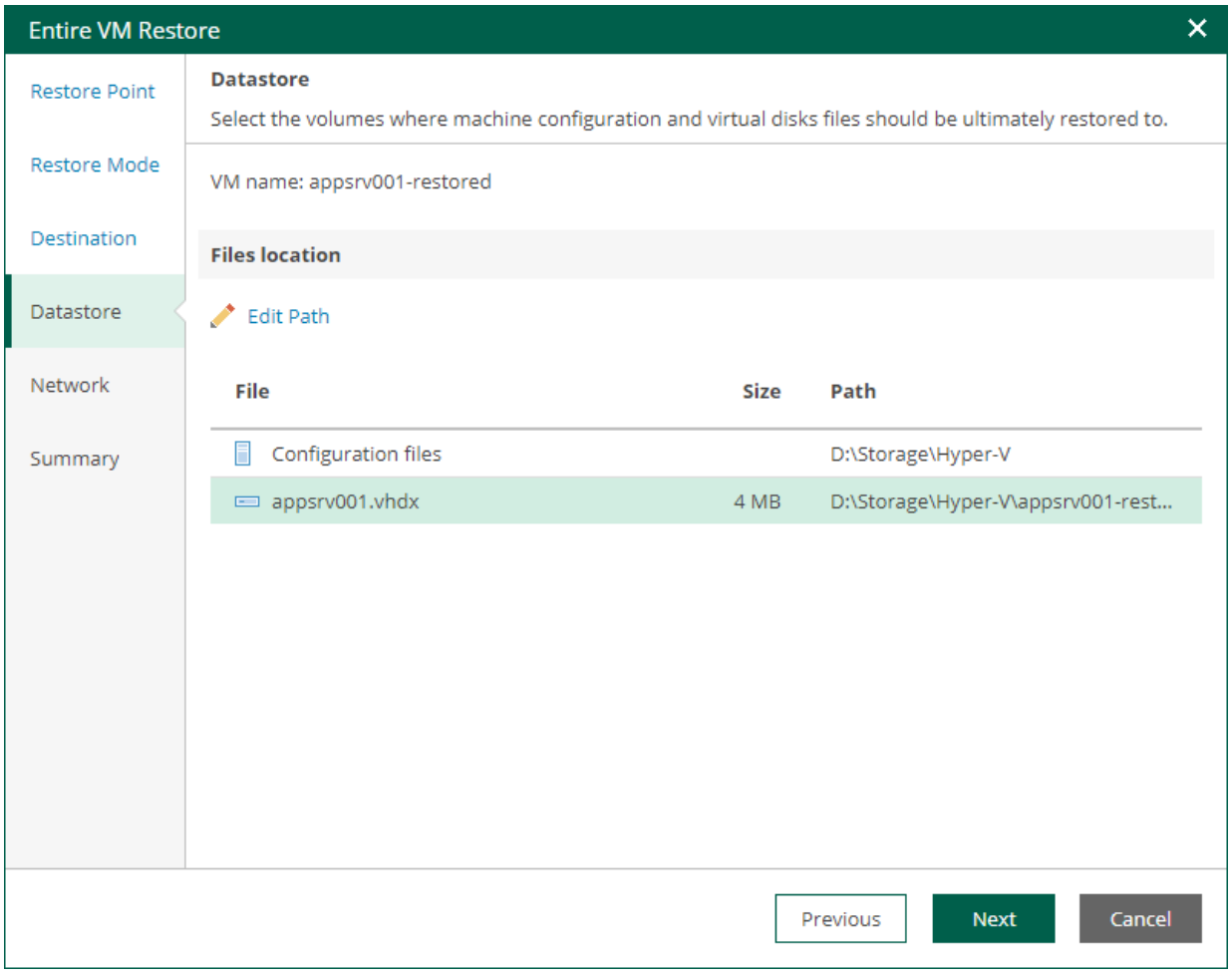
   Alternatively, you can double-click a file to edit its path.

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

3. Click **OK**.

IMPORTANT

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



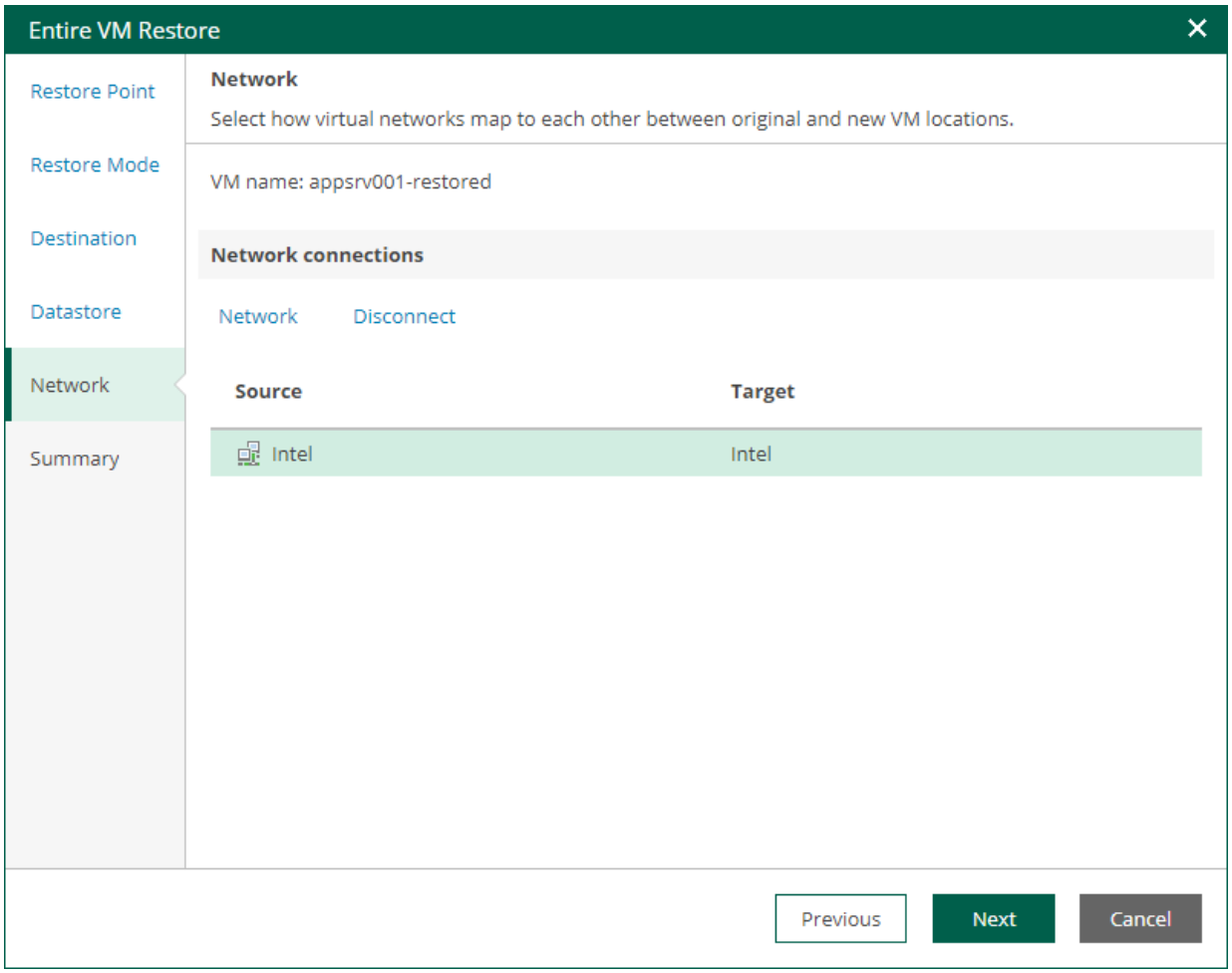
Step 6. Configure Network Mapping

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

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

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

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

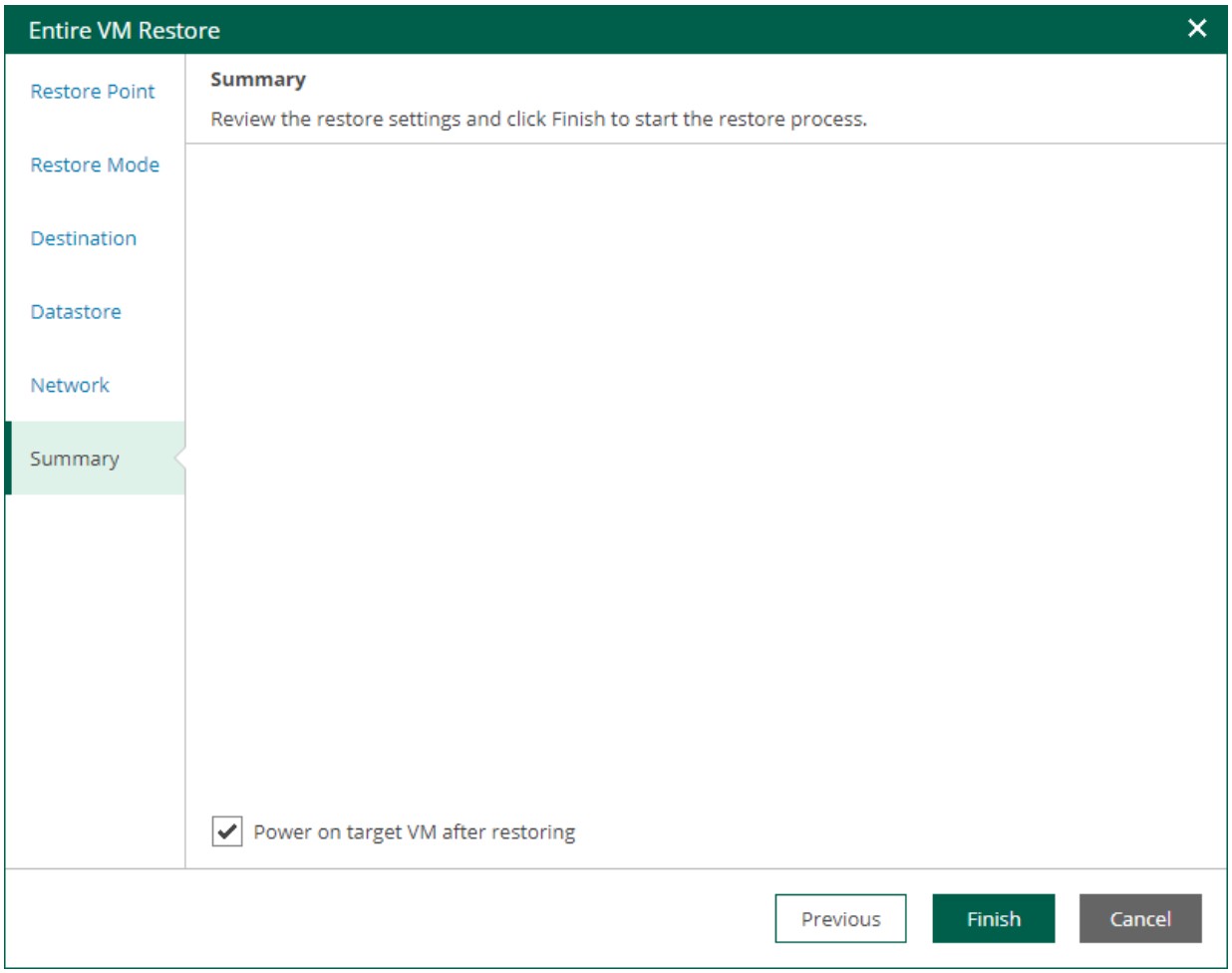


Step 7. Review Restore Settings

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



Virtual Disk Restore

Virtual disk restore may be helpful if a VM disk becomes corrupted for some reason. The restored virtual disk can be attached to the original VM to replace a corrupted drive, or connected to any other VM. For more information on virtual disk restore, see the Virtual Disk Restore section of the Veeam Backup & Replication User Guide.

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

Before you restore virtual disks, consider the following:

- Disk restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Disk restore is supported for backups of VMware vSphere VMs only.
- During the virtual disk restore, Veeam Backup & Replication powers off the target VM to reconfigure its settings and attach restored disks. It is recommended that you stop all activities on the target VM for the restore period.

To restore a VM disk from backup, use the **Virtual Disk Restore** wizard.

1. Launch the Virtual Disk Restore wizard.
2. Select a restore point.
3. Specify disk mapping.
4. Specify secure restore settings.
5. Review the restore settings.

Step 1. Launch Virtual Disk Restore Wizard

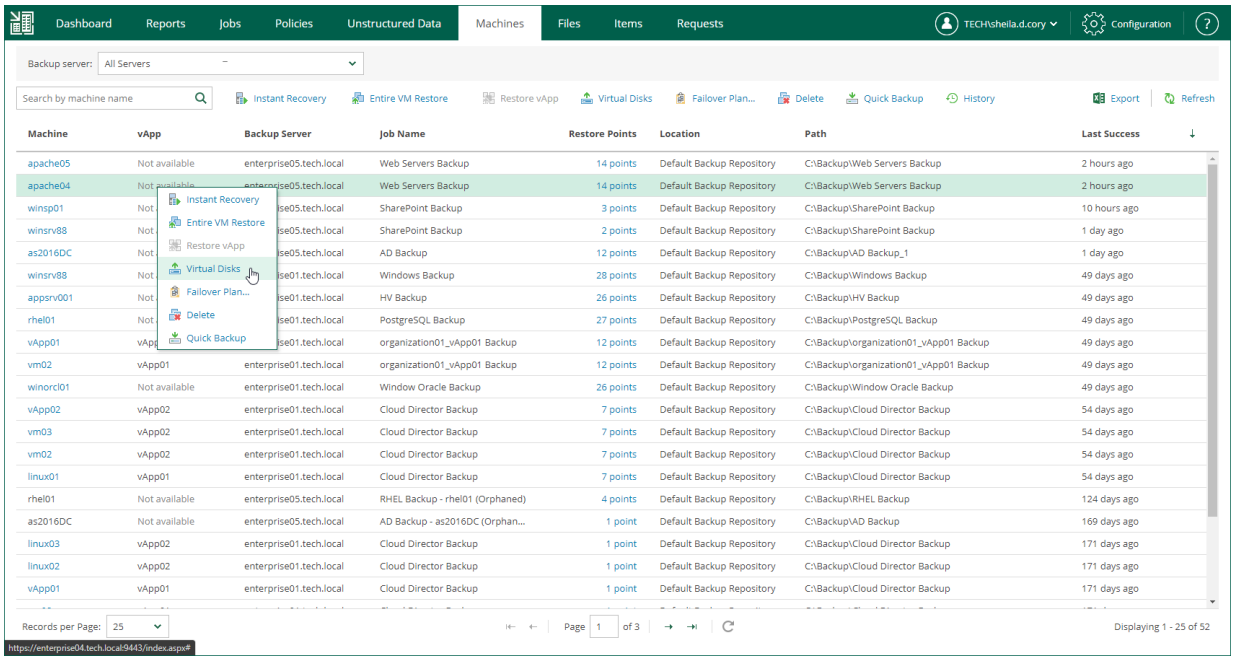
To launch the **Virtual Disk Restore** wizard, do the following:

1. Open the **Machines** tab and select the necessary VMware vSphere VM from the list.

   To quickly find a machine, you can filter machines in the list by a backup server or search for a specific machine by machine name.

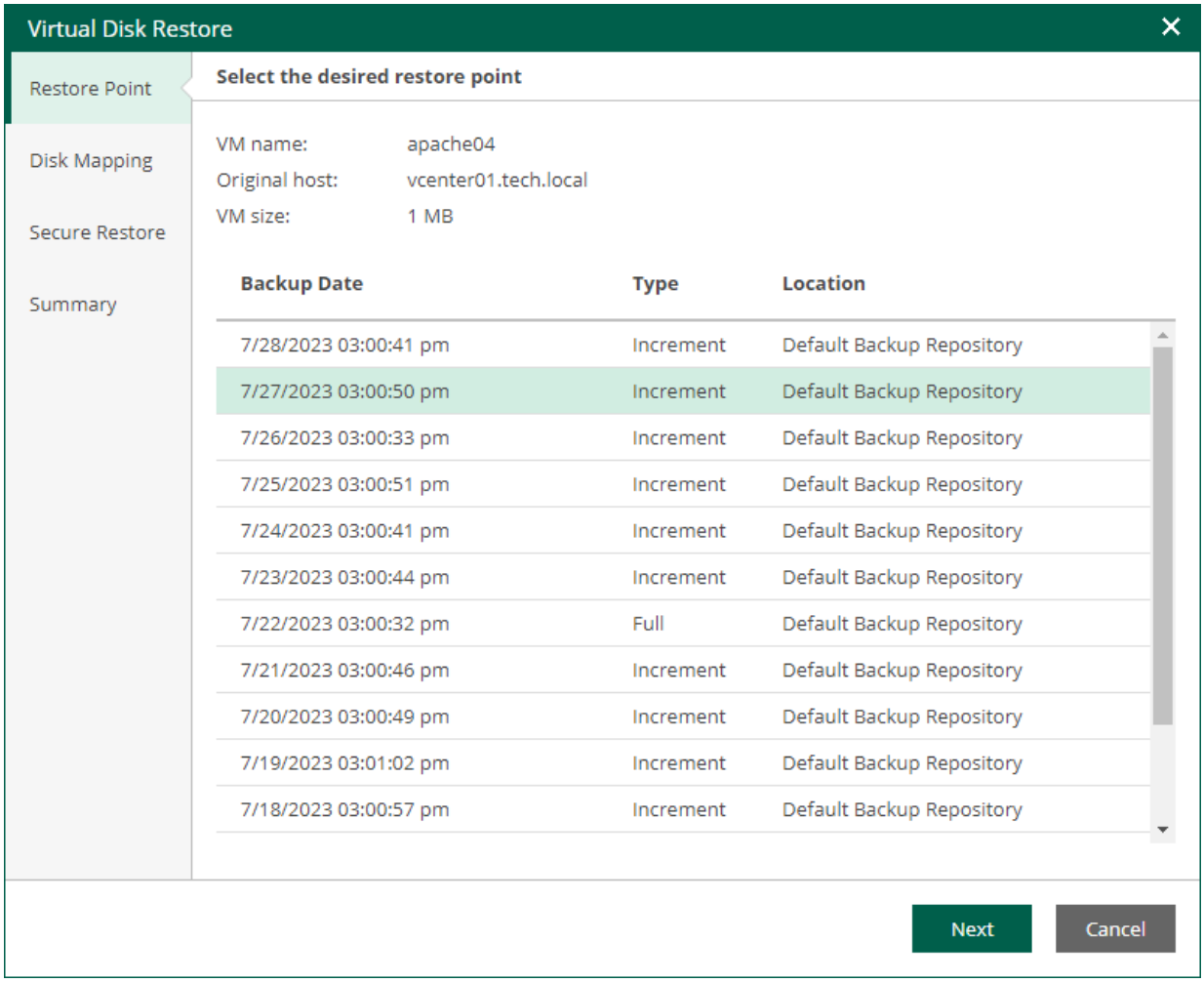
2. On the toolbar, click **Virtual Disks**.

Alternatively, you can right-click the VM and select **Virtual Disks**.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point that will be used to restore the VM disk.



Step 3. Specify Disk Mapping

At the **Disk Mapping** step of the wizard, specify VM disk restore settings.

1. By default, Veeam Backup Enterprise Manager restores virtual disks to the original VM. To select another VM, click **Choose** next to the **Virtual machine** field and select the necessary VM from the virtual environment.

   You cannot attach restored disks to a VM that has one or more snapshots.

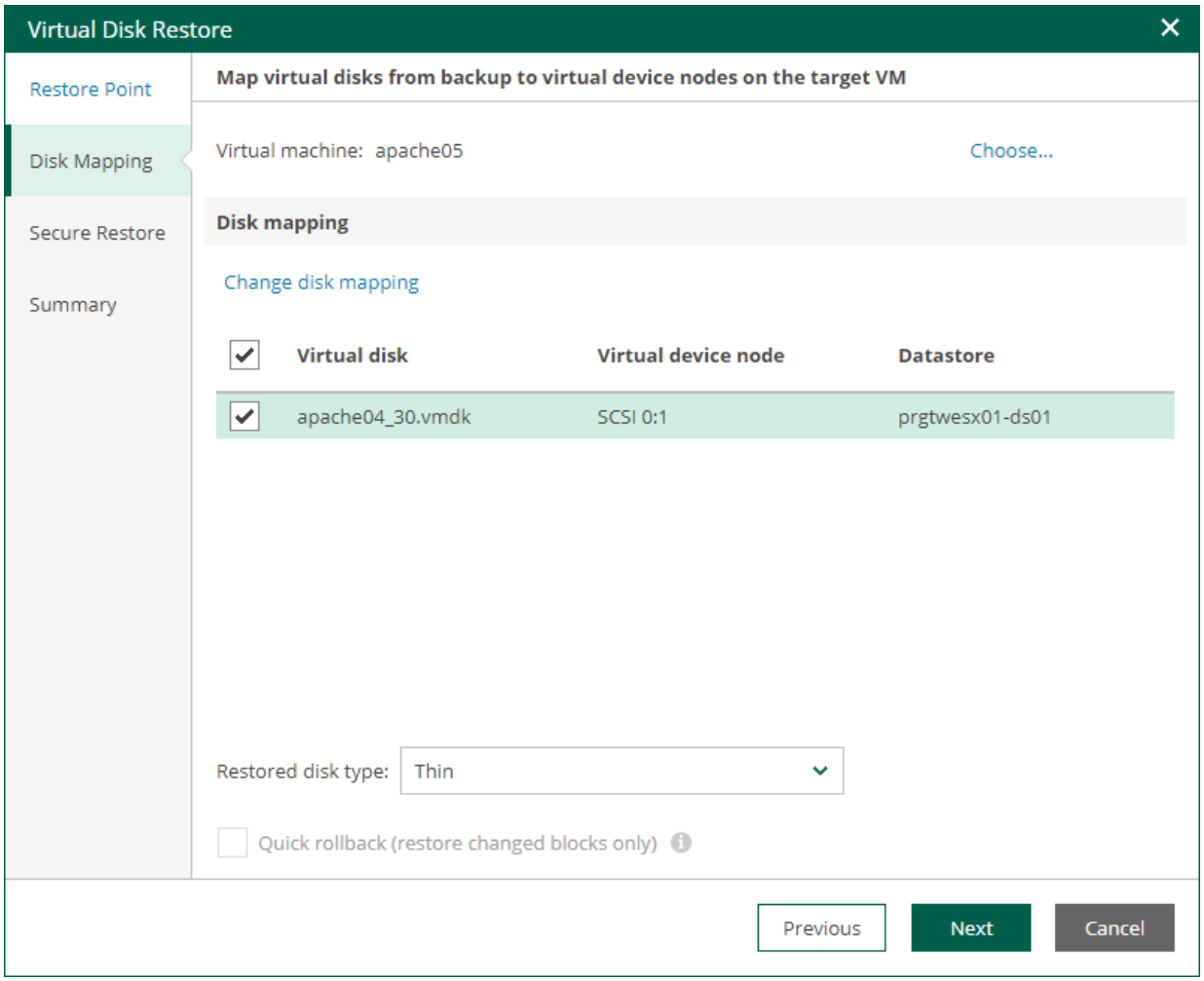
2. In the **Disk Mapping** section, select check boxes next to the virtual disks that you want to restore.

3. By default, virtual disks are restored in the original format. To change the disk format, select the necessary option from the Restore disks list: *Same as source*, *Thin*, *Thick (lazy zeroed)* or *Thick (eager zeroed)*. For more information about virtual disk formats, see the Virtual Disk Options section of the VMware vSphere documentation.

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

4. [For disk restore to the original location and with original format] Instead of restoring an entire virtual disk from a backup file, you can instruct Enterprise Manager to recover only those data blocks that are necessary to revert the disk to the selected restore point. To do this, select the **Quick rollback** check box. Quick rollback significantly reduces the recovery time and has little impact on the production environment.

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



5. By default, virtual disks are restored to the target machine with the original properties. To change disk properties, take the following steps for each disk:

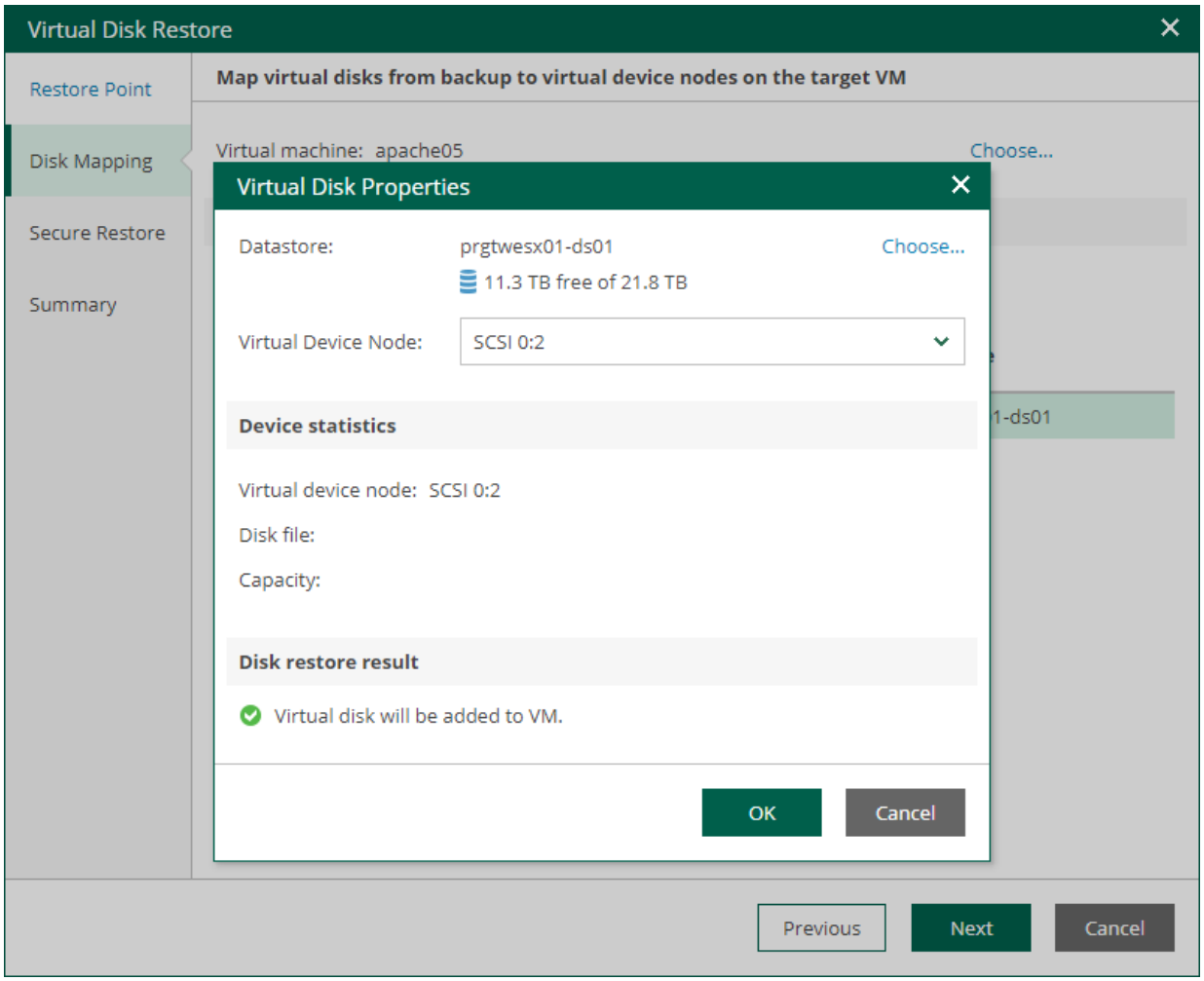
   a. In the **Disk Mapping** section, select the necessary virtual disk and click the **Change disk mapping** link.

   b. In the **Virtual Disk Properties** window, click **Choose** next to the **Datastore** field and select a datastore where the virtual disk file will be placed.

   c. From the **Virtual Device Node** list, select a virtual device node for the restored disk on the target VM:

      - If you want to replace an existing virtual disk, select an occupied virtual device node.

- If you want to attach the restored disk to the VM as a new drive, select a node that is not occupied yet.

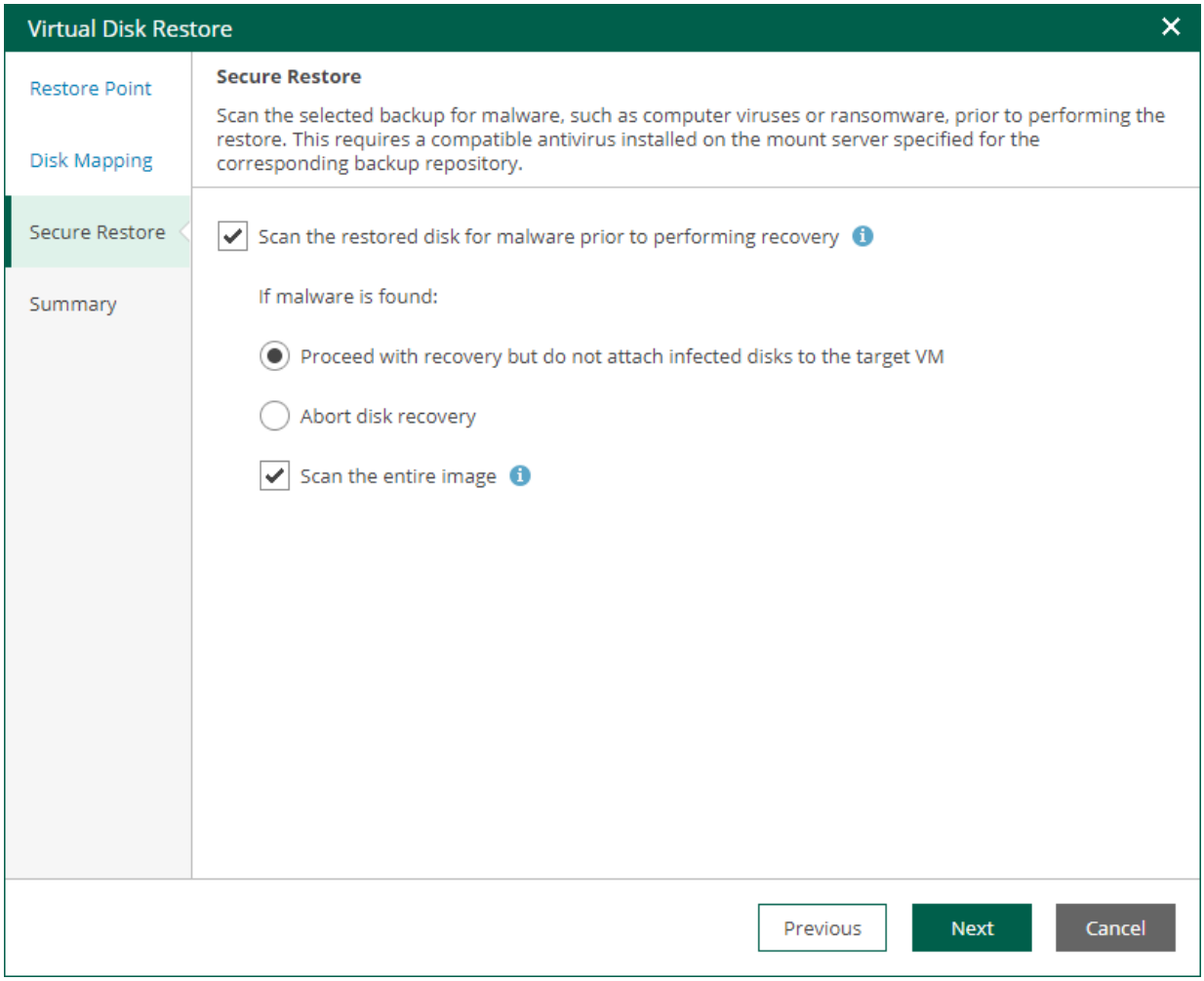


Step 4. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan virtual disk data with antivirus software before restoring the disk. For more information on secure restore, see the Secure Restore section of the Veeam Backup & Replication User Guide.

To specify secure restore settings, do the following:

1. Select the **Scan the restored disk for malware prior to performing recovery** check box.
2. Select the action that Veeam Backup & Replication will take if the antivirus finds a virus threat:
   - Select **Proceed with recovery but do not attach infected disks to the target VM** if you want to continue the virtual disk restore. In this case, the restored disk will not be attached to the target VM.
   - Select **Abort disk recovery** if you want to cancel the restore session.
3. Select the **Scan the entire image** check box if you want the antivirus to continue the machine data scan after the first malware is found.

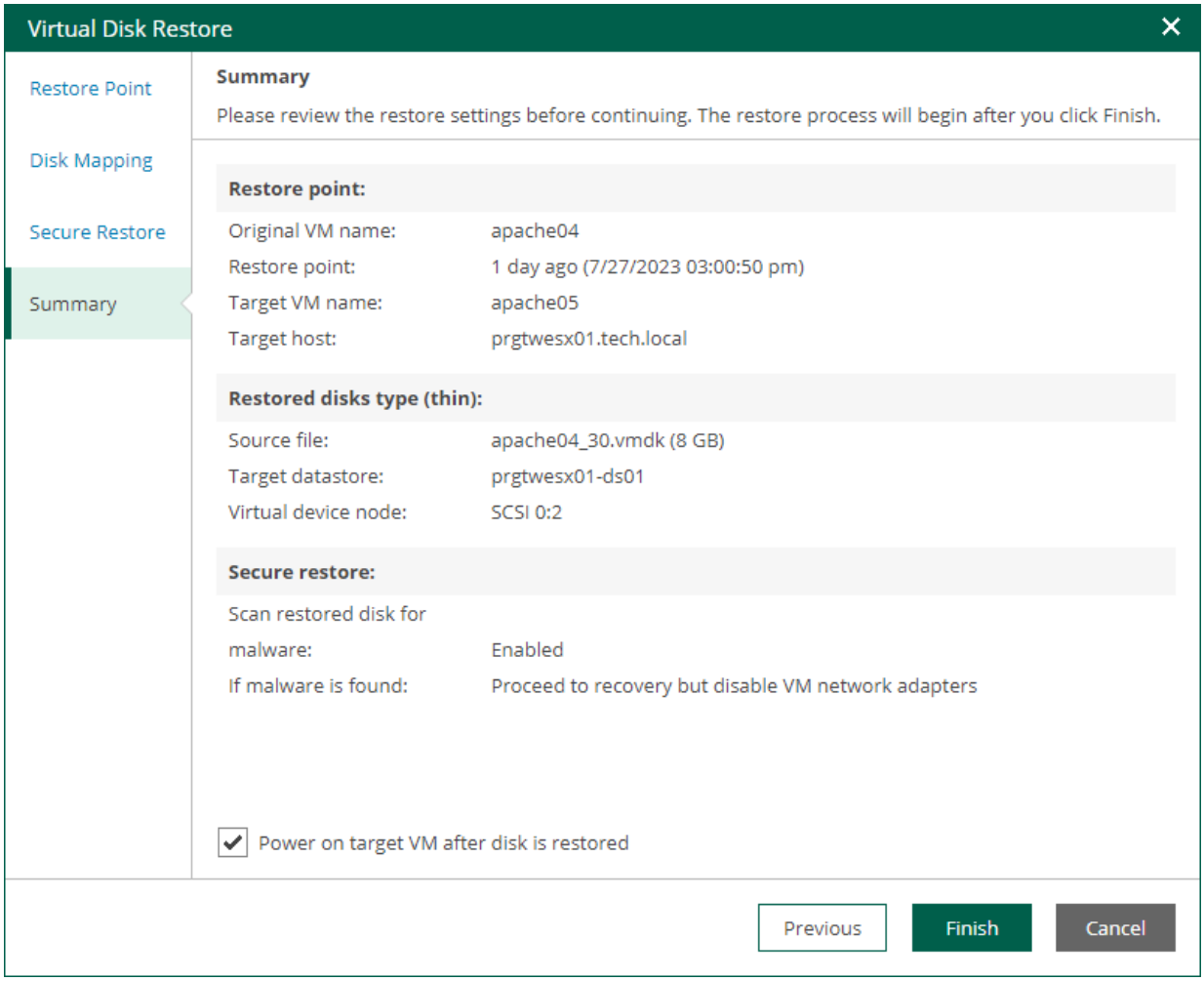


Step 5. Review Restore Settings

At the Summary step of the wizard, review the restore settings. To start a VM immediately after the restore process completes, select the **Power on target VM after disk is restored** check box. Then click **Finish**.

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **Machine and Disk Restore History** view. Note that the **Machine and Disk Restore History** view displays the restore operations initiated from both Enterprise Manager and Veeam Backup & Replication.

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



VM Failover

Failover is a process of switching from the original VM in the production site to its VM replica in the disaster recovery site.

Failover is an intermediate step that must be finalized in the Veeam Backup & Replication console. You can perform the following operations in the console:

- Undo failover to switch back to the source VM and discard all changes made to the replica while it was running.
- Perform permanent failover to permanently switch from the source VM to the replica and use this replica as the production VM.
- Perform failback to switch back to the source VM and send to the source VM all changes that took place while the replica was running.

For more information on finalizing failover, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

You can perform the following failover operations in Enterprise Manager:

- Failover of a VM processed by a regular replication job
- Failover of a VM processed by a CDP policy
- Failover of a vApp processed by a VMware Cloud Director replication job
- Failover of a vApp processed by a VMware Cloud Director CDP policy

Users with the Portal User and Restore Operator roles can perform failover of machines included in the restore scope. Users with the Portal Administrator role have no restore scope limitations. For more information on restore scope, see Configuring Restore Scope.

> **NOTE**
>
> Failover is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Failover to VM Replica

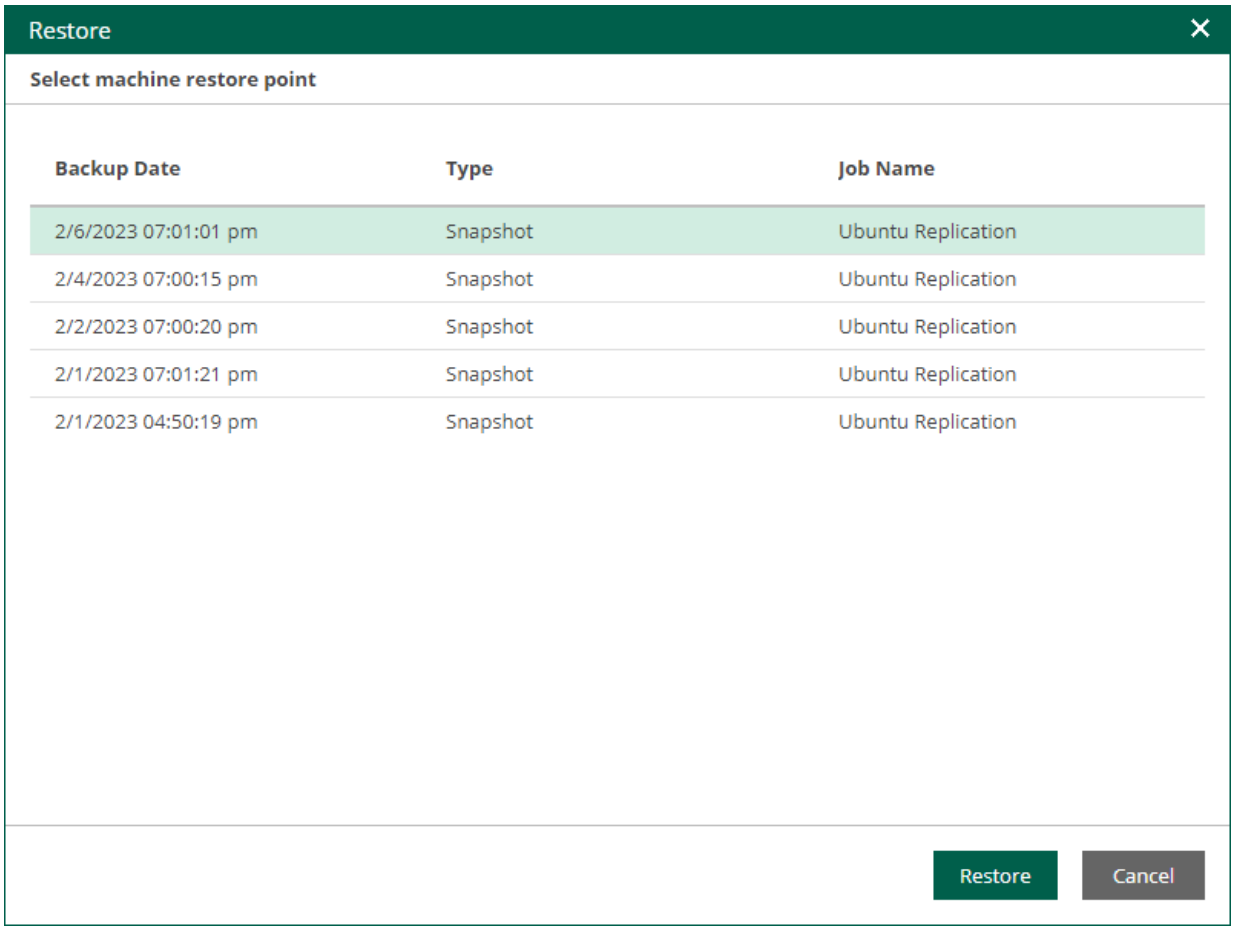
If a VM is processed by a regular replication job, you can fail over the VM to its replica. After the failover operation completes, the VM replica is powered on.

Failover is an intermediate step that you must finalize in the Veeam Backup & Replication console. In the console, you can undo failover, perform permanent failover or perform failback. For more information, see the Replica Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover:

1. On the **Machines** tab, select a machine processed by a replication job.
2. Click **Entire VM Restore**.
3. In the **Restore** window, select a restore point of the VM.
4. Click **Restore**.
5. To confirm failover, click **Yes**.

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



Failover to CDP Replica

If a VM is processed by a CDP policy, you can fail over the VM to its replica. After the failover operation completes, the VM replica is powered on.

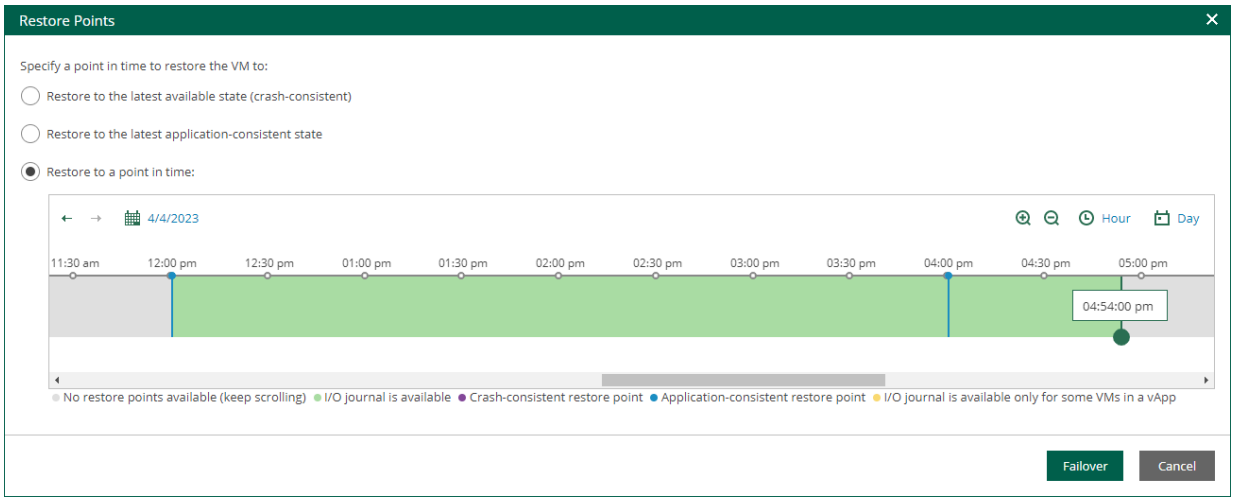
Failover is an intermediate step that you must finalize in the Veeam Backup & Replication console. In the console, you can undo failover, perform permanent failover or perform failback. For more information, see the Replica Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover:

1. On the **Machines** tab, select a machine processed by a CDP policy.
2. Click **Entire VM Restore**.
3. In the **Restore** window, select the restore point you need. You can fail over to the latest available crash-consistent state, to the latest application-consistent state or to a specific point in time.

   TIP
   - To quickly find a long-term restore point, use the calendar.
   - To zoom in or zoom out the time line, use the **Plus** and **Minus** buttons or switch between the **Hour** and **Day** views.
4. Click **Failover**.

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



Failover to Cloud Director Replica

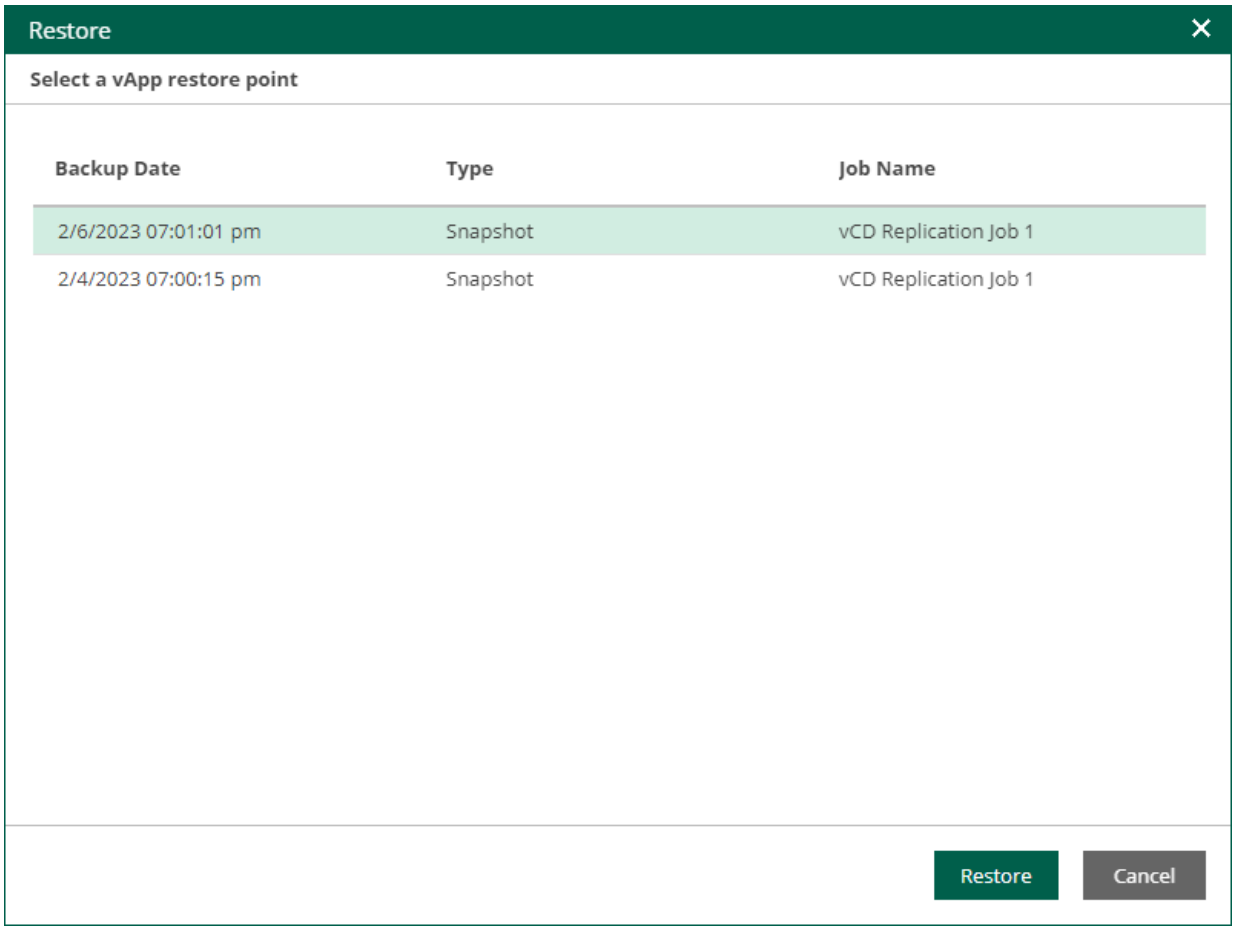
If a VM is processed by a VMware Cloud Director replication job, you can perform failover of the vApp that contains the VM.

Failover is an intermediate step that you must finalize in the Veeam Backup & Replication console. In the console, you can undo failover, perform permanent failover or perform failback. For more information, see the Replica Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover, take the following steps:

1. On the **Machines** tab, select a machine processed by a Cloud Director replication job.
2. Click **Failover Now**.
3. In the **Restore** window, select a restore point of the vApp.
4. Click **Restore**.
5. To confirm failover, click **Yes**.

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



Failover to Cloud Director CDP Replica

If a VM is processed by a VMware Cloud Director CDP policy, you can perform failover of the vApp that contains the VM.

Failover is an intermediate step that you must finalize in the Veeam Backup & Replication console. In the console, you can undo failover, perform permanent failover or perform failback. For more information, see the Replica Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover, do the following:

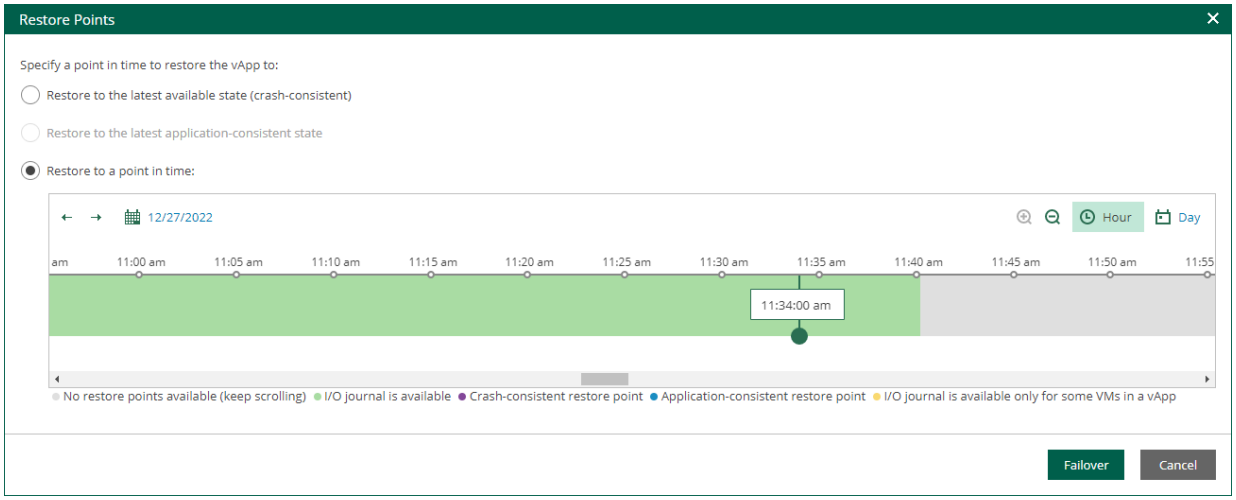
1. On the **Machines** tab, select a machine processed by a Cloud Director CDP policy.
2. Click **Restore vApp**.
3. In the **Restore Points** window, select the restore point you need. You can fail over to the latest available crash-consistent state, to the latest application-consistent state, or to a specific point in time.

   Application consistency is defined for the whole vApp. A vApp restore point is application-consistent if all VMs have application-consistent restore points. A vApp restore point is mixed if some VMs have crush-consistent restore points.

   TIP
   - To quickly find a long-term restore point, use the calendar.
   - To zoom in or zoom out the time line, use the **Plus** and **Minus** buttons or switch between the **Hour** and **Day** views.

4. Click **Failover**.

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



Failover Plans

This feature is not available for physical machine backups. If your infrastructure comprises machines running interdependent applications (for example, Exchange Server and domain controller), it is reasonable to failover them one by one, as a group. To do this automatically, you can prepare a failover plan using Veeam Backup & Replication console.

In Veeam Backup Enterprise Manager, you can run failover plans created in Veeam Backup & Replication console for VMware vSphere and Microsoft Hyper-V VMs.

Failover plan sets the following:

- The order in which the machines should be processed: for example, AD domain services server first, Exchange server after it.
- The delay time needed to start each machine. The delay time helps to ensure that certain machines (AD domain services server in our example) are already running at the time the dependent machines start.

The failover process is performed in the following way (either ad-hoc or on schedule):

1. For each machine included in the plan, Veeam Backup & Replication detects its replica (the machines whose replicas are already in Failover or Failback state are skipped from processing).
2. The replica machines are started sequentially, in the order they appear in the failover plan, within the set time intervals.

Consider that failover is a temporary intermediate step that needs to be finalized. The finalizing options for a group failover are similar to a regular failover: undoing failover, permanent failover or failback. To learn more about failover planning and recommended course of action, refer to Veeam Backup & Replication User Guide.

Veeam Backup Enterprise Manager allows you to carry out a failover following the existing plan, and also to undo planned failover.

> **NOTE**
>
> For failover plan creation, as well as for permanent failover or failback, use the Veeam Backup & Replication console.

Running Failover Plans

To run a failover plan:

1. Log in to Enterprise Manager using an administrative account or user account whose restore scope contains the machines from the failover plan.
2. Go to the **Machines** tab and click **Failover Plan**.
3. In the **Failover Plan** window, select the necessary plan from the list, then specify the starting option you need.

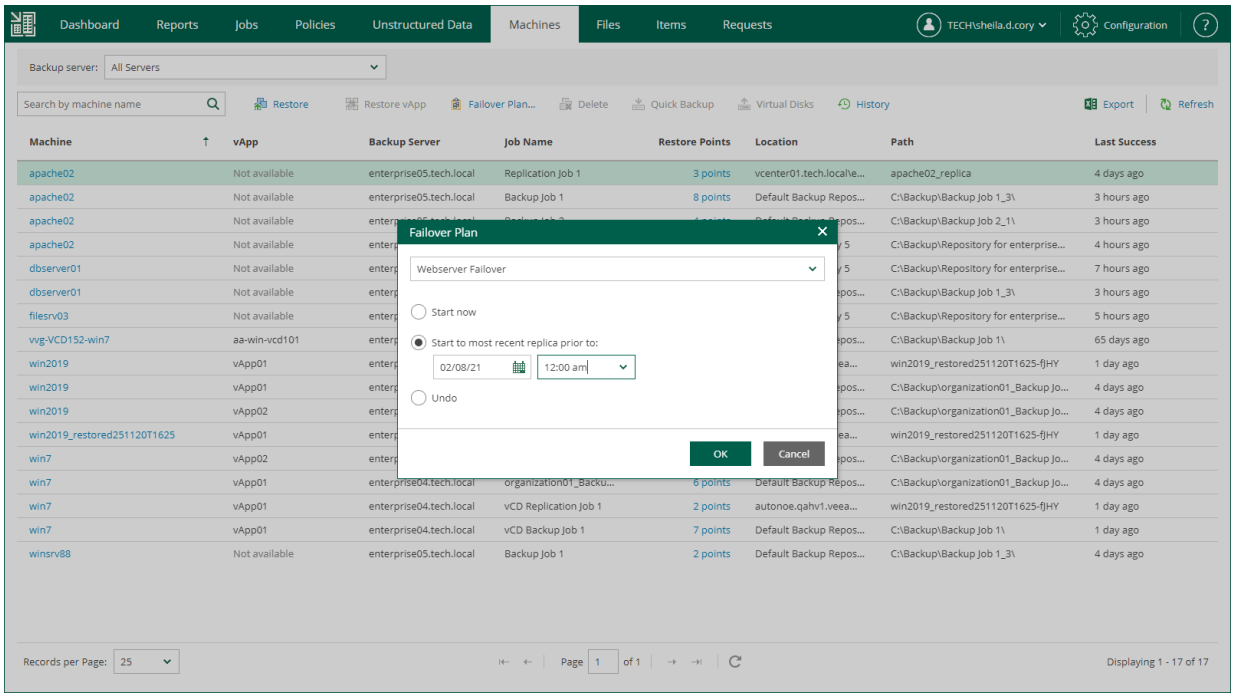
   The following options are available for a failover plan:

   - **Start now** – use this option if you need to fail over to the replicas' latest restore point.
   - **Start to most recent replica prior to** – use this option if you need to fail over to a certain restore point. For example, you may want your application server to failover to a state prior to the upgrade. In this case, for each machine participating in failover, Veeam will find the closest restore point (prior to the specified date and time) and fail over to it.

- **Undo** – use this option to switch the workload back to source machines discarding the changes that were made to the replicas during failover.

4. Click **OK** and wait for the process to complete.

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



Guest OS File Restore

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

Before you start recovering your files, consider the following:

- Browsing and restoring processes involve appropriate backup job setup, as well as file system mounting and data transfer operations. For details, see Preparing for File Browsing and Searching.
- Veeam Backup Enterprise Manager lets you browse and recover guest OS files from backups of Proxmox VE, Nutanix AHV and oVirt KVM (Oracle Linux Virtualization Manager and Red Hat Virtualization) machines. The following operations are supported:
  - For Proxmox VE and oVirt KVM, you can browse files and download them to the local machine.
  - For Nutanix AHV VMs, you can browse files, download them to the local machine, and restore them to the original location.
- To browse and restore guest OS files and application items from a physical machine backup stored in a Veeam backup repository, you need a certain Veeam Agent deployed on the machine and integrated with Veeam Backup & Replication. For more information, see Veeam Agents Support.
- 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.

How File Restore Works

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

1. To provide for browsing and search, Veeam Backup Enterprise Manager 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 backup server and copy these files from the backup server to the destination location.
3. If you select to restore files to the original location, an additional mount point will be created on the mount server associated with the backup repository storing the backup file. During restore, machine data will flow from the repository to the target, keeping the machine traffic in one site and reducing load on the network.
4. After you download or restore the necessary files, and finish the restore session, the machine disks will be unmounted.

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

1. To provide for browsing, disks of the machine from the backup file are mounted to the backup server. If you then select to download the necessary files, Veeam Backup & Replication will copy these files from the backup server to the destination location, using this mount point.
2. If you select to restore files from the backup to the original location on the production machine, an additional mount point will be created on the mount server associated with the backup repository storing the backup file.

3. If you restore files from replica, a single mount point for all these operations (browsing, download, restore to original location) will be created on the backup server.
4. After you download and restore the necessary files and finish the restore session, machine disks will be unmounted.

In This Section

- Preparing for File Browsing and Searching
- Browsing Machine Backups for Guest OS Files
- Searching for Guest OS Files in Machine Backups
- Performing 1-Click File Restore
- Restoring Files to Another Location
- Using Self-Service File Restore Portal to Restore Machine Guest Files

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 a backup server and Enterprise Manager server.

- Veeam Guest Catalog service on backup server works as a local catalog service. It collects index data for backup jobs on this specific backup server and stores data locally in the Veeam Backup Catalog folder.
- Veeam Guest Catalog service on the Enterprise Manager server works as a federal catalog service. It communicates with Veeam Guest Catalog services on backup servers connected to 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 backups for guest OS files

> **NOTE**
>
> If Veeam Backup & Replication and Veeam Backup Enterprise Manager are installed on the same machine, Veeam Backup Catalog works as a federal catalog service. This makes it impossible to replicate index data from this catalog to another Enterprise Manager. If you want to connect the backup server to another Enterprise Manager, uninstall Enterprise Manager from the current machine first.

Veeam Backup Search Capabilities

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

> **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.

By default, backup repository is the primary destination for the search. This means, in particular, that if a backup (with indexed guest) is stored both in the repository and tape, 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 for Index and History.

> **NOTE**
>
> This capability is supported in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

Searching for Physical Server Guest OS Files

If your Veeam Backup & Replication server is integrated with a Veeam Agent, you can set up the integrated Veeam Agent to create an index (catalog) of files and folders on the physical machine. This allows you to search for backed-up files and perform 1-Click file restore in Veeam Backup Enterprise Manager; all operations are similar to those performed for virtual machine backup.

For more information, see the following sections:

- Guest File Browsing and 1-Click Restore section of this guide

- Guest Processing section of the Veeam Agent for Windows User Guide
- File System Indexing section of the Veeam Agent for Linux User Guide
- File System Indexing section of the Veeam Agent for Oracle Solaris User Guide
- File System Indexing section of the Veeam Agent for IBM AIX User Guide

File-Level Restore Capabilities

When you restore files from the restore point created for a virtual or physical machine *with guest OS file indexing enabled*, Veeam uses the following workflow:

1. To provide for browsing and search, Veeam uses index data to represent the file system of the guest OS.
2. If you then select to download the necessary files, Veeam Backup & Replication will mount virtual or physical machine disks (from the restore point in repository) on the Veeam backup server and then copy these files from the backup server to the target location.
3. If you select to restore files to the original location, an additional mount point will be created on the mount server associated with the backup repository storing the backup file. During restore, machine data will flow from repository to target, keeping the machine traffic in one site and reducing load on the network.
4. After you download or restore the necessary files, and finish the restore session, the machine (or server) disks will be unmounted.

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

1. To provide for browsing, disks of the virtual machine or physical server from the backup file are mounted to the backup server.
2. If you then select to download the necessary files, Veeam Backup & Replication will copy these files from the backup server to the destination location, using this mount point.
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 backup server.
5. After you download or restore the necessary files, and finish the restore session, the machine (or server) disks will be unmounted.

How Indexing Works

When you run a backup job with the file indexing option enabled, Veeam Backup & Replication indexes the machine file system, collects indexing data and writes it to the *GuestIndexData.zip* file. The *GuestIndexData.zip* file is first stored in a temporary folder on the backup server.

As soon as the backup job completes, Veeam Backup & Replication notifies the local Veeam Backup Catalog service. The service saves indexing data in the Veeam Backup Catalog folder on the backup server. During the next catalog replication session started on Veeam Backup Enterprise Manager, indexing data from the backup server is replicated to the Veeam Backup Catalog on Veeam Backup Enterprise Manager server. By federating indexing data from all connected backup servers, the Veeam Backup Catalog service on Veeam Backup Enterprise Manager creates a global catalog for the whole backup infrastructure.

Veeam Backup & Replication supports file-level restore not only for machines included in guest catalog but also for the machines that are not indexed. Indexing may be disabled at the time of restore point creation, or indexing operation may fail. In this case, the restore point of a Windows machine is mounted to the backup server that manages the job, and the restore point of a non-Windows machine is mounted to a helper host or helper appliance.

