Veeam Explorers

Version 12

User Guide

June, 2023

© 2023 Veeam Software.

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

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

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

Contents

CONTACTING VEEAM SOFTWARE 10
ABOUT THIS DOCUMENT 11
VEEAM EXPLORERS OVERVIEW 12
VEEAM EXPLORER FOR MICROSOFT ACTIVE DIRECTORY 13
Planning and Preparation 14
System Requirements 15
Ports 16
Permissions 17
Required Backup Job Settings 18
Considerations and Limitations 19
Launching Application and Exploring Backups 21
Getting to Know User Interface 22
Browsing, Searching and Viewing Items 24
Enabling Extended Logging 27
Standalone Databases Management 28
Adding Standalone Databases 29
Removing Standalone Databases 30
Data Restore 31
Restoring Objects 32
Restoring Containers 41
Using 1-Click Restore 50
Data Export 53
Exporting Objects 54
Exporting Containers 55
Using 1-Click Export 56
Data Compare 57
Comparing Active Directory Containers 58
Comparing Object Attributes 59
VEEAM EXPLORER FOR MICROSOFT SQL SERVER 60
Planning and Preparation 61
System Requirements 62
Ports 63
Permissions 66
Required Backup Job Settings 67
Considerations and Limitations 68
Launching Application and Exploring Backups 70

Getting to Know User Interface 71
How Mounting Works 73
How Veeam SQL Restore Service Works 74
Viewing Database Information 75
General Application Settings 76
Configuring Staging SQL Server 77
Enabling Extended Logging 79
Standalone Databases Management 80
Adding Standalone Databases 81
Removing Standalone Databases 82
Data Restore 83
Restoring Single Database 84
Restoring Multiple Databases 100
Restoring Database Schema and Data 114
Data Publishing 124
Publishing to Specified Server 125
Publishing Latest or Point-in-Time State 132
Unpublishing Databases 138
Exporting as BAK 139
Refreshing Database Status 140
Instant Recovery 141
How It Works 142
Instant Recovery of Single Database 143
Instant Recovery of Multiple Databases 163
Switchover 183
Managing Instant Recovery Session 186
Data Export 191
Exporting as MDF 192
Exporting as BAK 216
Exporting Database Schema and Data 241
SQL Server Database Operations 250
VEEAM EXPLORER FOR ORACLE 253
Planning and Preparation 254
System Requirements 255
Ports 256
Permissions 259
Required Backup Job Settings 260
Considerations and Limitations 261
Launching Application and Exploring Backups 264

Getting to Know User Interface 265
How Mounting Works 267
Viewing Database Information 268
General Application Settings 270
Configuring Staging Oracle Server 271
Enabling Extended Logging 274
Exploring Oracle Backups 275
Exploring Application-Enabled Backups 276
Exploring Non-Application Enabled Backups 277
Exploring RMAN Backups 282
Data Restore 283
Restoring Single Database and Data Guard 284
Restoring Latest or Point-in-Time State 293
Restoring Multiple Databases 299
Restoring RMAN Backups 311
Data Publishing 323
Publishing to Specified Server 324
Publishing Latest or Point-in-Time State 333
Unpublishing Databases 339
Exporting as RMAN Backup 340
Refreshing Database Status 341
Instant Recovery 342
How It Works 343
Instant Recovery of Multiple Databases 344
Instant Recovery of Latest State 352
Instant Recovery of Point-in-Time State 355
Instant Recovery to Another Server 361
Switchover 372
Managing Instant Recovery Session 374
Data Export 379
Export as RMAN Backup 380
Export Database Files 391
VEEAM EXPLORER FOR POSTGRESQL 402
Planning and Preparation 403
System Requirements 404
Ports 405
Permissions 407
Required Backup Job Settings 408
Considerations and Limitations 409

Launching Application 410
Getting to Know User Interface 411
How Mounting Works 413
Viewing Instance Information 414
Enabling Extended Logging 415
Data Restore 416
Restoring Single Instance 417
Restoring Multiple Instances 430
Data Publishing 440
Publishing to Specified Server 441
Publishing Latest or Point-in-Time State 447
Unpublishing Instances 452
VEEAM EXPLORER FOR MICROSOFT EXCHANGE 453
Planning and Preparation 454
System Requirements 455
Ports 456
Permissions 458
Required Backup Job Settings 460
Considerations and Limitations 461
Launching Application and Exploring Backups 463
Getting to Know User Interface 465
Browsing, Searching and Viewing Items 467
General Application Settings 470
Extensible Storage Engine 471
SMTP Settings 472
Advanced Settings 473
Standalone Databases and External Servers 474
Adding Microsoft Exchange Databases 475
Adding Veeam Backup for Microsoft 365 Server 476
Adding Veeam Backup for Microsoft 365 Service Provider 477
Removing Stores 479
Data Restore 480
Restore to Microsoft 365 Organizations 481
Restore to On-Premises Microsoft Servers 497
1-Click Restore 510
Data Export 519
Exporting to Custom Location 520
Using 1-Click Export 522
Receiving Export Reports 525

Data Compare 527
Compare to Microsoft 365 Organizations 528
Compare to On-Premises Microsoft Servers 532
Saving Microsoft Exchange Items 535
Sending Microsoft Exchange Items 537
VEEAM EXPLORER FOR MICROSOFT SHAREPOINT 539
Planning and Preparation 540
System Requirements 541
Ports 542
Permissions 544
Required Backup Job Settings 546
Staging SQL Server 547
Considerations and Limitations 548
Launching Application and Exploring Backups 556
Getting to Know User Interface 558
Browsing, Searching and Viewing Items 560
General Application Settings 564
Staging SQL Server 565
Custom Lists 567
SMTP Settings 570
Advanced Settings 571
Standalone Databases 572
Adding Microsoft SharePoint Databases 573
Adding Veeam Backup for Microsoft 365 Databases 574
Adding Veeam Backup for Microsoft 365 Server 575
Adding Veeam Backup for Microsoft 365 Service Provider 576
Removing Databases 578
Data Restore 579
Restoring Sites 580
Restoring Document Libraries and Lists 604
Restoring Documents and List Items 627
Data Export 651
Exporting Microsoft SharePoint Data 652
Importing Microsoft SharePoint Data 653
Saving Microsoft SharePoint Documents and Libraries 654
Sending Microsoft SharePoint Documents and Libraries 655
VEEAM EXPLORER FOR MICROSOFT ONEDRIVE FOR BUSINESS 657
Planning and Preparation 658
Launching Application and Exploring Backups 659

Getting to Know User Interface 660
Browsing, Searching and Viewing Items 662
General Application Settings 666
SMTP Settings 667
Advanced Settings 668
Standalone Databases 669
Adding Veeam Backup for Microsoft 365 Databases 670
Adding Veeam Backup for Microsoft 365 Server 671
Adding Veeam Backup for Microsoft 365 Service Provider 672
Removing Organizations 674
Data Restore 675
Restoring Single OneDrive 676
Restoring Multiple OneDrives 681
Data Copy 687
Step 1. Launch Restore Wizard 688
Step 2. Select Authentication Method 689
Step 3. Log In to Microsoft 365 691
Step 4. Specify Target User 692
Step 5. Specify Target Folder 693
Step 6. Specify Restore Options 694
Saving Microsoft OneDrives 695
Saving Microsoft OneDrive Documents and Folders 698
Sending Microsoft OneDrive Data 699
VEEAM EXPLORER FOR MICROSOFT TEAMS 701
Planning and Preparation 702
Ports 703
Permissions 704
Considerations and Limitations 705
Launching Application and Exploring Backups 706
Getting to Know User Interface 707
Browsing, Searching and Viewing Items 709
General Application Settings 714
SMTP Settings 715
Advanced Settings 716
Standalone Databases 717
Adding Veeam Backup for Microsoft 365 Databases 718
Adding Veeam Backup for Microsoft 365 Server 719
Adding Veeam Backup for Microsoft 365 Service Provider 720
Removing Organizations 722

Data Restore 723
Restoring Teams 724
Restoring Channels and Tabs 732
Restoring Posts 739
Restoring Files 745
Data Export 752
Exporting Multiple Posts 753
Exporting Individual Posts 755
Saving Posts 757
Saving Files 759
Sending Posts and Files 761

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

About This Document

This guide provides information on how to use Veeam Explorers that come as part of Veeam Backup & Replication 12 or Veeam Backup for Microsoft 365 7.0 until it is replaced with a newer version of the product.

Intended Audience

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

Veeam Explorers Overview

Veeam Explorers Suite extends the functionality of Veeam Backup for Microsoft 365 and Veeam Backup & Replication and allows you to restore or export your data from backup or replica files.

Veeam Explorers are distributed as part of Veeam Backup for Microsoft 365 and Veeam Backup & Replication, and you do not need to install them separately. You also do not need to purchase any additional license to use Veeam Explorers: the available feature set for each Veeam Explorer depends entirely on the installed edition of Veeam Backup for Microsoft 365 and Veeam Backup & Replication. For information about how to deploy Veeam products, see the following sections:

- Deployment section of the Veeam Backup for Microsoft 365 User Guide
- Deployment section of the Veeam Backup & Replication User Guide

The following table lists all Veeam Explorers that come as part of Veeam Backup & Replication and Veeam Backup for Microsoft 365.

Veeam Explorer	Veeam Backup & Replication	Veeam Backup for Microsoft 365
Veeam Explorer for Microsoft Exchange	✔	✔
Veeam Explorer for Microsoft SharePoint	✔	✔
Veeam Explorer for Microsoft OneDrive for Business	✔	✔
Veeam Explorer for Microsoft Teams	✔	✔
Veeam Explorer for Microsoft Active Directory	✔	✖
Veeam Explorer for Microsoft SQL Server	✔	✖
Veeam Explorer for Oracle	✔	✖
Veeam Explorer for PostgreSQL	✔	✖

This document provides information on how to use Veeam Explorers that come as part of Veeam Backup & Replication. For information on Veeam Explorers available with Veeam Backup for Microsoft 365 only, see the Veeam Explorers User Guide for Veeam Backup for Microsoft 365.

Veeam Explorer for Microsoft Active Directory

Veeam Explorer for Microsoft Active Directory allows you to restore and export Active Directory objects and containers from backups created by Veeam Backup & Replication.

Planning and Preparation

Before you start using Veeam Explorer for Microsoft Active Directory, make sure your backup infrastructure meets the following requirements and limitations.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft Active Directory.

Component	Requirement
Microsoft Active Directory Domain Services	For more information about supported operating systems, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

Consider the following:

- Veeam Explorer for Microsoft Active Directory does not support Active Directory Lightweight Directory Services (AD LDS).
- Database files created by the domain controller can be opened for object recovery with Veeam Explorer for Microsoft Active Directory only if Veeam Explorer for Microsoft Active Directory is installed on a Windows machine with the same OS version or later than the version of the domain controller OS.
- To open database files, Veeam Explorer for Microsoft Active Directory uses a service dynamic link library (`esent.dll`) which is installed with Microsoft Active Directory Domain Services and can be found in the `%SystemRoot%` directory. The `Esent.dll` file on a machine with Veeam Explorer for Microsoft Active Directory must be of the same version as that of Microsoft Active Directory Domain Services that was used to create database files.

Ports

The following table lists network ports that must be opened to manage inbound and outbound traffic.

From	To	Protocol	Port	Notes
Backup server, Veeam Backup & Replication console	Microsoft Active Directory machine	TCP	135	Manages communication between the domain controller and the backup server.
		TCP, UDP	389	Utilized for LDAP connections.
		TCP	636, 3268, 3269	
		TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	The dynamic RPC range that is used by the runtime coordination process which is deployed on the Microsoft Active Directory machine for application-aware image processing (when working over the network, not over VIX API). For more information, see this Microsoft article.

Permissions

The account used to restore Microsoft Active Directory data must be a member of the following groups:

- *Domain Admins*
- *Exchange Organization Management*

  Membership in this group is required only for restore of Exchange attributes.

Assigning Role with PowerShell

To assign the **Organization Management** role using PowerShell, run the following cmdlet.

```
Add-RoleGroupMember "Organization Management" -Member "<user_name>"
```

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft Active Directory.

General

- When Veeam Explorer for Microsoft Active Directory is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft Active Directory does not support restore using PowerShell Direct, VIX API or vSphere Automation API.
- Data can only be restored back to the original domain. Cross-domain restore is not supported.
- Veeam Explorer for Microsoft Active Directory does not support recovery of the contents of the *Domain Controllers* container and most of the contents of the *System* container (in particular, the *Password Settings* container), as this may cause system stability issues on the target machine. Moreover, some of the contents of the *System* container, as well as the entire *Configuration Partition* container, the *Microsoft Exchange System Options* container, the *Integrated DNS* container and so on, can be recovered with Veeam Explorer for Microsoft Active Directory, but they are only visible in the **Advanced Features** view to prevent accidental errors during the recovery process. For more information, see the Browsing, Searching and Viewing Items section.
- Veeam Explorer for Microsoft Active Directory supports restore of both mailbox-enabled objects (including *hard-deleted items* and *Online Archives*), and *mail-enabled objects* for the following Microsoft Exchange versions: *Microsoft Exchange Server 2019*, *Microsoft Exchange Server 2016*, *Microsoft Exchange Server 2013* and *Microsoft Exchange Server 2010 SP1*. For other Microsoft Exchange versions, restore of *mailbox-enabled* objects is not supported (only *mail-enabled* objects can be restored).
- To restore passwords, Veeam Explorer for Microsoft Active Directory uses the registry database. To restore passwords, make sure the *System* registry hive is available. The default location of the hive is *%systemroot%|System32|Config*. When restoring an Active Directory database from the Active Directory backup using *Veeam file-level restore*, the registry hive will be located automatically. When restoring from an imported backup or from VeeamZIP backups, make sure that the system registry hive and the *.dit* file are located in the same directory.
- If you plan to restore database items from an *Active Directory Domain Services* server running *Microsoft Windows ReFS*, make sure that the backup server or Veeam Backup & Replication console is installed on a machine that runs Microsoft Windows Server 2012 or later.

  To restore from a server running Microsoft Windows ReFS 3.x, the Veeam Backup & Replication console must be installed on a machine that runs Microsoft Windows Server 2016 or later, and the ReFS version must be supported on this machine.
- Restore of *Group Policy objects*, *AD-integrated DNS records* and objects from the *Configuration Partition* is supported in the *Enterprise* and *Enterprise Plus* editions only.
- Veeam Explorer for Microsoft Active Directory does not restore object attributes such as *objectSID* and *objectGUID* from the backup. To restore deleted Active Directory objects, Veeam Explorer for Microsoft Active Directory uses existing tombstone objects on the target Active Directory server or objects in the AD Recycle Bin. In this case, the restored object will have its original *objectSID* and *objectGUID*. If an object you want to restore does not exist in the tombstone container or recycle bin in the target domain, Active Directory will assign new *objectSID* and *objectGUID* attributes to the restored object.

- To restore business-critical objects for which the tombstone object is missing, you can perform authoritative restore of the entire domain from the old DC backups. For more information on tombstone objects, see this Microsoft article.
- Always use backups that are newer than the tombstone lifetime interval for the Active Directory forest. To determine a tombstone lifetime interval, you can use *ADSIEdit* or *Dsquery*. For more information, see this Microsoft article.
- When you move an object from one domain to another within a forest (for example, using the *Movetree.exe* utility or any other 3rd party tool), no tombstone for this object will remain in the source Active Directory; such an object cannot be fully recovered to the original domain.

Export

- Veeam uses *Lightweight Data Interchange Format* to save Active Directory objects and containers to *.ldf* files. You can make an *.ldf* file available to the Active Directory Domain Services server by importing it with the *ldifde* utility. For more information, see this Microsoft article.
- Veeam Explorer for Microsoft Active Directory does not support exporting passwords.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Active Directory and load backups, you can use any of the following methods:

- Use the **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start**, click **Veeam Explorer for Microsoft Active Directory** and manually open Active Directory databases, as described in the Adding Standalone Microsoft Active Directory Databases section.

When starting the application from the **Start** menu, specify the following:

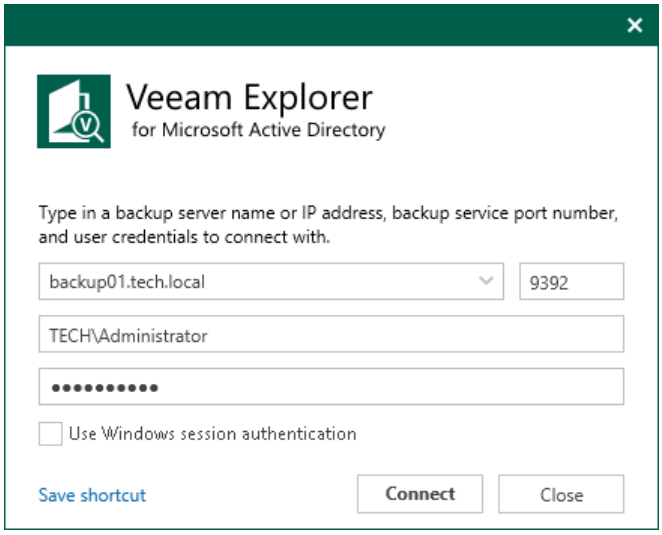
- The domain name or IP address of the backup server to which you want to connect
- The port number
- User account credentials

  Consider the following:

  - To perform recovery operations, Veeam Explorer for Microsoft Active Directory must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorers Suite is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft Active Directory is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

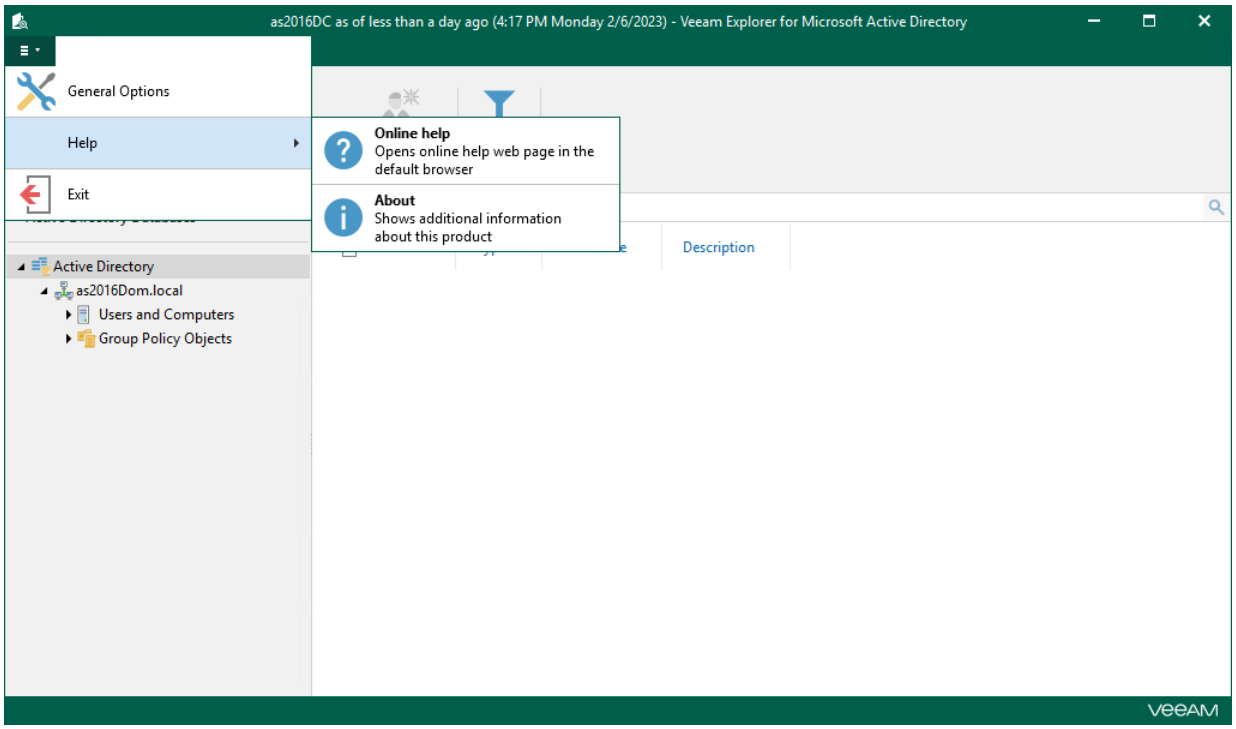
Veeam Explorer for Microsoft Active Directory provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft Active Directory window.

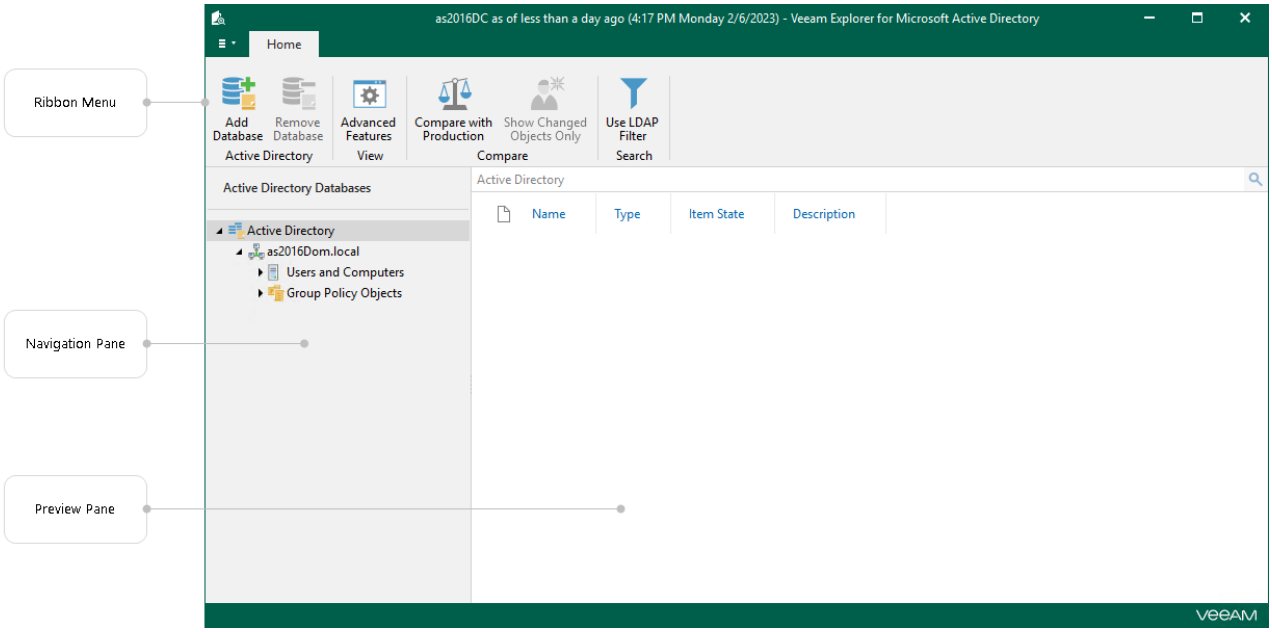
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft Active Directory wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

This topic explains how to use Veeam Explorer for Microsoft Active Directory to:

- Browse backup content
- Search for objects in a backup file

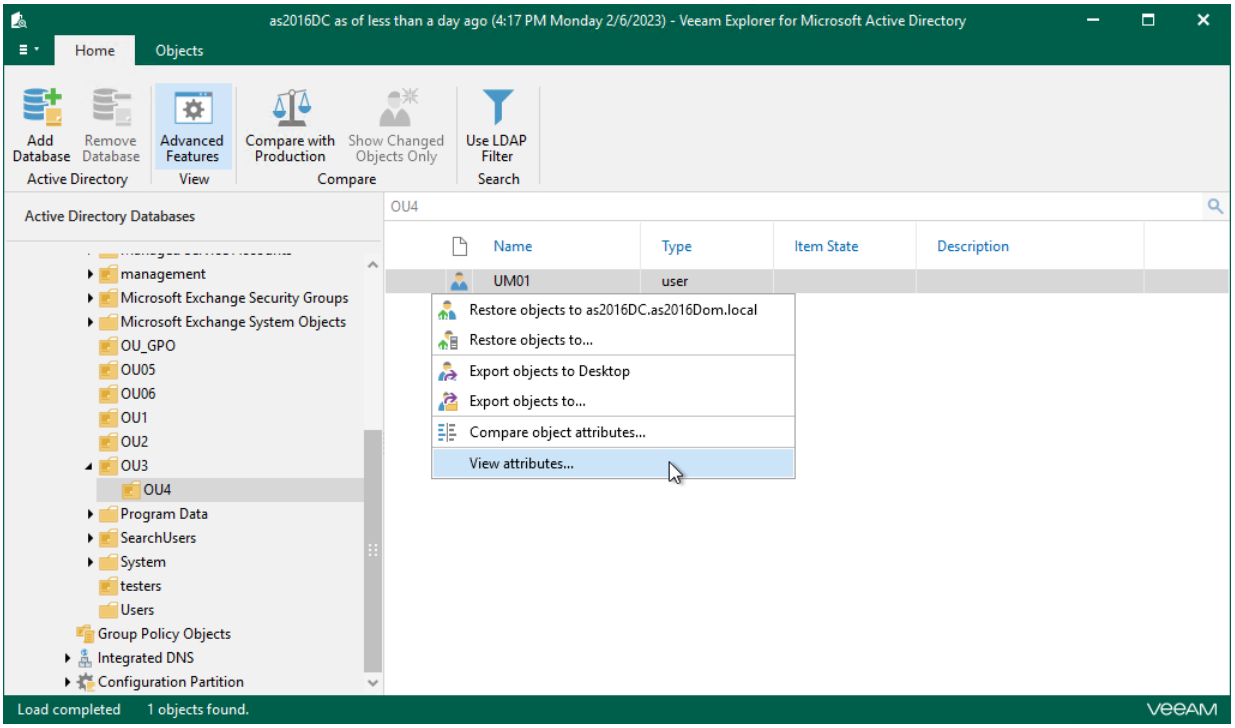
Browsing

To view the contents of a backup file, use the navigation pane which shows you the database structure containing your active directory objects. After you select a container in the navigation pane, you can see its contents in the preview pane.

Right-click an object and select **View attributes** to view object attributes. To copy necessary attributes to the clipboard, select an attribute and press [Ctrl+C] on the keyboard. Multiple selection is also supported.

Veeam Explorer for Microsoft Active Directory does not display some objects and containers in the default view, such as the entire *Microsoft Exchange System Options*, *System*, *Integrated DNS*, *Configuration Partition* containers, as well as the objects stored in the *Domain Controllers* container. This behavior is intended to prevent accidental errors during the recovery process that may affect the system stability of the target machine.

You can view and recover some of this data if you open the **Home** tab and enable **Advanced Features**, but you must manually verify all recovery operations to ensure stable operation of the system.



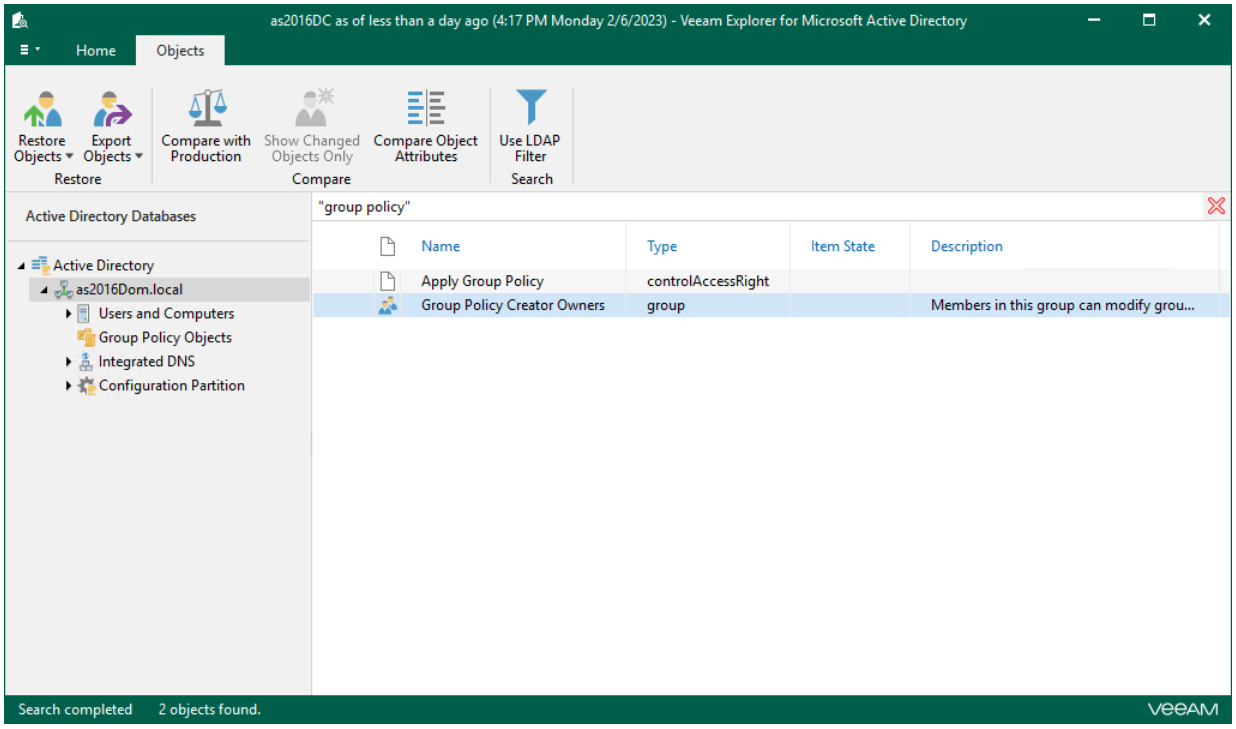
Searching

The search mechanism allows you to find items matching specified search criteria.

To search for the required items, do the following:

1. In the navigation pane, select an object in which you want to find your data.
2. Enter a search query in the search field at the top of the preview pane. Then press [Enter] or click the **Search** button to the right of the search field.

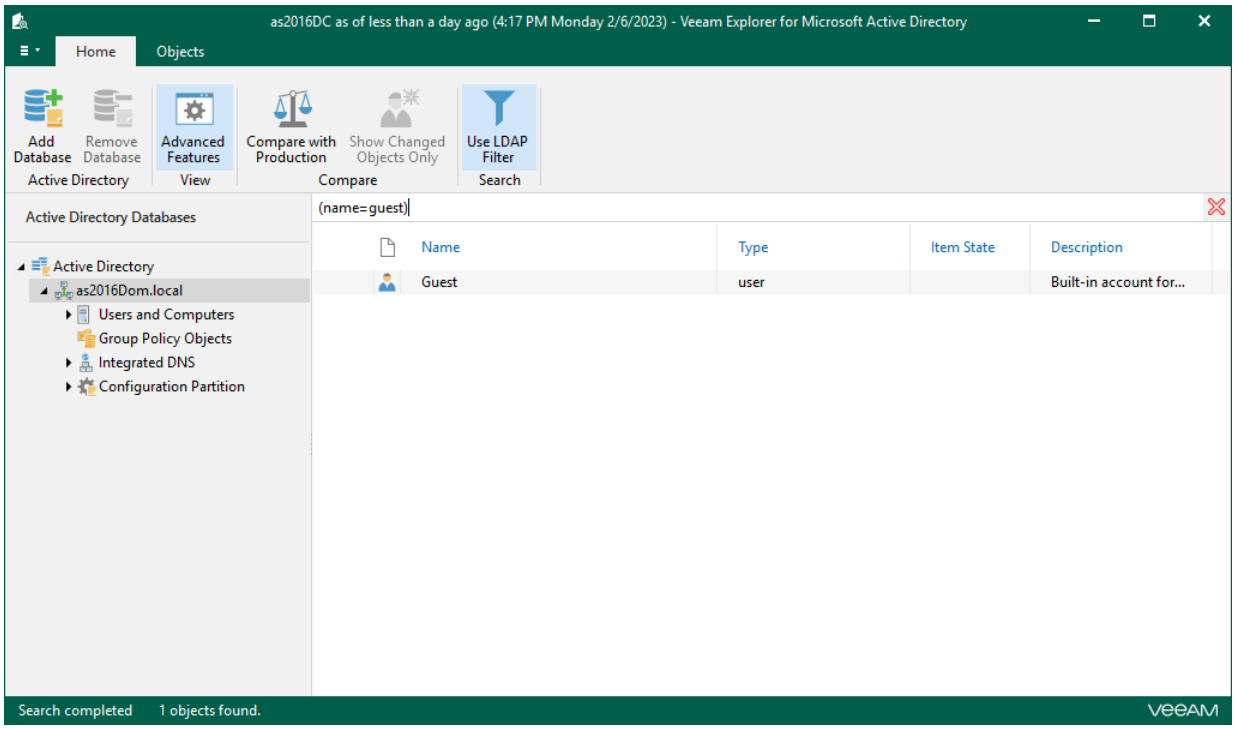
> **NOTE**
>
> To find the exact phrase, use double quotes. For example, "*group policy*".



Using LDAP Queries

To use the LDAP search query, do the following:

1. In the navigation pane, select a container.
2. On the ribbon menu, click **Use LDAP Filter**.
3. In the search field, enter an LDAP query. Then press [Enter] or click the **Search** button to the right of the search field.

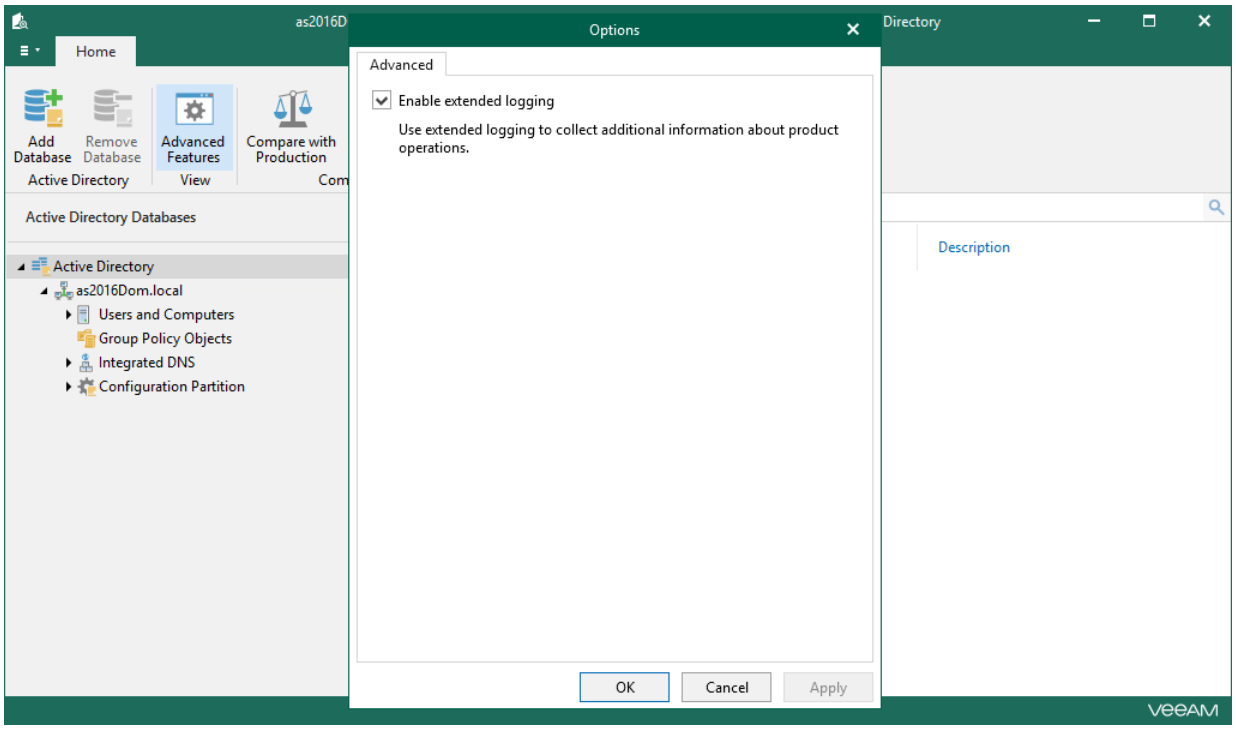


Enabling Extended Logging

Veeam Explorer for Microsoft Active Directory allows you to enable an extended logging mode to collect more detailed logs on specific operations. After you enable extended logging, you can go back to the application and perform the actions for which you want to collect additional information. Then you can collect the logs.

To configure extended logging mode, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box and click **OK**.
3. Go back to the application, perform necessary actions and then review the logs to see the details.



Standalone Databases Management

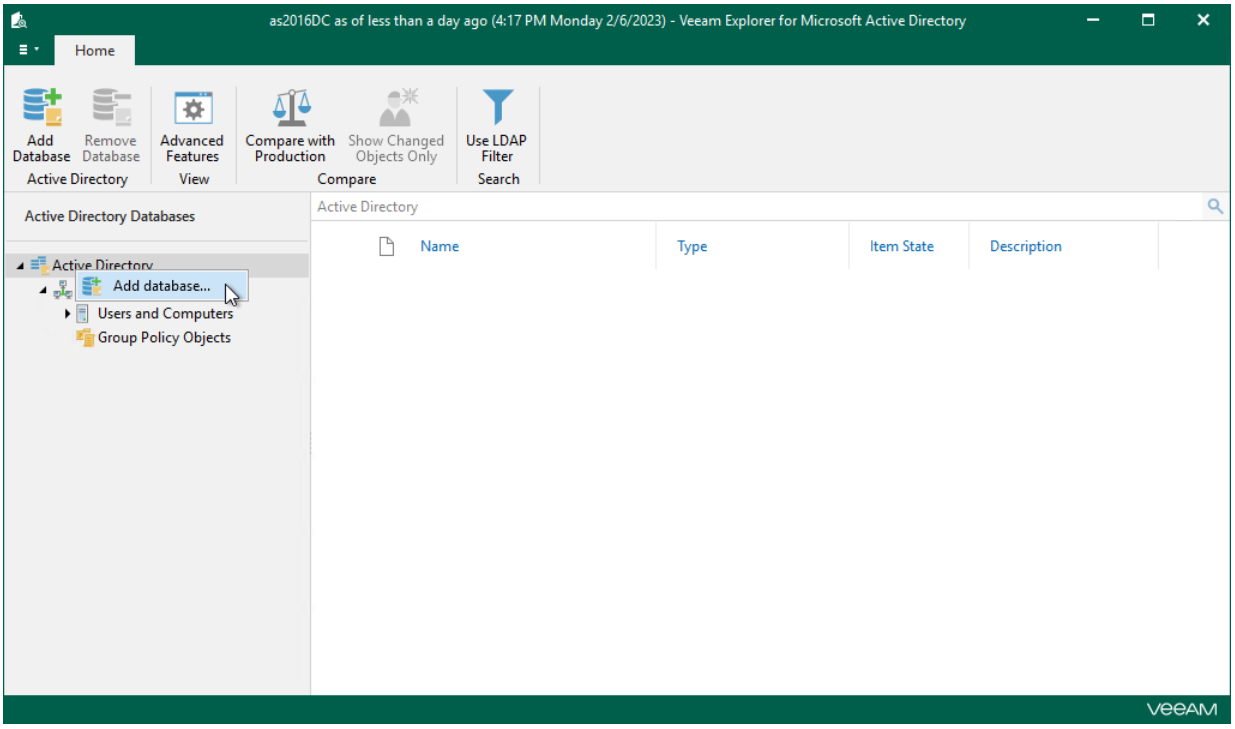
This section explains how to use Veeam Explorer for Microsoft Active Directory to add and remove standalone Microsoft Active Directory databases.

> **IMPORTANT**
>
> Make sure the database you are adding to the Veeam Explorer for Microsoft Active Directory scope was not locked by another process.

Adding Standalone Databases

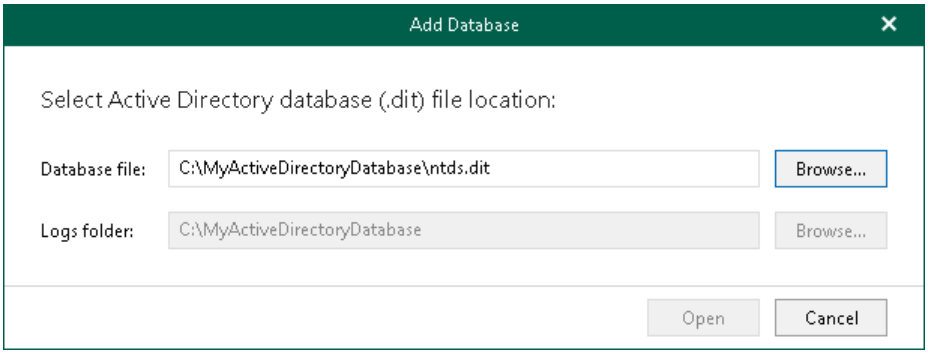
To add a standalone Active Directory database manually, do the following:

1. Select the root **Active Directory** node in the navigation pane and click **Add Database** on the ribbon or right-click the **Active Directory** node and select **Add database**.



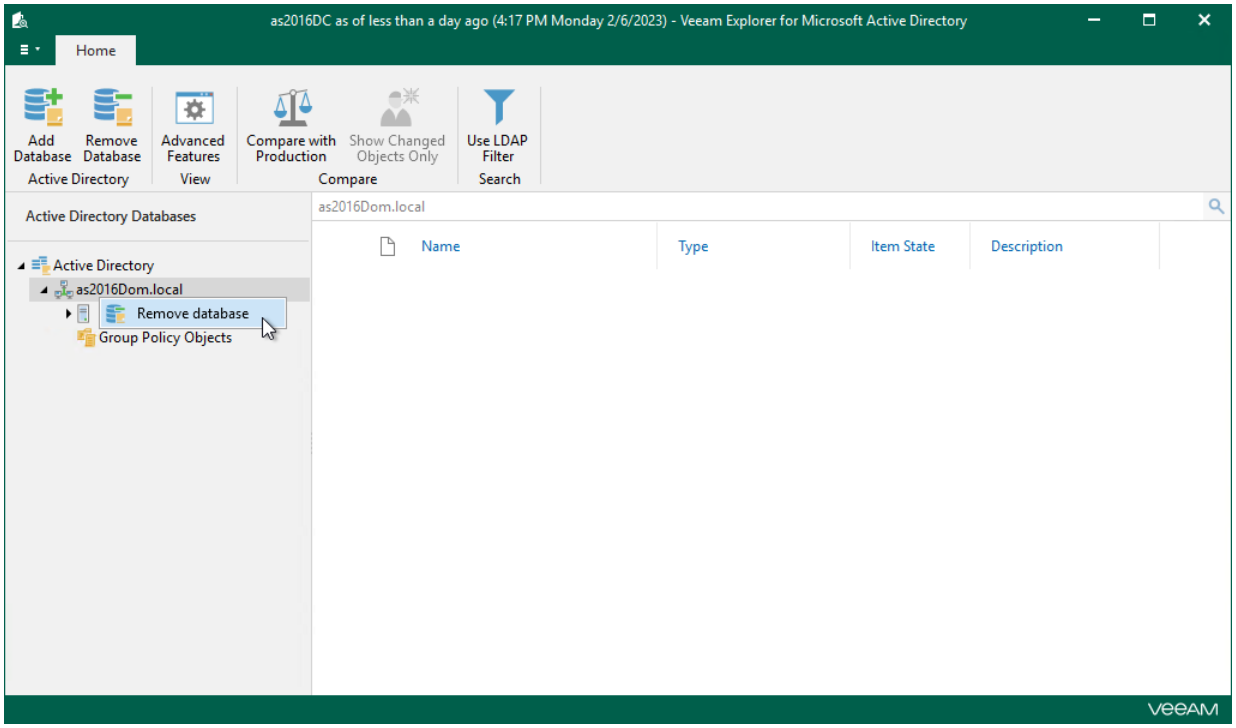
2. Specify the location of the Active Directory database file and folder that contains associated transaction log files (`Edb.log` and `Edb.chk`).

   By default, the Active Directory database file (`NTDS.DIT`) is located in the `%SystemRoot%\NTDS` directory. Make sure that the system registry hive is located in the same place.



Removing Standalone Databases

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove database**.



Data Restore

This section contains information about the available restore operations in Veeam Explorer for Microsoft Active Directory.

Before restoring data, read the Considerations and Limitations section.

Restoring Objects

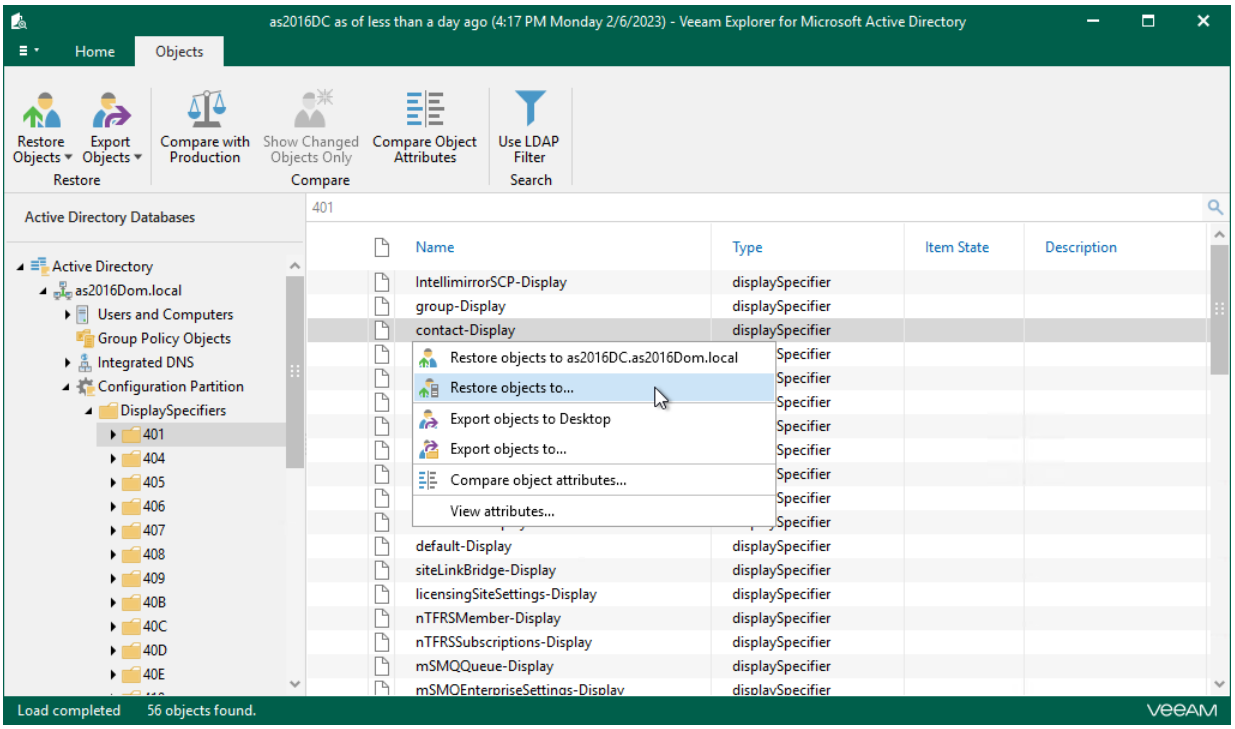
To restore Active Directory objects, do the following:

1. Launch the Restore wizard.
2. Specify connection parameters.
3. Specify the restore location.
4. Specify password restore options.
5. Specify the account state.
6. Specify restore options.
7. Specify attributes to restore.

Step 1. Launch Restore Wizard

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

1. In the preview pane, select an object.
2. On the **Objects** tab, select **Restore Objects** > **Restore objects to** or right-click an object and select **Restore objects to**.



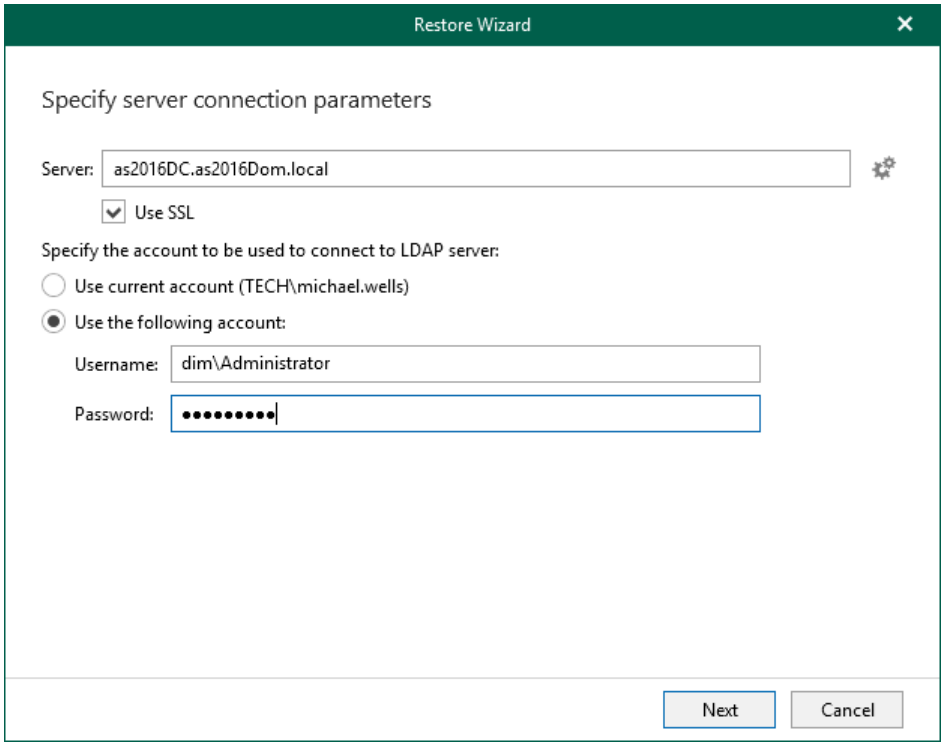
Step 2. Specify Connection Parameters

At this step of the wizard, specify the following:

- A target production server to which you want to restore your data.

  Select the **Use SSL** check box to establish a secure SSL connection.

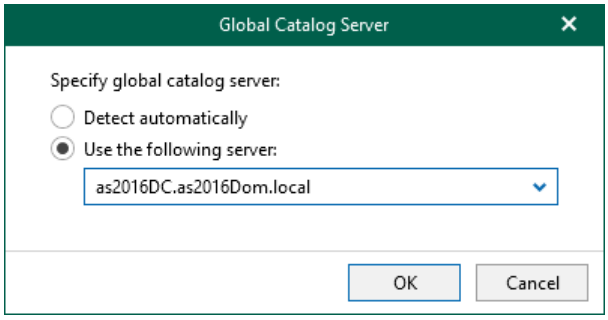
- User credentials to connect to the LDAP server.



Global Catalog Server

To specify a Global Catalog server, click the **Settings** button on the right side of the **Server** field and choose either of the following options:

- **Detect automatically** — to automatically detect a server.
- **Use the following server** — to choose a server from the list.



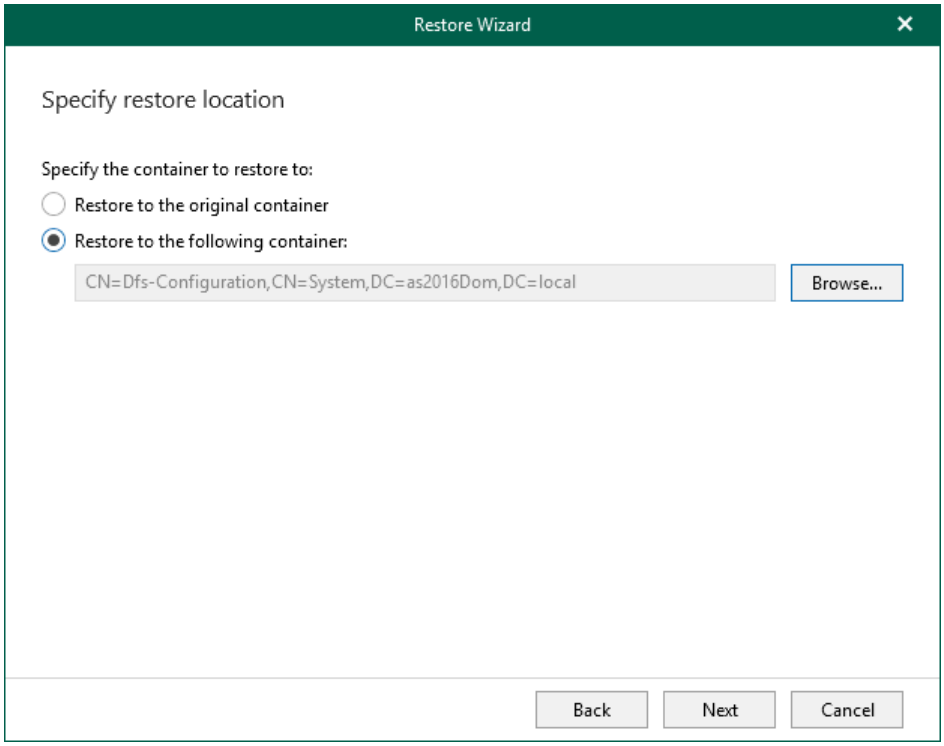
Step 3. Specify Restore Location

At this step of the wizard, select a container to which you want to restore the objects.

You can select the following:

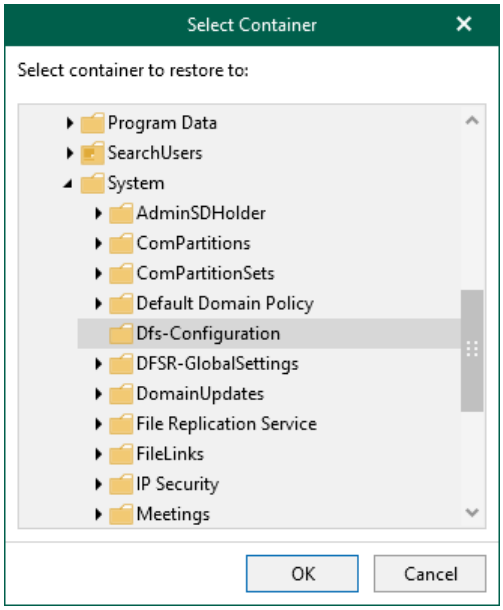
- **Restore to the original container** — to restore data to the original container in your production environment.
- **Restore to the following container** — to select a different container, as described in Browsing Container.

> **NOTE**
>
> If a container that is being restored was not found in the production environment, it will be restored anew.



Browsing Container

To select a different container, click **Browse** and choose a container you want to use.



Step 4. Specify Password Restore Options

At this step, select one of the following options:

- **Restore password**. To restore the password from the backup file.
- **Set password to**. To set a new password.
- **Do not restore password**. To skip restoring the password.

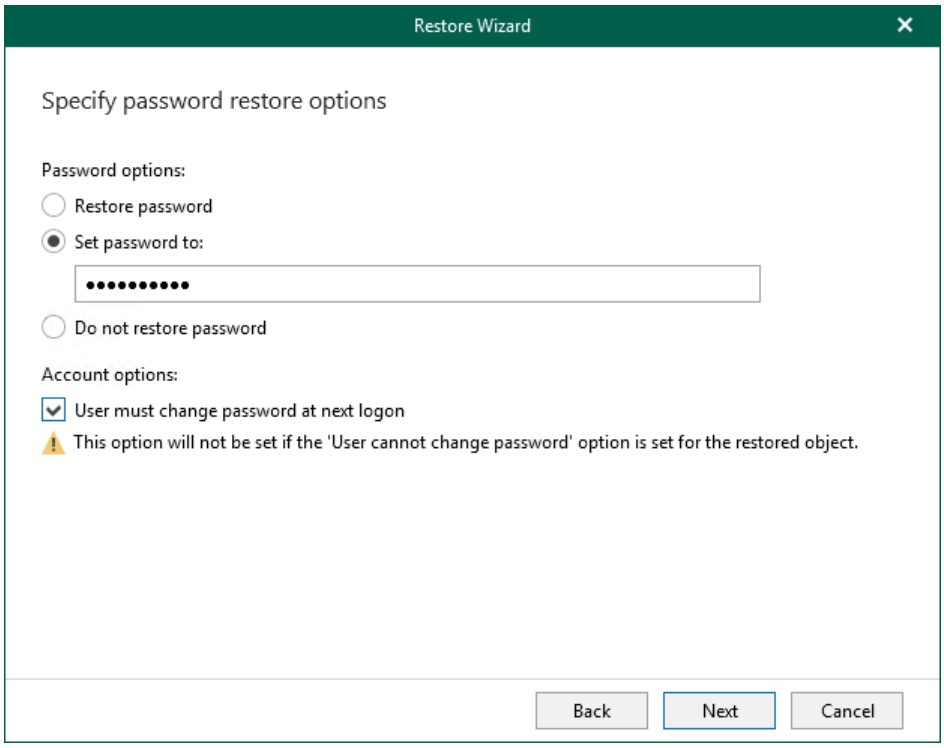
  This option will not make any changes to the currently configured passwords in your environment.

Consider the following:

- When providing a new password, check that it complies with the password policy in your production environment.
- If you select **Restore password** or **Set password to** options, you may also request a user to change the password at next log on.

  Keep in mind that this setting will not take effect if a user is not allowed to change the password due to security limitations.
- When restoring multiple accounts, a new password will be set for all the accounts altogether.
- To restore account passwords, Veeam Explorer for Microsoft Active Directory uses registry database. Make sure that the *System* registry hive is available.

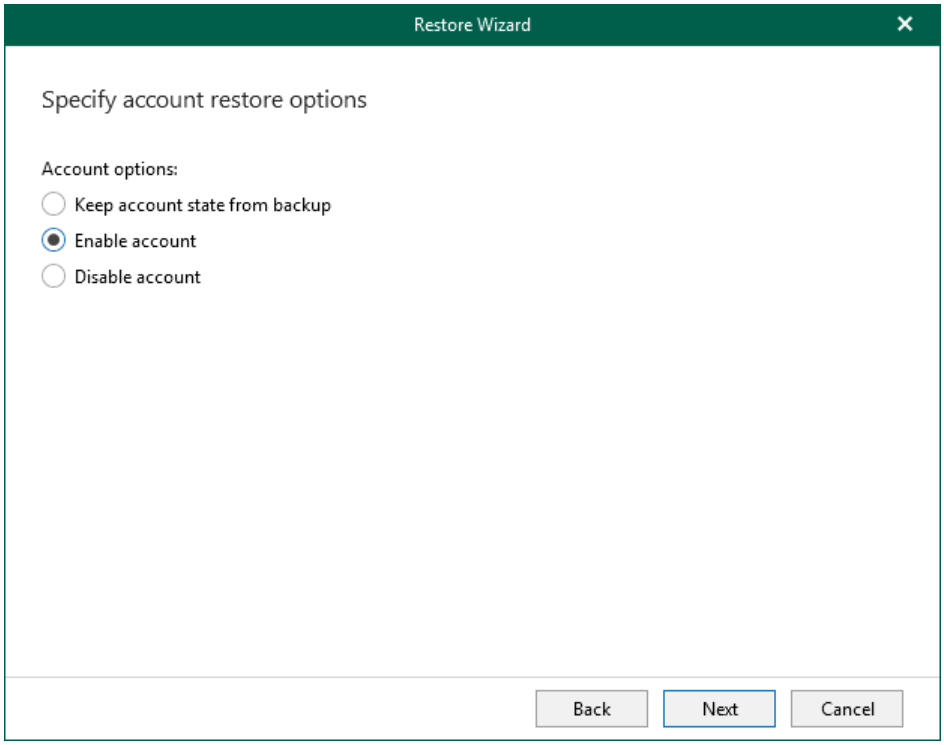
  The default location is `%systemroot%\System32\Config`.
- When restoring Active Directory database from an Active Directory backup file using Veeam file-level restore, the registry hive will be located automatically. Otherwise, make sure the system registry hive is located in the same folder as `.DIT` file.



Step 5. Specify Account State

At this step of the wizard, select one of the following options:

- **Keep account state from backup** — to keep the account state as it is in the backup file.
- **Enable account** — to change the account state to enabled.
- **Disable account** — to change the account state to disabled.



Step 6. Specify Restore Options

At this step of the wizard, specify restore options.

You can select the following:

- **Objects to process**:
  - **Changed objects** — to restore changed objects.
  - **Deleted objects** — to restore deleted objects.
- **Restore**:
  - **Entire objects** — to restore entire objects collection.
  - **Selected attributes only** — to select particular attributes.

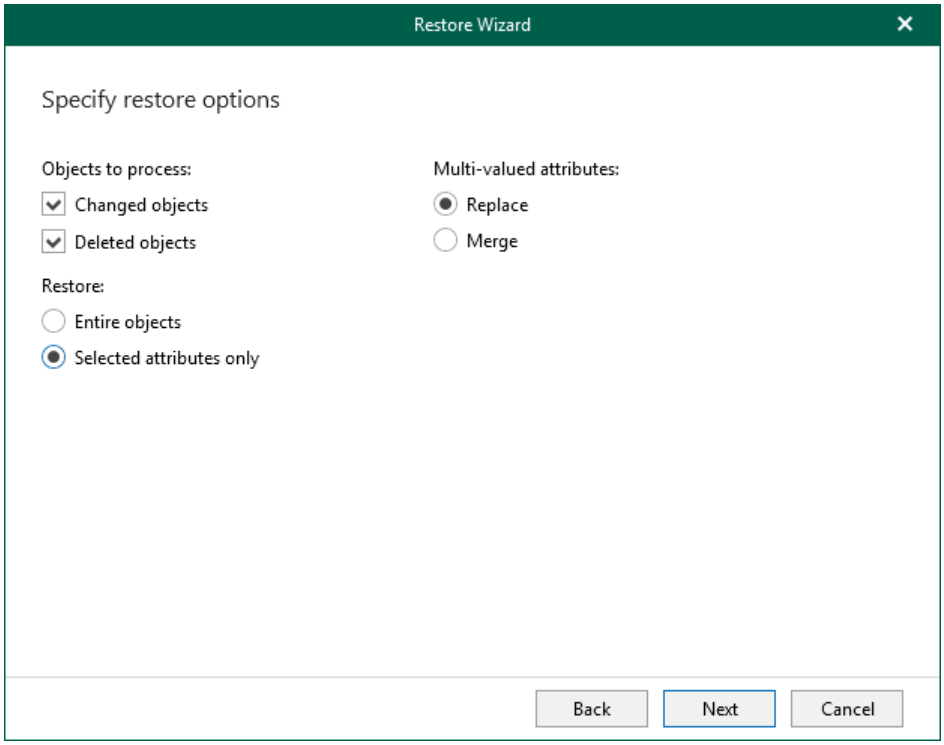
    When selecting **Selected attributes only**, you will be offered to choose the attributes you want to restore in the next step.

    This option is not applicable to restore of Group Policy Objects.
- **Multi-valued attributes**:
  - **Replace** — to replace production data with that of a backup file.
  - **Merge** — to merge existing data with that of a backup file.

  By default, multi-valued attributes will be replaced, not merged.

NOTE

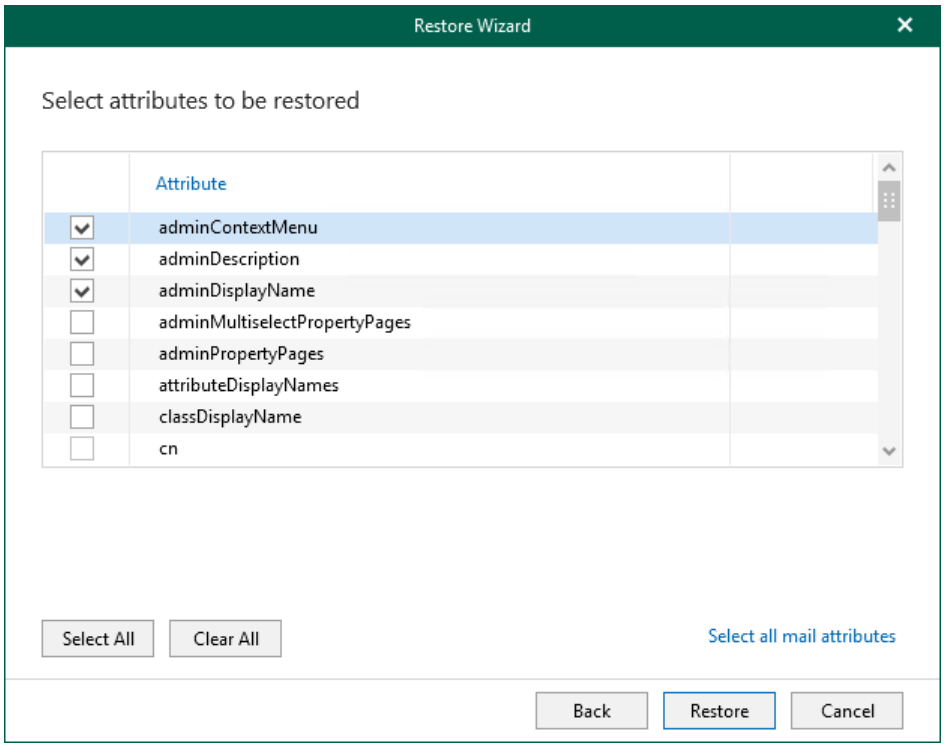
- When working with Active Directory 2016, this dialog will also include the **Restore expiration time** option, which allows you to restore expiration time for linked attributes.
- Users cannot change recovery settings for disabled attributes. Such attributes will be either restored or skipped according to the default configuration.



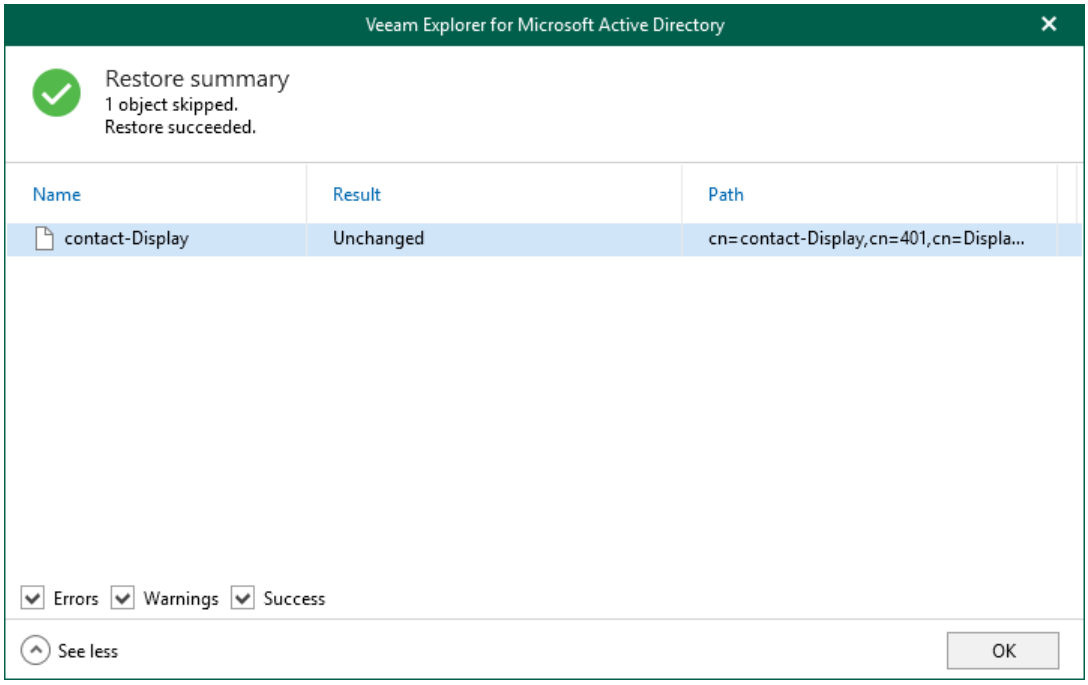
Step 7. Specify Attributes to Restore

At this step of the wizard, select attributes you want to restore.

This step is available only if you have chosen the **Selected attributes only** option at the previous step.



After the restore process is complete, review the results shown in the **Restore summary** window. You can filter notifications by their status: *Error*, *Warning* or *Success*.



Restoring Containers

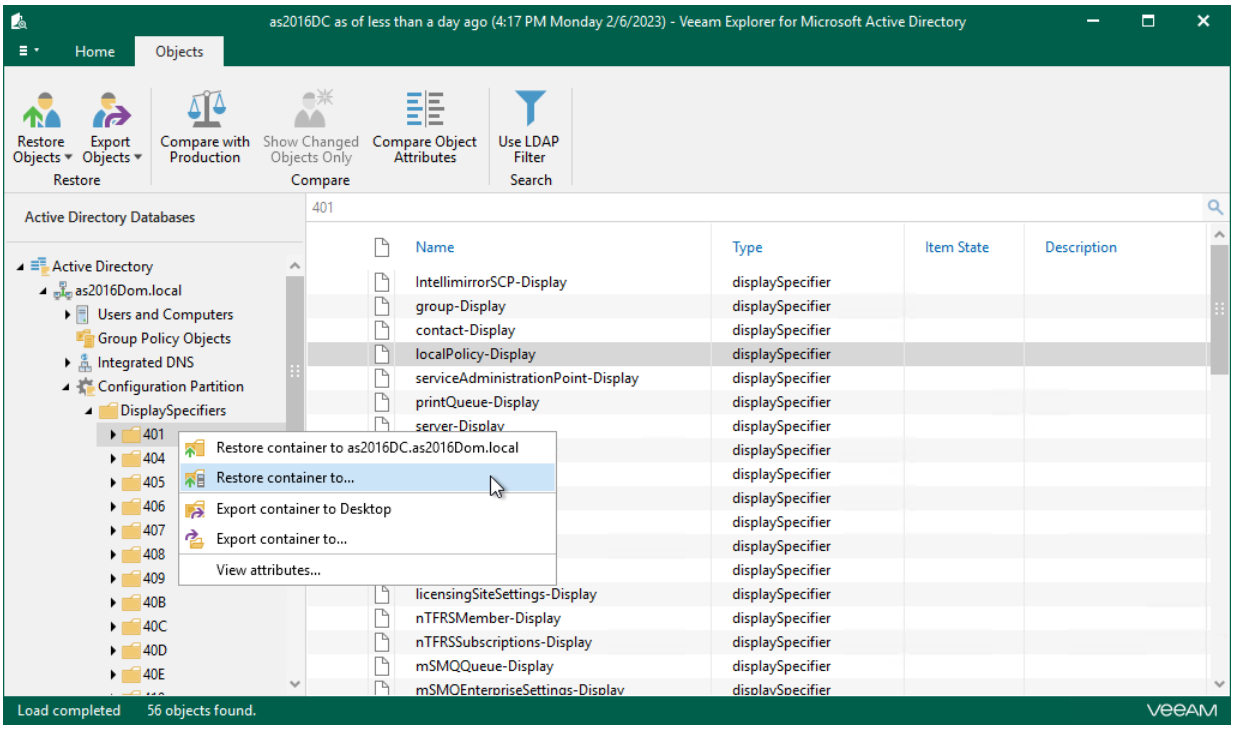
To restore Active Directory containers, do the following:

1. Launch the Restore wizard.
2. Specify connection parameters.
3. Specify the restore location.
4. Specify password restore options.
5. Specify the account state.
6. Specify restore options.
7. Specify attributes to restore.

Step 1. Launch Restore Wizard

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

1. In the preview pane, select an object.
2. On the **Container** tab, select **Restore Container** > **Restore container to** or right-click a container and select **Restore container to**.



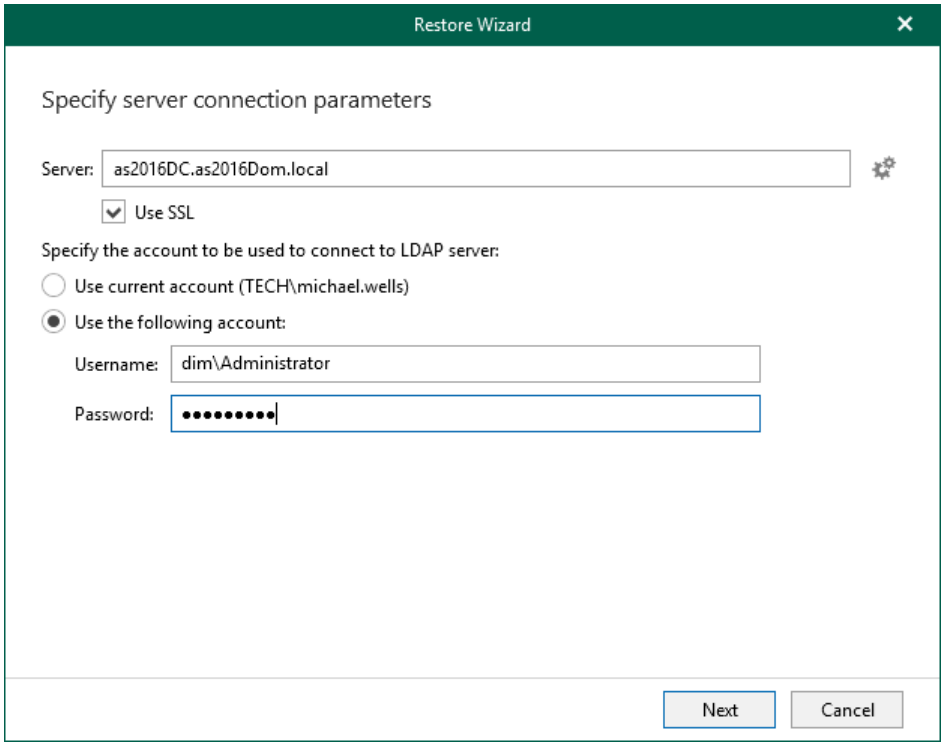
Step 2. Specify Connection Parameters

At this step of the wizard, specify the following:

- A target production server to which you want to restore your data.

  Select the **Use SSL** check box to establish a secure SSL connection.

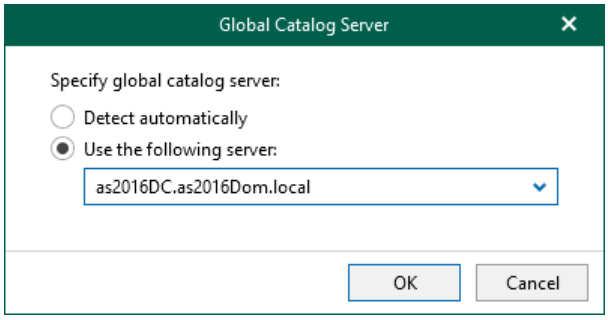
- User credentials to connect to the LDAP server.



Global Catalog Server

To specify a Global Catalog server, click the **Settings** button on the right side of the **Server** field and choose either of the following options:

- **Detect automatically** — to automatically detect a server.
- **Use the following server** — to choose a server from the list.



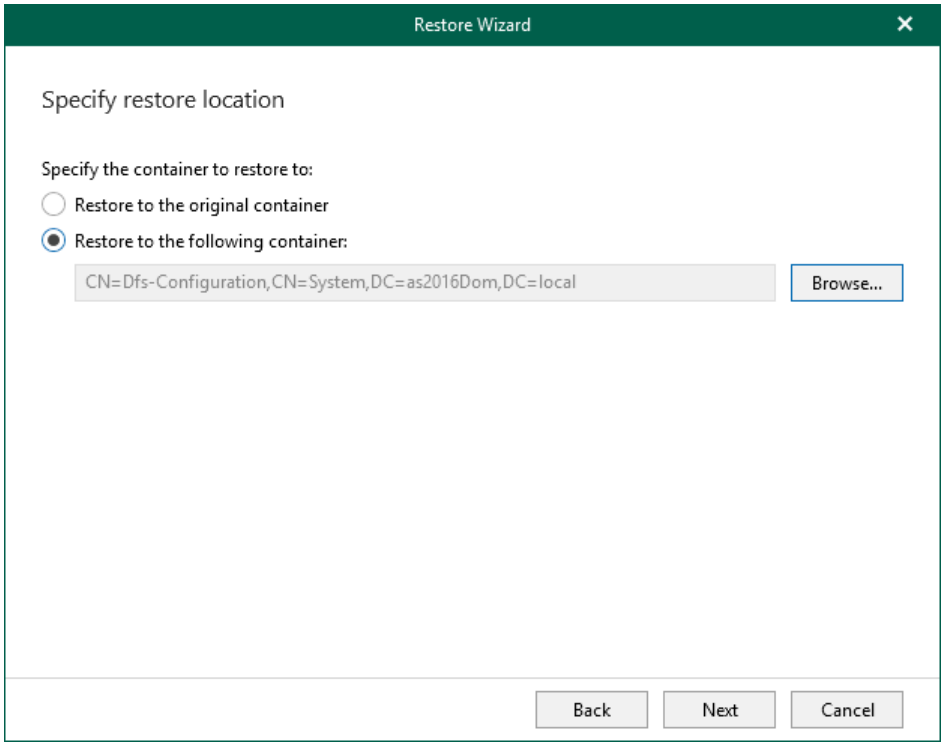
Step 3. Specify Restore Location

At this step of the wizard, select a container to which you want to restore the objects.

You can select the following:

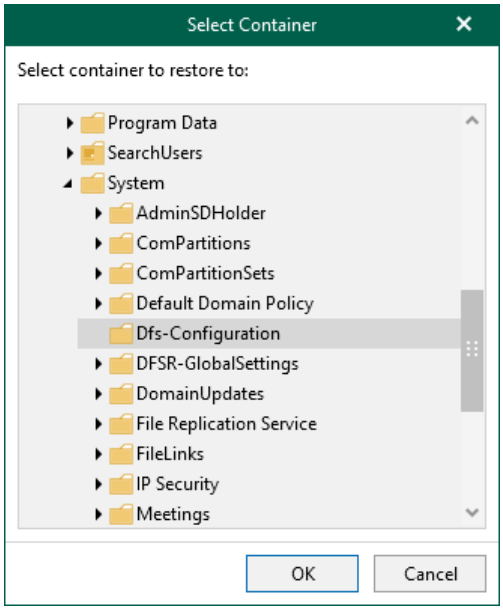
- **Restore to the original container** — to restore data to the original container in your production environment.
- **Restore to the following container** — to select a different container, as described in Browsing Container.

> **NOTE**
>
> If a container that is being restored was not found in the production environment, it will be restored anew.



Browsing Container

To select a different container, click **Browse** and choose a container you want to use.



Step 4. Specify Password Restore Options

At this step, select one of the following options:

- **Restore password**. To restore the password from the backup file.
- **Set password to**. To set a new password.
- **Do not restore password**. To skip restoring the password.

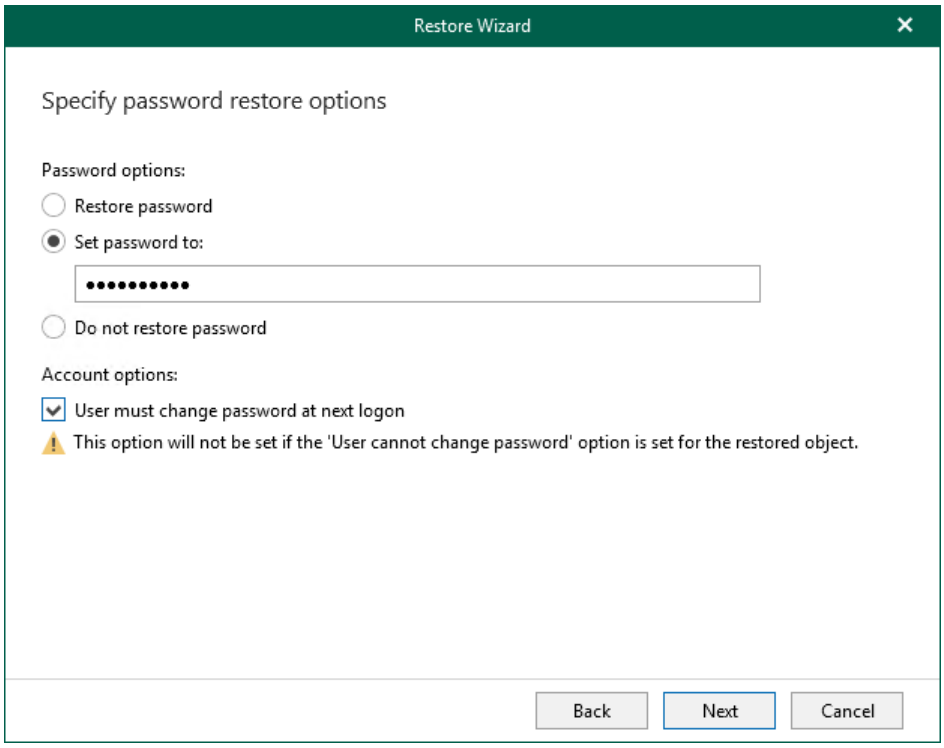
  This option will not make any changes to the currently configured passwords in your environment.

Consider the following:

- When providing a new password, check that it complies with the password policy in your production environment.
- If you select **Restore password** or **Set password to** options, you may also request a user to change the password at next log on.

  Keep in mind that this setting will not take effect if a user is not allowed to change the password due to security limitations.
- When restoring multiple accounts, a new password will be set for all the accounts altogether.
- To restore account passwords, Veeam Explorer for Microsoft Active Directory uses registry database. Make sure that the *System* registry hive is available.

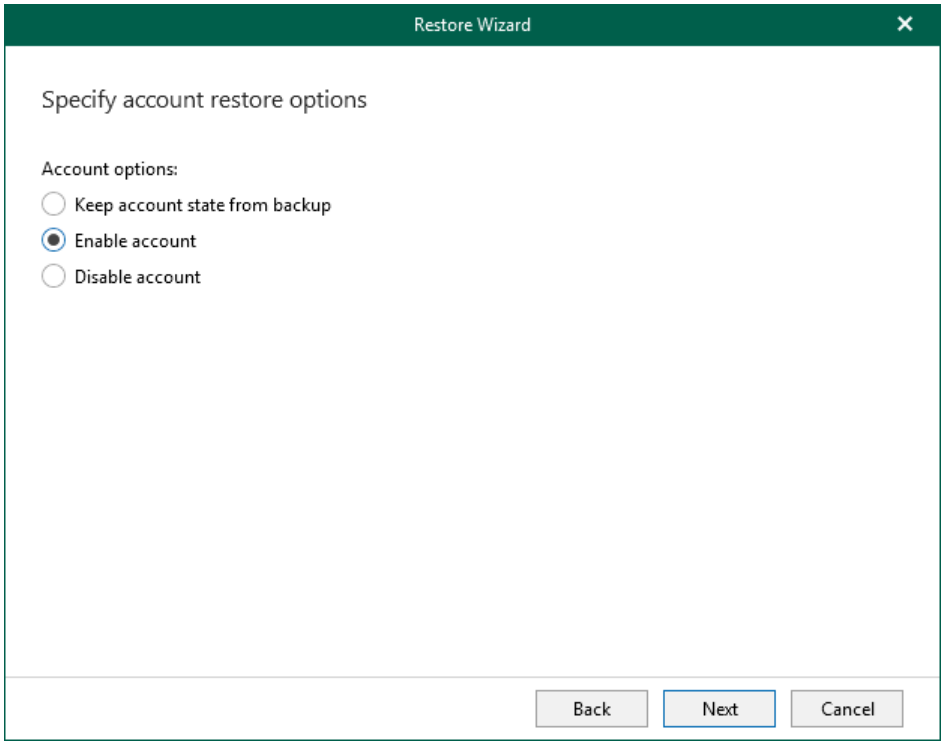
  The default location is `%systemroot%\System32\Config`.
- When restoring Active Directory database from an Active Directory backup file using Veeam file-level restore, the registry hive will be located automatically. Otherwise, make sure the system registry hive is located in the same folder as `.DIT` file.



Step 5. Specify Account State

At this step of the wizard, select one of the following options:

- **Keep account state from backup** — to keep the account state as it is in the backup file.
- **Enable account** — to change the account state to enabled.
- **Disable account** — to change the account state to disabled.



Step 6. Specify Restore Options

At this step of the wizard, specify restore options.

You can select the following:

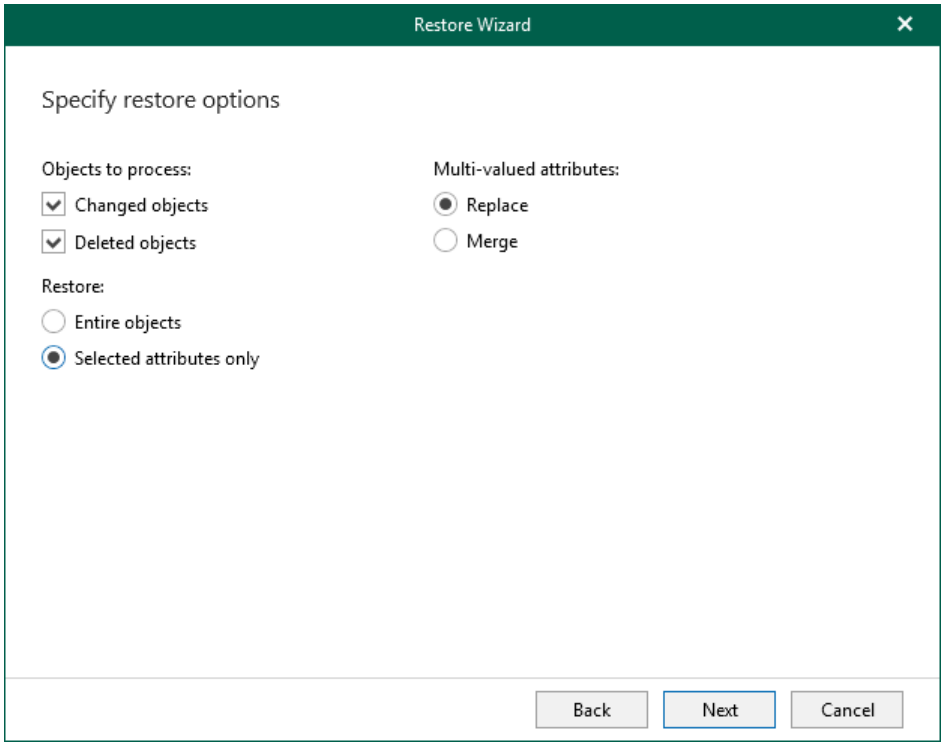
- **Objects to process**:
  - **Changed objects** — to restore changed objects.
  - **Deleted objects** — to restore deleted objects.
- **Restore**:
  - **Entire objects** — to restore entire objects collection.
  - **Selected attributes only** — to select particular attributes.