Then a user will be able to locate the necessary files and folders and perform restore operation. For more information, see Guest OS File Restore.

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.

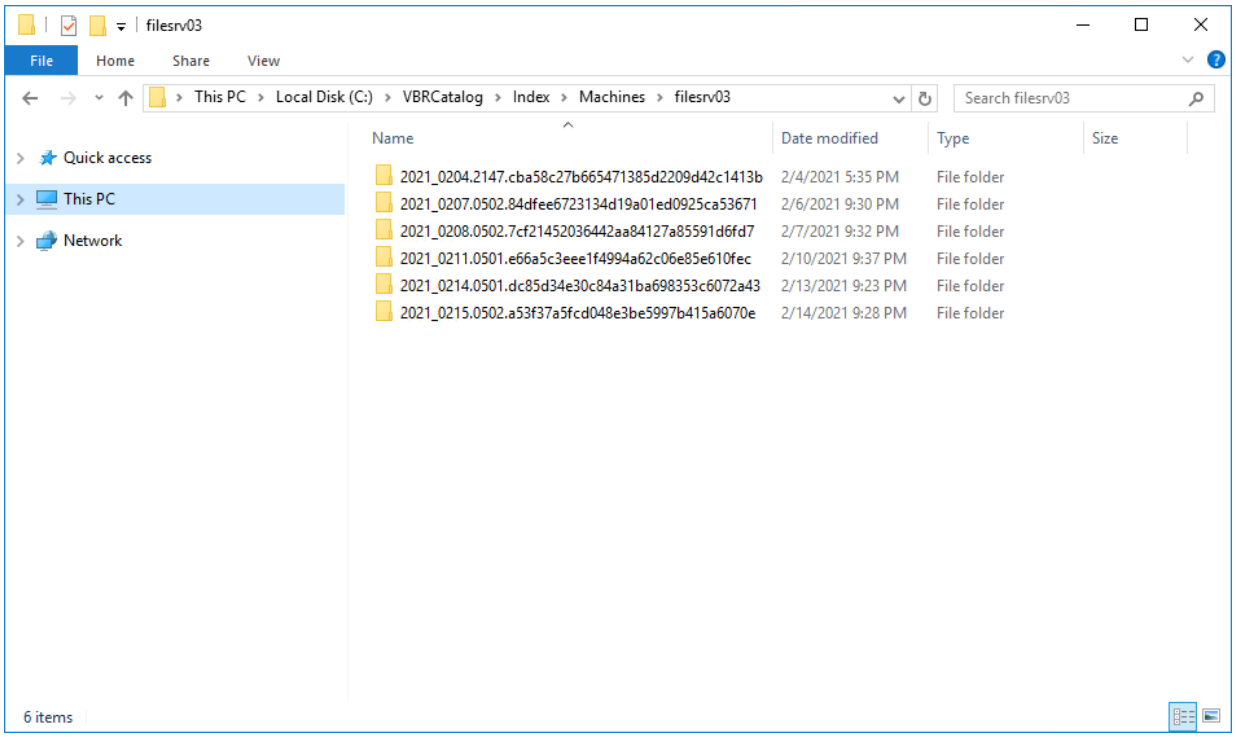
Veeam Backup Catalog comprises the following data:

- 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=05/13/2025 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\srv042025-05-13T010101.vib
grp0.file0.ModifyDateUtc=05/13/2025 08:04:10.293
grp0.file1.Server=BACKUP01
grp0.file1.Path=c:\backup\srv04\srv042025-05-13T004536.vib
grp0.file1.ModifyDateUtc=05/13/2025 07:47:52.077
grp0.file2.Server=BACKUP01
grp0.file2.Path=c:\backup\srv04\srv042025-05-13T000053.vib
grp0.file2.ModifyDateUtc=05/13/2025 07:04:24.38
grp0.file3.Server=BACKUP01
grp0.file3.Path=c:\backup\srv04\srv042025-05-12T230102.vib
grp0.file3.ModifyDateUtc=05/13/2025 06:04:25.003
grp0.file4.Server=BACKUP01
grp0.file4.Path=c:\backup\srv04\srv042025-05-12T220051.vib
grp0.file4.ModifyDateUtc=05/13/2025 05:03:53.817
grp0.file5.Server=BACKUP01
grp0.file5.Path=c:\backup\srv04\srv042025-05-12T210105.vbk
grp0.file5.ModifyDateUtc=05/13/2025 04:07:55.047
```

- **For reverse incremental backup chains**, a session indexing file contains information about all restore points engaged in the backup job session. In a reverse incremental chain, the last restore point is always a full backup. To produce a full backup and calculate incremental changes, Veeam Backup & Replication needs to address all points in the job. For this reason, the session indexing file refers not only to the restore point created with the backup job session, but also to all restore points preceding it. Additionally, a session indexing file describes groups of files that are required to restore a machine to all possible restore points. For every restore point, there is a separate group of files.

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

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

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