    When selecting **Selected attributes only**, you will be offered to choose the attributes you want to restore in the next step.
- **Multi-valued attributes**:
  - **Replace** — to replace production data with that of a backup file.
  - **Merge** — to merge existing data with that of a backup file.

  By default, multi-valued attributes will be replaced, not merged.

NOTE

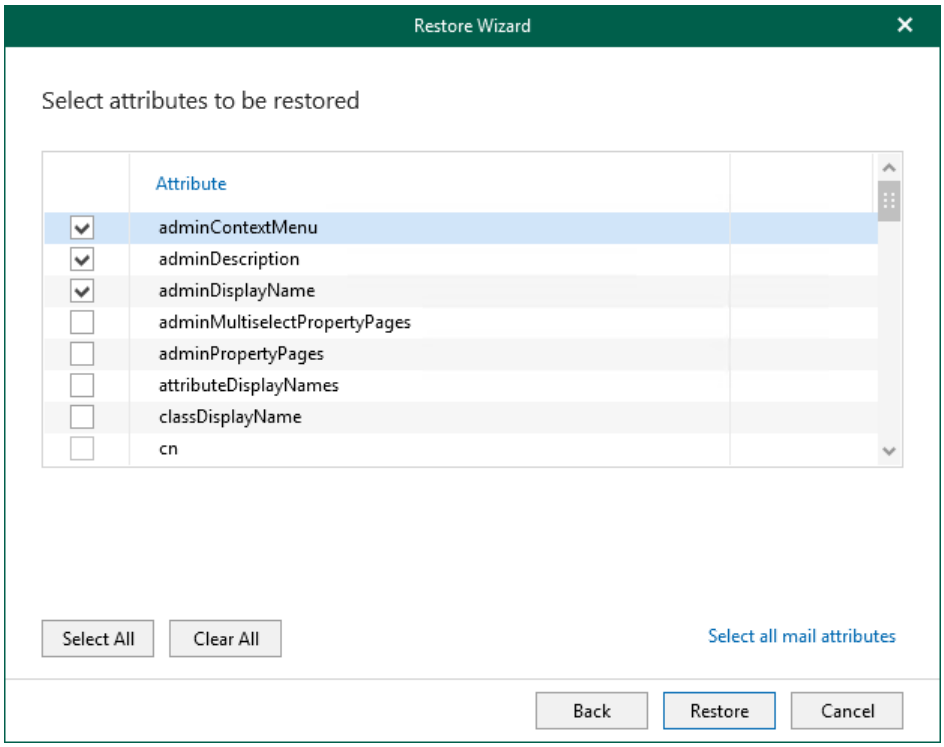
- When working with Active Directory 2016, this dialog will also include the **Restore expiration time** option which allows you to restore expiration time for linked attributes. If an attribute being restored expires during the restore session, the attribute will not be restored.
- Users cannot change recovery settings for disabled attributes. Such attributes will be either restored or skipped according to the default configuration.



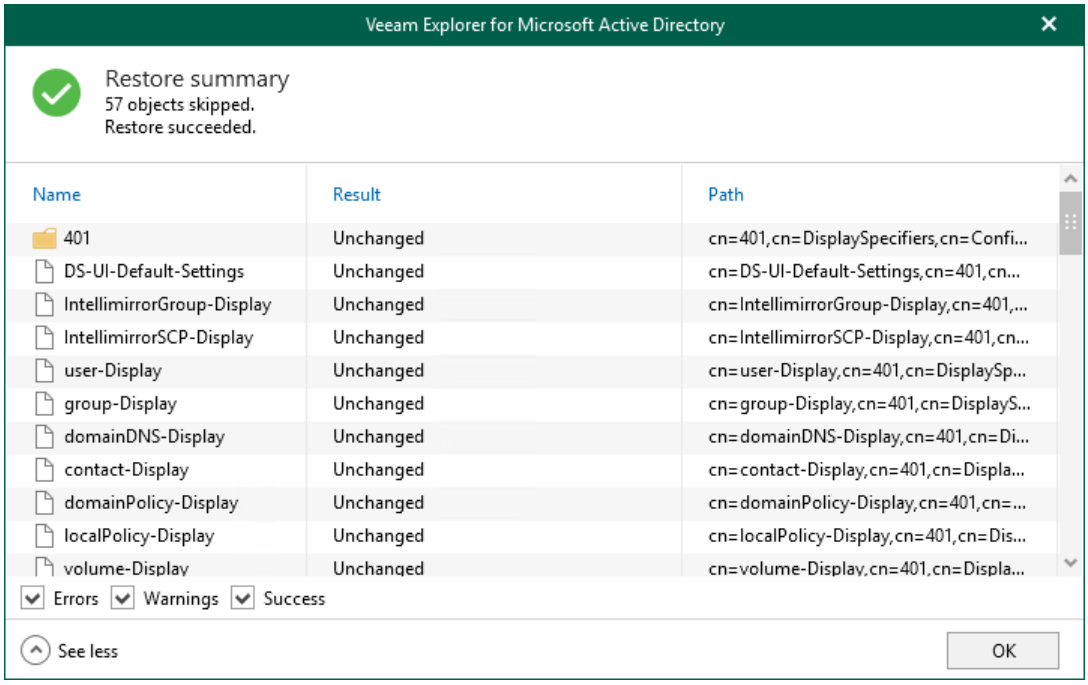
Step 7. Specify Attributes to Restore

At this step of the wizard, select attributes you want to restore.

This step is available only if you have chosen the **Selected attributes only** option at the previous step.



After the restore process is complete, review the results shown in the **Restore summary** window. You can filter notifications by their status: *Error*, *Warning* or *Success*.



Using 1-Click Restore

The 1-Click Restore feature allows you to quickly recover Active Directory objects and containers back to the original domain in your production environment.

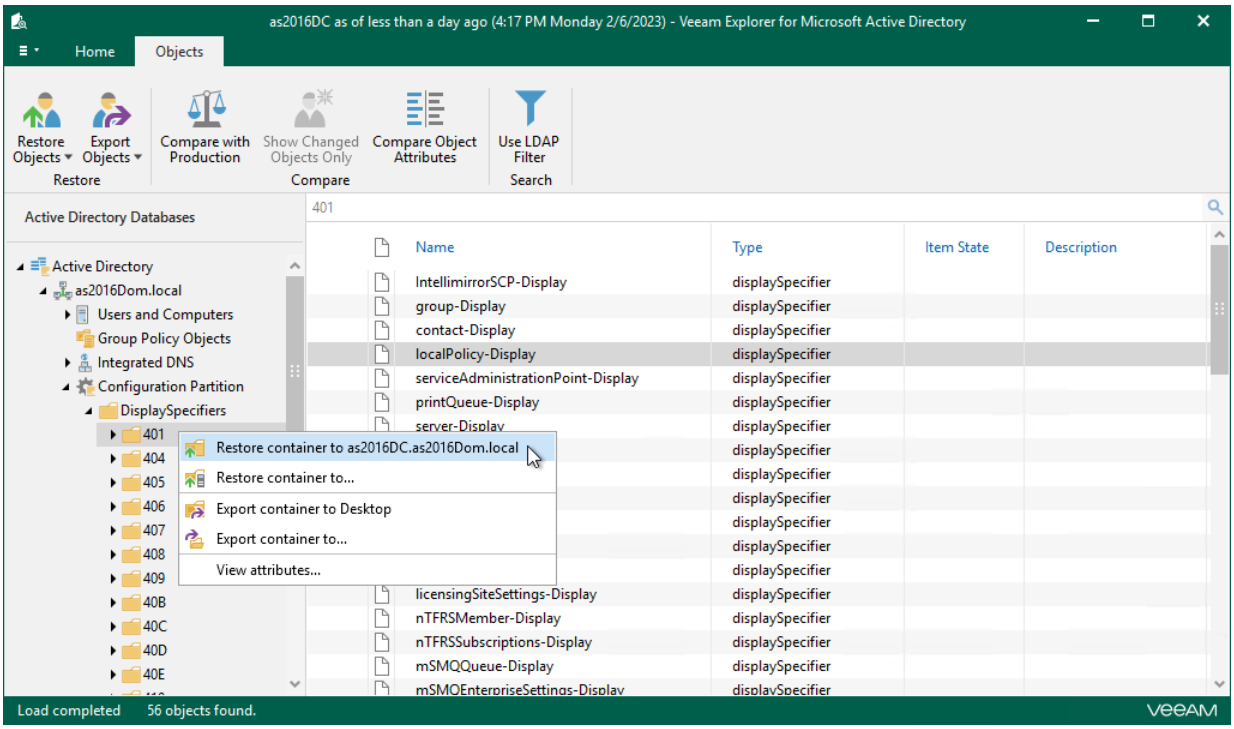
Consider the following:

- Both changed and deleted objects will be restored.
- All the attributes will be restored.
- Attribute values and security descriptors will be replaced with that of a backup file.

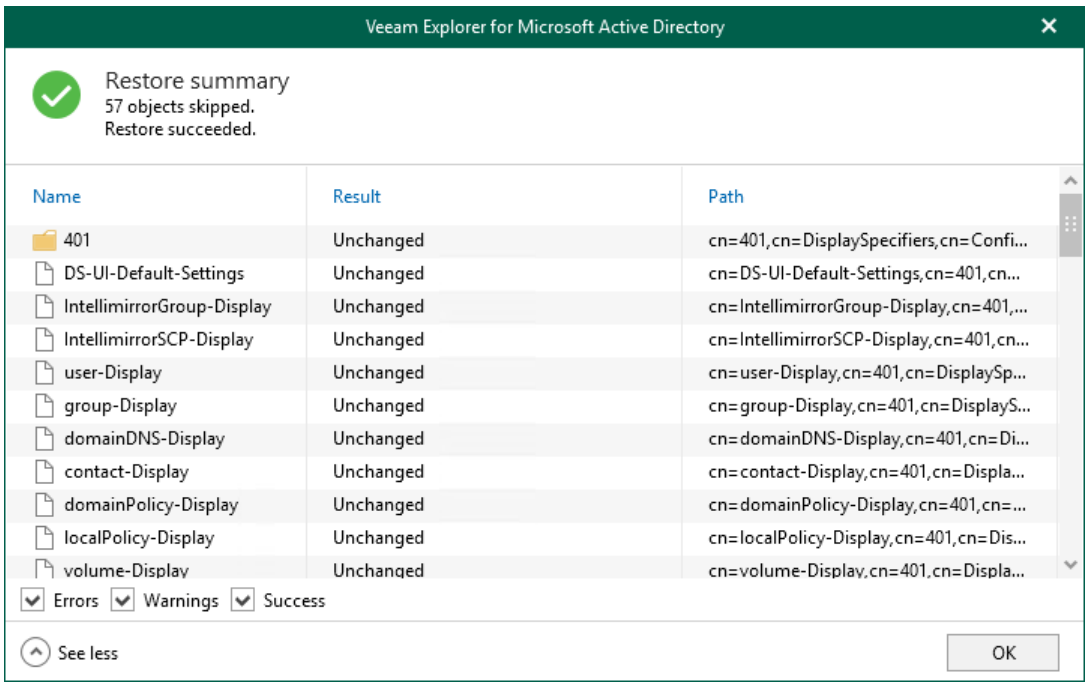
Restoring Containers

To restore a container, do the following:

1. In the navigation tree, select a container.
2. On the **Container** tab, select **Restore Container** > **Restore container to** *<server_name>* or right-click a container and select **Restore container to** *<server_name>*.



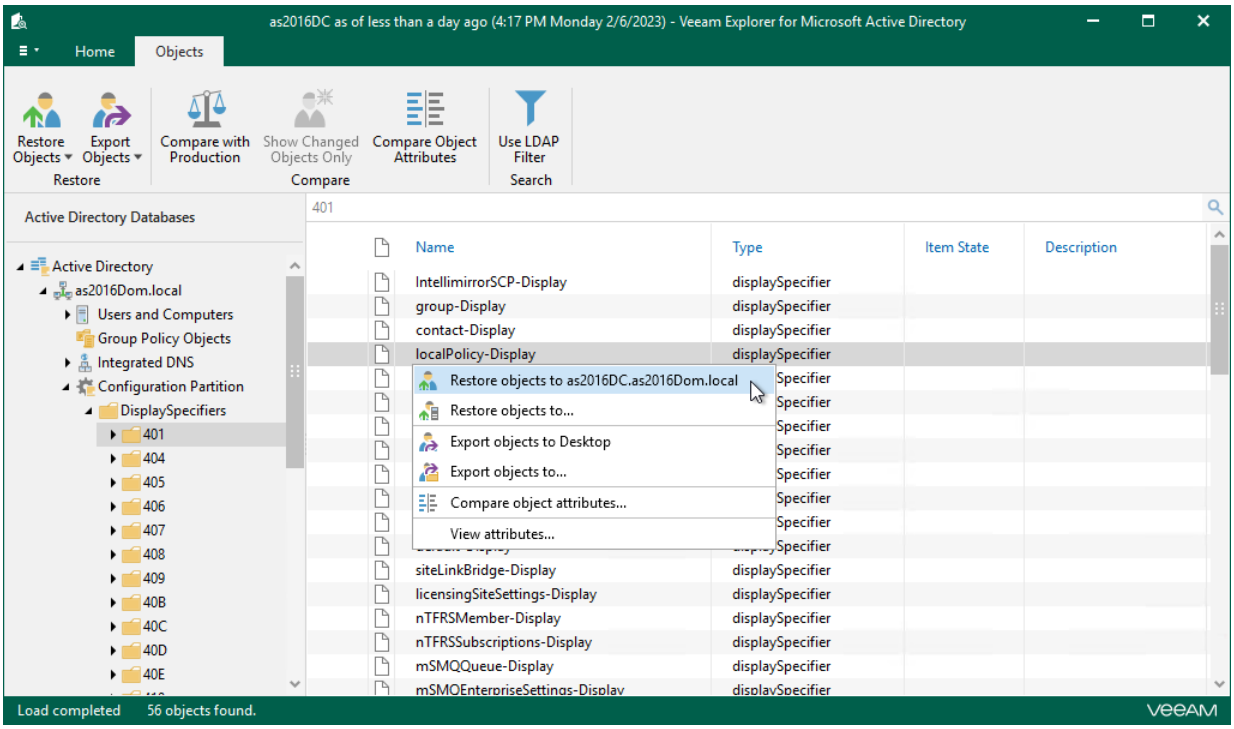
After the restore process is complete, review the results shown in the **Restore Summary** window. You can filter notifications by their status: *Error*, *Warning* or *Success*.



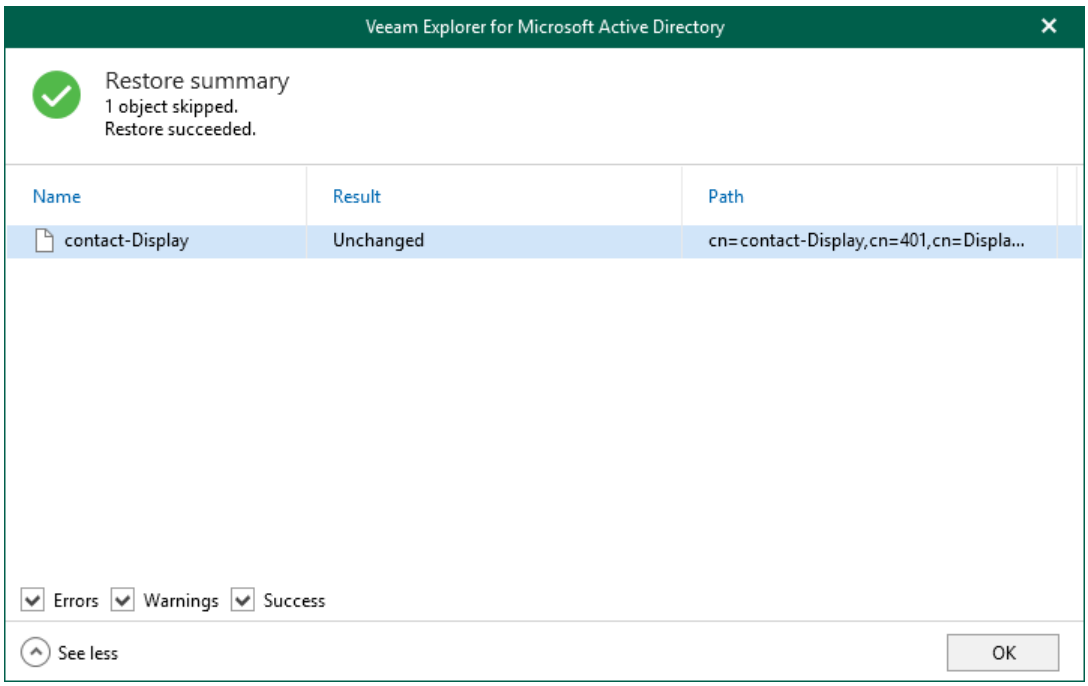
Restoring Objects

To restore an object, do the following:

1. In the preview pane, select objects.
2. On the **Objects** tab, select **Restore Objects** > **Restore objects to** *<server_name>* or right-click an object and select **Restore objects to** *<server_name>*.



After the restore process is complete, review the results shown in the **Restore Summary** window. You can filter notifications by their status: *Error*, *Warning* or *Success*.



Data Export

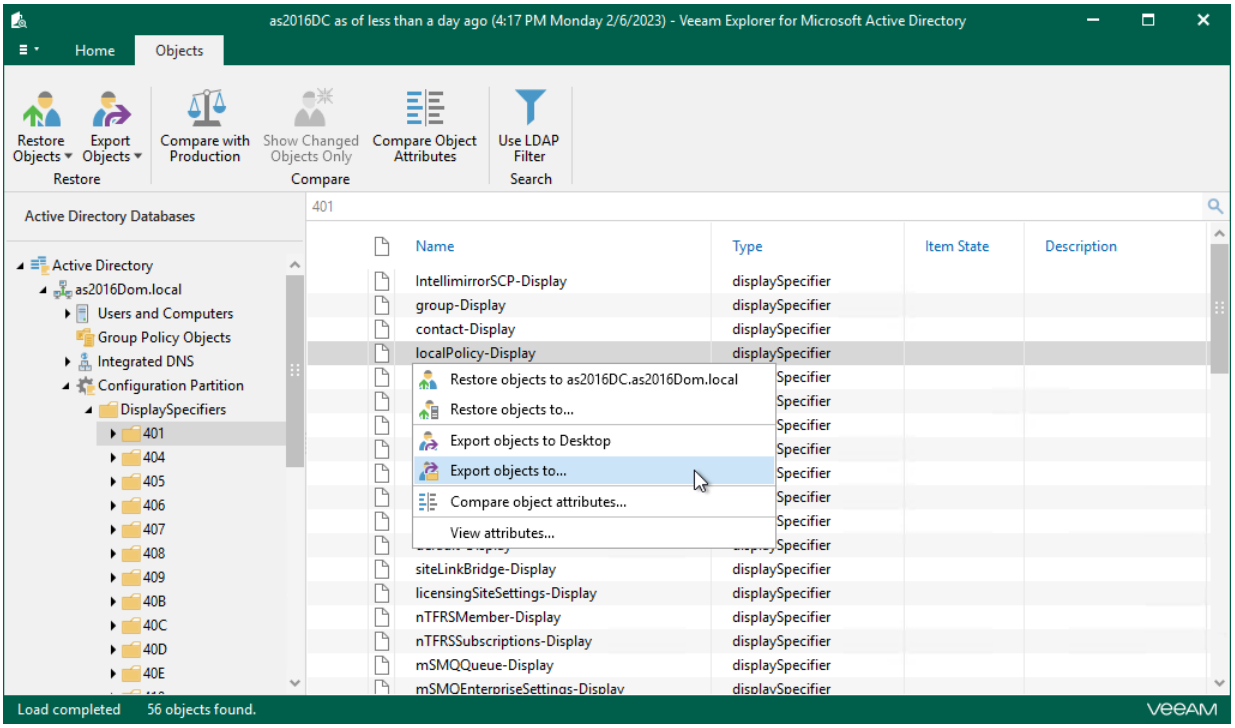
This section contains information about the available export options for Active Directory objects and containers.

Before exporting data, read the Considerations and Limitations section.

Exporting Objects

To export Active Directory objects, do the following:

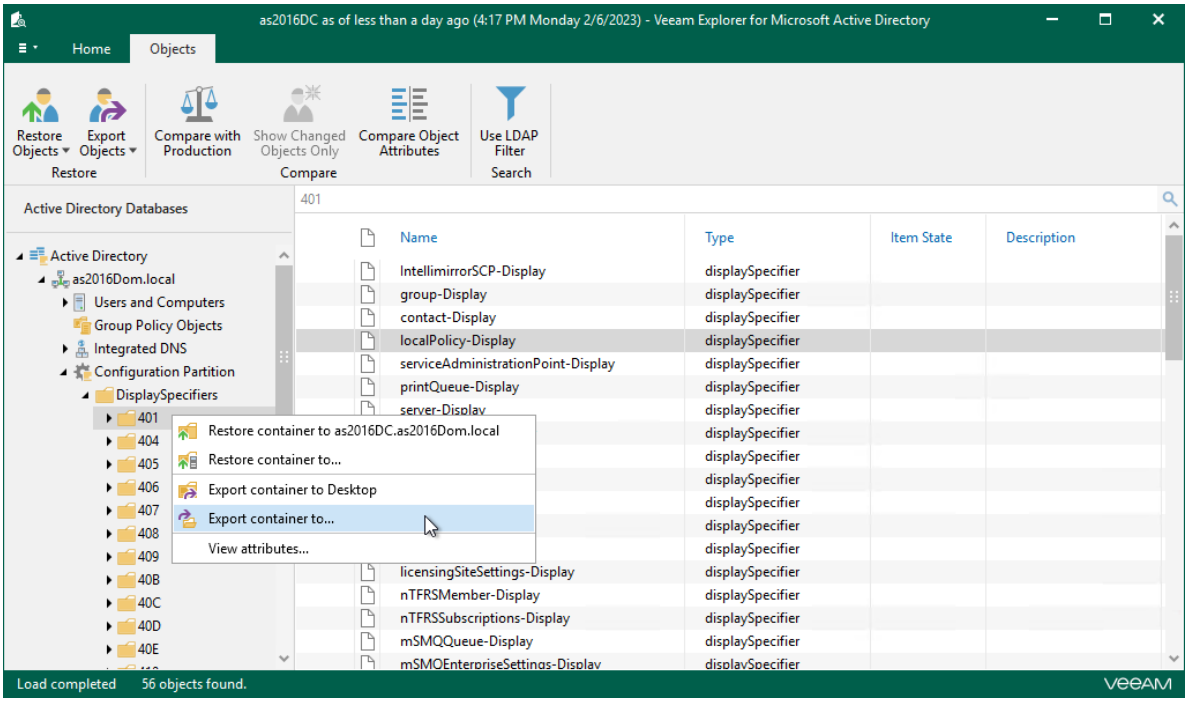
1. In the preview pane, select an object.
2. On the **Objects** tab, select **Export Objects** > **Export objects to** or right-click an object and select **Export objects to**.
3. Specify the destination folder and click **Save**.



Exporting Containers

To export containers and their contents, do the following:

1. In the preview pane, select a container.
2. On the **Container** tab, select **Export Container** > **Export container to** or right-click a container and select **Export container to**.



3. In the **Export Container** window, in the **Export to** field, specify the destination location.

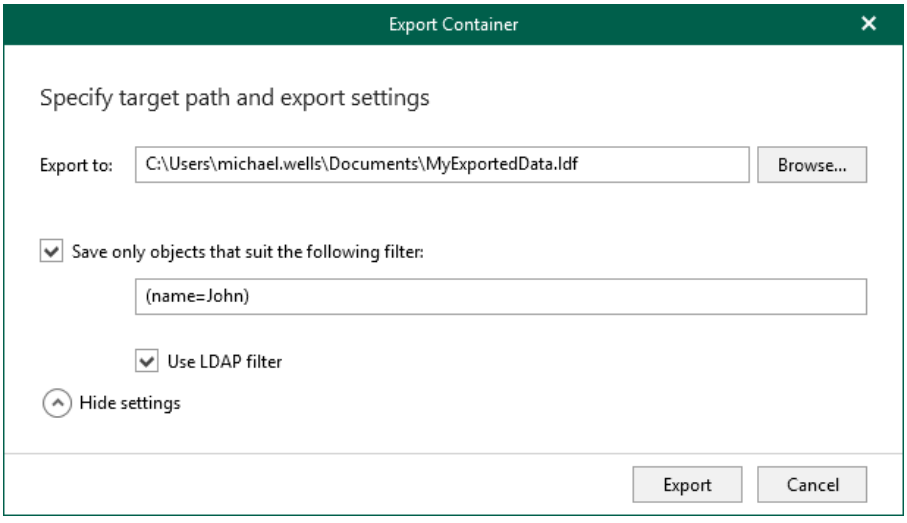
   To save only objects included in the selected container and meet specific filtering criteria, click **Show settings** to set the filter.

4. [Optional] Select the **Save only objects that suit the following filter** check box and enter filtering criteria.

   If necessary, select the **Use LDAP filter** check box to switch to the LDAP filtering mode.

5. Click **Export**.

   All the nested containers (if any) will be preserved during the export.

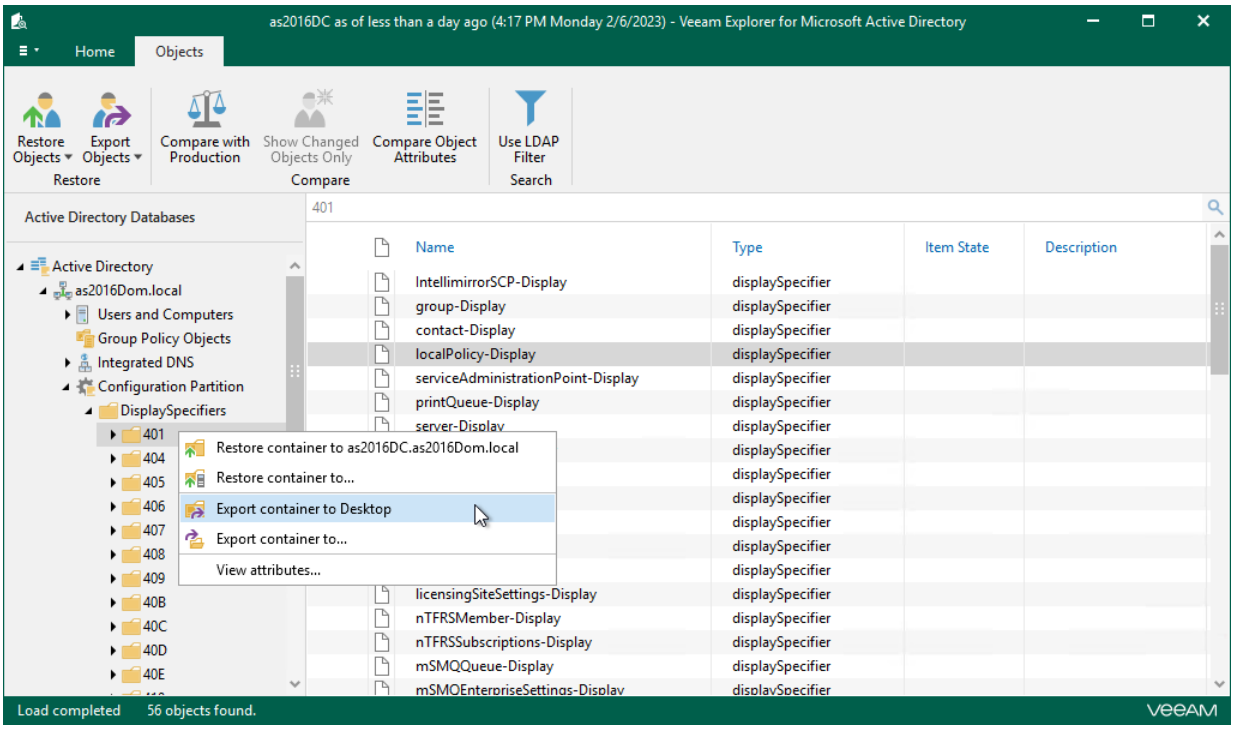


Using 1-Click Export

To export a container or object to a default location, do the following:

1. Select a container or object.
2. On the **Container** tab, select **Export Container** > **Export Container to <target_folder>** or **Export Objects** > **Export Object to <target_folder>**. Alternatively, you can use the associated context menu command.

> **NOTE**
>
> The **<target_folder>** destination depends on the location you used during the last export operation.



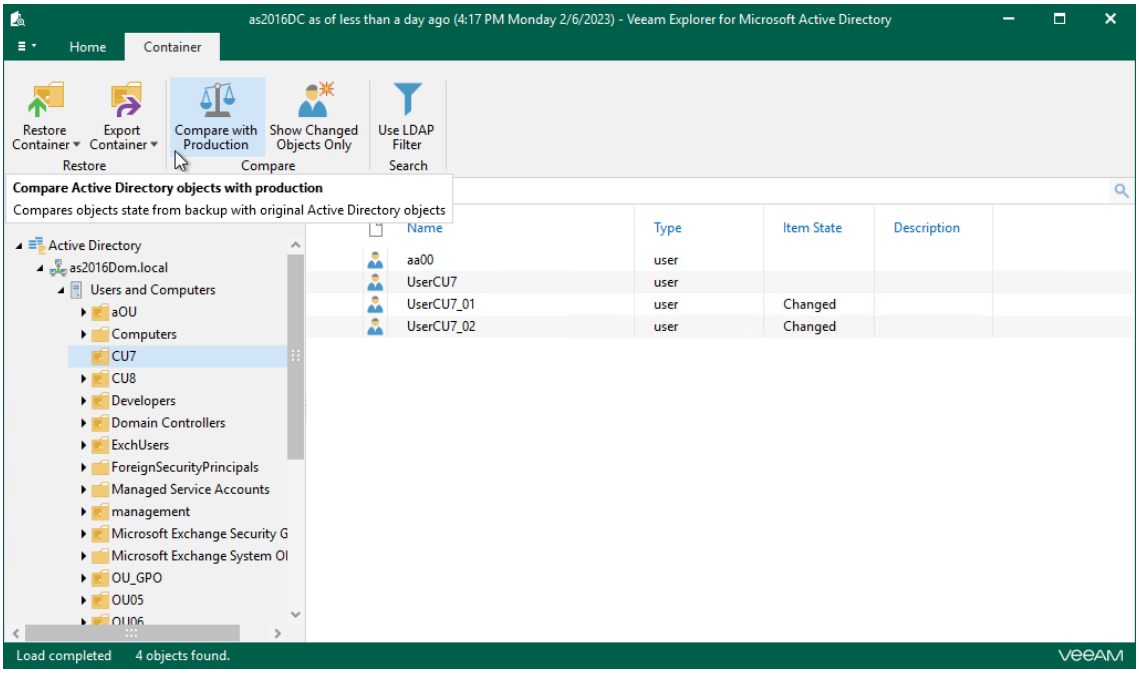
Data Compare

This section explains how to use Veeam Explorer for Microsoft Active Directory to compare data in a backup file with that of the production state.

Comparing Active Directory Containers

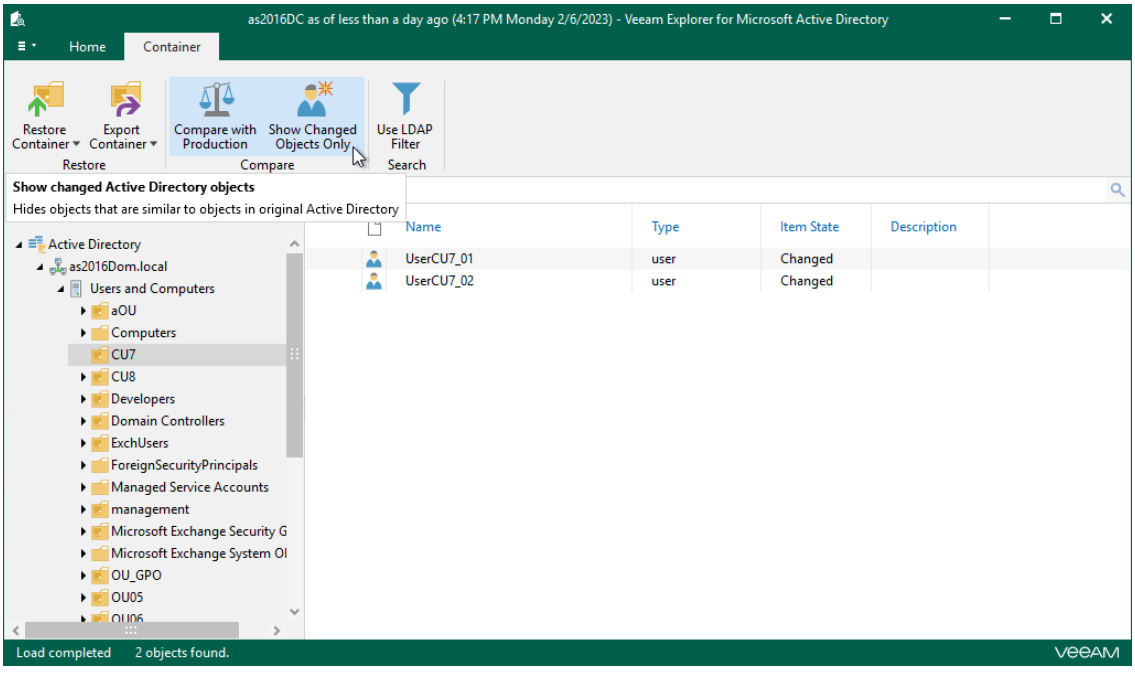
To compare Active Directory containers, do the following:

1. In the navigation pane, select a container.
2. On the **Home** tab, select **Compare with Production** to detect changed, moved or deleted objects since the last Active Directory backup.



3. Click **Show Changed Objects Only** on the ribbon to view only those items that have been changed since the last backup.

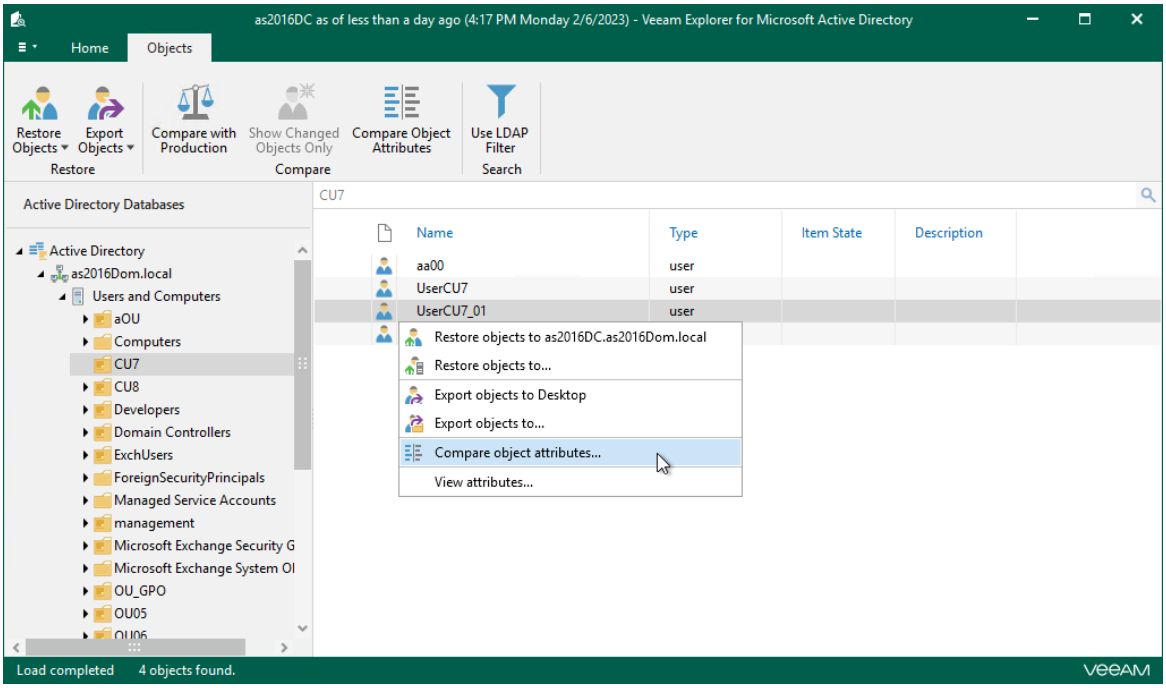
   The following figure shows user accounts the attributes of which have been changed since the last time they were backed up. Veeam can also combine item states to represent the most accurate state of an object. For example, if object attributes have been changed and the object was moved to a different location, the object status in this case will be shown as *Moved*, *Changed*.



Comparing Object Attributes

To compare Active Directory objects attributes, do the following:

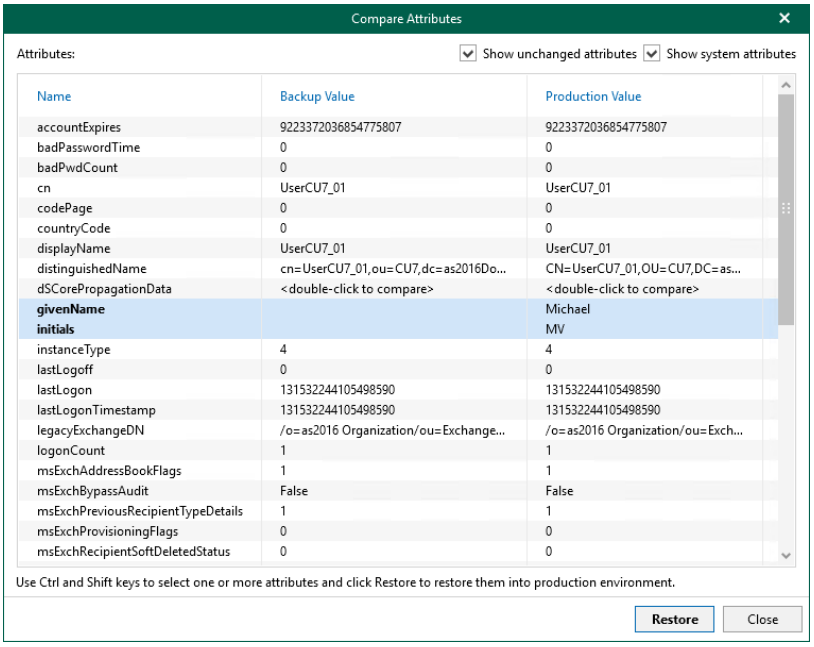
1. In the navigation pane, select a container.
2. In the preview pane, select an object.
3. On the **Objects** tab, select **Compare object attributes** or right-click an object and select **Compare object attributes**.



4. Review changed attributes.

   To show unchanged attributes, select **Show unchanged attributes** at the top-right corner. To show system properties, select **Show system attributes**.

   To restore an attribute, select it and click **Restore**. Multiple selection is also supported.



Veeam Explorer for Microsoft SQL Server

Veeam Explorer for Microsoft SQL Server allows you to restore and export Microsoft SQL Server databases and schema objects from backups created by Veeam Backup & Replication.

Planning and Preparation

Before you start using Veeam Explorer for Microsoft SQL Server, make sure your backup infrastructure meets the following requirements and limitations.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft SQL Server.

Component	Requirement
Microsoft SQL Server	For more information about supported versions of Microsoft SQL Server, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

NOTE

AlwaysOn Availability Groups are supported for Microsoft SQL Server 2012 and higher.

Consider the following:

- By default, the **AUTO_CLOSE** option for Microsoft SQL Server databases is set to **False**.

  If **AUTO_CLOSE** is enabled, your databases may be skipped from processing.
- To restore database items from a Microsoft SQL Server that is running Microsoft Windows ReFS, the backup server or Veeam Backup & Replication console must be installed on a machine that runs Microsoft Windows Server 2012 or later.
- To restore data from a server that is running Microsoft Windows ReFS 3.x, the backup server or Veeam Backup & Replication console must be installed on a machine that runs Microsoft Windows Server 2016.
- Nodes participating in AlwaysOn Availability Groups are supported, but using *Availability Group Listeners* as staging servers is not recommended.

Staging SQL Server Requirements

Consider the following:

- Make sure that the staging Microsoft SQL Server has the same or later version as the original SQL Server.
- A SQL Server included in Microsoft SQL Server Failover Cluster cannot be used as a staging system.
- Configure domain trusts when planning to add databases to the Veeam Explorer for Microsoft SQL Server scope manually. For more information, see Configuring Staging SQL Server.
- The following *Microsoft SQL Server Express Editions* can be used as a staging system:
  - *Microsoft SQL Server 2012 Express Edition* — for Microsoft Windows 2008 R2 and Windows 7
  - *Microsoft SQL Server 2016 Express Edition* — for other later versions

  Both editions come as part of the Veeam Backup & Replication distribution package.
- A Microsoft SQL Server instance can be used as a staging system.

NOTE

Databases that exceed 10 GB cannot be attached to the Microsoft SQL Server Express Edition due to Express Edition limitations. For more information, see the Editions and supported features of SQL Server 2022 Microsoft article.

Ports

The following tables list network ports that must be opened to manage inbound and outbound traffic.

Backup

From	To	Protocol	Port	Notes
Backup server, guest interaction proxy (Enterprise and Enterprise Plus editions)	Source machine with Microsoft SQL Server	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on the source machine.
		TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range that is used by the runtime coordination process which is deployed on the source machine for application-aware processing.[1]
		TCP	6167	**For Microsoft SQL Server transaction logs shipping** Port used by the runtime process on the source machine from which transaction logs are collected.
Source machine with Microsoft SQL Server	Backup server, guest interaction proxy (Enterprise and Enterprise Plus editions)	TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range used by the runtime coordination process that is deployed on the source machine for application-aware processing.[1] For more information, see this Microsoft article.
	Log shipping server, backup repository	TCP	2500 to 3300	**For Microsoft SQL Server transaction logs shipping** Default range of ports used by the Veeam Data Mover Service for data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information, see this Microsoft KB article.

Restore

From	To	Protocol	Port	Notes
Backup server, Veeam Backup & Replication console, mount server associated with the backup repository (only for Instant Recovery or restore from Enterprise Manager)	Target machine with Microsoft SQL Server, staging server	TCP, UDP	135, 445	Ports used to deploy the runtime coordination process on the target machine.
		TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range used by the runtime coordination process that is deployed on the target machine.[1] For more information, see this Microsoft article.
		TCP	6160	Port used to communicate with the installer service.
		TCP	1433, 1434	Ports used to communicate with the Microsoft SQL Server installed on the target machine during application-item restore. For more information, see this Microsoft article.
		UDP	1434	Port used by the Microsoft SQL Server Browser service. For more information, see this Microsoft article.
		TCP	1025 to 1034	Default RPC range for the runtime component installed on a target or staging Microsoft SQL Server machine to support restore. This port range is opened only during application item restore. **Note:** You must manually open these ports for `Veeam.SQL.Service.exe` in Microsoft Windows Firewall.

From	To	Protocol	Port	Notes
Target machine with Microsoft SQL Server, staging server	Mount server associated with the backup repository	TCP	3260 to 3270	Port range opened by Veeam Backup & Replication to manage iSCSI traffic during restore to the target machine. This port range is opened only during application item restore. For more information, see Mount Operations.

[1] If you use default Microsoft Windows Firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Permissions

The following table lists the required permissions for user accounts to restore Microsoft SQL Server data.

Operation	Required Roles and Permissions
Veeam Explorer for Microsoft SQL Server launch	The account used to run Veeam Explorer for Microsoft SQL Server must be a member of the local *Administrators* or *Users* group.
Restore, Publish, Instant Recovery	The account must be a member of the local *Administrators* group and must be granted the *sysadmin* role on the target Microsoft SQL Server. To learn more about Microsoft SQL Server roles, see this Microsoft article. The *sysadmin* role is required for connections with Microsoft SQL Server Virtual Device Interface (VDI) that Veeam Explorer for Microsoft SQL Server uses to perform recovery operations. For more information, see this Microsoft article.
Staging Microsoft SQL Server configuration	The account used to connect to the staging server must be a member of the *sysadmin* role on the Microsoft SQL Server. If you want to use a local Microsoft SQL Server as a staging server and Veeam Explorer for Microsoft SQL Server runs under an account that does not belong to the local *Administrators* group, you must specify the current account for connection to the staging server, or you will get an impersonation error. For more information on how to configure and use the staging Microsoft SQL Server, see Configuring Staging SQL Server.

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Configuring Transaction Logs

For more information about configuring transaction logs, see the Microsoft SQL Server Transaction Log Settings section of the Veeam Backup & Replication User Guide.

Recovery Model

> **NOTE**
>
> To be able to restore your data as of a point in time or as of a state before undesired transactions, make sure the recovery model for the database is set to **full** or **bulk-logged**.

The following table lists database logging models and applicable Veeam options.

SQL DB Logging Model	Veeam Options		
	Truncate logs	**Do not truncate logs**	**Backup logs periodically**
Simple	Databases are skipped from processing.	Applicable option.	Databases are skipped from processing. Log files do not grow (and do not need to be backed up).
Full	Applicable option. Veeam performs "backup to NUL" for log files on guest.	Applicable but not recommended to use without native or 3rd party means of log truncation or backup – otherwise, logs will increase in size.	Applicable option. Log backup files (.BAK) are copied from the temporary folder on the Microsoft SQL Server to a Veeam repository. As soon as the data is copied to the target, BAK files are deleted from the source.
Bulk-logged	Applicable option. Veeam performs "backup to NUL" for log files on guest.	Applicable but not recommended to use without native or 3rd party means of log truncation or backup – otherwise, logs will increase in size.	Applicable option. Log backup files (.BAK) are copied from the temporary folder on the Microsoft SQL Server to a Veeam repository. As soon as the data is copied to the target, BAK files are deleted from the source.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft SQL Server.

General

- When Veeam Explorer for Microsoft SQL Server is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft SQL Server does not support restore using PowerShell Direct, VIX API or vSphere Automation API.
- Table-level recovery is supported only for database tables with no external dependencies. Tables with external dependencies are tables extended to Microsoft Azure using the Stretch Database functionality and so on.
- To restore an encrypted database, consider reading this Veeam Knowledge Base article.
- The *Replace* logic is not supported when restoring schema objects.
- To restore a database from the AlwaysOn availability group node as of the selected transaction state, the nodes of such a group must be in the same time zone.
- Databases located on VM disks excluded from backup are displayed in Veeam Explorer for Microsoft SQL Server with a question mark next to each database. It is not possible to restore data of such databases.

Publishing

- During publishing, Veeam Explorer for Microsoft SQL Server mounts VMs disks from the backup file to the target machine (under the *C:|VeeamFLR* directory), retrieves required database files and attaches associated databases directly to your Microsoft SQL Server instance so that you can perform required operations using Microsoft SQL tools such as Microsoft SQL Server Management Studio.

  When publishing to a cluster, all VMs disks become part of the target cluster. Publishing to a cluster requires a free drive letter on all cluster nodes according to the number of clustered disks in the backup.
- You can publish the same database more than once.
- After you unpublish a database, Veeam Explorer for Microsoft SQL Server detaches such a database from the target Microsoft SQL Server but the restore point will continue to remain on the target machine for the next 15 minutes.
- If a Veeam Explorer for Microsoft SQL Server session has been terminated in any way other than by clicking **Exit** in the main menu (or by clicking the **X** button in the upper-right corner), then all the published databases will continue to remain attached to the target Microsoft SQL Server with the *Recovery pending* state.
- If published databases have been renamed manually using SQL tools (for example, *Microsoft SQL Management Studio*), Veeam Explorer for Microsoft SQL Server will not be able to unpublish such databases properly. In this case, all the renamed databases will continue to remain attached to the target Microsoft SQL Server and you will have to remove them manually using the SQL tools.
- Veeam Explorer for Microsoft SQL Server does not back up published databases.

- Upon closing the Veeam Explorer for Microsoft SQL Server console, all the published databases will be detached from the target Microsoft SQL Server instance automatically. Mount points will be also dismounted from under the `C:\VeeamFLR` directory.

Instant Recovery

- To restore an encrypted database, consider reading this Veeam Knowledge Base article.
- If you perform instant recovery of a database from the AlwaysOn availability group node, Veeam Explorer for Microsoft SQL Server restores it as a standalone database.
- For desktop versions of Microsoft Windows (7, 8, 8.1, 10), you must perform instant recovery of multiple databases one by one. The limitation occurs because desktop versions of Microsoft Windows OS do not allow more than 20 incoming concurrent TCP/IP connections. For details, see Microsoft Windows 10 License Terms.

  As a workaround, you can perform instant recovery of multiple databases in parallel using the Restore-VESQLIRDatabase PowerShell cmdlet.
- Instant recovery to a SQL Server cluster requires free drive letters on all cluster nodes. The number of free drive letters on each cluster node must be twice the number of clustered disks in the backup.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft SQL Server and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start**, click **Veeam Explorer for Microsoft SQL Server** and manually open Microsoft SQL databases, as described in the Adding Standalone Microsoft SQL Databases section.

If you open Veeam Explorer for Microsoft SQL Server from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

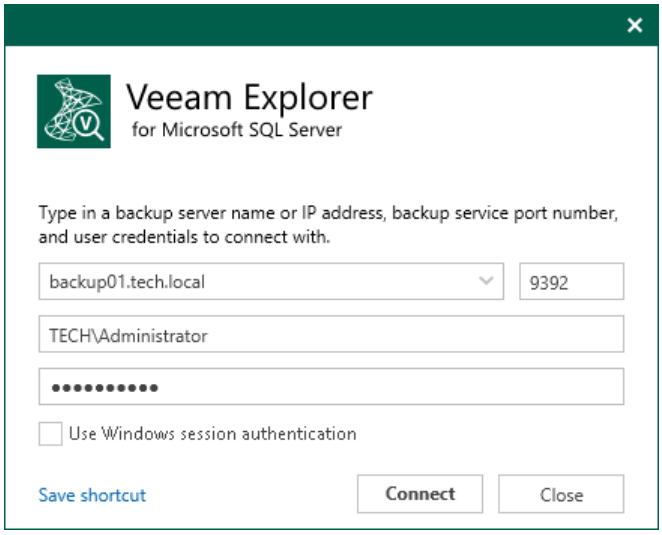
- The domain name or IP address of the backup server to which you want to connect
- The port number
- User account credentials

  Consider the following:

  - To perform recovery operations, Veeam Explorer for Microsoft SQL Server must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorers Suite is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft SQL Server is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

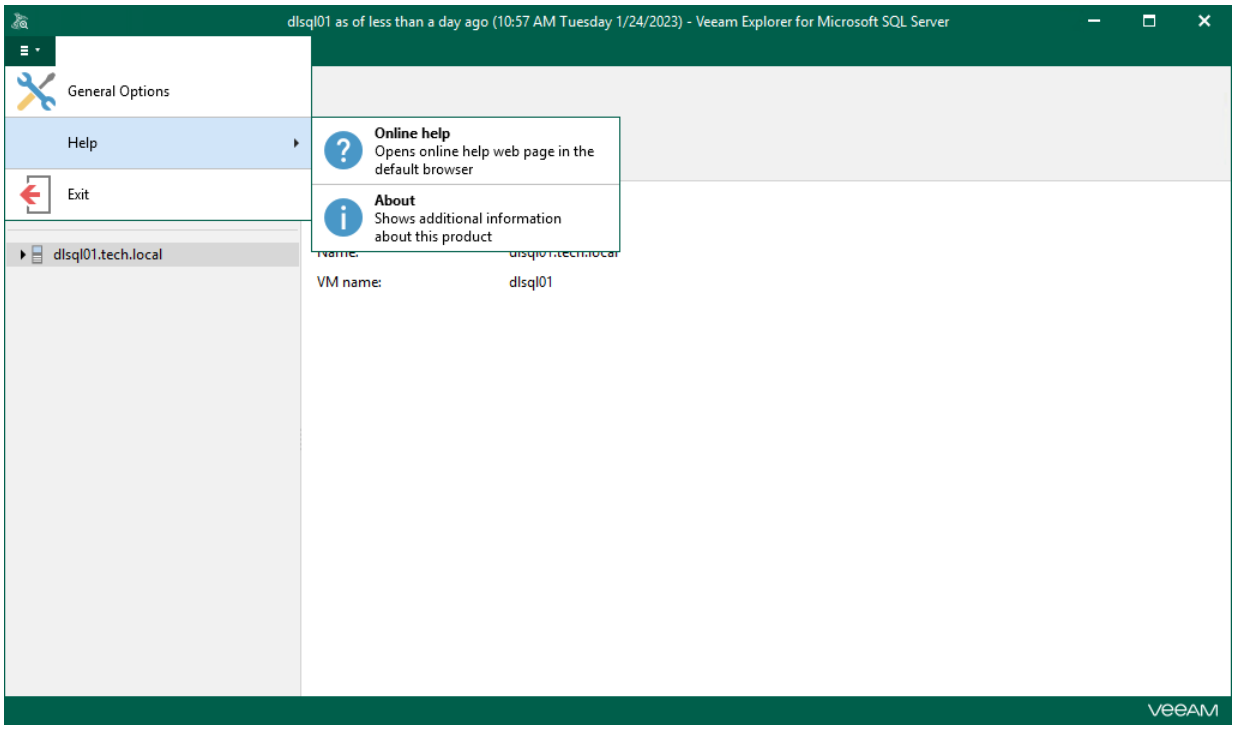
Veeam Explorer for Microsoft SQL Server provides you with a convenient user interface that allows you to perform the required operations in a user-friendly manner.

Main Menu

The main menu consists of the following:

- **General Options**. Allows you to configure general application settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows additional information, including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft SQL Server window.

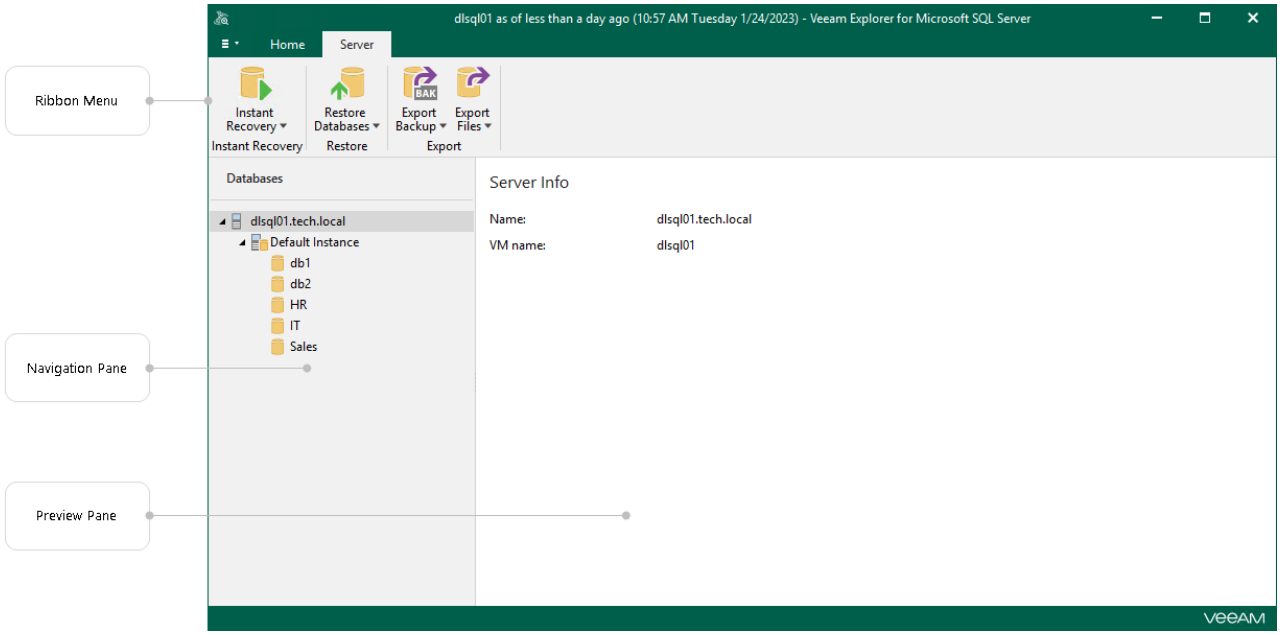
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft SQL Server wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your SQL databases.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



How Mounting Works

When restoring Microsoft SQL Server data, Veeam Explorer for Microsoft SQL Server requires an additional mount point to be created to display SQL Server transactions.

Mounting is performed by the *Veeam Mount Service* component which is deployed on a backup repository machine or any other machine you define in the backup repository settings. For more information, see the Mount Server section of the Veeam Backup & Replication User Guide.

During mounting, *Veeam Mount Service* retrieves a VM file system from the backup file, attaches it to the hard drive of the target machine and creates a mount point.

To mount a VM file system on to machines with the Microsoft Windows operating system, Veeam uses the iSCSI protocol. The original virtual machine or staging Microsoft SQL Server acts as an iSCSI initiator, and a mount server associated with the backup repository acts as an iSCSI target. The iSCSI mount point is non-persistent and only exists during the recovery process.

> **NOTE**
>
> When using fine-tune restore or point-in-time state restore, Veeam always uses a staging Microsoft SQL Server to mount the VM file system.

How Veeam SQL Restore Service Works

The *Veeam SQL Restore Service* runtime component is used to support restore activities on a VM guest operating system during the restore session. It checks the valid rights assignments required for database restore, gets information about the databases, and performs required file operations including database and transaction logs copy.

After the recovery session is ended, the service is stopped and removed from the guest operating system.

All service activities are logged to the `Veeam.SQL.Service_<timestamp>.log` file stored in the `Temp` folder which is located in the system directory.

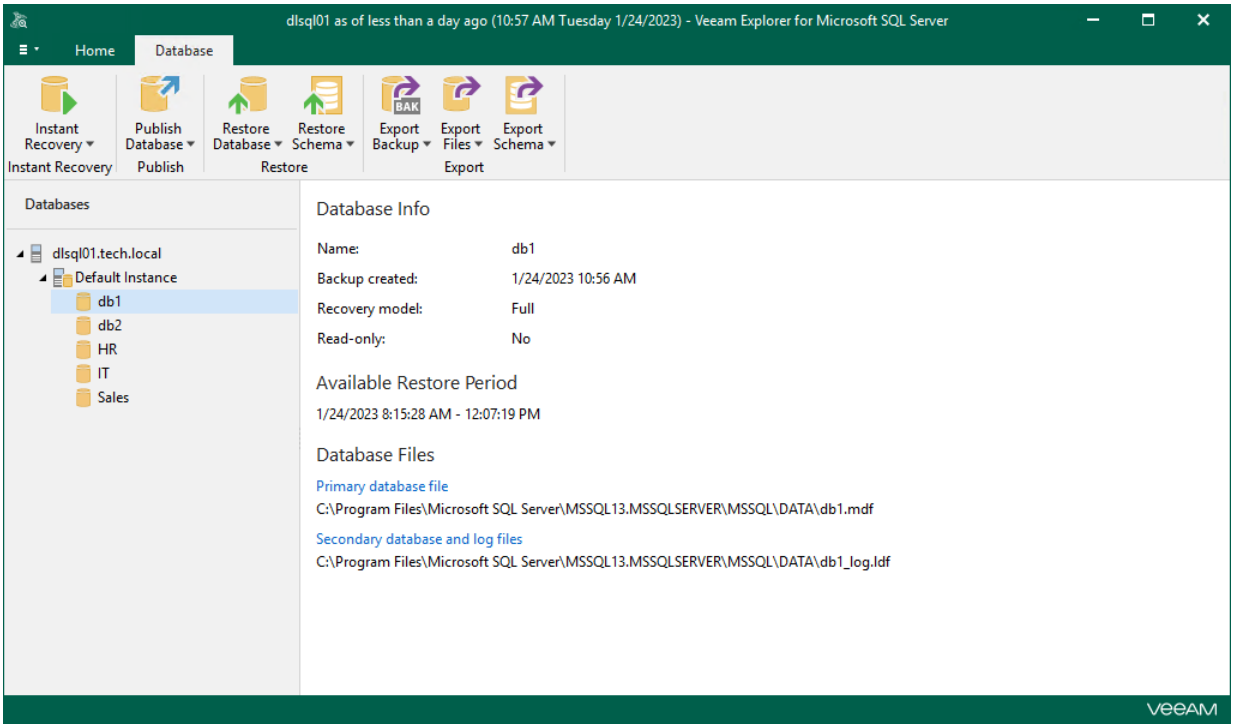
The *Veeam SQL Restore Service* component requires the Local System account.

Inbound and outbound traffic management between Veeam Explorer for Microsoft SQL Server and the *Veeam SQL Restore Service* component is performed over the RPC protocol. For more information, see Ports.

> **NOTE**
>
> When restoring to the local server instance, the Veeam SQL Restore Service component is not installed on the Microsoft SQL Server machine.

Viewing Database Information

To get information about databases, select a database in the navigation pane and review database info in the preview pane.



General Application Settings

This section explains how to configure the required application settings and components in Veeam Explorer for Microsoft SQL Server.

Configuring Staging SQL Server

A staging Microsoft SQL Server is required in the following cases:

- When exporting data, as described in Data Export.
- When using the fine-tune restore, as described in Data Restore and Data Publishing.
- When adding standalone Microsoft SQL Server databases to Veeam Explorer for Microsoft SQL Server, as described in Adding Standalone Databases.

A machine used as a staging Microsoft SQL Server for the data export, data restore and data publishing operations can reside in the same domain as the machine hosting Veeam Explorer for Microsoft SQL Server, as well as in a trusted domain or untrusted domain.

For the add standalone database operation, consider the following:

- A machine used as a staging SQL Server can reside in the same domain as the machine hosting Veeam Explorer for Microsoft SQL Server or in a trusted domain. You cannot use a staging server that belongs to an untrusted domain to add a standalone database to Veeam Explorer for Microsoft SQL Server.
- Both *Windows authentication* and *SQL Server authentication* methods are supported for the staging SQL Server. If you want to use *Windows authentication*, complete the following steps to configure delegation settings:
  a. In **Active Directory Users and Computers**, select a staging SQL Server.
  b. Open server properties and go to the **Delegation** tab.
  c. Select the **Trust this computer for delegation to specified services only** and **Use any authentication protocol** options for the *cifs* service on a computer with Veeam Explorer for Microsoft SQL Server.
  d. Restart the staging SQL Server VM.
  e. Select a domain user account that you want to use when connecting to the staging SQL Server VM and make sure the **Account is sensitive and cannot be delegated** check box is not selected.

To configure a staging server, do the following:

1. In the Veeam Explorer for Microsoft SQL Server main menu, click **General Options**.
2. On the **Staging Server** tab, select the **Use this helper SQL Server for advanced recovery functionality** check box and do the following:
   a. In the **SQL Server name** drop-down list, select a server that you want to use as your staging SQL Server.

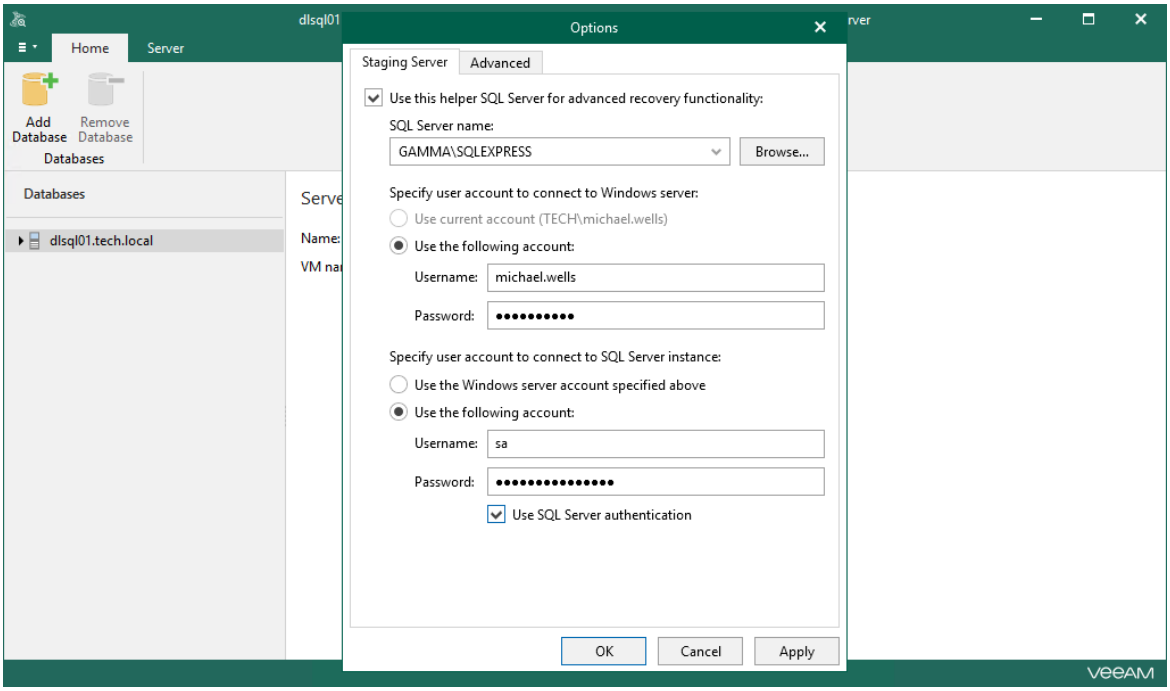
      You can click **Browse** to locate a server using the built-in browser, as described in Browsing for Servers.
   b. In the **Specify user account to connect to Windows server** section, select the following:
      - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Microsoft SQL Server running.
      - **Use the following account**. To connect to the specified server under a custom user account.

        When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.
   c. In the **Specify user account to connect to SQL Server instance** section, select the following:

- **Use the Windows server account specified above**. To connect to the specified instance under the user account that you have specified in the **Specify user account to connect to Windows server** section.
- **Use the following account**. To connect to the specified instance under a custom user account.

  When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.

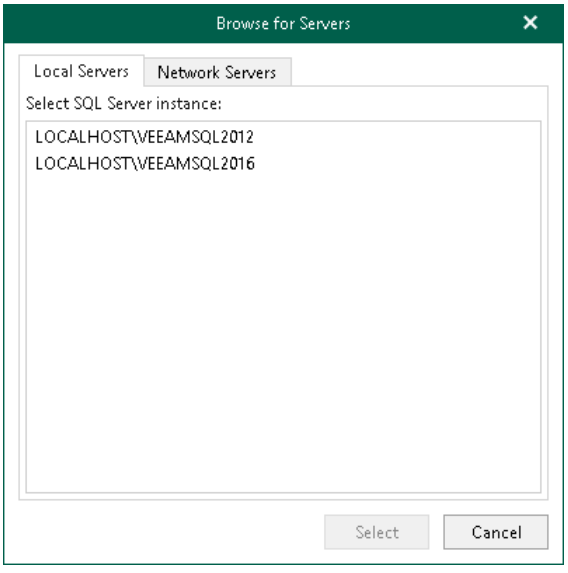
  To use SQL Server authentication, select the **Use SQL Server authentication** check box.



Browsing for Servers

To browse for a server, do either of the following:

- On the **Local Servers** tab, select a local SQL Server that is located on the machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL Server over the network.

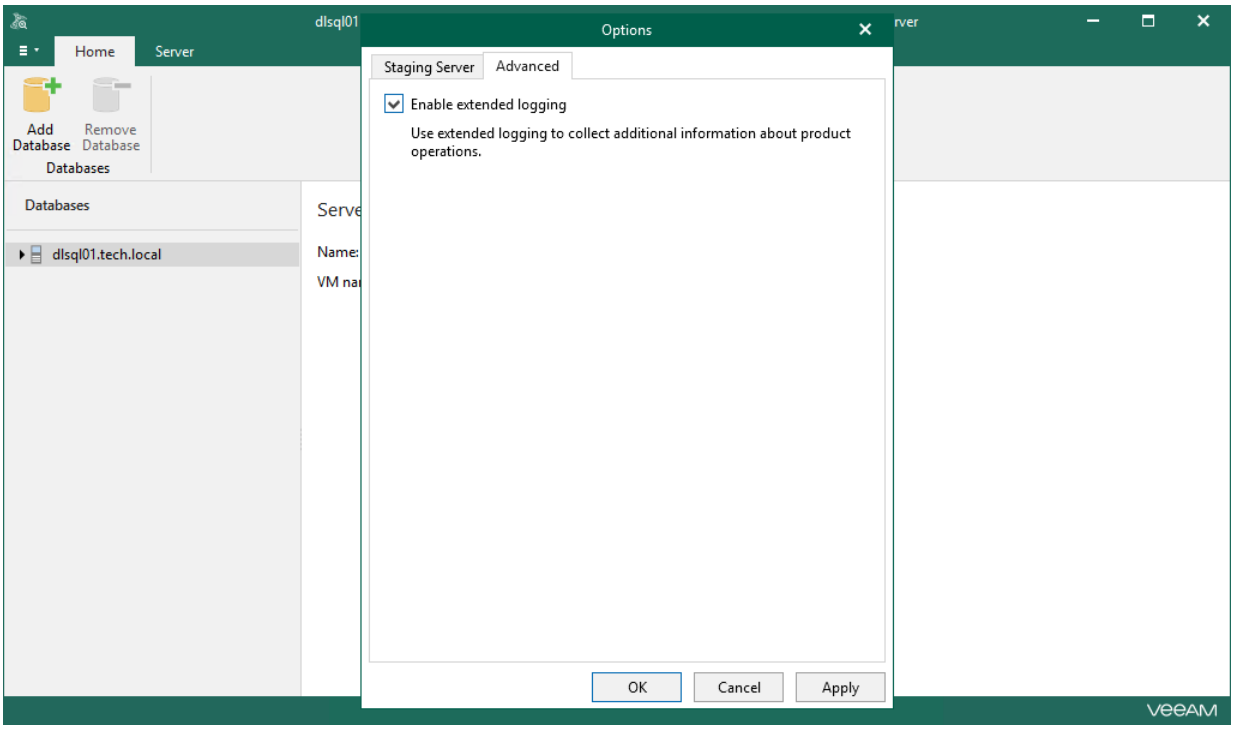


Enabling Extended Logging

Veeam Explorer for Microsoft SQL Server allows you to enable an extended logging mode to collect logs that contain more details on specific operations. After you enable extended logging, you can go back to the application and perform the actions for which you want to collect additional information. Then you can collect the logs.

To enable extended logging, do the following:

1. In the Veeam Explorer for Microsoft SQL Server main menu, click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box and click **OK**.



Standalone Databases Management

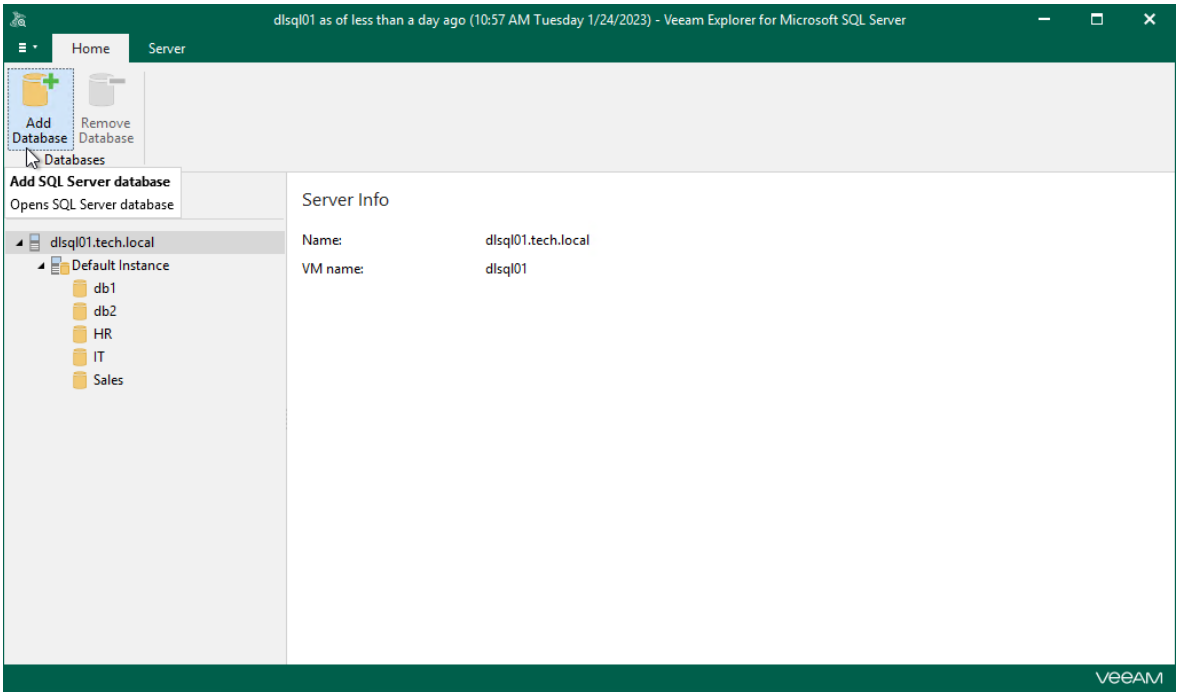
This section explains how to add and remove standalone Microsoft SQL Server databases.

Adding Standalone Databases

> **NOTE**
>
> Before you add a standalone Microsoft SQL database, you must configure a staging SQL Server. For more information, see Configuring Staging SQL Server.

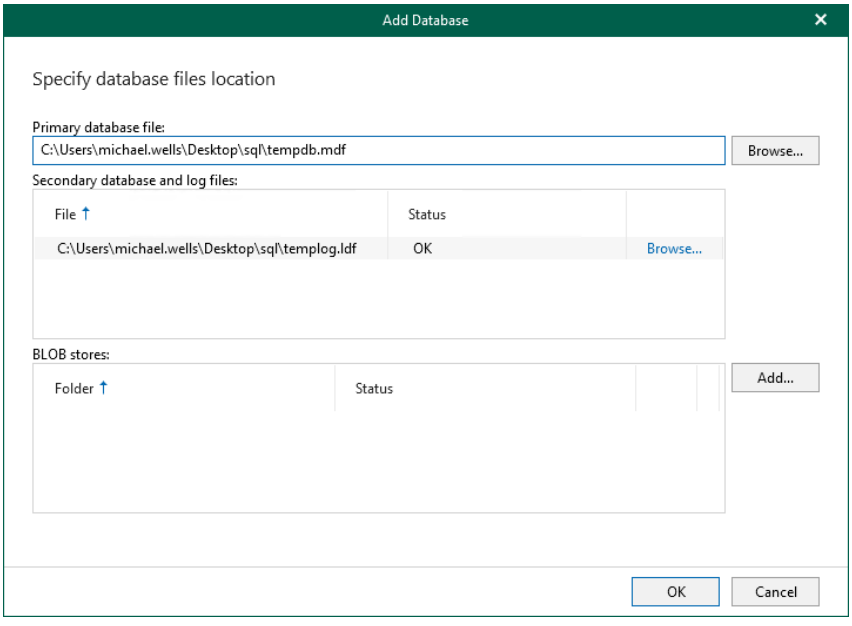
To add a standalone Microsoft SQL database manually, do the following:

1. On the **Home** tab, click **Add Database**.



2. Specify the location of a primary database file, a secondary database file and associated log files. If necessary, specify the BLOB store location.

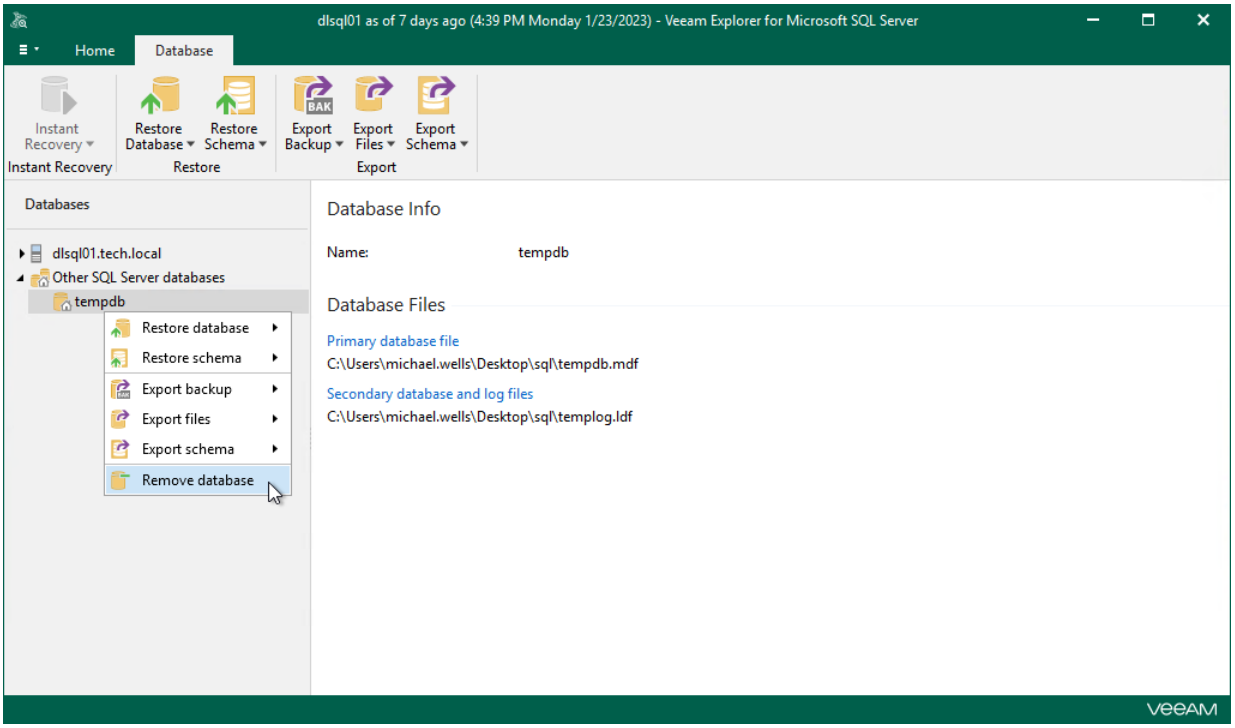
   Manually added databases will be displayed in the navigation pane under the **Other SQL Server Databases** node.



Removing Standalone Databases

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove database** or select a database in the navigation pane and click **Remove Database** on the **Home** tab.

> **NOTE**
>
> You can only remove databases that have been added to the application scope manually.



Data Restore

This section contains information about the available restore operations in Veeam Explorer for Microsoft SQL Server.

Before restoring data, read the Considerations and Limitations section.

Restoring Single Database

You can restore a Microsoft SQL Server database by following one of these scenarios:

- Restoring Latest State
- Restoring Point-in-Time State
- Restoring To Another Server

Restoring Latest State

You can restore a Microsoft SQL Server database as of the latest state in your backup file.

The data will be restored in the following manner:

- Database files will be copied to the original location and then mounted to the original Microsoft SQL Server.
- If a database with the same name already exists on a target Microsoft SQL Server, it will be replaced with the database from a backup file.

To restore the latest available state of a Microsoft SQL Server database, do the following:

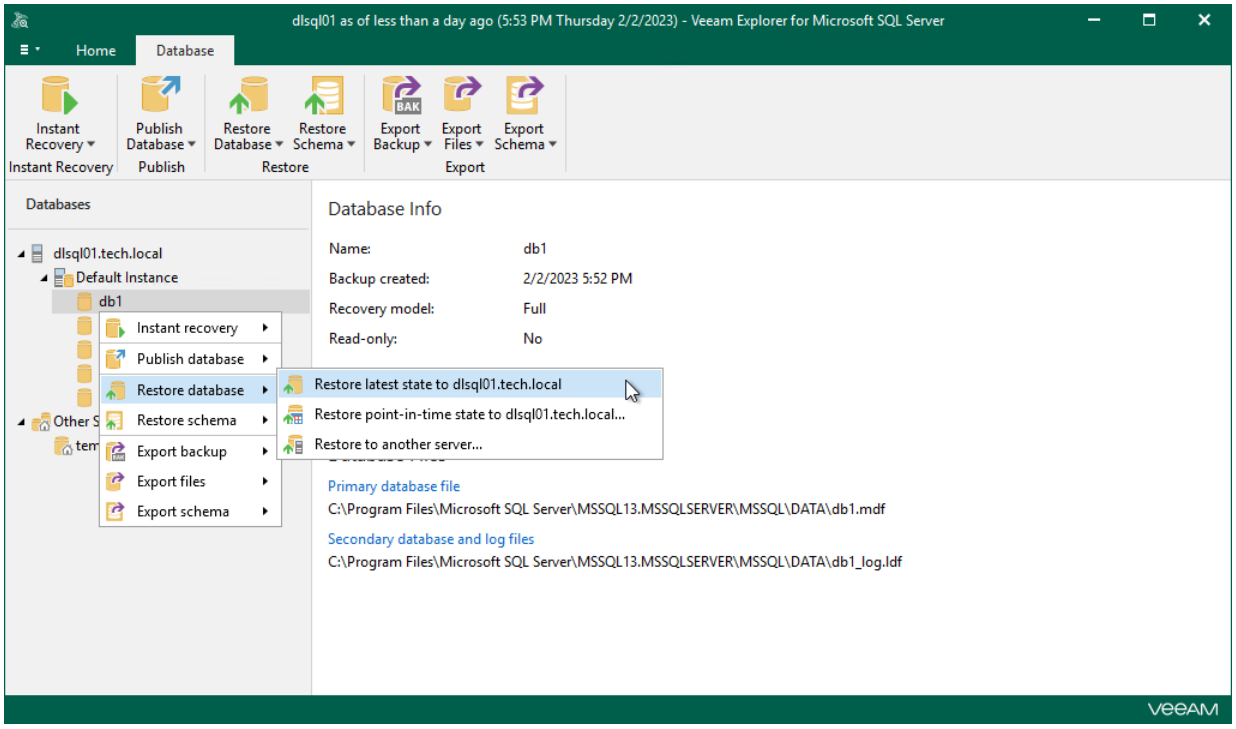
1. In the navigation pane, select a database.

   You can select the root instance node to restore all the available databases at once.

2. On the **Database** tab, select **Restore Database > Restore latest state to <original_location>**.

Alternatively, you can right-click a database and select **Restore database** > **Restore latest state to <original_location>**.

> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Restoring Point-in-Time State

You can restore a Microsoft SQL Server database as of a point-in-time state in your backup file.

The data will be restored in the following manner:

- Database files will be copied to the original location and then mounted to the original Microsoft SQL Server.
- If a database with the same name already exists on a target Microsoft SQL Server, it will be replaced with the database from a backup file.

To restore SQL Server databases as of a point-in-time state, use the **Restore** wizard.

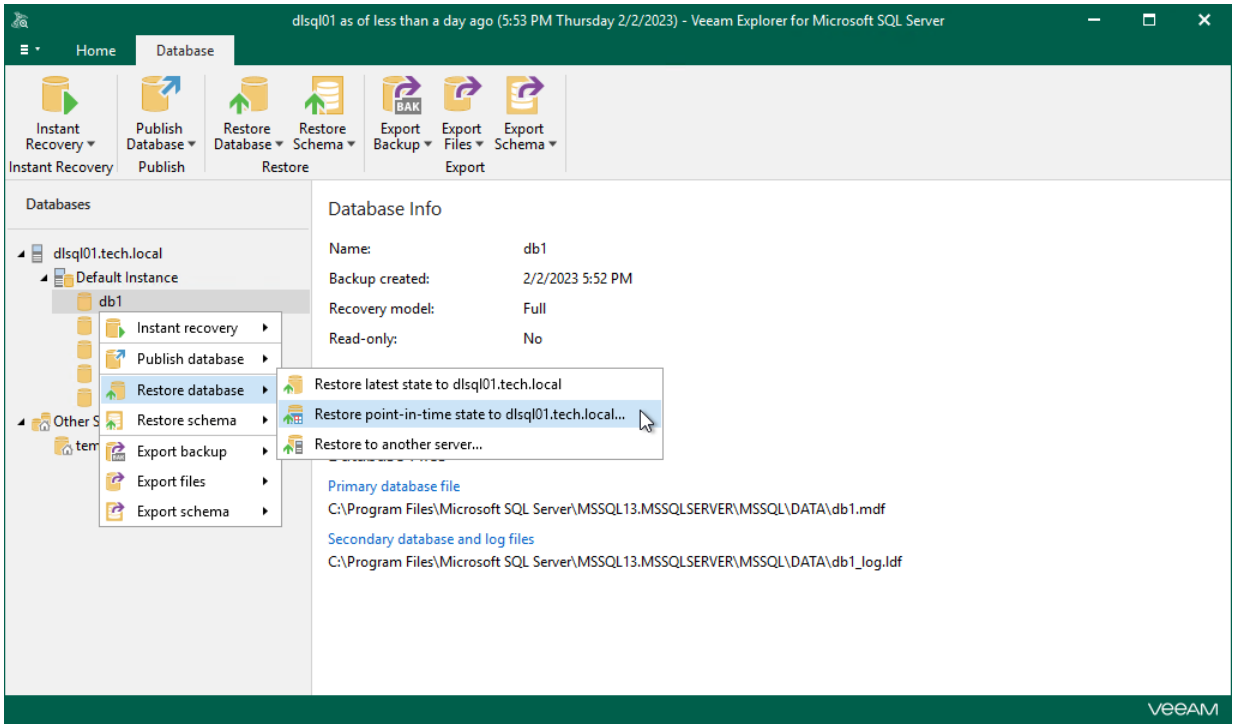
1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Restore Database > Restore point-in-time state to <server_name>\<instance_name>**.

Alternatively, you can right-click a database and select **Restore database** > **Restore point-in-time state to <server_name>\<instance_name>**.