```
BackupServer=SRV02
JobName=srv01_reversed
SessionDateUtc=05/14/2025 11:20:18.952
####################################################
#  OIBS
oib0.VmName=srv01
oib0.BackupTimeUtc=05/14/2025 10:56:55.993
oib0.OibUID=47c62e82-3066-478c-8272-1fb65a47d601
oib0.Platform=EVmware
oib0.Group=grp1
oib1.VmName=srv01
oib1.BackupTimeUtc=05/14/2025 11:02:20.15
oib1.OibUID=d39f4a3c-2b5b-415a-ae0d-e9acc49f63a0
oib1.Platform=EVmware
oib1.Group=grp2
oib2.VmName=srv01
oib2.BackupTimeUtc=05/14/2025 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_reversed2025-05-14T035606.vrb
grp0.file0.ModifyDateUtc=05/14/2025 10:56:55.993
grp0.file1.Server=BACKUP
grp0.file1.Path=c:\backup\srv01_reversed\srv01_reversed2025-05-14T040137.vrb
grp0.file1.ModifyDateUtc=05/14/2025 11:18:14.43
grp0.file2.Server=BACKUP
grp0.file2.Path=c:\backup\srv01_reversed\srv01_reversed2025-05-14T041612.vbk
grp0.file2.ModifyDateUtc=05/14/2025 11:18:45.973
grp1.file0.Server=BACKUP
grp1.file0.Path=c:\backup\srv01_reversed\srv01_reversed2025-05-14T040137.vrb
grp1.file0.ModifyDateUtc=05/14/2025 11:18:14.43
grp1.file1.Server=BACKUP
grp1.file1.Path=c:\backup\srv01_reversed\srv01_reversed2025-05-14T041612.vbk
grp1.file1.ModifyDateUtc=05/14/2025 11:18:45.973
grp2.file0.Server=BACKUP
grp2.file0.Path=c:\backup\srv01_reversed\srv01_reversed2025-05-14T041612.vbk
grp2.file0.ModifyDateUtc=05/14/2025 11:18:45.973
BSessionVersion=5
```

A full backup file "moves forward" with every new backup job run, and Veeam Backup & Replication updates groups of files. This helps maintain valid groups of files required to restore a machine to a necessary point in time.

The session indexing files maintain groups of files for all restore points that have ever existed in the backup chain. This behavior lets you search and restore machine guest OS files in archived backups.

When a backup is archived to tape or to a secondary backup repository, you can still browse the machine file system to this point in time using historical indexing data. Once you find a necessary file, Veeam Backup Enterprise Manager uses the session indexing file to inform you what group of files is required to restore the machine to the selected point in time.



Related Topics

Current and Historical Indexing Data

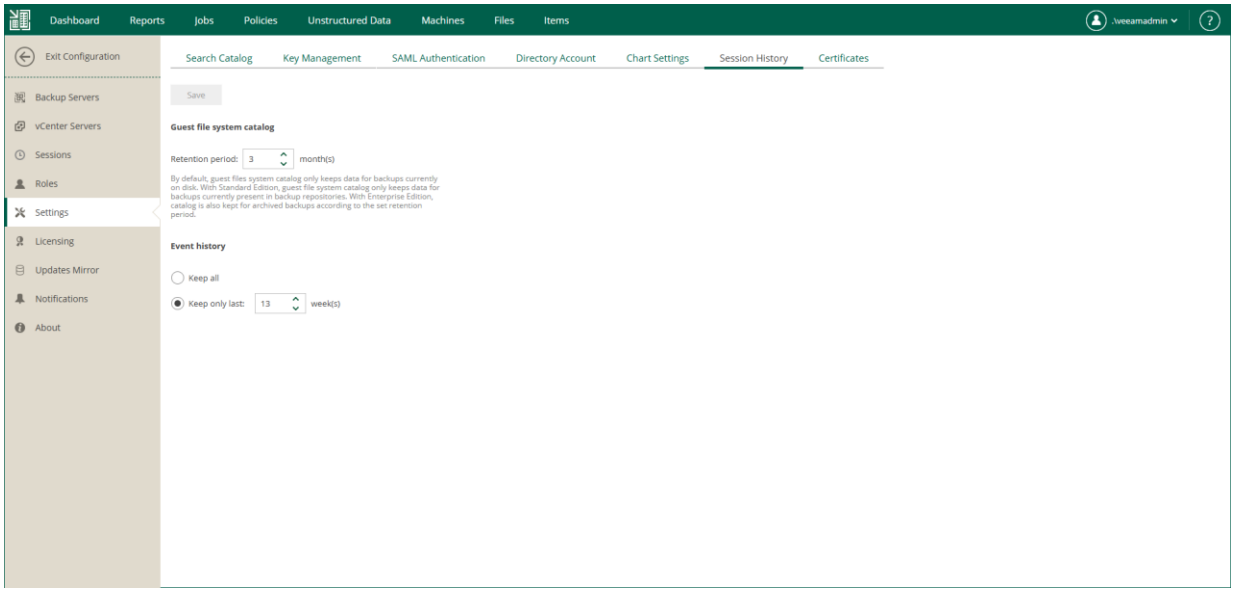
Current and Historical Indexing Data

Indexing data structures in Veeam Backup Catalog are divided into two groups:

- Current indexing data stores information for valid restore points that are currently available in the backup chain in the backup repository. For example, if the retention policy for a backup job is set to 14, Veeam Backup Catalog will contain indexing data for 14 restore points and 14 backup job sessions.
- Historical indexing data stores information for obsolete restore points: the points that were removed from the backup chain. When you run a backup job to create a new restore point, the earliest restore point is marked as obsolete and removed from the backup chain. Indexing data for this restore point in the Veeam Backup Catalog is not removed. Instead, it is marked as historical.

  Historical indexing data helps the user accomplish file search in backup files that were archived to tape or to a secondary backup repository.

By default, Veeam Backup Enterprise Manager keeps historical indexing data for 3 months. To change this value, navigate to the **Configuration** > **Settings** > **Session History** > **Guest file system catalog** section in Veeam Backup Enterprise Manager.



Related Topics

Configuring Retention Settings for Index and History

Indexing Data Retention

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

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

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

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

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

Retention for Forward Incremental Backups

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

Retention period = MAX (Catalog Retention, X)

where:

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

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

- The retention policy for a backup job is set to 5 points. The backup job is run daily.
- The retention period in Veeam Backup Enterprise Manager is set to 1 month, or 30 days.

In this case, Veeam Backup Enterprise Manager will retain indexing data for 30 days, because this value is greater than the number of restore points in the job.

Retention for Reverse Incremental Backups

For reverse incremental backup chains, Veeam Backup Enterprise Manager keeps more indexing data in Veeam Backup Catalog than it may seem to be required according to the retention policy. This happens due to backward nature of reverse incremental backups.

When Veeam Backup Enterprise Manager deletes indexing data by retention, it removes the whole set of files: machine indexing data and session indexing data. Before removing indexing data for a specific machine restore point, Veeam Backup Enterprise Manager makes sure that this restore point is not referenced by any of backup job sessions:

- If no relations are detected, indexing data for this machine restore point is removed from Veeam Backup Catalog.
- If the machine restore point is referenced by any backup job session, indexing data for this machine restore point remains in Veeam Backup Catalog.

However, in reverse incremental chains, session indexing data references the machine restore point that was created in the backup job sessions, and restore points preceding it. To learn more, see Indexing Data.



For this reason, Veeam Backup Enterprise Manager retains more indexing data for reverse incremental chains. The retention period is calculated by the following formula:

Retention period = MAX (Catalog Retention, X) + X

where:

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

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

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

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

> **IMPORTANT**
>
> The longer the backup chain, the more indexing data is stored in Veeam Backup Catalog.
>
> In case of long backup chains, indexing data may take a lot of space on the Veeam Backup Enterprise Manager server. To overcome this situation, you can adjust the retention policy scheme or provide enough space for indexing data in Veeam Backup Catalog on Veeam Backup Enterprise Manager.

Preparing for File Browsing and Searching

If you have Veeam Backup & Replication and Veeam Backup Enterprise Manager installed, you can use indexing capabilities to quickly find necessary files and folders.

To use guest file system indexing:

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

Alternatively, you can process the machine without guest file system indexing. Indexing may be disabled at the time of restore point creation, or indexing operation may fail. In this case, the restore point of a Windows machine is mounted to the backup server that manages the job, and the restore point of a non-Windows machine is mounted to a helper host or helper appliance.

Then you will be able to locate necessary files and folders and perform restore operation. For more information, see Browsing Machine Backups for Guest OS Files.

In This Section

- Performing Catalog Replication and Indexing
- Preparing for File Search and Restore (non-Windows machines)

Performing Catalog Replication and Indexing

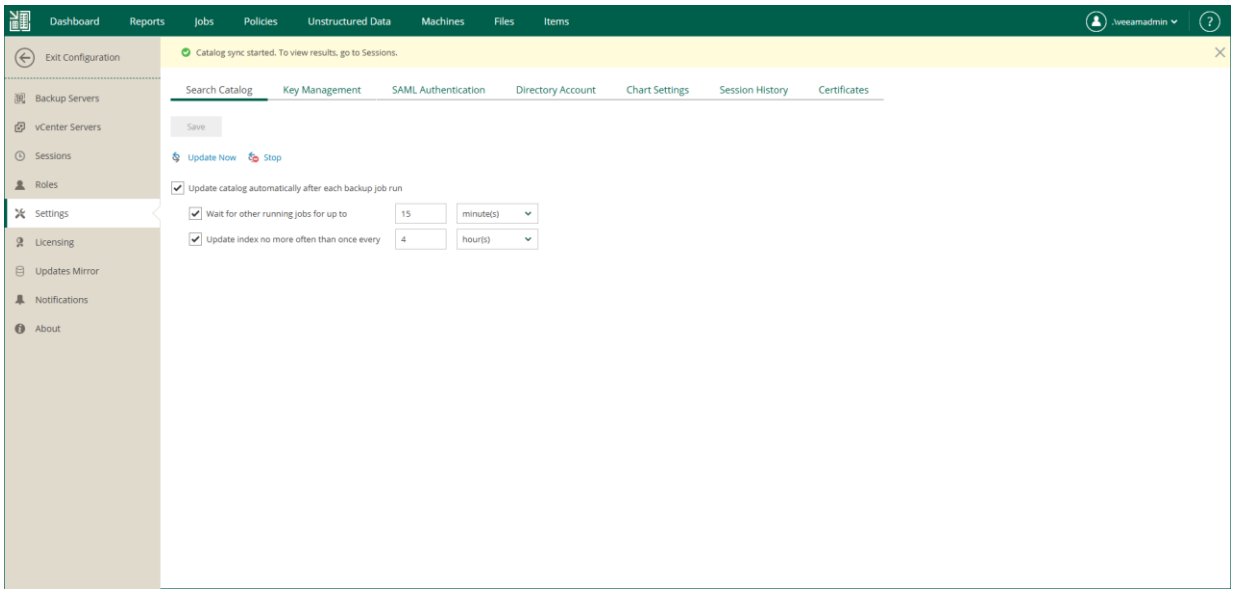
Once you have run backup jobs with guest OS file system indexing enabled, perform catalog replication to consolidate index files from multiple backup servers. During this operation, Veeam Backup Enterprise Manager aggregates index data from multiple backup servers and stores them on the Veeam Backup Enterprise Manager server to enable file browsing and search.

> **NOTE**
>
> Catalog replication is performed for the machines with indexed guest OS file systems on all managed backup servers.

Veeam Backup Enterprise Manager provides two options to perform catalog replication:

- To perform manual catalog replication, open the **Settings** tab of the **Configuration** view and click **Update Now** on the **Search Catalog** tab.
- To automatically run catalog replication after every backup job, open the **Settings** tab of the **Configuration** view. On the **Search Catalog** tab, select **Update catalog automatically after each backup job run** and specify other options as required.

Every run of a catalog replication job initiates a new job session which can be tracked on the **Sessions** tab of the **Configuration** view. To view detailed information for a specific session, select it in the list of sessions and click the link in the **Status** column.



Preparing for File Search and Restore (non-Windows machines)

To view, search and restore guest files of non-Windows machines, take the following preparatory steps:

1. To enable guest file indexing, use one of the options of the machine backup job: **Index everything**, **Index everything except**, or **Index only following folders** option. For more information, see the Guest OS File Indexing section of this guide and the VM Guest OS File Indexing section of the Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > Guest file indexing is optional. You can browse and restore files from the restore points created without guest indexing. For more information, see Browsing Machine Backups for Guest OS Files and Performing 1-Click File Restore.
   >
   > If you want Veeam Backup Enterprise Manager to display symbolic links to folders when browsing through the machine file system at 1-click file restore, enable indexing in the backup job for that machine.

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

3. By default, guest file restore to the original location is performed using the account specified in the machine backup job. If it does not have sufficient access to target machine, you are prompted to specify another account with sufficient access rights.

   For more information, see the Guest OS Credentials section of this guide and the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Preparing Helper Host or Helper Appliance

When restoring guest OS files, Veeam Backup & Replication mounts machine disks from backup or replica to a helper host or appliance. You specify helper host (or appliance) settings on the backup server when you configure guest OS file restore. These settings are saved in the backup server configuration database for the specific user that configured the restore. Before you start file-level restore from Enterprise Manager, ensure the settings are properly configured on the backup server. For more information, see the Guest OS File Restore section of the Veeam Backup & Replication User Guide.

When you start guest OS file restore from Enterprise Manager, the helper host or appliance is selected according to the following algorithm:

1. Enterprise Manager attempts to obtain the helper host or appliance settings from the configuration database of the backup server.

2. If no helper host or appliance configuration is found for the user account, Veeam Backup & Replication uses the configuration that was last selected at the **Helper host** step of the **Guest File Restore** wizard. For details, see the Specify Helper Host section of the Veeam Backup & Replication User Guide.

3. If the **Guest File Restore** wizard has not been launched, Enterprise Manager checks whether a default Linux mount server is configured on the backup server. If the mount server exists, Enterprise Manager uses it for Linux file restore.

4. If no default Linux mount server is found, Enterprise Manager displays an error.

NOTE

- Enterprise Manager does not support mounting the restore point to the original host. If the configuration obtained from the backup server is set to original host, Enterprise Manager displays an error. In this case, you must configure a helper host or appliance on the backup server. For details, see the Specify Helper Host section of the Veeam Backup & Replication User Guide.
- If you plan to deploy multiple helper appliances to restore machines backed up by different backup servers, their initial configuration must be performed on the backup servers. Centralized configuration from Enterprise Manager is not supported.
- If you configure a helper appliance for tenants that will perform self-service restore (from Veeam Self-Service Backup Portal or vSphere Self-Service Backup Portal), be aware that multiple tenants may run the restore procedure at the same time. In this case, if you have configured a static IP address for helper appliances, a tenant will not be able to deploy a helper appliance until the IP address is in use by a helper appliance of another tenant. To let tenants start multiple helper appliances, use a DHCP server in your network and configure the helper appliance to obtain an IP address automatically.

Browsing Machine Backups for Guest OS Files

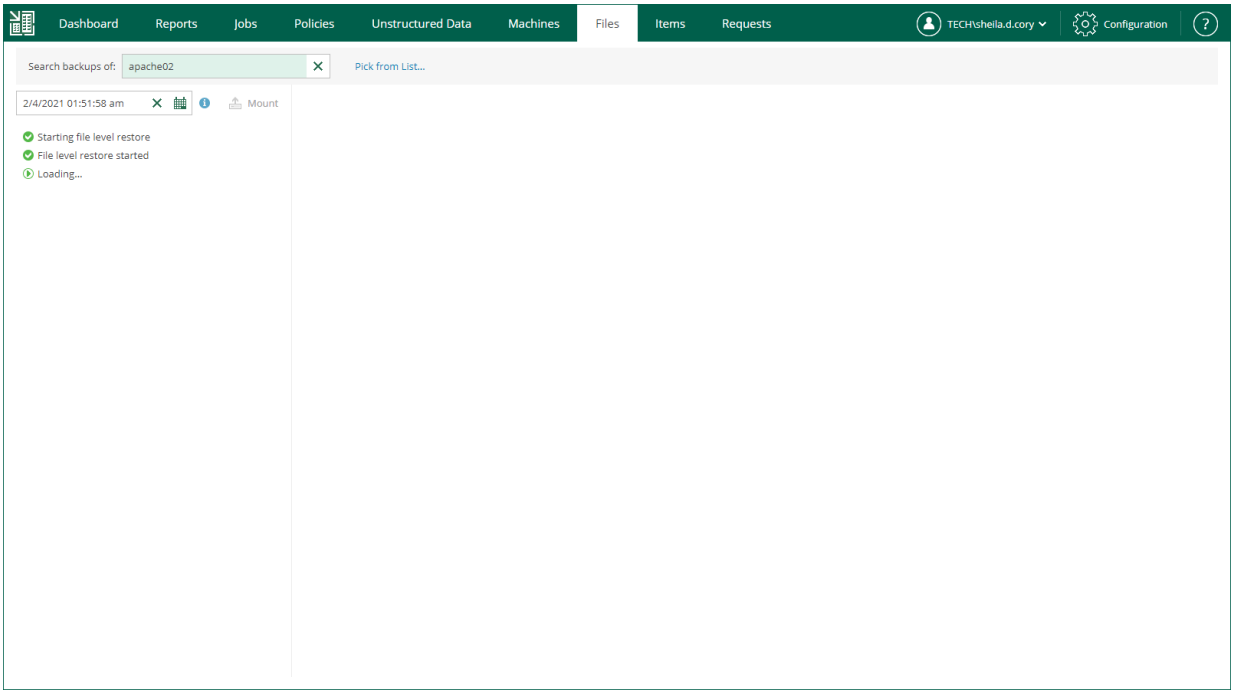
After catalog replication, you can browse any machine backup for OS guest files. Note that with the file browsing functionality, you can browse and search for files in the selected machine backup at a specific restore point only.

If you are using the Enterprise or Enterprise Plus license edition in your virtual environment, consider that Veeam Backup Enterprise Manager keeps index files for backups that are currently stored on disk, and for archived backups (for example, backups that were recorded to tape). Thus, you will be able to browse and search through backup contents even if the backup in repository is no longer available.

To browse guest OS files in a machine backup:

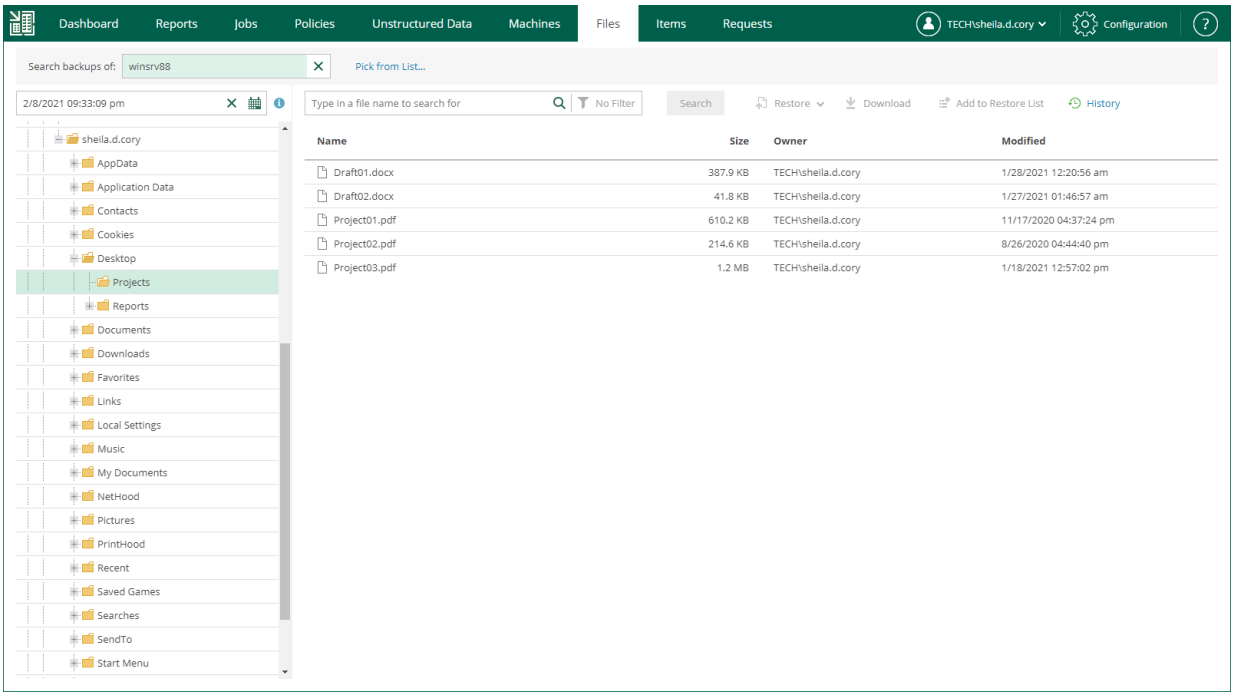
1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a machine whose files you want to restore or click the **Pick from List** link and select the necessary machine in the **Select Object** window.
3. To specify a restore point from which to restore guest OS files, click the calendar icon in the restore point field and select a date and a restore point created on that date. If multiple jobs have processed the machine, a job name will be also displayed for each restore point.

   You can only choose the dates when at least one restore point was created. By default, the latest restore point is selected in the restore point field.
4. If the machine has been backed up without guest indexing, click **Mount**. If the machine guest OS information has not been collected during the backup, you will be also prompted to specify the guest OS type. Machine disks from the backup will be mounted to Veeam backup server to present machine file system to you; wait for the process to complete.



If the machine has been backed up with guest indexing enabled, no additional operations are needed.

As a result, the file tree of the machine as of the selected backup and restore point date will be displayed. You can manually browse the file tree or use the search field to find a necessary file. Consider that depending on the number of files on the machine, the search process may take some time.



IMPORTANT

For machines processed without indexing, you can only use browsing or search to find the necessary files within the selected restore point. Advanced search capabilities (including search through multiple restore points) are available only for machines processed with guest indexing enabled.

Searching for Guest OS Files in Machine Backups

Veeam Backup Enterprise Manager allows you to search for guest OS files in all machine backups with guest indexing enabled. After you find necessary files, you can select them to perform file restore.

> **IMPORTANT**
>
> By default, backup repository is the primary destination for the search. This means, in particular, that if a backup (with an indexed guest) is stored both in a repository and tape, the Enterprise Manager search results will only include the files from backup stored in the repository. Files from tape-archived backup will appear in search results only if nothing is found in the repository (the capability is supported in the Enterprise and Enterprise Plus editions).

You can use one of the following search modes:

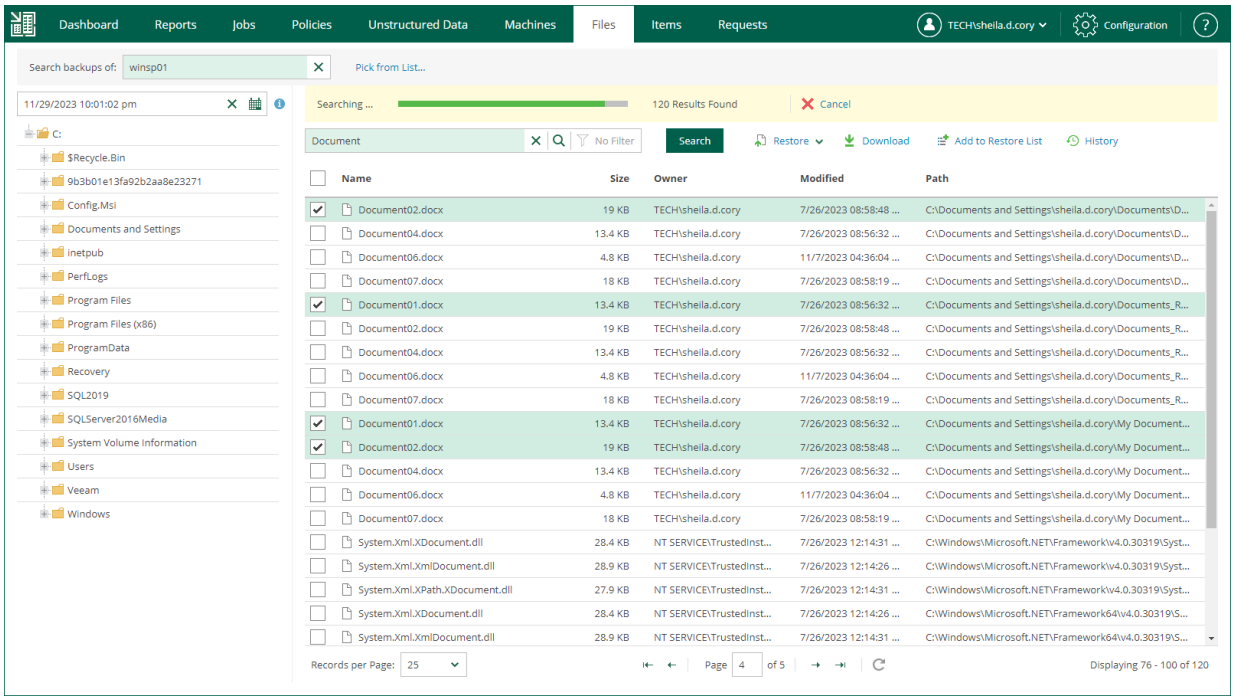
- Simple search — allows you to search for files in a selected restore point of a selected machine backup
- Advanced search — allows you to search for files in all restore points of a selected machine backup and filter search results by certain criteria

Performing Simple Search

With simple search, you can search for files in a selected restore point of a selected machine backup. After you find necessary files, you can select them to perform file restore.

To perform simple search, do the following:

1. Open the **Files** tab.
2. In the **Search backups of** field, enter the name of a machine whose files you want to restore or click the **Pick from List** link and select the necessary machine in the **Select Object** window.
3. In the search field, enter a file or folder name, or a part of it.
4. To view the search results, press [Enter] or click **Search**.

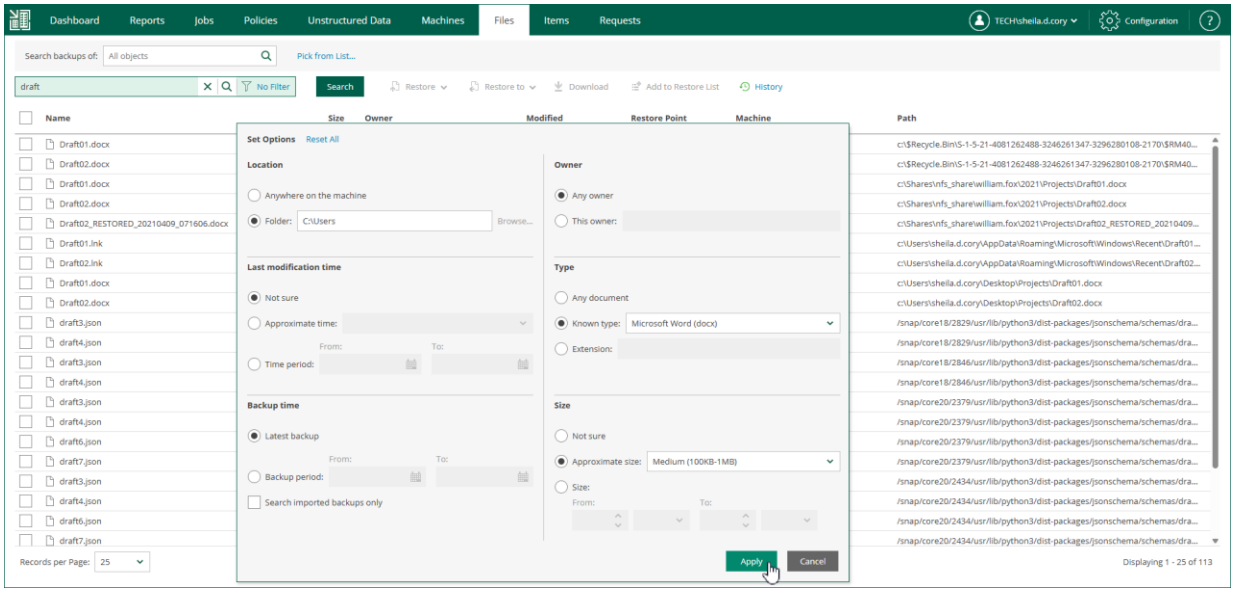


Performing Advanced Search

With advanced search, you can search for files in all restore points of a selected machine backup and filter search results by certain criteria. After you find necessary files, you can select them to perform file restore.

To perform an advanced search, take the following steps:

1. Open the **Files** tab.
2. If you know the necessary file name or a part of the name, specify it in the search field.
3. To open advanced search options, click **No Filter** next to the search field.
4. In the **Set Options** window, define the necessary search criteria:
   - **Location** – select a specific folder on the machine to search in.
   - **Last modification time** – specify approximate time when the file was last modified or set a time interval.
   - **Backup time** – choose to search through the latest backup of the specified machine or all backups of the machine created within a certain time interval.
   - **Owner** – select to search for files with a specific owner.
   - **Type** – select to search for files of specific type or with a certain extension.
   - **Size** – specify approximate size of file or set a size range.
5. To apply the filter, click **Apply**.
6. Click **Search** on the right of the search field.



Performing 1-Click File Restore

After you find the necessary files and folders, you can use Veeam Backup Enterprise Manager to restore them from backup with one click. You can choose to restore it to the original location or download it to the local machine.

IMPORTANT

Consider the following:

- 1-Click file restore capability is available if you have the Enterprise or Enterprise Plus edition.
- 1-Click file restore from a storage snapshot is not supported by Veeam Backup Enterprise Manager.

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

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

NOTE

Consider the following:

- If you plan to restore a file from a machine backed up without guest indexing, consider that for restore operation this machine disk will be mounted directly from the backup in the repository to the mount server associated with that repository; when restoring from replica, it will be mounted to the backup server. When restoring from an indexed machine, no interim mount operations are needed.
- If you want Veeam Backup Enterprise Manager to display symbolic links to folders when browsing through the machine file system at 1-click file restore, then you should enable indexing in the backup job for that machine (running Linux or another non-Windows OS).

In This Section

- Restoring Files to the Original Location
- Downloading Files to the Local Machine
- Using Restore Lists

Restoring Files to Original Location

In this restore scenario, Veeam Backup Enterprise Manager extracts file system objects (files or folders) from the backup and restores it to the original production machine. File restore 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.

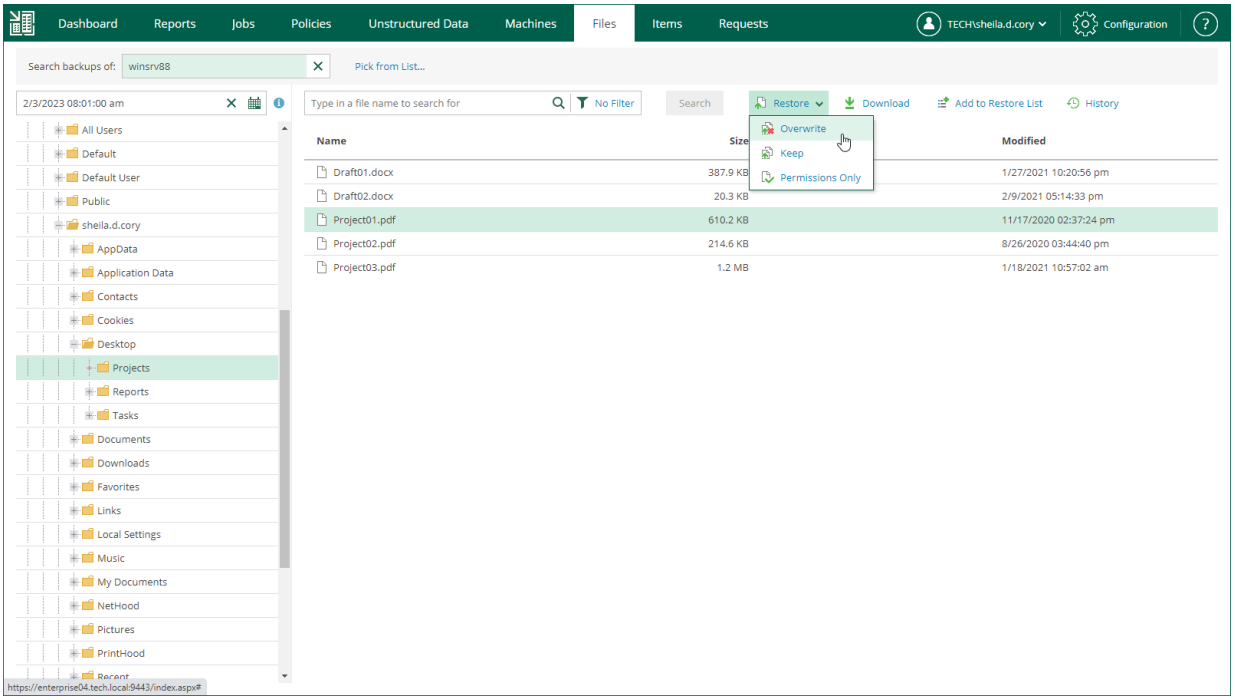
> **IMPORTANT**
>
> Consider the following:
>
> - This type of restore is only possible if the original machine is powered on and resides in the original location.
> - By default, guest file restore to the original location is performed using the account specified in the backup job for guest OS access. If it does not have sufficient rights to access the target machine, you are prompted for the credentials. Specify user account and password, as required. For more information, see Guest OS Credentials.

To restores objects to the original location, do the following:

1. Find the objects you want to restore. You can select one or multiple objects. For details, see Browsing Machine Backups for Guest OS Files and Searching for Guest OS Files in Machine Backups.
2. Click **Restore** and choose how to restore the selected objects:
   - If you select **Overwrite**, the object from the backup will replace the original object on the target machine.
   - If you select **Keep**, the object from the backup will be restored next to the original object on the target machine. The restored object will have the *_RESTORED_<DATE>_<TIME>* prefix in its name, where *<DATE>_<TIME>* is the restore date and time.
   - [For Microsoft Windows] If you select **Permissions Only**, you will restore file (or folder) permissions that were granted to users and groups to access the object. You can restore permissions only if the object exists on the target machine.
3. In the displayed window, click **Yes**.

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

Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **File Restore History** view. Note that the **File Restore History** view displays only the restore operations initiated from Enterprise Manager; restore operations initiated from Veeam Backup & Replication are not displayed.

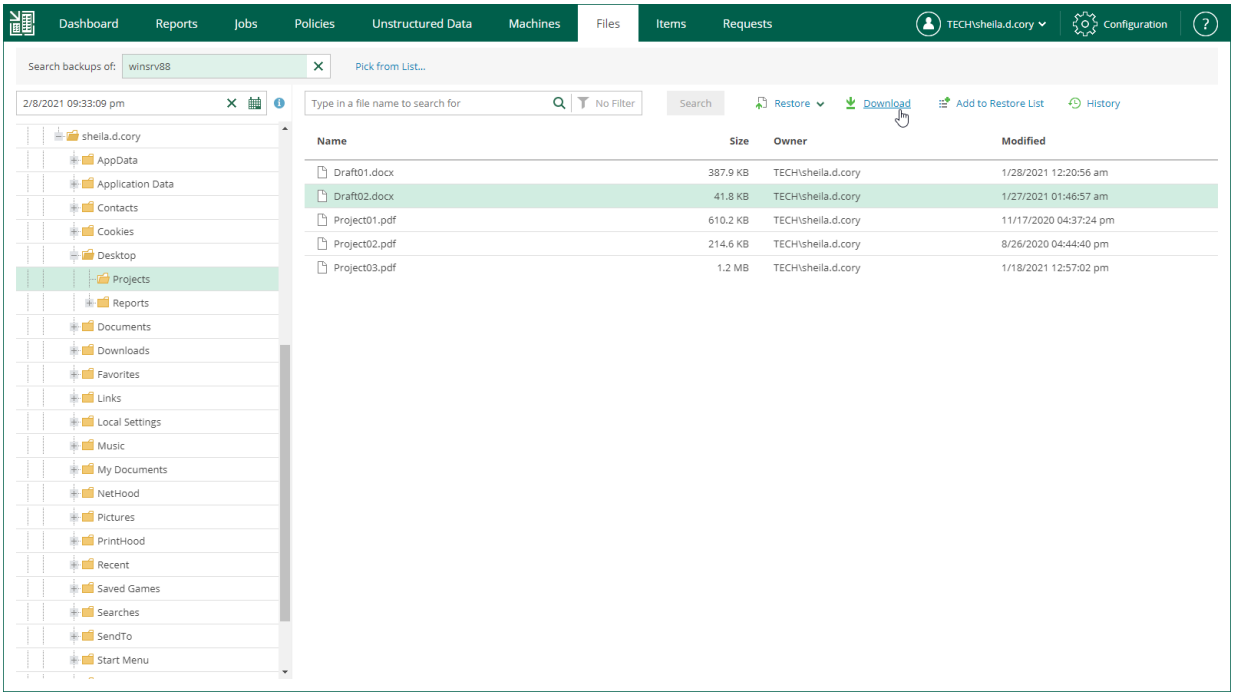


Downloading Files to Local Machine

You can download file system objects (files and folders) to your local machine. After you choose to download the objects, Veeam Backup Enterprise Manager interacts with the backup server to extract them from a backup and saves them to the default download folder on your local machine. If you download a single file, it is also saved in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Multiple files are packed in a ZIP file named `FLR_<date>_<time>.zip` and stored in the same folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.

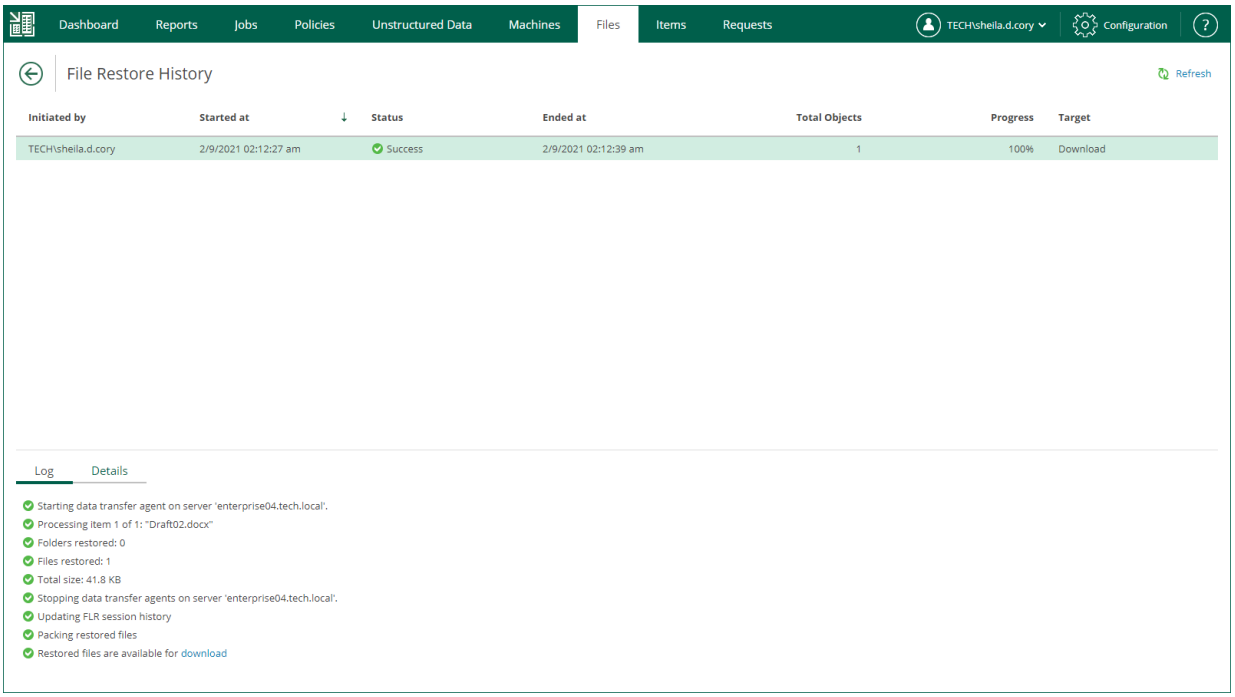
To download objects to the local machine, do the following:

1. Find the objects you want to restore. You can select one or multiple objects. For details, see Browsing Machine Backups for Guest OS Files and Searching for Guest OS Files in Machine Backups.
2. Click **Download**.



3. In the displayed window, click **Yes**.
4. Wait for restore session to complete and for the objects to be retrieved from the backup.
5. In the **File Restore History** view, select the restore session from the list.

6. On the **Log** tab, find the *Restored files are available for download* record of the session log and click the **download** link.



Using Restore Lists

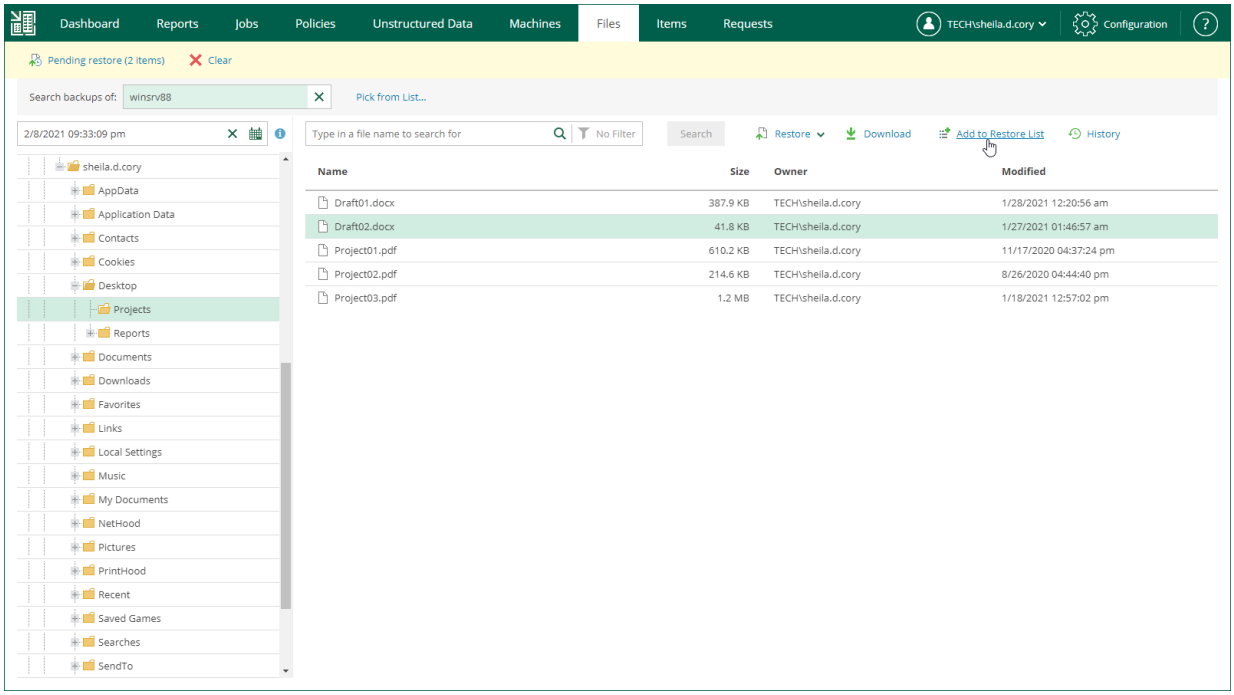
If you want to restore multiple file system objects (files or folders), you can add the necessary files to the restore list and then restore all files at once. Using the restore list helps you prepare for file restore from different machines and restore points.

Adding Objects to Restore Lists

To add objects to the restore list, do the following:

1. Find the objects you want to restore. You can select one or multiple objects. For details, see Browsing Machine Backups for Guest OS Files and Searching for Guest OS Files in Machine Backups.
2. Click **Add to Restore List**.

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



Restoring Objects from Restore Lists

After you add all objects to the restore list, you restore them. To restore the objects, do the following:

1. In the restore list notification, click **Pending restore**.
2. In the **Pending Restore** window, select check boxes next to files in the restore list that you want to restore. Use the check box next to the header of the **Name** column to select all files in the list at once.

   If you want to remove a file from the restore list, select the file and click **Delete**.
3. Click the **Restore** or **Download** link to perform the necessary restore operation for the selected files.
4. In the displayed window, click **Yes**.

5. [For the download operation] Wait for restore session to complete. On the **Log** tab of the **File Restore History** view, click the **download** link.

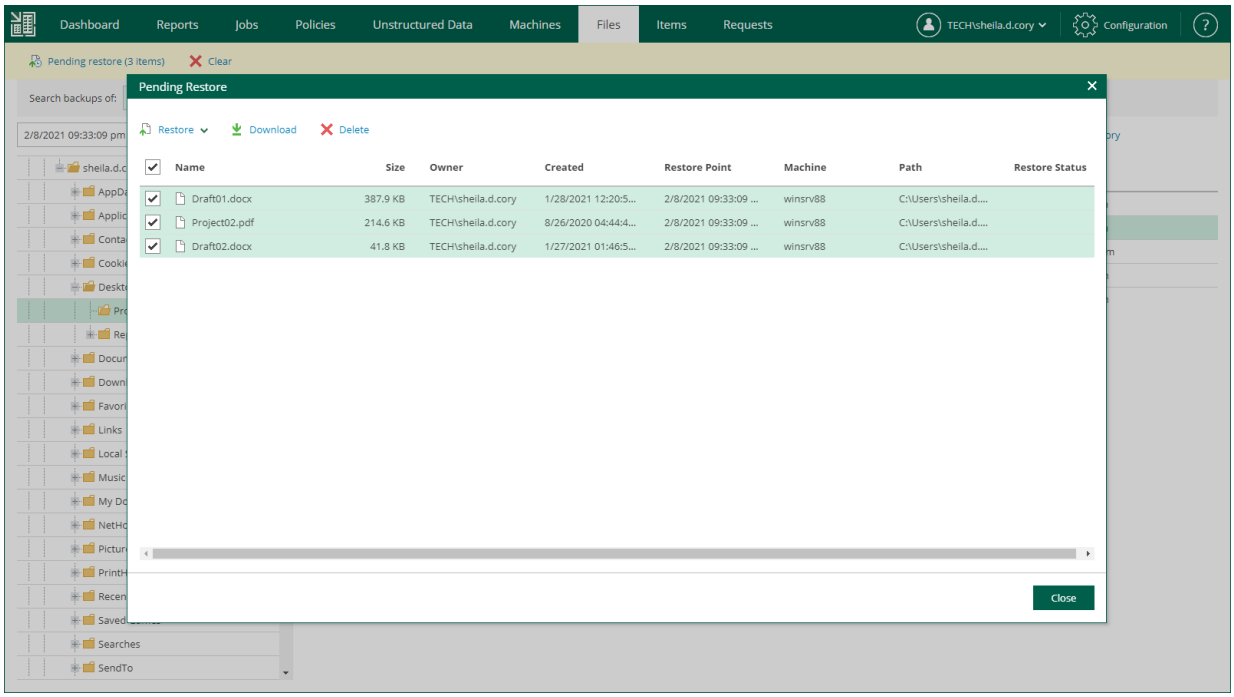
   The objects are saved to the default download folder on your local machine.

   Multiple files are also saved in a ZIP file named `FLR_<date>_<time>.zip` in the `%ProgramData%\Veeam\Backup\WebRestore` folder. Veeam Backup Enterprise Manager cleans up the folder periodically. Files older than 24 hours are automatically deleted. To change the default storage folder, contact Veeam Customer Support.

TIP

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

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



Restoring Files to Another Location

Enterprise Manager enables you to restore specific files from backup of a Microsoft Windows VM to another Microsoft Windows VM. You can also use this option to restore files to to the same VM but a different location.

To restores files to another location, do the following:

1. Find the objects you want to restore. You can select one or multiple objects. For details, see Browsing Machine Backups for Guest OS Files and Searching for Guest OS Files in Machine Backups.
2. Click **Restore to** and choose one of the following options:
   - Select **Overwrite**, to replace an object with the same name on the target machine with the object from the backup.
   - Select **Keep**, to restore the object from the backup next to the object on the target machine. The restored object will have the *_RESTORED_<DATE>_<TIME>* prefix in its name, where *<DATE>_<TIME>* is the restore date and time.
3. In the displayed window, click **Yes** to proceed.
4. In the **Restore To** window, specify restore location and credentials for connection to the target machine.

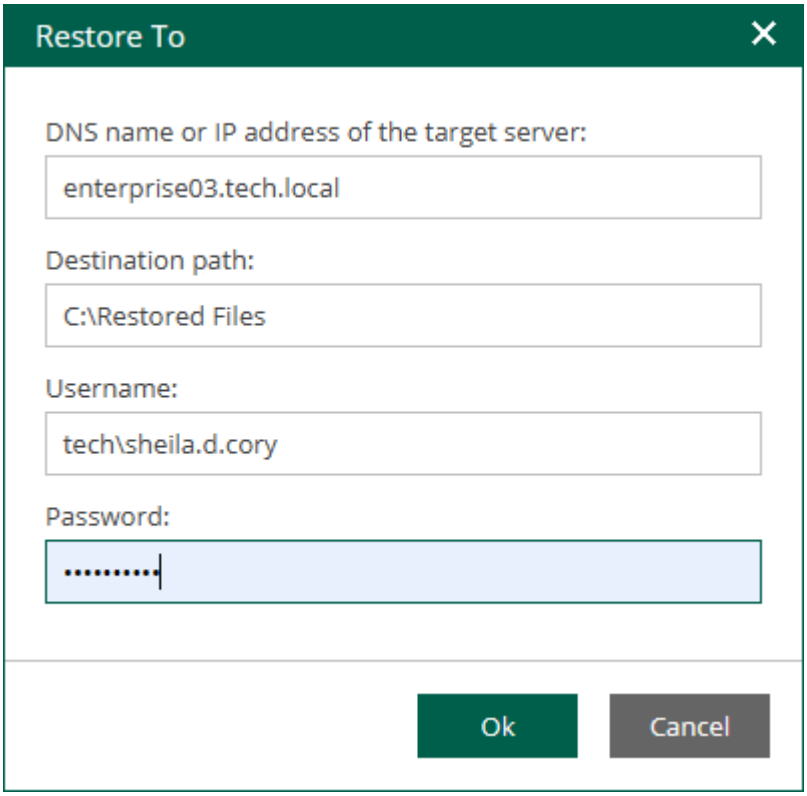
   For Microsoft Windows machines, specify the following settings:

   a. In the **DNS name or IP address of the target server** field, specify a DNS name, IPv4 or IPv6 address of a Microsoft Windows machine.

   b. In the **Destination path** field, specify a path to the folder on the target machine where the files must be restored. If the destination folder does not exist, it will be created.

   c. In the **Username** and **Password** fields, specify credentials required for connection to the target machine.

d. To start restoring files, click **OK**.



For Linux machines, specify the following settings:

a. In the **DNS name or IP address of the target server** field, specify a DNS name, IPv4 or IPv6 address of a Linux machine.

b. In the **Destination path** field, specify a path to the folder on the target machine where the files must be restored. If the destination folder does not exist, it will be created.

c. In the **Username** and **Password** fields, specify credentials required to connect to the target machine.

   If you specify a non-root account that does not have root privileges on the Linux machine, you can grant this account elevated permissions as follows:

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

   ii. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the root account password.

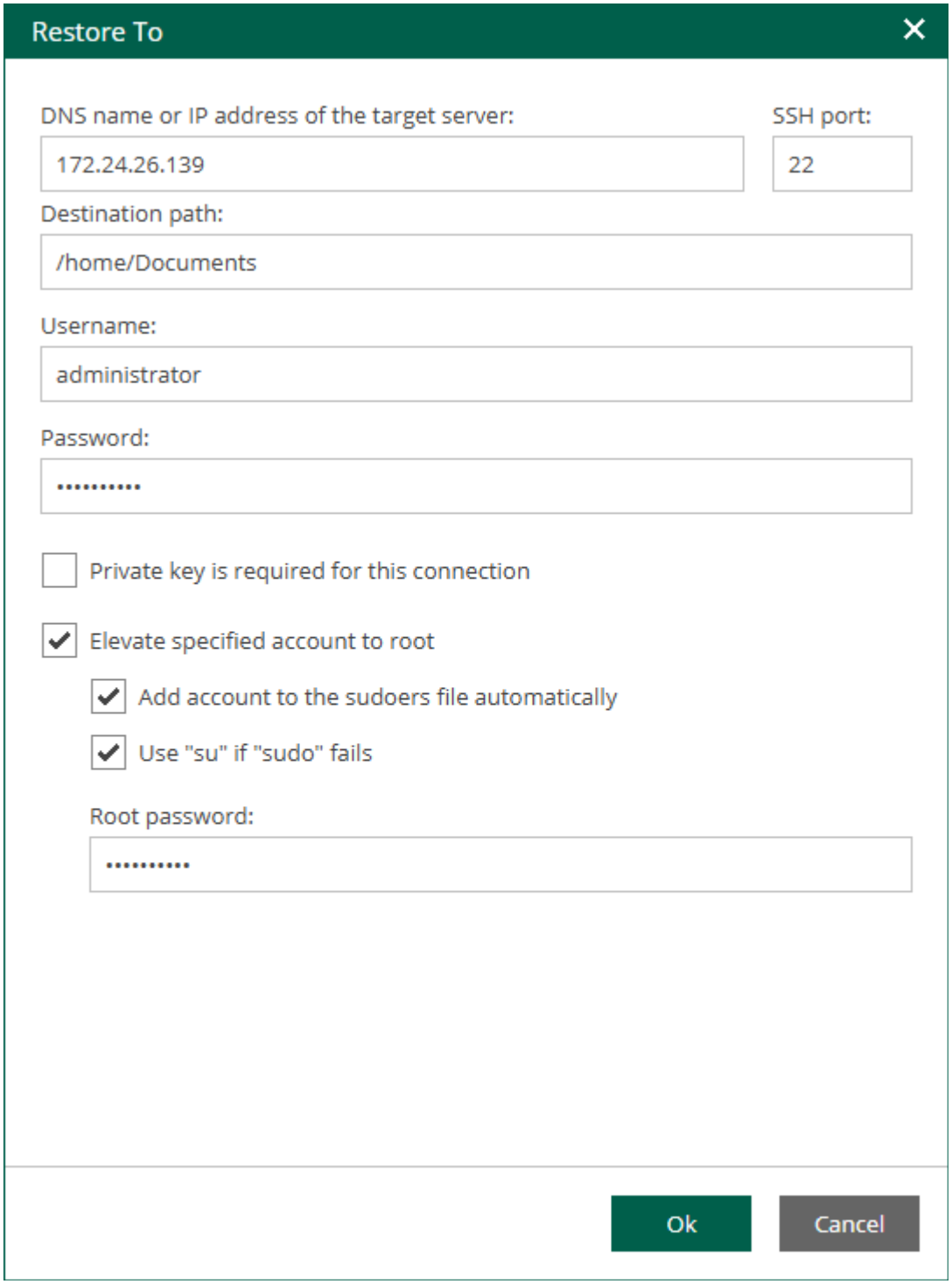
   If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

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

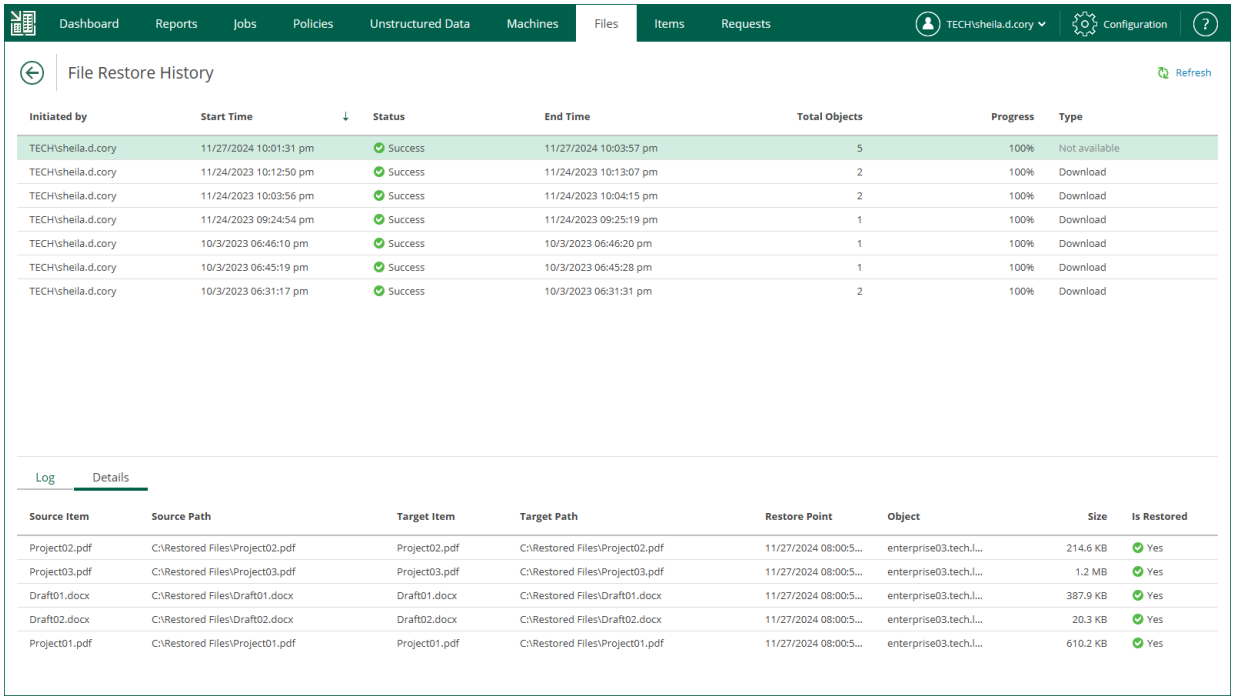
   Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

   Alternatively, you can use a Linux private key. Ensure that the public key is stored on the target machine in the `authorized_keys` file. In this case, specify the private key and private key passphrase.

i. To start restoring files, click **OK**.



Veeam Backup Enterprise Manager starts the restore operation and displays its progress and result in the **File Restore History** view. Note that the **File Restore History** view displays only the restore operations initiated from Enterprise Manager; restore operations initiated from Veeam Backup & Replication are not displayed.



1.

Using Self-Service File Restore Portal to Restore Guest Files

The Self-Service File Restore Portal is a web-based UI in Veeam Backup Enterprise Manager that lets users restore files from their own Windows machines. Users do not need any Enterprise Manager roles to use the portal. Access is granted automatically if the domain account of the user is identified as a local administrator on the protected machine.

The portal helps you delegate in-place file restores to end users or first-line support without granting administrative access to the backup infrastructure. To delegate file restores to local administrators, provide the users with a link to the Self-Service File Restore Portal.

Before You Begin

Before you use the Self-Service File Restore Portal, consider the following requirements and limitations:

- The Self-Service File Restore Portal supports restoring guest OS files only from Microsoft Windows machines. To restore guest OS files from Linux-based machines, use the main Enterprise Manager UI with a user account configured in Enterprise Manager. For more information, see Configuring Accounts and Roles.
- To allow a user account to access the Self-Service File Restore Portal, make sure the account meets the following requirements:
  - The user account is a domain account. Local accounts are not supported.
  - The account belongs to the same or trusted domain as the Enterprise Manager server, so the user account to be resolved to a SID. Users from untrusted domains cannot use self-restore.
  - The account has local administrator rights on the backed-up machine.
- A Self-Service File Restore Portal user have access only to restore points created after the user was granted local administrator rights on the backed-up machine. If local administrator rights are later revoked, the restore points remain available until the next restore point is created (after that, the user can no longer access guest files).
- Enterprise Manager does not support guest OS files restore from storage snapshots. You can use the Veeam Backup & Replication console instead.
- Self-Service File Restore Portal is supported only in the Enterprise Plus edition of Veeam Backup & Replication.
- If the Veeam Backup Enterprise Manager server is added to the Veeam ONE monitoring scope, restore operations performed with the Self-Service File Restore Portal are included in the Restore Operator Activity report in Veeam ONE.

Browsing Guest OS Files Through Self-Service Portal

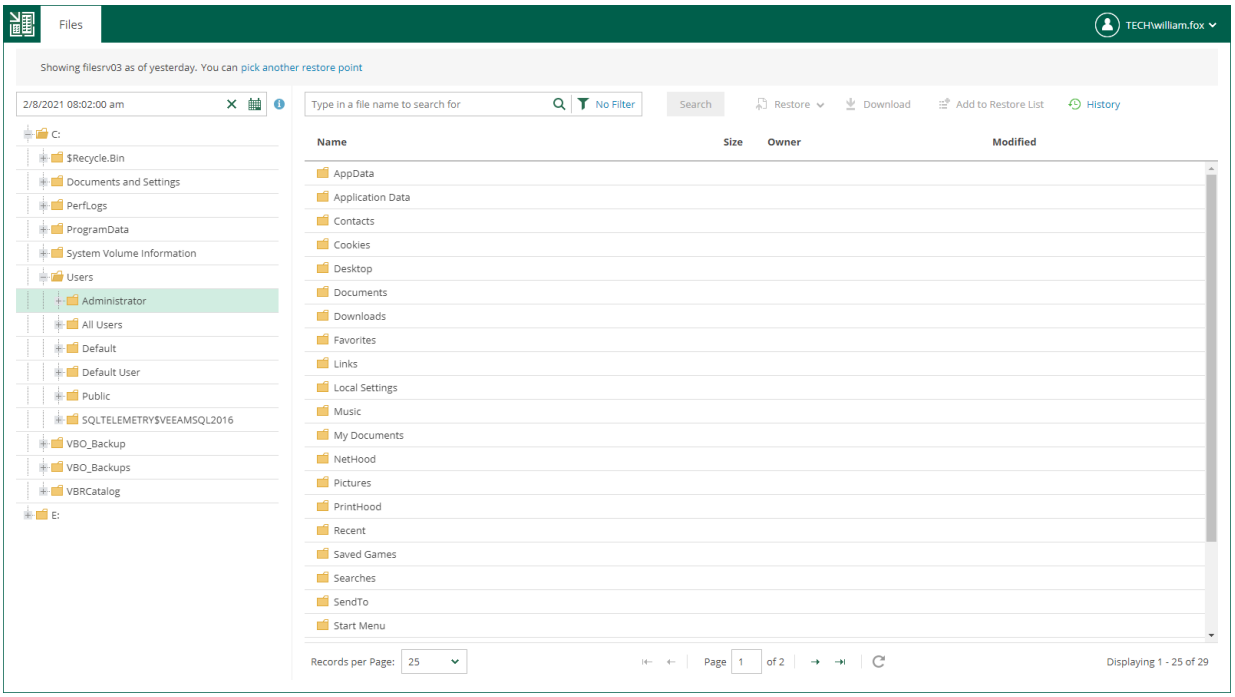
To access the guest files in a machine backup:

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, specify the portal URL in the following format:

   ```
   https://<enterprise_manager_address>/selfrestore
   ```

   Note that the communication with the portal is performed over the HTTPS protocol.

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.



3. 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.

4. 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 for Guest OS Files in Machine Backups, and Performing 1-Click File Restore.

Troubleshooting

If no guest OS files are visible to the user, check the following reasons:

- The backup server that manages the job is not added to the Enterprise Manager infrastructure. For more information, see Adding Backup Servers.
- The recent backup job data has not been yet collected from the backup server (default time interval is 15 minutes). For more information on how to run data collection manually, see Collecting Data from Backup Servers.
- The **Enable guest file system indexing** option is turned off in the machine backup job. Edit the job setting and restart the job with indexing enabled.

- When the machine restore point was created, the user was not assigned local administrative rights. To access the guest OS files the user must be a part of the guest OS local administrator group.

If you cannot find your machine from the **Pick from List** window, you can select the **I don't see my machine** option to rebuild a security scope for your user account. Once complete, this action will reveal machines that were added to your security scope.

Disabling Self-Service File Restore Portal

You can prevent local administrators from accessing the self-service file restore functionality. You can do it by disabling Self-Service File Restore Portal. To disable the portal, change the Enterprise Manager registry key. For more information, contact Veeam Customer Support.

Application Item Restore

Veeam Backup Enterprise Manager supports item-level recovery from backups or replicas. These backups and replicas must be created with enabled application-aware processing. To restore a database to its specific point in time, choose the backups (or replicas) created by a job that processes database logs. For more information, see Application-Aware Processing.

You can restore application items from restore points created by Veeam Backup & Replication or one of Veeam Agents. For more information on Veeam Agents support in Enterprise Manager, see Veeam Agents Support.

With Enterprise Manager, you can restore the following application items:

- Microsoft Exchange items
- Microsoft SQL Server databases
- Oracle databases
- PostgreSQL instances

Before You Begin

Before you restore application items, consider the following:

- Application item restore is available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- Enterprise Manager does not support application item restore from storage snapshots.
- Enterprise Manager users can only restore Microsoft Exchange items to the original location within their restore scope. Users must also have sufficient permissions to restore application items. Users with the Portal Administrator role have no limitations. For more information, see Configuring Accounts and Roles.
- For details on supported application versions, see the Platform Support section of the Veeam Backup & Replication User Guide.
- You can restore deleted Microsoft Exchange items to the production mailbox only.
- Enterprise Manager does not support application item restore from backups created by Veeam Plug-in for Oracle RMAN.
- When you restore application items with Enterprise Manager, restore limitations listed in the Veeam Explorers User Guide are also applied:
  - Veeam Explorer for Microsoft Exchange
  - Veeam Explorer for Microsoft SQL Server
  - Veeam Explorer for Oracle
  - Veeam Explorer for PostgreSQL

Restoring Microsoft Exchange Items

You can restore Microsoft Exchange items (emails, tasks, calendars) from backups and replicas of Microsoft Exchange Server machines.

You can restore Microsoft Exchange items located in different domains. To use this feature, you must be able to provide a specific Microsoft Active Directory account to restore your data in the necessary domain. For that, select the **Prompt for AD account credentials every time** option when configuring Active Directory account settings. For more information, see Configuring Permissions for File and Application Item Restore.

Before restoring application items, read the considerations and limitations.

Performing Restore

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

1. Open the **Items** tab and click **Mailbox Items**.
2. In the **Username** field, enter the account of Active Directory user whose mailbox you want to restored.

   You can leave the **Username** field empty and click the search icon to display all mailboxes that currently exist in the production environment, or enter a search criteria.
3. If you have preconfigured a Microsoft Active Directory account for Microsoft Exchange item restore, Enterprise Manager will use this account for browsing mailbox items and restore. For more information, see Configuring Permissions for File and Application Item Restore.

   If you have not preconfigured the account, specify the following settings in the **Mail Server Credentials** window:

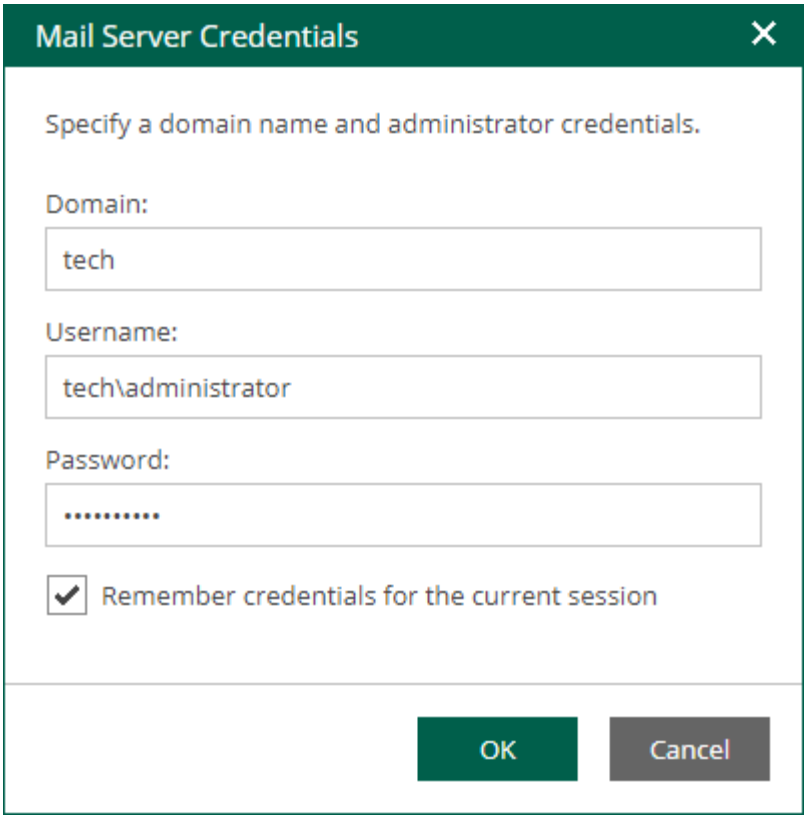
   a. In the **Domain** field, enter a name of the domain that the Microsoft Exchange machine belongs to.

   b. In the **Username** field, specify an account name in the following format: *DOMAIN|USERNAME*. The account must have necessary permissions. For details, see the Permissions section of the Veeam Explorers User Guide.

   c. In the **Password** field, enter a password of the specified user account.

d. Select **Remember credentials for the current session** to use these credentials for all mailbox items restore operations during the current login session.

Enterprise Manager uses Global Catalog to examine Active Directory database and find the specified user mailbox, as well as the DNS name for the Exchange Server where the data should be restored. Then it looks for the VM backup or replica and its restore points.

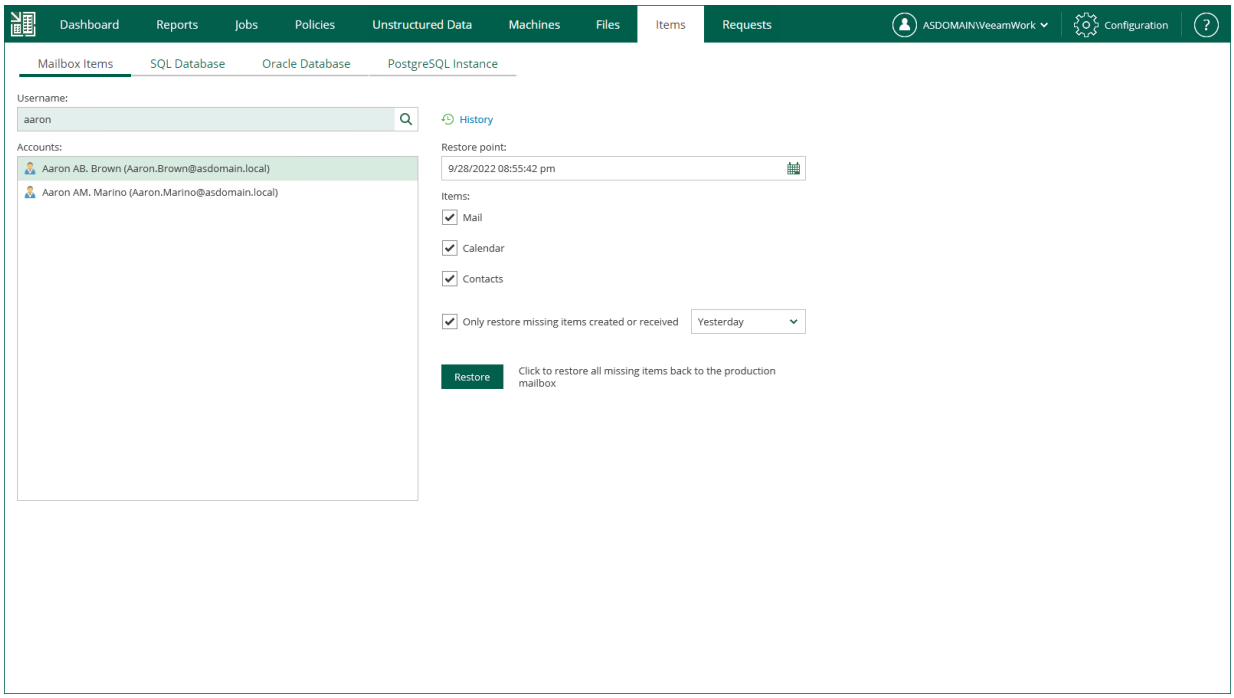


4. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date and a restore point created on that date. By default, the latest valid restore point is selected.

> **NOTE**
>
> Consider the following:
>
> - Restore points on tape are not supported (only those stored in repository can be used).
> - If the specified user mailbox does not exist in the restore point, Veeam Backup Enterprise Manager will display an error message.

5. In the **Items** section, select the type of item you want to restore:
   - Mail
   - Calendar
   - Contacts
6. To restore only missing items created or received during a certain period, select the **Only restore missing items created or received <time period>** check box and select the period from the drop-down list.
7. Click **Restore**. Items that meet the specified conditions will be restored to the production Exchange Server.

To view a restore session log, click **History**.



Restoring Microsoft SQL Server Databases

You can restore a Microsoft SQL Server database by following one of the following scenarios:

- Restore to the original location — to restore a Microsoft SQL Server database to the original location with the same settings.
- Restore with custom settings — restore a Microsoft SQL Server database to a new location, or to any location but with different settings.

Before restoring application items, read the considerations and limitations.

Restore to Original Location

This scenario allows you to restore a Microsoft SQL Server database to the original location.

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

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the Microsoft SQL Server machine or the account you are currently logged in.
2. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to provide the necessary credentials.

   The security role specified for this account in Enterprise Manager must allow the user to restore Microsoft SQL Server databases. For more information, see Configuring Permissions for File and Application Item Restore.

> **NOTE**
>
> If you restore a database that belongs to an AlwaysOn Availability Group, this database will be restored to the original server and added to the Availability Group.

To restore a Microsoft SQL Server database, take the following steps:

1. Open the **Items** tab and click **SQL Database**.
2. In the **SQL Server** field, enter a name of Microsoft SQL Server hosting the database you need to restore; use the *server_name*|*instance_name* format.

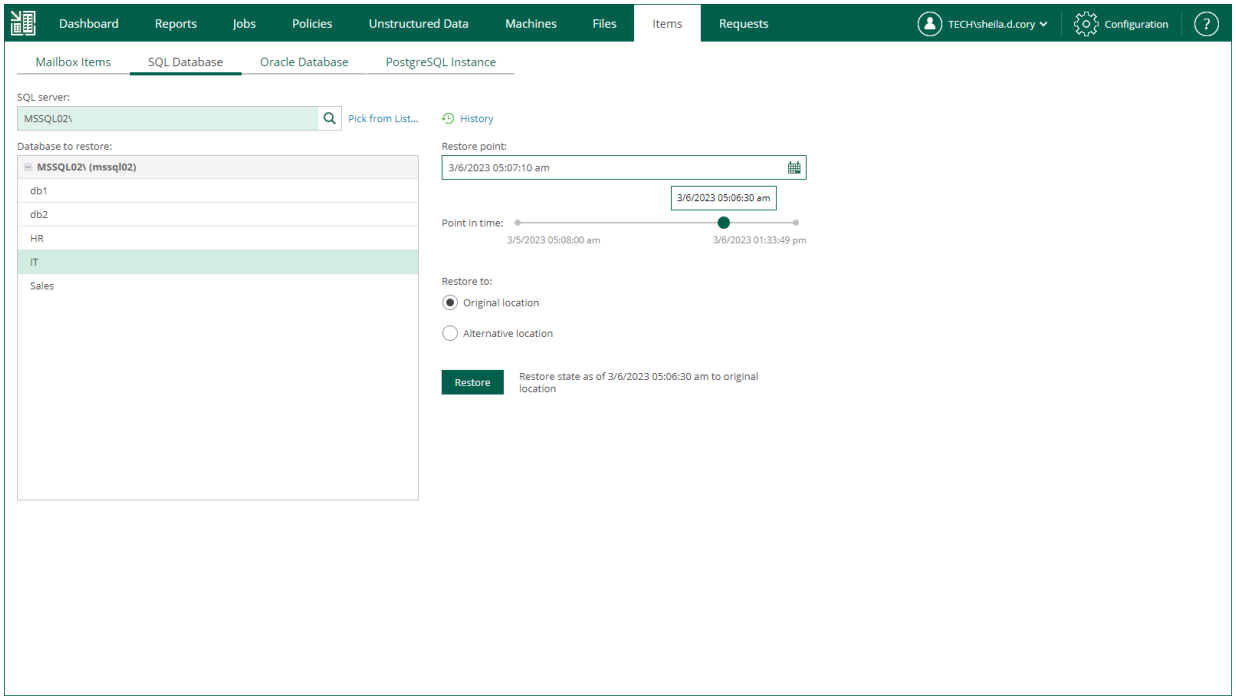