Step 2. Specify Restore Point

At this step of the wizard, specify a state to which you want to restore your database:

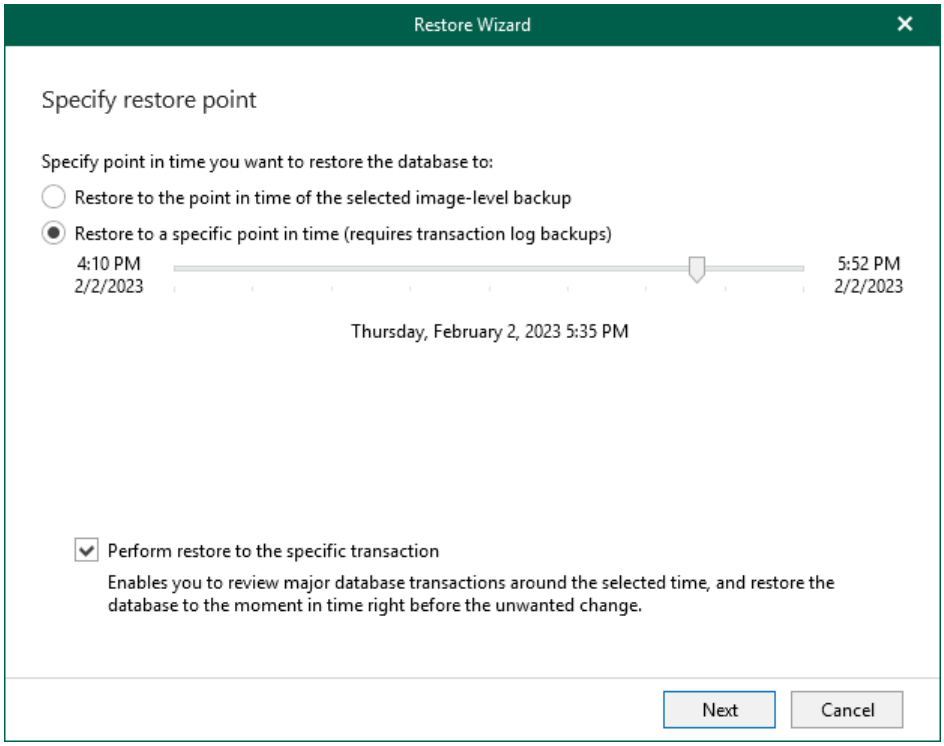
1. In the **Specify point in time you want to restore the database to** section, select one of the following options:
   - **Restore to the point in time of the selected image-level backup**. Select this option to load database files as per date of the current restore point.
   - **Restore to a specific point in time**. Select this option to load database files as per selected point in time. Use the slider control to choose a point you need.

     This option is available in case the following conditions are met:

     - [For restore from a backup created by a backup job] The backup is created by a job that is set to back up transaction logs or process transaction logs in the copy only mode.
     - [For restore from a backup created by a backup copy job] The backup is created by a job that is set to process transaction logs.
     - The recovery model for the database is set to *full* or *bulk-logged*.
2. [Optional] Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions. If you select this option, you will be able to specify an exact transaction at the next step of the wizard.

   This option requires a staging Microsoft SQL Server. For more information, see Configuring Staging SQL Server.

   This option is unavailable when restoring multiple databases.

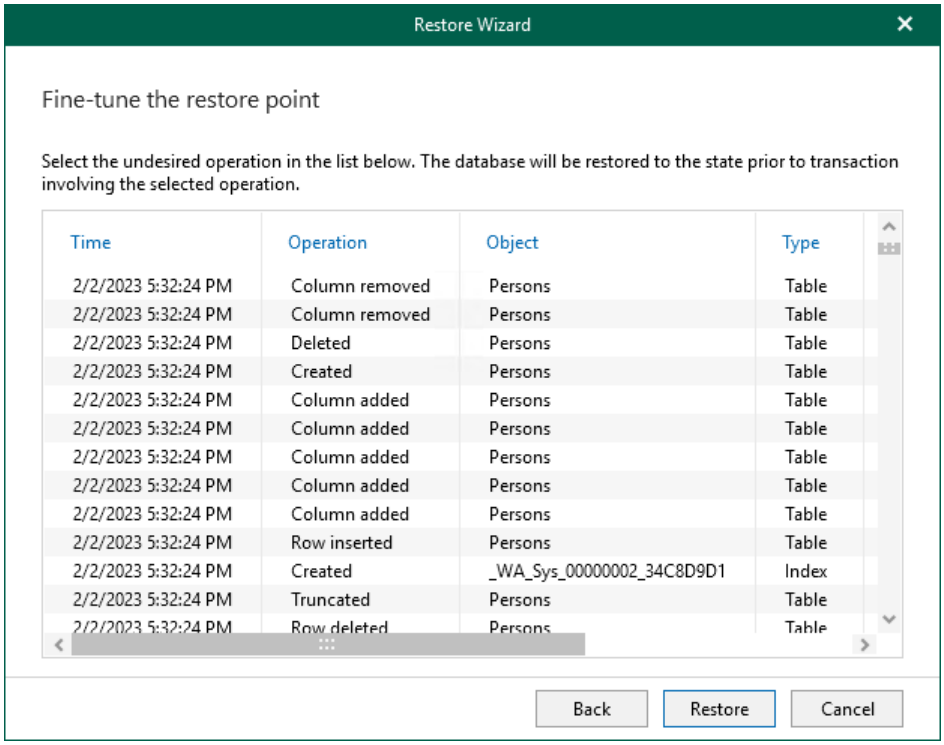


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore your database and click **Restore**.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Restoring to Another Server

To restore a single Microsoft SQL Server database to another server, use the **Restore** wizard.

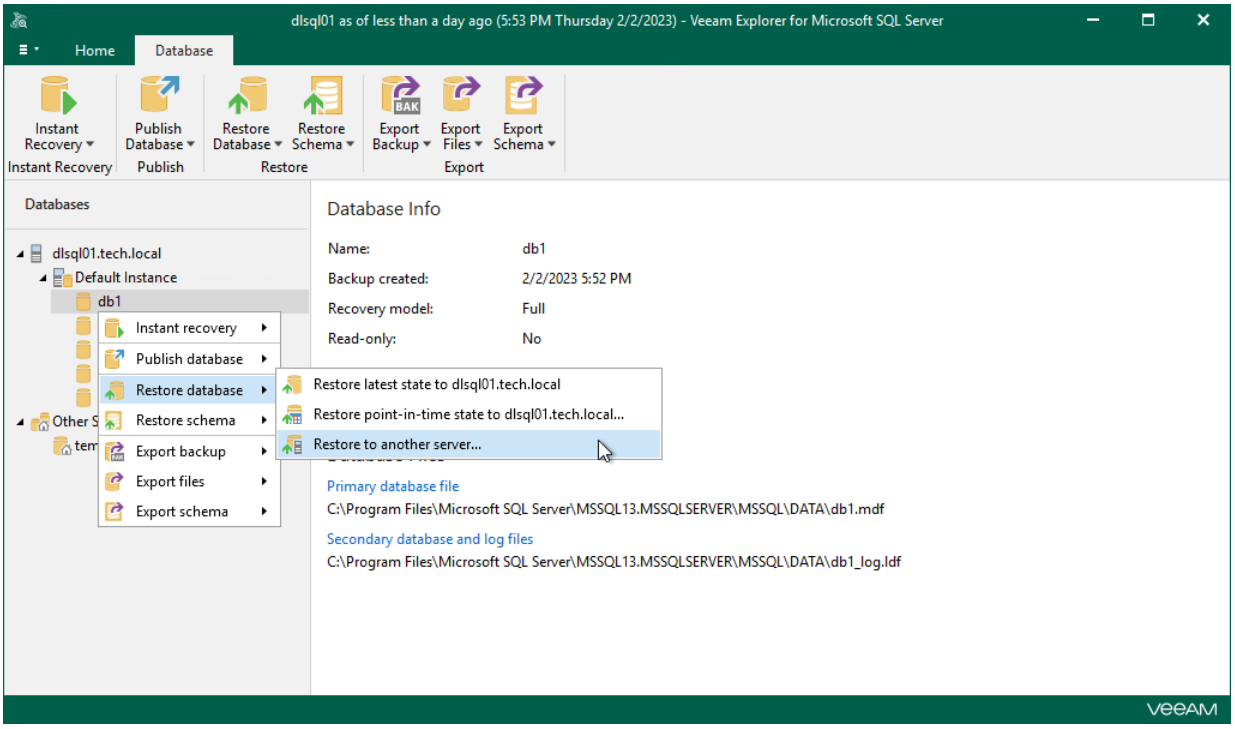
1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify AlwaysOn restore options.
6. Specify files location.
7. Specify the recovery state.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Restore Database** > **Restore to another server**.

Alternatively, you can right-click a database and select **Restore database** > **Restore to another server**.



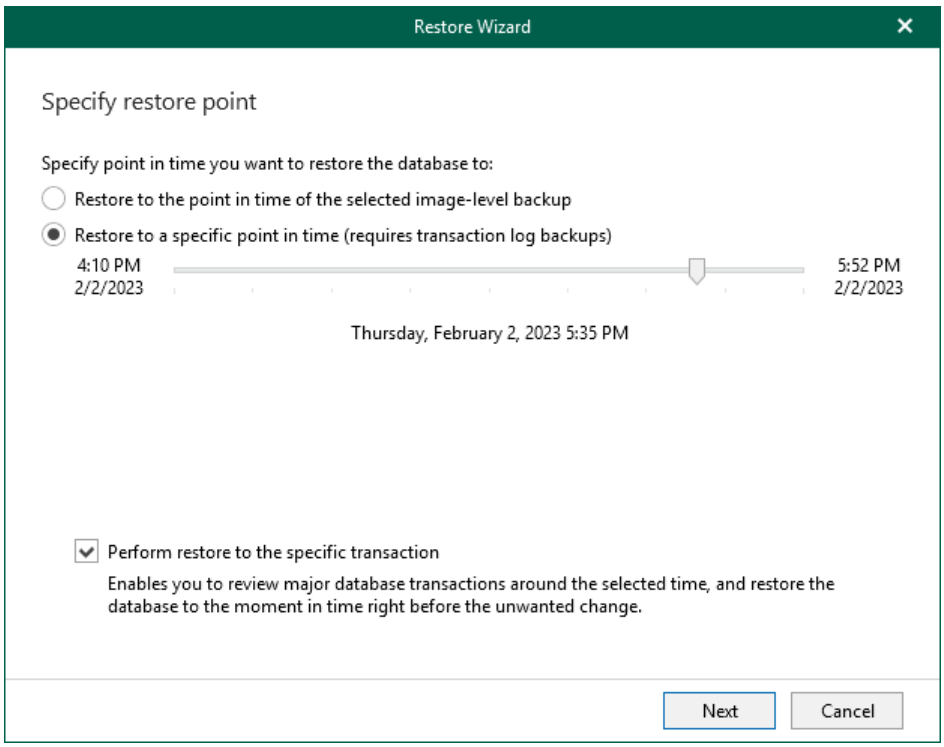
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Microsoft SQL Server. For more information, see Configuring Staging SQL Server.

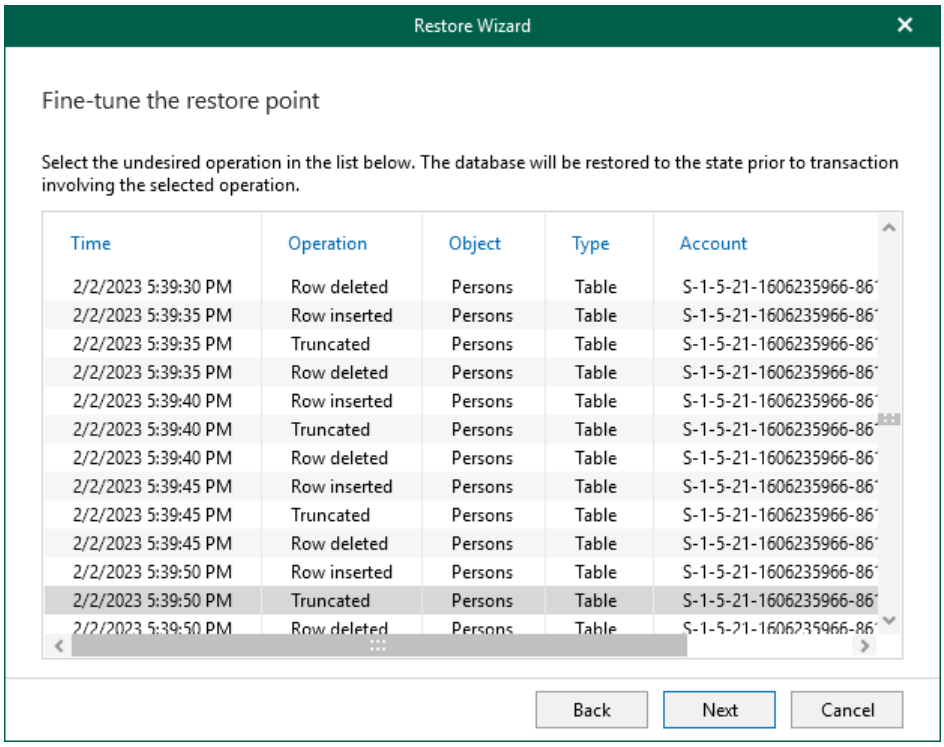


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to recover your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Server

At this step of the wizard, do the following:

1. In the **Server name** field, specify the name of the Microsoft SQL Server machine or SQL Server instance to which you want to restore your database.

   Use the *<server IP or FQDN>|<instance name>* format. You can select a server or instance from the drop-down list or use the **Browse** button, as described in Browsing for Servers.

   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 **Database name** filed, specify a name for the restored database.

3. In the **Specify user account to connect** section, select either of the following options:

   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Microsoft SQL Server is running.

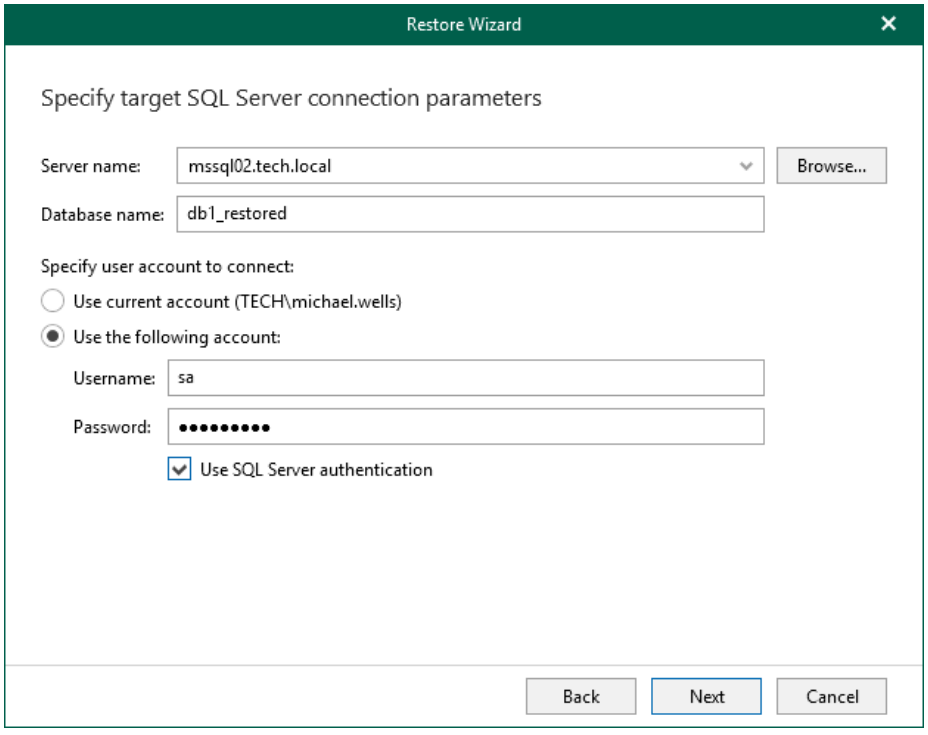
     You cannot use this option if Veeam Explorer for Microsoft SQL Server and mount server are located on separate machines.

   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

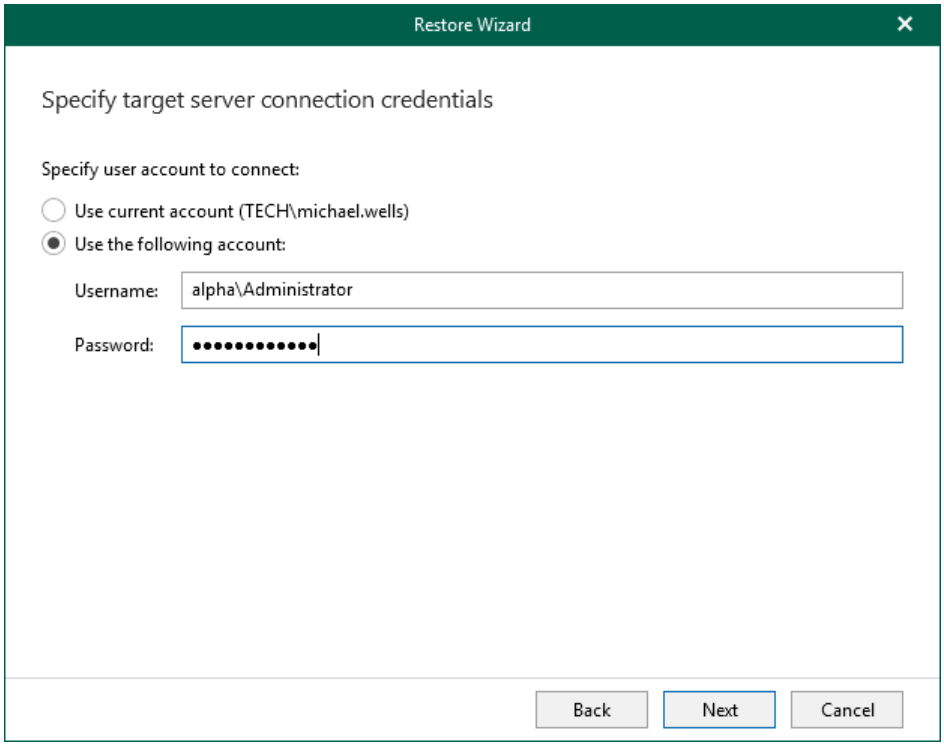
   Make sure the account you are using has been granted the **sysadmin** role on the target SQL Server machine.

4. If you selected the **Use the following account** option and want to use Microsoft SQL Server authentication, select the **Use SQL Server authentication** check box. If you do not select the check box, Veeam Explorer for Microsoft SQL Server will use Windows authentication.

> **IMPORTANT**
>
> Make sure that the administrative share (for example, `\\myserver\ADMIN$`) on the target machine is available. **Read** and **Write** are minimum required, **Full Control** is recommended.



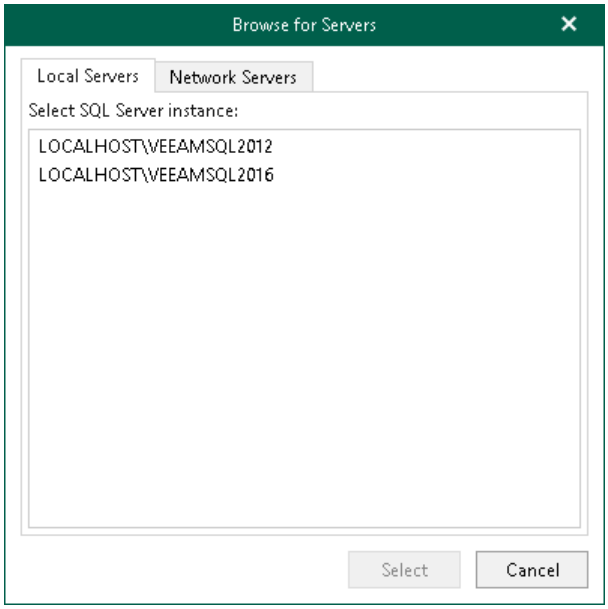
If you select the **Use SQL Server authentication** check box and provide a Microsoft SQL Server account, you will be prompted to provide an account to connect to the target server at the next step of the wizard.



Browsing for Servers

To browse for a server, do either of the following:

- On the **Local Servers** tab, select a local Microsoft SQL Server that is located on the machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL Server over the network.



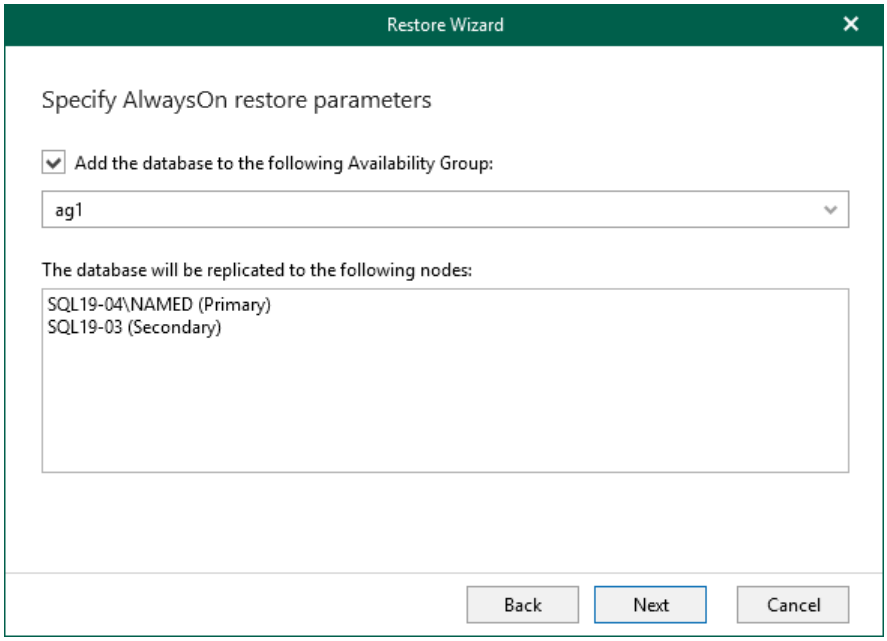
Step 5. Specify AlwaysOn Restore Options

If the specified target Microsoft SQL Server supports AlwaysOn Availability Groups, you will be offered to specify AlwaysOn restore options. To use the AlwaysOn capabilities for the restored database, do the following:

1. Select the **Add the database to the following Availability Group** check box and select an availability group from the drop-down list.
2. In the **The database will be replicated to the following nodes** list, review information about the primary and secondary nodes of the availability group.

   During the restore process, Veeam Explorer for Microsoft SQL Server will restore the database to the primary server and then replicate it to secondary nodes.

If you do not plan to use the AlwaysOn capabilities when restoring a database, clear the **Add the database to the following Availability Group** check box.



Step 6. Specify Files Location

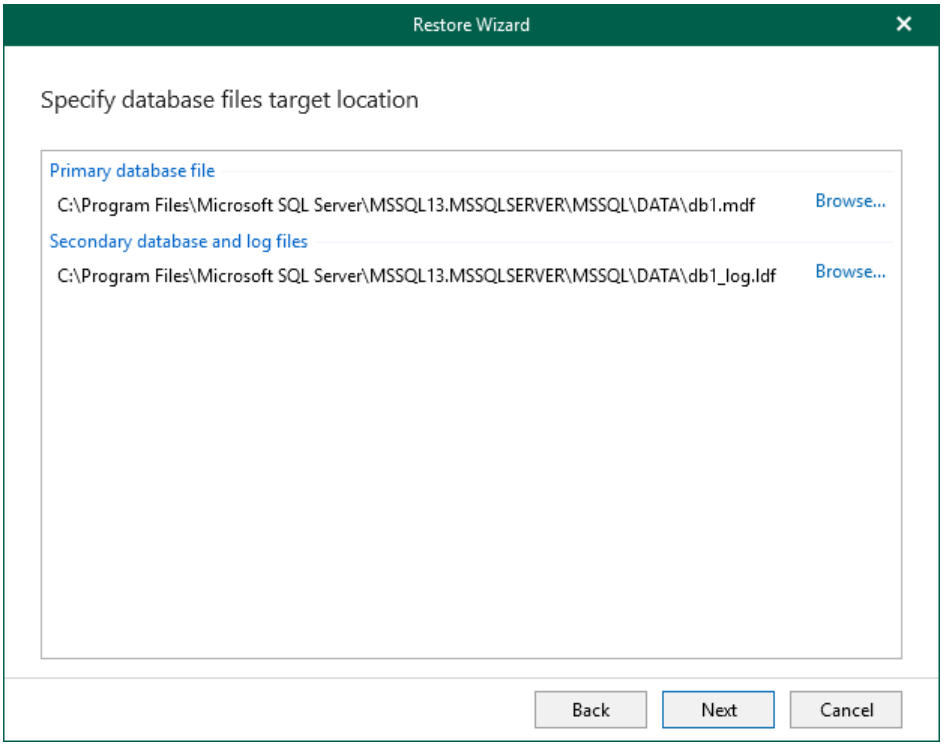
At this step of the wizard, specify the following file locations.

- Primary database file
- Secondary database file and log files
- BLOB stores (if necessary)

> **NOTE**
>
> Make sure the account you are using has **Read** and **Write** permissions.

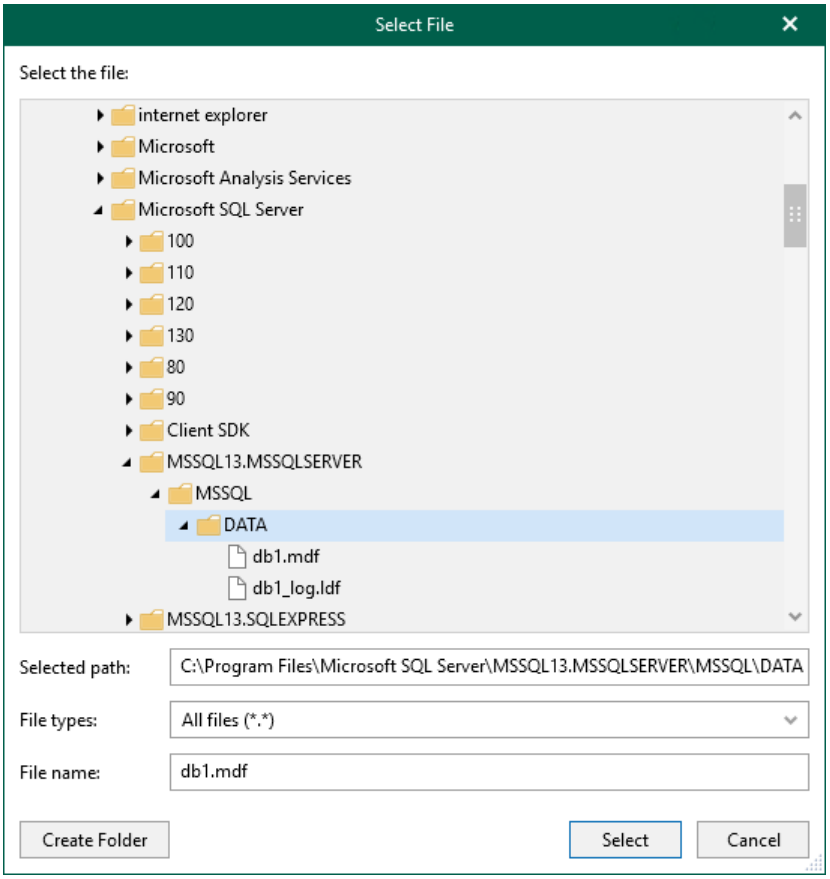
To specify a file location, do the following:

1. Click **Browse** next to the necessary database file type.



2. In the **Select File** dialog, choose a database file or folder for the restored database and click **Select**. To create a new folder, click **Create Folder**.

   [For restore to another location] To prevent you from storing BLOBs from different databases in the same directory, Veeam Explorer for Microsoft SQL Server supports creating a BLOB stores folder using the **Restore** wizard only. If you select an already existing folder, Veeam Explorer for Microsoft SQL Server will display an error.



Step 7. Specify Recovery State

At this step of the wizard, select recovery state:

- **Default (RECOVERY)**

  Rolls back (*undo*) any uncommitted changes.

- **NORECOVERY**

  Skips the undo phase so that uncommitted or incomplete transactions are held open.

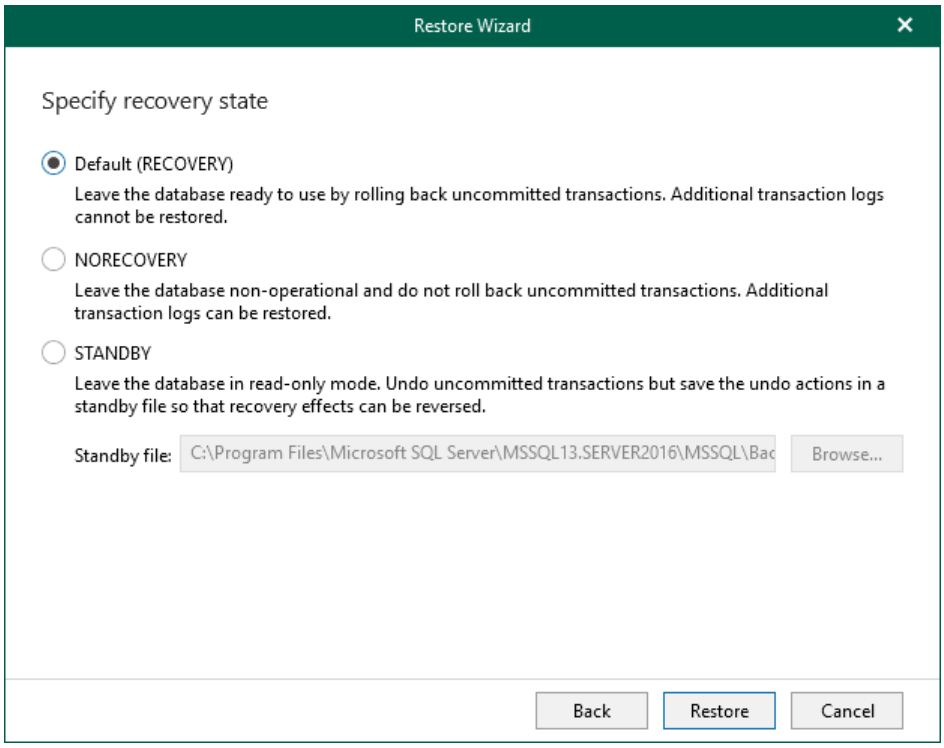
  This allows further restore stages to carry on from the restore point. When applying this option, the database will be in a *norecovery* state and inaccessible to users.

- **STANDBY**

  The database will be in *standby* state and therefore available for read operations. You can also provide a standby file with uncommitted transactions.

For more information on recovery modes, see this Microsoft article.

> **NOTE**
>
> This step is unavailable if the **Add the database to the following group** check box is selected at the Specify AlwaysON Restore Options step.



Restoring Multiple Databases

You can restore multiple Microsoft SQL Server databases by following one of these scenarios:

- Restoring Latest State
- Restoring Point-in-Time State
- Restoring To Another Server

Restoring Latest State

You can restore the latest available state of multiple Microsoft SQL Server databases. You can select databases from a specific server instance or across all instances on the machine.

To restore the latest available state of multiple databases, use the **Restore** wizard.

1. Launch the Restore wizard.
2. Select databases you want to restore.

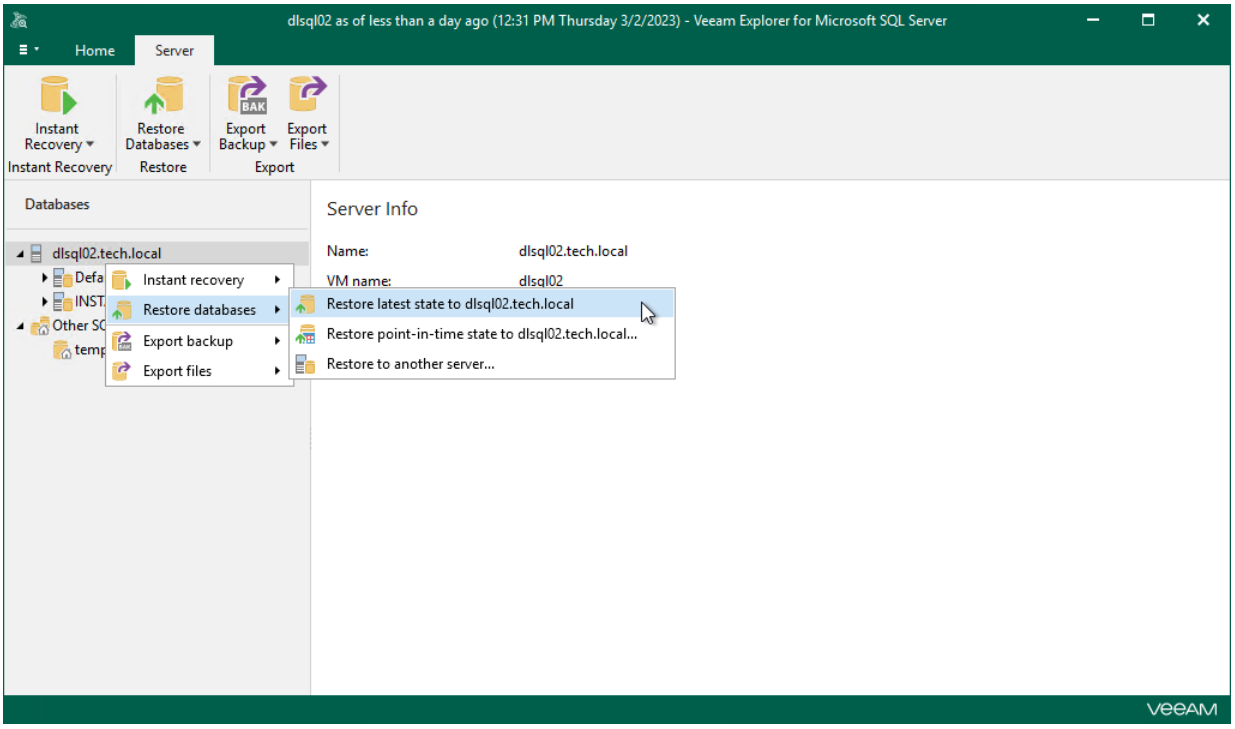
Step 1. Launch Restore Wizard

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

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Restore Databases > Restore latest state to <original_location>**.

Alternatively, you can right-click an instance or the server and select **Restore databases** > **Restore latest state to <original_location>**.

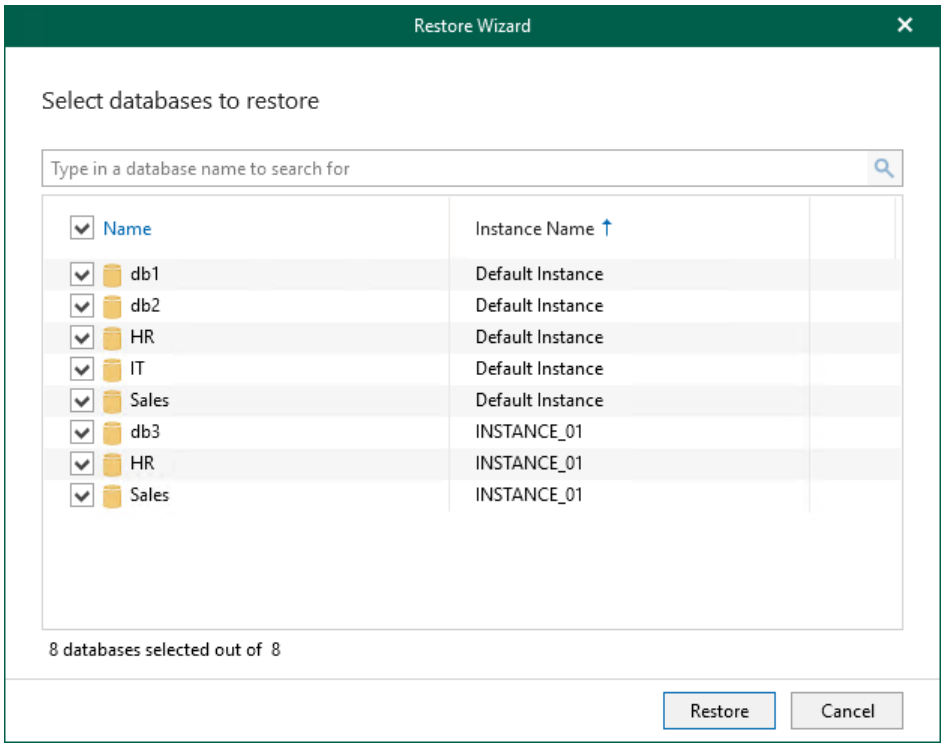
> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to recover.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



Restoring Point-in-Time State

When restoring multiple databases, consider that depending on the database recovery model the following cases are possible:

- Some databases may be restored as of the different time interval.
- Some databases cannot be restored if there are no transaction logs available for the specified period.

To restore Microsoft SQL Server databases as of the point-in-time state, use the **Restore** wizard.

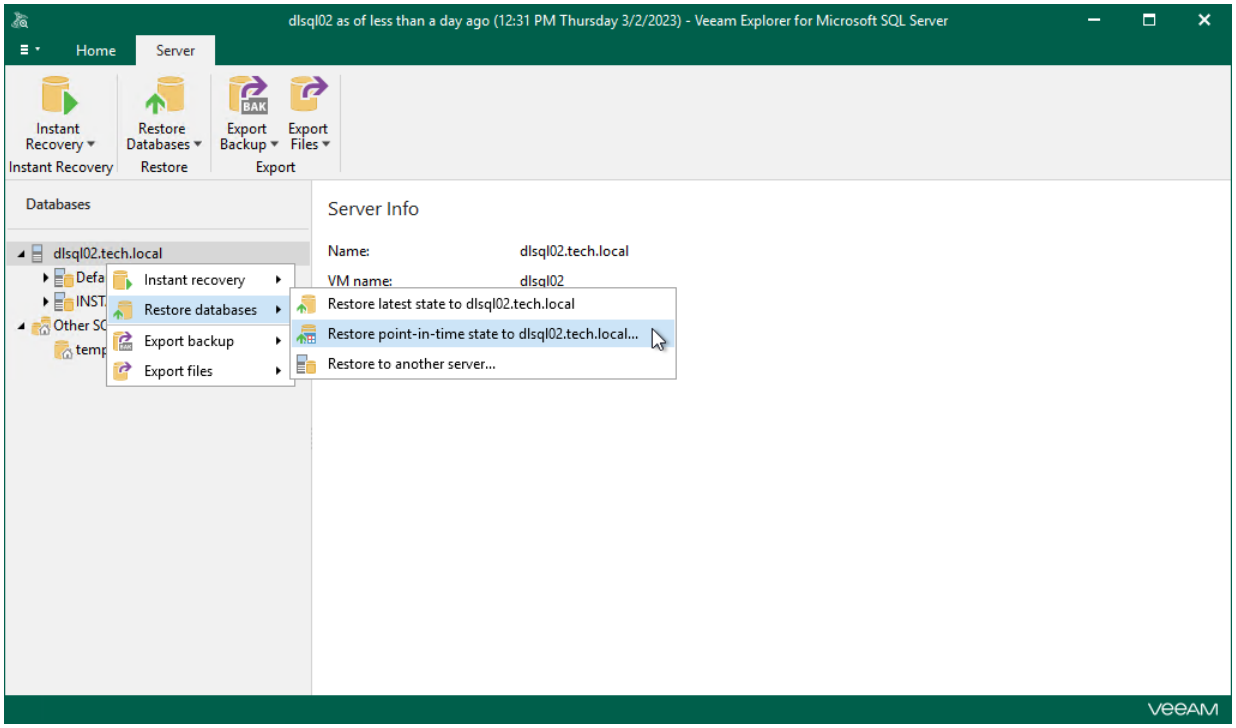
1. Launch the Restore wizard.
2. Select databases you want to restore.
3. Specify a restore point.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Restore Databases > Restore point-in-time state to <original_location>**.

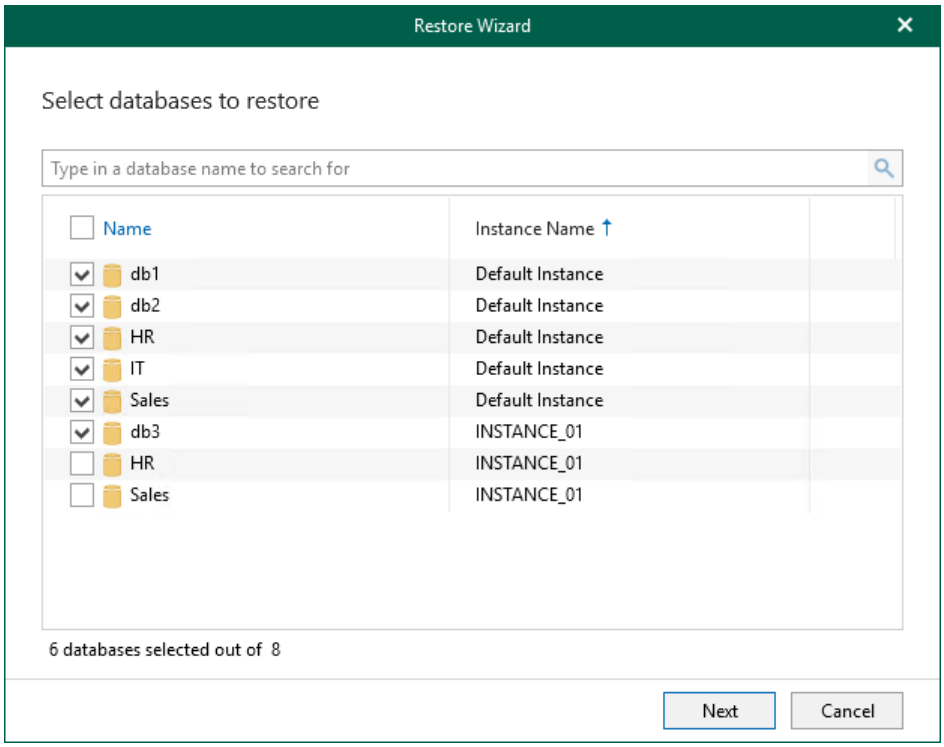
Alternatively, you can right-click an instance or the server and select **Restore databases** > **Restore point-in-time state to <original_location>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to restore.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.

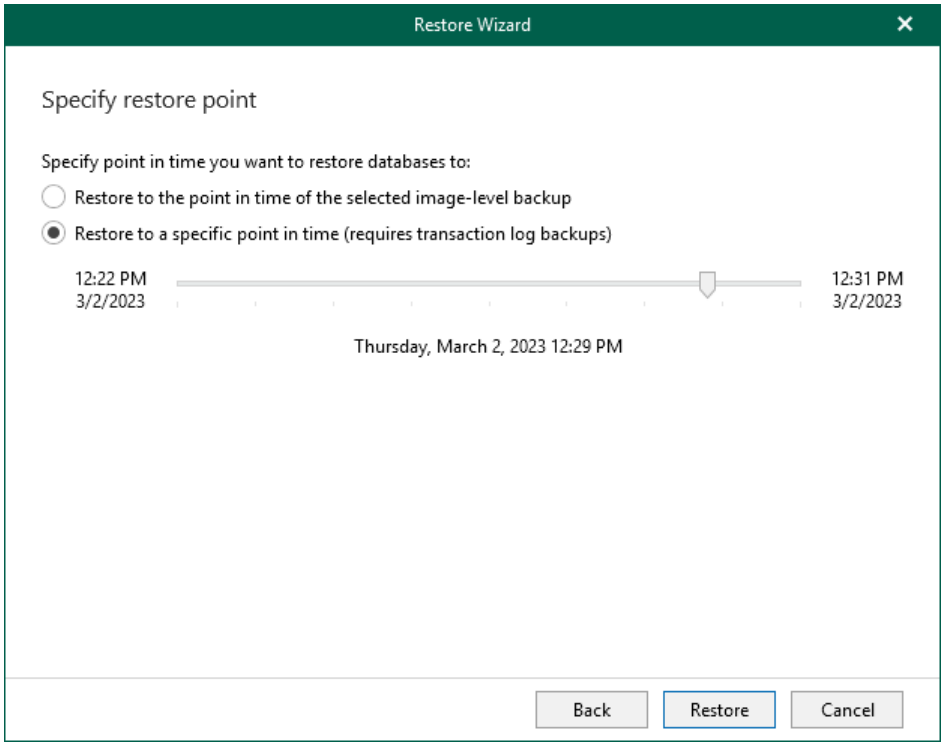


Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.



Restoring to Another Server

To restore multiple Microsoft SQL Server databases to another server, use the **Restore** wizard.

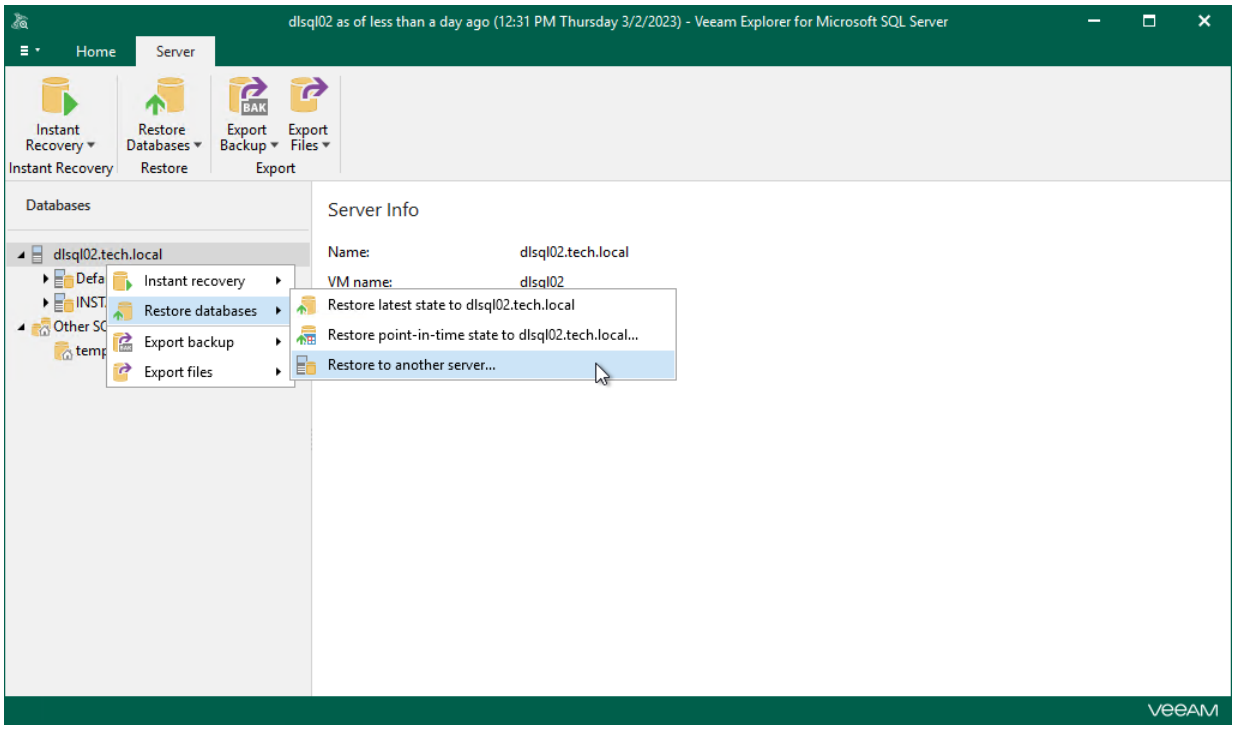
1. Launch the Restore wizard.
2. Select databases you want to restore.
3. Specify a restore point.
4. Specify the target server.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select an instance or server.
2. On the **Instance** (or **Server**) tab, select **Restore Databases** > **Restore to another server**.

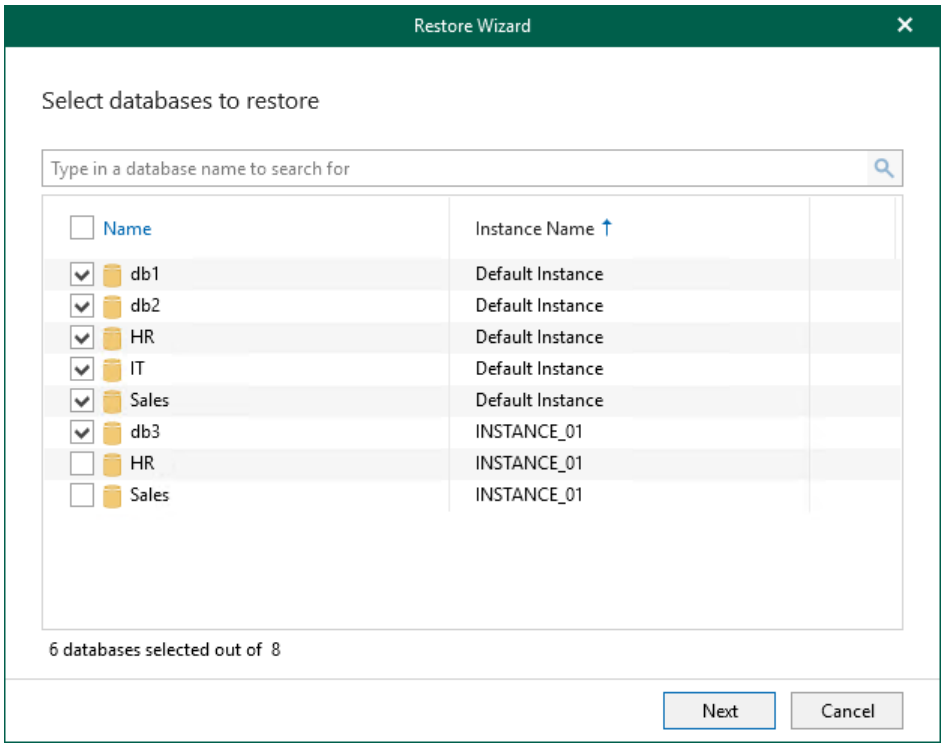
Alternatively, you can right-click an instance or the server and select **Restore databases** > **Restore to another server**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to restore.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.

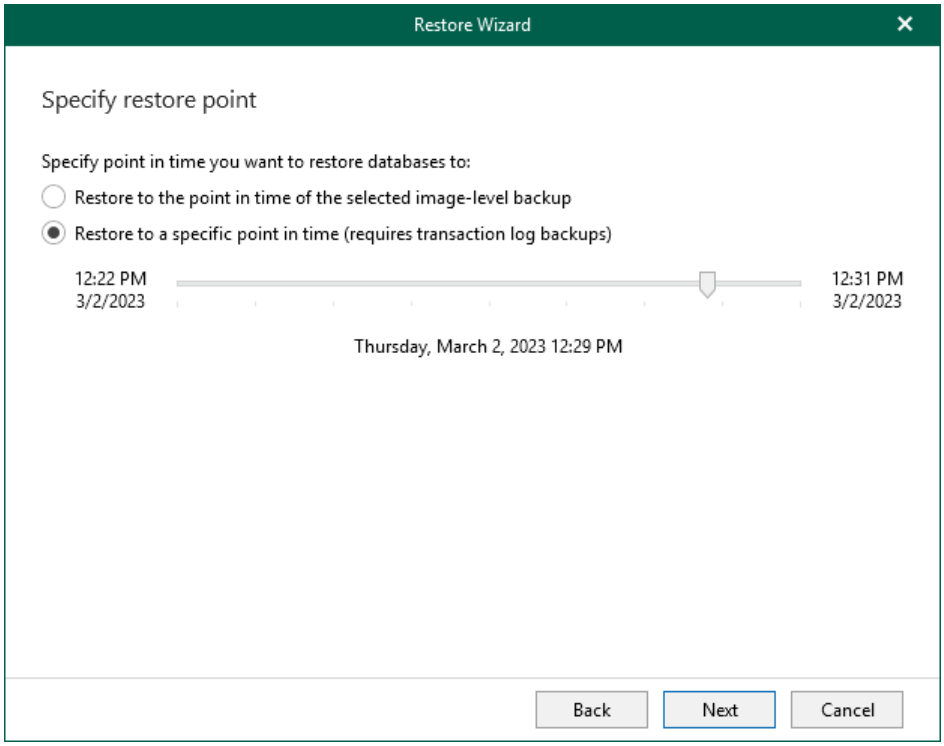


Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.



Step 4. Specify Target Server

At this step of the wizard, do the following:

1. In the **Server name** field, specify the name of the Microsoft SQL Server machine or SQL Server instance to which you want to restore your database.

   Use the *server_name|instance* format. You can select a server or instance from the drop-down list or use the **Browse** button, as described in Browsing for Servers.

   When you restore multiple databases, Veeam Explorer for Microsoft SQL Server places database files to their default location specified in the properties of the target SQL Server instance.

2. In the **Specify user account to connect** section, select either of the following options:

   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Microsoft SQL Server is running.

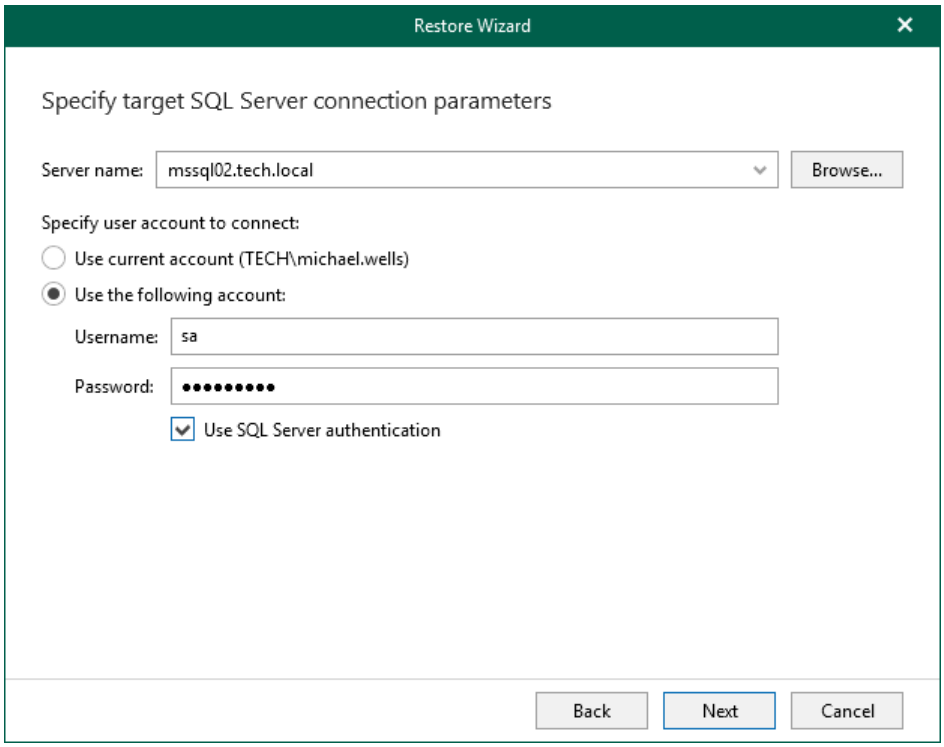
     You cannot use this option if Veeam Explorer for Microsoft SQL Server and mount server are located on separate machines.

   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

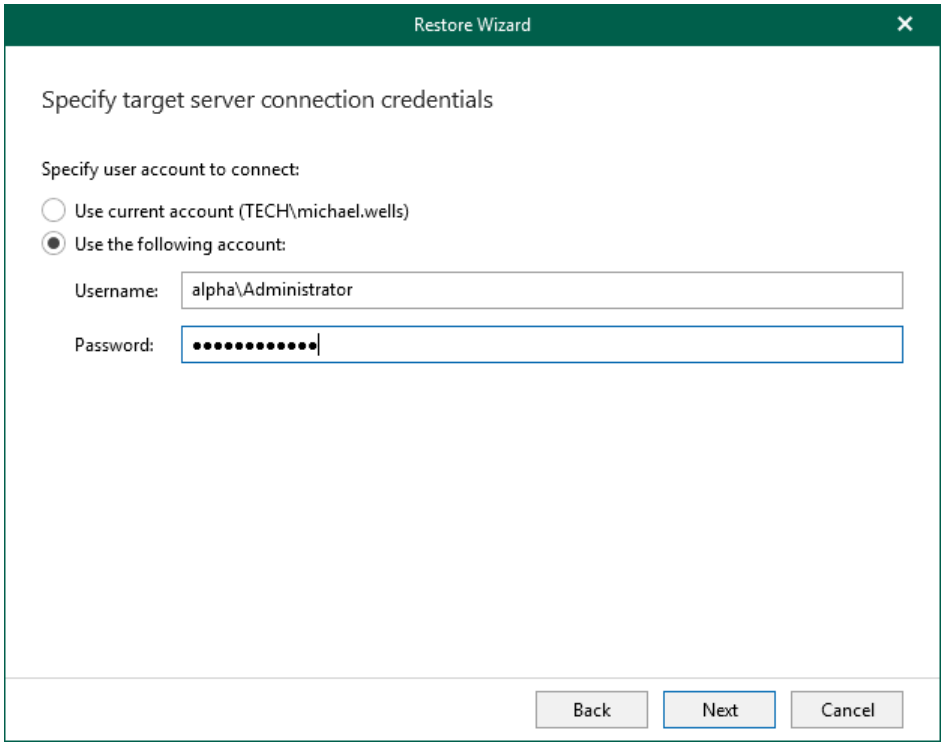
   Make sure the account you are using has been granted the **sysadmin** role on the target SQL Server machine.

3. If you selected the **Use the following account** option and want to use Microsoft SQL Server authentication, select the **Use SQL Server authentication** check box. If you do not select the check box, Veeam Explorer for Microsoft SQL Server will use Windows authentication.

> **IMPORTANT**
>
> Make sure that the administrative share (for example, `\\myserver\C$`) on the target machine is available. **Read** and **Write** are minimum required permissions, **Full Control** is recommended.



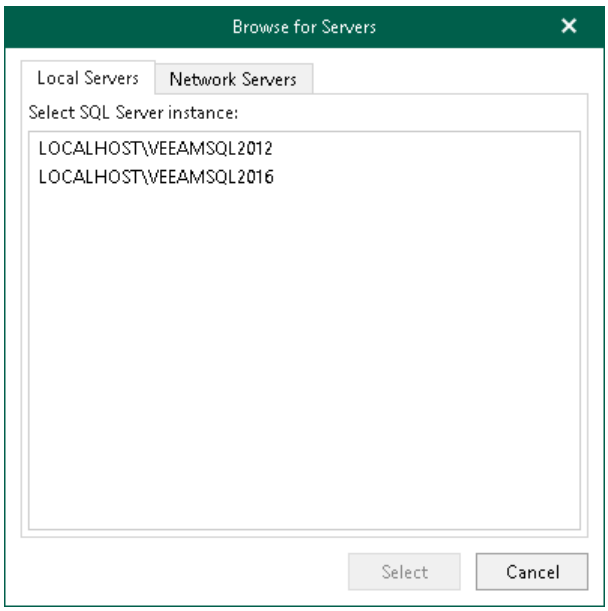
If you select the **Use SQL Server authentication** check box and provide a SQL Server account, you will be prompted to provide an account to connect to the target server at the next step of the wizard.



Browsing for Servers

To browse for a server, do either of the following:

- On the **Local Servers** tab, select a local SQL Server that is located on the machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL Server VM over the network.



Restoring Database Schema and Data

To restore database schema and data, do the following:

1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify target SQL server settings.
5. Select database objects.
6. Specify names for restored objects.
7. Specify directory names for file tables.
8. Specify additional restore options.

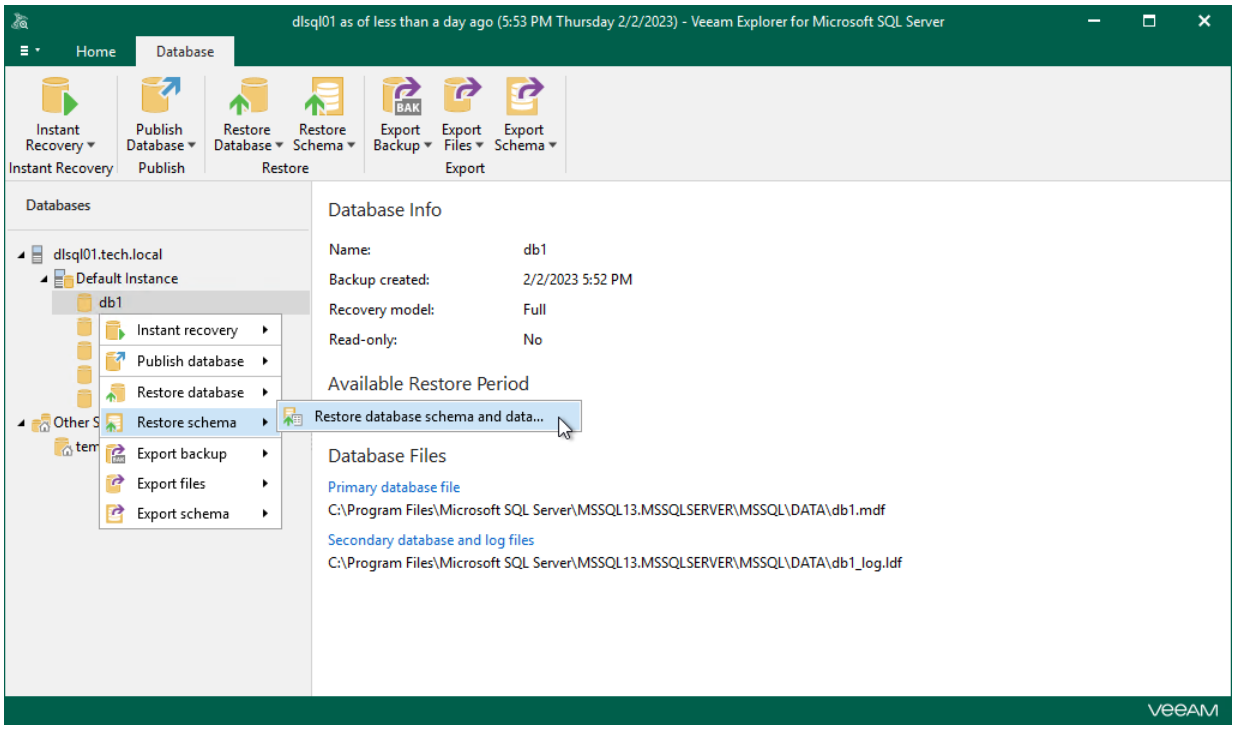
Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Restore Schema** > **Restore database schema and data**.

Alternatively, you can right-click a database in the navigation pane and select **Restore schema** > **Restore database schema and data**.

> **IMPORTANT**
>
> Consider the following:
>
> - A staging SQL Server is required to perform a restore of database schema and data. For more information, see Configuring Staging SQL Server.
> - FILESTREAM must be enabled on a staging SQL Server to restore file tables. For more information on enabling FILESTREAM, see this Microsoft article.

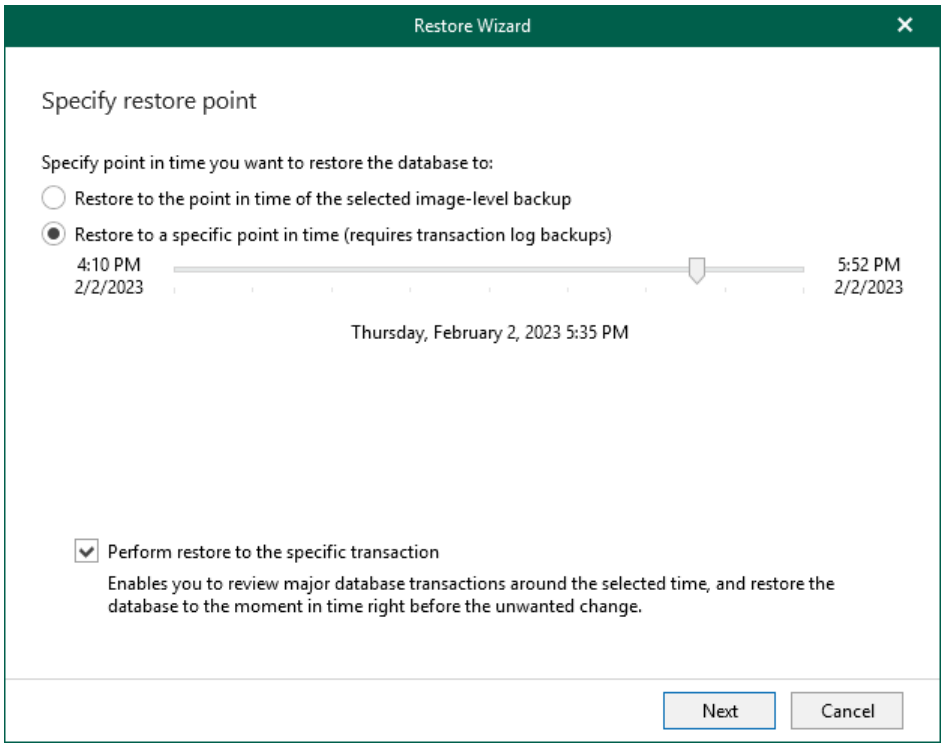


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

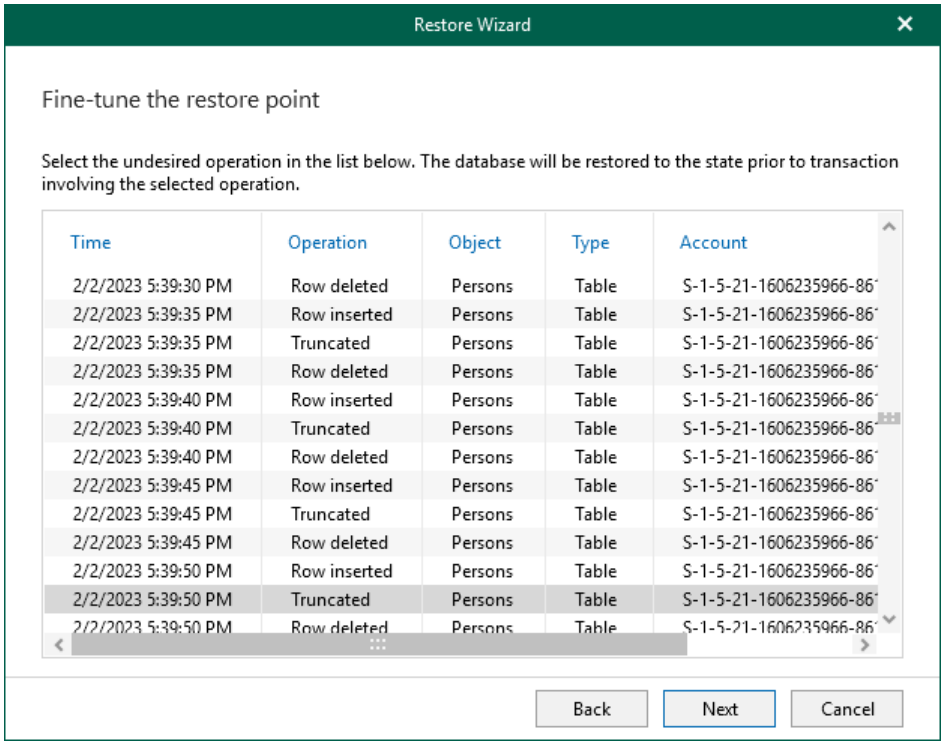


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to recover your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target SQL Server Settings

At this step of the wizard, specify the target SQL Server connection parameters:

1. In the **Server name** field, specify the target SQL Server instance to which you want to restore your database.

   You can specify the instance name in the *server_name*|*instance* format. Also, you can select an instance from the drop-down list or use the **Browse** button, as described in Browsing for Servers.

2. In the **Specify user account to connect** section, select either of the following options:

   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Microsoft SQL Server is running.

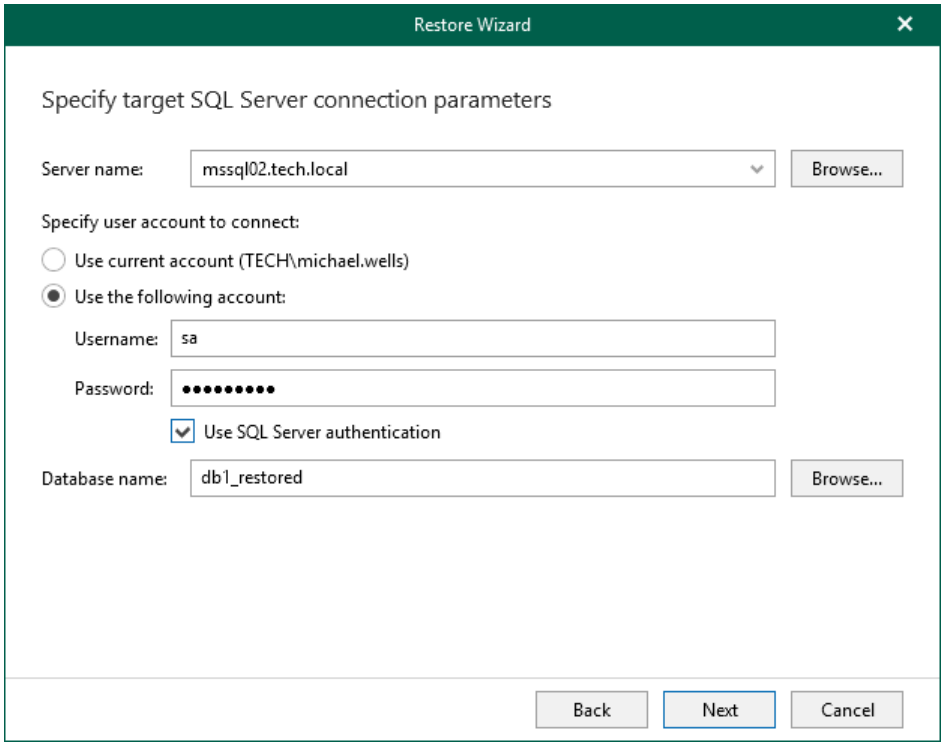
     You cannot use this option if Veeam Explorer for Microsoft SQL Server and mount server are located on separate machines.

   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

   Make sure the account you are using has been granted the **sysadmin** role on the target SQL Server machine.

3. If you selected the **Use the following account** option and want to use SQL Server authentication, select the **Use SQL Server authentication** check box. If you do not select the check box, Veeam Explorer for Microsoft SQL Server will use Windows authentication.

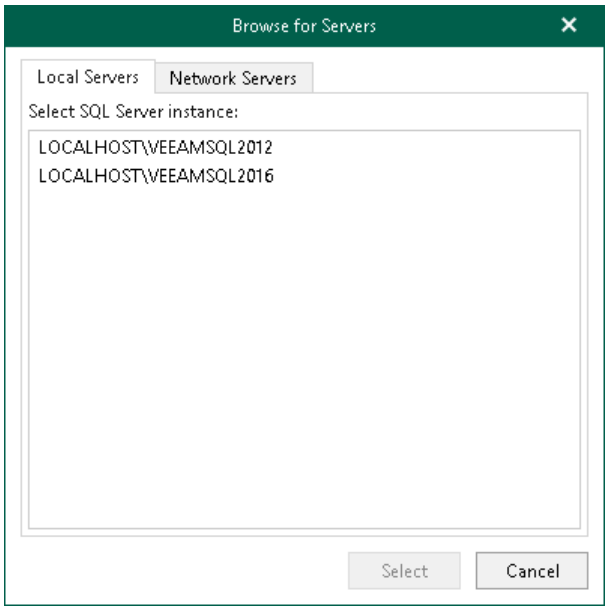
4. In the **Database name** field, specify the target database name. Click **Browse** to select a database to which you want to restore the schema.



Browsing for Servers

To browse for a server, do either of the following:

- On the **Local Servers** tab, select a local SQL Server that is located on the machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL Server instance on another server. Veeam Explorer for Microsoft SQL Server displays servers from your network where Microsoft SQL Server is installed.

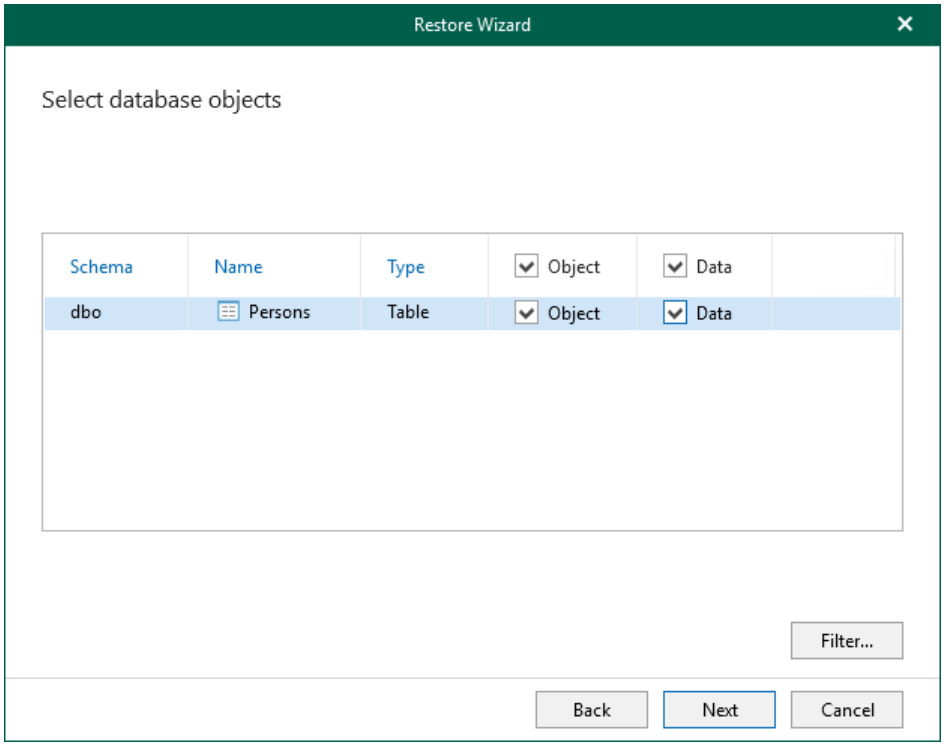


Step 5. Select Database Objects

At this step of the wizard, specify database objects you want to restore.

Use the **Object** and **Data** check boxes to specify what database objects and data should be restored.

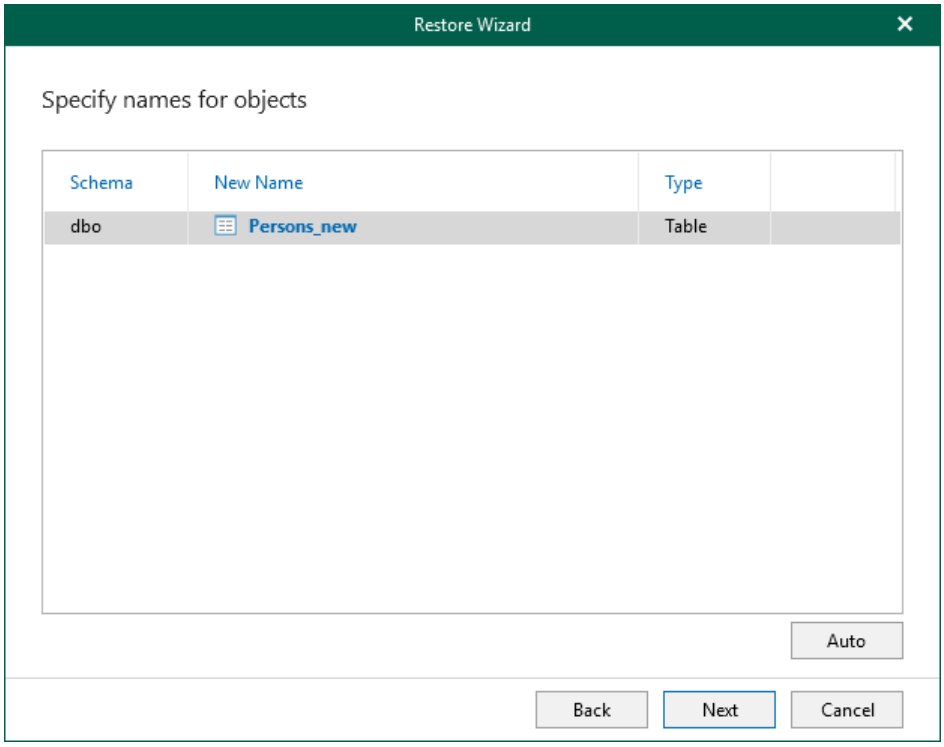
To display only specific objects, click **Filter** and select the object type.



Step 6. Specify Names for Objects

At this step of the wizard, specify a new name for the object.

- To specify a new name, select a database and provide a new name.
- To assign a default name to the object that already exists, click **Auto**. In this case, the *_new* suffix will be added.



Step 7. Specify Directory Names for File Tables

At this step of the wizard, specify directory names for file tables.

The following options are available:

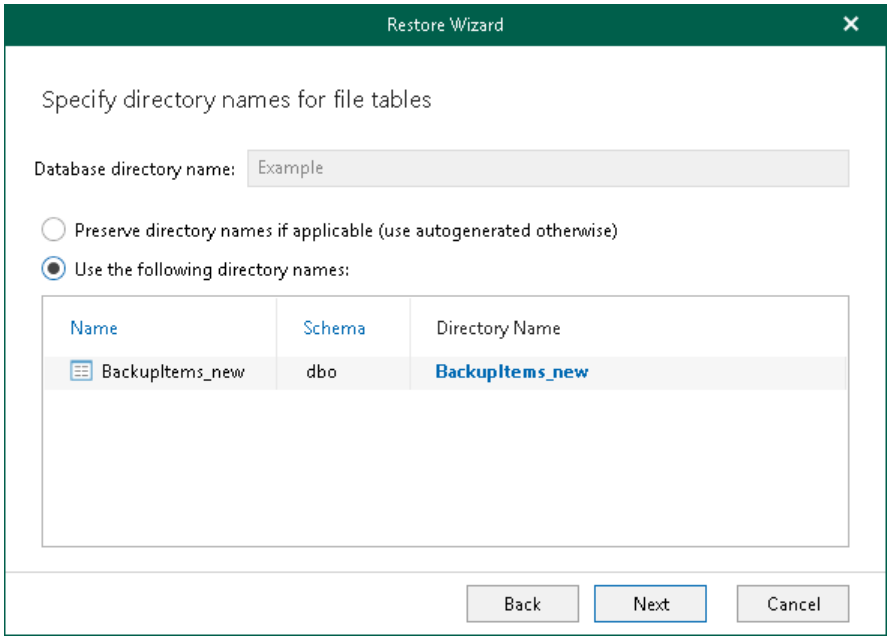
- **Preserve directory names if applicable (use autogenerated otherwise)**.

  To use the original names.

  If such names already exist on a target server, Veeam will add *_new* suffix to each name. For example, *<existing_name>_new*.

- **Use the following directory names**.

  To provide a different name under the **Directory Name** column.

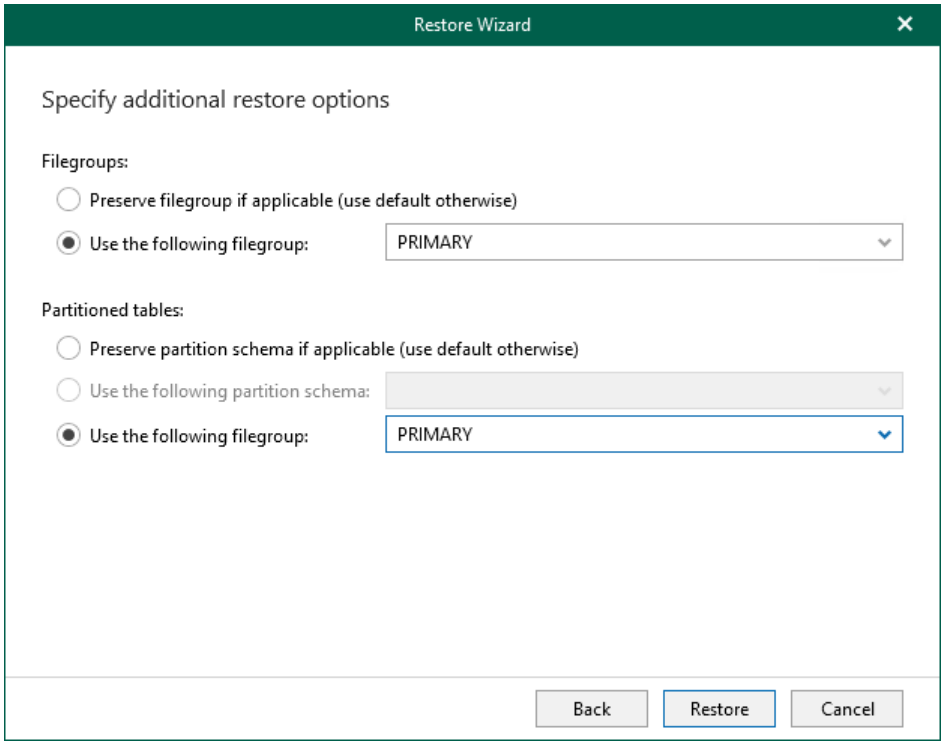


Step 8. Specify Additional Restore Options

At this step of the wizard, specify additional restore options and click **Restore**.

- In the **Filegroups** section, select how filegroups should be restored for selected schema objects:
  - **Preserve filegroup if applicable** — to preserve the file group state.
  - **Use the following filegroup** — to select a file group on a target SQL Server instance.

  For more information on filegroups, see Microsoft Docs.
- In the **Partitioned tables** section, select how partitioned tables should be restored:
  - **Preserve partition schema if applicable** — to restore tables to the original partition schema.
  - **Use the following partition schema** — to select a partition schema on a target SQL Server instance.
  - **Use the following filegroup** — to select a file group on a target SQL Server instance.



Data Publishing

Publishing a Microsoft SQL Server database allows you to temporarily attach the database to the target Microsoft SQL Server without launching restore. Publishing typically occurs faster than using standard restore features and could be convenient when, for example, your time to perform disaster-recovery operations is limited.

After you have launched a publishing operation to a Microsoft SQL Server, you can quickly republish the latest or point-in-time state of the database to the same server.

Before publishing data, read the Considerations and Limitations section.

Publishing to Specified Server

Publishing to the specified server allows you to select a target Microsoft SQL Server to which you can publish your databases.

To publish data, do the following:

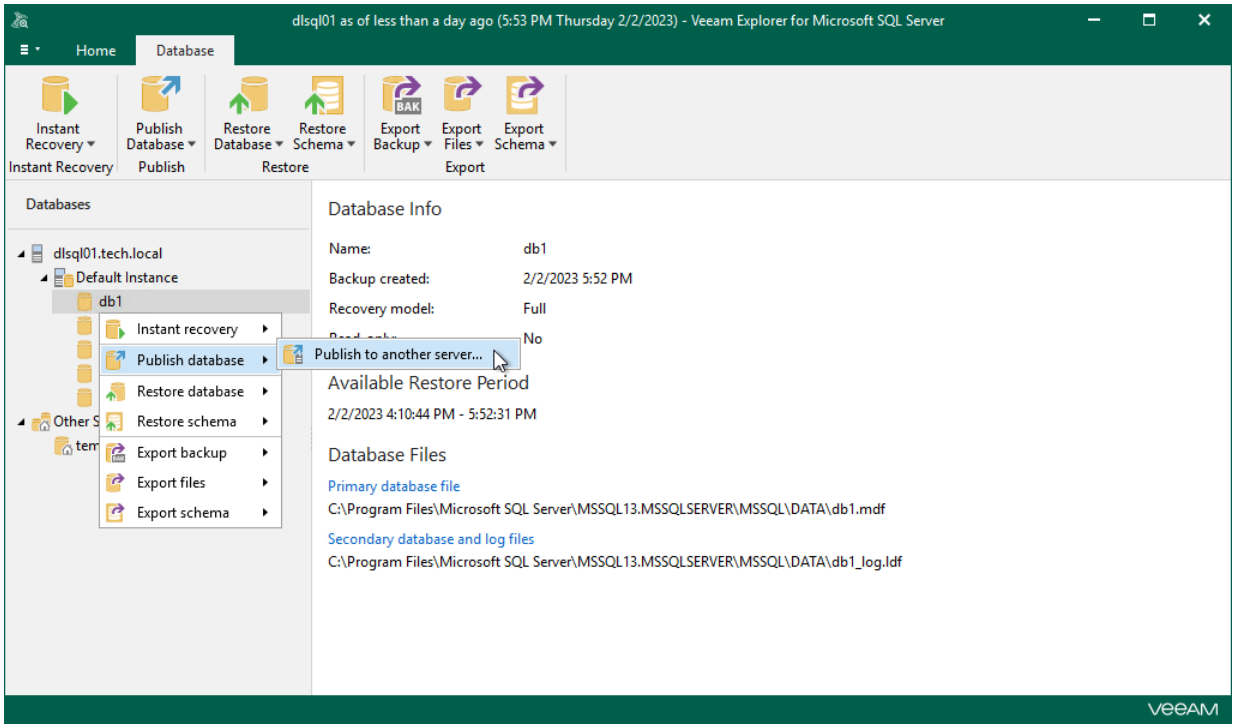
1. Launch the Publish Database wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.

Step 1. Launch Publish Database Wizard

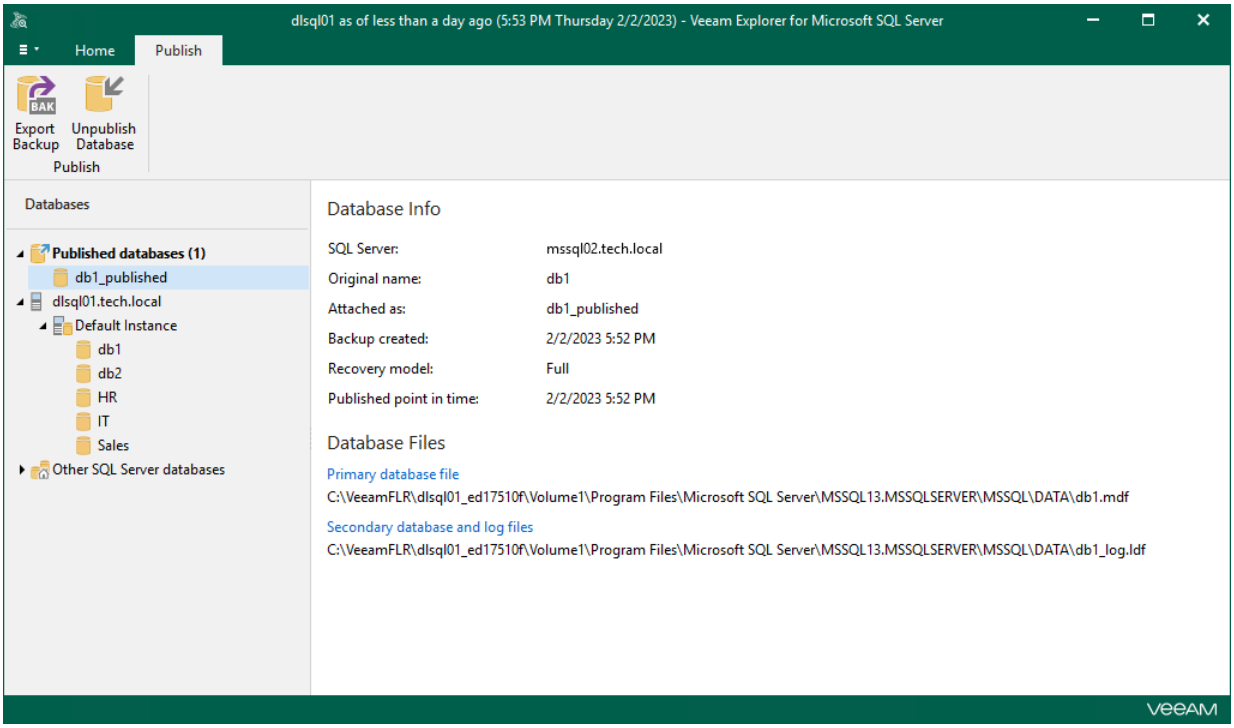
To launch the **Publish Database** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish to another server**.