   Alternatively, click the **Pick from List** link to choose a machine from the list of available Microsoft SQL Server backups.
3. From the **Database to restore** list, select the database you need.
4. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon, and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):

   - The beginning point refers to the previous restore point of the Microsoft SQL Server machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see Microsoft SQL Server Transaction Log Settings.
6. In the **Restore to** section, select the **Original location** option.

7. Click **Restore**.

To view a restore session log, click **History**.



Restore with Custom Settings

You can use this scenario to restore a Microsoft SQL Server database to a new location, or to any location but with different settings.

To restore an Oracle database with custom settings, use the **SQL Restore** wizard.

1. Launch the SQL Restore wizard.
2. Specify a target server.
3. Specify AlwaysOn restore settings.
4. Specify files location.

Step 1. Launch SQL Restore Wizard

To launch the **SQL Restore** wizard, do the following:

1. Open the **Items** tab and click **SQL Database**.
2. In the **SQL Server** field, enter a name of Microsoft SQL Server hosting the database you need to restore; use the *server_name*|*instance_name* format.

   Alternatively, click the **Pick from List** link to a machine from the list of available Microsoft SQL Server backups.
3. From the **Database to restore** list, select the database you need. Consider that user credentials for carrying out the restore procedure will be picked as follows:

   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Microsoft SQL Server machine.

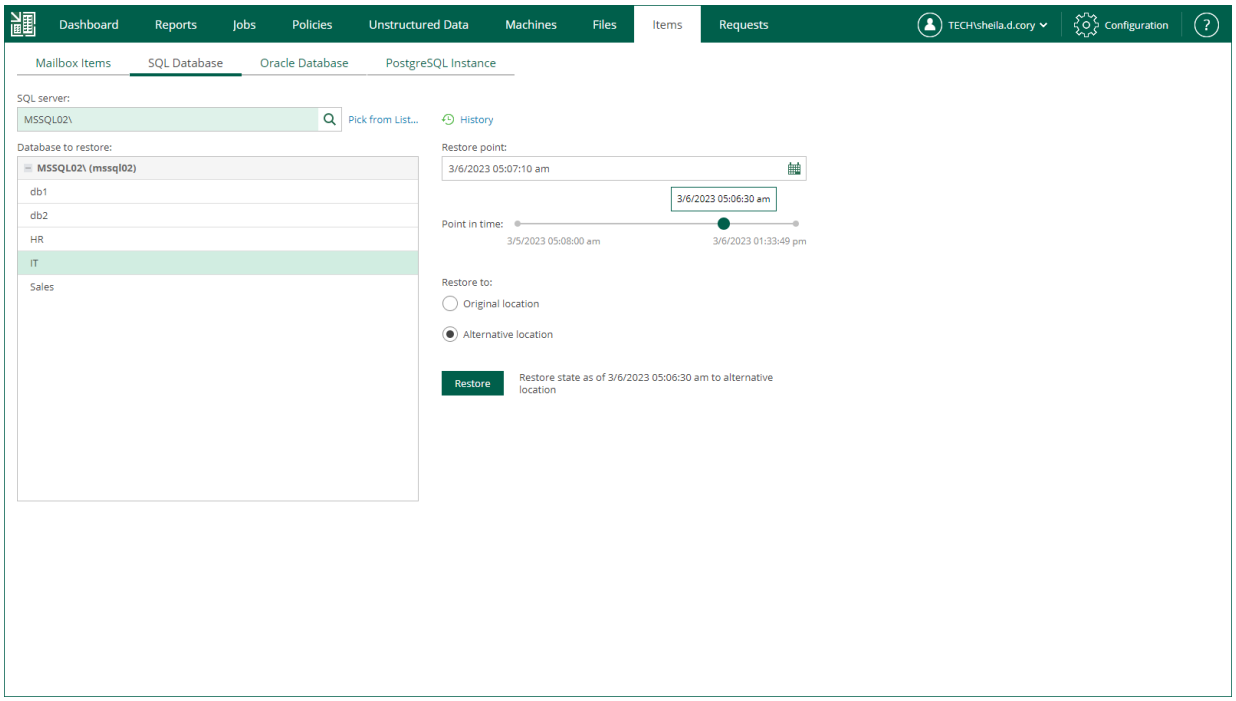
   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), user will be prompted to provide the necessary credentials.

      The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see Configuring Permissions for File and Application Item Restore.
4. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):

   - The beginning point refers to the previous restore point of the Microsoft SQL Server machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see Microsoft SQL Server Transaction Log Settings.
6. In the **Restore to** section, select the **Alternative location** option.

7. Click **Restore**.



Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify settings to connect to the target server and the database.

1. In the **Target Server** section, enter the name of the Microsoft SQL Server or Microsoft SQL Server instance in the *<server IP or FQDN>|<instance name>* format, and credentials of the account that will be used to connect to the target server.

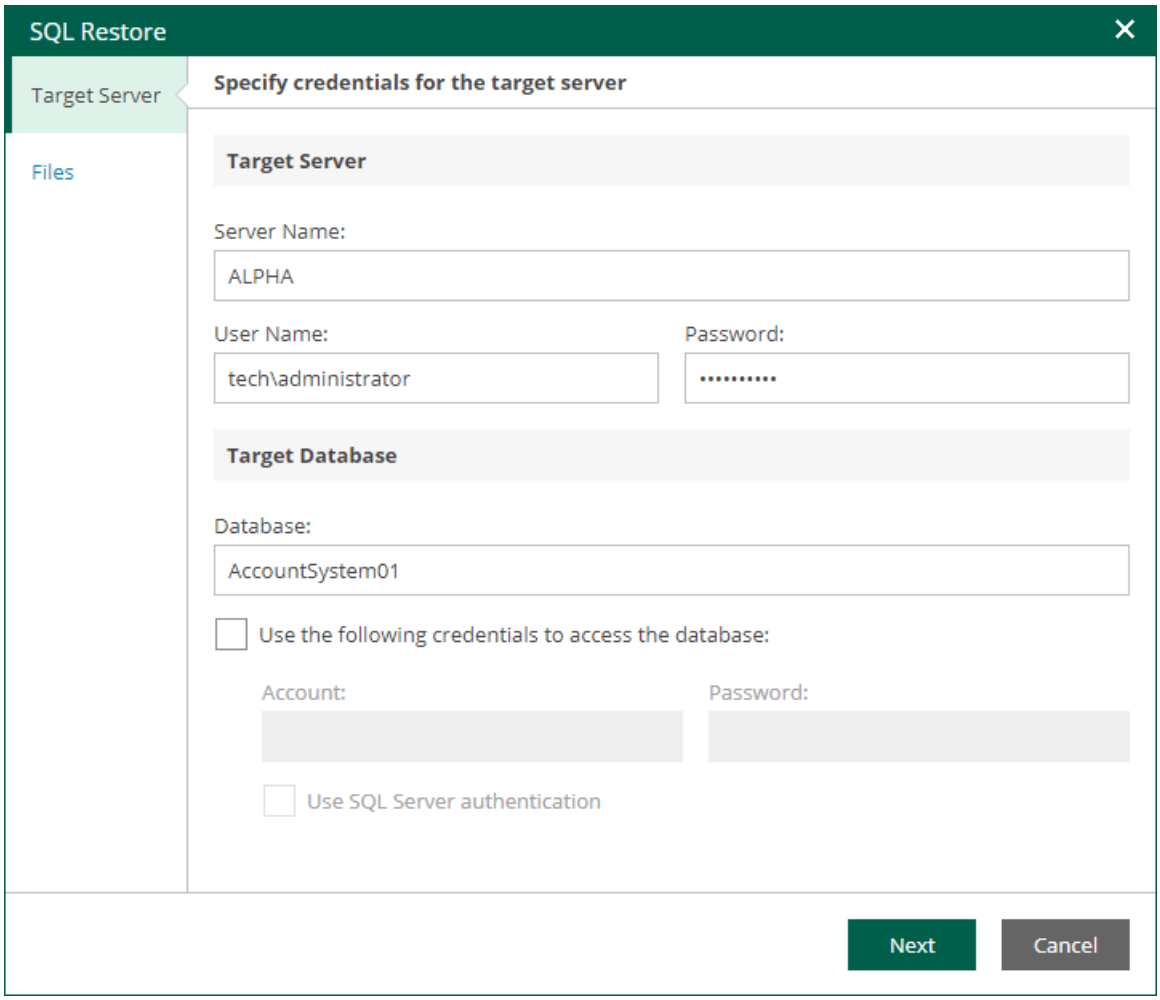
   If the SQL Server instance is assigned a custom port, and Microsoft SQL Browser is not running on the machine, specify the instance port in the following format: *<server IP or FQDN>,<port>*.

2. In the **Target Database** section, specify the following database connection settings:

   a. In the **Database** field, enter the name of the target database.

   b. To use a separate account for connection to the target database, select the **Use the following credentials to access the database** check box and specify credentials of the necessary account.

   c. To use Microsoft SQL Server authentication when connecting to the database, select the **Use SQL Server authentication** check box.



Step 3. Specify AlwaysOn Restore Settings

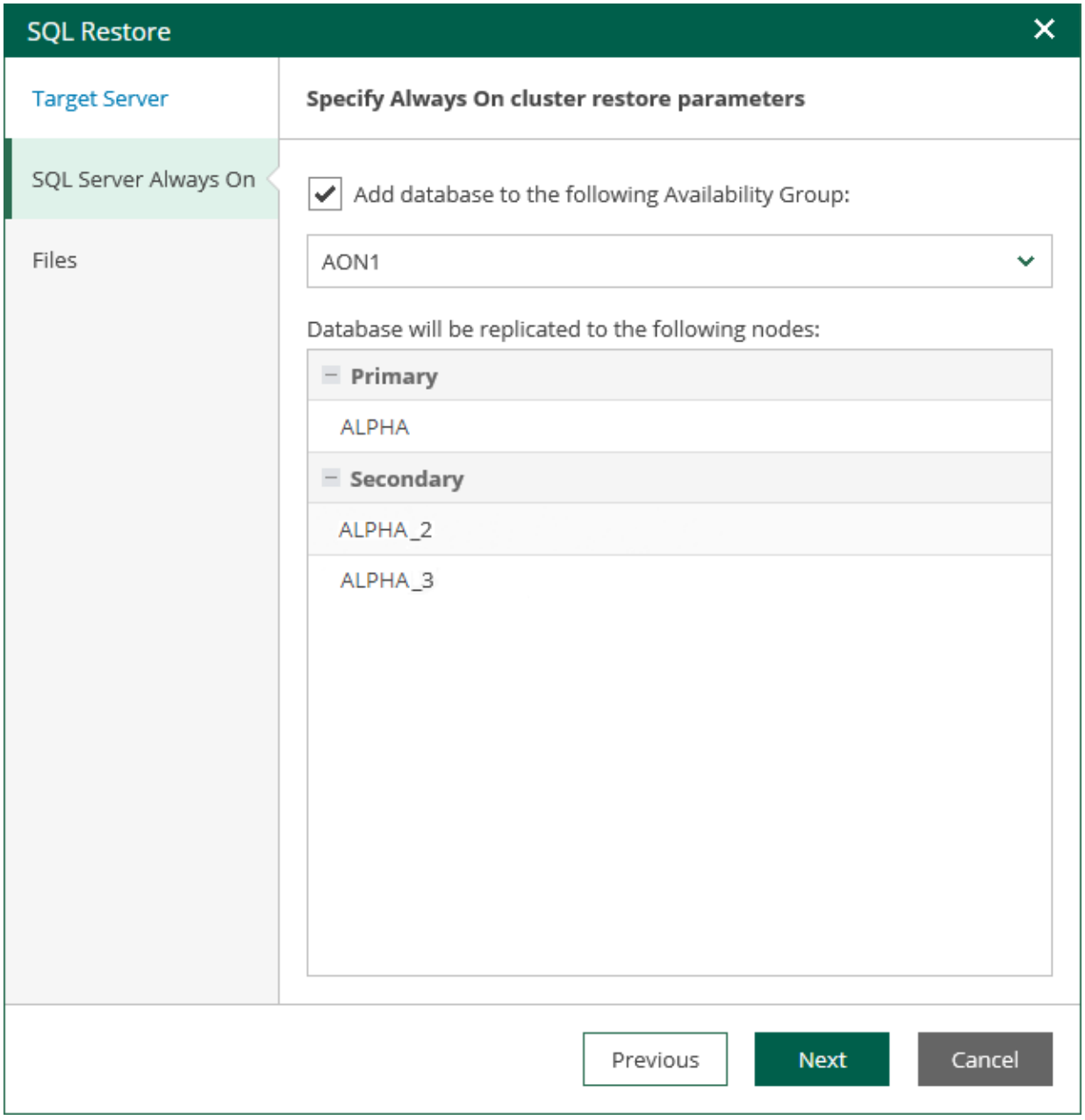
The **SQL Server Always On** step of the wizard is available if the specified target SQL Server supports AlwaysOn Availability Groups.

At this step of the wizard, you can add the restored database to an Availability Group.

1. Select the **Add the database to the following Availability Group** check box and select an availability group from the drop-down list.
2. In the **Database will be replicated to the following nodes** list, review information about the primary and secondary nodes of the availability group.

   During the restore process, Veeam Backup & Replication will restore the database to the primary server and then replicate it to secondary nodes.

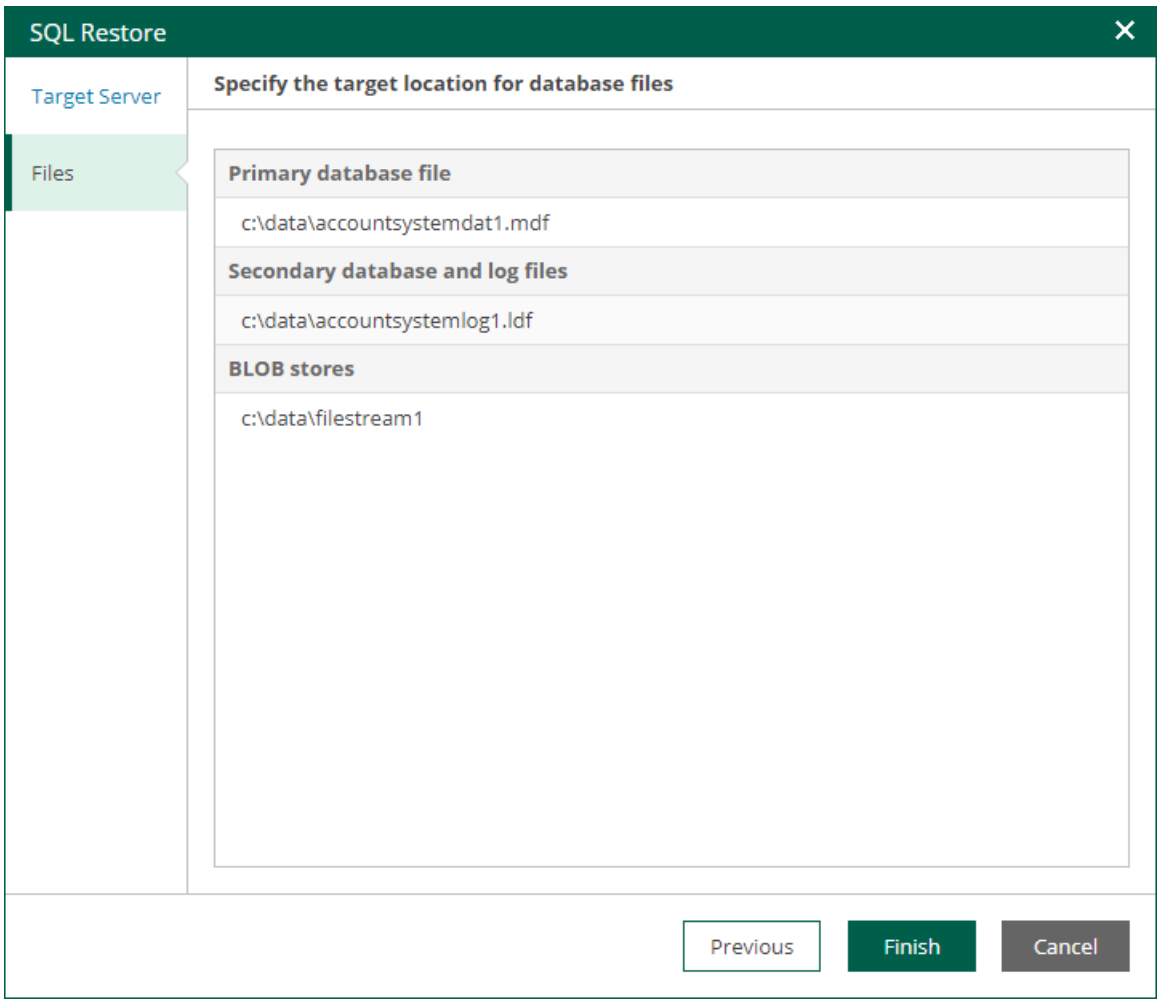
If you do not plan to use the AlwaysOn capabilities when restoring a database, clear the **Add the database to the following Availability Group** check box.



Step 4. Specify Files Location

At the **Files** step of the wizard, you can specify paths to database files on the target server. You can specify separate target locations for the primary database file and secondary database file with logs. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.



Restoring Oracle Databases

With Veeam Backup Enterprise Manager, you can restore

To restore an Oracle database, follow one of the following scenarios:

- Restore to the original location — to restore an Oracle instance to the original location with the same settings.
- Restore with custom settings — restore an Oracle instance to a new location, or to any location but with different settings.

Before restoring application items, read the considerations and limitations.

Restore to Original Location

This scenario allows you to restore an Oracle database to the original location.

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

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Oracle server machine or the account you are currently logged in.
2. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on Windows server, then you may need to enter password for Oracle home.

   The security role specified for this account in Enterprise Manager must allow the user to restore Oracle databases. For more information, see Configuring Permissions for File and Application Item Restore.

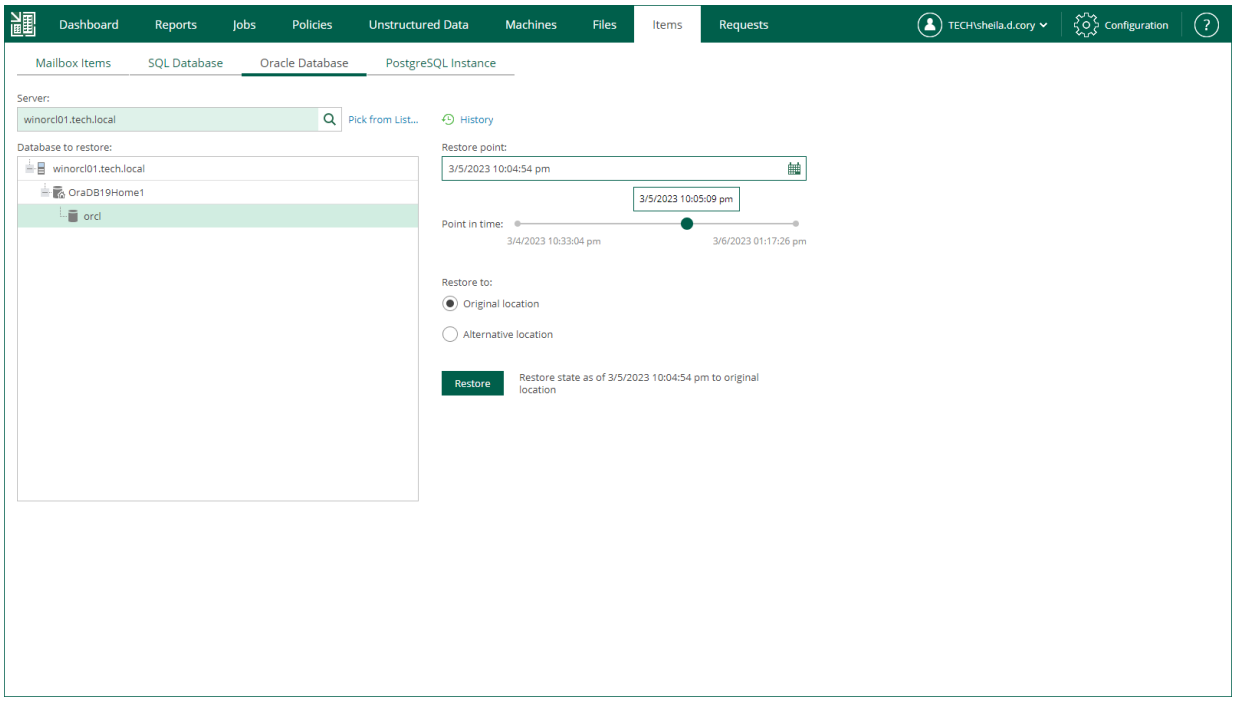
To restore an Oracle database, take the following steps:

1. Open the **Items** tab and click **Oracle Database**.
2. In the **Server** field, enter a name of the Oracle server hosting the database you need to restore.

   Alternatively, click the **Pick from List** link to select a machine from the list of available Oracle backups.
3. From the **Database to restore** list, select Oracle home and the database you need.
4. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):
   - The beginning point refers to the previous restore point of the Oracle machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see Oracle Archived Redo Log Settings.
6. In the **Restore to** section, select the **Original location** option.
7. Click **Restore**.

To view a restore session log, click **History**.



Restore with Custom Settings

You can use this scenario to restore a PostgreSQL instance to a new location, or to any location but with different settings.

To restore an Oracle database with custom settings, use the **Oracle Restore** wizard.

1. Launch the Oracle Restore wizard.
2. Specify a target server.
3. Specify Oracle home settings.
4. Specify database files location.

Step 1. Launch Oracle Restore Wizard

To launch the **Oracle Restore** wizard, do the following:

1. Open the **Items** tab and click **Oracle Database**.
2. In the **Server** field, enter a name of the Oracle server hosting the database you need to restore.

   Alternatively, click the **Pick from List** link to select a machine from the list of available Oracle backups.
3. From the **Database to restore** list, select Oracle home and the database you need. Consider that user credentials for carrying out the restore procedure will be picked as follows:

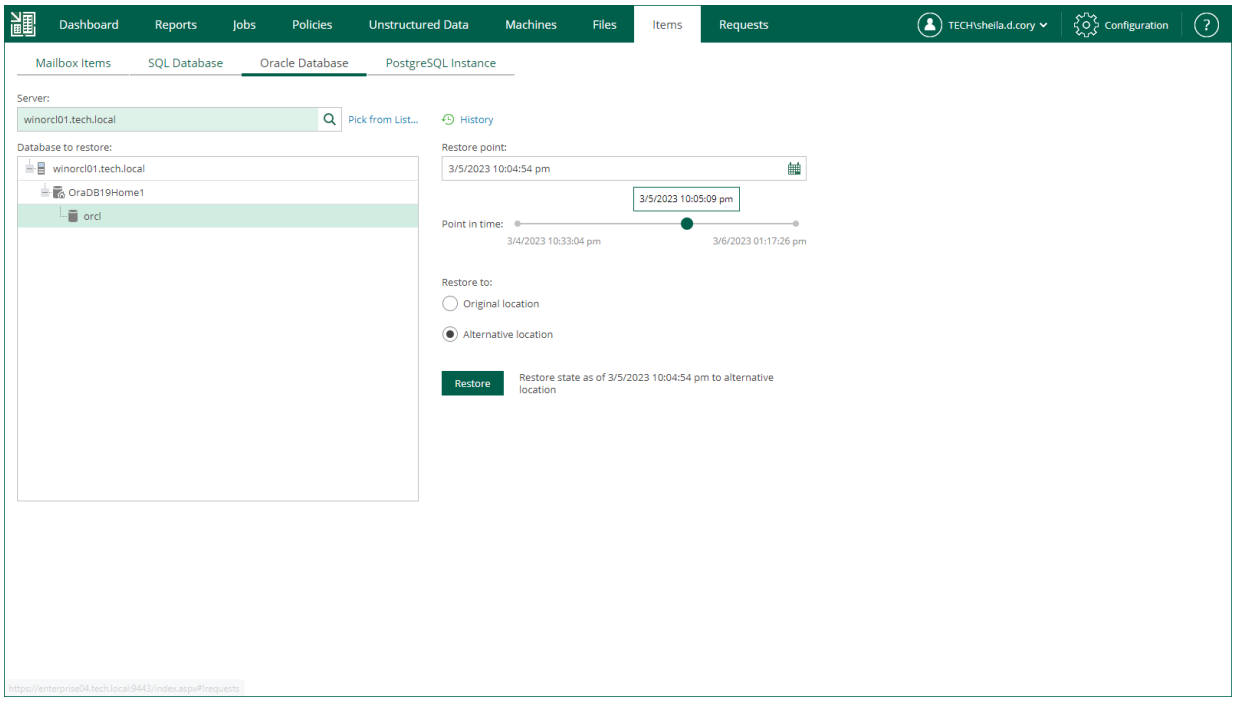
   a. Veeam Backup Enterprise Manager will try to use the account of the backup job that contains the Oracle server machine, or the account which is currently logged in.

   b. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to supply the necessary credentials. Make sure the account has access to the original machine guest OS (Windows or Linux); if restoring an Oracle 12 Database on Windows server, then you may need to enter password for Oracle home.
4. To specify a restore point from which to restore the database, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. For a database backed up with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):

   - The beginning point refers to the previous restore point of the Oracle machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see Oracle Archived Redo Log Settings.
6. In the **Restore to** section, select the **Alternative location** option.

7. Click **Restore**.



Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify connection settings required to access the target Oracle server. The set of connection settings depends on the OS type of the target server: Windows or Linux.

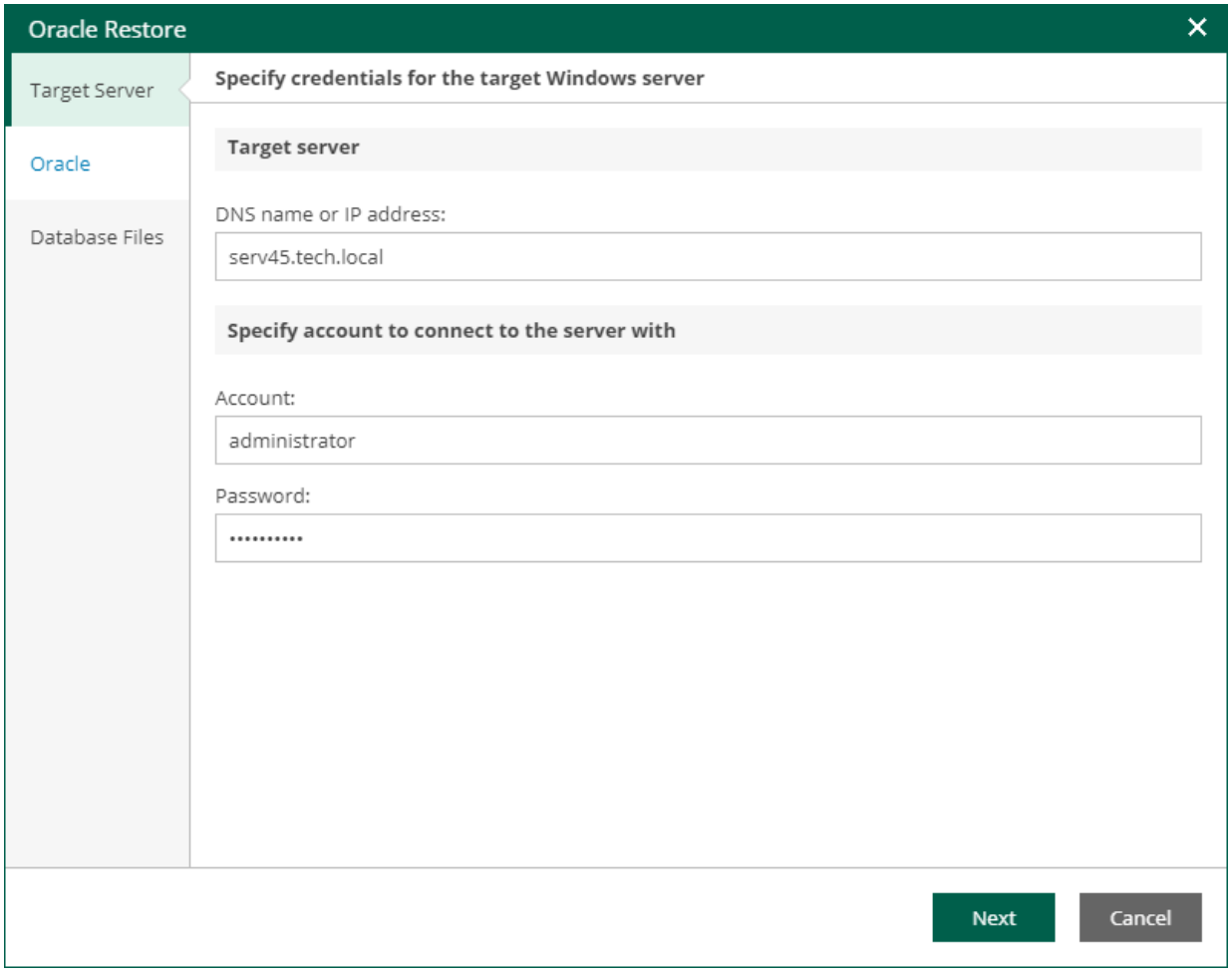
Windows-Based Oracle Server

For database restore to a Microsoft Windows server, specify the following connection settings:

1. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Microsoft Windows server.
2. In the **Account** and **Password** fields, specify credentials of the account that will be used for connection with the target Windows-based Oracle server.

Consider the following:

- The user account must be a member of the **local Administrator** group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



Linux-Based Oracle Server

For database restore to a Linux server, specify the following connection settings:

1. In the **DNS name or IP address** field, enter a DNS name or IP address of the target Linux server.
2. In the **SSH port** field, specify a port number of the target Oracle server (by default, port 22 is used).
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If a private key is required to connect to the selected server, do the following:
   a. Select the **Private key is required for this connection** check box.
   b. In the **Private key** filed, specify a key.

      To select a key, click **Browse** and select a key.

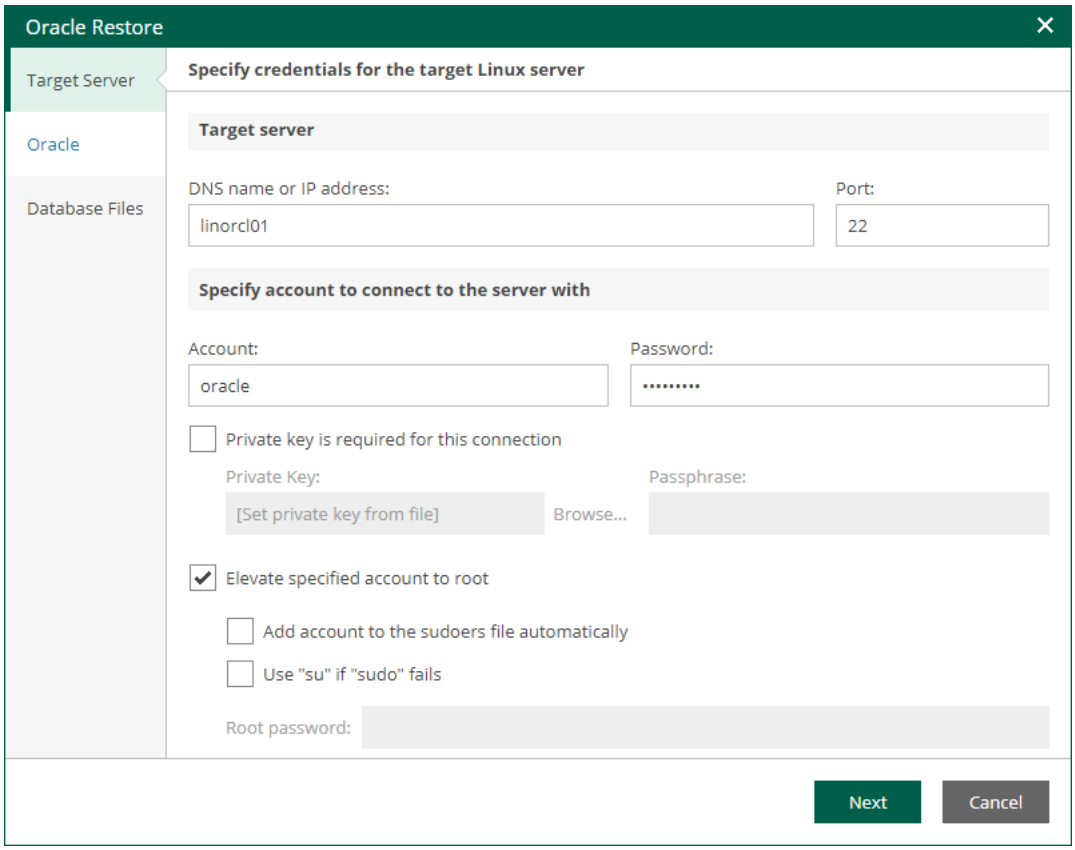
   c. In the **Passphrase** field, enter the passphrase.
6. If you have specified a non-root account that does not have root permissions on the target server, do the following.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password for the root account.

      Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, the `su` command will be used.

Consider that the user account must be a member of the **dba** group.

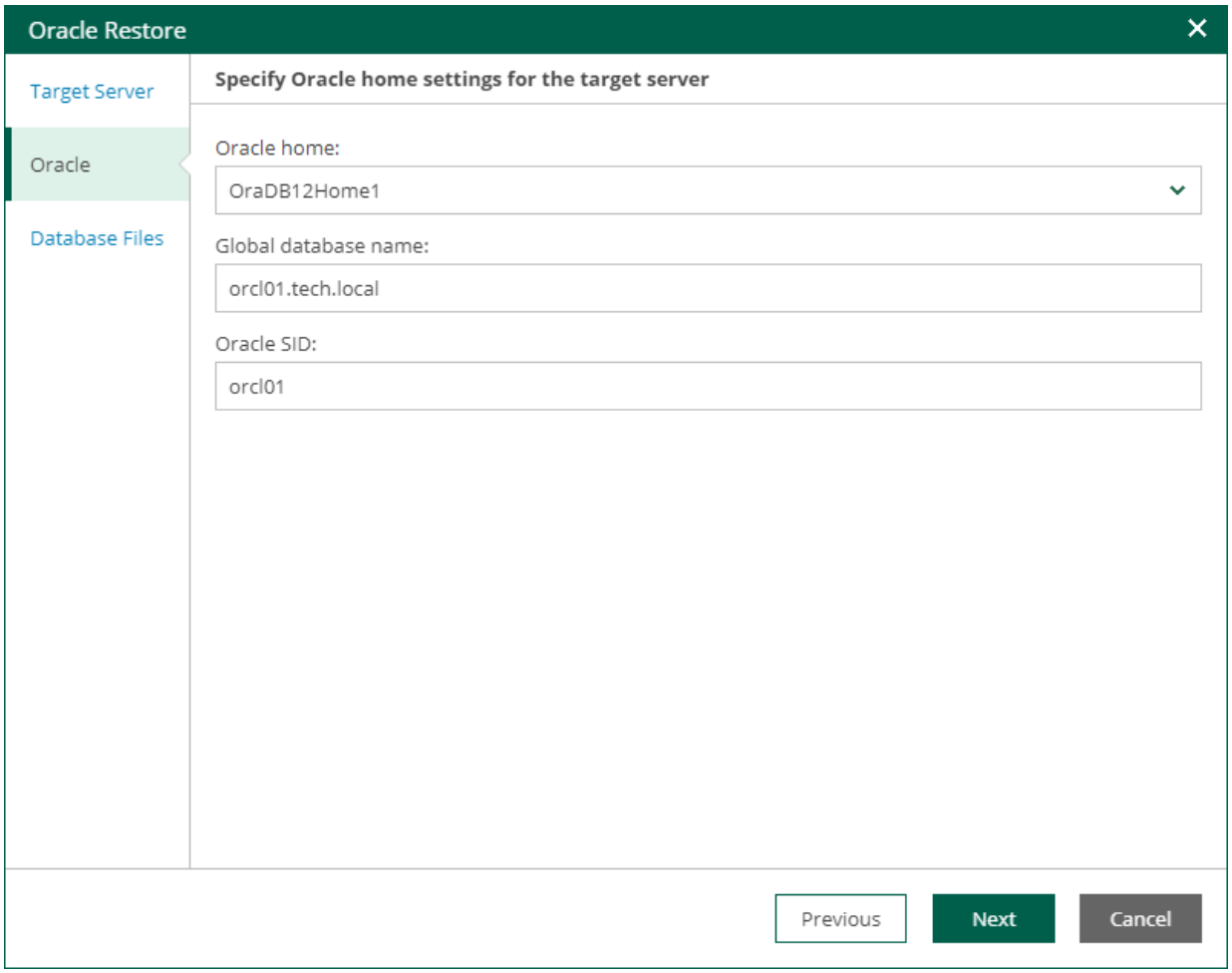


Step 3. Specify Oracle Home Settings

At the **Oracle** step of the wizard, specify Oracle home settings.

1. In the **Oracle home** field, specify Oracle home.
2. In the **Global database name** field, specify a full name of the database including its network domain.
3. In the **Oracle SID** field, specify the database system identifier.

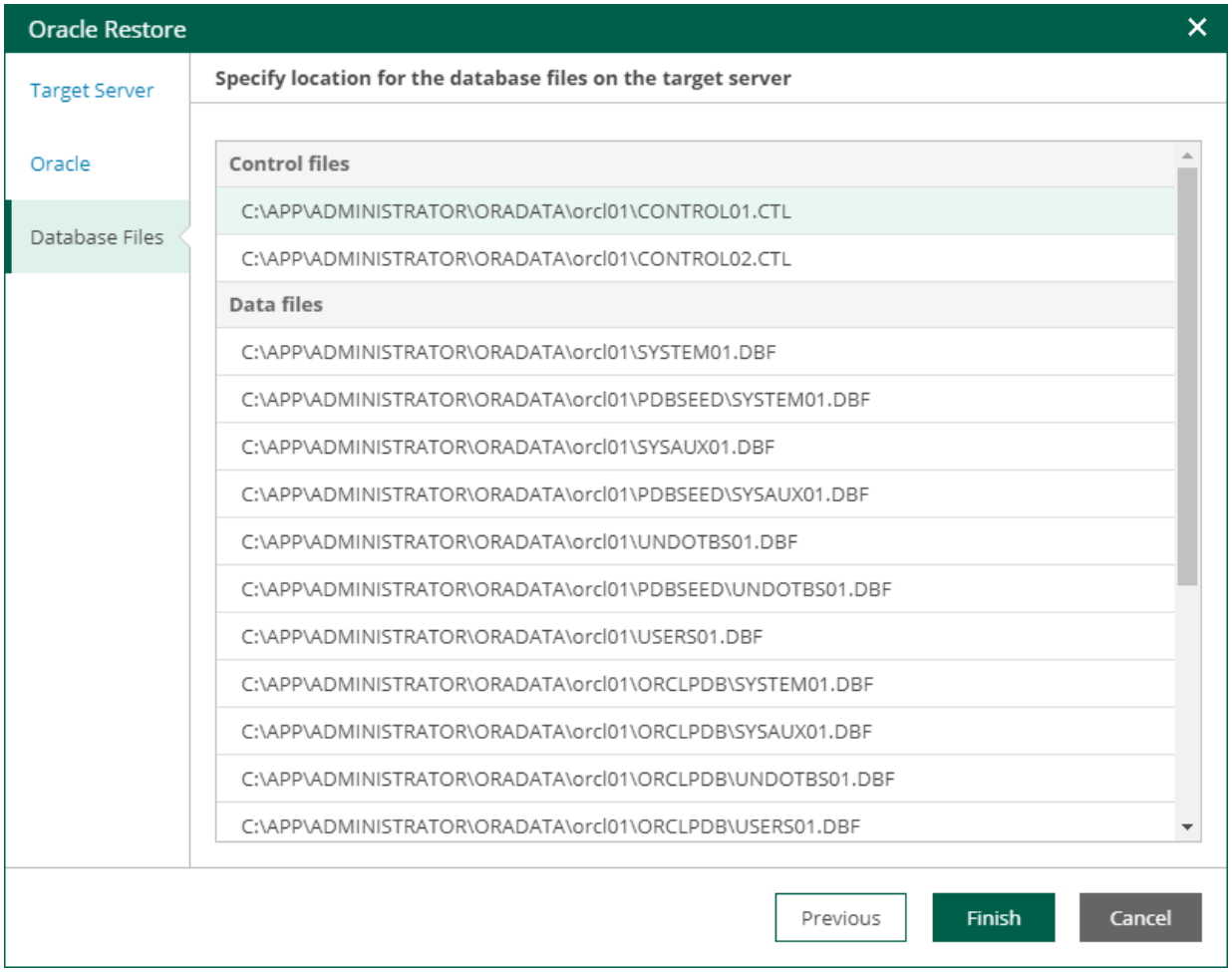
   If a database with the specified SID exists on the target Oracle home, the restore process will delete it and replace with the database from backup. Thus, before starting the restore process, a message will be displayed, asking you to confirm the operation.



Step 4. Specify Database Files Location

At the **Database Files** step of the wizard, specify paths to database files on the target server. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.



Restoring PostgreSQL Instances

With Enterprise Manager you can restore PostgreSQL data at the instance level. To restore a PostgreSQL instance, follow one of the following scenarios:

- Restore to the original location — to restore a PostgreSQL instance to the original location with the same settings.
- Restore with custom settings — restore a PostgreSQL instance to a new location, or to any location but with different settings.

Before restoring application items, read the considerations and limitations.

Restore to Original Location

This scenario allows you to restore a PostgreSQL instance to the original location.

Consider that user credentials for carrying out the restore procedure will be picked as follows:

1. Veeam Backup Enterprise Manager tries to use the account specified in the backup job that contains the PostgreSQL machine or the account you are currently logged in.
2. If this account does not have sufficient rights to perform the restore procedure (for example, in case of imported backup), you will be prompted to provide the necessary credentials.

   For more information on the account roles in Veeam Backup Enterprise Manager that allow a user to restore PostgreSQL, see Configuring Permissions for File and Application Item Restore.

To restore a PostgreSQL instance to the original location, take the following steps:

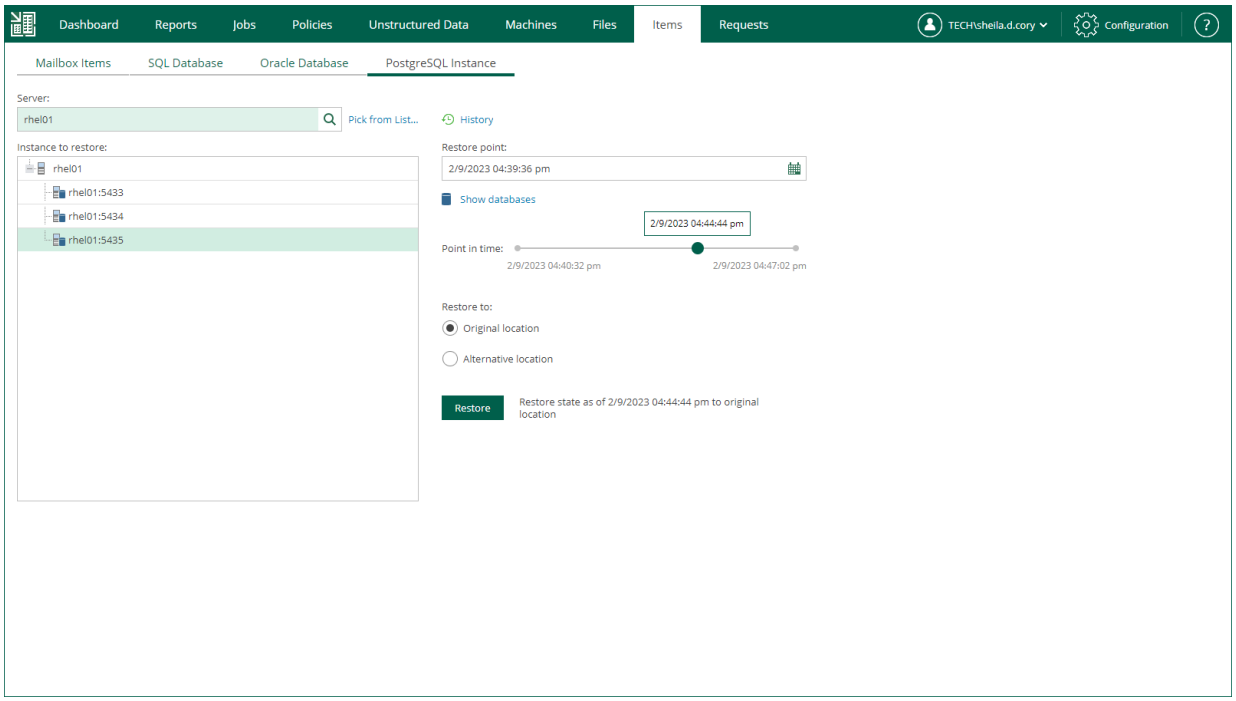
1. Open the **Items** tab and click **PostgreSQL Instance**.
2. In the **Server** field, enter a VM name where the necessary PostgreSQL instance resides.

   Alternatively, click the **Pick from List** link to select from the list of available PostgreSQL machine backups.
3. From the **Instance to restore** list, select a PostgreSQL instance you need.
4. To specify a restore point from which to restore the instance, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. To view a list of databases included in the restore point, click **Show databases**.
6. For PostgreSQL instances with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):

   - The beginning point refers to the previous restore point of the PostgreSQL machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see PostgreSQL Archive Log Settings.
7. In the **Restore to** section, select the **Original location** option.
8. Click **Restore**.

To view a restore session log, click **History**.



Restore with Custom Settings

You can use this scenario to restore a PostgreSQL instance to a new location, or to any location but with different settings.

To restore a PostgreSQL instance with custom settings, use the **PostgreSQL Restore** wizard.

1. Launch the PostgreSQL Restore wizard.
2. Specify a target server.
3. Specify restore settings.
4. Specify location for database tablespaces.

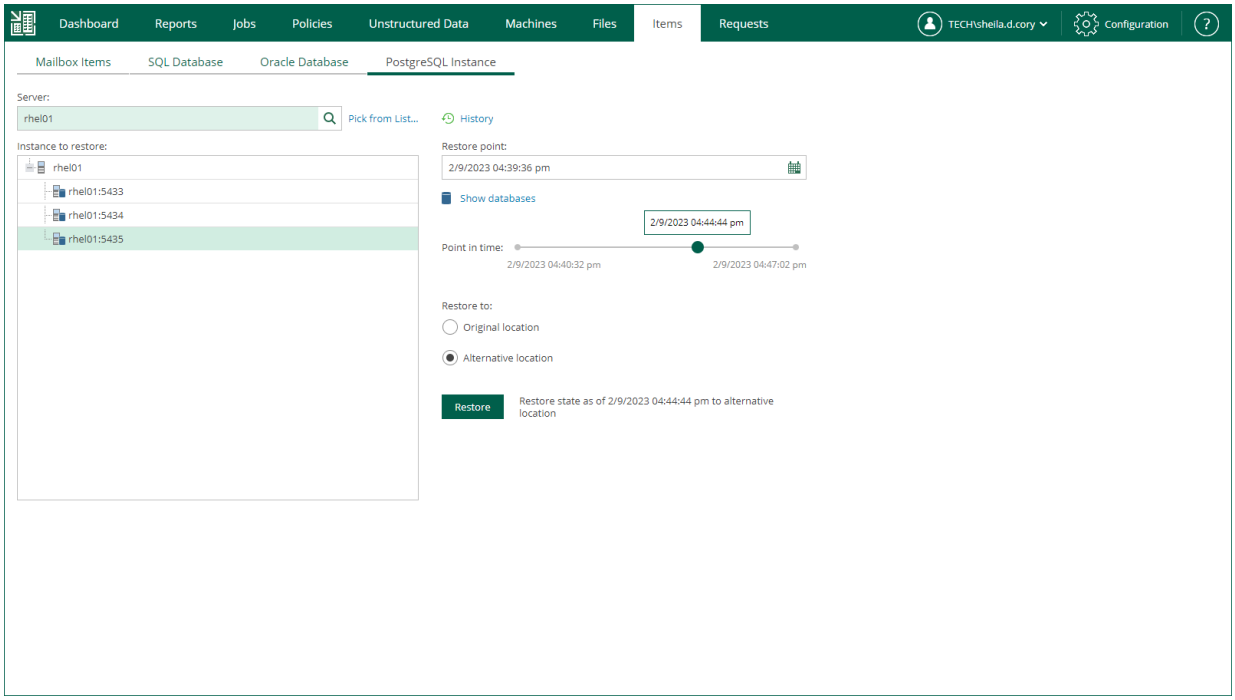
Step 1. Launch PostgreSQL Restore Wizard

To launch the **PostgreSQL Restore** wizard, do the following:

1. Open the **Items** tab and click **PostgreSQL Instance**.
2. In the **Server** field, enter a VM name where the necessary PostgreSQL instance resides.

   Alternatively, click the **Pick from List** link to select from the list of available PostgreSQL machine backups.
3. From the **Instance to restore** list, select a PostgreSQL instance you need.
4. To specify a restore point from which to restore the instance, in the **Restore point** field, click the calendar icon and select the necessary date when backup was performed and a restore point created on that date. By default, the latest valid restore point is selected.
5. To view a list of databases included in the restore point, click **Show databases**.
6. For PostgreSQL instances with transaction log backup turned on, you can also select the necessary point in time using the **Point in time** slider. The slider displays the following timestamps (relative to the currently selected restore point):
   - The beginning point refers to the previous restore point of the PostgreSQL machine that contains the selected database backup. If the previous restore point (server backup) is not found, or the database backup does not exist in it, then the beginning point refers to the current restore point.
   - The ending point refers to the next restore point that contains the selected database backup. If the next restore point (server backup) and the associated transaction log backup are not found, or if the database backup does not exist in the server backup, then the ending point will refer to the current restore point. If the next restore point (server backup) is not found, but the transaction log backup exists for the preceding period, then the ending point refers to the latest log backup time.

   For more information on configuring transaction log backup, see PostgreSQL Archive Log Settings.
7. In the **Restore to** section, select the **Alternative location** option.
8. Click **Restore**.



Step 2. Specify Target Server

At the **Target Server** step of the wizard, specify settings for connection to the target PostgreSQL server.

1. In the **Target Server** section, enter a DNS name or IP address of the target server, as well as an SSH port (by default, port 22 is used).
2. Specify credentials of the account that will be used to connect to the target server:
   a. In the **Account** field, specify the account name.
   b. In the **Password** field, specify the account password.
   c. If you want to use a Linux private key for this connection, select the **Private key is required for this connection** check box and specify the following private key settings:
      i. In the **Private key** field, specify a file that contains a private key.
      ii. In the **Passphrase** field, enter the passphrase used to decrypt the private key.
   d. If you have specified a non-root account that does not have root permissions on the target server, select the **Elevate specified account to root** check box.

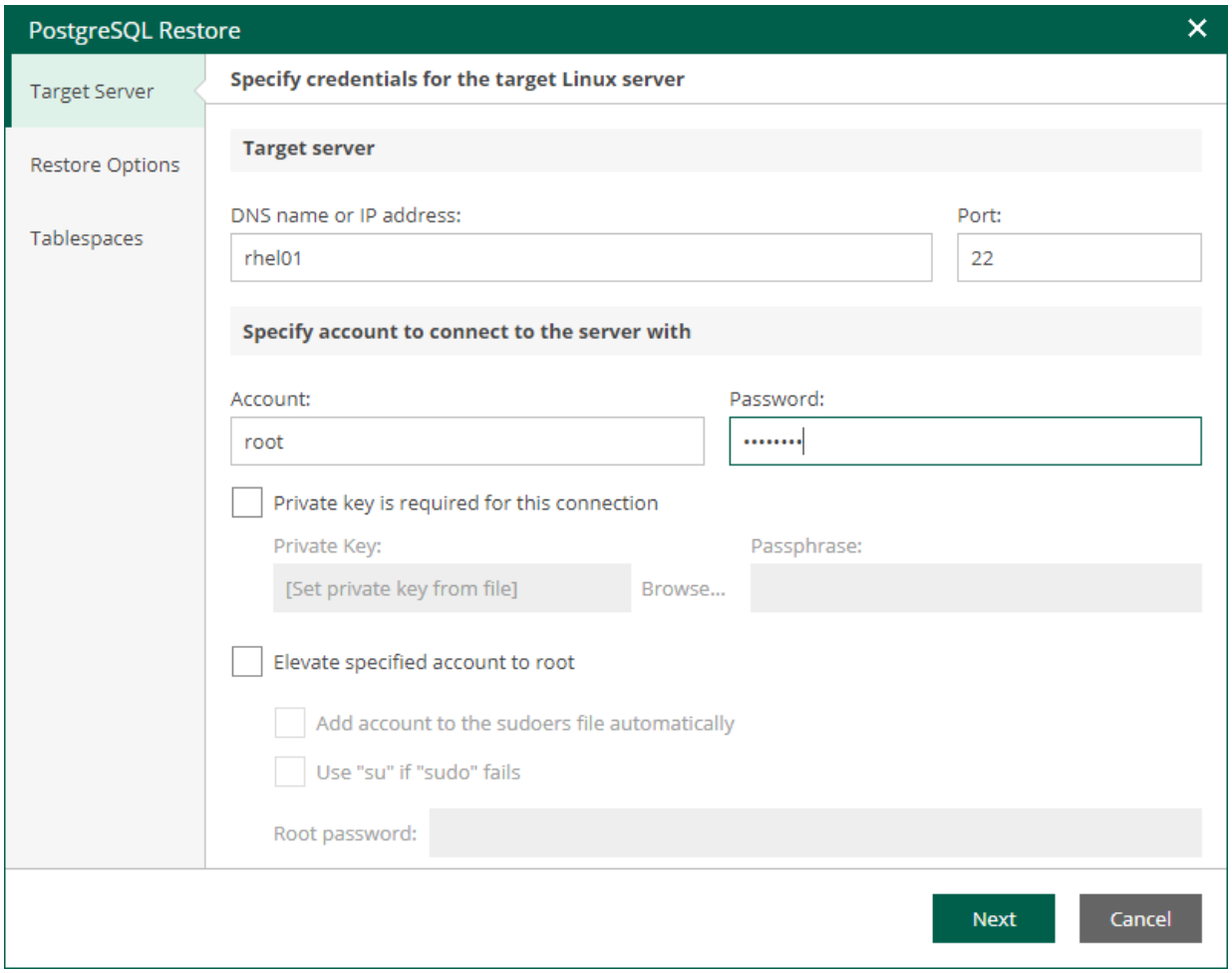
      The account must have root privileges to mount the backed up file system to mount the backed up file system to the target server and to communicate with PostgreSQL.

      i. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

         If you do not enable this option, you will have to manually add the user account to the sudoers file.

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

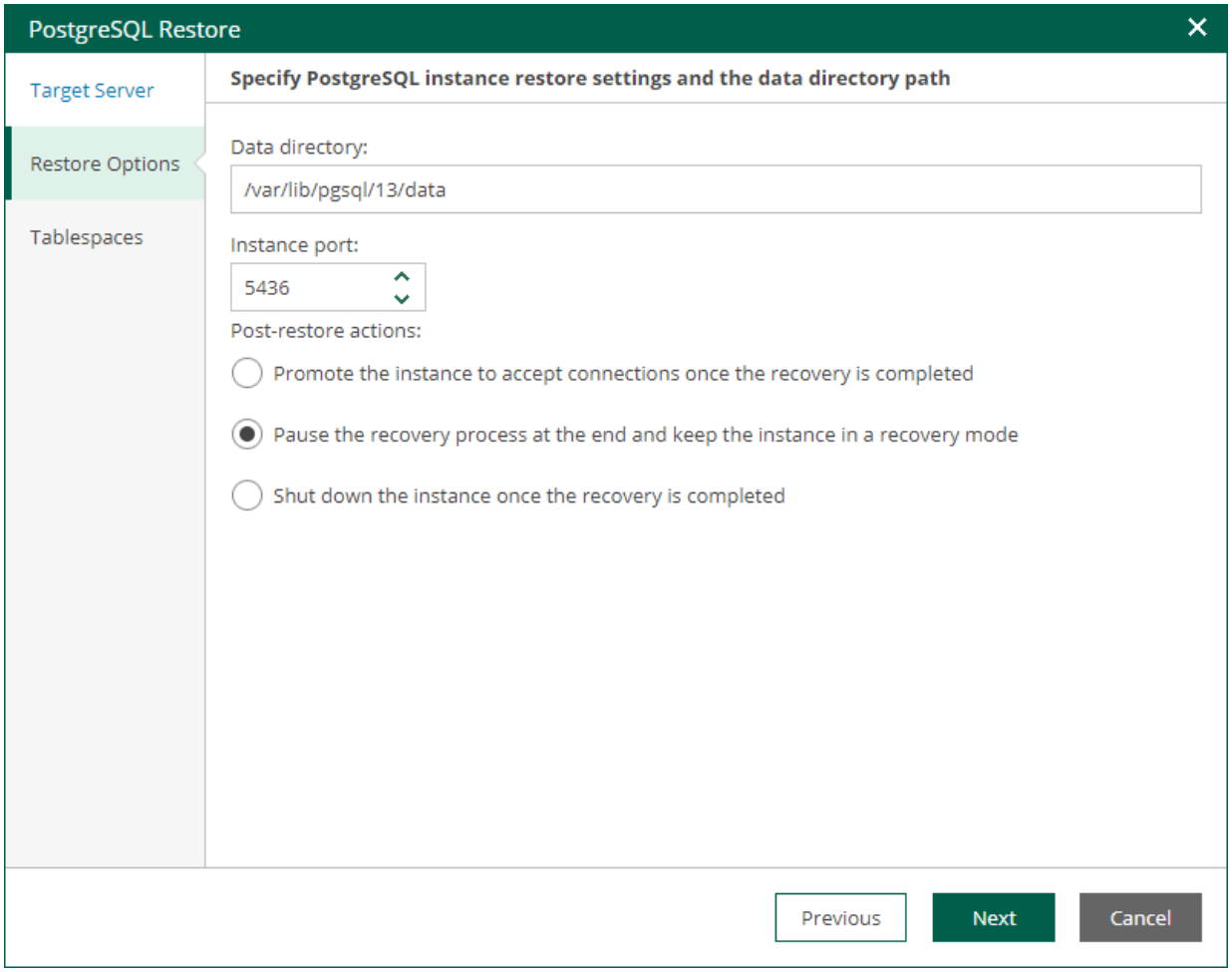
Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.



Step 3. Specify Restore Settings

At the **Restore Settings** step of the wizard, specify instance folder and instance port.

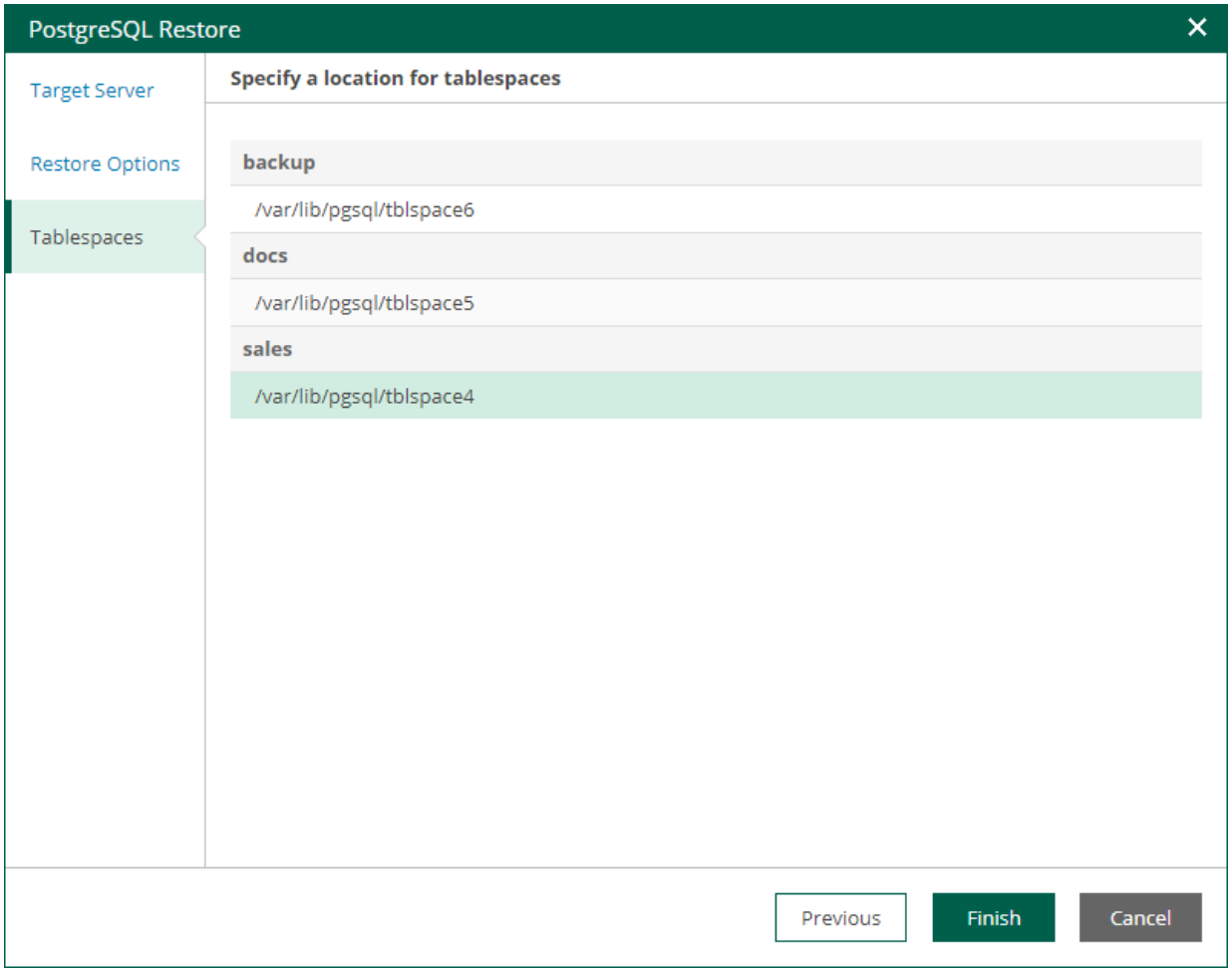
1. In the **Data directory** field, specify a path to the directory where the restored instance data will be stored.
2. In the **Instance port** field, specify a TCP port that will be used to connect to the instance.
3. Select one of the following post-restore actions that the PostgreSQL server must take after the instance is restored. For more information, see the Specify Post-Restore Action section of the Veeam Explorers User Guide.
   - Select **Promote the instance to accept connections once the recovery is completed** to make the PostgreSQL instance available for connections.
   - Select **Pause the recovery process and keep the instance in a recovery mode** to make the PostgreSQL instance run but not accepting incoming remote TCP connections.
   - Select **Shut down the instance once recovery is completed** to make the PostgreSQL instance stop upon recovery.



Step 4. Specify Tablespaces

At the **Tablespaces** step of the wizard, enter paths of directories where database tables will be stored. Then, click **Finish** to start the restore operation.

To view the status of the restore process, on the **Items** tab, click **History**.



Veeam Agents Support

Veeam Backup Enterprise Manager allows you to browse and restore guest OS files and application items from backups created with the following Veeam Agents:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux (Veeam Agent for Linux on Power is not supported)
- Veeam Agent for Mac
- Veeam Agent for Oracle Solaris
- Veeam Agent for IBM AIX

> **NOTE**
>
> File restore from backups of Veeam Agent for Mac, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX to the original location is not available.

Before you start browsing or restore, check the following prerequisites:

- You have the Enterprise or Enterprise Plus edition of Veeam Backup & Replication.
- For 1-Click restore of guest OS files and for restore of application items, you must have the Server edition of Veeam Agents. For more information, see Product Comparison.

> **NOTE**
>
> You can work with both Veeam Agent backup jobs managed by Veeam Agent and Veeam Agent backup jobs managed by the backup server. For more information on Veeam Agent backup jobs and policies, see the Working with Veeam Agent Backup Jobs and Policies section of the Veeam Agent Management Guide.

In This Section

- Guest File Browsing and 1-Click Restore
- Application Item Restore

Guest File Browsing and 1-Click Restore

If you have Veeam Backup & Replication and Veeam Agent that both meet the prerequisites, you can browse, search and restore guest OS files from the backups created by Veeam Agent.

In This Section

- Preparing for File Browsing and Restore
- Browsing and Restore Procedures

Preparing for File Browsing and Restore

You can browse and restore files from a backup of a physical server created by Veeam Agent with or without enabling guest OS file indexing. Take some preparatory steps for the server processed by Veeam Agent:

- Preparing for restore from a Windows Server backup
- Preparing for restore from a Non-Windows Server backup

Windows Server

Preparing Backup

You can restore files from a backup of a physical Windows server created with or without indexing.

To prepare a backup with guest file indexing:

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

If you restore files from an indexed guest OS, you do not need to mount the restore point for browsing purposes — file hierarchy is presented using the index. The restore point will be only mounted once (during 1-Click file restore process itself) — to the mount server associated with backup repository where Veeam Agent backups are stored.

Alternatively, you can process the backups created without guest file system indexing — for example, if indexing was disabled at restore point creation time, or if indexing operation failed. For such a server, its selected restore point first will be mounted (for the browsing and search purposes) to the Veeam backup server integrated with Veeam Agent. After you locate the necessary file and initiates 1-Click file restore, the restore point will be mounted to the mount server associated with the repository.

Other Prerequisites

During guest file restore to the original location, you are prompted for the credentials to access the target Windows server. Enter a user name and password; make sure that the account has sufficient access rights.

Non-Windows Server

Preparing Backup

You can restore files from a backup of a physical server created with or without indexing.

> **NOTE**
>
> Veeam Agent for Mac and Veeam Agent for Linux on Power do not support file system indexing.

To prepare a backup with guest file indexing:

1. Check for the following utilities to be installed on the server: `mlocate`, `gzip`, and `tar`. These utilities are required for file indexing. When you enable file indexing, Veeam Agent will prompt you to deploy them in case they are not found.
2. Enable guest file system indexing in the backup job settings.

   For more information, see the File System Indexing section of the following guides:

   - Veeam Agent for Linux User Guide
   - Veeam Agent for Oracle Solaris User Guide
   - Veeam Agent for IBM AIX User Guide
3. Run the backup job with guest file system indexing enabled.
4. Make sure the indexing data is imported to Veeam backup database, and catalog data replication is completed successfully. For more information, see Performing Catalog Replication and Indexing.

Whether you restore from a backup with or without guest file indexing, prepare a machine to operate as a helper host or helper appliance.

Preparing Helper Host or Helper Appliance

When restoring guest OS files, Veeam Backup & Replication mounts machine disks from the backup or replica to a mount server (helper host or helper appliance). For the mount server, you can use a machine running on VMware vSphere or Microsoft Hyper-V. You specify helper host (or appliance) settings on the backup server when you configure guest OS file restore. These settings are saved in the backup server configuration database for the specific user that configured the restore. Before you start file-level restore from Enterprise Manager, ensure the settings are properly configured on the backup server. For more information, see the Guest OS File Restore section of the Veeam Backup & Replication User Guide.

When you start guest OS file restore from Veeam Backup Enterprise Manager, the mount server settings are obtained from the configuration database of the backup server. If no helper host or helper appliance configuration is found for the user account, Veeam Backup & Replication uses the configuration set during the latest file-level restore performed on the backup server. Thus, before you start file-level restore from Enterprise Manager, make sure the mount server settings are configured on the backup server with which Veeam Agent is integrated.

When you start guest OS file restore from Enterprise Manager, the helper host or appliance is selected according to the following algorithm:

1. Enterprise Manager attempts to obtain the helper host or appliance settings from the configuration database of the backup server.
2. If no helper host or appliance configuration is found for the user account, Veeam Backup & Replication uses the configuration that was last selected at the **Helper host** step of the **Guest File Restore** wizard. For details, see the Specify Helper Host section of the Veeam Backup & Replication User Guide.
3. If the **Guest File Restore** wizard has not been launched, Enterprise Manager checks whether a default Linux mount server is configured on the backup server. If the mount server exists, Enterprise Manager uses it for Linux file restore.
4. If no default Linux mount server is found, Enterprise Manager displays an error.

NOTE

If you plan to deploy multiple helper appliances to restore machines backed up by Veeam Agents integrated with different backup servers, their initial configuration must be performed on the backup servers. Centralized configuration from Veeam Backup Enterprise Manager is not supported.

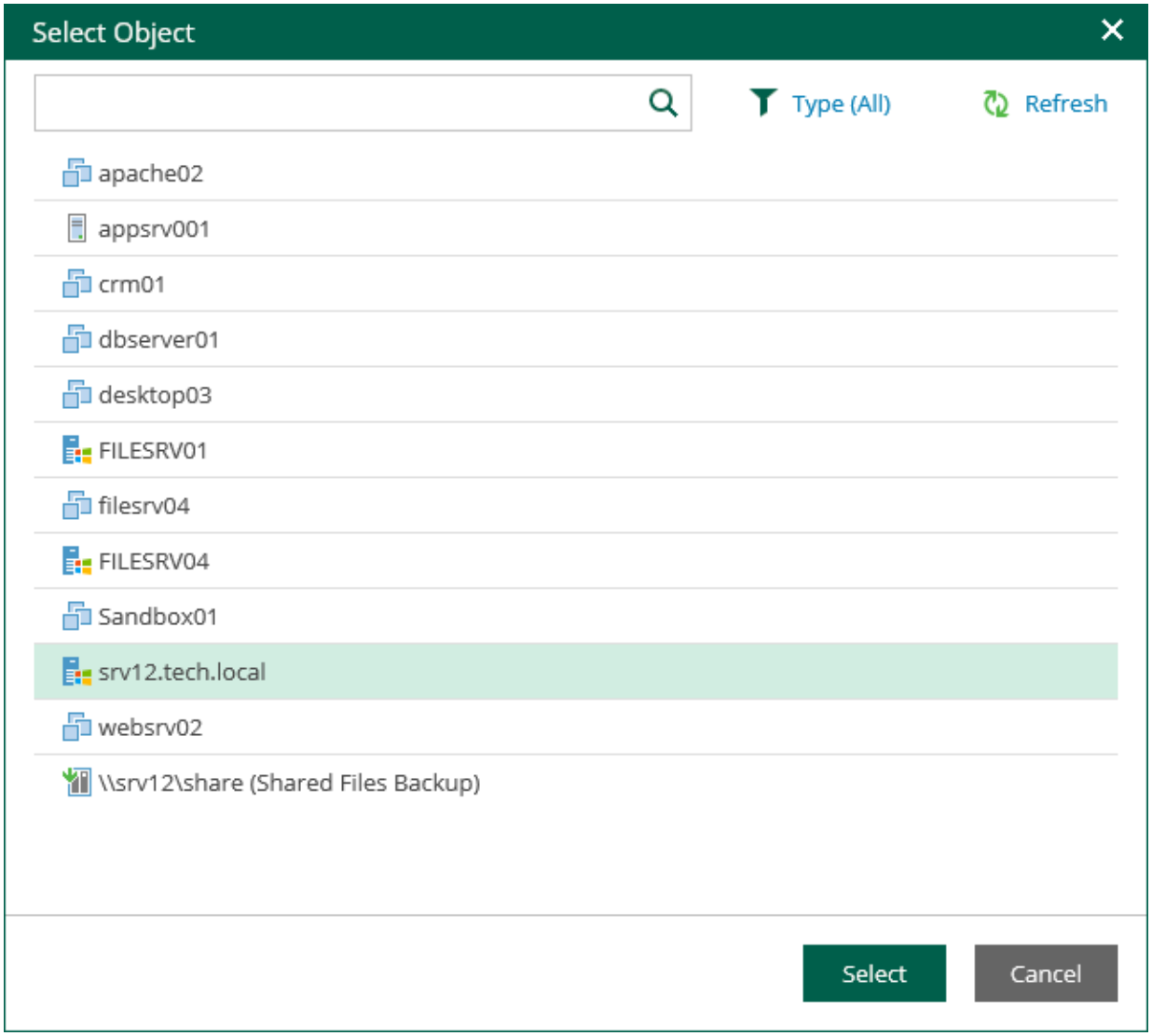
Other Prerequisites

1. Make sure that the DNS name of the target (original) server where you plan to restore the files is resolved properly.
2. During guest file restore to the original location, you are prompted for the credentials to access the target server. Specify a user name and password or private key for the account with sufficient access rights.

Browsing and Restoring Guest OS Files

To browse guest OS files in a physical server backup:

1. In the Enterprise Manager main window, click the **Files** tab.
2. Select a necessary server. You can type in a server name or pick it from the list. Note that server icons indicate server OSes.



3. If the server is backed up without guest indexing, click **Mount Backup** and wait for the process to complete.
4. In the **Restore point** field in the upper-left corner of the **Files** tab, select a necessary date of backup and a restore point. Note that the dates when backup of the selected server was performed are highlighted in the calendar.
5. To search for a file or folder, take the steps similar to the Searching for Guest OS Files in Machine Backups procedure.
6. To restore a file or folder, take the steps similar to the Performing 1-Click File Restore procedure.

NOTE

File restore from backups of Veeam Agent for Mac, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX to the original location is not available.

When restoring files to the original location, you are prompted for user credentials to the target machine. Make sure the account you provide has sufficient access rights.

Application Item Restore

If your Veeam Backup & Replication is integrated with the Server edition of Veeam Agent, and other prerequisites are met, you can use the backups of the physical application servers to restore the necessary application items.

To restore application items, take the steps described in the following sections:

- Restoring Microsoft Exchange Items
- Restoring Microsoft SQL Server Databases
- Restoring Oracle Databases
- Restoring PostgreSQL Instances

vSphere Self-Service Backup Portal

Veeam Backup & Replication allows backup administrators to delegate VM backup and restore operations to VMware vSphere users. For that, Veeam Backup & Replication offers vSphere Self-Service Backup Portal — a web tool based on Veeam Backup Enterprise Manager. With the portal, users can create and manage backup jobs that process VMware vSphere VMs and restore data from backups created with these jobs. All operations are performed from the web UI without the need to deploy the Veeam Backup & Replication console on the user machine.

To define what VMs vSphere users can back up and restore, Veeam Backup Enterprise Manager offers the concept of delegation mode. The delegation mode specifies conditions that must be met to allow a user to add a VM to the backup job. The administrator can choose from 3 delegation modes based on vSphere tags, vSphere roles or VM privileges. For more information, see Configuring Delegation Mode.

In terms of vSphere Self-Service Backup Portal, a vSphere user that works with the portal is considered a tenant. To access the portal, a tenant uses the tenant account created by the Enterprise Manager administrator. The administrator can create tenant accounts for a separate vSphere user and a group of users. Tenant account settings define storage quota available to the tenant in the backup repository and settings for backup jobs created by the tenant. For more information, see Managing Tenant Accounts.

To simplify backup job management for tenants, advanced job settings (such as backup settings and storage settings) are automatically populated from job templates. The administrator can assign a separate template to each tenant account.

When working with vSphere Self-Service Backup Portal, you can perform the following tasks:

- Administrator tasks
- Tenant tasks

Administrator Tasks

To let tenants work with vSphere Self-Service Backup Portal, the Enterprise Manager administrator performs the following tasks:

1. Configures the delegation mode

   The default delegation mode allows tenants to access VMs with the *VirtualMachine.Interact.Backup* privilege. The administrator can change the delegation mode, if necessary.

2. Creates and manages tenant accounts

   By default, Veeam Backup Enterprise Manager offers a group tenant account for users of the domain that includes the Enterprise Manager server. Each user can access the portal and use a 30 GB quota on the default backup repository to create VM backups. Users can create backup jobs with default advanced settings and custom schedule. The administrator can edit settings of the default account and create other accounts to configure granular access to storage quotas and backup settings.

Tenant Tasks

Tenants access the vSphere Self-Service Backup portal using the portal URL obtained from the Veeam Backup Enterprise Manager administrator. Tenants can log in to the portal under a domain user account or single sign-on account. For more information, see Using vSphere Self-Service Backup Portal.

Tenants can use the portal to work with vSphere VMs that are available to them according to the selected delegation mode. VM backup settings are defined by the properties of the tenant account.

Tenants can use vSphere Self-Service Backup Portal to perform the following operations:

- Create and manage backup jobs that process vSphere VMs.
- View VM backup statistics.
- Restore vSphere VMs to the original location.
- Restore files from indexed and non-indexed guest OS file systems of vSphere VMs.
- Perform item-level restore for Microsoft SQL Server and Oracle databases.

For more information, see Using vSphere Self-Service Backup Portal.

In This Section

- Configuring Delegation Mode
- Managing Tenant Accounts
- Using vSphere Self-Service Backup Portal

Configuring Delegation Mode

To define what VMs the tenants of vSphere Self-Service Backup Portal can back up and restore, the Enterprise Manager administrator can configure the delegation mode. The delegation mode specifies conditions that must be met to allow a tenant to add a VM to the backup job.

Before you configure the delegation mode, make sure the following requirements are met:

- If you have configured a single sign-on service to access vSphere Self-Service Backup Portal, you must use the delegation mode based on vSphere tags only. For more information on single sign-on, see SAML Authentication Support.
- The **vSphere** tab is not displayed if all your vCenter Servers are added as part of VMware Cloud Director infrastructure and you do not have any tenant accounts that were previously added for one of the VMware vCenter Servers.
- If you change the delegation mode when tenants already work with vSphere Self-Service Backup Portal, tenants can lose access to VMs that were available to them according to the original delegation mode. Make sure that the necessary tags, roles or privileges are configured in VMware vSphere.

To configure the delegation mode, take the following steps:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one backup server with a vCenter Server as part of its infrastructure.
4. If a VMware Cloud Director server is added to your backup infrastructure, make sure that the **vSphere** tab is selected.
5. In the **Delegation Mode** window, select a delegation mode:
   - **vSphere tags** — to allow tenants to work with VMs to which the specified tags are assigned. If you select this option, you must specify the necessary tags in the properties of the tenant account. You can specify tags for each tenant account individually. For more information, see Adding Tenant Account and Editing Tenant Account.

     > **NOTE**
     >
     > To enable your tenants to restore entire VMs to a new location, you must assign the specified tags to all VMware vSphere parent objects in the target location, including the host, VM folder, resource pool, datastore and network.

   - **vSphere role** — to allow tenants to work with VMs that are available through the specified vSphere role. Note that Enterprise Manager determines whether a vSphere user has access to a VM, based on the effective user permission on the VM. Because direct user permissions override group permissions, and permissions on child objects override inherited permissions from parent objects, a VM may be unavailable to the tenant even if the delegation role is assigned higher in the vCenter hierarchy. For more information on vSphere permissions, see this VMware KB article.

     To specify a vSphere role:

     i. Next to the **vSphere role** option, click **Select Role**.

        Alternatively, if you have already selected a role before, click the name of the currently selected role.

ii. In the **Select Role** window, select the required vSphere role.

iii. Click **OK**.

- **VM privilege** – to allow tenants to work with VMs for which they have the specified vSphere privilege.

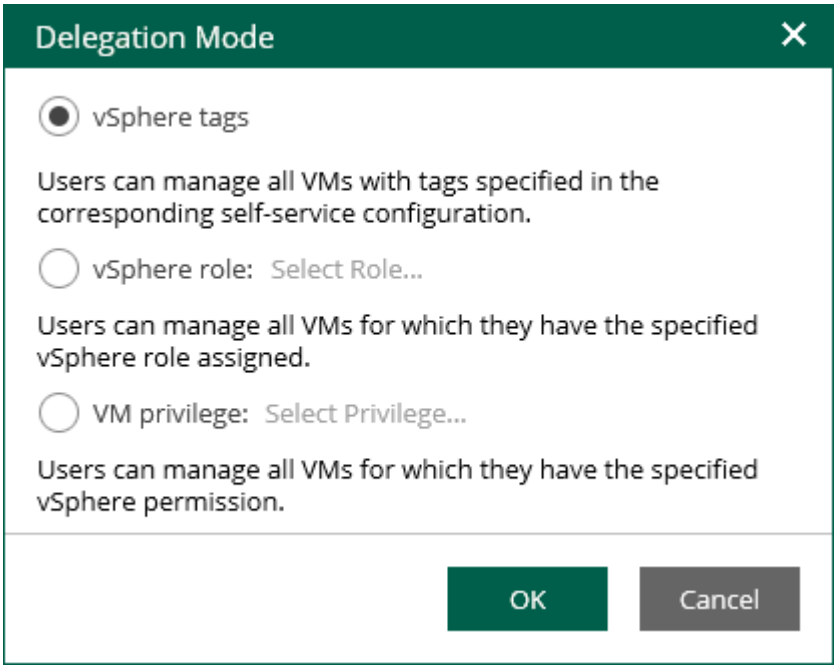
  To select a vSphere privilege:

  i. In the **VM privilege** field, click the name of the currently selected privilege. By default, the *VirtualMachine.Interact.Backup* privilege is selected.

  ii. In the **Select Privilege** window, select the required privilege.

  iii. Click **OK.**

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



Managing Tenant Accounts

Veeam Backup Enterprise Manager offers the following types of vSphere Self-Service Backup Portal tenant accounts: User, Group, External User and External Group.

Type	Description	How to Sign In	Name Format
User	AD user	By specifying a user name and password	• Windows-based Enterprise Manager: *DOMAIN\Username* (domain is optional) • Linux-based Enterprise Manager: *Username@DOMAIN* (domain is mandatory for AD users)
Group	AD group	By specifying a user name and password	• Windows-based Enterprise Manager: *DOMAIN\Groupname* (domain is optional) • Linux-based Enterprise Manager: *Groupname@DOMAIN* (domain is mandatory for AD groups)
External User	IdP user	By using single sign-on*	*Username@Suffix*
External Group	IdP group	By using single sign-on*	Free-form string

* For more information on the single sign-on capability, see SAML Authentication Support.

> **NOTE**
>
> You cannot create a vSphere Self-Service Backup Portal tenant account for a local user account.

Veeam Backup Enterprise Manager administrators can perform the following tasks with the tenant accounts:

- Add a new tenant account
- Edit an already created tenant account
- Export a report on the created tenant accounts
- Remove a tenant account

Adding Tenant Account

Veeam Backup Enterprise Manager offers the default Domain Users account for vSphere Self-Service Backup Portal tenants. It is a group account that includes all users from the Enterprise Manager server domain. To configure granular access to storage quotas and backup settings, the Enterprise Manager administrator can add new tenant accounts.

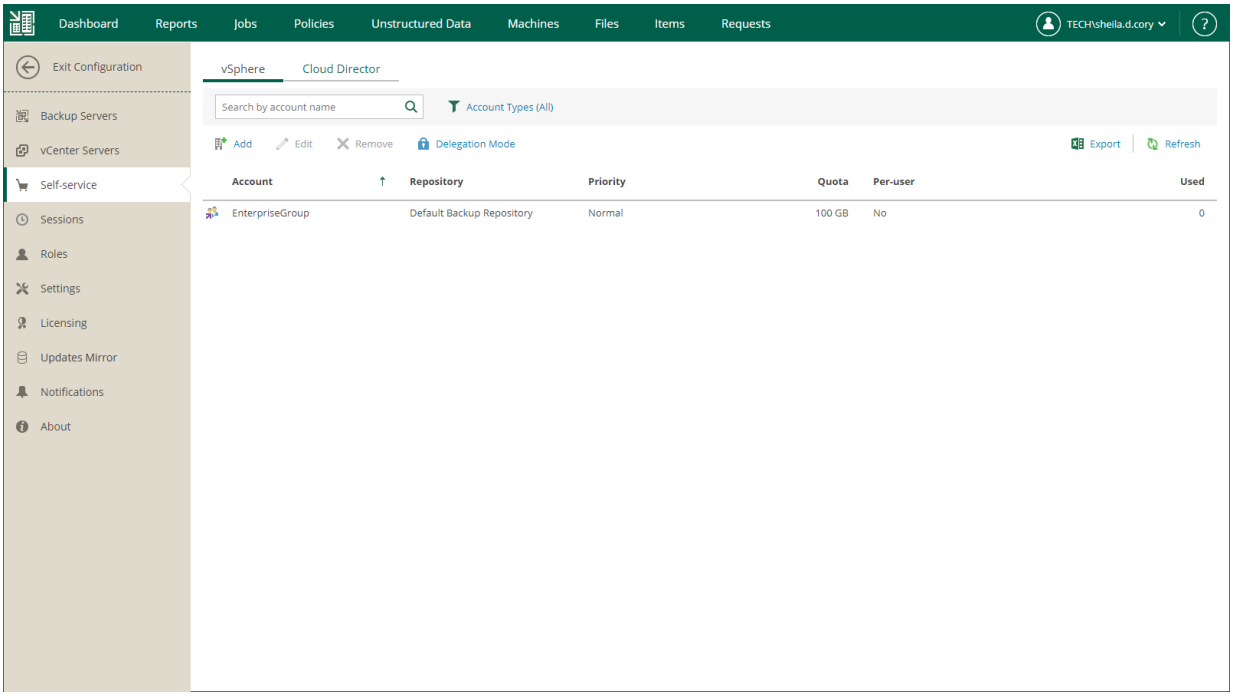
Before you add a tenant account, consider the following:

- If you plan to provide a user with access to vSphere Self-Service Backup Portal only, and not to the main Enterprise Manager UI, you do not need to configure an account for this user on the **Roles** tab of the **Configuration** view.
- The **vSphere** tab is not displayed if all your vCenter Servers are added as part of VMware Cloud Director infrastructure and you do not have any tenant accounts that were previously added for one of the vCenter Servers.

To add a tenant account for vSphere Self-Service Backup Portal:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter Server as part of its infrastructure.
4. If a VMware Cloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Click **Add**.



6. From the **Type** drop-down list, select a type of the account: *User*, *Group*, *External User* or *External Group*. For more information, see Managing Tenant Accounts.
7. In the **Account** field, specify an account name in the *DOMAIN|Username* or *Username@Suffix* format depending on the account type. For more information, see Managing Tenant Accounts.

> **NOTE**
>
> You cannot create a vSphere Self-Service Backup Portal tenant account for a local user account.

8. From the **Repository** drop-down list, select a target repository that will contain VM backups created by the tenant. The list includes repositories configured on Veeam backup servers added to Veeam Backup Enterprise Manager.

   Backup repository settings specified at this step will take priority over backup repository settings prescribed by the selected job template.

   > **NOTE**
   >
   > You cannot assign to tenants Veeam Cloud Connect repositories, as well as NetApp or Nimble storage systems storing snapshots created by Veeam snapshot-only jobs.

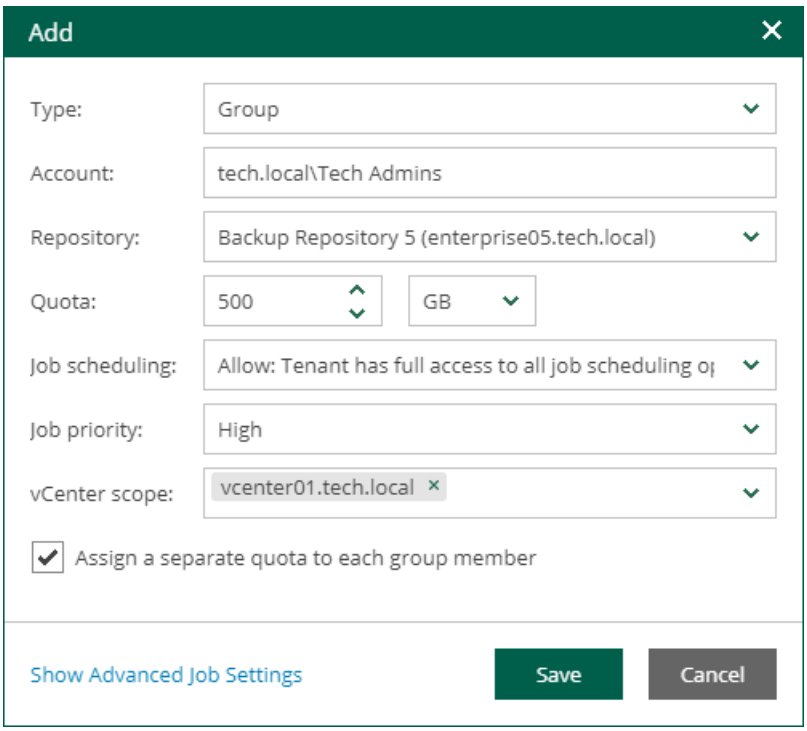
9. In the **Quota** field, specify the repository storage quota for the tenant account. Choose *GB* or *TB* from the drop-down list and enter the required quota size.
10. From the **Job scheduling** drop-down list, select how the job scheduling will be organized. The following options are available:
    - *Allow: Tenant has full access to all job scheduling options*
    - *Allow: Tenant can create daily and monthly jobs only*
    - *Deny: Creates daily jobs with randomized start time within the backup window*

      For tenant backup jobs, the backup window is defined by backup window settings specified in Veeam Backup Enterprise Manager. Backup window settings specified for the job template that you will select at the step 12 do not affect tenant jobs. For information on how to specify the backup window in Enterprise Manager, see Customizing Dashboard Chart.
    - *Deny: Creates job with no schedule assigned*

    For more information on job scheduling, see Edit Job Schedule.
11. From the **Job priority** drop-down list, select a normal or high priority for backup jobs of the tenant.