Alternatively, you can right-click a database and select **Publish database** > **Publish to another server**.

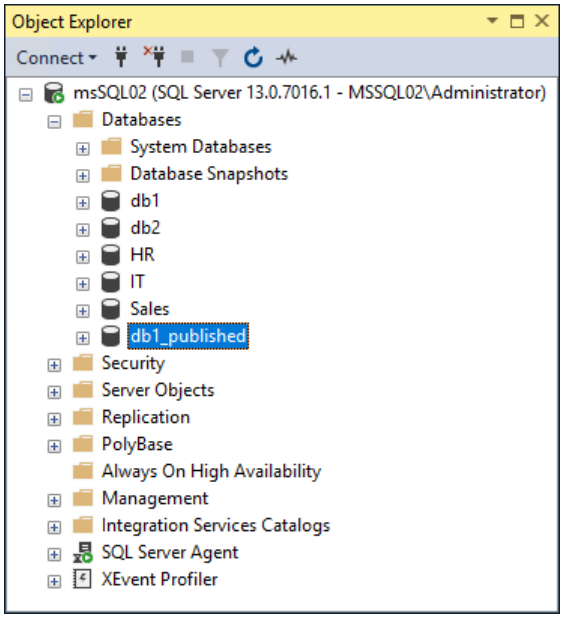


After you complete the wizard steps, a new **Published databases** node appears at the top of the navigation pane. Under this node, you can find the databases that have been published during the current session of Veeam Explorer for Microsoft SQL Server.



To work with published databases, open a SQL tool you prefer, for example, *Microsoft SQL Management Studio* and locate your published databases.

The figure below demonstrates a published database (*db1_published*) available in the **Object Explorer** window of your *Microsoft SQL Server Management Studio* console. This database is also being referenced by Veeam Explorer for Microsoft SQL Server under its **Published databases** node.



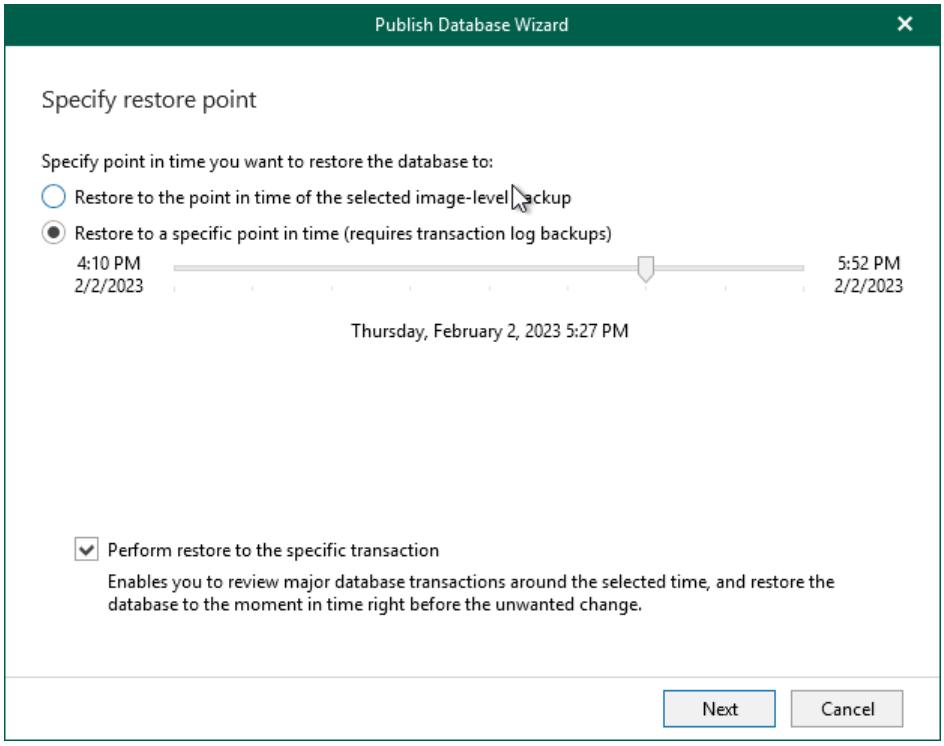
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

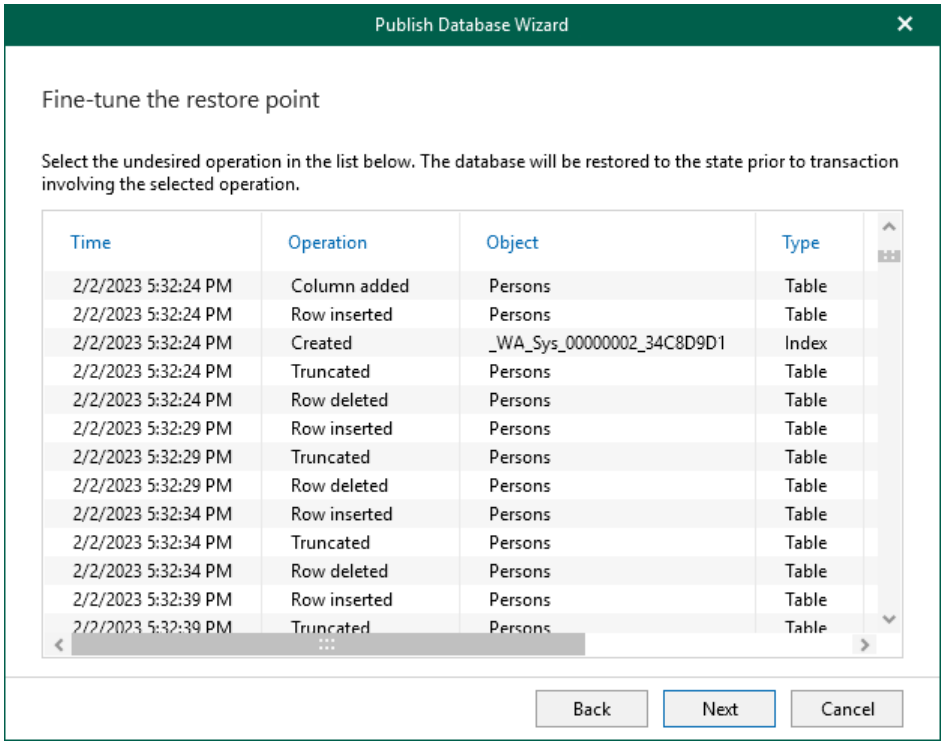


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Server

At this step of the wizard, do the following:

1. In the **Server name** field, specify a target SQL server name/SQL server instance/SQL cluster to which you want to publish the database.

   Use the *server_name*|*instance* format. You can select a server/instance/cluster from the drop-down list or use the **Browse** button on the left, as described in Browsing for Servers.

2. In the **Database name** filed, specify a new name under which you want to publish your database.

   Consider that if you leave the original database name, Veeam Explorer for Microsoft SQL Server will overwrite the associated database on the target server.

3. In the **Specify user account to connect** section, select either of the following options:

   - **User current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Microsoft SQL Server is running.

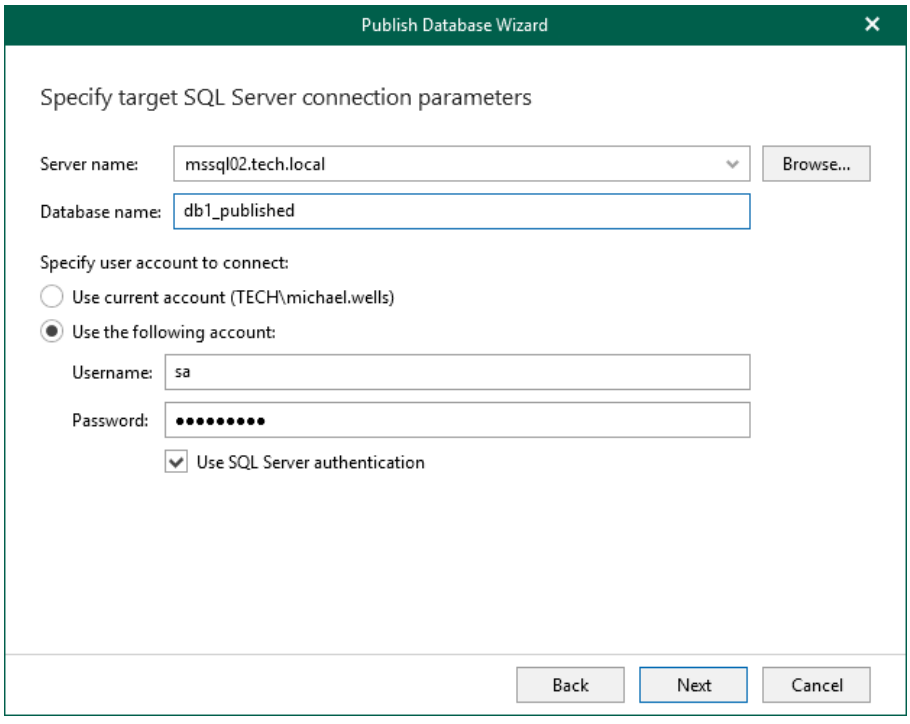
     You cannot use this option if Veeam Explorer for Microsoft SQL Server and mount server are located on separate machines.

   - **User the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

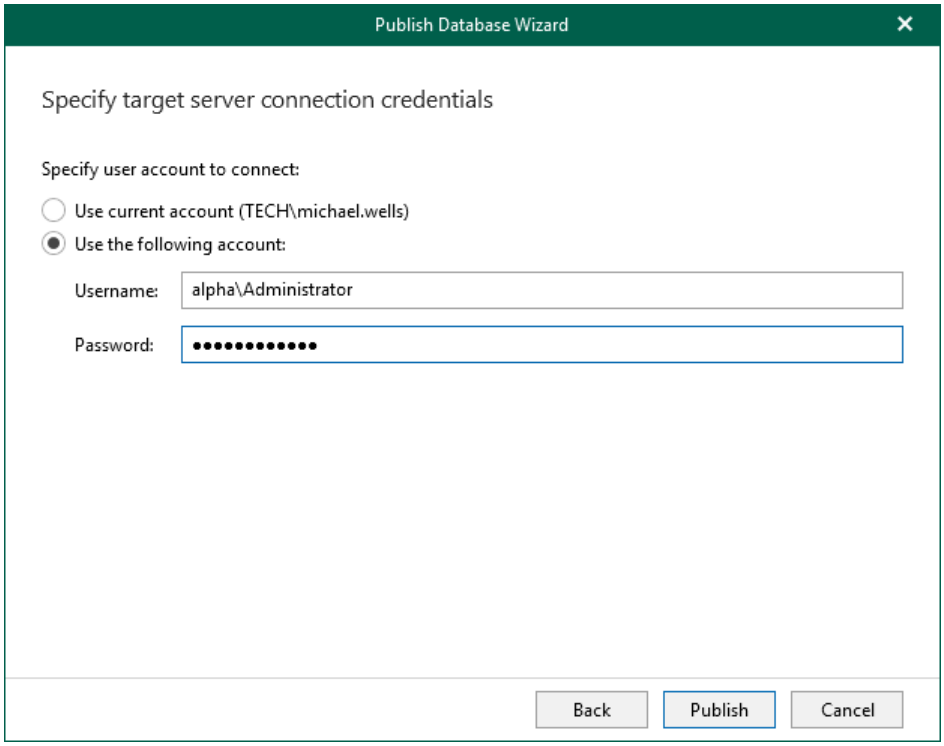
   Make sure the account you are using has been granted the **sysadmin** role on the target SQL Server machine.

4. If you selected the **Use the following account** option and want to use SQL Server authentication, select the **Use SQL Server authentication** check box. If you do not select the check box, Veeam Explorer for Microsoft SQL Server will use Windows authentication.

> **NOTE**
>
> Make sure that the administrative share for example, `\\myserver\ADMIN$`) on the target machine is available; **Read** and **Write** are minimum required, **Full Control** is recommended.



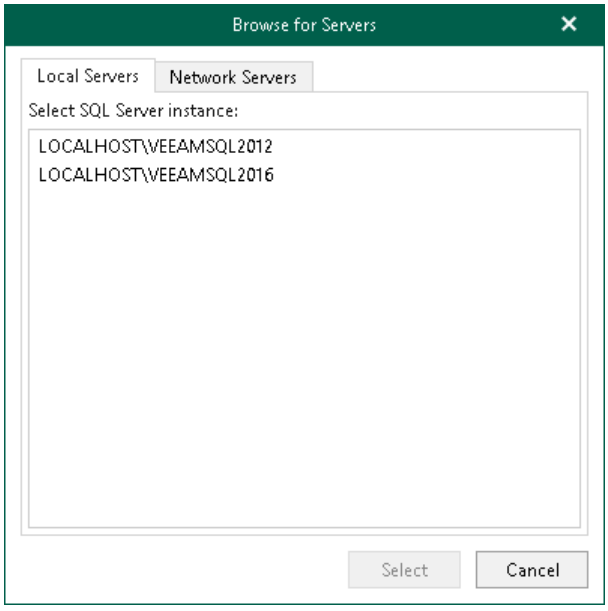
If you select the **Use SQL Server authentication** check box and provide a SQL Server account, you will be prompted to provide an account to connect to the target server at the next step of the wizard.



Browsing for Servers

To browse for a server to which you want to restore your databases, do either of the following:

- On the **Local Servers** tab, select a local SQL server/instance/cluster that is located on a machine with Veeam Explorer for Microsoft SQL Server.
- On the **Network Servers** tab, select a SQL server/instance/cluster over the network.



Publishing Latest or Point-in-Time State

After you have launched a publishing operation to a Microsoft SQL Server (as described in Publishing to Specified Server), you can quickly republish a state of the database to the same server.

You can republish either of the following states:

- The latest available state — to publish data as of the latest state in the backup file.
- A point-in-time state — to publish data as of the selected point-in-time state. This option is available only if backups of Microsoft SQL Server transaction logs exist. For more information, see Required Backup Job Settings.

When you unpublish a database, both options continue to remain until you close the application so that you can quickly republish a database if required.

Publishing Latest State

Veeam Explorer for Microsoft SQL Server allows you to republish an unpublished database. When republishing a database, it will be attached to the target SQL server as of the latest state.

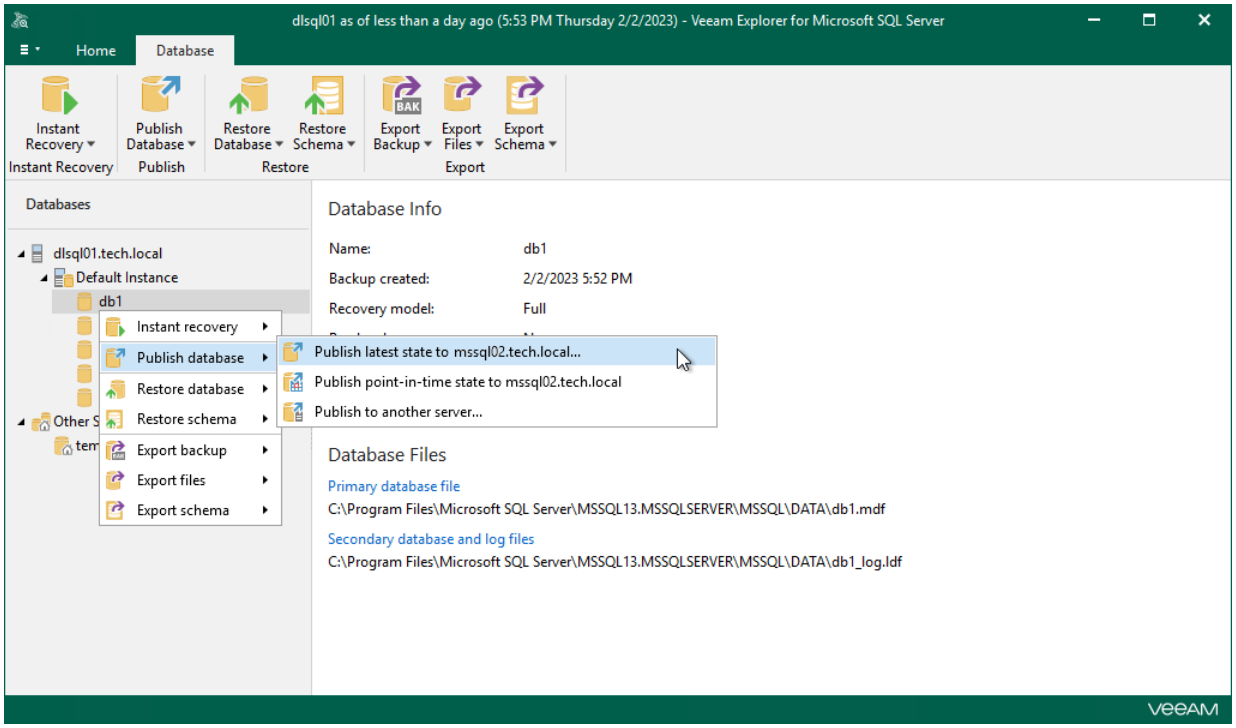
To republish a database as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish latest state to <target_server>**.

Alternatively, you can right-click a database and select **Publish database > Publish latest state to <target_server>**.

> **NOTE**
>
> The name of the publish option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Publish latest state to <target_server>**.
> - If you select any other restore point, the option name is displayed as **Publish state of <point_in_time> to <target_server>**.

Once this process is completed, the database will be published with the same name as it was during the initial publishing session.



Publishing Point-in-Time State

Publishing a point-in-time state allows you to obtain a required database state and unroll specified transactions if needed.

To publish databases as of the point-in-time state, do the following:

1. Launch the Publish Database wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

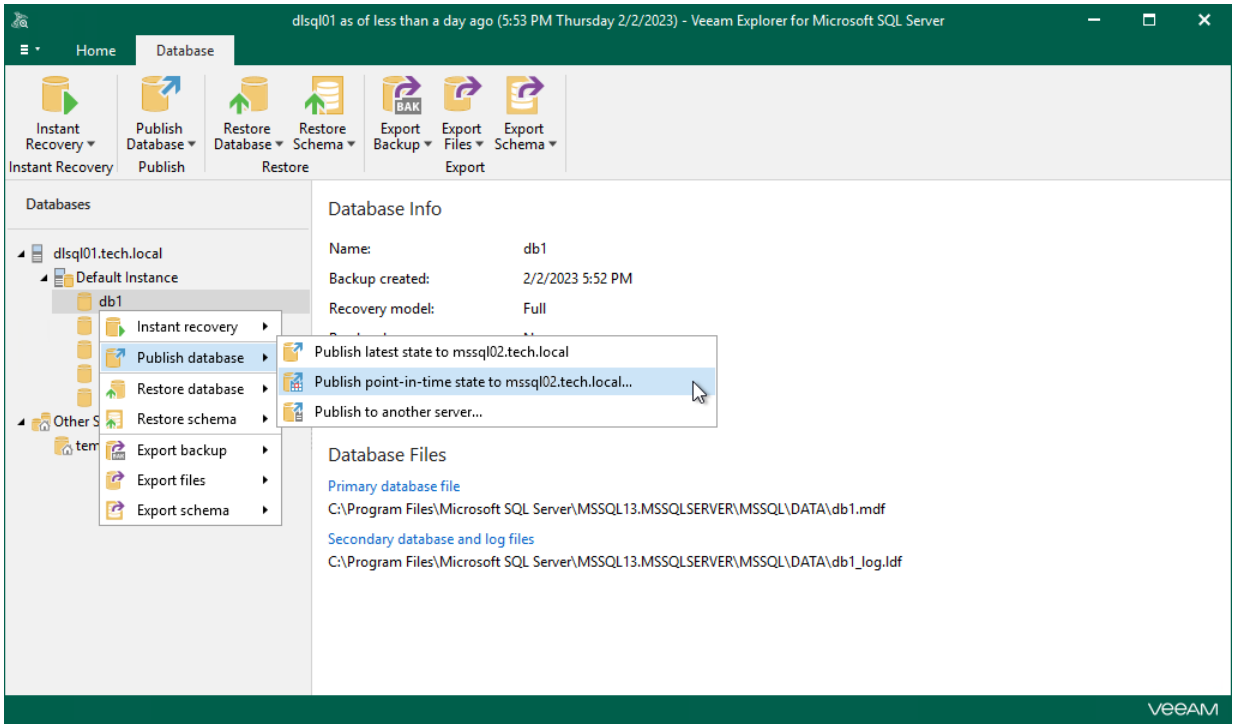
Step 1. Launch Publish Database Wizard

To launch the **Publish Database** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish point-in-time state to <server_name>\<instance_name>**.

Alternatively, you can right-click a database and select **Publish database** > **Publish point-in-time state to <server_name>\<instance_name>**.

Once the publishing process is completed, the database will be published with the same name as it was during the initial publishing session.



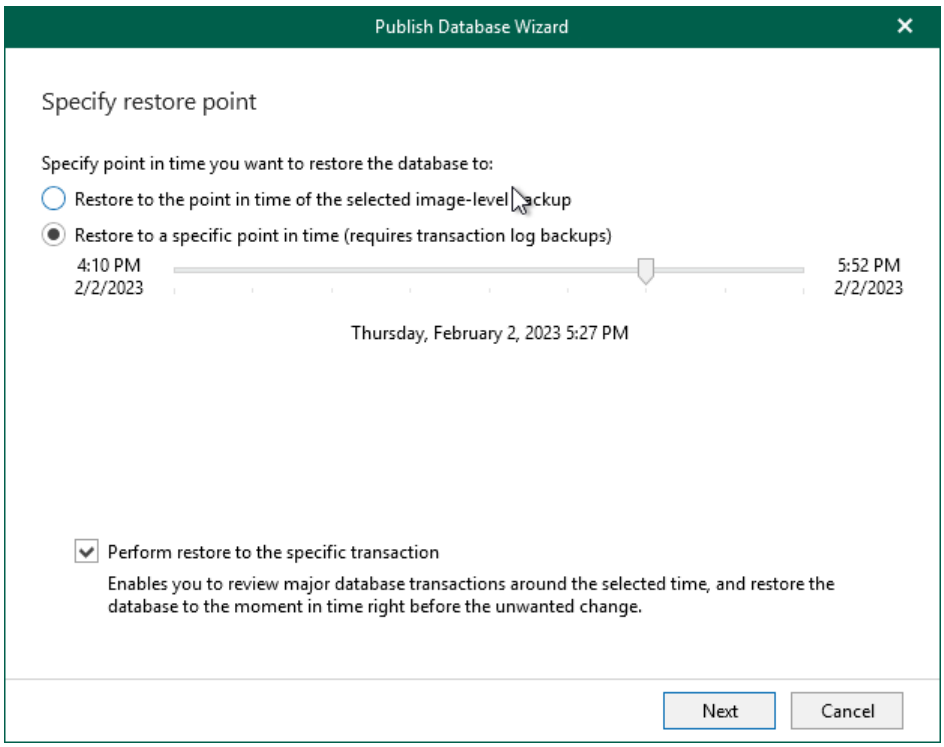
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL Server. For more information, see Configuring Staging SQL Server.

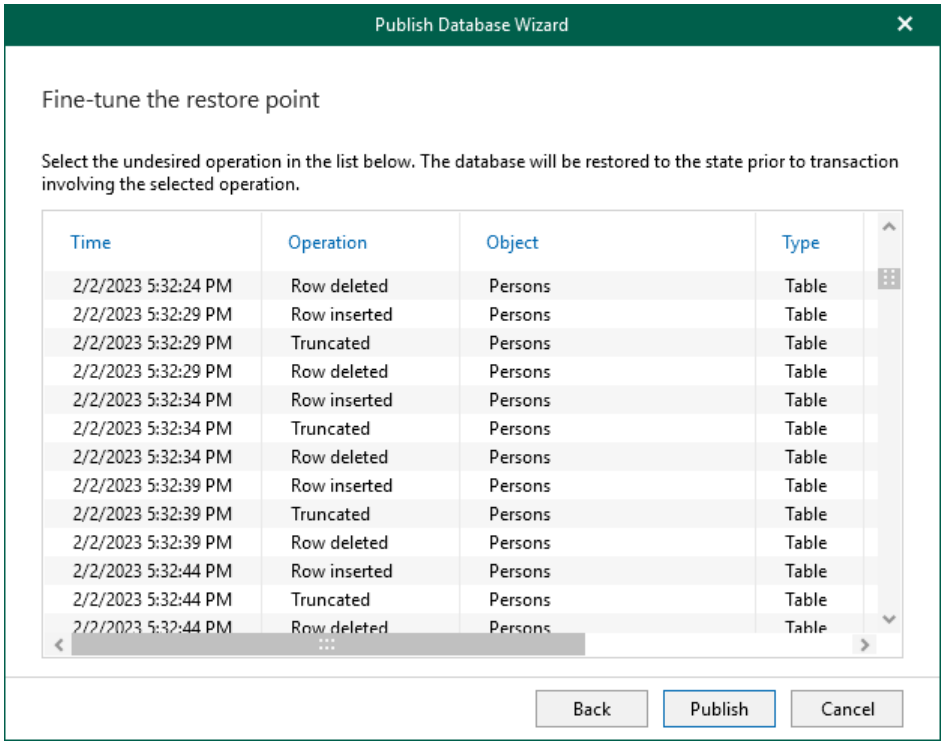


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database and click **Publish**.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Unpublishing Databases

Once you have finished working with published SQL databases, you may want to unpublish (detach) these databases from the target SQL server.

Detachment occurs in the following manner:

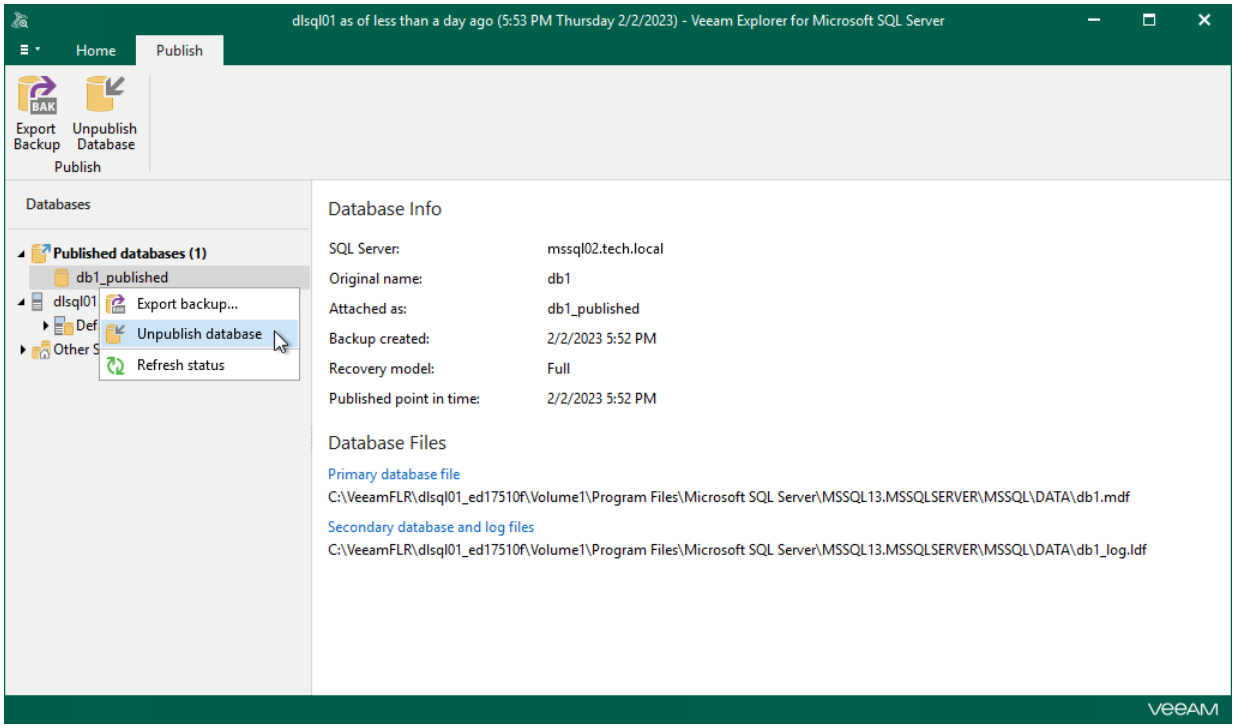
- Upon closing the Veeam Explorer for Microsoft SQL Server console, all published databases will be detached from the target SQL server automatically. Mount points will be also dismounted from under the `C:\VeeamFLR` directory.
- On manual unpublishing, databases will be detached at once but the restore point will remain mounted on the target machine for the next 15 minutes.

To unpublish a database manually, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Unpublish Database**.

Alternatively, in the navigation pane, right-click a published database and select **Unpublish database**.

To detach more than one published database simultaneously, right-click the root **Published databases** node and select **Unpublish databases** or select the root **Published databases** node and click **Unpublish Databases** on the **Publish** tab.

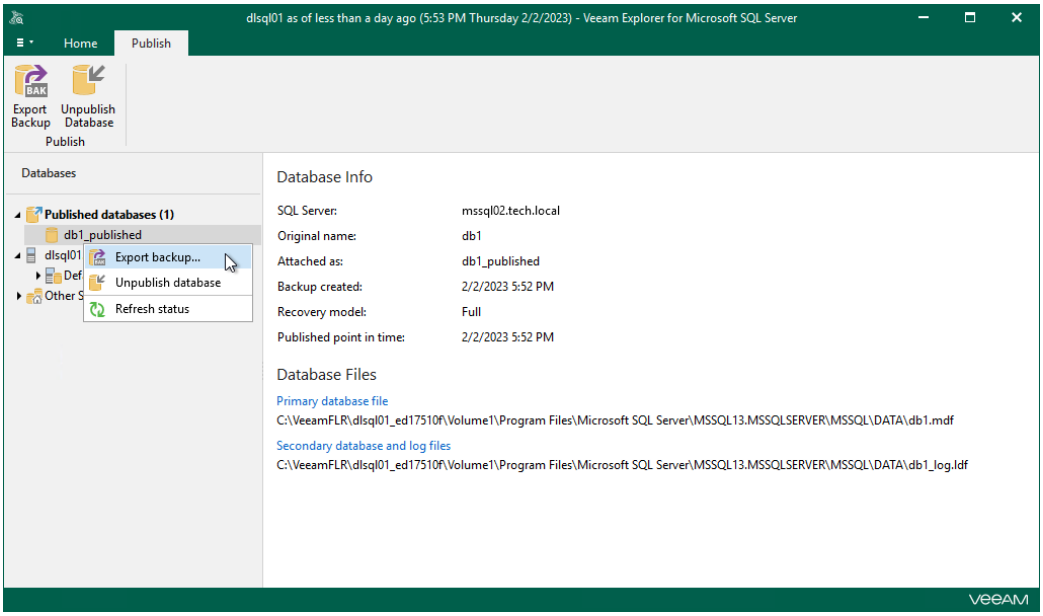


Exporting as BAK

To save changes that have been made while working with your published database to a local computer, you can use the export feature. This feature will export modified databases as BAK, preserving all the changes that have been done during the publishing session.

To export a published database, do the following:

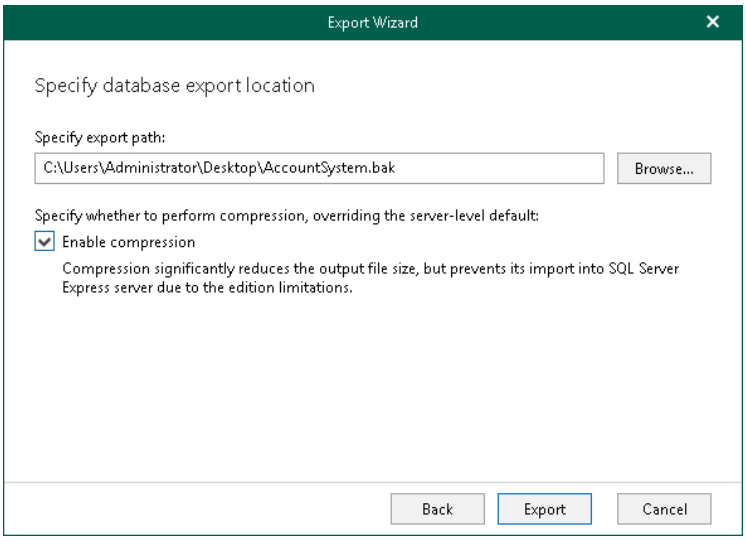
1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Export backup** or you can right-click a database and select **Export backup**.



3. In the **Export** wizard, click **Browse** next to the **Specify export path** field to specify the location where to export your data.

   To compress data, select the **Enable compression** check box. Compression will be applied according to configuration of the SQL server to which the database is published.

> **NOTE**
>
> Compression is unavailable if the server to which the database is published runs Microsoft SQL Server 2005 or any Express Edition of Microsoft SQL Server.

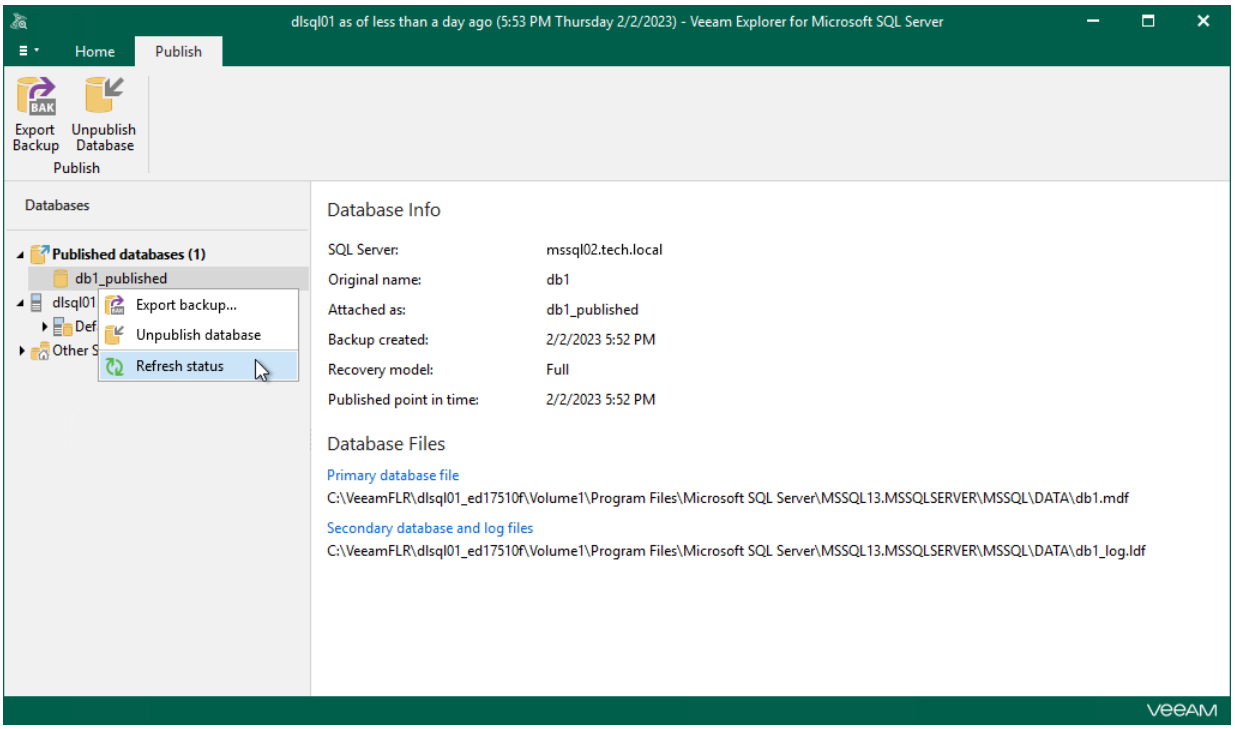


Refreshing Database Status

While the databases are attached to the target SQL server, Veeam Explorer for Microsoft SQL Server synchronizes each published database state to verify its availability. By default, synchronization occurs every five seconds.

If something went wrong with any of the published databases, the question mark appears next to each of such databases indicating the database unavailability. In the **Database Info** section, you will also see the notification message describing the problem.

To refresh a published database state manually, in the navigation pane, under the **Published databases** node, right-click a published database and select **Refresh status**.



Instant Recovery

Instant recovery combines capabilities of the data restore and data publishing features. If you want databases to be online as quickly as possible, you can use the **Instant Recovery** option and restore databases in the background.

Before performing instant recovery, read the Considerations and Limitations section.

How It Works

To perform instant recovery, Veeam Explorer for Microsoft SQL Server uses the *Veeam Explorers Recovery Service*. The service is installed on the backup server and every mount server deployed in the backup infrastructure, and runs in the background. During instant recovery, Veeam Explorer for Microsoft SQL Server uses the service running on the mount server associated with the backup repository. This removes the necessity to keep Veeam Explorer for Microsoft SQL Server running during an entire instant recovery session. Once you have started an instant recovery session, you can close Veeam Explorer for Microsoft SQL Server and then launch it later when necessary.

When you start an instant recovery session in Veeam Explorer for Microsoft SQL Server, the following happens:

1. Veeam Explorer for Microsoft SQL Server uses backup files to start two iSCSI mount sessions in parallel:
   - The first mount is used to publish the database on the target production server and attach it to the target SQL Server instance.
   - The second mount is used to copy database files to the target server in the background.
2. While the published database is online, all changes in database files that occur after publishing are saved in cache on the mount server.

   You can view and change the write cache location in the mount server settings. For more information, see the Specify Mount Server Settings section of the Veeam Backup & Replication User Guide.
3. After all database files are copied to the target server, Veeam Explorer for Microsoft SQL Server uses the cache to synchronize changes in database files.
4. After synchronization, you can switch over to the up-to-date copy of the database on the production server. Depending on the option you choose, switchover starts in one of the following ways:
   - Automatically, immediately after synchronization
   - Automatically, according to a specified schedule
   - Manually

   During switchover, Veeam Explorer for Microsoft SQL Server does the following:
   a. Stops the published database.
   b. Uses the cache to synchronize differences between the published database and the copied database files.
   c. Drops the published database.
   d. Starts the recovered database.

Instant recovery session is resilient to network disruption, backup server or mount server crash. If anything disrupts the restore process, the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch retry after the server or network is up.

Instant Recovery of Single Database

You can perform instant recovery of a Microsoft SQL Server database by following one of these scenarios:

- Instant Recovery of Latest State
- Instant Recovery of Point-in-Time State
- Instant Recovery to Another Server

Instant Recovery of Latest State

To perform instant recovery of a single database to the latest state, use the **Instant Recovery** wizard.

1. Launch the Instant Recovery wizard.
2. Specify switchover settings.
3. Finalize the Instant Recovery session.

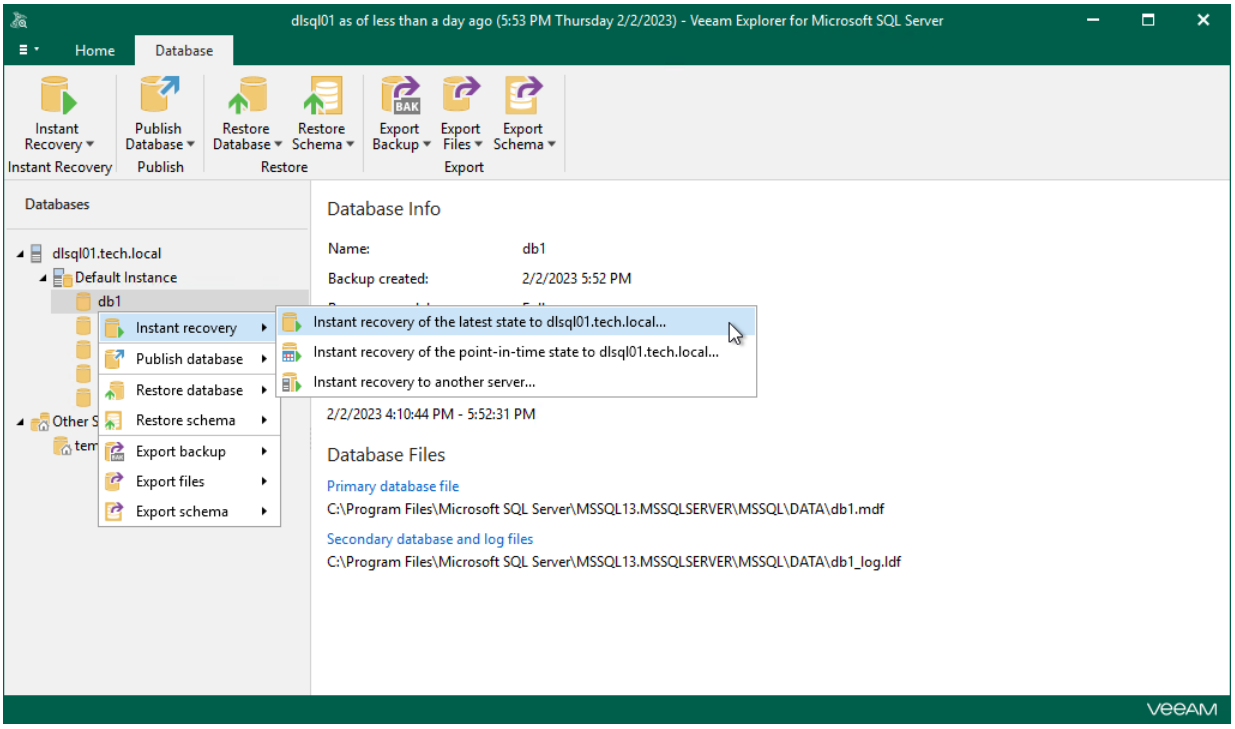
Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of the latest state to <original_location>**.

Alternatively, you can right-click a database and select **Instant recovery** > **Instant recovery of the latest state to <original_location>**.

> **NOTE**
>
> The name of the instant recovery option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Instant recovery of the latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Instant recovery of the state of <point_in_time> to <original_location>**.