12. If you have multiple vCenter Servers in your infrastructure and want to provide the tenant account with access to VMs of specific vCenter Servers only, from the **vCenter scope** drop-down list, select the necessary vCenter Servers. By default, the *All vCenter Servers* options is selected.
13. If you have selected the delegation mode that is based on vSphere tags, in the **vSphere tags** field, specify tags assigned to VMs that will be available to the tenant.

    For more information on delegation modes, see Configuring Delegation Mode.

14. If you add a tenant account of the Group or External Group type, select the **Assign a separate quota to each group member** check box to provide each user of the group with individual quota on the backup repository. Each user will be able to work with backup jobs and VM backups created by this user only. Backups and jobs of other users will not be displayed.



15. Specify advanced settings for backup jobs of the tenant:

    a. Click the **Show Advanced Job Settings** link.

    b. In the **Advanced job settings** section, view the currently used backup job settings.

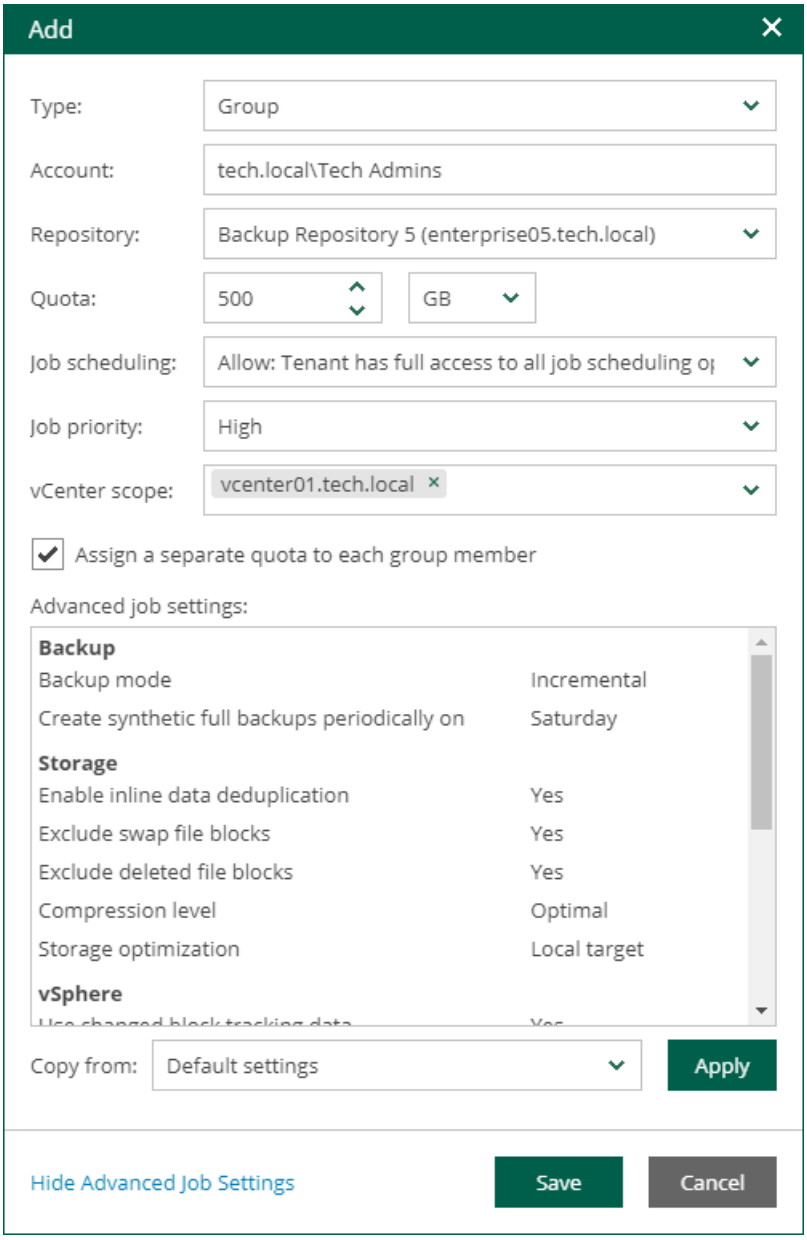
    c. From the **Copy from** list, select the advanced settings that you want to apply to tenant jobs. For more information on the specific settings, see the Specify Advanced Backup Settings section of the Veeam Backup & Replication User Guide.

    - Select *Default settings* to use the default advanced settings as they are shown in the Veeam Backup & Replication console. This option is applied by default.
    - Select *<Job name>* to use the advanced settings of an existing backup job as a template for tenant backup jobs. When a tenant creates a backup job on the vSphere Self-Service Backup Portal, Enterprise Manager will copy the advanced settings from the template and apply them to the job.

      Note that, in the **Copy from** list, Enterprise Manager displays only VMware vSphere backup jobs that are configured in advance on a backup server added to Enterprise Manager.

    d. To apply the job template, click **Apply**.

16. To add the account, click **Save**.



Editing Tenant Account

The Veeam Backup Enterprise Manager administrator can edit tenant accounts configured for vSphere Self-Service Backup Portal. For example, the administrator changes backup scheduling settings or other settings for tenant backup jobs.

Consider the following recommendations for modifying tenant account settings for vSphere Self-Service Backup Portal:

- Make sure to establish a proper connection between the backup server and Enterprise Manager server. Otherwise, the changes of the tenant account settings will not be saved to the configuration database.
- If you plan to modify job template for a tenant account, remember that the new settings will be applied only to the new jobs created by the tenant; the changes will not affect existing jobs.
- If you want an existing backup job to create backups in another backup repository instead of the repository that is currently specified in the properties of the tenant account, do the following:

  a. In Veeam Backup Enterprise Manager, specify the new backup repository in the properties of the tenant account.

  b. Move vSphere VM backups created by the tenant to the new repository.

  c. In Veeam Backup & Replication, specify the new backup repository in the properties of tenant backup jobs.

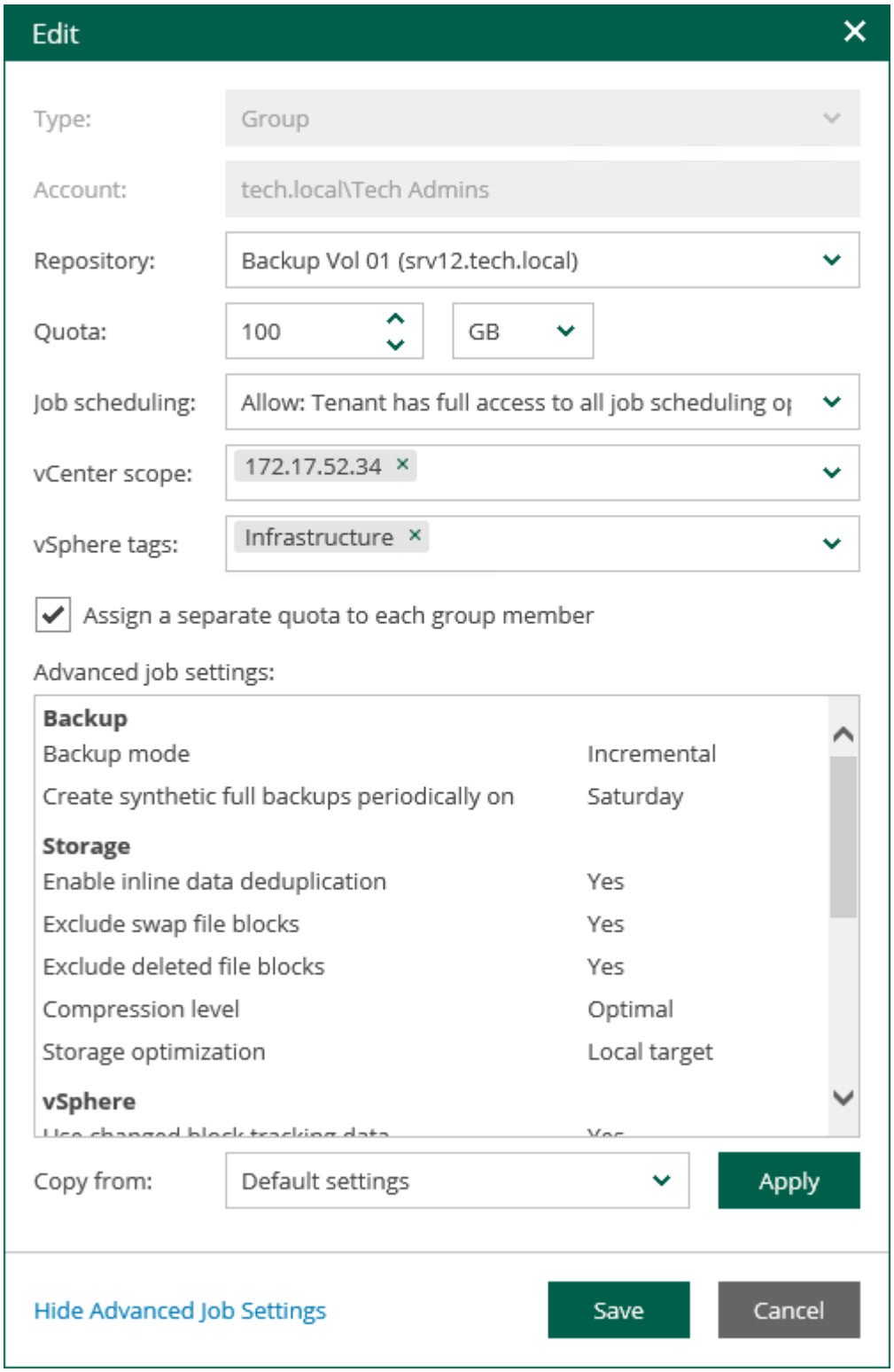
  Otherwise, tenant backup jobs will continue creating backups in the former repository.

To change settings of a tenant account:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter Server as part of its infrastructure.
4. If a VMware Cloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Select the account you need and click **Edit**.
6. In the **Edit** window, edit tenant account settings as required. For more information, see Adding Tenant Account.

7. Click **Save**.


Edit
Type:
Group
Account:
tech.local\Tech Admins
Repository:
Backup Vol 01 (srv12.tech.local)
Quota:
100
GB
Job scheduling:
Allow: Tenant has full access to all job scheduling o
vCenter scope:
172.17.52.34
vSphere tags:
Infrastructure
Assign a separate quota to each group member
Advanced job settings:
Backup
Backup mode
Incremental
Create synthetic full backups periodically on
Saturday
Storage
Enable inline data deduplication
Yes
Exclude swap file blocks
Yes
Exclude deleted file blocks
Yes
Compression level
Optimal
Storage optimization
Local target
vSphere
Copy from:
Default settings
Apply
Hide Advanced Job Settings
Save
Cancel

Exporting List of Tenant Accounts

The Veeam Backup Enterprise Manager administrator can generate a report on tenant accounts configured for vSphere Self-Service Backup Portal. This report includes information on the account name, backup repository used by the account, storage quota allocated to the account, and space used by the account.

To generate a report:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter Server as part of its infrastructure.
4. If a VMware Cloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Click the **Export** link in the upper-right corner.

The report is saved to the `excelreport.xls` file.

	A	B	C	D	E
1	**Account**	**Repository**	**Quota**	**Per-user**	**Used space**
2	John Smith	Default Backup Repository	40 GB	No	0.00 GB
3	Mark Green	Default Backup Repository	100 GB	No	0.00 GB
4	William Fox	Default Backup Repository	100 GB	No	0.00 GB

Removing Tenant Account

The Veeam Backup Enterprise Manager administrator can remove tenant accounts configured for vSphere Self-Service Backup Portal.

To remove a tenant account:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.

   The **Self-service** section is available if you have added to Enterprise Manager at least one Veeam backup server with a vCenter Server as part of its infrastructure.
4. If a VMware Cloud Director server is added to your Veeam backup infrastructure, make sure that the **vSphere** tab is selected.
5. Select the account you want to remove.
6. Click **Remove**.
7. In the **Remove configuration** window, select necessary options:
   - To delete backup jobs created by the tenant, select the **Delete jobs** check box.
   - To delete all backups created by the tenant, select the **Delete backup files** check box.

     If four-eyes authorization is enabled on the backup server, backup files will remain in the backup repository and become orphaned.
8. To confirm the removal, click **Yes**.

Using vSphere Self-Service Backup Portal

vSphere Self-Service Backup Portal is a tool for VMware vSphere users that facilitates operations with delegated VM protection, including VM restore and files restore. These operations do not require access to the Veeam Backup & Replication console. For backup and restore operations, tenants access vSphere Self-Service Backup Portal.

Accessing Portal

To access vSphere Self-Service Backup Portal:

1. Open your web browser and enter the following address in the address bar:

   ```
   https://<EnterpriseManagerServer>/backup
   ```

   For example:

   ```
   https://enterprise01.tech.local/backup
   ```

2. From the drop-down list, select a language that you want to use as the display language. For more information, see Managing Languages.

3. Log in using your credentials:

   - To log in with Enterprise Manager credentials:

     i. In the **Username** and **Password** fields, specify credentials of the domain user for which the Enterprise Manager administrator created a vSphere Self-Service Backup Portal tenant account. The username must be provided in the *DOMAIN|Username* format.

     ii. To save the entered credentials for future access, select the **Remain signed in** option.

     iii. Click **Sign in**.

   - To log in with the credentials of the Microsoft Windows account that you are currently signed in on the machine where you are launching Enterprise Manager, click **Sign in as current user** option.

   - To log in with single sign-on, click **Sign in with SSO**. You will be redirected to the login webpage of the single sign-on service. Complete the sign-in procedure on the login page. If the account is already authenticated in the single sign-on service, you will immediately access the Enterprise Manager website.

     The **Sign in with SSO** option is available if SAML authentication is configured for Veeam Backup Enterprise Manager. For more information, see Configuring SAML Authentication Settings.

Working with Portal

You can use vSphere Self-Service Backup Portal to perform the following operations:

- View statistics on backups of vSphere VMs. For more information, see Viewing Self-Service Backup Portal Statistics.

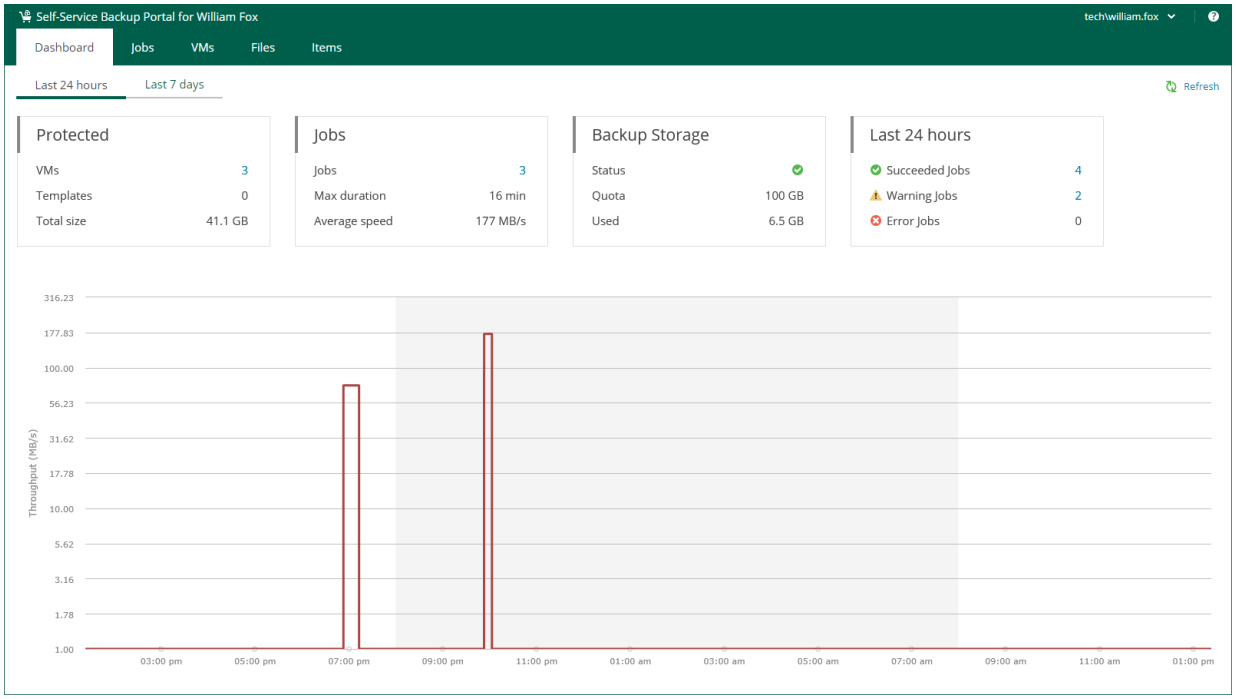
- Work with backup jobs that process vSphere VMs: create and edit backup jobs; examine and export backup job session data; start, stop and retry backup jobs. For more information, see Managing Backup Jobs.
- Perform backup and restore operations with vSphere VMs. For more information, see Managing VMs.
- Search for files in guest file systems of backed-up VMs and restore the necessary files to the original location or download them to a local machine. For more information, see Restoring Guest OS Files.
- Perform item-level restore of Microsoft SQL Server and Oracle databases. For more information, see Restoring Application Items.

NOTE

If the Veeam Backup Enterprise Manager server is added to the Veeam ONE monitoring scope, the restore operations performed with vSphere Self-Service Backup Portal are included in the Restore Operator Activity report available in Veeam ONE.

Viewing Self-Service Backup Portal Statistics

The **Dashboard** tab contains statistics on tenant backup infrastructure, including information about protected VMs, backup jobs, backup storage and the number of jobs that completed successfully, finished with warnings and errors. You can view statistics for the last 24 hours or last 7 days. To switch between the views, click **Last 24 hours** or **Last 7 days** in the upper-left corner of the working area.



The **Protected** block displays the following information:

- **VMs** – number of VMs successfully processed during the selected period. At least one restore point was created for these VMs.
- **Templates** – number of virtual machine templates successfully protected during the specified period.
- **Total size** – total size of successfully protected VMs and templates.

The **Jobs** block displays the following information:

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

The **Backup Storage** block displays the following information:

- **Status** – status of the backup storage assigned to the user: *Green* – more than 10% of storage space is free; *Yellow* – less than 10% of storage space is free; *Red* – no free space on backup storage.
- **Quota** – storage quota assigned to the user.
- **Used** – storage quota used by the user.

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

To visualize on-going job data, the **Dashboard** tab also comprises a graph showing time and date when jobs were performed, and the network throughput rate during the job.

The highlighted part of the graph represents the configured backup window if this option was specified in the dashboard settings. For more information, see Customizing Dashboard Chart.

Managing Backup Jobs

On the **Jobs** tab of Self-Service Backup Portal, you can perform the following operations with backup jobs:

- Create a new backup job for vSphere VMs
- Start, stop and retry jobs
- Enable and disable jobs
- Edit backup job settings
- Delete backup jobs

IMPORTANT

- For the vSphere Self-Service Backup Portal tenants, job cloning is not available.
- In vSphere Self-Service Backup Portal, you cannot create and edit jobs managed by backup servers of earlier major or minor versions. For example, after you upgrade Enterprise Manager to version 13.1, you will not be able to create and edit jobs managed by a backup server with version 12.3. To resolve the issue, upgrade the backup server as well.

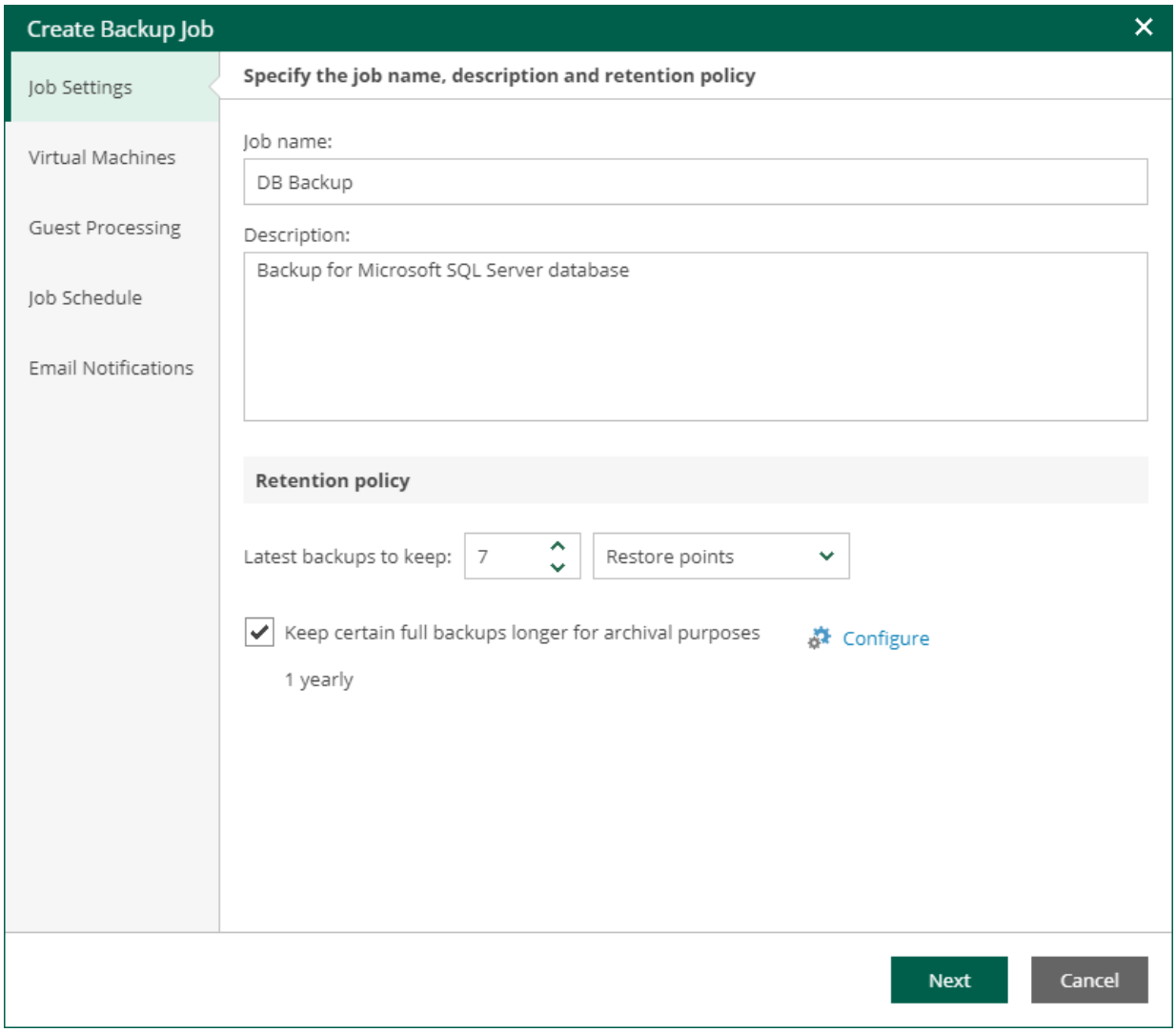
Creating Backup Job

To create a new vSphere backup job:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal and click **Create**.

2. At the **Job Settings** step of the wizard, specify the backup job name, description and retention policy settings. The retention policy defines how many restore points are kept in the backup repository and can be used for data restore.

   For more information, see the Retention Policy section of the Veeam Backup & Replication User Guide.



3. At the **Virtual Machines** step of the wizard, select which vSphere VMs the job will process. For more information, see Edit the List of Virtual Machines.

4. At the **Guest Processing** step of the wizard, select the guest OS processing options and guest OS credentials. For more information, see Configure Guest Processing Settings.

5. At the **Job Schedule** step of the wizard, configure the backup job scheduling options. For more information, see Schedule the Job.

   You can configure backup job scheduling options only if the Enterprise Manager administrator allowed this in the properties of the tenant account. For more information, see Adding Tenant Account.

6. At the **Email Notifications** step of the wizard, select the **Enable e-mail notifications** check box and configure notification settings:

   a. In the **Recipients** field, enter email addresses of recipients separated by comma.

   b. [Optional] In the **Subject** field, specify the subject for notification emails.

   c. Select **Notify on success** to receive an email notification when the job completes successfully.

d. Select **Notify on warning** to receive an email notification when the job completes with a warning.

e. Select **Notify on error** to receive an email notification when the job fails.

f. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.

7. Click **Finish**.

The backup job will create backups in the backup repository that the Enterprise Manager administrator selected as the target repository in the properties of the tenant account. Advanced job settings such as the backup settings and storage settings will be obtained from the job template assigned to the tenant by the administrator. For more information, see Editing Tenant Account.

Editing Backup Job

You can edit a backup at any time you need. For example, you may want to change scheduling settings for the job or add VMs to the job.

To edit backup job settings, do the following:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal.
2. In the working area, select the job you want to edit and click **Edit**.
3. In the **Edit** window, edit backup job settings as required. You will follow the same steps as you have followed when creating the job. For more information, see Creating Backup Job.

Removing Backup Job

You can permanently remove a backup job from the configuration database. Information about the deleted job will be removed from the Veeam Backup & Replication configuration database (and the Enterprise Manager database as well), and the job will no longer appear in the UI.

To remove a job, do the following:

1. Open the **Jobs** tab of vSphere Self-Service Backup Portal.
2. In the working area of the **Jobs** tab, select the job you want to delete.
3. Click **Delete**.
4. You will be prompted to delete backup files. To delete backup files, select the **Delete backup files** check box and click **Yes** to confirm the operation.

   If four-eyes authorization is enabled on the backup server, backup files will remain in the backup repository and become orphaned.

Managing VMs

You can use vSphere Self-Service Backup Portal to perform the following operations with backed-up VMs:

- Restore entire VM to VMware vSphere
- Perform Instant Recovery to VMware vSphere
- Restore VM disks
- Delete VMs

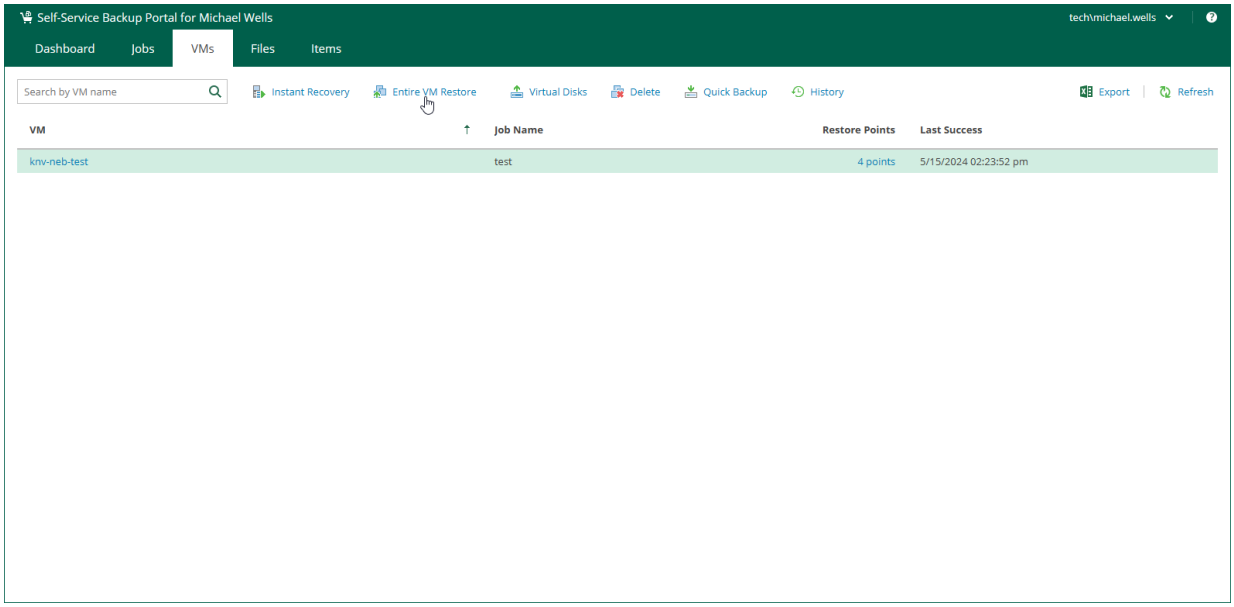
Restoring Entire VM to VMware vSphere

You can restore and entire VM to the original location or a new location included in your restore scope.

> **NOTE**
>
> If your delegation mode is set to *vSphere tags*, the required tags must be assign to all VMware vSphere parent objects in the target location, including the host, VM folder, resource pool, datastore and network. For details on delegation modes, see Configuring Delegation Mode.

To restore an entire VM:

1. On the **VMs** tab, select a VM that you want to restore. You can also use the search field to search for the necessary VM by its name.
2. Click **Entire VM Restore**.
3. Follow the steps of the **Entire VM Restore** wizard. For details, see Restoring Entire VM to VMware vSphere.

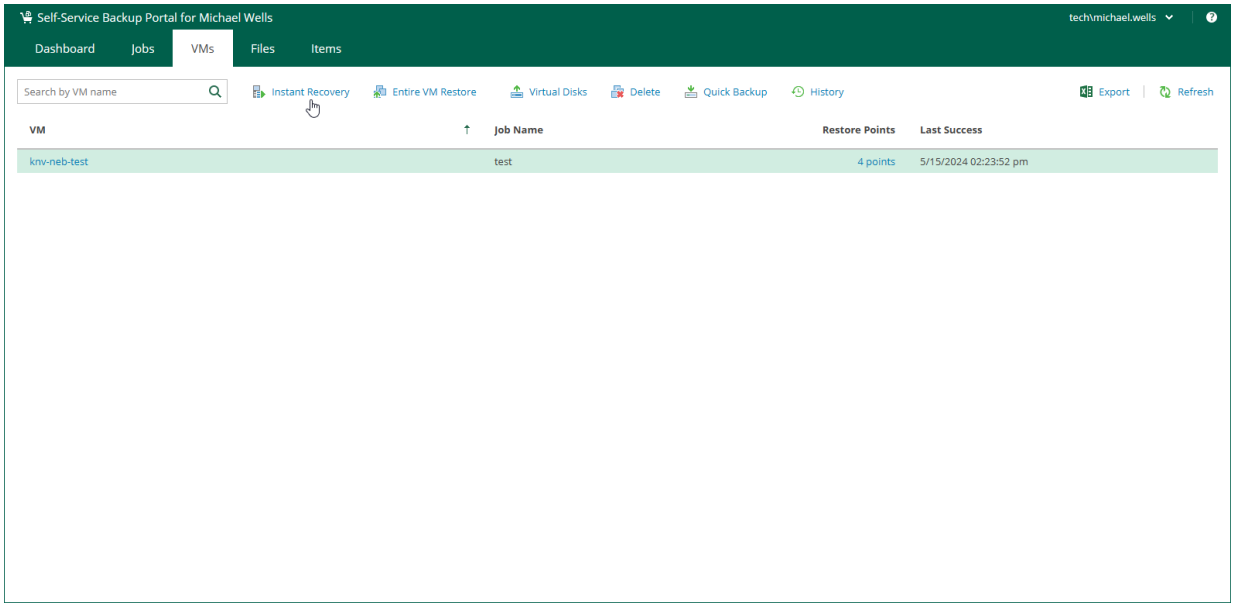


Performing Instant Recovery to VMware vSphere

You can instantly recover a VMware vSphere VM to VMware vSphere. You can recover VMs from backups to the original location or a new location included in your restore scope. After you have performed Instant Recovery, you have to finalize it. For more information, see Finalizing Instant Recovery to VMware vSphere.

To instantly recover a VM:

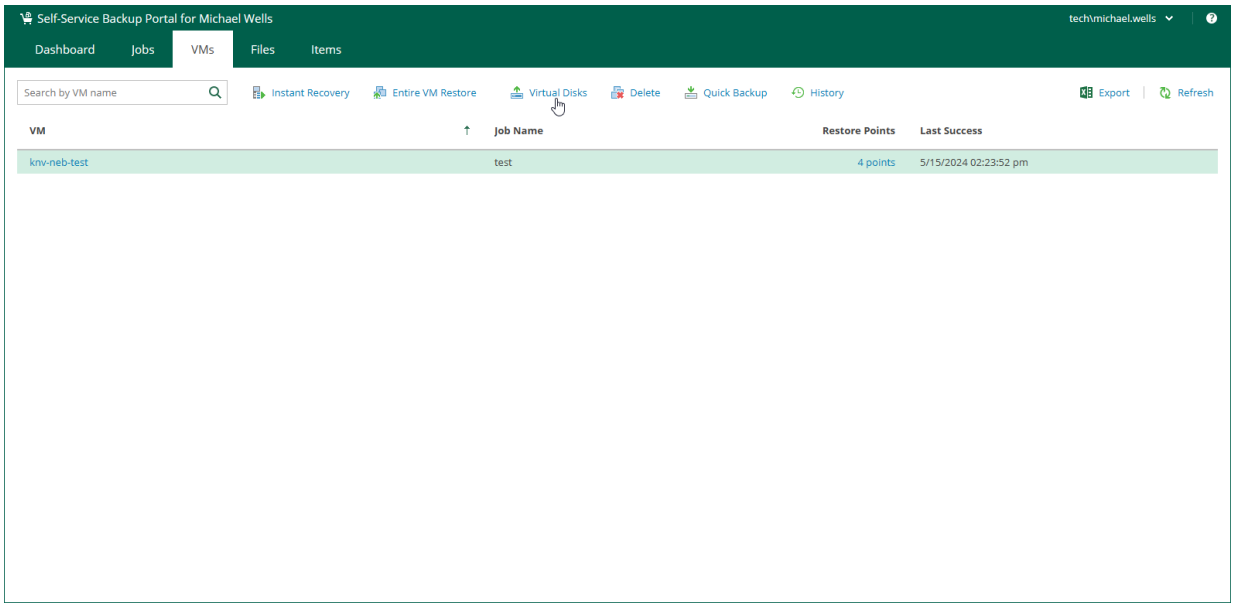
1. On the **VMs** tab, select a VM that you want to recover. You can also use the search field to search for the necessary VM by its name.
2. Click **Instant Recovery**.
3. Follow the steps of the **Instant Recovery to VMware vSphere** wizard. For details, see Instant Recovery to VMware vSphere.



Restoring Virtual Disks

To restore individual virtual disks from backups of VMware vSphere VMs, do the following:

1. On the **VMs** tab, select a VM whose disks you want to restore. You can also use the search field to search for the necessary VM by its name.
2. Click **Virtual Disks**.
3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Virtual Disk Restore.



Deleting VMs

You can delete a VM using vSphere Self-Service Backup Portal. This operation may be useful if you want to delete data of the backed-up VM from the backup repository. The deleted VM is not removed from the list of VMs immediately. The VM will be removed from the list after the VM records are removed from the configuration database of the backup server.

When you delete a VM, Enterprise Manager removes records about the VM from the UI and configuration database. In addition, Enterprise Manager removes data of the deleted VM from the backup.

> **NOTE**
>
> If four-eyes authorization is enabled on the backup server, you cannot delete a VM backup using either the portal or Enterprise Manager.

To delete a VM, do the following:

1. On the **VMs** tab, select a VM. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Delete**.
3. Click **Yes** to confirm the deletion.

Restoring Guest OS Files

The **Files** tab of vSphere Self-Service Backup Portal allows you to browse the guest OS file system in a VM backup and restore individual files. You can restore files from indexed and non-indexed guest OS file systems.

To restore guest OS files, follow the steps described in Performing 1-Click File Restore.

NOTE

- When you restore from non-indexed guest OS file system, mount operation is performed using mount server associated with the backup repository that stores the backup file.
- Before you restore files from a non-Windows VM, make sure that a helper host or helper appliance is configured on the backup server. For more information, see Preparing for File Search and Restore (non-Windows machines).

Restoring Application Items

The **Items** tab of vSphere Self-Service Backup Portal allows you to perform item-level recovery from application-aware backups of Microsoft SQL Server databases, Oracle databases and PostgreSQL instances.

For more information, see the following sections:

- Restoring Microsoft SQL Server Databases
- Restoring Oracle Databases
- Restoring PostgreSQL Instances

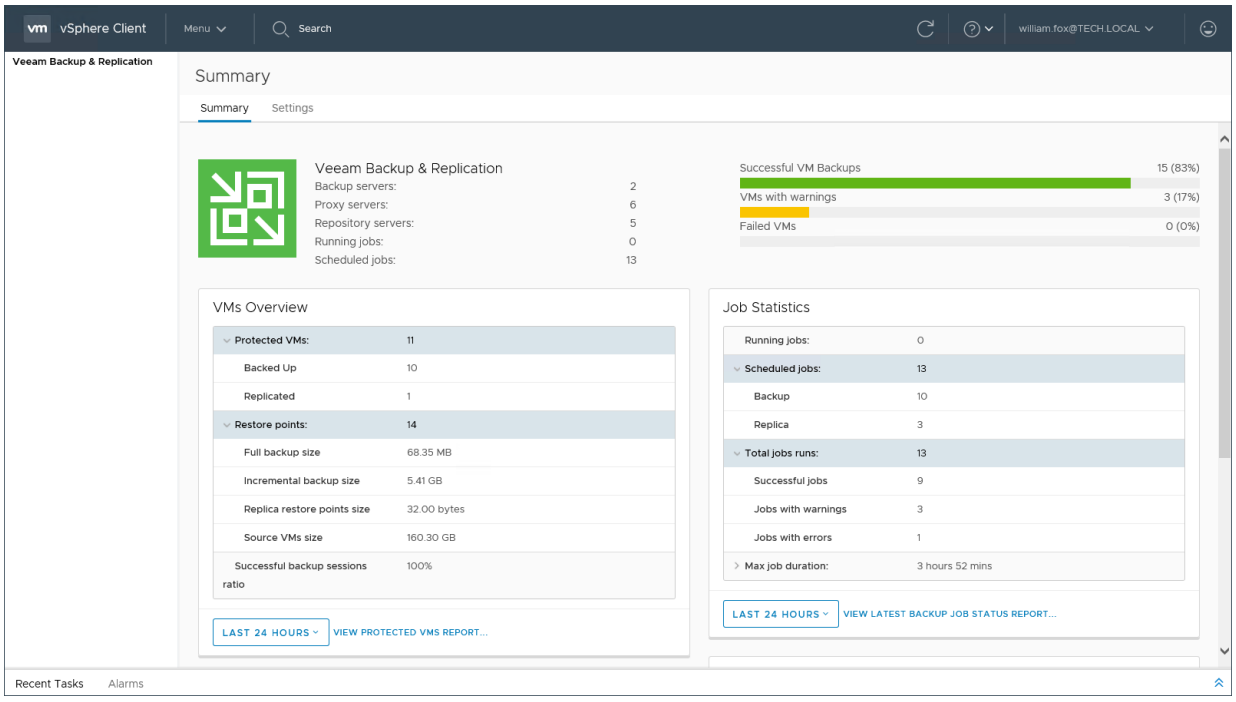
Veeam Plug-in for VMware vSphere Client

Veeam Plug-in for VMware vSphere Client extends the capabilities of the VMware vSphere Client by enabling you to view detailed information about the status of the Veeam Backup & Replication infrastructure and create restore points on demand.

VMware vSphere administrators can perform the following operations using Veeam Plug-in for VMware vSphere Client:

- View the number of successful, warning and failed jobs.
- Access aggregated statistics about used and available storage capacity and processing statistics for VMs.
- Identify unprotected VMs and perform capacity planning.
- Create restore points for selected VMs using VeeamZIP and Quick Backup functions.

Veeam Plug-in for VMware vSphere Client is installed remotely on the Veeam Backup Enterprise Manager server. For more information, see Plug-in Deployment.



Plug-in Deployment

Veeam Plug-in for VMware vSphere Client is installed remotely on the Veeam Backup Enterprise Manager server. During deployment, the installer registers the plug-in as an extension on the VMware vCenter Server, and the vCenter Server downloads the plug-in manifest file. This allows the *vsphere-ui* service to define how the plug-in extends the VMware vSphere Client user interface. The back-end service of the plug-in runs on the Enterprise Manager server.

You can install Veeam Plug-in for VMware vSphere Client using Veeam Backup Enterprise Manager under an account with the Portal Administrator role. For more information, see Installing vSphere Client Plug-in.

For more information on VMware vSphere Client, see the vCenter and Host Management section of the VMware vSphere documentation.

Before you install the plug-in, make sure the following requirements are met:

- The plug-in supports vSphere Client version 7.0.1 and later.
- The vCenter Server must be added to the backup server infrastructure.

  For more information, see the Adding VMware vSphere Servers section of the Veeam Backup & Replication User Guide.
- The backup server that contains the vCenter Server in its infrastructure must be connected to Enterprise Manager.

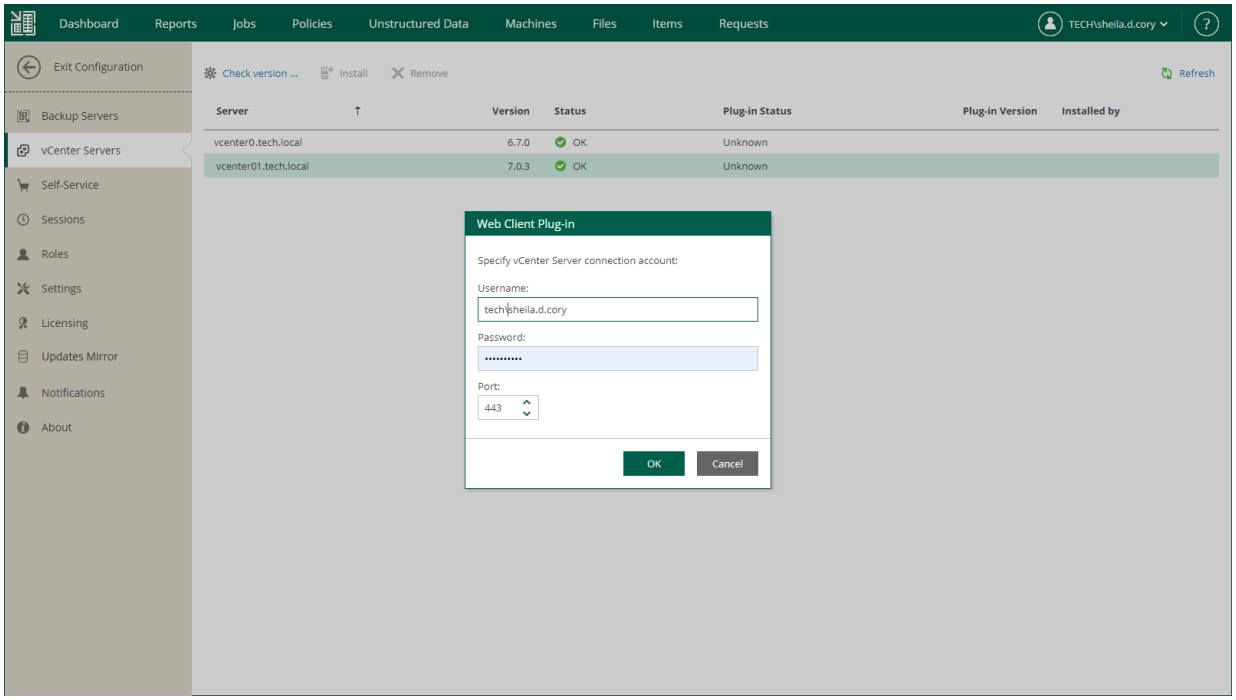
  For more information, see Adding Backup Servers.
- The Enterprise Manager server must be able to resolve the FQDN of the vCenter Server and must have access to the vCenter Server over HTTPS. In particular, this is necessary if the plug-in uses the default vCenter Single Sign-On for authentication.
- Account used to install the plug-in must have sufficient access rights for vCenter Server:
  - **Extension > Register extension** — to install the plug-in
  - **Extension > Unregister extension** — to uninstall the plug-in

  The account must belong to the same domain as the vCenter Server in case of cross-domain access.
- Note that when accessing VMware vSphere Client, you must enter the vCenter Server FQDN (or IP address) that you specified when adding the vCenter Server to the backup server infrastructure. This FQDN is stored in the configuration database and used to authenticate the vCenter Server. vCenter Server alias names are not supported.

Installing vSphere Client Plug-in

To install Veeam Plug-in for VMware vSphere Client, take the following steps:

1. Log in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, go to the **vCenter Servers** section.
4. Select the vCenter Server you need, and click **Check version**.
5. In the **Web Client Plug-in** window, enter a user name and password to connect to the vCenter Server, and specify a connection port (default port is 443). Veeam Backup Enterprise Manager will use these credentials to access the vCenter Server and check if Veeam plug-in has been already installed there. If discovered, the plug-in version will be displayed in the **Plug-in Version** column.
6. If the connection to vCenter Server is successful, and the plug-in has not been installed yet, then the **Install** link will become active. Click it to install the plug-in.
7. After installation, the plug-in will be displayed in the list of vCenter Servers and plug-ins.



Uninstalling vSphere Client Plug-in

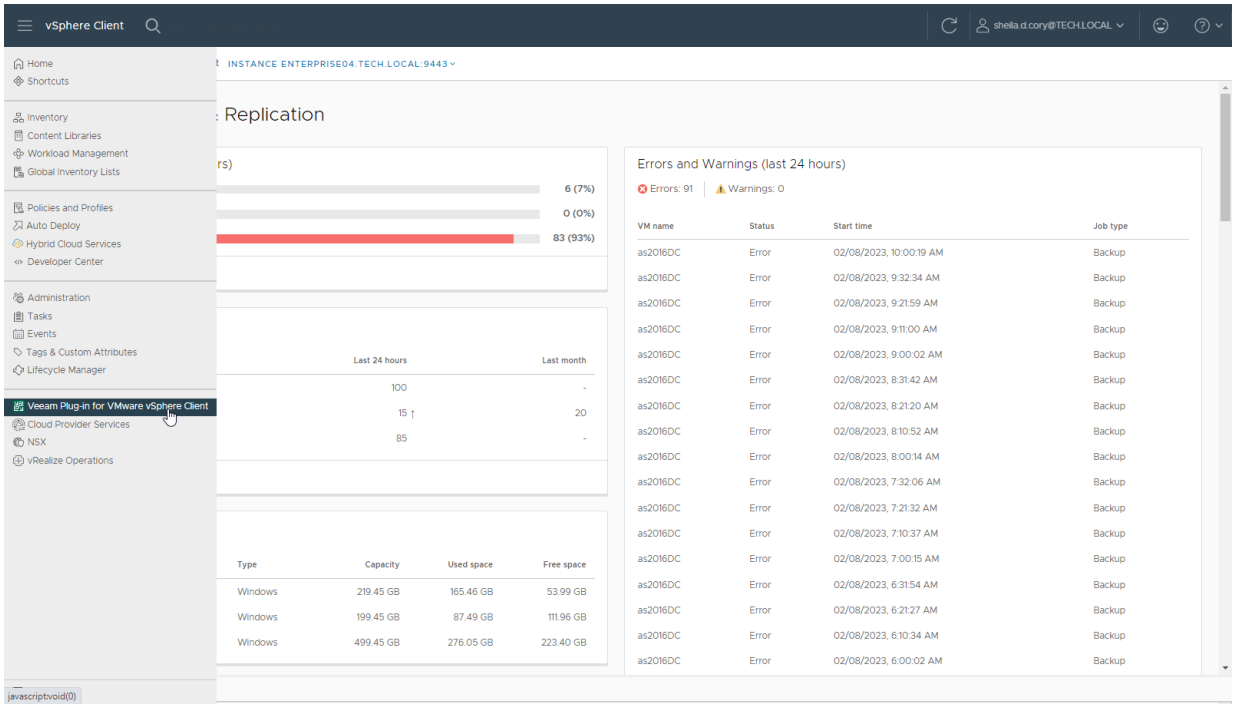
To uninstall Veeam Plug-in for VMware vSphere Client, take the following steps:

1. Log in to Veeam Backup Enterprise Manager using an account with the Portal Administrator role.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, go to the **vCenter Servers** section.
4. Select the vCenter Server you need, and click **Remove**.
5. In the displayed window, click **Yes** to confirm the removal.
6. To finish the uninstallation, restart the vSphere Client service on the vCenter Server.

Accessing vSphere Client Plug-in

To access the plug-in, open the VMware vSphere Client and select **Veeam Plug-in for VMware vSphere Client** from the menu.

Make sure, the account used to access the plug-in has permissions to connect to the Veeam Backup Enterprise Manager server and perform backup operations. For details, see Veeam Plug-in for VMware vSphere Client Authentication.



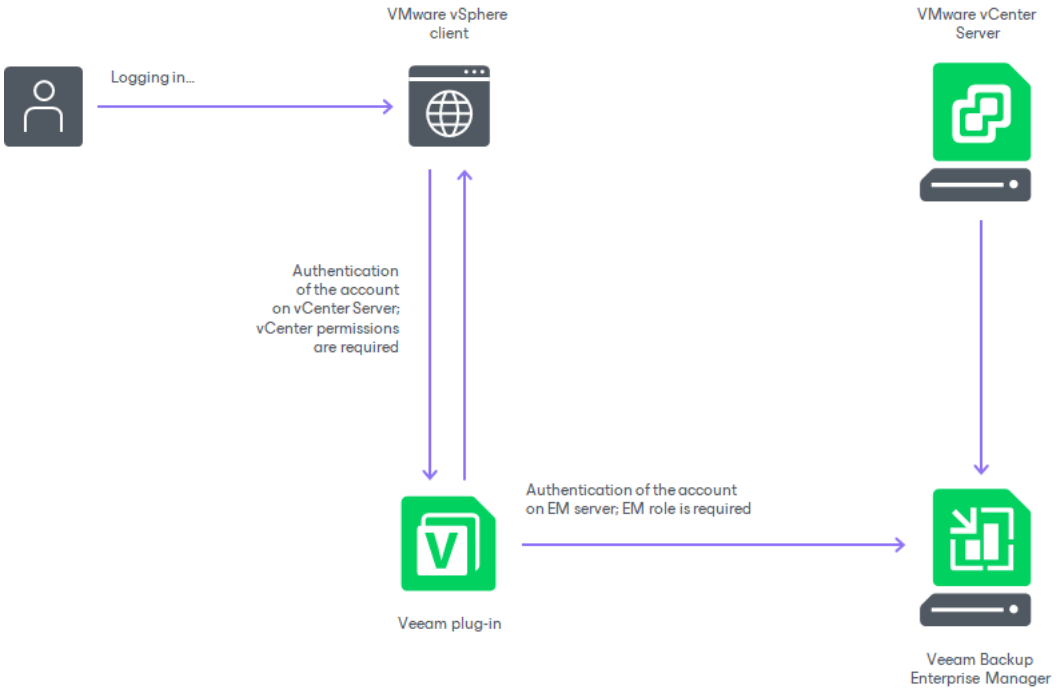
Veeam Plug-in for VMware vSphere Client Authentication

Veeam Plug-in for VMware vSphere Client is installed remotely on the Veeam Backup Enterprise Manager server. During deployment, the installer registers the plug-in as an extension on the VMware vCenter Server, and the vCenter Server downloads the plug-in manifest file. This allows the *vsphere-ui* service to define how the plug-in extends the VMware vSphere Client user interface. The back-end service of the plug-in runs on the Enterprise Manager server.

When using the plug-in, the authentication process includes the following steps:

1. You log in to VMware vSphere Client. To work with the Veeam Plug-in for VMware vSphere Client, your user account must belong to a vCenter Server role that is mapped to an Enterprise Manager role. For more information on role mapping, see Configuring VMware vSphere Roles.
   - To create a VeeamZIP backup or Quick Backup, the Portal Administrator or Portal User role is required.
   - To browse backup infrastructure, the Restore Operator role is enough.

   [Optional] If you have Veeam ONE deployed in your environment and you want to open Veeam ONE reports from the plug-in, the accounts used to log in to the VMware vSphere Client must be also included in the *Veeam ONE Power Users*, *Veeam ONE Read-Only Users* or *Veeam ONE Administrators* group on the machine where Veeam ONE Server is installed. For more information, see the Security Groups section of the Veeam ONE Deployment Guide.
2. Veeam Plug-in for VMware vSphere Client connects to Enterprise Manager, and Enterprise Manager verifies the user account. To perform VeeamZIP and Quick Backup operations, the user account must have the following permissions at the vCenter level: *VirtualMachine.Interact.Backup*, *Task.Create*, *Task.Update*.

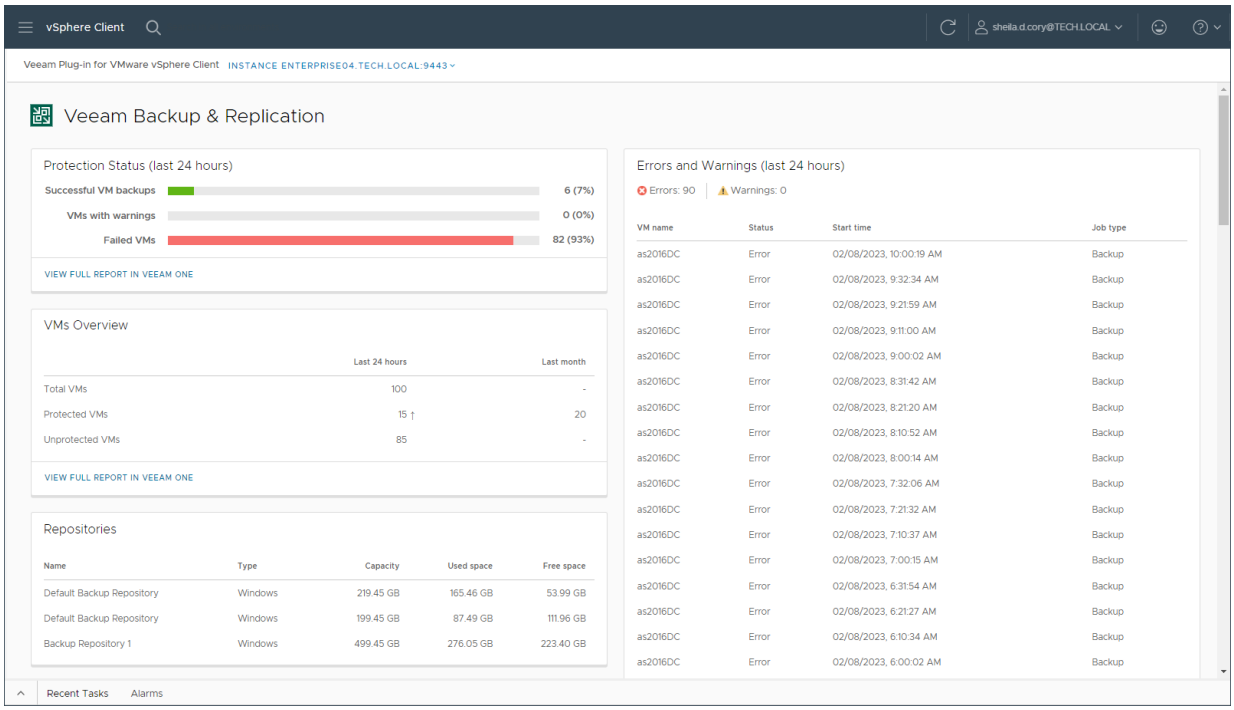


Examining Backup Infrastructure

On the Veeam Plug-in for VMware vSphere Client main page, you can view statistics on the Veeam Backup & Replication infrastructure. The statistics are shown for the VMs that are included in the restore scope specified for your vCenter Server role. For more information on the restore scope, see Configuring VMware vSphere Roles.

You can view the following statistics:

- **Protection Status** – statistics on the status of VM backup and replication jobs for the last 24 hours.
  - **Successful VM backups** – number of successfully backed up or replicated VMs
  - **VMs with Warnings** – number of VMs that were backed up or replicated with a warning
  - **Failed VMs** – number of VMs that were backed up or replicated with an error
- **Errors and Warnings** – statistics on backup and replication sessions that completed with a warning or error for the last 24 hours.
- **VMs Overview** – statistics about all available VMs for the last 24 hours and last month.
  - **Total VMs** – number of all available VMs
  - **Protected VMs** – number of VMs that were backed up or replicated
  - **Not protected VMs** – number of VMs that were not backed up or replicated
- **Repositories** – information about backup repositories, including repository name, type, overall capacity, backup size and free space.
- **Active Sessions** – statistics about all active backup and replication sessions for all vCenter Server VMs.



Creating Restore Points with VeeamZIP and Quick Backup

You can quickly create a VM restore point using VeeamZIP (full backup) or Quick Backup (incremental backup) right from VMware vSphere Client, with no need to use the Veeam Backup & Replication console. To utilize these capabilities, you need to pair a vCenter Server role of your account with the Portal Administrator or Portal User role of Enterprise Manager. For more information on assigning Enterprise Manager roles, see Configuring VMware vSphere Roles.

In This Section

- Creating Full VM Backup with VeeamZIP
- Creating Incremental VM Backup with Quick Backup

Creating Full VM Backup with VeeamZIP

You can use Veeam Plug-in for VMware vSphere Client to create an ad-hoc VeeamZIP backup of a VM. For more information on VeeamZIP, see the VeeamZIP section of the Veeam Backup & Replication User Guide.

Configuring VeeamZIP Settings

Before you create a full VM backup with VeeamZIP, you need to configure VeeamZIP settings. The specified configuration is stored for the user account in your browser settings.

To configure the VeeamZIP settings, do the following:

1. In VMware vSphere Client, open the vCenter Server inventory.
2. In the inventory tree, select a VM.
3. On the **Configure** tab, select **Veeam Plug-in for VMware vSphere Client** > **VeeamZIP**.

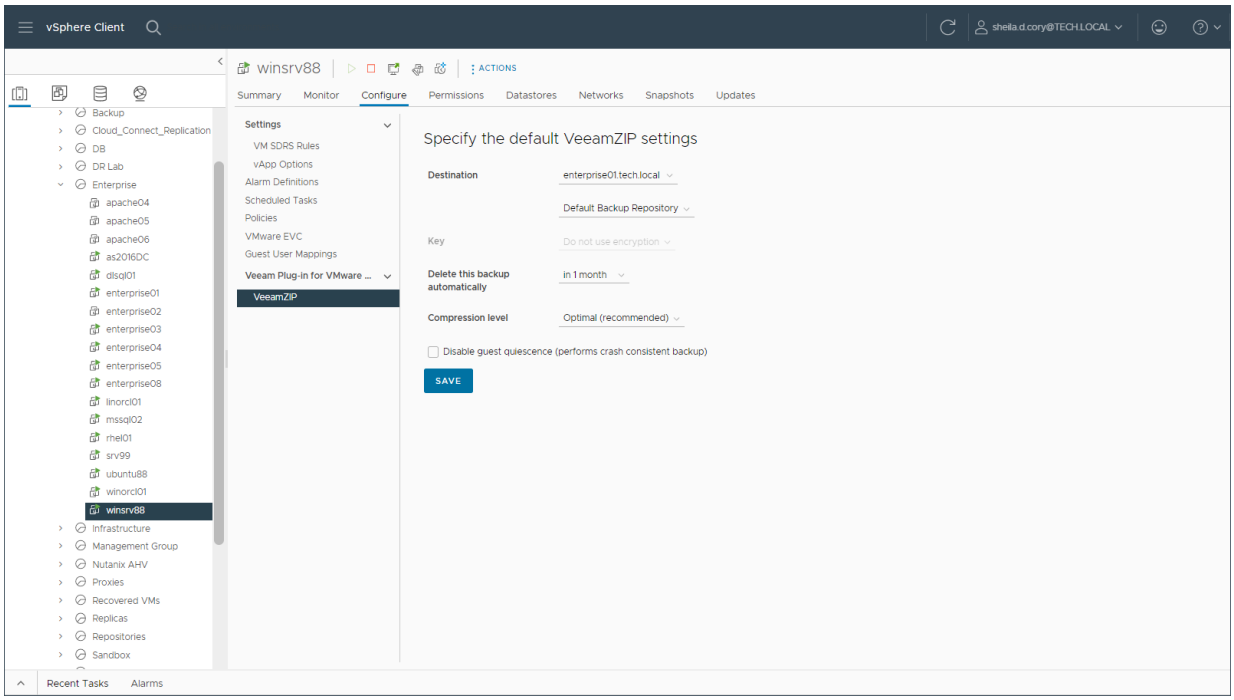
   Alternatively, you can right-click the VM and select **Veeam Web Client plug-in** > **VeeamZIP**.
4. In the **Destination** section, select the Veeam backup server that will process the VM and the repository where to store the VeeamZIP file.

   The plug-in displays Veeam backup servers added to the Veeam Backup Enterprise Manager infrastructure and backup repositories created in the backup infrastructure of these backup servers.
5. In the **Key** section, specify the encryption key if necessary.
6. In the **Delete this backup automatically** section, specify whether the resulting backup file should be automatically deleted after a certain time interval.
7. In the **Compression level** section, select the necessary compression level for the backup.
8. By default, the **Disable guest quiescence** option is selected, meaning that guest OS quiescence is deactivated. If you want a crash-consistent backup, leave it that way.

   If you want, however, an application-consistent backup, then clear the **Disable guest quiescence** check box, and Veeam will create a transactionally consistent image of VMs using VMware Tools quiescence for guest OS.

   For more information about guest OS quiescence, see the VMware Tools Quiescence section of the Veeam Backup & Replication User Guide.

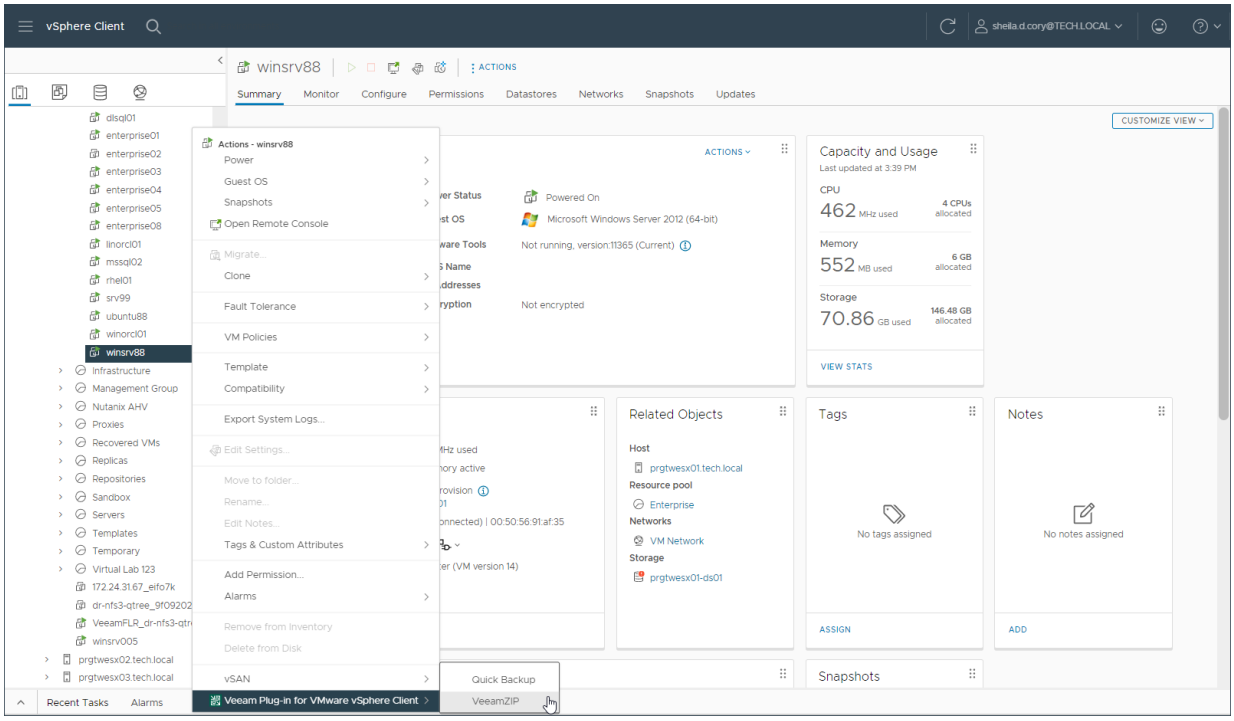
9. Click **Save**.



Creating Full VM Backup with VeeamZIP

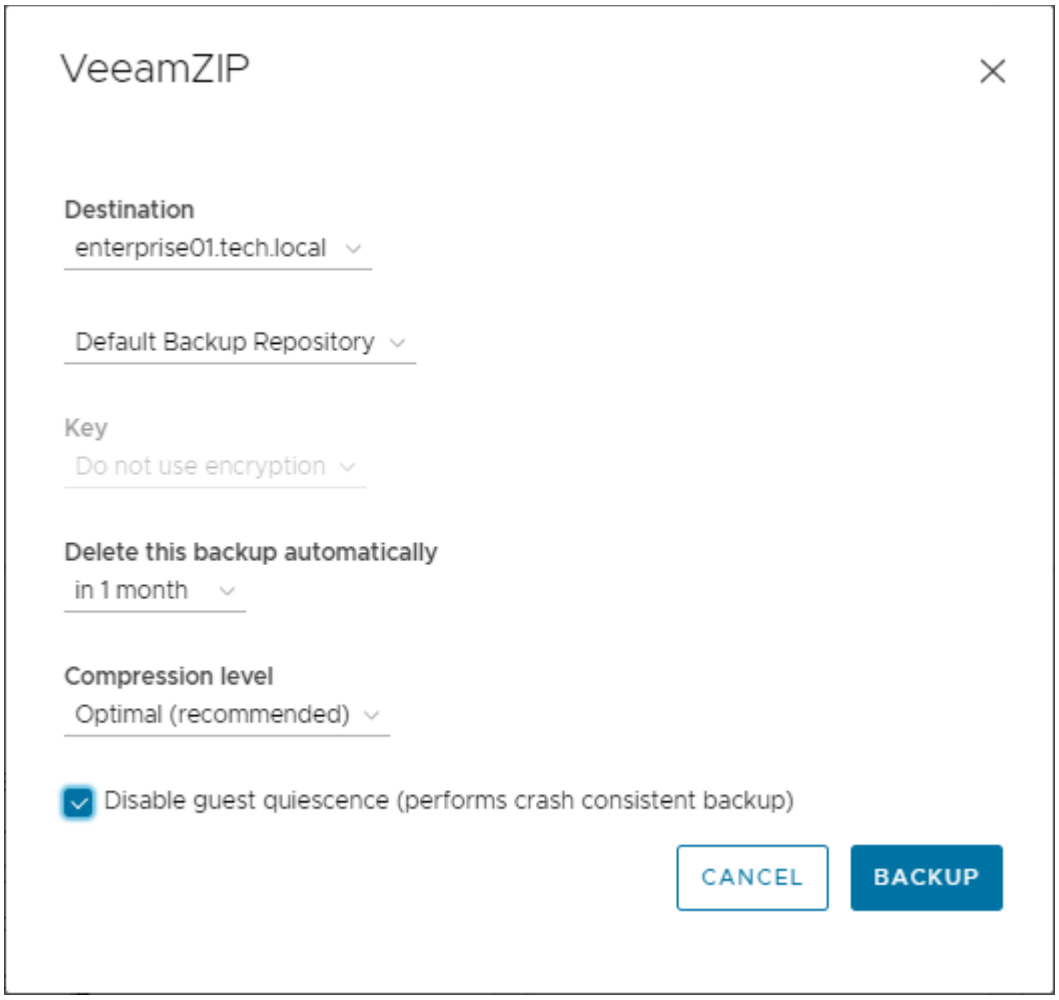
To create a full VM backup with VeeamZIP, do the following:

1. In vSphere Client, the vCenter Server inventory.
2. In the inventory tree, right-click the VM that you want to back up and select **Veeam Web Client plug-in** > **VeeamZIP**.



3. If you have already configured VeeamZIP settings, review the settings and click **Backup**.

   If you have not configured VeeamZIP settings, specify the settings in the **VeeamZIP** window in the same way as described in the Configuring VeeamZIP Settings.



You can view the backup creation progress in the **Recent Tasks** pane of vSphere Client.

> **NOTE**
>
> A VeeamZIP job fails to start if the *Location* property of the VM and backup repository do not match — for example, if you try to use a repository with location set to Sydney to back up a VM with location set to Helsinki. To read more about location settings, refer to the Veeam Backup & Replication User Guide.

Creating Incremental VM Backup with Quick Backup

You can use Veeam Plug-in for VMware vSphere Client to create a quick backup for the selected VM. For more information on quick backup, see the Quick Backup section of the Veeam Backup & Replication User Guide.

You can perform quick backup for any VM that meets the following requirements:

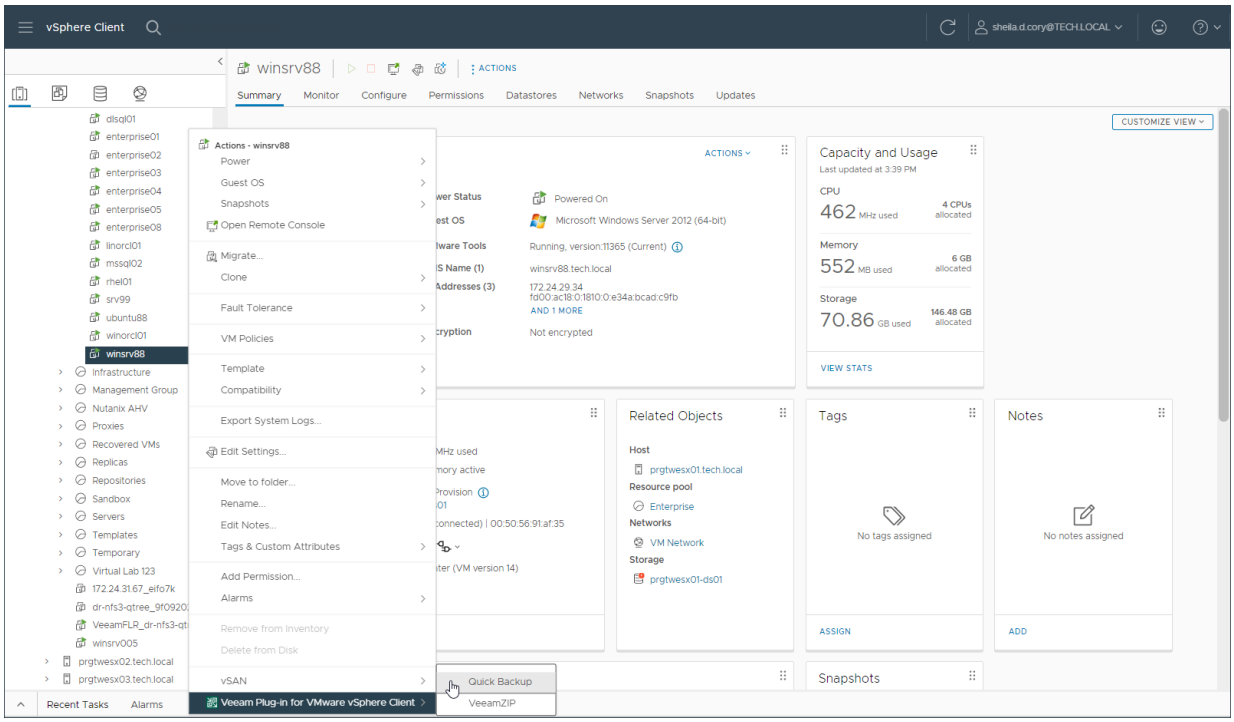
- A backup job processing the VM exists on the backup server that is added to Veeam Backup Enterprise Manager.
- There is a full backup file for this VM in the backup repository.

To perform quick backup, do the following:

1. In VMware vSphere Client, open the vCenter Server inventory.
2. In the inventory tree, select a VM.
3. Right-click the VM and select **Veeam Plug-in for VMware vSphere Client** > **Quick Backup**.

This will trigger a backup job processing the selected VM to create a new incremental restore point (VIB file) for the latest full backup found in the repository for this VM. Details of a running quick backup task can be seen in the **Recent Tasks** pane on the right.

> **NOTE**
>
> A quick backup job fails to start if the *Location* property of the VM and backup repository do not match — for example, if you try to use a repository with location set to Sydney to back up a VM with location set to Helsinki. To read more about location settings, refer to the Veeam Backup & Replication User Guide.



Veeam Self-Service Backup Portal for Cloud Director

Veeam Backup Enterprise Manager allows you to perform the following operations with VMware Cloud Director objects:

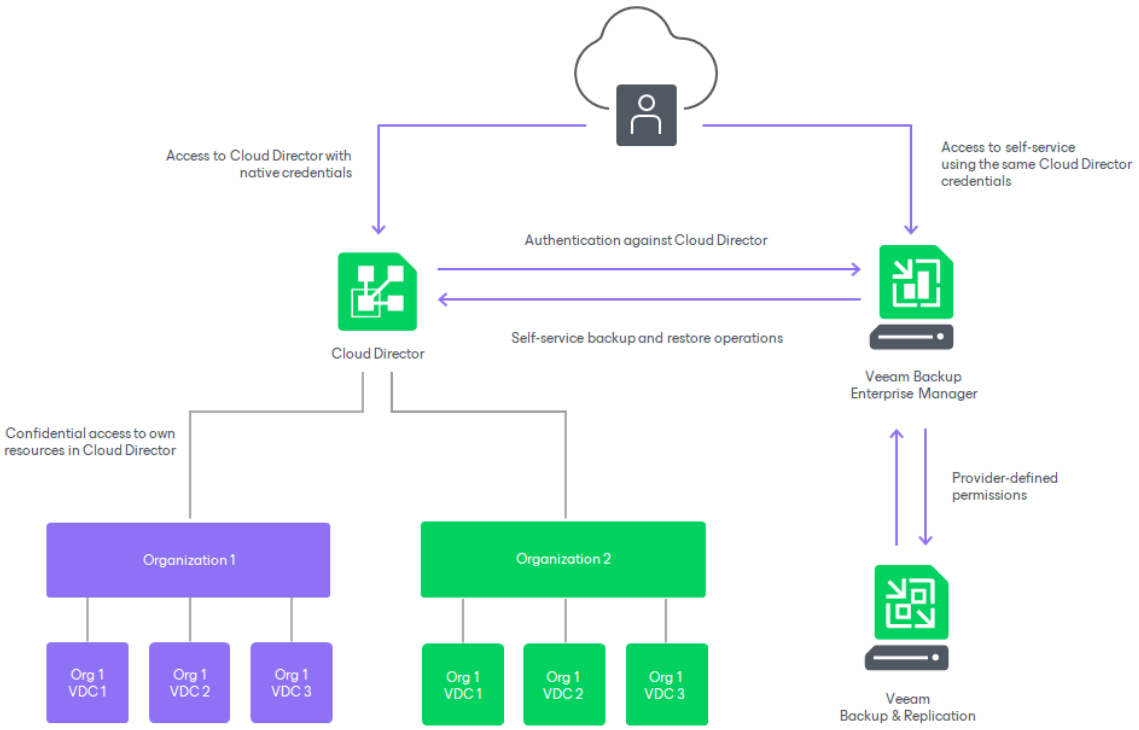
- Back up VMs, vApps and other containers
- Restore VMs and vApps
- Restore VM guest OS files

Cloud Director service providers can allow their customers to perform self-service restore operations in the web UI based on Veeam Backup Enterprise Manager.

- Service provider administrators have administrative rights in Veeam Backup Enterprise Manager. Thus, they have access to the **Configuration** view of Enterprise Manager where they can create Cloud Director organization configurations, including repository quota and backup job template. These administrators typically have access to Veeam Backup & Replication console that controls VMware Cloud Director as part of backup infrastructure on the provider side.
- Members of Cloud Director organizations do not need administrative rights for Veeam Backup Enterprise Manager — instead, they get access to Veeam Self-Service Backup Portal. There they can manage their Cloud Director jobs, as well as restore VMs, files and application items within their scope.

How It Works

Veeam Backup Enterprise Manager uses native VMware Cloud Director authentication to authorize users that log in to Enterprise Manager. The authentication process and components interactions are shown in the figure below.



This approach helps to streamline administration and management tasks for service providers, as now they need to configure a tenant account only once in VMware Cloud Director, and then any change like a new password or a disable operation will be immediately reflected in Veeam Backup Enterprise Manager.

What Service Provider Administrators Can Do

Service provider administrators can perform the following operations when adding or editing organization configurations:

- Configure settings for their tenants (Cloud Director organizations), including backup job templates to be used, backup destination, and repository quota.
- Restrict job scheduling for particular tenants, for example, prevent the jobs from running too often. Administrators can even prohibit the tenant's ability to schedule jobs completely, instead setting the required schedule themselves (manually or using a script).

For more information, see Adding Organization Configuration.

These capabilities and the built-in load balancing allow administrators to ensure infrastructure is protected from excessive resource consumption.

What Members of Cloud Director Organizations Can Do

Members of Cloud Director organizations can use their Cloud Director credentials to access Veeam Self-Service Backup Portal. Once they log in, Enterprise Manager identifies the resources included in their scope — the entities the user is allowed to see and manage — and automatically filters Cloud Director objects when displaying them.

Members of Cloud Director organizations can perform the following operations:

- Create new backup jobs for objects in their scope, based on the predefined templates. Organization members are allowed to configure essential job settings (such as VMs to back up, retention, schedule, notifications, and guest OS processing options).
- Modify or delete jobs.
- Enable or disable jobs.
- Start, stop, retry jobs.
- View statistics on Cloud Director backups.
- Restore Cloud Director VMs to the original vApps and vApps to the original VDC.
- Perform application item restore for SQL Server and Oracle databases.
- Restore files from indexed and non-indexed VMs guest file system.

To simplify job management for tenants, advanced job parameters (like backup mode and repository settings) are automatically populated from the job templates. These templates are assigned by the service provider administrator to the particular organization.

In This Section

- Managing Configurations for Cloud Director Organizations
- Configuring Veeam Self-Service Backup Portal UI
- Using Veeam Self-Service Backup Portal

Managing Configurations for Cloud Director Organizations

In Veeam Backup Enterprise Manager, users with the Portal Administrator role can manage configurations for VMware Cloud Director organizations. Each configuration defines a backup repository that can be used by the organization, repository quota and backup job settings. To specify multiple repositories per organization, add a separate configuration for each repository.

Before you manage Cloud Director organization configurations, check prerequisites.

You can perform the following operations with Cloud Director organizations:

- View the list of organization configurations
- Add a new configuration for a Cloud Director organization
- Edit a Cloud Director organization configuration
- Remove a Cloud Director organization configuration
- Export a configuration report

Before You Begin

You can add configurations for VMware Cloud Director organizations created on multiple VMware Cloud Director servers that are added to the Veeam Backup Enterprise Manager infrastructure.

Before you manage Cloud Director organization configurations, check the following prerequisites:

1. The Cloud Director server version must be supported. For more information, see System Requirements.
2. All Cloud Director servers must be added to the backup infrastructure of backup servers. For more information, see the Adding VMware Cloud Director section of the Veeam Backup & Replication User Guide.
3. Backup servers that contain the Cloud Director servers in their infrastructure must be connected to Enterprise Manager. Make sure that the version of Veeam Backup & Replication installed on the backup server matches the version of Enterprise Manager. For more information, see Managing Backup Servers.
4. Enterprise Manager must complete data collection from the added backup server. For more information, see Collecting Data from Backup Servers.
5. The account that you will use to manage Cloud Director organization configurations must be assigned the Portal Administrator role. For more information, see Configuring Accounts and Roles.

Managing Multiple Cloud Director Servers

You can add Cloud Director organization configurations for multiple Cloud Director servers. In this case, organization members that work with Veeam Self-Service Backup Portal by the portal URL must specify the host of their Cloud Director server when accessing the portal. They can also open the portal from the native VMware Cloud Director environment. For more information, see Accessing Veeam Self-Service Backup Portal.

Members of Cloud Director organizations can access Veeam Self-Service Backup Portal by the following portal URLs:

- Full URL that contains the host address where the necessary Cloud Director server resides:

  ```
  https://<EnterpriseManagerServer>/vcloud/<VCDServer>/<OrgName>
  ```

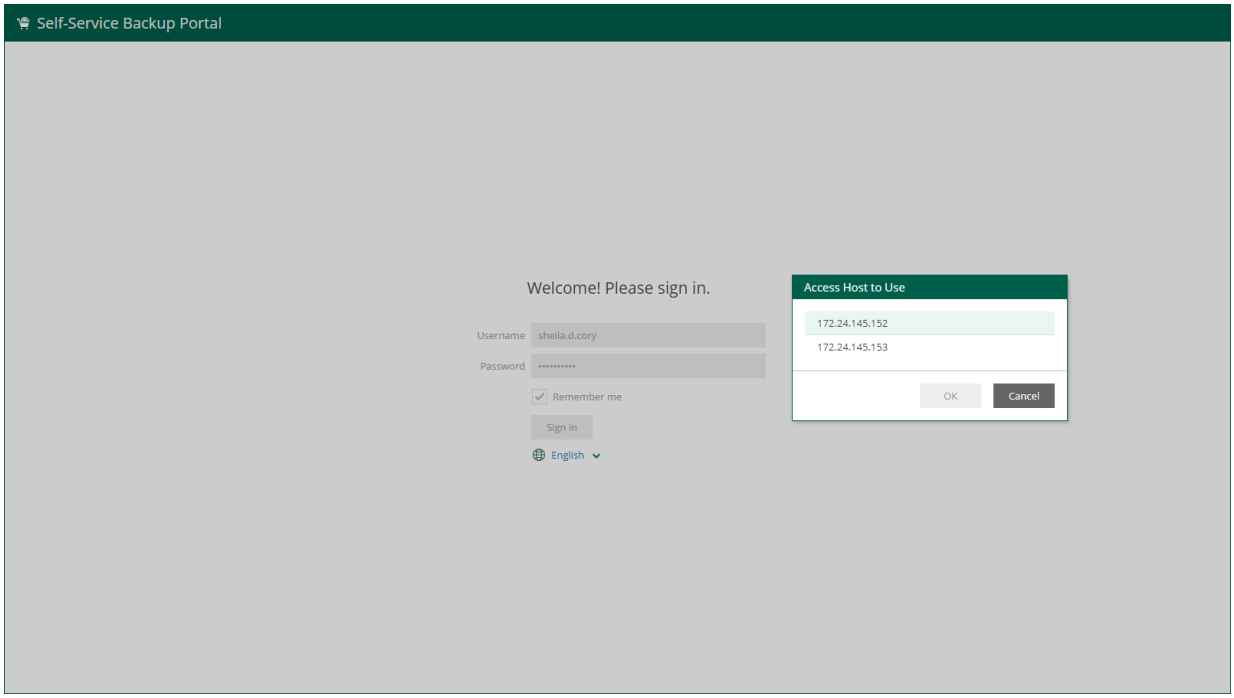
  In this case, Veeam Self-Service Backup Portal will open right after clicking the **Sign in** button.

- Shorter URL that does not contain the host address where the necessary Cloud Director server resides:

  ```
  https://<EnterpriseManagerServer>/vcloud/<OrgName>
  ```

  In this case, after clicking the **Sign in** button, Veeam Self-Service Backup Portal will prompt to select a Cloud Director host from the list of available Cloud Director hosts.

If you do not want Cloud Director organization members to see addresses of all Cloud Director hosts added to the Enterprise Manager infrastructure, add each Cloud Director server to a separate Enterprise Manager infrastructure.



About Organization Quota

When setting up an organization configuration, you specify a repository storage quota for the organization. This quota defines the amount of data that the backup jobs associated with the organization can send to the dedicated backup repository or scale-out backup repository.

When calculating used quota, Veeam Backup Enterprise Manager takes into account data compression and deduplication performed by Veeam Backup & Replication. However, 3rd party compression and deduplication performed after the data is transferred to the repository (for example, by ReFS and XFS file systems or by cloud services) do not affect on the used quota calculation.

The used quota is recalculated each time a job associated with the organization runs. If you manually remove backup files from a backup repository, or if backup files are removed automatically according to a retention policy, the used quota is recalculated after any job associated with the organization completes.

> **NOTE**
>
> Replication jobs and CDP policies do not consume storage quota of backup repositories because replicas are stored on the target VMware Cloud Director VDC. If you want to set a quota for replicas, configure storage policies of the target VDC.

Managing Backups and Used Quota

If you want to protect backups created by organizations, you can create backup copy jobs on your backup server. The size of backup files copied by backup copy jobs is not included in the used quota calculation. For more information about backup copy jobs, see the Backup Copy section of the Veeam Backup & Replication User Guide.

You can also manually copy or move an organization backup from one backup repository to another. You may need to move some backups to another repository, for example, if the quota limit of one of the organization repositories is reaching. When you copy or move a backup to another repository, the used quota will be recalculated. For more information on copying and moving backups, see the Copying Backups and Moving Backups sections of the Veeam Backup & Replication User Guide. Before you copy or move an organization backup, make sure that the organization has access to the target repository. To provide the access, add a new organization configuration for this repository. For details, see Adding Organization Configuration.

For organizations whose backups are stored on a scale-out backup repository, the portal shows quota consumption broken down by repository tier. The total used quota is the sum of the data stored on the performance tier, the capacity tier, and the archive tier:

- Performance tier — backup data currently residing on the performance extents (the total consumption minus any data that has been moved to the capacity or archive tiers).
- Capacity tier — backup data stored on the capacity extent.
- Archive tier — backup data stored on the archive extent.

Any data compression and deduplication performed on a target capacity or archive extent does not influence used quota calculation. To learn more about scale-out backup repositories, see the Scale-Out Backup Repositories section of the Veeam Backup & Replication User Guide.

Viewing Organization Configurations

In Veeam Backup Enterprise Manager, users with the Portal Administrator role can view the list of configurations for VMware Cloud Director organizations.

To view the list of organization configurations:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.

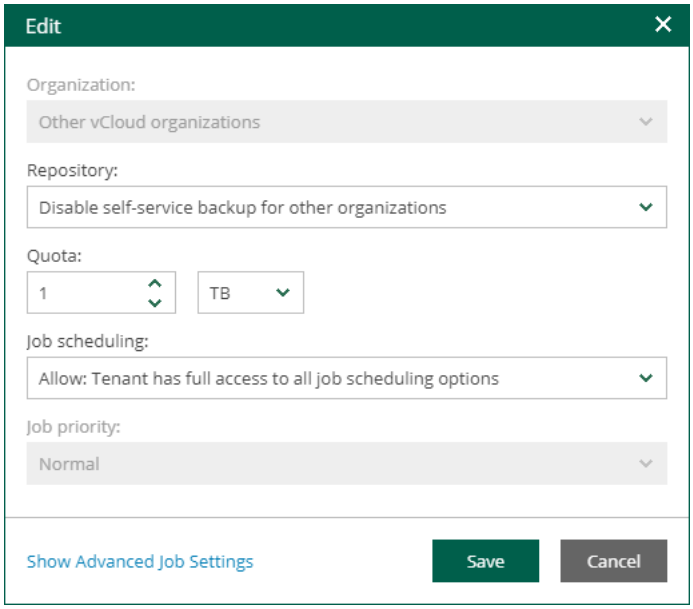
Veeam Backup Enterprise Manager offers a default configuration that you can use for Cloud Director organizations. The configuration is applied to each organization that does not have a specific configuration added for it.

The default configuration contains the following parameters:

- **Organization** – *Other VMware Cloud Director organizations*
- **Repository** – *Disable self-service backup for other organizations*

  Initially the default configuration is not active. To enable it, select a repository for the configuration.
- **Quota** – *1 TB*
- **Job scheduling** – *Allow: Tenant has full access to all job scheduling*
- **Job priority** – *Normal*

For more information on configuration parameters, see Adding Organization Configuration.



Adding Organization Configuration

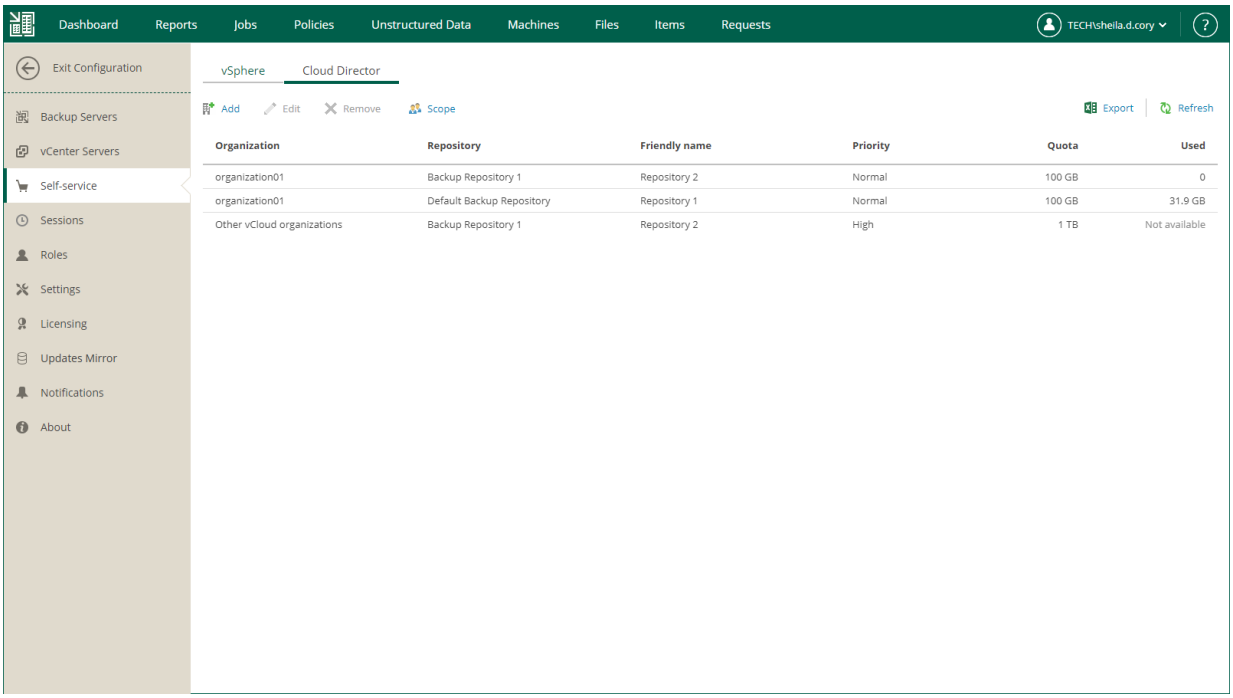
Users with the Portal Administrator role can add a new configuration for a VMware Cloud Director organization. Each configuration defines a backup repository that can be used by the organization, repository quota and backup job settings.

You can specify multiple repositories per organization. In this case, users of Veeam Self-Service Backup Portal will be able to select a backup repository when configuring their jobs. For details, see Creating Jobs. To specify multiple repositories per organization, add a separate configuration for each repository.

Before you add a new configuration, check prerequisites.

To add a new organization configuration:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.



5. To add a new configuration, click **Add**.
6. From the **VMware Cloud Director server** drop-down list, select a VMware Cloud Director server you need.

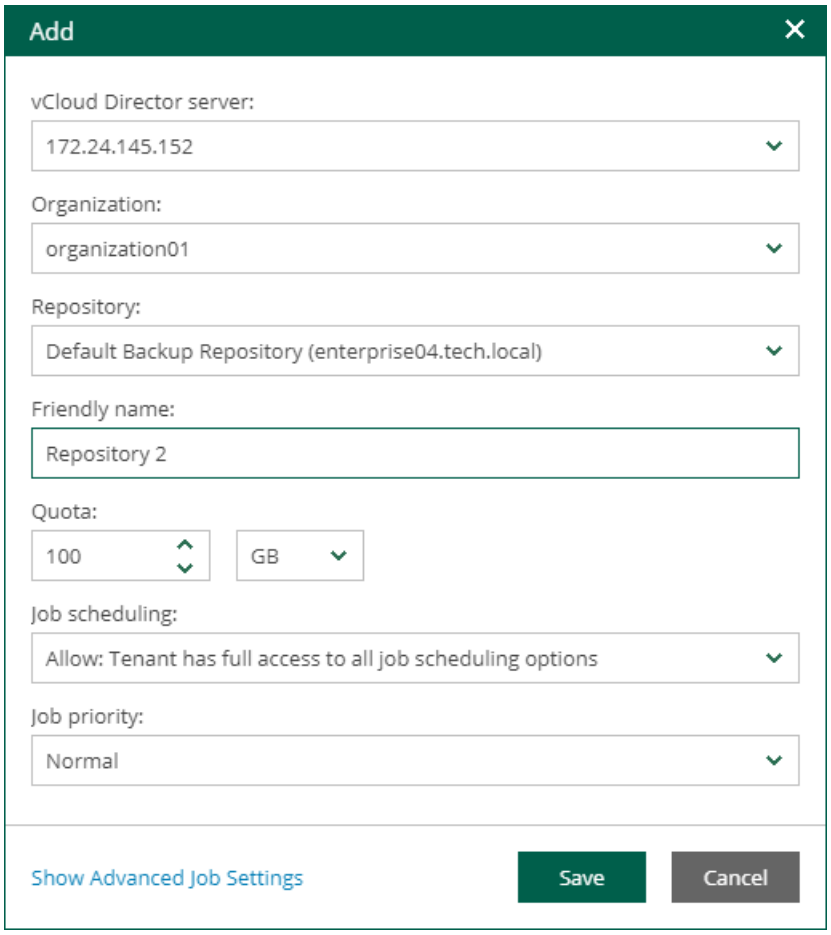
   The field is available if you have multiple Cloud Director servers in the Enterprise Manager infrastructure.
7. From the **Organization** drop-down list, select an organization you need. The list contains organizations from the selected Cloud Director server processed by the backup server that is added to Enterprise Manager.
8. From the **Repository** drop-down list, select a repository that will be used for backups. The list includes repositories configured on backup servers that has a Cloud Director server added to its infrastructure.

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

9. In the **Friendly name** field, specify a repository name that will be displayed to organization members.
10. In the **Quota** section, specify a repository storage quota. You can choose GB or TB from the drop-down list and enter the required quantity. For details on the quota usage see About Organization Quota.
11. From the **Job scheduling** drop-down list, select one of the following options:
    a. *Allow: Tenant has full access to all job scheduling options*
    b. *Allow: Tenant can create daily and monthly jobs only*
    c. *Deny: Creates daily jobs with randomized start time within the backup window*

       For backup jobs of Cloud Director organizations, the backup window settings are specified in Veeam Backup Enterprise Manager. Backup window settings specified for the job template that you will select from the advanced job settings do not affect organization jobs. For information on how to specify the backup window in Veeam Backup Enterprise Manager, see Customizing Dashboard Chart.
    d. *Deny: Creates job with no schedule assigned*

    For more information on job scheduling, see Edit Job Schedule.



12. Specify advanced settings for backup jobs of the Cloud Director organization.
    a. Click the **Show Advanced Job Settings** link.

b. In the **Advanced job settings** section, view the currently used backup job settings.

c. From the **Copy from** list, select the advanced settings that you want to apply to backup jobs of the Cloud Director organization. For more information on the specific settings, see the Specify Advanced Backup Settings section of the Veeam Backup & Replication User Guide.

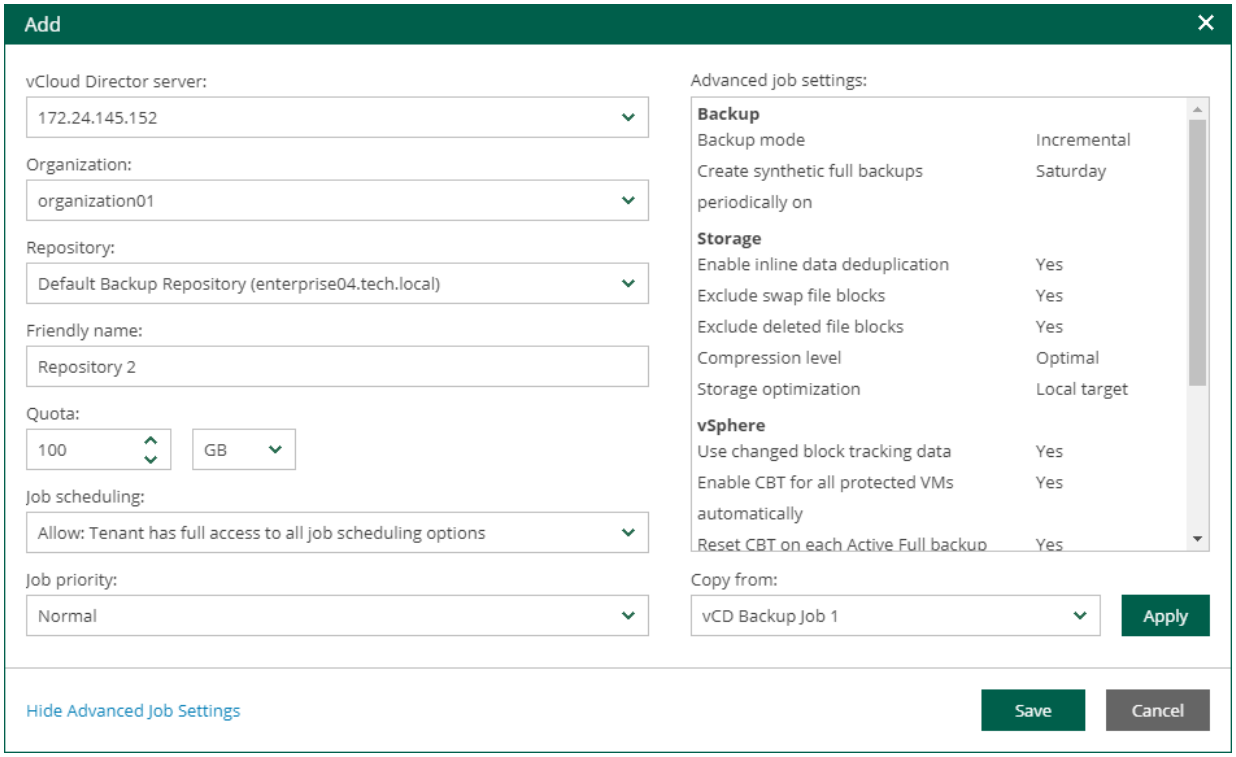
- Select *Default settings* to use the default advanced settings as they are shown in the Veeam Backup & Replication console. This option is applied by default.
- Select *<Job name>* to use the advanced settings of an existing backup job as a template. When an organization member creates a backup job on the Veeam Self-Service Backup Portal, Enterprise Manager will copy the advanced settings from the template and apply them to the job.

  Note that, in the **Copy from** list, Enterprise Manager displays only VMware Cloud Director backup jobs that are configured in advance on the backup server added to Enterprise Manager.

d. To apply the job template, click **Apply**.

> **IMPORTANT**
>
> The backup repository that is selected from the **Repository** drop-down list for the organization takes priority over the repository used by the selected job template.

13. To save the configuration, click **Save**.



Mapping Jobs and CDP Policies to Organization Configurations

Service providers can map backup jobs, replication jobs, and CDP policies created in Veeam Backup & Replication to the organization configurations of their tenants. You can map jobs and policies configured on any backup server added to Enterprise Manager. After mapping, tenants can manage jobs and policies and perform recovery operations independently in Veeam Self-Service Backup Portal.

> **NOTE**
>
> Tenants can create their own backup jobs in Veeam Self-Service Backup Portal. However, if a tenant wants to manage replication jobs and CDP policies in the portal, the service provider must create them and map to the tenant organization configuration.

To map a CDP policy to an organization, take the following steps:

1. In Enterprise Manager, create organization configurations for your tenants. For details, see Adding Organization Configuration.
2. In Veeam Backup & Replication, create jobs or CDP policies for your tenants. Ensure that each job (or policy) includes only the objects that belong to a particular Cloud Director organization. Otherwise, you will not be able to map the job.

   For backup and replication jobs, you can include any objects from the organization, and your tenant can edit the job later. Editing of CDP policies is not available in Veeam Self-Service Backup Portal.
3. To map the created jobs and policies to the organization configuration, use the Set-VBRvCloudOrganizationJobMapping cmdlet.

   You can also use this cmdlet to unmap jobs and policies from an organization configuration.

Editing Organization Configuration

Users with the Portal Administrator role can edit VMware Cloud Director organization configurations.

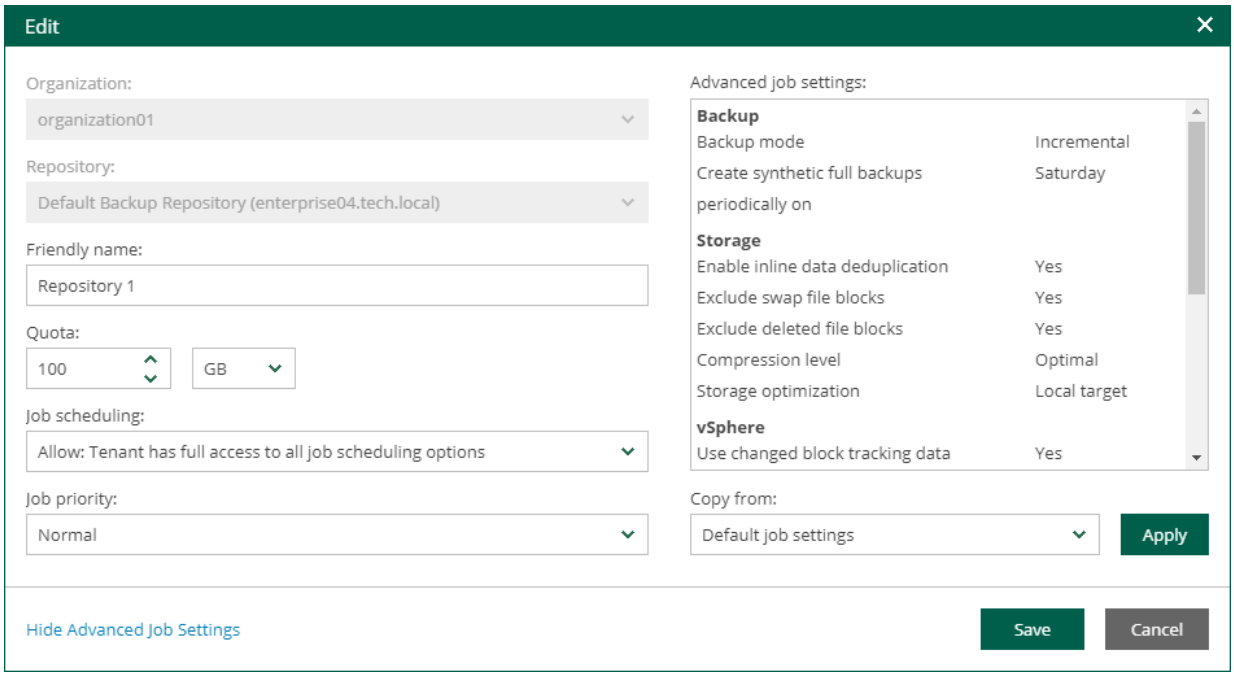
Before you edit a configuration, consider the following recommendations:

- When you change a job template for a Cloud Director organization, the new configuration will be applied only to the new jobs, existing jobs will not be affected.
- To make an existing backup job save backups to another repository instead of the currently configured for a specific organization, take the following steps:
  a. Add a new configuration for this organization. In the configuration settings, specify the new repository that you want to move backups to. For details, see Adding Organization Configuration.
  b. In the Veeam Backup & Replication console, change the current repository to the new one for each backup job. When you specify a new repository, Veeam Backup & Replication prompts you to move the existing backups to the new repository or keep them on the current one. For details, see the Specify Backup Storage Settings and Backup Move sections of the Veeam Backup & Replication User Guide.

To edit an organization configuration, do the following:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.
5. On the **Cloud Director** tab, select an organization configuration and click **Edit**.
6. To edit organization settings, follow the same steps as for adding a configuration.

   For more information, see Adding Organization Configuration.



Removing Organization Configuration

Users with the Portal Administrator role can remove VMware Cloud Director organization configurations.

After you remove a configuration, the backup files created by existing backup jobs will remain in the backup repository. The backup jobs associated with this configuration will also remain but will fail to run because the backup repository will not be available to the organization. If you add a new configuration with the same backup repository for this organization, the organization's backup jobs will continue existing backup chains.

If you want to replace an organization configuration with the one that uses a different backup repository and and you want to keep all created backup chains, create the new configuration first, move backups to the new repository, and then remove the unnecessary organization configuration. For details, see About Organization Quota.

To remove an organization configuration, do the following:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.
5. On the **Cloud Director** tab, select a configuration and click **Remove**.
6. To confirm the removal, click **Yes**.

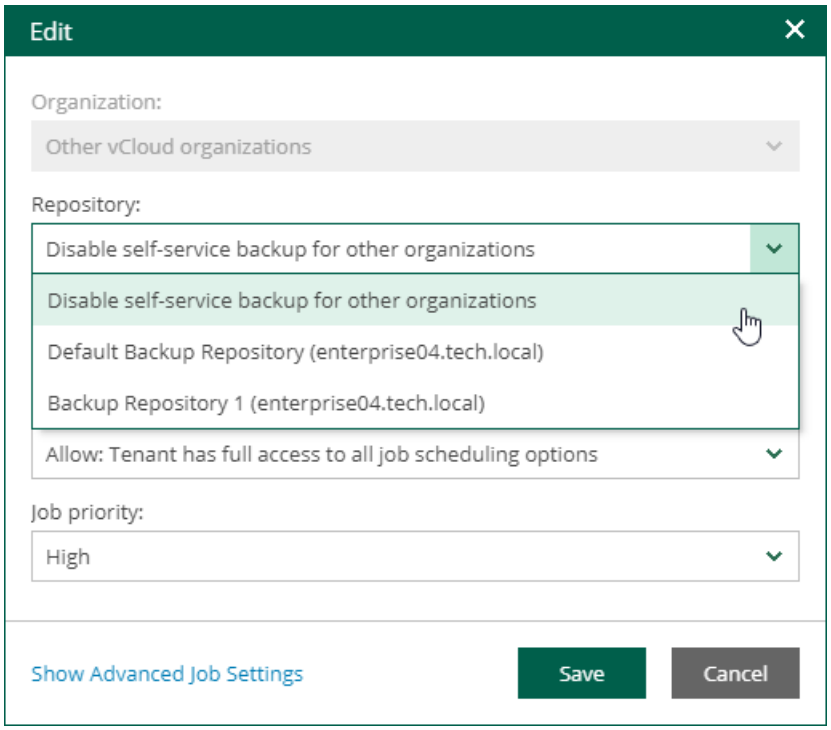
Disabling Default Configuration

The default configuration cannot be removed from the list — instead, you can disable it.

To disable the default configuration:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.
5. On the **Cloud Director** tab, select the default organization configuration and click **Edit**.

6. From the **Repository** drop-down list, select *Disable self-service backup for other organizations*.



Exporting Configuration Report

Users with the Portal Administrator role can export a report with a list of configurations that were created for VMware Cloud Director organizations. The list does not include the default configuration. When you export the report, it is saved as an XLSX file.

To export a configuration report:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.
5. On the **Cloud Director** tab, click **Export**.

	A	B	C	D	E
1	**Organization**	**Repository**	**Used space**	**Quota**	
2	organization01	Backup Repository 1	0	100 GB	
3	organization01	Default Backup Repository	31.9 GB	100 GB	
4					
5					
6					

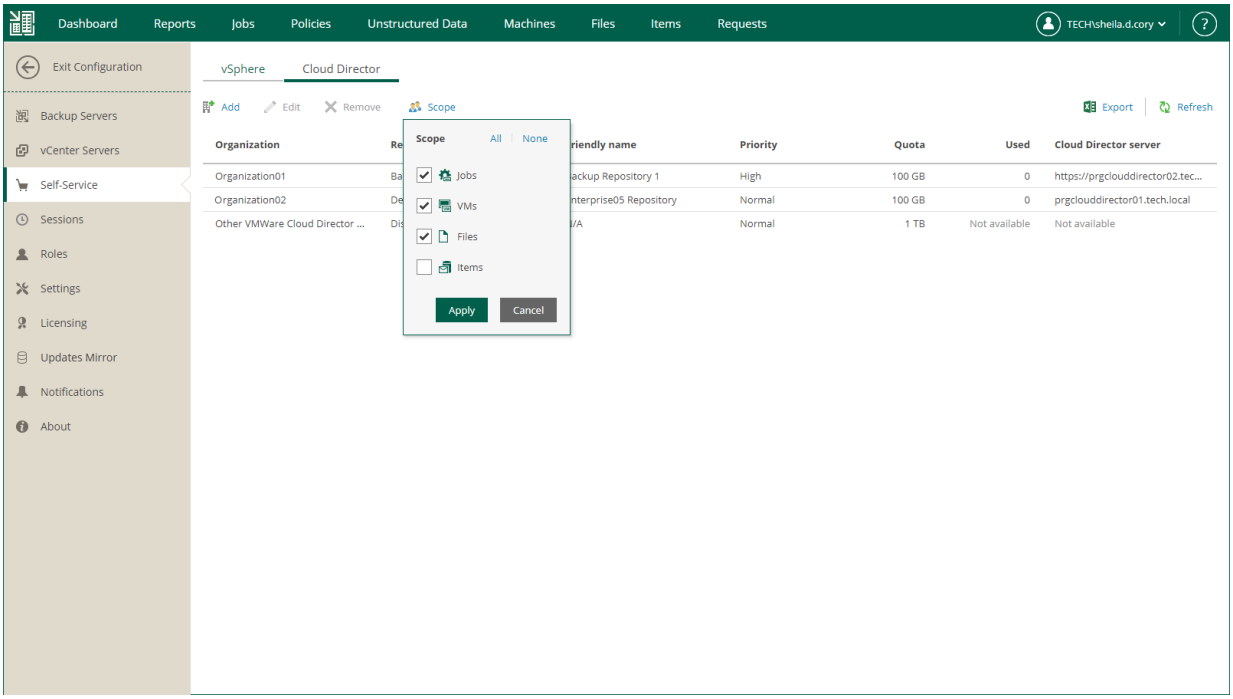
Configuring Veeam Self-Service Backup Portal UI

Users with the Portal Administrator role can configure what operations are available for portal users by choosing the tabs that must displayed in Veeam Self-Service Backup Portal. By default, all portal tabs are displayed. The **Dashboard** tab is always available in the portal. You can change visibility of the following portal tabs:

- Jobs
- VMs
- Files
- Items

To change visibility of Veeam Self-Service Backup Portal tabs, do the following:

1. Log in to Veeam Backup Enterprise Manager using an administrative account.
2. Click **Configuration** in the upper-right corner.
3. In the **Configuration** view, select the **Self-service** section.
4. In the **Self-service** section, select the **Cloud Director** tab.
5. Click **Scope** and select the tabs that you want to be displayed.
6. To save the settings, click **Apply**.



Using Veeam Self-Service Backup Portal

Veeam Self-Service Backup Portal is a web-based portal that provides members of VMware Cloud Director organizations with self-service operations for Cloud Director VMs protection, including VM and file restore. These operations do not require to create specific user accounts or assign specific roles to them at the Veeam Backup Enterprise Manager level. The organization members access Veeam Self-Service Backup Portal with their native Cloud Director credentials.

In This Section

- Access Control
- Accessing Veeam Self-Service Backup Portal
- Working with Veeam Self-Service Backup Portal

Access Control

Members of VMware Cloud Director organizations can use Veeam Self-Service Backup Portal to back up and restore resources of their organizations.

The following organization members have access to Veeam Self-Service Backup Portal:

- Cloud Director organization administrator
- Cloud Director organization member that has all of the following rights granted in VMware Cloud Director:
  - *General: Administrator Control*
  - *General: Administrator View*
  - *User: View Users and Groups*
  - *Organization: View Organization Administrative Details* (required for access using Veeam Plug-in for VMware Cloud Director only)
- Any Cloud Director organization members whose roles (or associated LDAP user roles) are defined in registry keys and with the *Group / User: View* right granted in VMware Cloud Director. For more information, contact Veeam Customer Support.

For details on how to access the portal, see Accessing Veeam Self-Service Backup Portal.

> **NOTE**
>
> Cloud Director system administrators cannot access Veeam Self-Service Backup Portal since they are not organization members.

Accessing Veeam Self-Service Backup Portal

Members of VMware Cloud Director organizations can access Veeam Self-Service Backup Portal in the following ways:

- Access by URL
- Access from Cloud Director

For details on required user access rights, see Access Control.

Supported Authentication Types

Veeam Self-Service Backup Portal supports the following types of user authentication:

- Cloud Director local users
- LDAP authentication

Accessing Veeam Self-Service Backup Portal by URL

To access Veeam Self-Service Backup Portal by URL:

1. Open your web browser and enter the following URL in the address bar:

   ```
   https://<EnterpriseManagerServer>/vcloud/<OrgName>/<VCDServer>
   ```

   where:

   - `<EnterpriseManagerServer>` is a host name or IP address of the host where the Enterprise Manager server resides.
   - `<OrgName>` is a name of the Cloud Director organization.
   - `<VCDServer>` is a host name or IP address of the host where the Cloud Director server resides.

     This URL part is optional. If you do not specify a Cloud Director host here, you may be asked to select the host when you log in to the portal.

   For example:

   ```
   https://enterprise01.tech.local/vcloud/organization01/172.17.53.16
   ```

2. From the drop-down list, select a display language.

   For more information on display languages, see Managing Languages.

3. In the **Username** and **Password** fields, specify credentials of a Cloud Director account with proper rights. If you use LDAP authentication, enter the user name in the following format: `organization\user` (for example, `organization01\username@domain`).

4. To save the entered credentials for future access, select the **Remember me** check box.

5. Click **Sign in**.
6. From the list of hosts with Cloud Director servers, select the one where your organization has been created.

   The list of hosts is displayed if multiple Cloud Director servers are added to the Enterprise Manager infrastructure.

Accessing Veeam Self-Service Backup Portal from VMware Cloud Director

In the VMware Cloud Director environment, Veeam Self-Service Backup Portal is displayed in English by default. When you access the portal by its URL, you can select a preferred language from the drop-down list on the login page. After you select the language here, you can work with the portal in the selected language from the VMware Cloud Director environment. For more information, see Accessing Veeam Self-Service Backup Portal by URL.

Before members of Cloud Director organizations can access Veeam Self-Service Backup Portal from the Cloud Director UI, the Cloud Director system administrator must upload and configure Veeam Plug-in for VMware Cloud Director. For more information, see Veeam Plug-in for VMware Cloud Director.

To access Veeam Self-Service Backup Portal from Cloud Director:

1. Log in to VMware Cloud Director Tenant Portal under a Cloud Director account with proper rights.
2. From the **More** menu, select **Data Protection with Veeam**.

   If you have a connection error when accessing Veeam Plug-in for VMware Cloud Director, add the Veeam Backup Enterprise Manager certificate as trusted to your browser.

Veeam Plug-in for VMware Cloud Director

Veeam Plug-in for VMware Cloud Director lets members of VMware Cloud Director organizations access Veeam Self-Service Backup Portal from the native VMware Cloud Director environment.

You can upload and configure the plug-in in VMware Cloud Director Service Provider Admin Portal. When you upload the plug-in, you specify the scope — a set of Cloud Director organizations that can use the plug-in.

If you need to modify the scope of Cloud Director organizations after you configure the plug-in, update the plug-in configuration. For more information, see Updating Plug-in Configuration.

> **IMPORTANT**
>
> In VMware Cloud Director Service Provider Admin Portal, you cannot upgrade plug-ins. To switch to a newer version of Veeam Plug-in for VMware Cloud Director, delete the current plug-in version and then upload a newer one. For more information on deleting the plug-in, see the Delete a Plug-in From Your VMware Cloud Director section of the VMware Cloud Director documentation. For details on uploading the plug-in, see Uploading and Configuring Plug-in.
>
> Before you delete the plug-in, make a note of the Cloud Director organizations that are allowed to use the plug-in. For more information on how to view them, see the Publish or Unpublish a Plug-in from a VMware Cloud Director Organization section of the VMware Cloud Director documentation.

Before You Begin

Before you start uploading Veeam Plug-in for VMware Cloud Director, check the following prerequisites:

- Members of Cloud Director organizations using the plug-in must have network access to the Cloud Director server and Veeam Backup Enterprise Manager server.

  You specify the Veeam Backup Enterprise Manager server URL in Cloud Director Service Provider Admin Portal when you configure the plug-in. For more information, see Uploading and Configuring Plug-in.

- The Veeam Backup Enterprise Manager server should use a certificate issued by a Certificate Authority instead of a default self-signed certificate. In case of a self-signed certificate, users of the plug-in have to add the Enterprise Manager certificate as trusted to their browser before they access the plug-in. Otherwise, they will get a connection error.

  For more information on the Enterprise Manager certificate, see Installing Certificates.

Uploading and Configuring Plug-in

To upload and configure Veeam Plug-in for VMware Cloud Director, follow these steps:

1. Log in to VMware Cloud Director Service Provider Admin Portal under a Cloud Director system administrator account.
2. Upload the `plugin.zip` file to the portal. You can download the file from the **Additional Downloads** section at veeam.com or my.veeam.com.

   For more information, see the Upload a Plug-in to Your VMware Cloud Director section of the VMware Cloud Director documentation.
3. From the **More** menu, select **Data Protection with Veeam**.

   If the **Data Protection with Veeam** option is not available, log out of the VMware Cloud Director Service Provider Admin Portal and log in again.
4. In the **Plug-in Configuration** section, specify the URL to the Veeam Backup Enterprise Manager server, for example: `https://hostname:443`.
5. Click **Save**.

   > **NOTE**
   >
   > When you save the plug-in configuration, it is applied to all Cloud Director organizations. For that, a separate operation is performed for each organization. If you have operation limits that are set through the VMware Cloud Director API, the operations may fail with HTTP status 400.
   >
   > In this case, use the VMware Cloud Director API to set the *QueuedOperationsPerOrg* and *QueuedOperationsPerUser* elements to zero until you save the plug-in configuration. For more information, see the OperationLimitsSettingsType section of VMware Cloud Director API documentation.

6. [For Microsoft Windows-based Enterprise Manager] On the Enterprise Manager server in IIS Manager, recycle the VeeamBackup application pool.

   For more information, see the Recycling Settings for an Application Pool <recycling> section of Microsoft Docs.

Updating Plug-in Configuration

After you configure the plug-in, you can modify the scope of Cloud Director organizations. It may be useful, for example, if you create a new Cloud Director organization and you want members of this organization to use the plug-in. To include or exclude Cloud Director organizations, update the plug-in configuration.

To update the plug-in configuration:

1. Log in to VMware Cloud Director Service Provider Admin Portal under a Cloud Director system administrator account.
2. Modify the scope of Cloud Director organizations.

   For more information, see the Publish or Unpublish a Plug-in from a VMware Cloud Director Organization section of the VMware Cloud Director documentation.
3. From the **More** menu, select **Data Protection with Veeam**.
4. In the **Plug-in Configuration** section, click **Save** to apply the changes to all Cloud Director organizations.

Working with Veeam Self-Service Backup Portal

In Veeam Self-Service Backup Portal, members of VMware Cloud Director organizations can perform the following operations:

- On the Dashboard tab — view statistics on Cloud Director backups.
- On the Jobs tab — examine and export job sessions data, search for jobs, create new jobs and edit jobs.
- On the VMs tab — search by a VM name, restore VMs and vApps to their original location (preserving or overwriting the production VM or vApp), and delete VM backups.
- On the Files tab — search for the files on the VM guest file system and restore the necessary files to the original location or download to the local machine.
- On the Items tab — perform application item-level restore (currently, for Microsoft SQL Server and Oracle databases).

> **NOTE**
>
> If the Veeam Backup Enterprise Manager server is added to the Veeam ONE monitoring scope, the restore operations performed with Veeam Self-Service Backup Portal are included in the Restore Operator Activity report available in Veeam ONE.

Viewing Statistics on Cloud Director Backups and Replicas

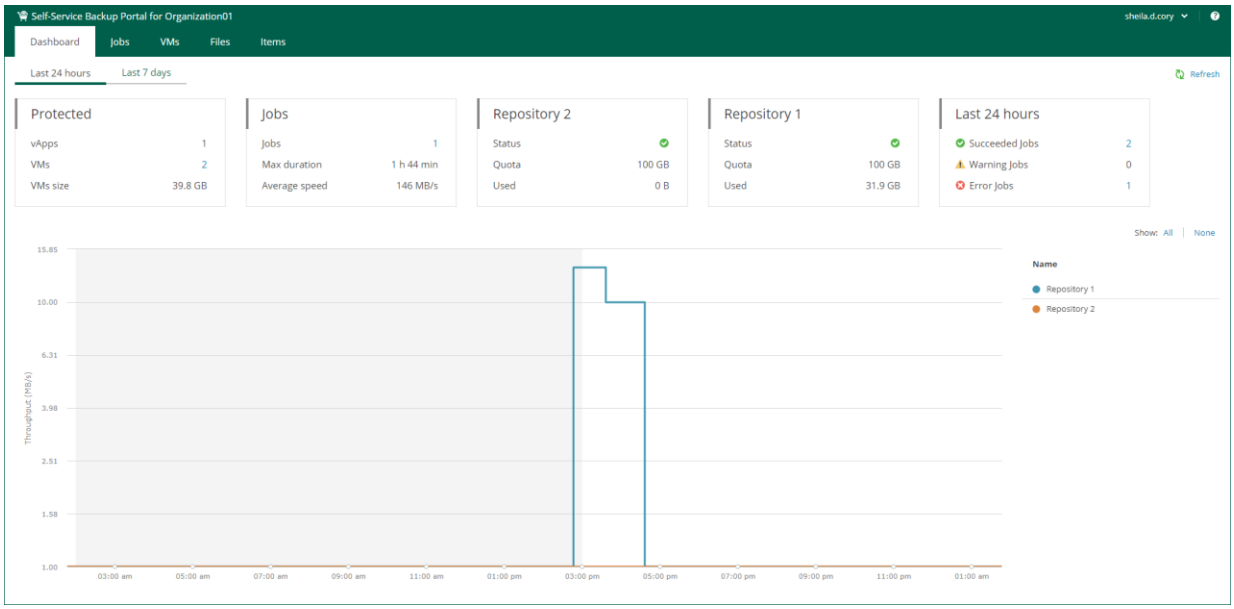
The **Dashboard** tab contains statistics on VMware Cloud Director backup jobs, replication jobs, and CDP policies of your Cloud Director organization, including information on protected VMs, job runs, and backup repositories.

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

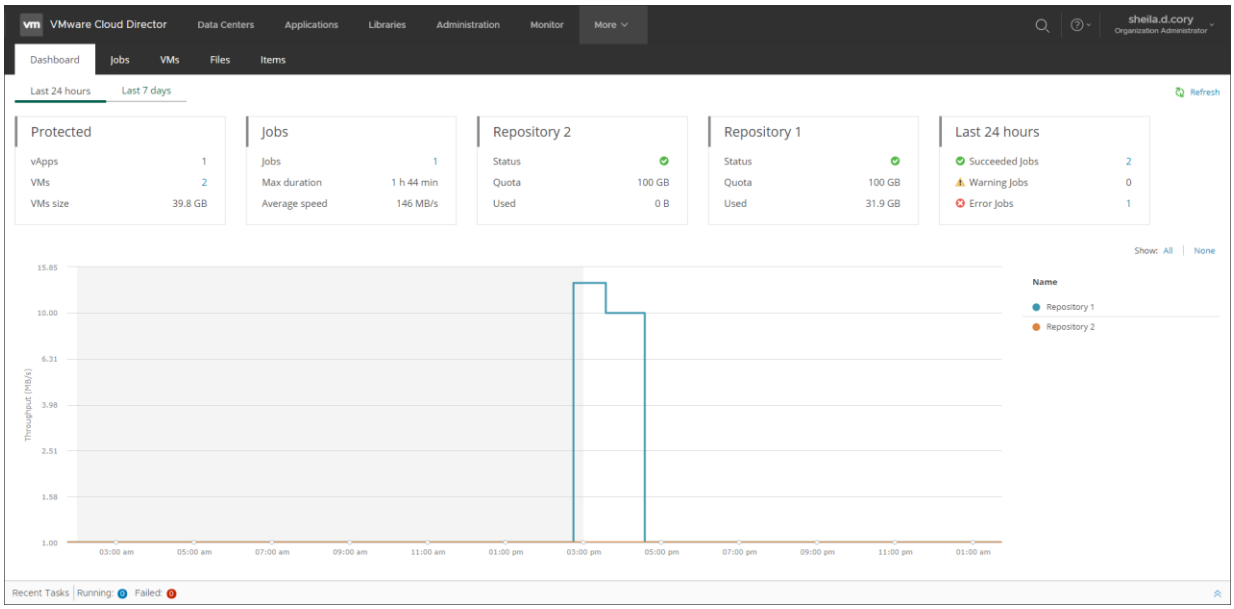
- Last 24 hours
- Last 7 days

To switch between the ranges, select a necessary tab in the upper-left corner.

Veeam Self-Service Backup Portal accessed by URL



Veeam Self-Service Backup Portal accessed from Cloud Director using Veeam Plug-in for VMware Cloud Director



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

- *vApps* — the number of vApps for which restore points were successfully created during the specified period.
- *VMs* — the number of VMs for which restore points were successfully created during the specified period.
- *VMs size* — total size of source VMs successfully processed.

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

- *Jobs* — the number of created jobs.
- *Max duration* — maximum job duration.
- *Average speed* — average data transfer speed.

The **Backup Storage / <Repository name>** widgets display statistics about backup repositories available to the organization. Each widget represents a single repository and contains the following information:

- *Status* — a status of the backup repository assigned to the organization:
  - *Green* — more than 10% of storage space is free.
  - *Yellow* — less than 10% of storage space is free.
  - *Red* — no free space on backup storage.
- *Quota* — storage quota.
- *Used* — used storage size. Note that replication jobs do not consume storage quota of backup repositories because replicas are stored on the target VMware Cloud Director VDC.

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

To visualize on-going jobs data, the **Dashboard** tab also comprises a chart showing date and time when jobs were performed, and the network throughput rate during the job.

The highlighted part of the chart represents the configured backup window if this option is specified in the chart settings. For more information, see Customizing Dashboard Chart.

Managing Cloud Director Jobs and Policies

On the **Jobs** tab, members of the VMware Cloud Director organization can perform the following operations with Cloud Director backup jobs, replication jobs, and CDP policies:

- Create backup jobs
- Start, Stop and Retry backup jobs and replication jobs
- Enable and disable backup jobs, replication jobs, and CDP policies
- Edit backup jobs and replication jobs
- Delete backup jobs, replication jobs, and CDP policies

Before You Begin

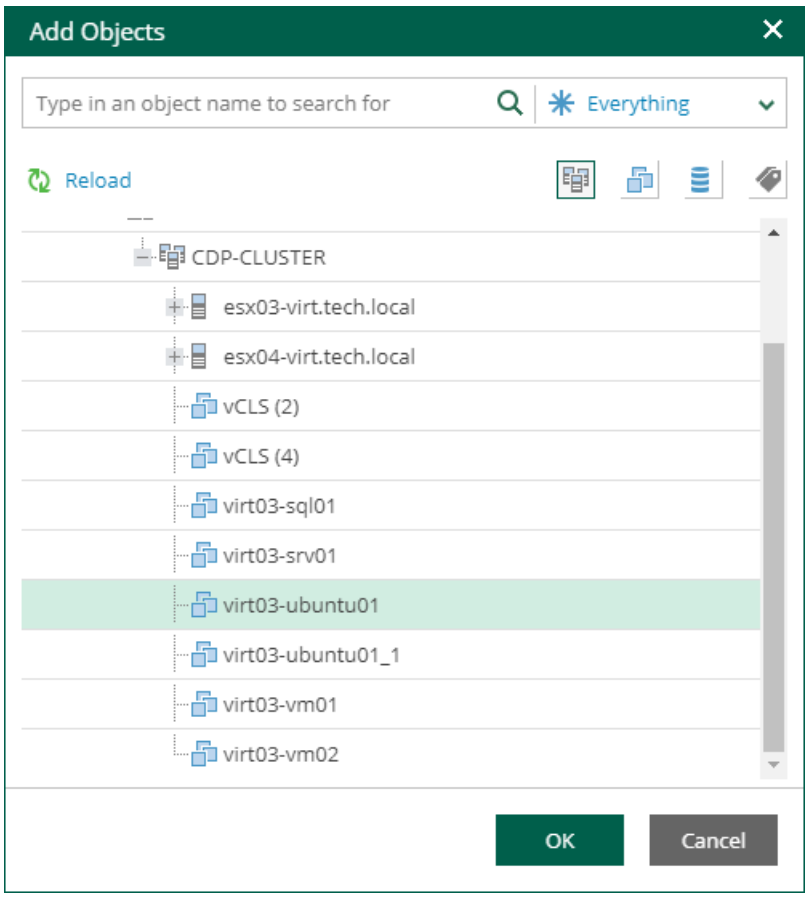
Before you start working with jobs, consider the following:

- Organization members cannot see jobs and CDP policies created by the service provider in Veeam Backup & Replication if the jobs and policies are not mapped to the organization configuration. For more information, see Mapping Jobs and CDP Policies to Organization Configurations.
- Job cloning is not available.
- In Veeam Self-Service Backup Portal, you cannot create and edit jobs managed by backup servers of earlier major or minor versions. For example, after you upgrade Enterprise Manager to version 13.1, you will not be able to create and edit jobs managed by a backup server with version 12.3. To resolve the issue, upgrade the backup server as well.
- The following limitations apply to scenario involving VM backup and subsequent restore using Veeam Self-Service Backup Portal:
  a. You create a backup job that will process a VM added explicitly (that is, not as a part of a vApp container).

b. This job runs creating a number of restore points.

c. Then you restore this VM to the original location by using the portal.

After restore, the VM identifier changes in Cloud Director hierarchy. Due to this reason, the backup job cannot locate this VM any longer. So, you need to edit job settings, adding this VM anew. To ensure that job configuration will store this VM with the new metadata (not the old one from Cloud Director hierarchy cache), you should first click **Reload** in the **Add Objects** window.



d. At the next job run, a new full backup will be created for this VM. However, if you try to perform file-level restore with the portal from the restore points created initially for that VM (on step 2), the restore operation will fail, as that VM identifier does not exist any longer.

Creating Jobs

With Veeam Self-Service Backup Portal, members of a VMware Cloud Director organization can create Cloud Director backup jobs. The jobs that you create are also shown in the Veeam Backup & Replication console under the **Jobs** node and in Veeam Backup Enterprise Manager on the **Jobs** tab. The jobs have the *<Cloud Director_org_name>* prefix.

To create a Cloud Director backup job, use the **Create Backup Job** wizard:

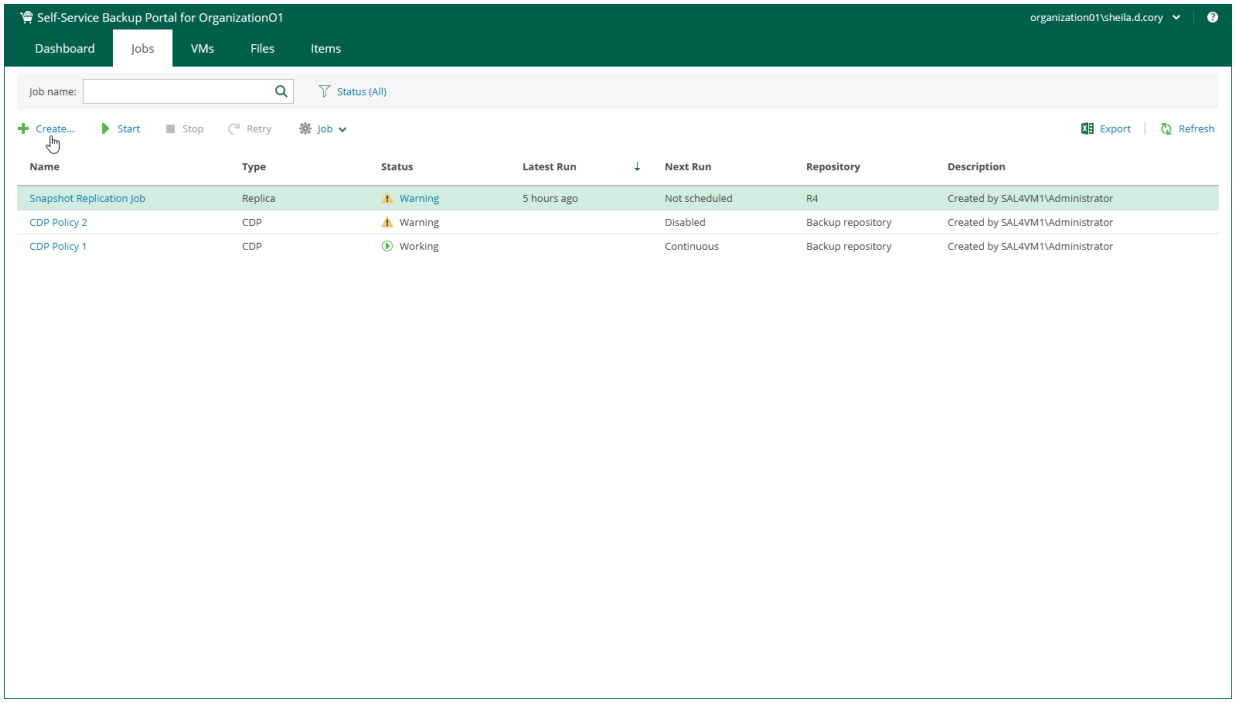
1. Launch the wizard.
2. Specify job name and retention settings.
3. Specify a list of VMs.
4. Configure VM processing order.
5. Configure guest OS processing settings.

6. Configure job schedule.
7. Configure email notifications.

Step 1. Launch Wizard

To launch the **Create Backup Job** wizard, do the following:

1. Log in to the Veeam Self-Service Backup Portal under a Cloud Director account with proper rights. For more information on required user rights, see Access Control.
2. On the **Jobs** tab, click **Create**.



Step 2. Specify Job Name and Retention Settings

At the **Job Settings** step of the wizard, specify a job name, repository, job description, retention policy and job priority.

1. In the **Job name** field, enter a name for the job.
2. From the **Repository** list, select a backup repository where the created backup files must be stored.

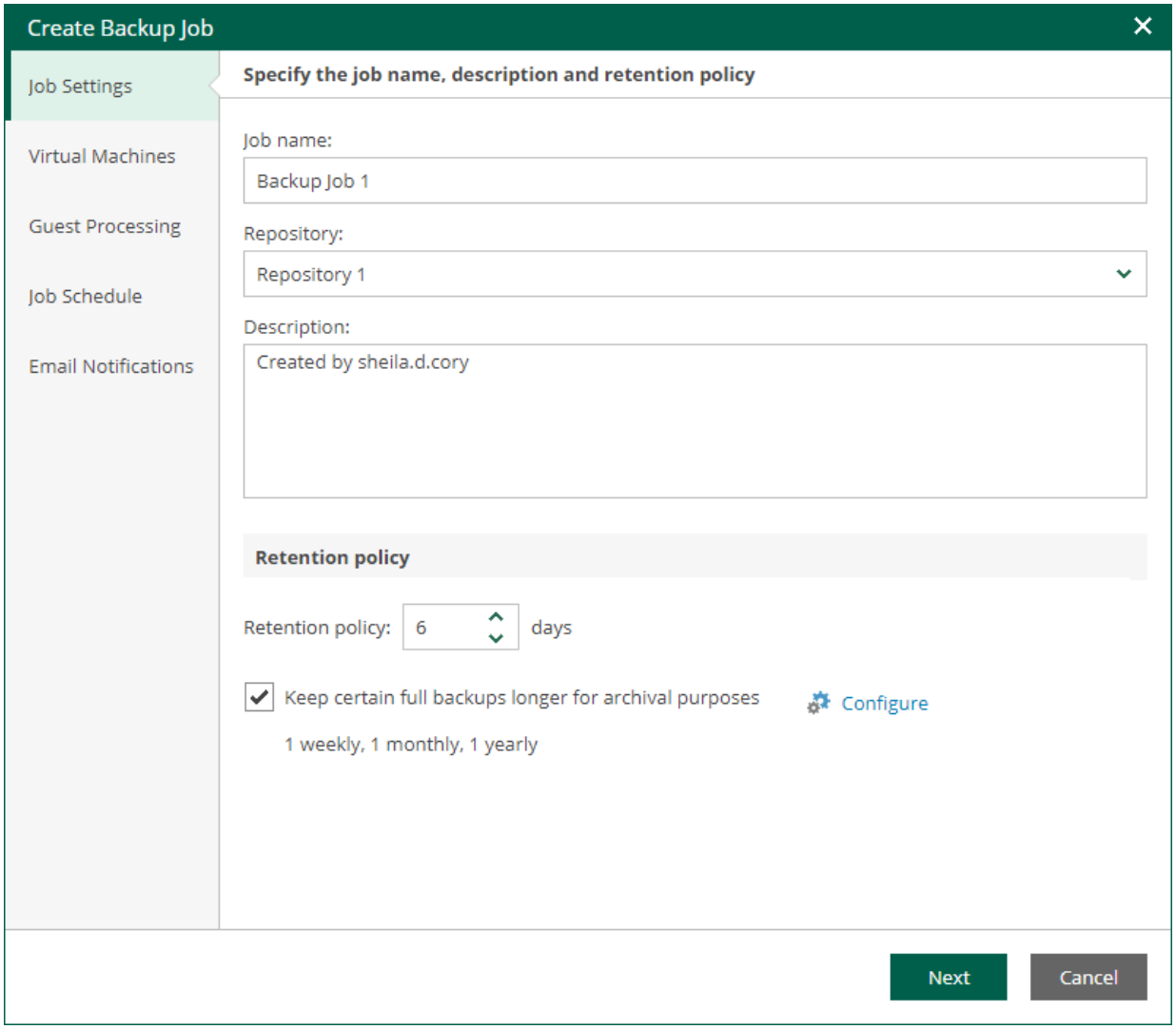
   You can select a repository only if more than one configuration is added for the organization. For more information, see Adding Organization Configuration.
3. In the **Description** field, provide an optional description for future reference. The default description contains information about the user who created the job, date and time when the job was created.
4. To configure retention policy settings, in the **Retention policy** section, specify the number of days that you want to keep restore points in the backup repository. After this period, restore points will be removed from the backup chain.

   Jobs created in previous versions of Veeam Backup & Replication may have the retention policy defined by the number of restore points rather than by days. For such jobs, you can change the retention unit to days.

   For more information on retention, see the Short-Term Retention Policy section of the Veeam Backup & Replication User Guide. You can also refer to this Veeam KB article.
5. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how often full backups are retained. For more information, see the Long-Term Retention Policy (GFS) section of the Veeam Backup & Replication User Guide.

   The **Keep certain full backups longer for archival purposes** check box is available only if GFS retention policy can be applied to the job. For more information on GFS limitations, see the Long-Term Retention Policy (GFS) section of the Veeam Backup & Replication User Guide.

6. Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. For more information on job priorities, see the Job Priorities section of the Veeam Backup & Replication User Guide.



Step 3. Specify List of VMs

At the **Virtual Machines** step of the wizard, you can add or remove VMs, vApps and VDCs of the organization. Jobs with VM containers are dynamic in their nature: if a new machine is added to the container after the job is created, the job is automatically updated to include the added machine.

Adding VMs and VM containers

To add a VM or a VM container:

1. Click the **Add**.
2. In the virtual infrastructure tree, select the necessary VMs or VM containers.

   If you select a VM container and later add a new VM to the container, Veeam Backup & Replication will update job settings automatically to include the VM.

   > **TIP**
   >
   > To quickly find the necessary objects, you can do the following:
   >
   > - Search for objects: type a name or part of a name in the search field. Specify the type of the object from a scroll list next to the search field.
   > - Switch between virtual infrastructure views using the buttons in the upper-right corner. For VMware objects, you can switch between the **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs**, and **Tags and VMs** views.

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

Removing VMs and VM containers

To remove a VM or VM container, select it in the list and click **Remove**.

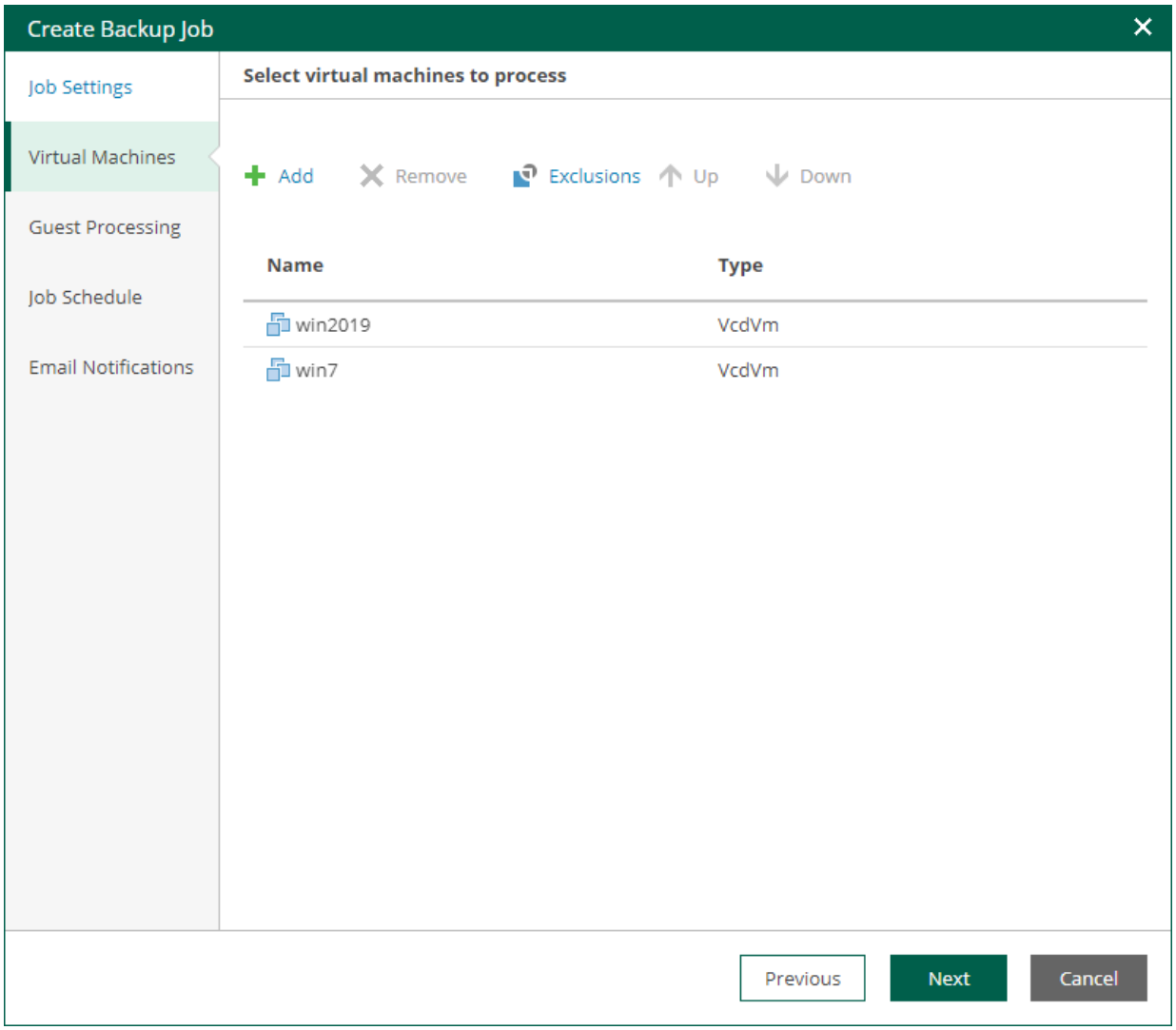
Excluding VMs

You can also exclude individual VMs from VM containers.

To exclude VMs from a VM container:

1. Select a VM container in the list and click **Exclusions**.

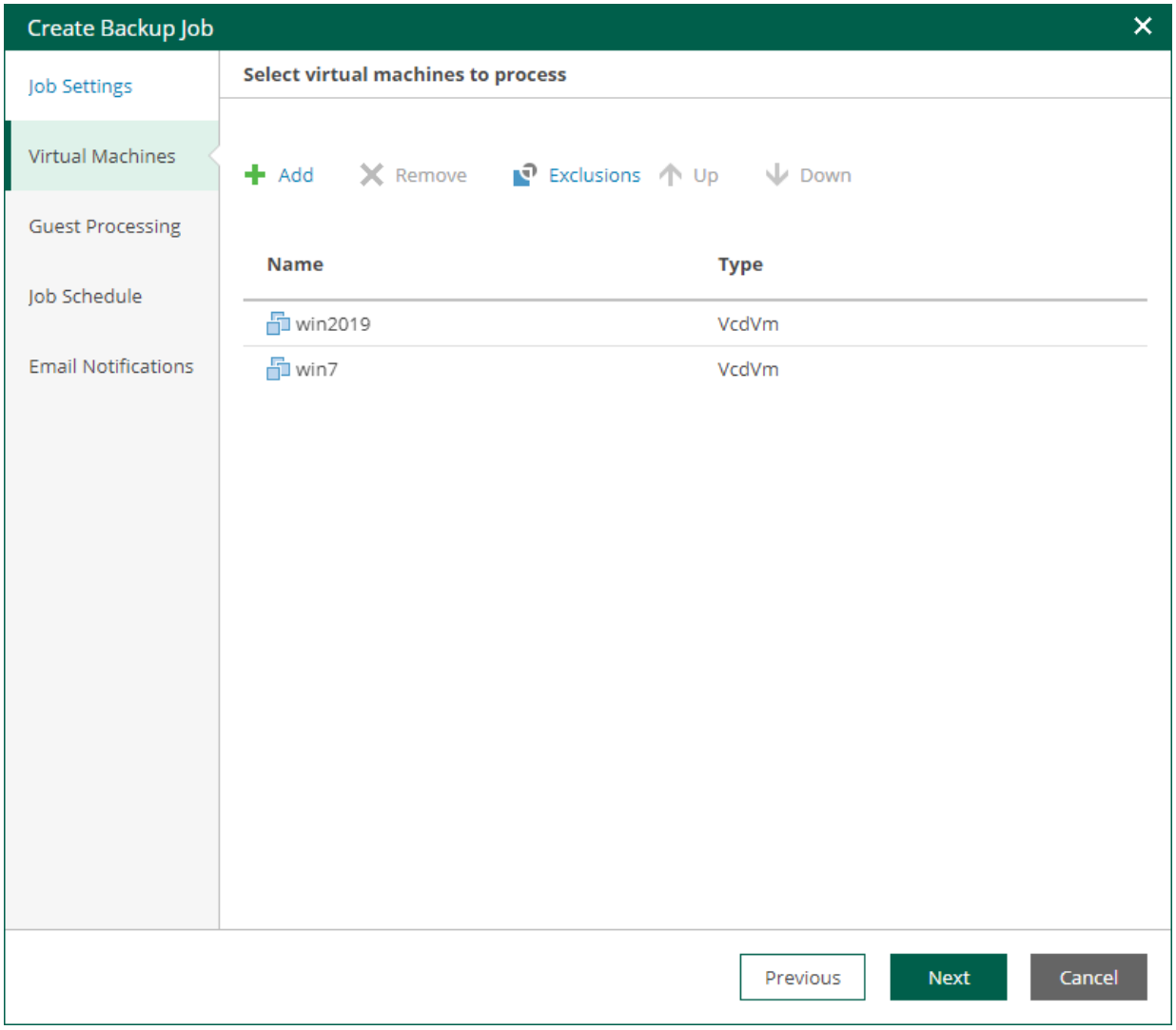
2. In the **Exclusions** window, click **Add** and select machines that you want to exclude.



Step 4. Configure VM Processing Order

At the **Virtual Machines** step of the wizard, you can change the VM processing order. It can be helpful if specific VMs must be processed first, if you want to ensure that processing of a MV does not overlap with other scheduled activities, or that VM processing is completed before the certain time.

To change the VM processing order, select the necessary machines and move them up or down the list using the **Up** and **Down** buttons on the right. In the same manner, you can set the backup order for containers in the backup list. You can change the order of the following VMware Cloud Director objects: VMs, vApps, organization VDCs, organizations and the Cloud Director instance. The scope depends on your Cloud Director access rights.



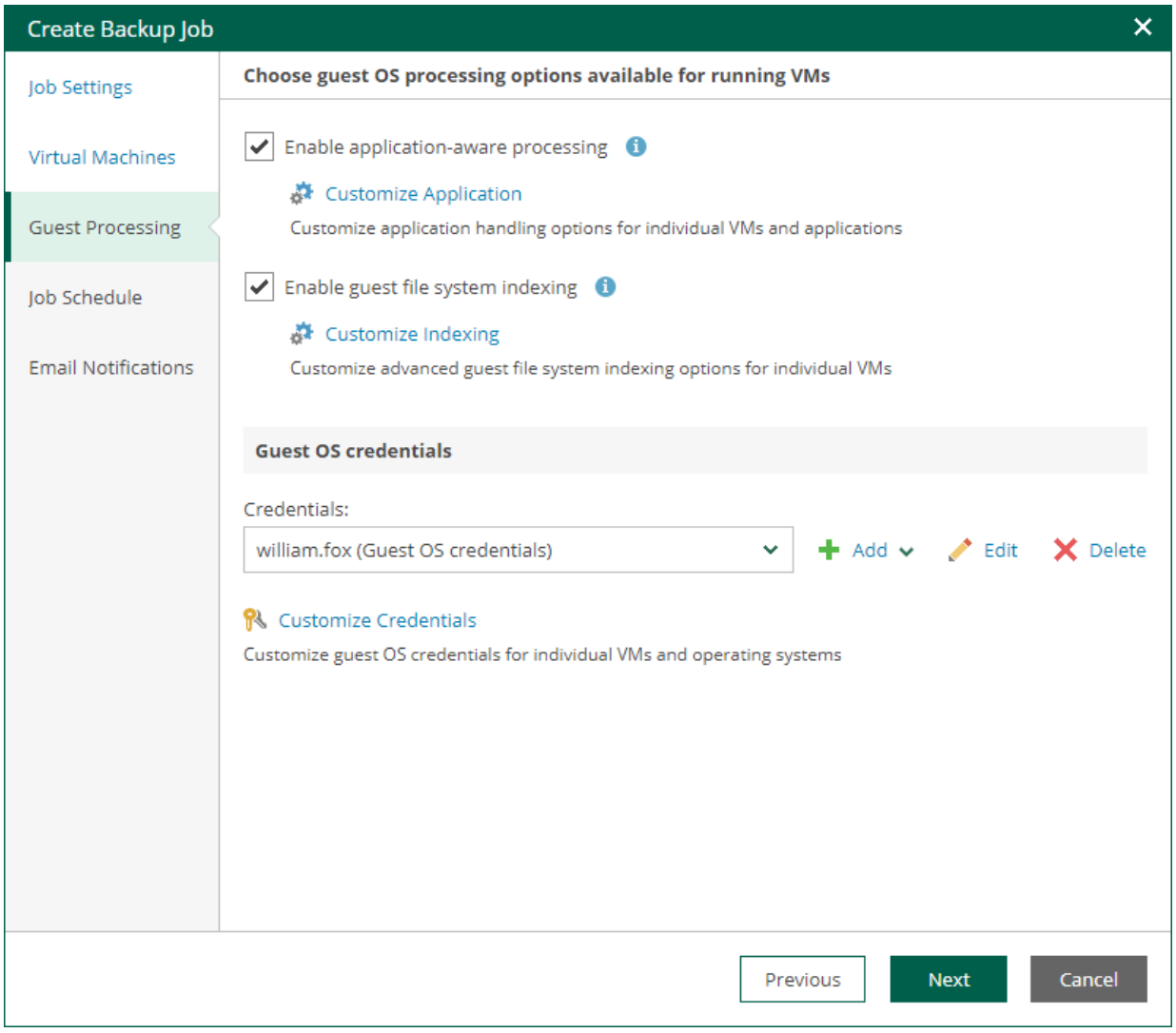
Step 5. Configure Guest Processing Settings

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

- Application-Aware Processing
- Guest OS File Indexing
- Guest OS Credentials

NOTE

VMware Cloud Director system administrators can access guest OS credentials available for their organizations. They can also supply new credentials for guest OS processing.



Application-Aware Processing

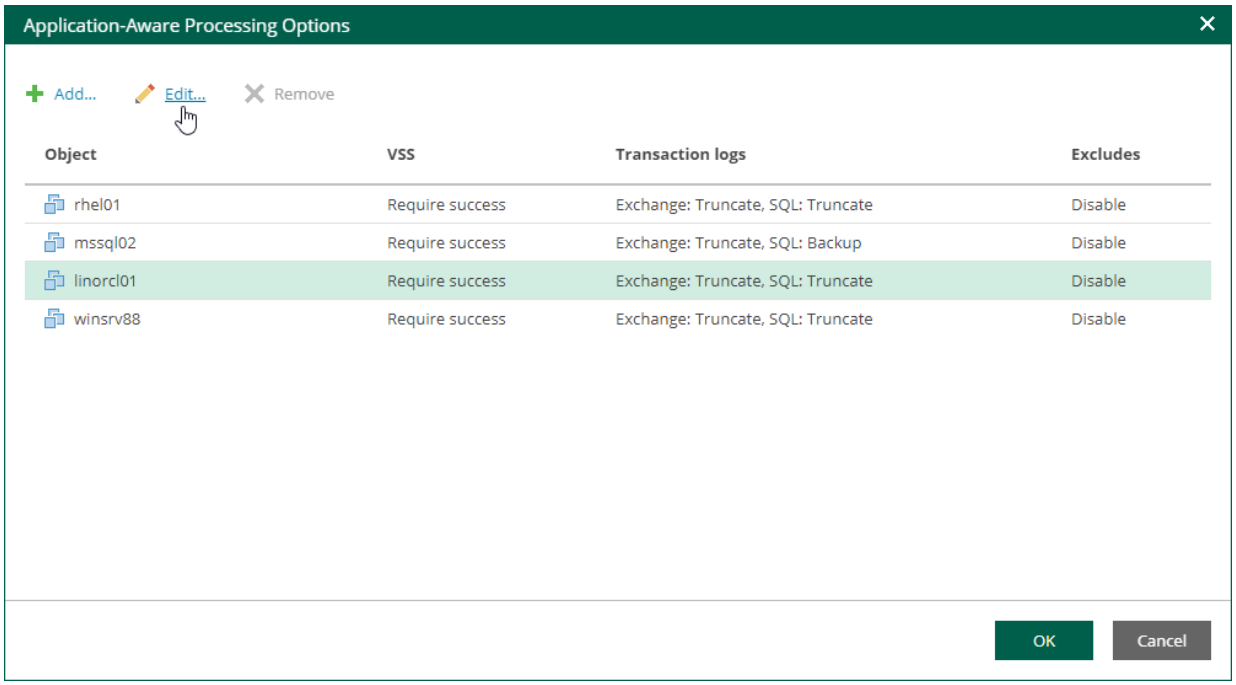
At the **Guest Processing** step of the wizard, you can enable application-aware processing. Application-aware processing is a Veeam technology based on Microsoft VSS and used to create transactionally consistent backups or replicas of VMs that run Microsoft Active Directory, Microsoft SQL Server, Microsoft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

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

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

   To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.

   To discard custom settings of a machine, select the machine in the list and click **Remove**.
4. Configure the necessary settings for the selected application server:
   - General Settings
   - Microsoft SQL Server Transaction Log Settings
   - Oracle Archived Log Settings
   - PostgreSQL Archive Log Settings
   - VM Guest OS File Exclusion



General Settings

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

1. In the **Applications** section, select the option that corresponds to your transactionally-consistent backup creation scenario.
   - Select **Require successful processing** (default option) if you want Veeam Backup & Replication to stop the backup job if an error occurs.
   - Select **Try application processing, but ignore failures** if you want to continue the backup process even if an error occurs. This option guarantees completion of the job. The created backup image will not be transactionally consistent, but rather crash-consistent.

- Select **Disable application processing** if you do not want to enable application-aware processing for the VM. This option makes the **Transaction Logs Processing** section unavailable.

2. [For Microsoft Exchange, Microsoft SQL Server, Oracle and PostgreSQL] In the **Transaction Logs Processing** section, specify whether this job should process transaction logs upon a successful backup.

   - Select **Process transaction logs with this job** if you want Veeam Backup & Replication to process transaction logs.

     [For Microsoft Exchange] With this option selected, the non-persistent runtime components or persistent components running on the VM guest OS will wait for backup to complete successfully and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched on the VM guest OS until the next start of the non-persistent runtime components or persistent components.

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

     - For Microsoft SQL Server transaction log processing — on the **SQL** tab. For more information, see Microsoft SQL Server Transaction Log Settings.
     - For Oracle database archived logs processing — on the **Oracle** tab. For more information, see Oracle Archived Log Settings.
     - For PostgreSQL database archive logs processing — on the **PostgreSQL** tab. For more information, see PostgreSQL Archive Log Settings.

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

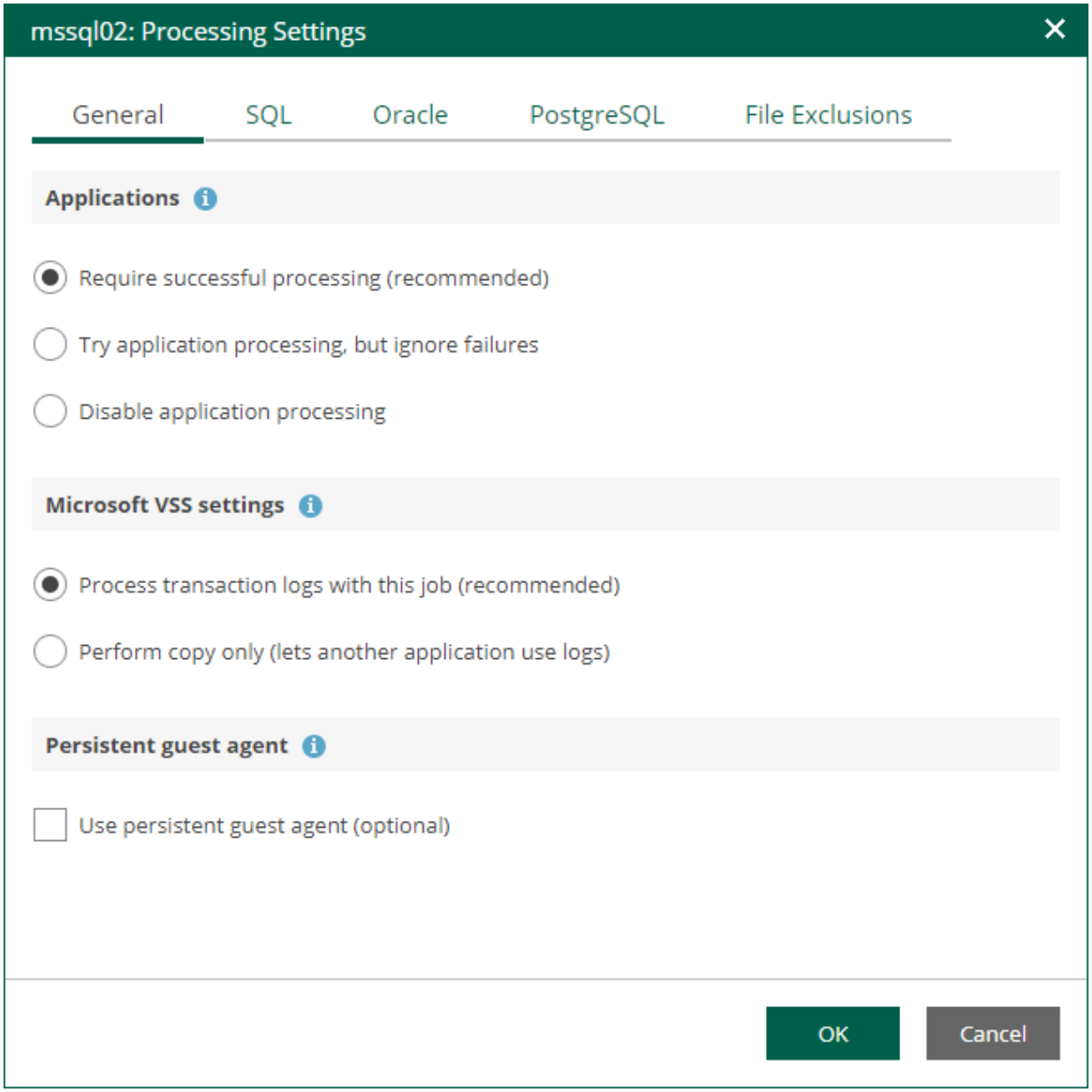
     With this option selected, the **SQL**, **Oracle** and **PostgreSQL** tabs are not available.

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

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

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

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

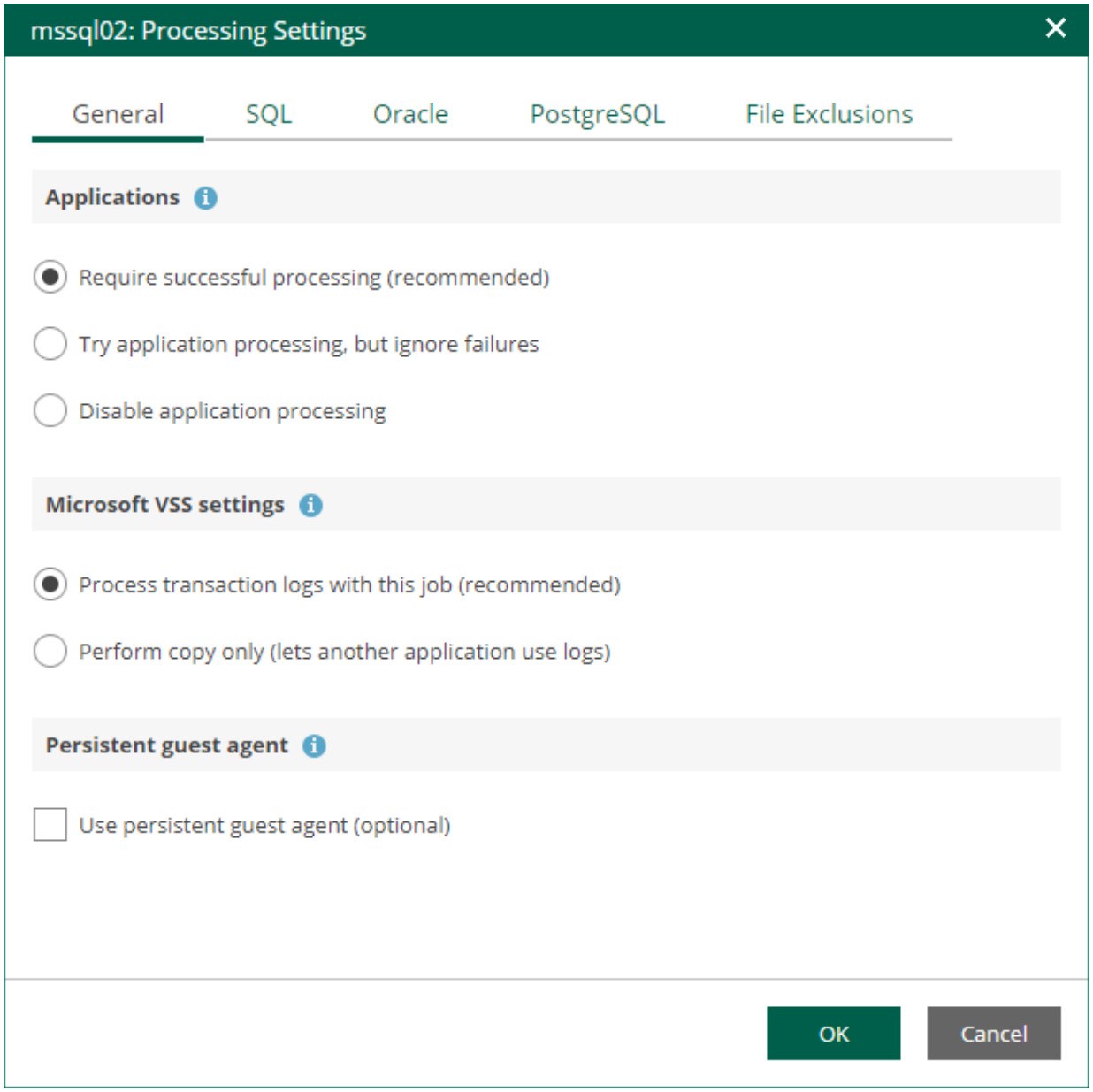


Microsoft SQL Server Transaction Log Settings

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

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

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



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

     > **NOTE**
     >
     > If the account specified at the Guest Processing step does not have enough rights, Veeam Backup & Replication tries to truncate logs using the *NT AUTHORITY|SYSTEM* account. Make sure that the account has permissions listed in the Permissions section of the Veeam Explorers User Guide.

- Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Backup & Replication will not truncate transaction logs on the Microsoft SQL Server VM.

  Select this option for databases that use the Simple recovery model. If you enable this option for databases that use the Full or Bulk-logged recovery model, transaction logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrators must take care of transaction logs themselves.

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

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

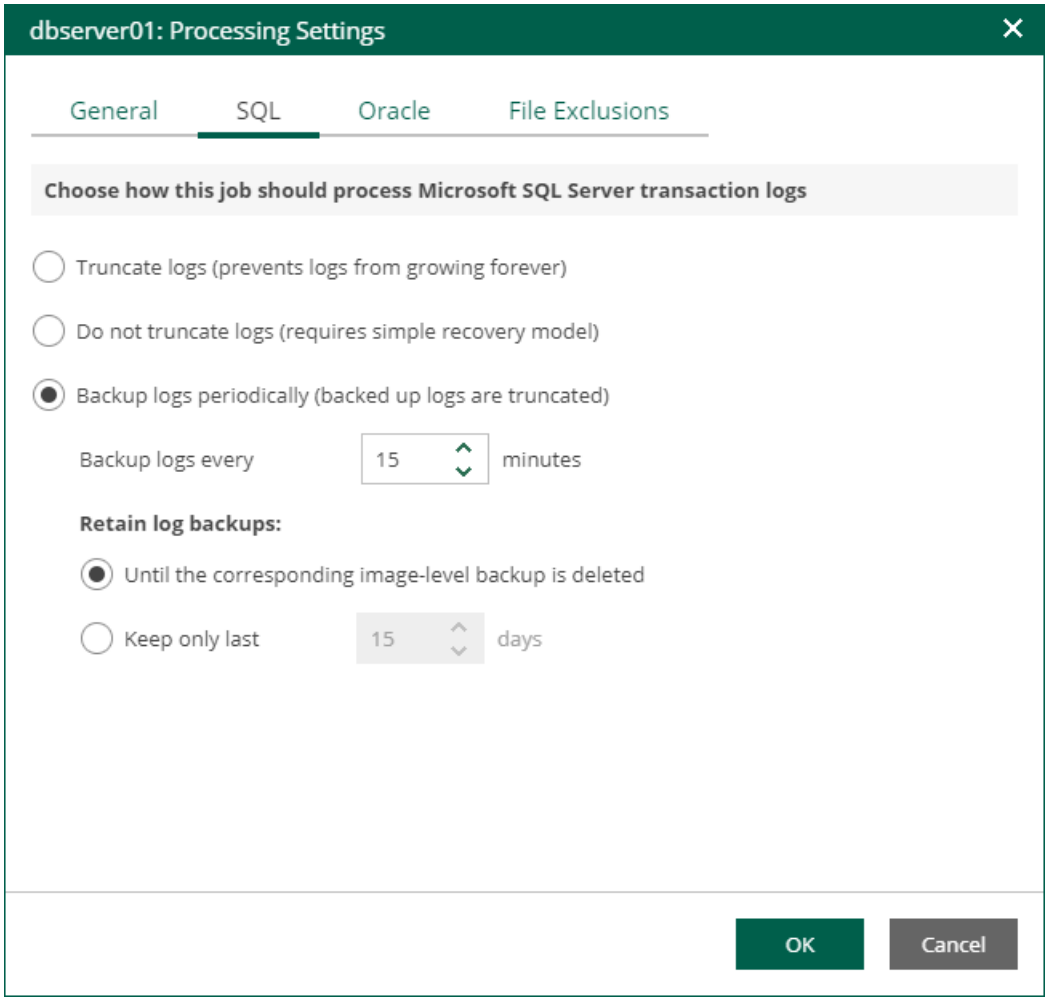
7. If you have selected the **Backup logs periodically** option, specify settings for transaction log backup:

   a. In the **Backup logs every <N> minutes** field, specify the frequency for transaction log backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

   b. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup repository.

      - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
      - Select **Keep only last <N> days** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backups. For more information, see Retention for Transaction Log Backups section of the Veeam Backup & Replication User Guide.

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

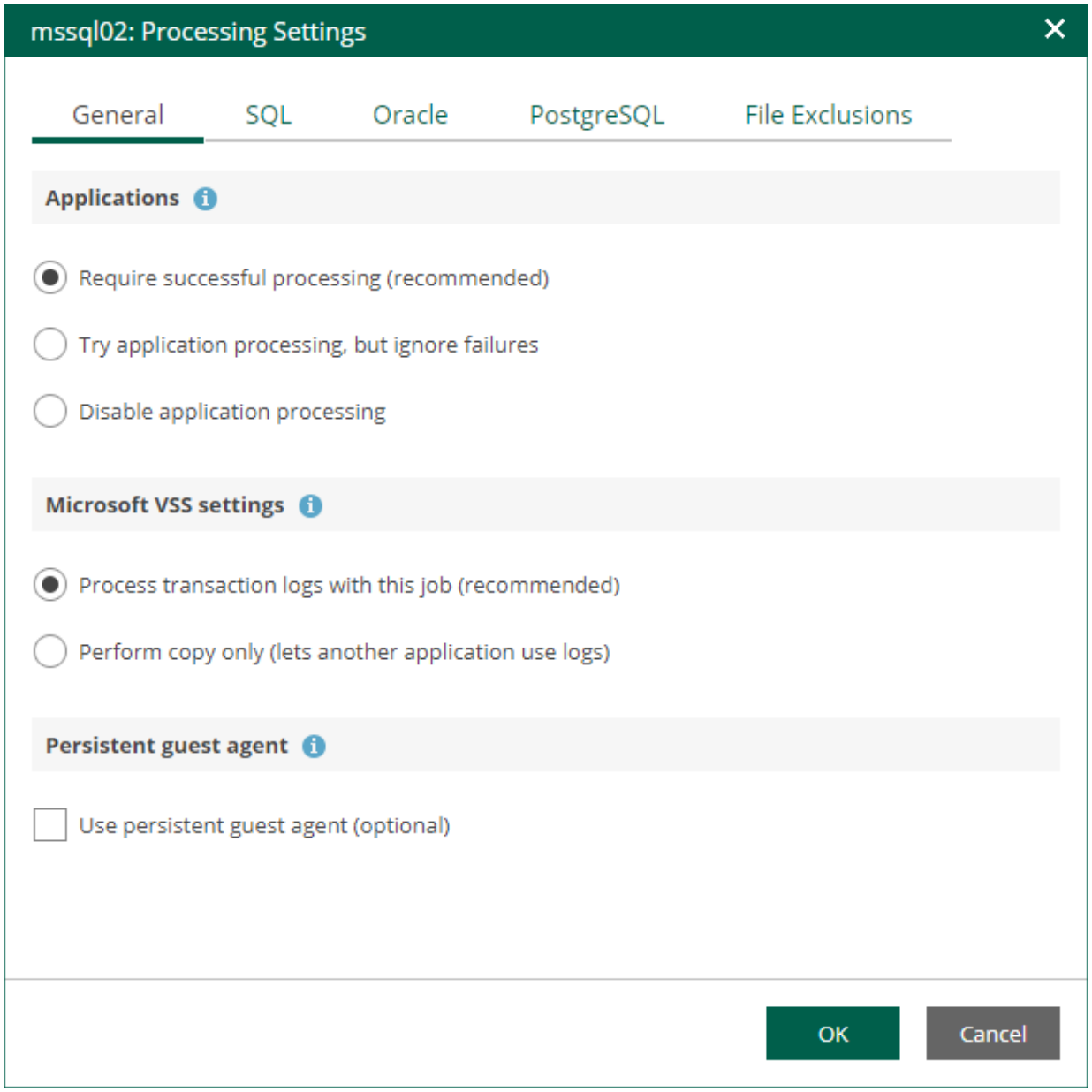


Oracle Archived Log Settings

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

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

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



5. On the **Oracle** tab of the **VM Processing Settings** window, specify log processing settings.

   a. Specify a user account that will connect to the Oracle database and perform Oracle archived logs backup and deletion.

      - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.
      - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

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

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

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

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

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

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

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

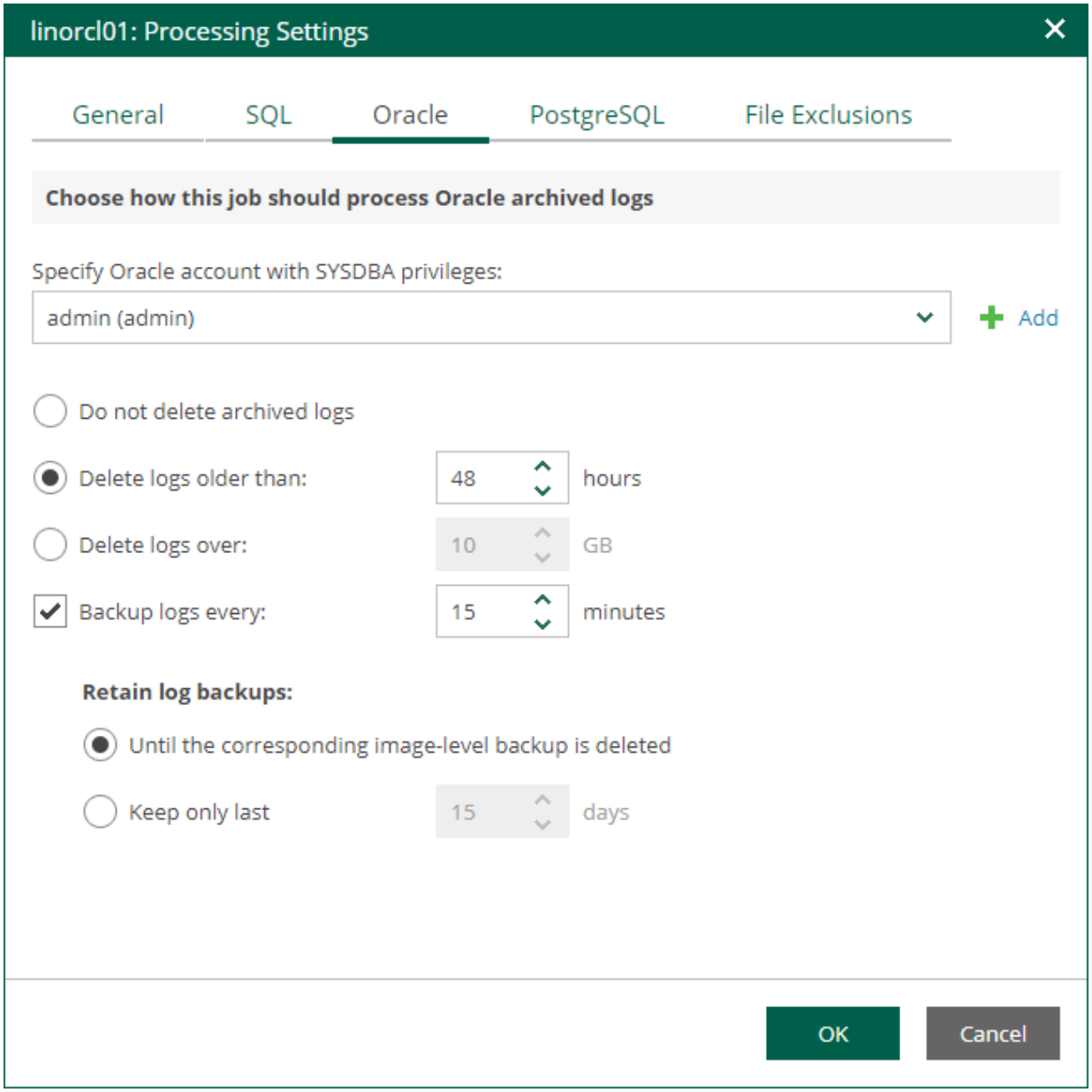
c. To back up Oracle archived logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archived log backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

> **IMPORTANT**
>
> If you plan to use this option together with archived logs deletion from Oracle machine guest, make sure that these settings are consistent: logs should be deleted after they are backed up to repository. Thus, you need to set up backup schedule and log removal conditions appropriately.

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

   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
   - Select **Keep only last <N> days** to keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the image-level backups. For more information, see the Retention for Archived Log Backups section of the Veeam Backup & Replication User Guide.

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

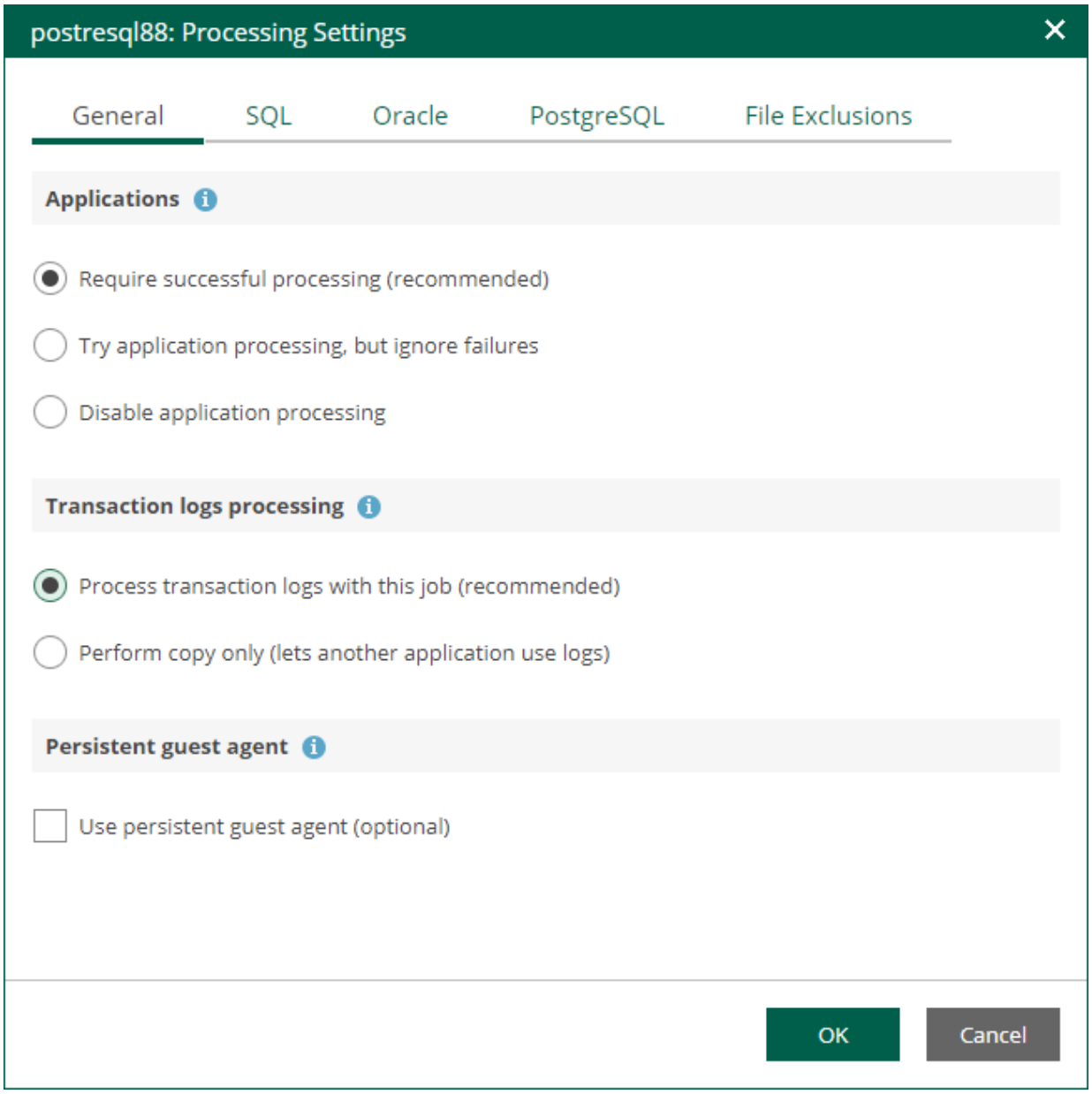


PostgreSQL Archive Log Settings

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

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

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



5. On the **PostgreSQL** tab of the **VM Processing Settings** window, specify settings for PostgreSQL logs processing.

   a. Specify an account that will connect to the PostgreSQL instance and perform PostgreSQL archive logs backup and deletion. The `pg_hba.conf` configuration file of the PostgreSQL instance must contain a record with the account.

      - Select **Use guest credentials** to use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the PostgreSQL instance.
      - Specify another account. To do this, select the necessary account from the drop-down list or click **Add** and add a new account.

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

   b. Specify an authentication method for the selected user account.

- Select **Database user with password** if you have specified an account with password-based authentication. In this case, you must provide Veeam Backup & Replication with the account password that will be stored in the Veeam Backup & Replication database.
- Select **Database user with password file (.pgpass)** if you have specified an account with password-based authentication. In this case, you do not have to specify the account password when adding the account in Veeam Backup & Replication. Instead, the account password must be specified in the PGPASS password file stored in the user's home directory.
- Select **System user without password (peer)** if you have specified a local system account with peer authentication.

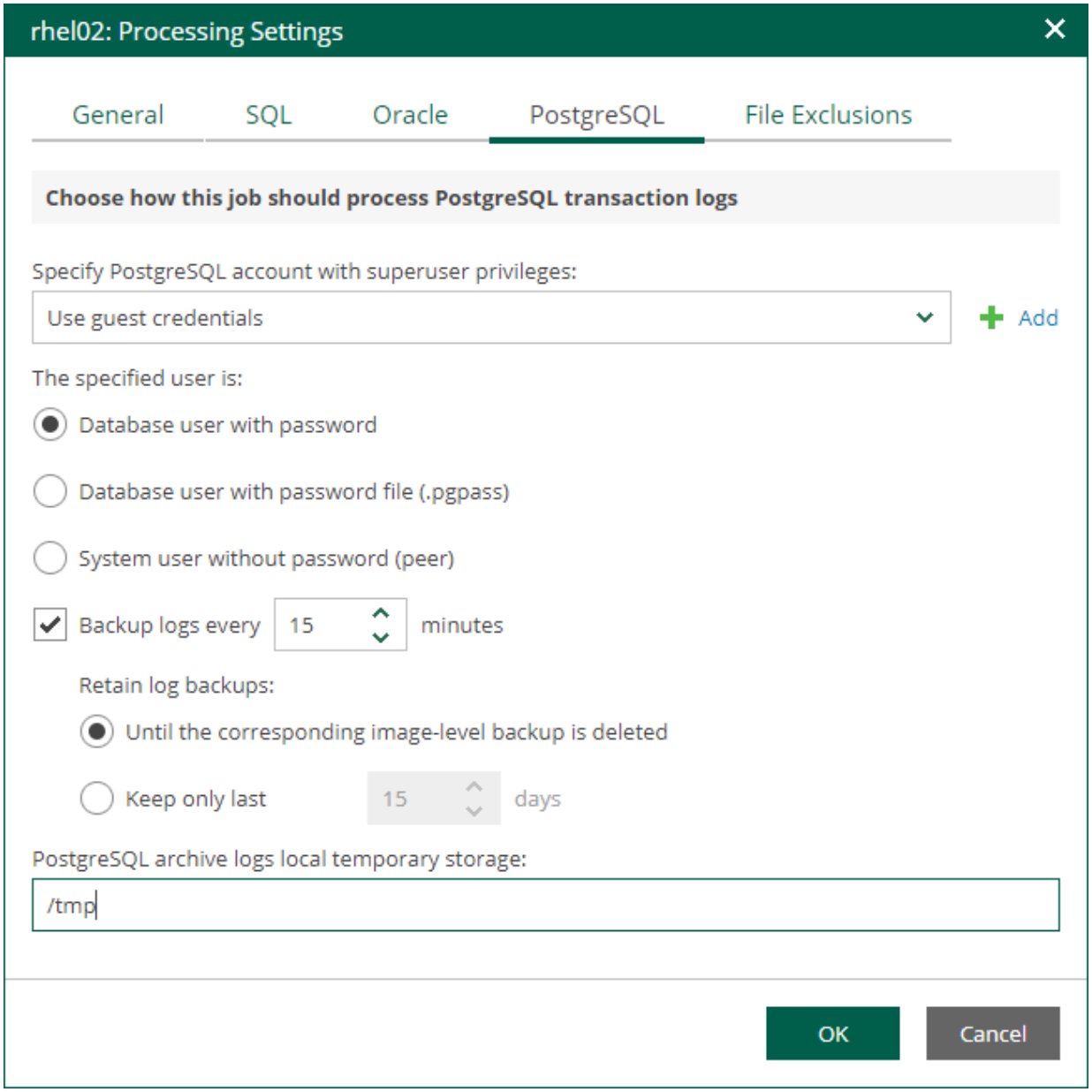
c. To back up PostgreSQL archive logs with Veeam Backup & Replication, select the **Backup logs every <N> minutes** check box and specify the frequency for archive log backup. By default, archive logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

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

- Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
- Select **Keep only last <N> days** to keep archive logs for a specific number of days. By default, archive logs are kept for 15 days. If you select this option, you must make sure that retention for archive logs is not greater than retention for the image-level backups. For more information, see the Retention for PostgreSQL WAL Files section of the Veeam Backup & Replication User Guide.

e. In the **PostgreSQL archive logs local temporary storage** field, specify a path on the PostgreSQL machine that Veeam Backup & Replication will use to temporarily store PostgreSQL archive logs until they are backed up. Veeam Backup & Replication does not create the temporary storage folder so the folder must exist on the machine. Make sure the temporary location has enough free space for storing the log files.

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



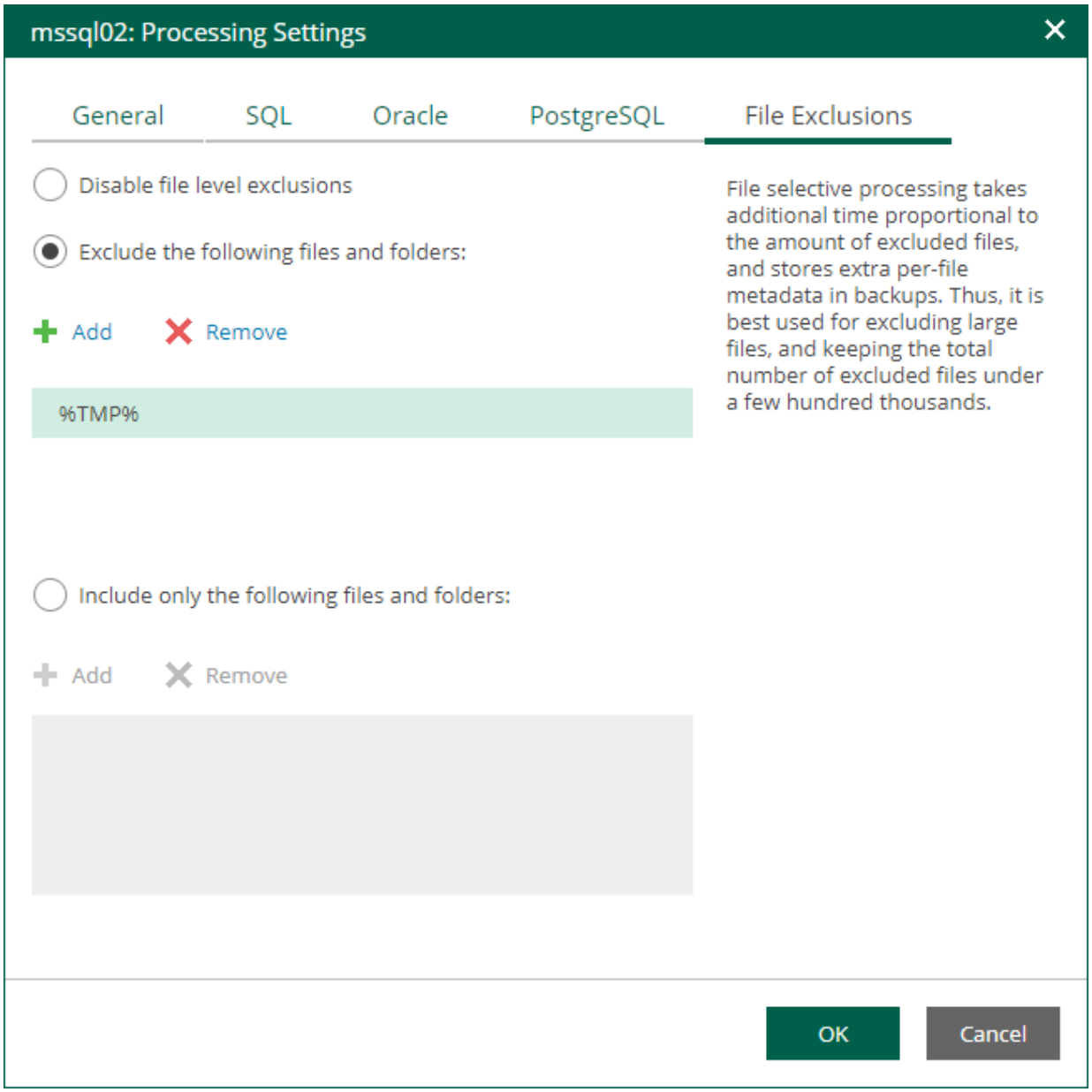
VM Guest OS File Exclusion

If you do not want to back up specific files and folders on the VM guest OS, you can exclude them from the backup. Exclusions can help decrease the backup file size. However, selective processing takes additional time that depends on the number of excluded files. It also requires obtaining per-file metadata (stored in backups). Thus, it is recommended to use this option for excluding large files. By default, exclusions are disabled.

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

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

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



Guest OS File Indexing

To quickly find the necessary guest OS files in backups, select the **Enable guest file system indexing** check box. This setting provides, in particular, advanced search capabilities when viewing guest OS files and performing 1-Click file restore using Enterprise Manager web UI. If indexing is disabled, you can only use quick search within the selected restore point.

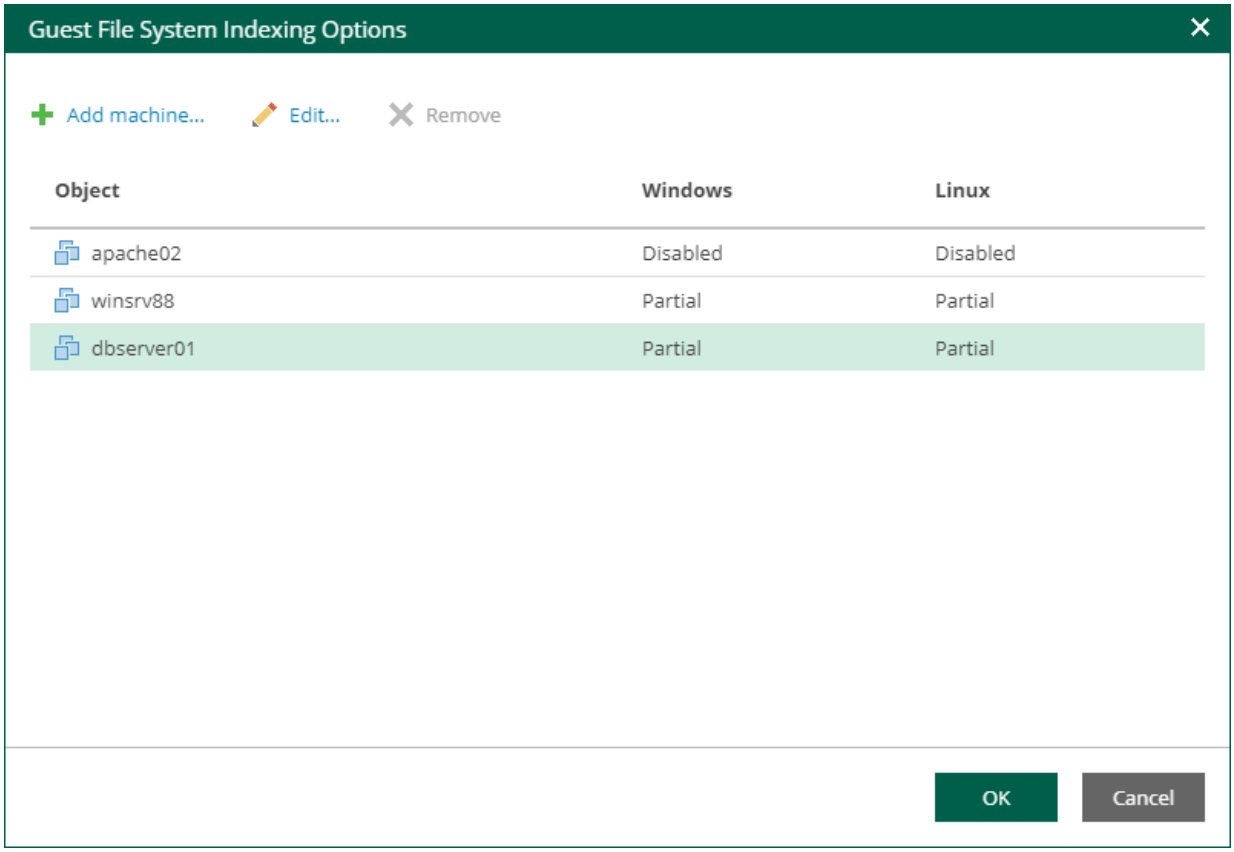
> **NOTE**
>
> For proper file indexing of Linux machines, Veeam Backup & Replication requires several utilities to be installed on the machines: `mlocate`, `gzip`, and `tar`. If these utilities are not found, you are prompted to deploy them to support index creation.

To provide granular indexing options for individual machines:

1. Click the **Customize Indexing** link.
2. In the **Guest File System Indexing Options** window, select a machine from the list and click **Edit**.

   Consider the following:

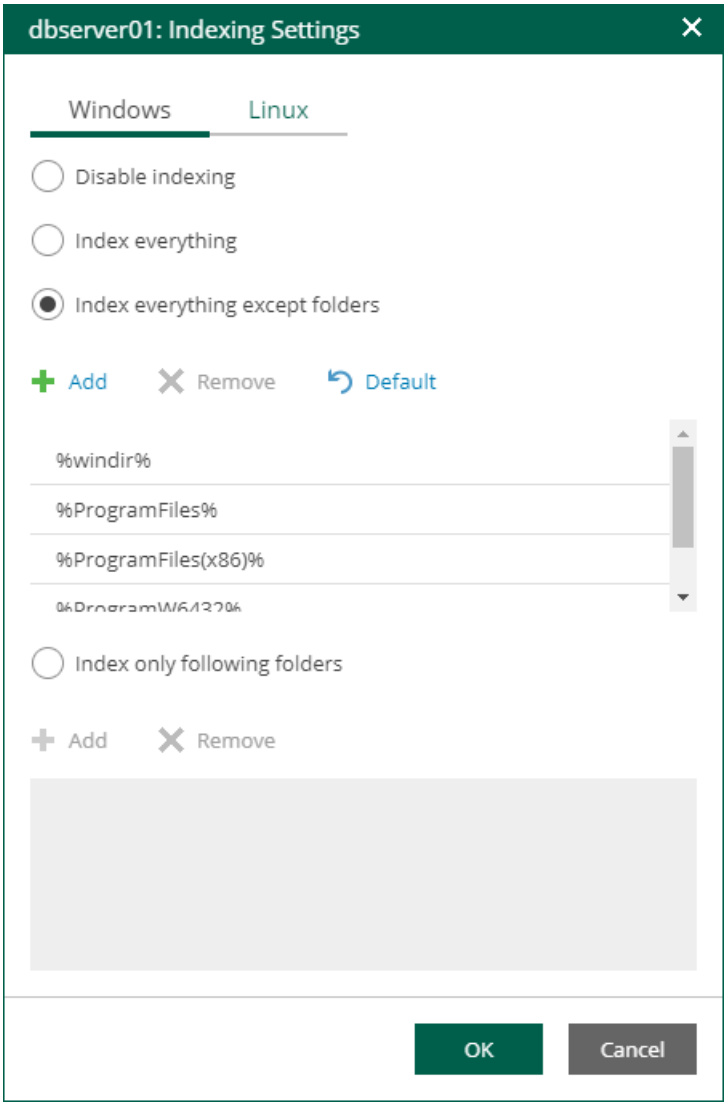
   - To customize settings of a machine added to the job as part of a container, add the machine as a standalone instance. For that, click **Add Machine** and choose the necessary VM. Next, select the machine from the list and click **Edit** to customize VM settings.
   - To discard custom settings of a machine, select it from the list and click **Remove**.



3. In the **Indexing Settings** window displayed for the selected machine, go to the **Windows** or **Linux** tab and specify what files should be indexed:

   - Select **Disable indexing** if you do not want to index guest OS files of the machine.
   - Select **Index everything** if you want to index all guest OS files inside the machine.
   - Select **Index everything except folders** if you want to index all guest OS files except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders to exclude using the **Add** and **Remove** buttons.

- Select **Index only following folders** to select specific folders that you want to index. To form the list of folders, use the **Add** and **Remove** buttons.



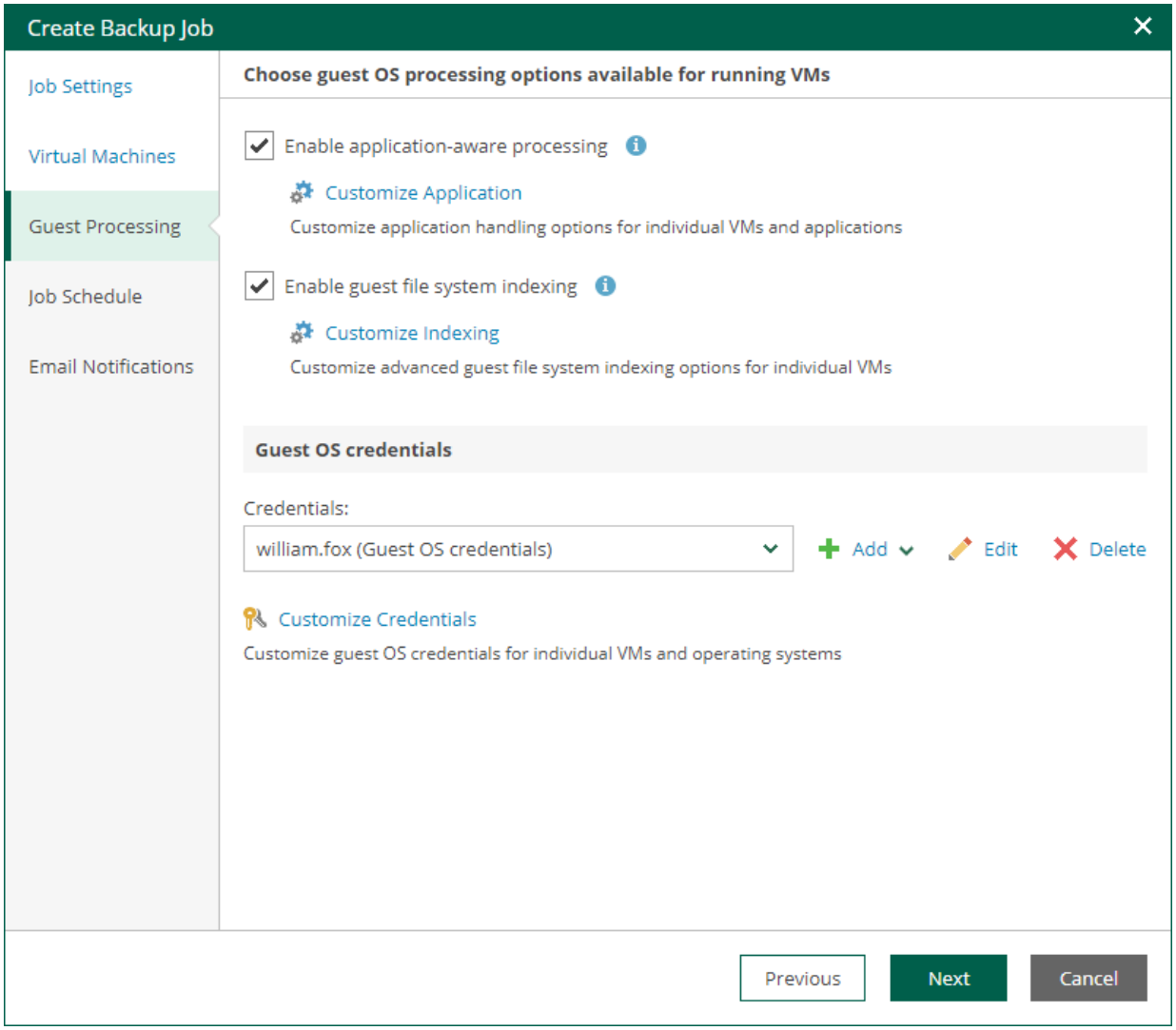
4. Click **OK** to save the settings and close the window.

Guest OS Credentials

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

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

> **NOTE**
>
> VMware Cloud Director system administrators can access guest OS credentials available for their organizations. They can also supply new credentials for guest OS processing.



In the **Guest OS credentials** section, you can select credentials from the list, or click the **Add** button to add new credentials.

- For Windows guest OS, specify a user account (name and password) with local administrative rights on target machine, and optional description. Credentials must be specified in the following format:
  - For Active Directory accounts: *DOMAIN|Username*
  - For local accounts: Username or *HOST|Username*
- For Linux guest OS, you can choose one of the following options:
  - If Management Agent is installed on the VM, you can select the **Use management agent** option.
  - If Management Agent is not installed on the VM, specify a user name, password, and SSH port (by default, port 22 is used).

    If you specify data for a non-root account that does not have root privileges on a Linux server, you can use the **Non-root account** section to grant this account elevated permissions as follows:

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

ii. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the root account password.

If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

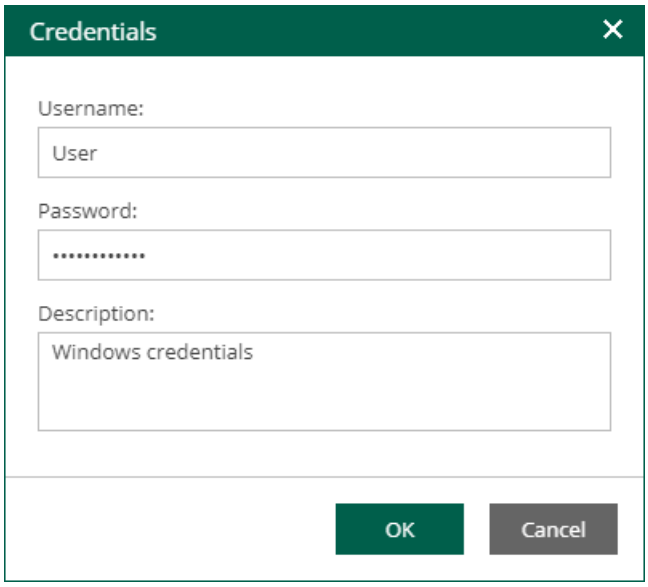
iii. If you plan to use the account to connect to Linux servers where the `sudo` command is not available or may fail, you have an option to use the `su` command instead. To enable the `su` command, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the root account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

Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.

IMPORTANT

For machine guest OS indexing of Linux-based machines, a user account with root privileges on the machine is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based machine, grant root privileges to this account and specify settings of this account in the **Guest OS credentials** section.

It is also recommended to avoid additional commands output for the specified user (like messages echoed from within `~/.bashrc` or command traces before execution), because they may affect Linux machine processing.



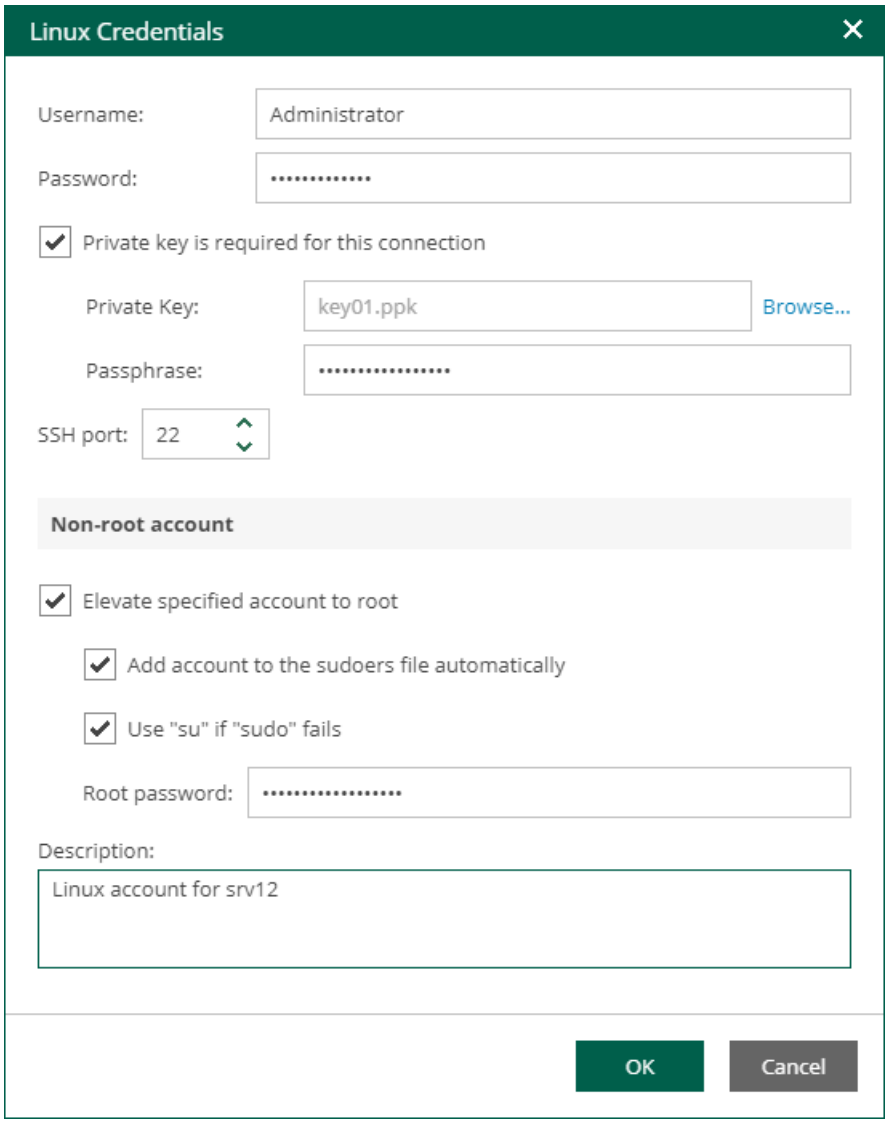
Linux Private Key

Another option is to use Linux private key. This method eliminates the need to supply password at each login, helps to protect against malicious applications like keyloggers, thus strengthening security, and simplifies launch of automated tasks, decreasing administrative load in Linux environments. For this method, a user must create a pair of keys:

- *Private key* is stored on the client (user's) machine — that is, on the machine where Veeam Backup & Replication runs. The key is usually stored in the encrypted form. To decrypt a private key, you need to supply a passphrase specified at key creation.
- *Public key* is stored on the server (Linux machine) in a special `authorized_keys` file that contains a list of public keys.

If you plan to use Linux private key for authentication, make sure you have created private and public keys and stored them appropriately: private key on the client side (Veeam backup server) and public key on the server side (Linux machine). You should also have the passphrase for the private key if it is encrypted. If you select to use Linux private key credentials, you should specify the following:

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



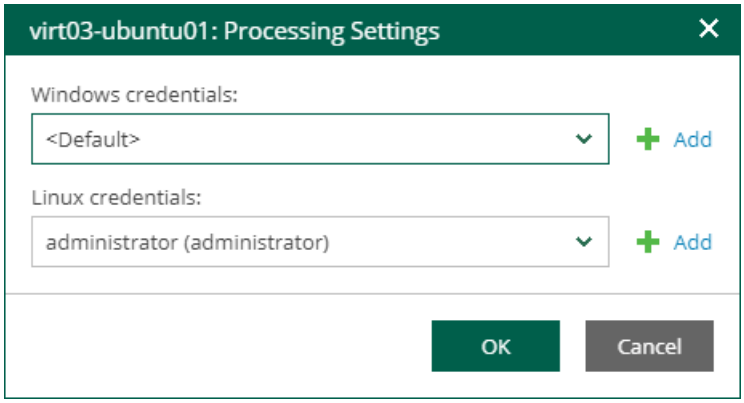
Special Credentials for Machine

By default, for all machines in the list, Veeam Backup & Replication uses common credentials you provided in the **Guest OS credentials** section. To use a different account for deploying the agent inside a specific machine, you can customize credentials for the machine.

To customize credentials:

1. In the **Guest OS credentials** section, select **Customize Credentials**.

2. Select the necessary machine from the list and click **Set User**.
3. Specify custom guest OS credentials and click **OK**.



To remove custom credentials for a machine:

1. In the **Guest OS credentials** section, select **Customize Credentials**.
2. Select the necessary machine from the list and click **Remove**.

> **NOTE**
>
> To customize settings of a machine added as part of a container, the machine should be included in the list as a standalone instance. For that, click **Add machine** and choose a machine whose settings you want to customize.

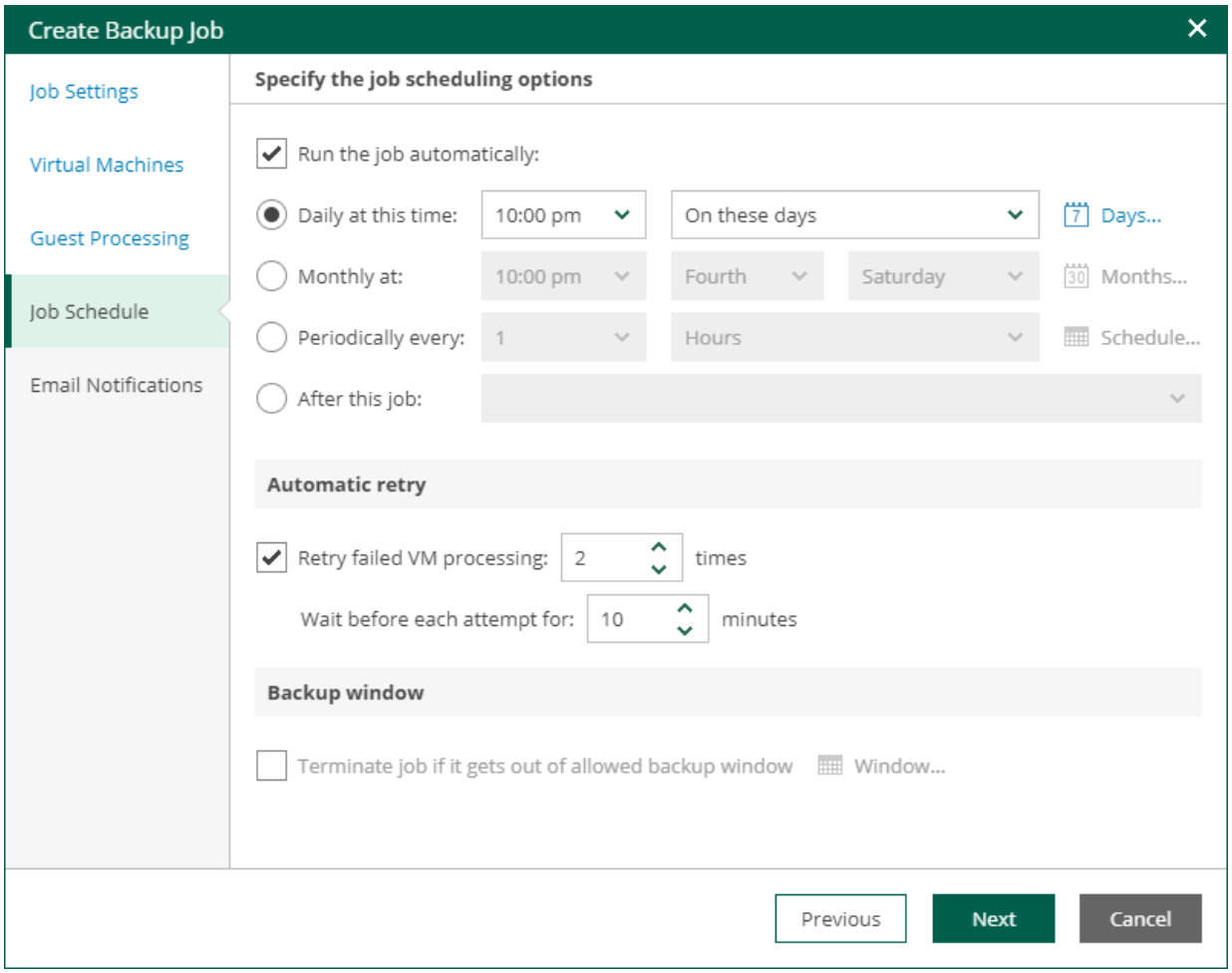
Step 6. Configure Job Schedule

At the **Job Schedule** step of the wizard, you can select to run the job manually or schedule the job to run on a regular basis.

To edit the job schedule:

1. Select the **Run the job automatically** check box. If the check box is not selected, you will need to start the job manually.
2. Edit the scheduling settings. You can select to run the job daily, monthly, periodically with a specific time interval, continuously or after a specific job.

   For more information, see Schedule Settings.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication must attempt to run the backup job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed machines only. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job runs.
4. In the **Backup window** section, edit the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not provide unwanted overhead on the production environment. To set up a backup window for the job:
   a. Select the **Terminate job if it gets out of allowed backup window** check box and click **Window**.
   b. Define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.



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

Schedule Settings

If you have selected to run the job automatically, you can select one of the following options:

- To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
- To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

  > **NOTE**
  >
  > When you configure the job schedule, keep in mind possible date and time changes (for example, related to daylight saving time transition).

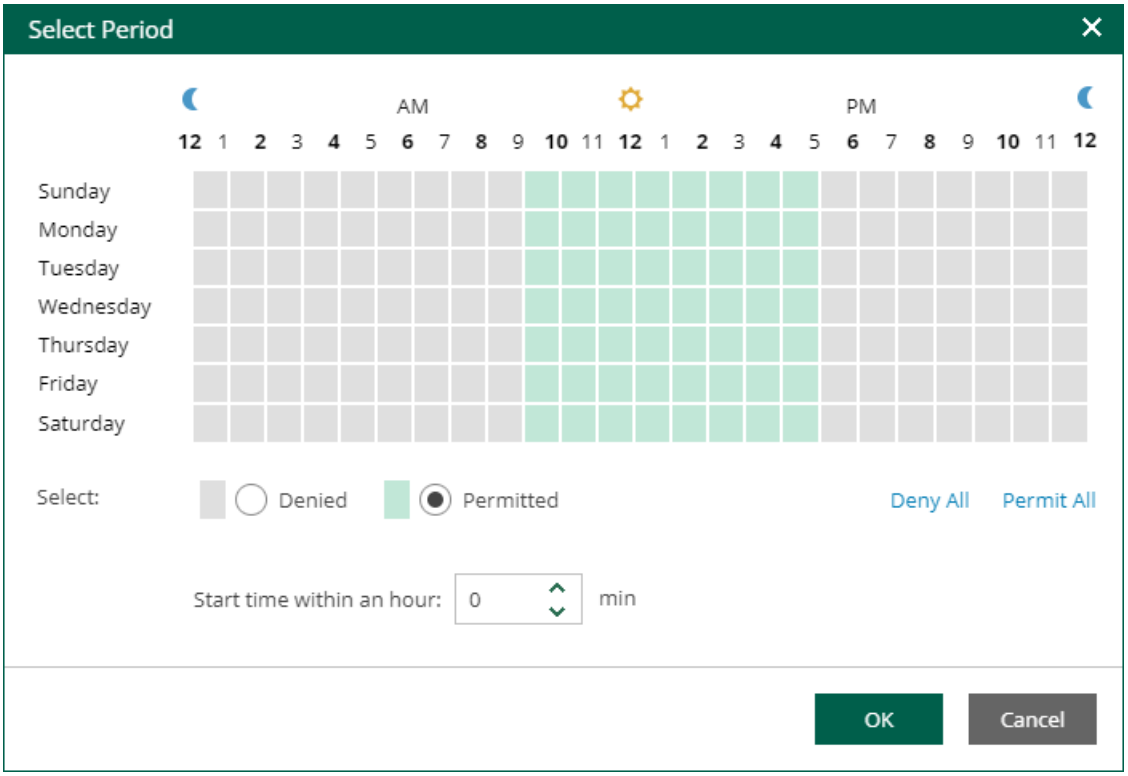
- To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

  A repeatedly run job is started by the following rules:

  - Veeam Backup & Replication always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.

- If you define permitted hours for the job, after the denied interval is over, Veeam Backup & Replication will immediately start the job and then run the job by the defined schedule.

For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.



- To run the job continuously, select the **Periodically every** option and choose **Continuously** from the drop-down list on the right. A new backup job session will start as soon as the previous backup job session finishes.
  - To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list. If you start the first job manually, Veeam Backup Enterprise Manager will display a notification. You will be able to choose whether to start the chained job as well.

Step 7. Configure Email Notifications

At the **Email Notifications** step, you can configure email notifications.

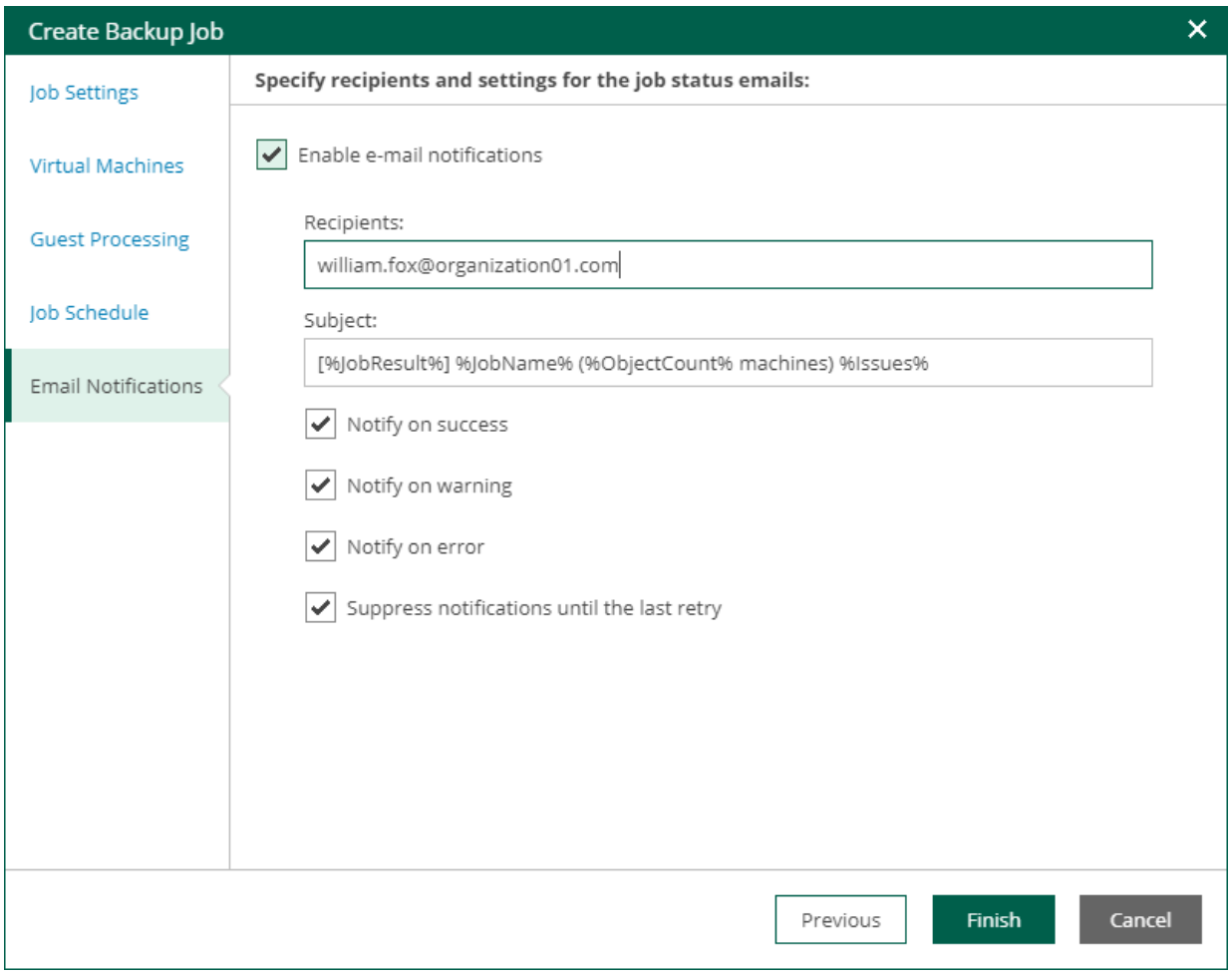
Email notifications will be sent daily if you configure global notification settings in Veeam Backup Enterprise Manager. For more information, see Notifications on Job Results. If you want to receive a notification after each job run, configure notification setting for this job in Veeam Backup & Replication. For details, see the Notification Settings section of the Veeam Backup & Replication User Guide.

To configure email notifications for this job, take the following steps:

1. Select the **Enable e-mail notifications** check box if you want to receive notifications about the job completion status by email.
2. In the **Recipients** field, specify recipient's email address. You can enter several addresses separated by a semicolon.
3. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of VMs in the job) and *%Issues%* (number of VMs in the job that have finished with the Warning or Failed status).
4. Select **Notify on success** to receive an email notification when the job completes successfully.
5. Select **Notify on warning** to receive an email notification when the job completes with a warning.
6. Select **Notify on error** to receive an email notification when the job fails.
7. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.

8. To create the job, click **Finish**.

   Other job settings are obtained from the job configuration specified for the organization. For more information, see Adding Organization Configuration.

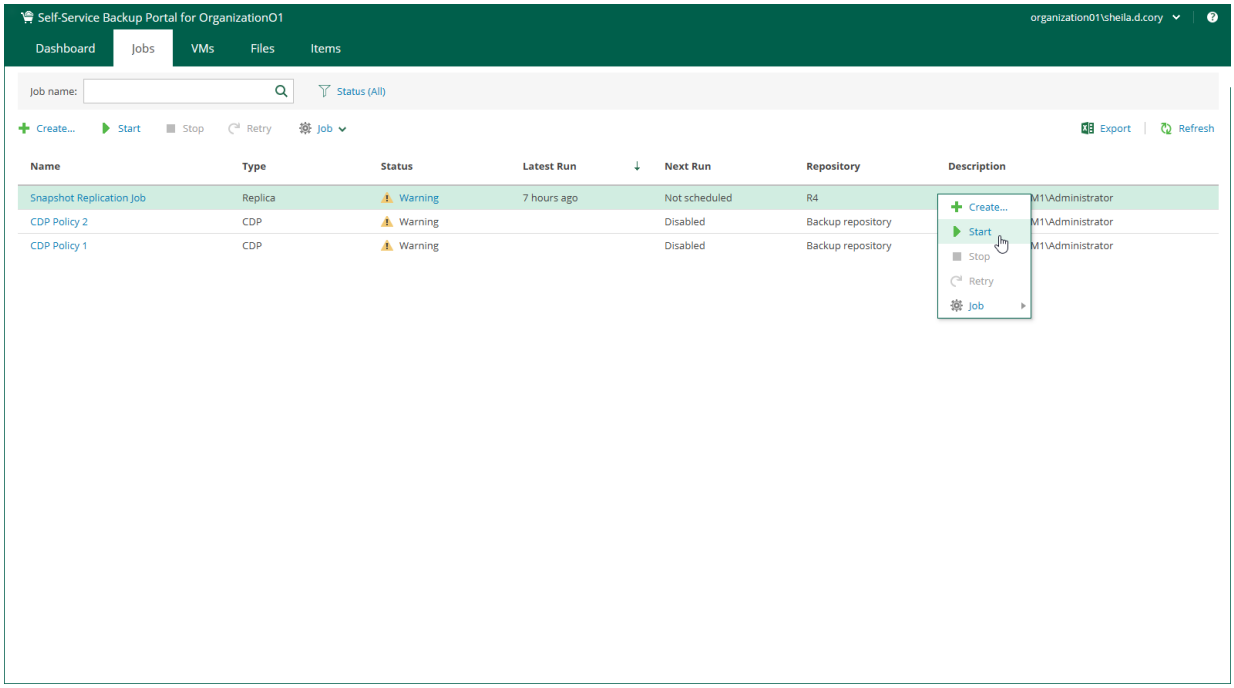


Starting, Stopping and Retrying Jobs

Members of a VMware Cloud Director organization can start, stop and retry organization backup jobs and replication jobs.

- To start a job, right-click a job from the list and select **Start**.
- To stop a job, right-click a job from the list and select **Stop**.

- To retry a failed job, right-click a job from the list and select **Retry**.



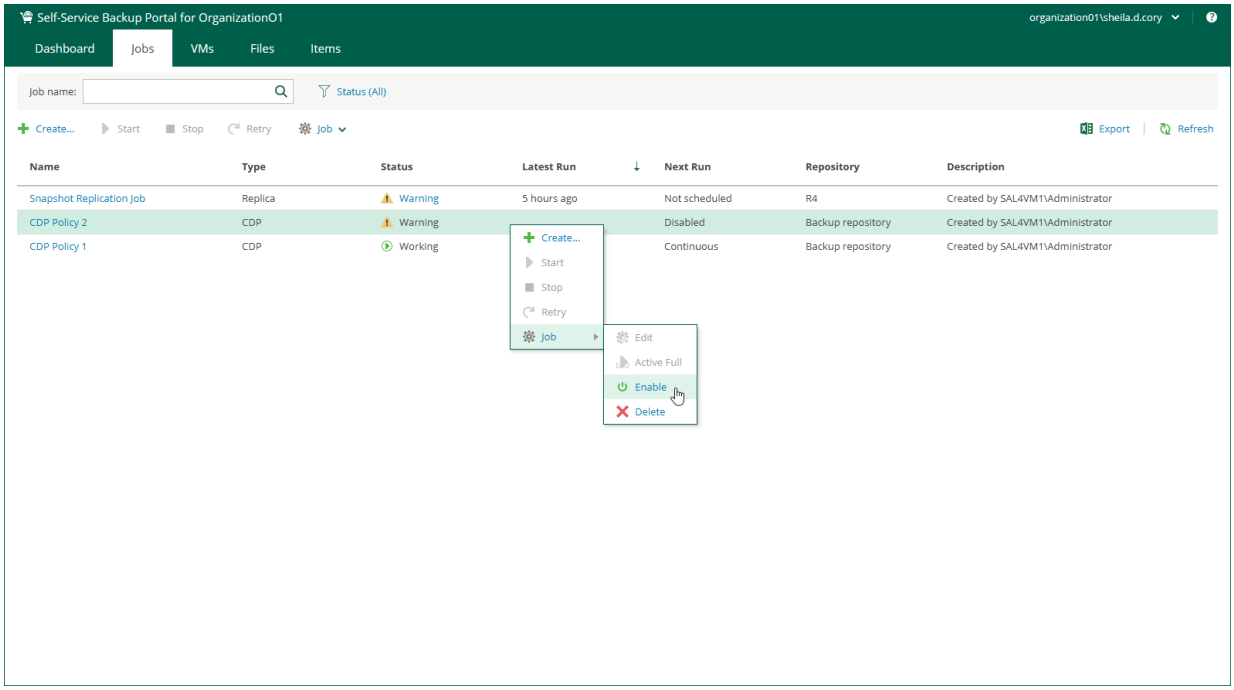
Enabling and Disabling Jobs and Policies

Members of a VMware Cloud Director organization can enable and disable organization backup jobs, replication jobs and CDP policies. Disabled jobs and policies are temporary paused.

To enable or disable a policy:

1. On the **Jobs** tab, select a job or policy from the list.
2. On the toolbar, click **Enable** or **Disable**.

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



Deleting Jobs and Policies

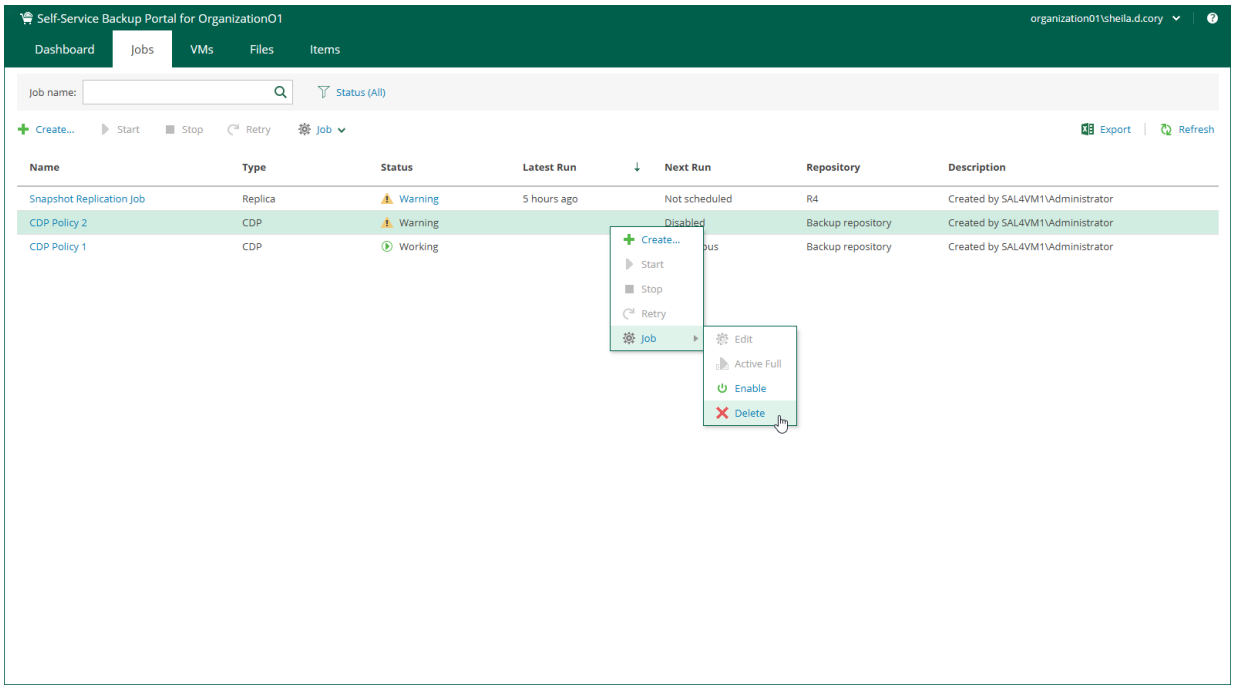
Members of a VMware Cloud Director organization can delete organization backup jobs, replication jobs and CDP policies. Deleted jobs and policies are removed and no longer appear in Veeam Self-Service Backup Portal, Veeam Backup & Replication console and in Veeam Backup Enterprise Manager.

To delete a job, do the following:

1. On the **Jobs** tab, select a job from the list.
2. On the toolbar, click **Job** > **Delete**.

   Alternatively, you can right-click a job or policy and select **Job** > **Delete**.
3. You will be prompted to delete backup files. To delete backup files, select the **Delete backup files** check box and click **Yes** to confirm the operation.

   If four-eyes authorization is enabled on the backup server, backup files will remain in the backup repository and become orphaned.



Managing Cloud Director VMs and vApps

On the **VMs** tab, members of a VMware Cloud Director organization can perform the following tasks:

- Browse VMs and vApps
- Recover VMs
- Restore vApps
- Fail over vApps to their snapshot or CDP replicas
- Restore VM disks
- Delete VMs and vApps from Backups

VM Recovery

You can recover VMs from backups to the original (production) vApp or another vApp within you organization.

You can perform the following types of VM recovery:

- Instant Recovery
- Entire VM Restore

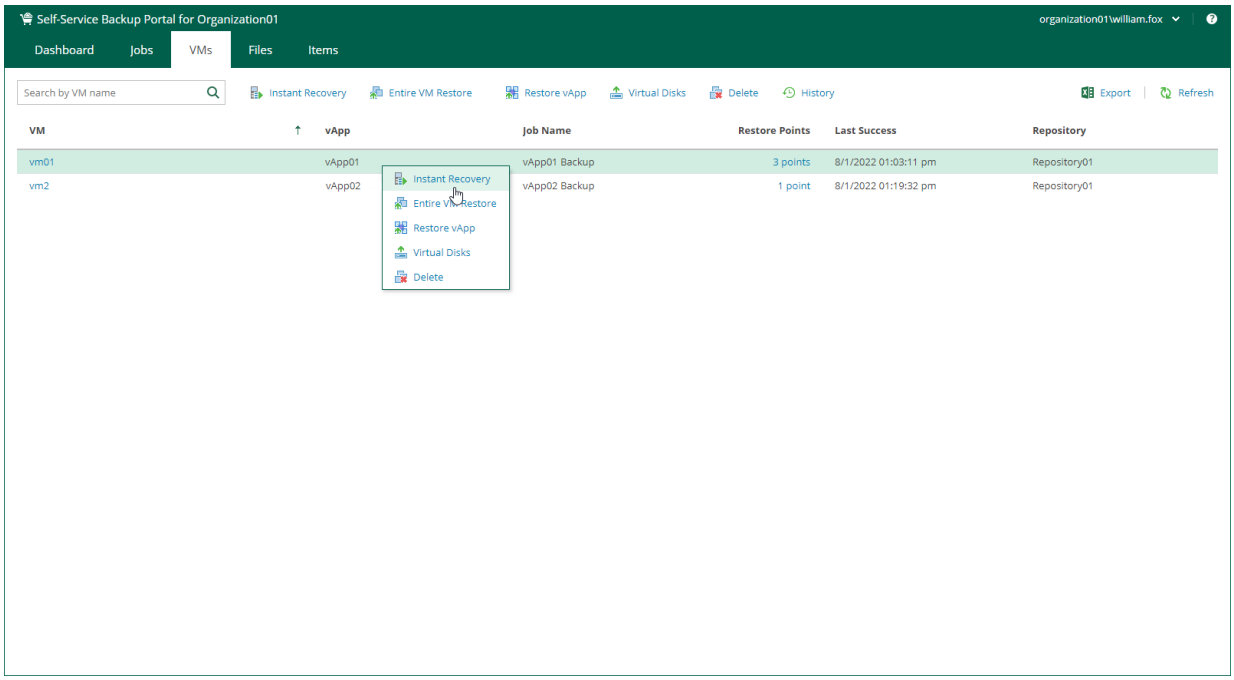
Instant Recovery

You can instantly recover VMware Cloud Director VMs from backups to the original vApp or another vApp that belongs your VMware Cloud Director organization.

To instantly recover a VM, do the following:

1. On the **VMs** tab, select a VM you want to recover. To quickly find the necessary VM, use the search field at the top of the window.
2. On the toolbar, click **Instant Recovery**.

   Alternatively, you can right-click the VM and select **Instant Recovery**.
3. Follow the steps of the **Instant Recovery** wizard. For more information, see Instant Recovery to VMware Cloud Director.



Entire VM Restore

You can restore VMware Cloud Director VMs from backups to the original vApp or another vApp that belongs your VMware Cloud Director organization.

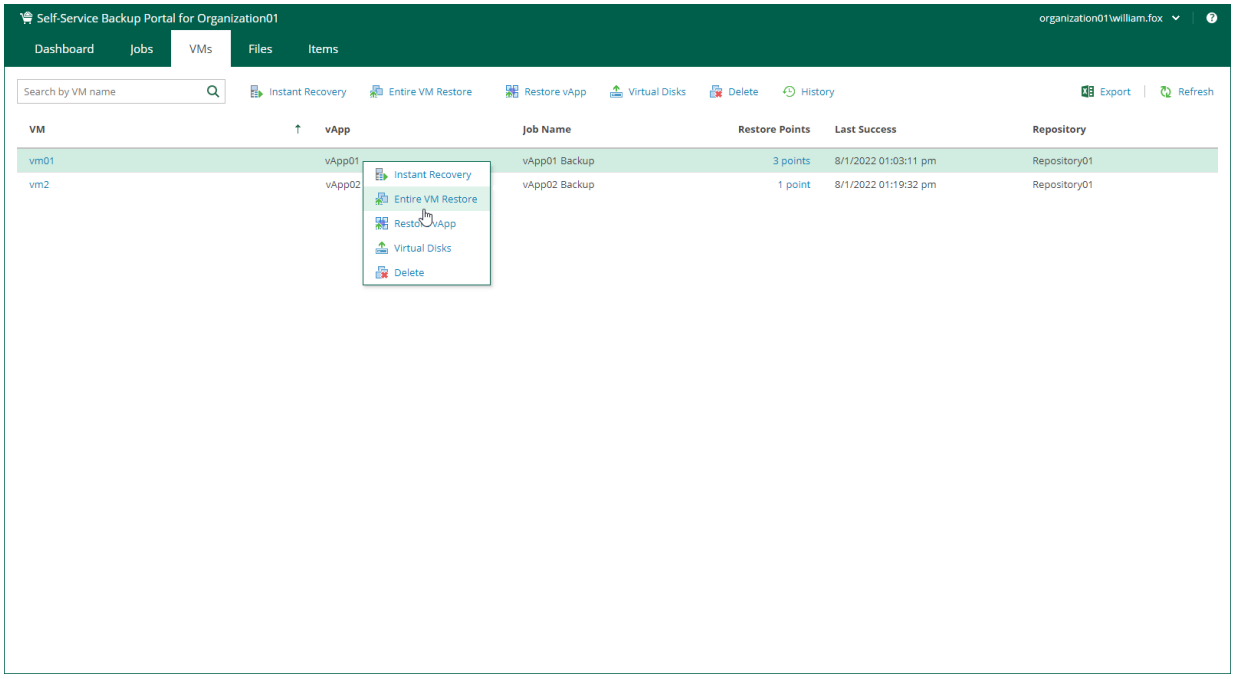
To restore an entire VM, do the following:

1. On the **VMs** tab, select a VM you want to restore. To quickly find the necessary VM, use the search field at the top of the window.

2. On the toolbar, click **Entire VM Restore**.

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

3. Follow the steps of the **Entire VM Restore** wizard. For more information, see Restoring Entire VM to VMware Cloud Director.



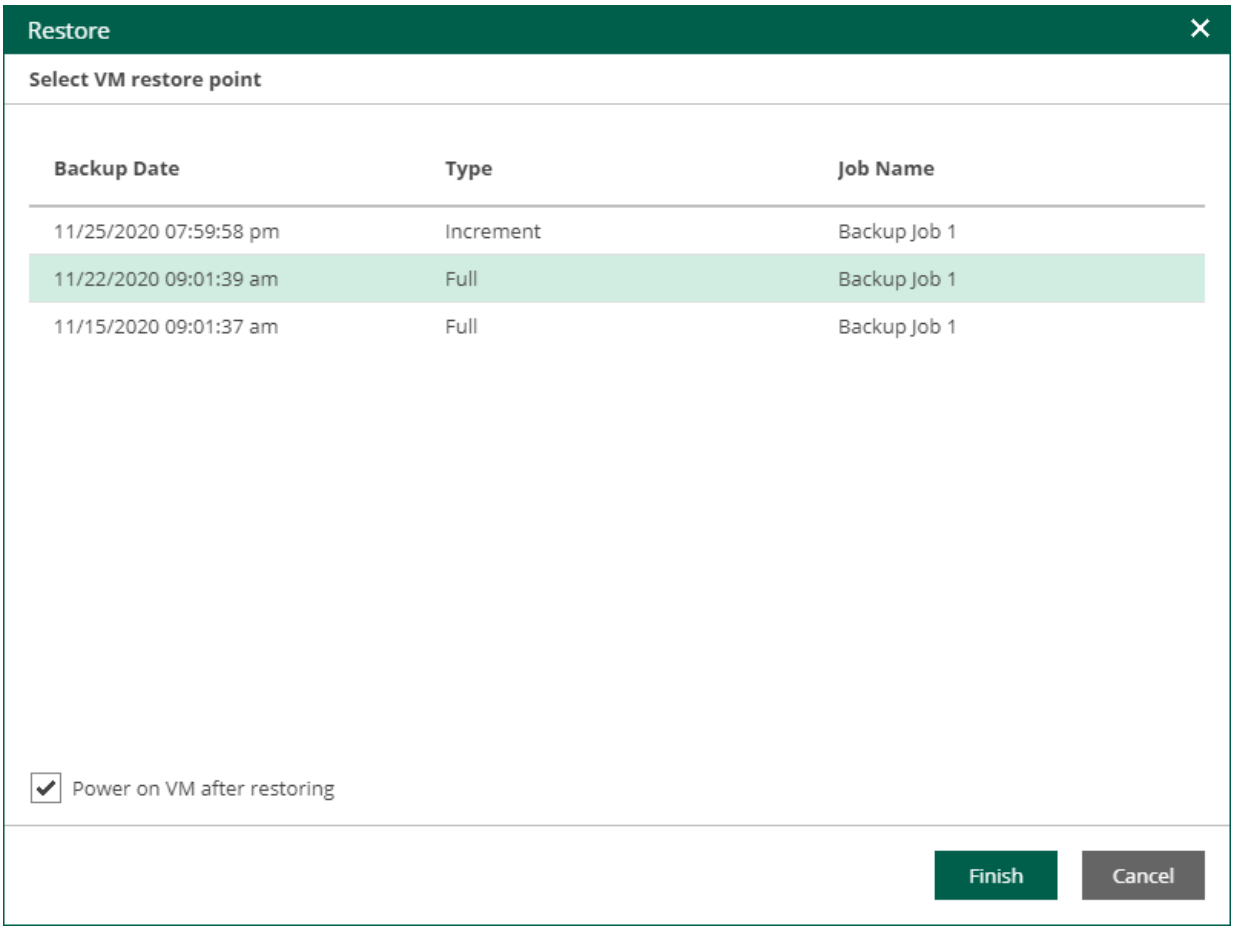
Restoring vApps

You can restore a vApp to the original (production) VDC.

To restore a vApp:

1. On the **VMs** tab, select a vApp. To quickly find the necessary vApp, use the search field at the top of the window.
2. Click **Restore vApp** and select the option you need:
   - Select **Overwrite** if you want to restore the vApp from the backup to the original VDC, replacing the production vApp.
   - Select **Keep** if you want to keep the original vApp in the original VDC. The vApp from the backup will be located next to the original production vApp and will have the same name with the *_restored* suffix. Names of VMs in the vApp will remain the same.
3. Select the restore point that will be used to restore the vApp.

4. [Optional] To start VMs in the restored vApp immediately after recovery, select **Power on VM after restoring**.



5. Click **Finish**.
6. Click **Yes** in the message window to confirm the operation.

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

> **IMPORTANT**
>
> Restore job of a vApp with a standalone VM will return an ordinary and not standalone VM.

vApp Failover

Failover is a process of switching from the original vApp in the production site to its vApp replica in the disaster recovery site.

Failover is an intermediate step that your service provider must finalize in the Veeam Backup & Replication console. The service provider can perform the following operations in the console:

- Undo failover to switch back to the source vApp and discard all changes made to the replica while it was running.
- Perform permanent failover to permanently switch from the source vApp to the replica and use this replica as the production vApp.
- Perform failback to switch back to the source vApp and send to the source vApp all changes that took place while the replica was running.

For more information on finalizing failover, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

You can perform the following failover operations in Veeam Self-Service Backup Portal:

- Failover to Snapshot Replica
- Failover to CDP Replica

Failover to Snapshot Replica

If a VM is processed by a VMware Cloud Director replication job, you can perform failover of the vApp that contains the VM. When you perform failover, you shift all processes from the source vApp in the production organization VDC to the replica in the disaster recovery organization VDC.

Failover is an intermediate step that your service provider must finalize in the Veeam Backup & Replication console. The service provider can perform the following operations in the console:

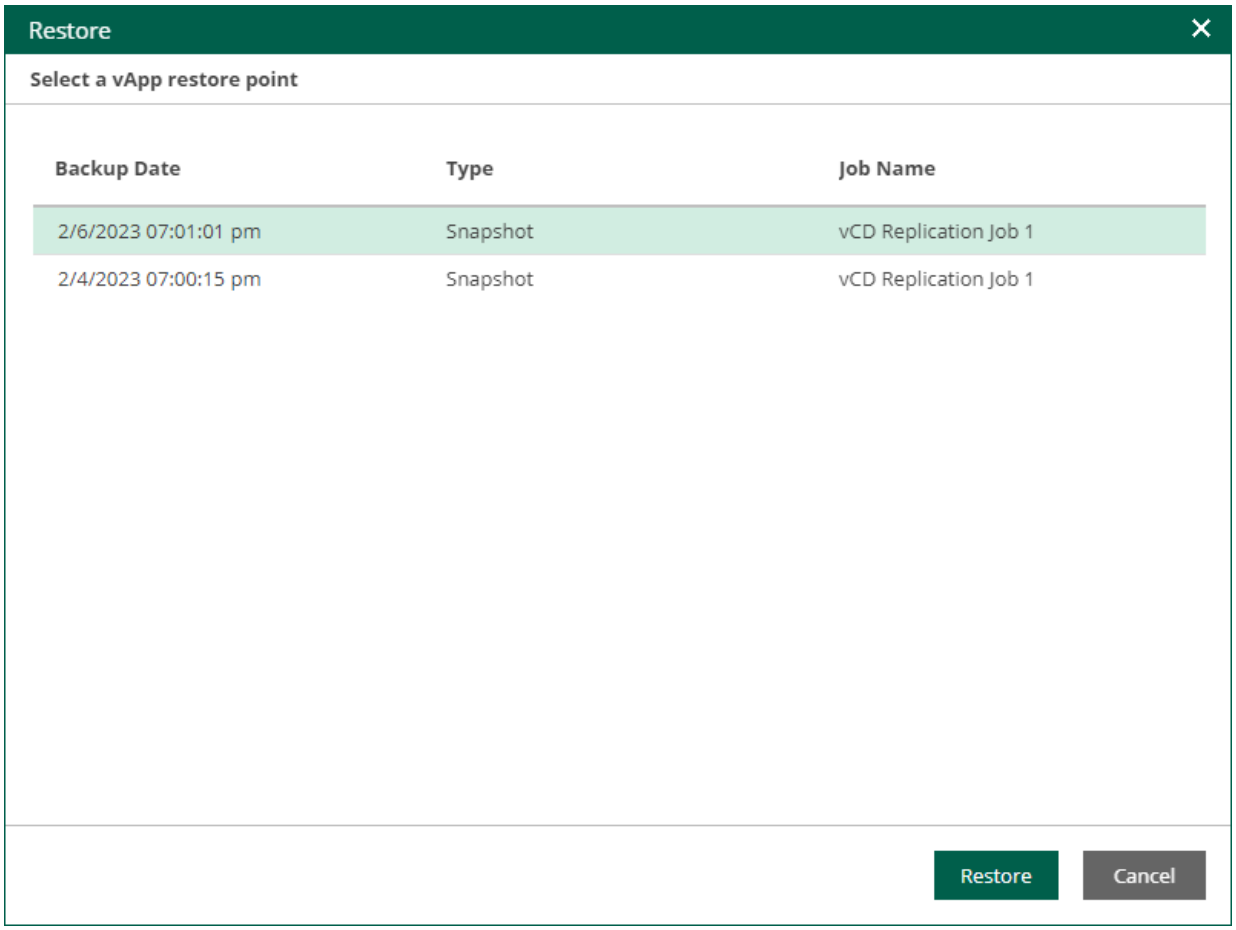
- Undo failover to switch back to the source vApp and discard all changes made to the replica while it was running.
- Perform permanent failover to permanently switch from the source vApp to the replica and use this replica as the production vApp.
- Perform failback to switch back to the source vApp and send to the source vApp all changes that took place while the replica was running.

For more information on finalizing failover, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover, take the following steps:

1. On the **Machines** tab, select a machine processed by a Cloud Director replication job.
2. Click **Restore vApp**.
3. In the **Restore** window, select a restore point of the vApp.
4. Click **Restore**.
5. To confirm failover, click **Yes**.

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



Failover to CDP Replica

If a VM is processed by a VMware Cloud Director CDP policy, you can perform failover of the vApp that contains the VM. When you perform failover, you shift all processes from the source vApp in the production organization VDC to the replica in the disaster recovery organization VDC.

Failover is an intermediate step that your service provider must finalize in the Veeam Backup & Replication console. The service provider can perform the following operations in the console:

- Undo failover to switch back to the source vApp and discard all changes made to the replica while it was running.
- Perform permanent failover to permanently switch from the source vApp to the replica and use this replica as the production vApp.
- Perform failback to switch back to the source vApp and send to the source vApp all changes that took place while the replica was running.

For more information on finalizing failover, see the Failover and Failback section of the Veeam Backup & Replication User Guide.

To perform failover, do the following:

1. On the **Machines** tab, select a machine processed by a Cloud Director CDP policy.
2. Click **Restore vApp**.

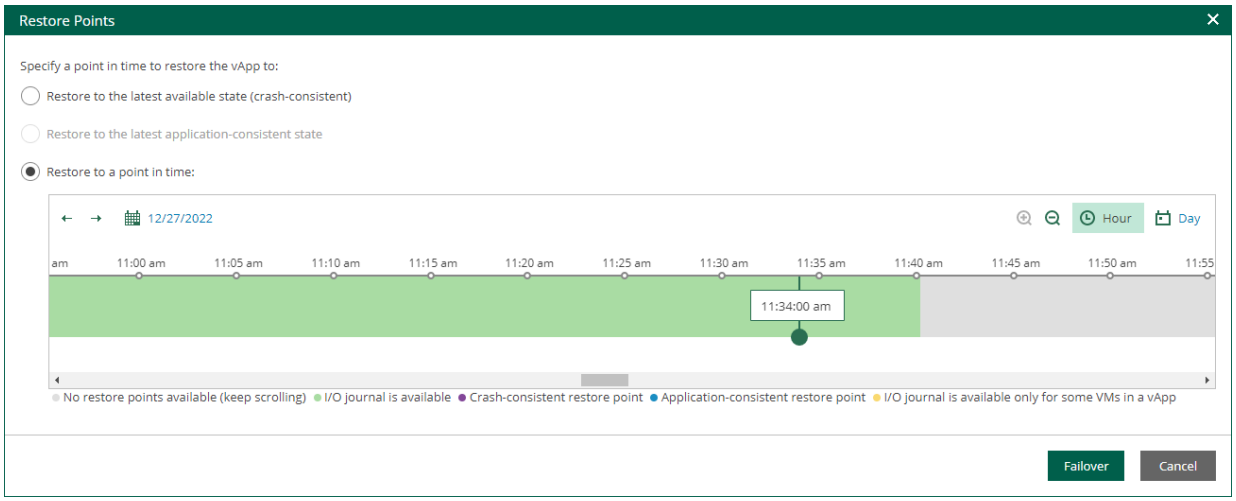
3. In the **Restore Points** window, select the restore point you need. You can fail over to the latest available crash-consistent state, to the latest application-consistent state, or to a specific point in time.

   Application consistency is defined for the whole vApp. A vApp restore point is application-consistent if all VMs have application-consistent restore points. A vApp restore point is mixed if some VMs have crush-consistent restore points.

   > **TIP**
   > - To quickly find a long-term restore point, use the calendar.
   > - To zoom in or zoom out the time line, use the **Plus** and **Minus** buttons or switch between the **Hour** and **Day** views.

4. Click **Failover**.

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



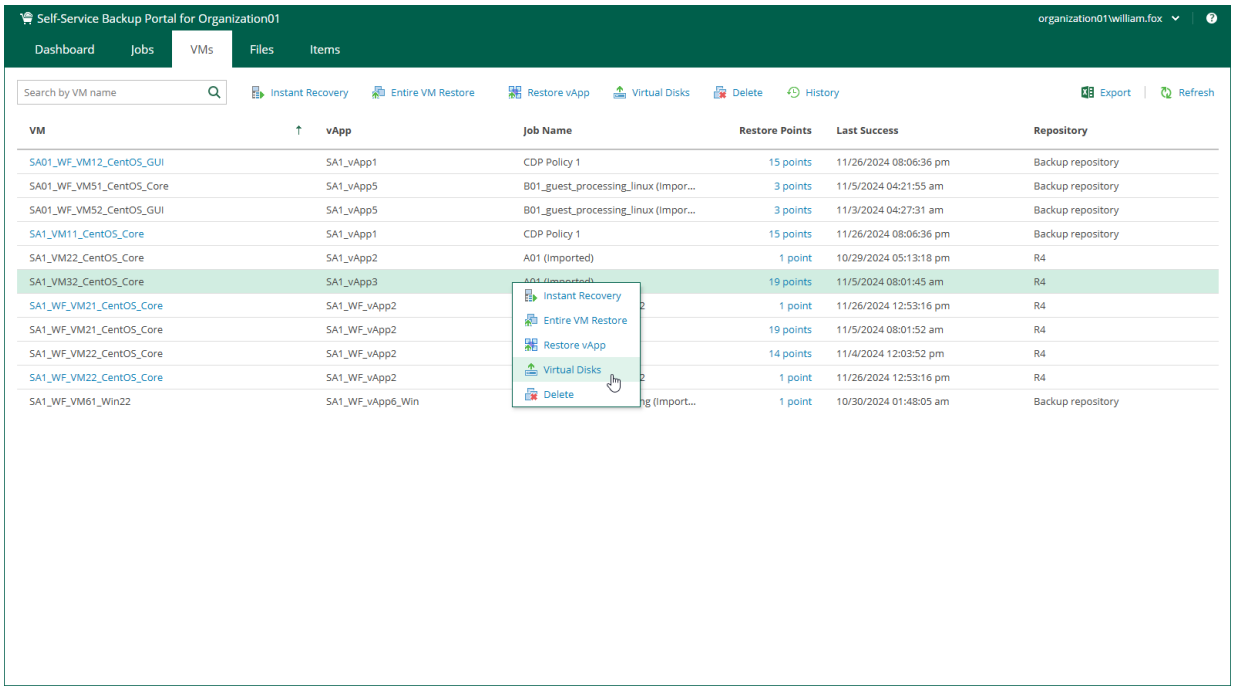
Restoring Virtual Disks

You can restore individual virtual disks from backups of VMware Cloud Director VMs.

To restore a virtual disk:

1. On the **VMs** tab, select a VM with disks you want to restore. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Virtual Disks**.

3. Follow the steps of the **Virtual Disk Restore** wizard. For details, see Virtual Disk Restore.



Deleting VMs and vApps from Backups

If you no longer need a VM backup, you can delete it. The deleted VM is not removed from the list of VMs immediately. The VM will be removed from the list after the VM records are removed from the configuration database of the backup server.

Before You Begin

Before you delete a machine from backup, consider the following considerations and limitations:

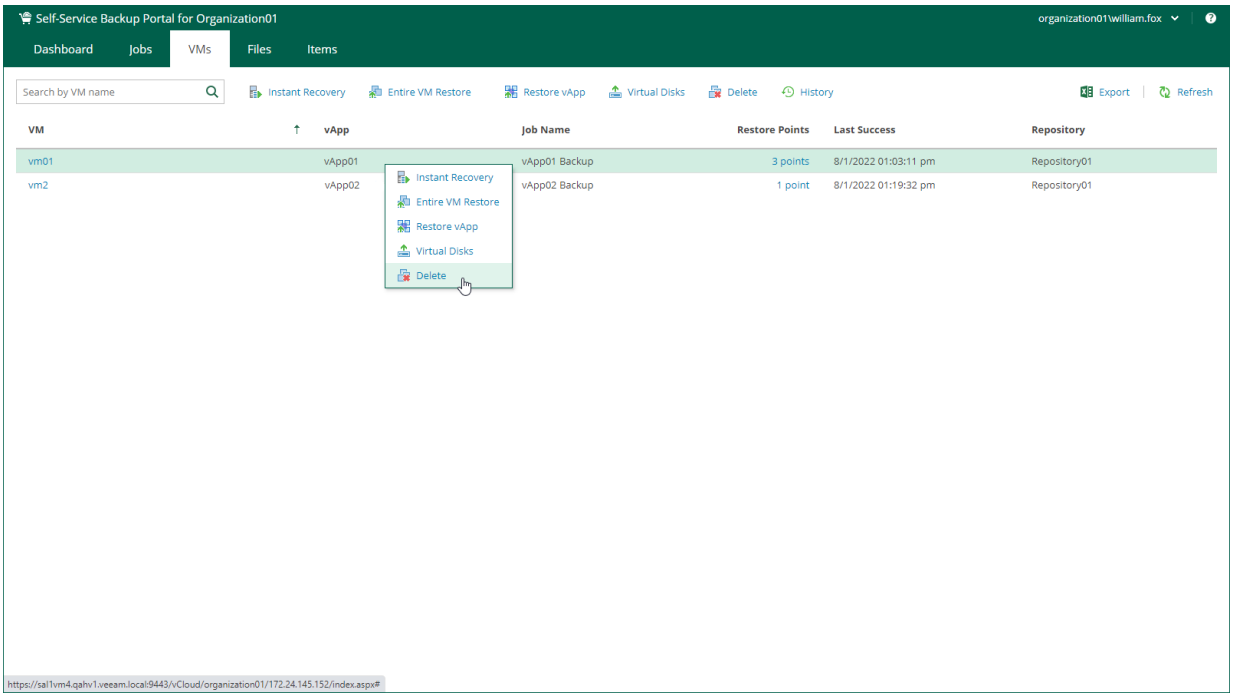
- If four-eyes authorization is enabled on the backup server, you cannot delete a VM backup using either Veeam Self-Service Backup Portal or Enterprise Manager.
- If the selected VM is the last one in its vApp, the VM will be deleted from the backup with its vApp. If this vApp is the last one in its backup, the whole backup will be deleted.
- If you delete a VM that has GFS backups, they will not be deleted. You can delete them in Enterprise Manager. For more information, see Deleting Machine from Backup.
- When you remove data of deleted VMs from per-VM backup chains, it does not mark the space as available but deletes backup files since they contain data for one VM only. When you remove data of deleted VMs from regular backup chains, the space is not freed up on the backup repository. It is marked as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.

Deleting VMs

To delete a VM, do the following:

1. On the **VMs** tab, select a VM. To quickly find the necessary VM, use the search field at the top of the window.
2. Click **Delete**.

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



Restoring Guest OS Files

Members of a VMware Cloud Director organization can browse the VM file system, search for specific files and restore them. As a source, you can use a VM backup or snapshot replica. Both indexed and non-indexed guest OS file systems are supported.

To restore guest OS files, open the the **Files** tab and follow the steps described in Performing 1-Click File Restore.

> **NOTE**
>
> - When you restore from non-indexed guest OS file system, mount operation is performed using mount server associated with the backup repository that stores the backup file.
> - Before you restore files from a non-Windows VM, make sure that a helper host or helper appliance is configured on the backup server. For more information, see Preparing for File Search and Restore (non-Windows machines).

Restoring Application Items

On the **Items** tab, members of a VMware Cloud Director organization can perform item-level recovery of Microsoft SQL Server databases, Oracle databases and PostgreSQL instances from application-aware backups. For more information, see the following sections:

- Restoring Microsoft SQL Server Databases
- Restoring Oracle Databases
- Restoring PostgreSQL Instances

Getting Support

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

- Search for information on the required topic in the current Veeam Backup Enterprise Manager User Guide or across Veeam Help Center.
- Explore troubleshooting guides, best practices and other articles that address specific practical or technical issues in Veeam Knowledge Base.
- Watch product demos to learn more about Veeam solutions.
- Visit Veeam R&D Forums and share your opinion or ask a question.
- Submit a support case to Veeam Customer Support. In your support request, include all Enterprise Manager logs. For more information on how to collect log files, see Enterprise Manager Logs.

Enterprise Manager Logs

Veeam Backup Enterprise Manager provides detailed logging of performed activities, data protection and disaster recovery tasks. You can use Enterprise Manager logs to submit a support ticket at the Veeam Customer Support Portal.

Downloading Enterprise Manager Logs

To ensure that Veeam Customer Support receives complete diagnostic information, include all log files when submitting a support ticket.

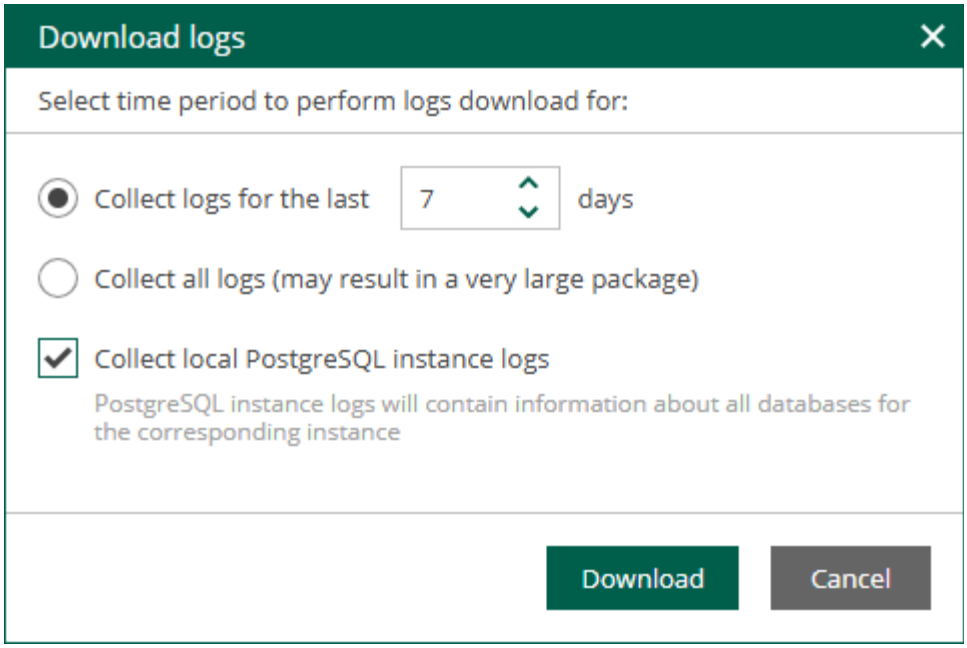
> **NOTE**
>
> If you use Enterprise Manager on Linux, you can download the entire Veeam Software Appliance log bundle using Veeam Host Management. For details, see Performing Maintenance Tasks.

To download all Enterprise Manager logs, perform the following steps:

1. Log in to Enterprise Manager using an administrative account.
2. To open the **Configuration** view, click **Configuration** in the upper-right corner.
3. Open the **About** section on the left of the **Configuration** view.
4. Click **Download support logs**.
5. Choose the time interval for which logs must be collected. You can select one of the following options:
   - Collect logs for the last N days
   - Collect all available logs

6. [Optional] Select **Collect local PostgreSQL instance logs** to include logs from the Enterprise Manager configuration database stored in a local PostgreSQL instance. The logs will contain information about all databases contained on the selected instance.

   The option is not available if the Enterprise Manager configuration database is located remotely or if the database is based on the Microsoft SQL Server engine.



Log Files Location

Log files are stored on the Enterprise Manager server in the following locations:

- Linux-based Enterprise Manager (Veeam Software Appliance):
  - Enterprise Manager logs:

    ```
    /var/log/VeeamBackup
    ```

  - Nginx logs for the Enterprise Manager web application.

    ```
    /var/log/nginx
    ```

  - Veeam Host Management logs:

    ```
    /var/log/veeam/veeam_hostmanager
    ```

  - Veeam Updater logs:

    ```
    /var/log/veeam/veeam-updater
    ```

- Microsoft Windows-based Enterprise Manager:

```
C:\ProgramData\Veeam\Backup
```

Enterprise Manager components generate the following primary log files. For more information on the components, see Enterprise Manager Components.

Logs	Description	Linux	Microsoft Windows
Svc.Identity.EM.log	Veeam Enterprise Manager Identity Service logs.	✔	✔
Svc.VeeamBES.log	Main Veeam Backup Enterprise Manager Service logs.	✔	✔
Svc.VeeamBES.Collect.log	Veeam Backup Enterprise Manager Service log for data collection.	✔	✔
Svc.VeeamCatalog.log	Main Veeam Catalog Service logs.	✔	✔
Svc.Veeam.EM.RestAPI.log	Veeam Backup Enterprise Manager REST API logs.	✔	✔
Veeam.RemotePlugin.log	Veeam Plug-in for VMware vSphere Client Service logs.	✔	✔
Veeam.WebApp.log	Veeam Backup Enterprise Manager web application logs.	✔	✔
/var/log/nginx	Nginx logs for the Veeam Backup Enterprise Manager web application.	✔	✘
/var/log/veeam/veeam_hostmanager	Veeam Host Management logs.	✔	✘
/var/log/veeam/veeam-updater	Veeam Updater logs.	✔	✘