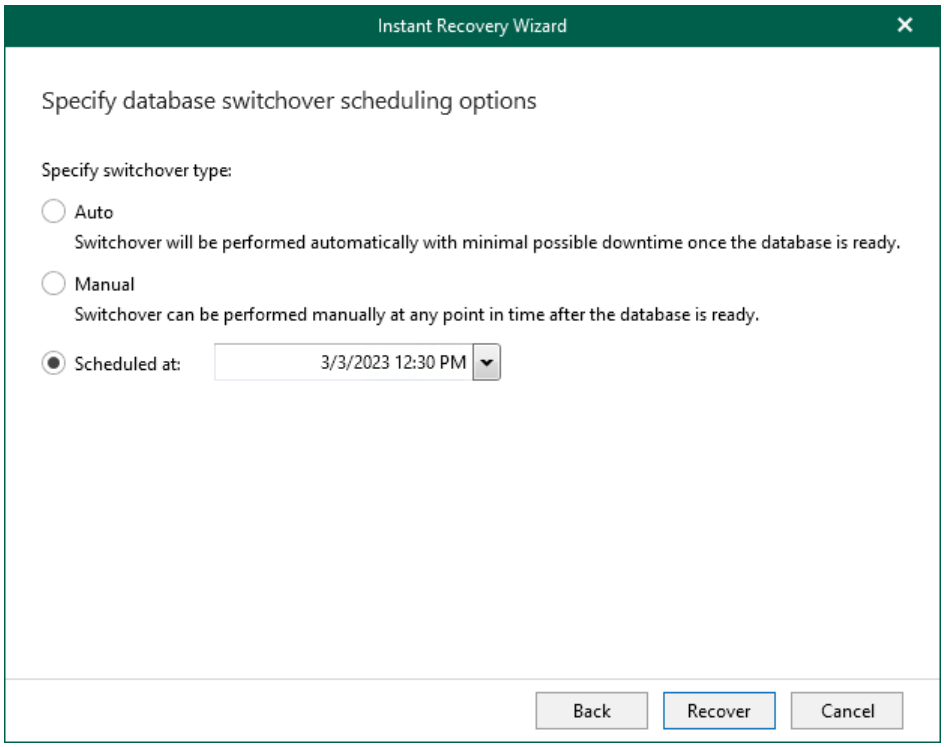
Step 2. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 3. Finalize Instant Recovery Session

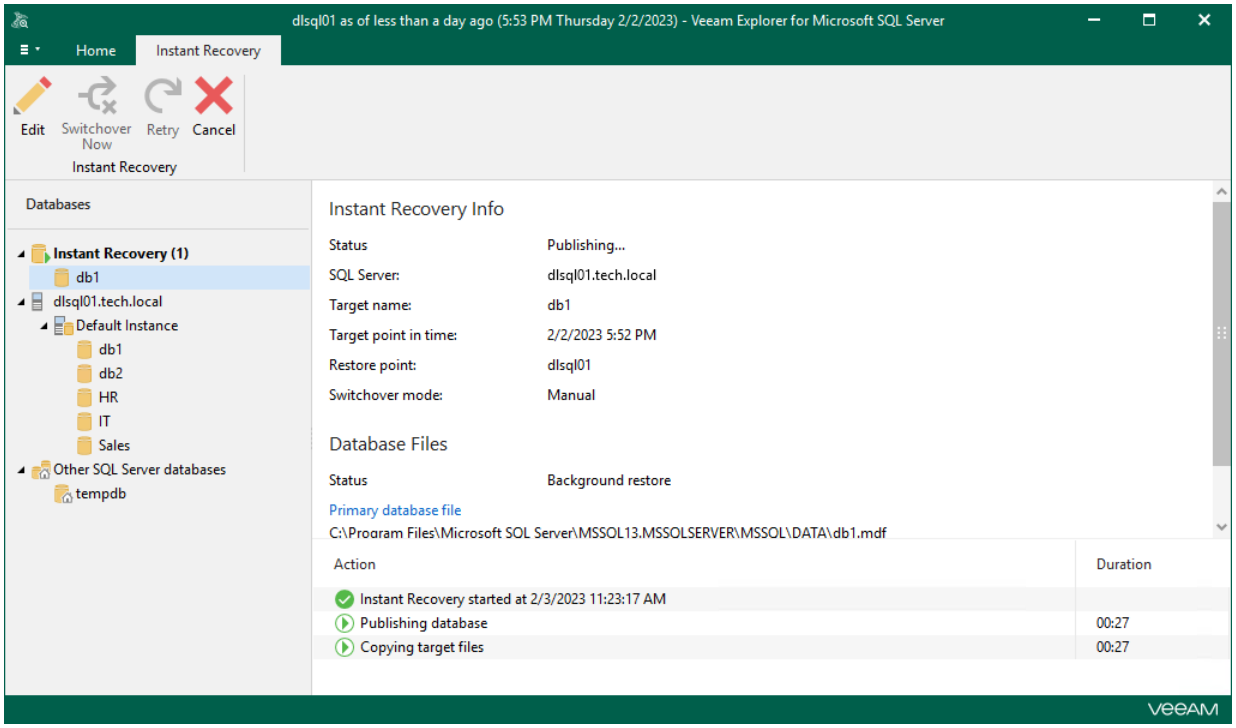
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery of Point-in-Time State

To perform instant recovery of a database to a selected point-in-time state, use the **Instant Recovery** wizard.

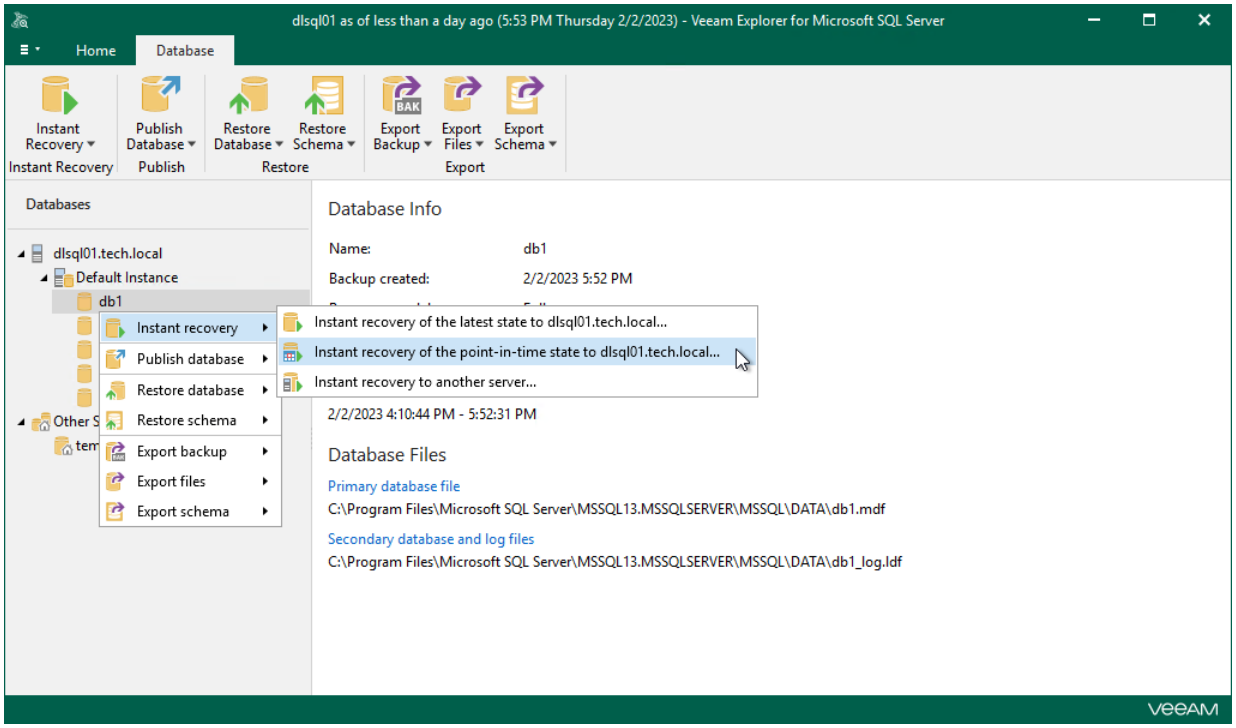
1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify switchover settings.
5. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of the point-in-time state to <original_location>**.

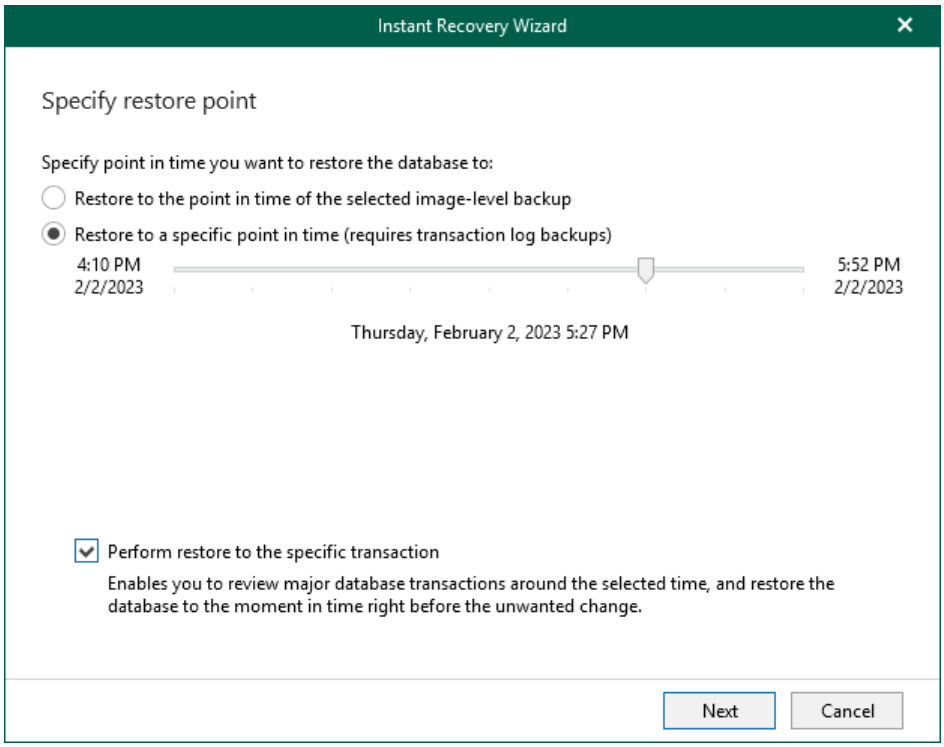
Alternatively, you can right-click a database and select **Instant recovery** > **Instant recovery of the point-in-time state to <original_location>**.



Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging server where Microsoft SQL Server is deployed. For more information, see Configuring Staging SQL Server.

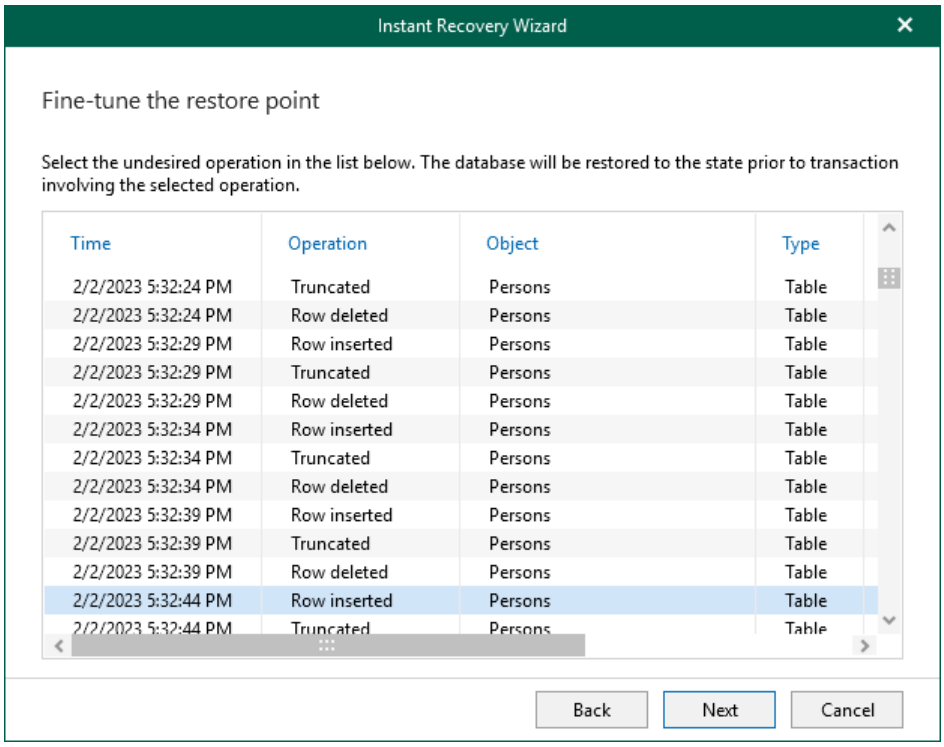


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



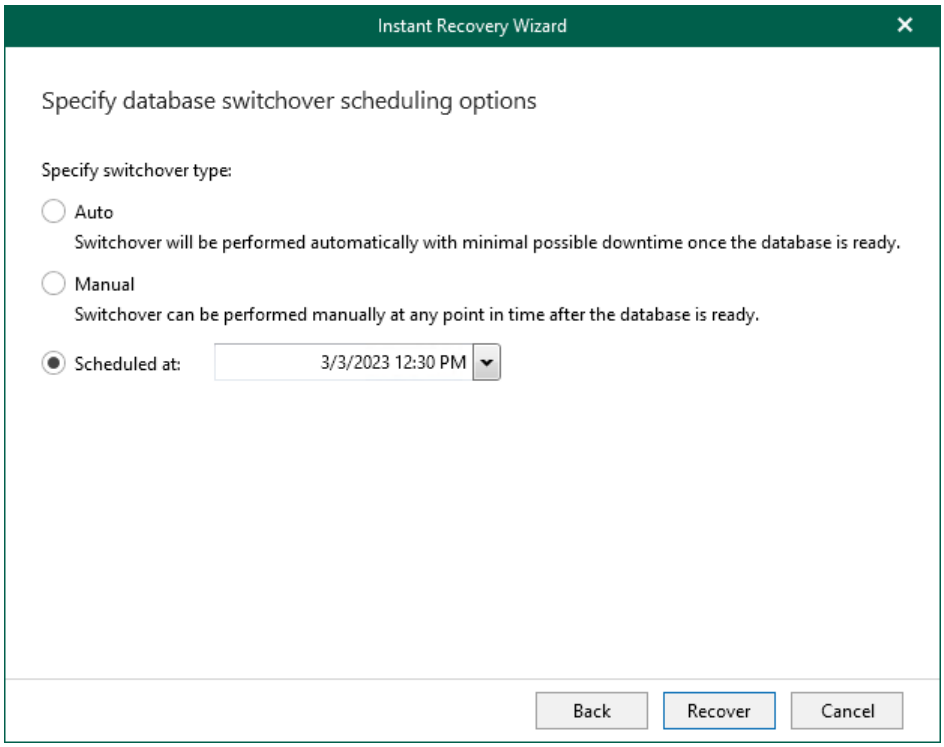
Step 4. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 5. Finalize Instant Recovery Session

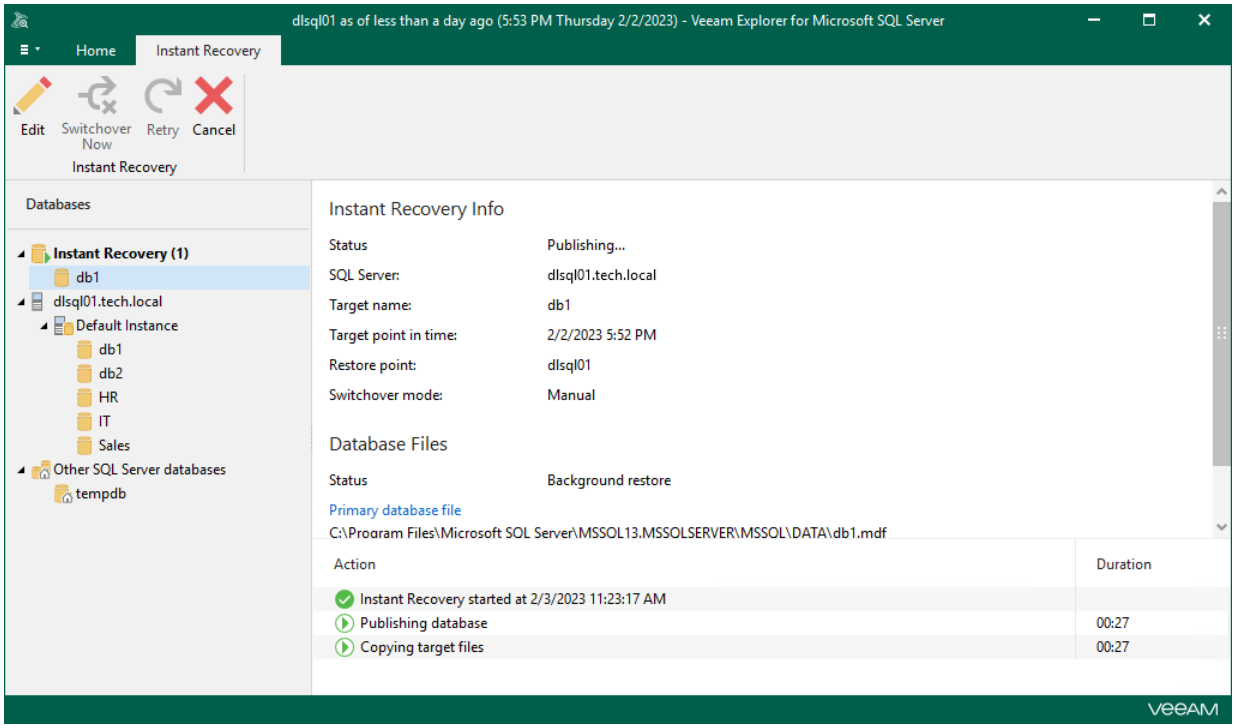
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery to Another Server

To perform instant recovery of a database to another server, use the **Instant Recovery** wizard.

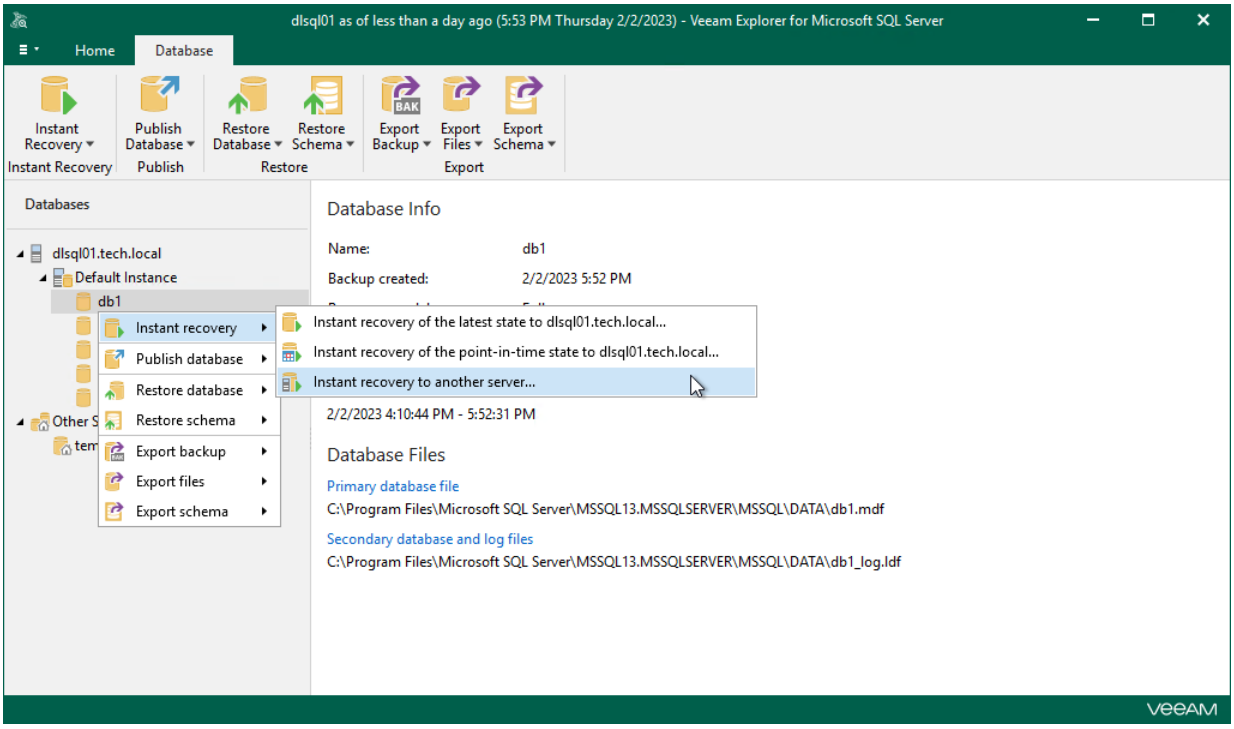
1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify database files location.
6. Specify switchover settings.
7. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery to another server**.

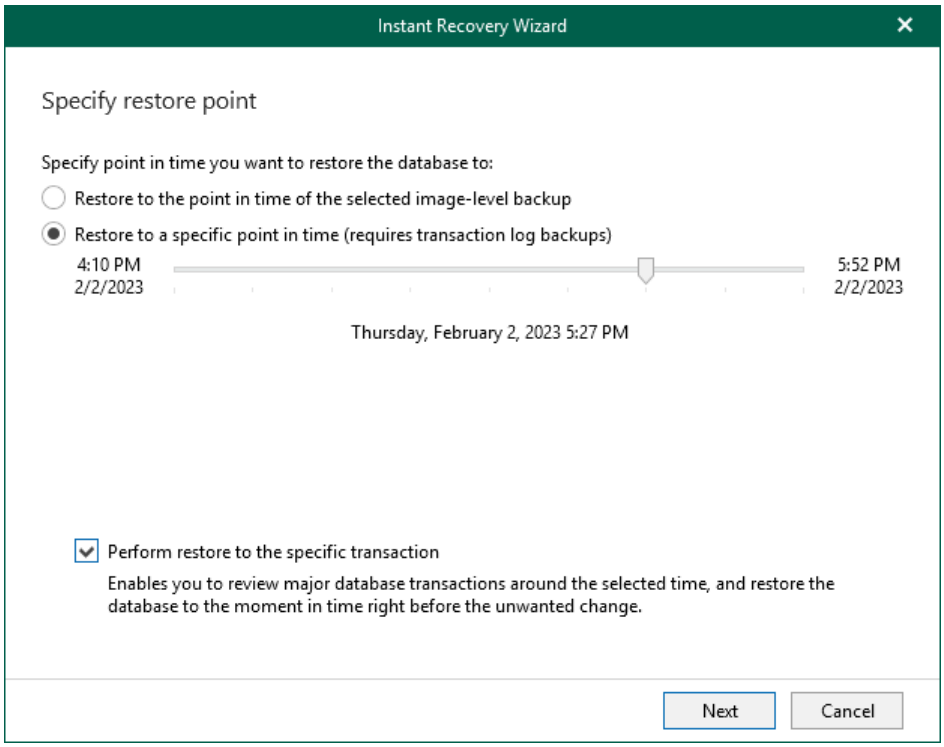
Alternatively, you can right-click a database and select **Instant recovery** > **Instant recovery to another server**.



Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
    a. Use the slider to choose a required point in time.
    b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging server where Microsoft SQL Server is deployed. For more information, see Configuring Staging SQL Server.

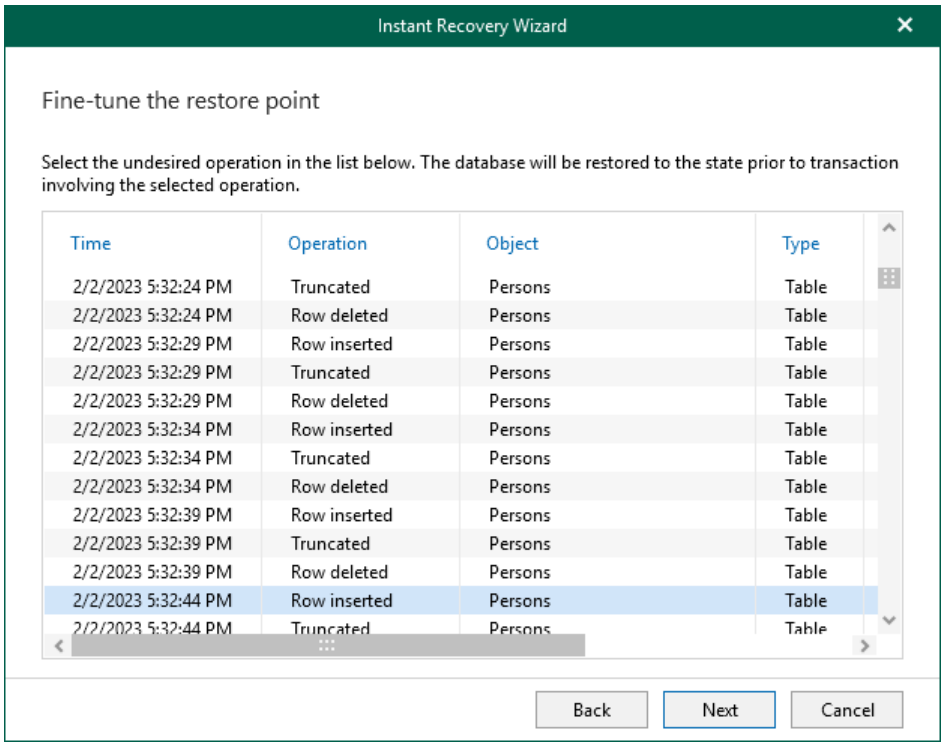


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Server

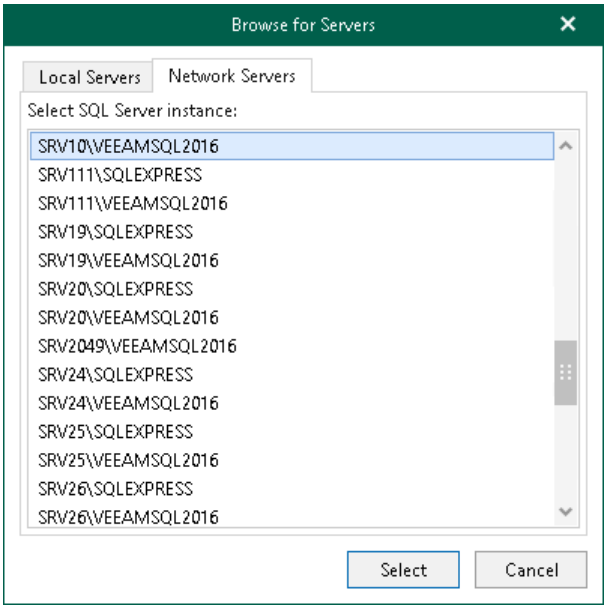
At this step of the wizard, specify credentials to access the target server.

1. In the **Server name** field, specify the target instance to which you want to restore the database. Use the `server\instance` or `IP_address\instance` format. You can select an instance from the drop-down list or use the **Browse** button on the right.

   To browse for other servers and SQL Server instances:

   a. Click the **Browse** button.

   b. You can select a SQL Server instance residing on the local machine on the **Local Servers** tab or click the **Network Servers** tab and select an instance on another server. Veeam Explorer for Microsoft SQL Server display servers from your network where SQL Server is installed.

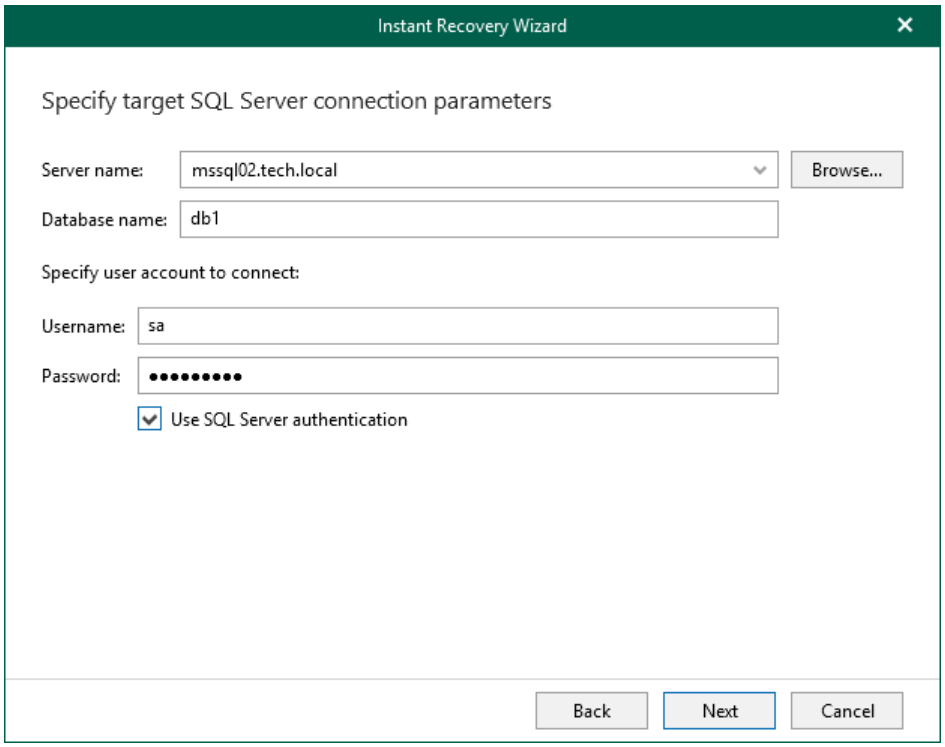


2. In the **Database name** field, specify a name for the restored database.

3. In the **Specify user account to connect** section, specify credentials which will be used to connect to the target SQL Server instance.

   - Select the **Use SQL Server authentication** check box to use SQL Server authentication. If not selected, Veeam Explorer for Microsoft SQL Server will use Windows authentication.
   - Make sure the account has been granted the sysadmin role privileges on a target SQL server.

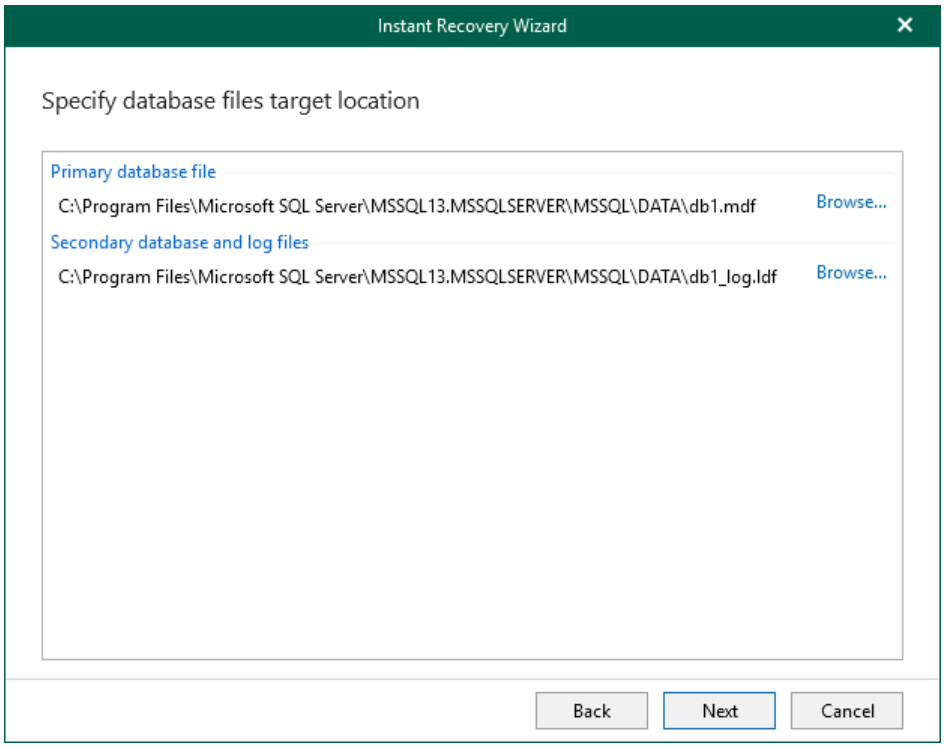
- Make sure that the account has at least **Read** and **Write** permissions on the administrative share (for example, `\\myserver\ADMIN$`) on the target server.



Step 5. Specify Database File Location

At this step of the wizard, specify the location for database files (control files, data files, log files and temp files).

To edit the path, click the path row and specify the location you want to use. If specified folders do not exist, Veeam Explorer for Microsoft SQL Server will create these folders.



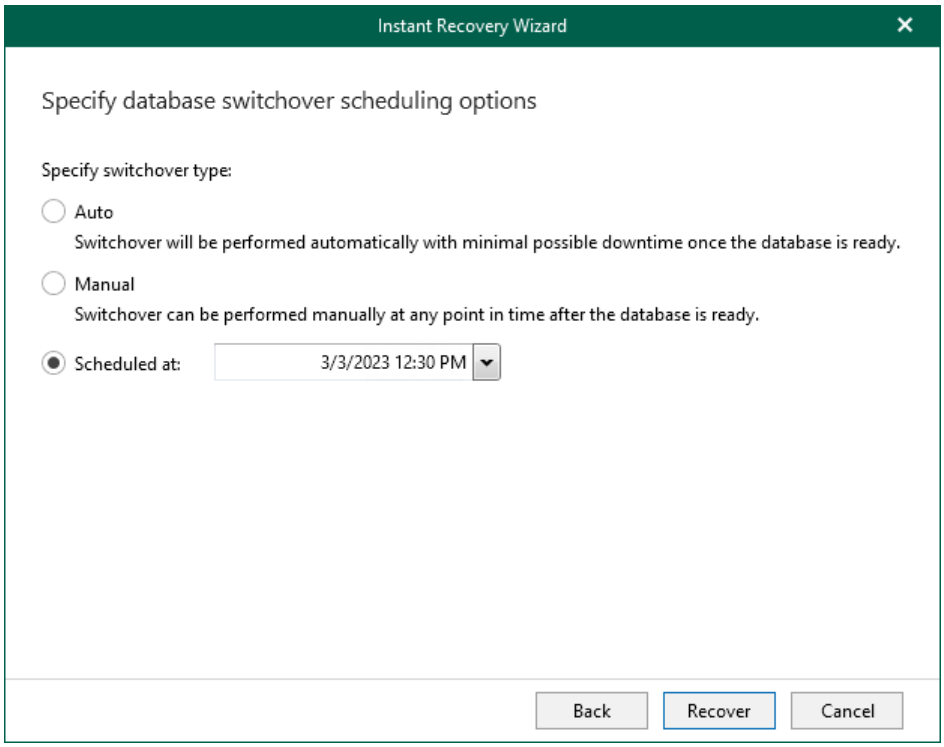
Step 6. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 7. Finalize Instant Recovery Session

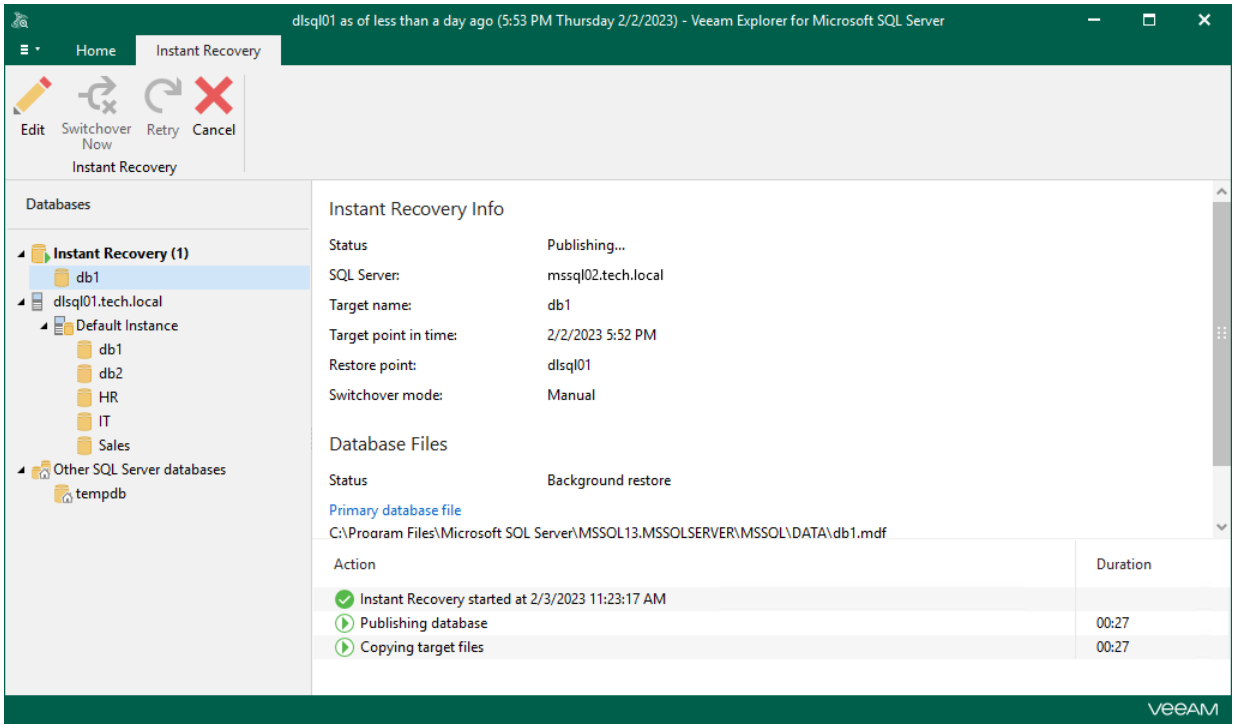
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery of Multiple Databases

You can perform instant recovery of multiple Microsoft SQL Server databases hosted on a server or a certain SQL Server instance. You can perform instant recovery to the original server or any other server in your network where SQL Server is installed.

To instantly recover Microsoft SQL Server databases, follow one of these scenarios:

- Instant Recovery of Latest State
- Instant Recovery of Point-in-Time State
- Instant Recovery to Another Server

Instant Recovery of Latest State

To perform instant recovery of multiple databases to the latest state, use the **Instant Recovery** wizard.

1. Launch the Instant Recovery wizard.
2. Select databases you want to recover.
3. Specify switchover settings.
4. Finalize the Instant Recovery session.

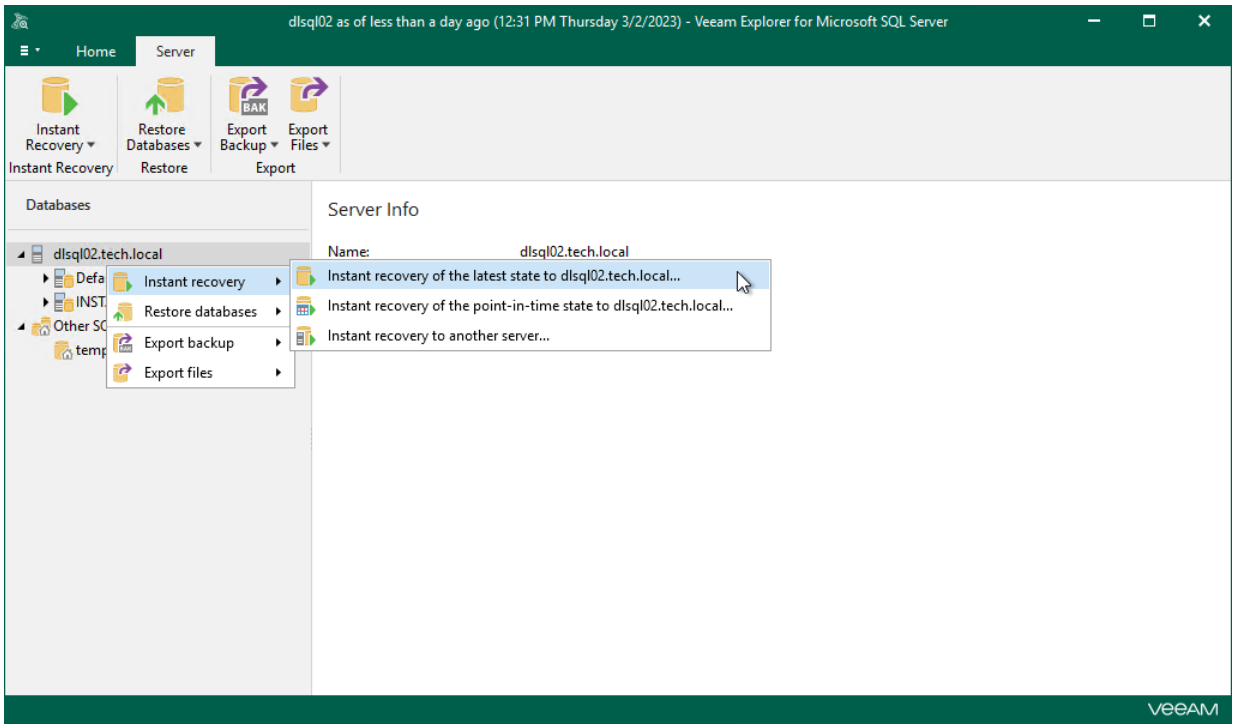
Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Instant Recovery** > **Instant recovery of the latest state to <original_location>**.

Alternatively, you can right-click an instance or the server and select **Instant recovery** > **Instant recovery of the latest state to <original_location>**.

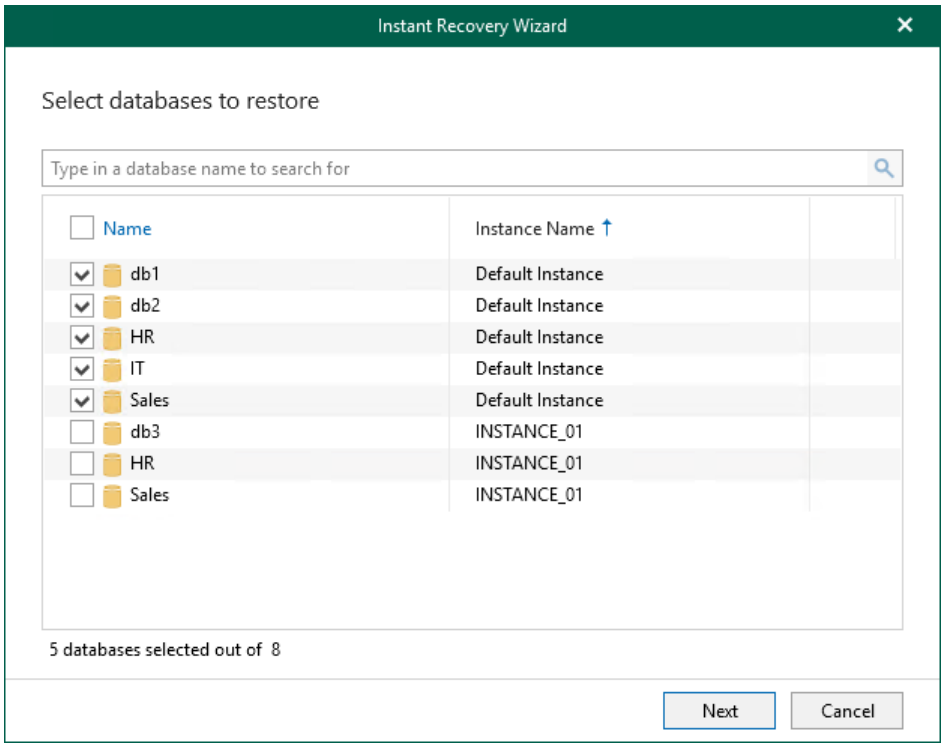
> **NOTE**
>
> The name of the instant recovery option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Instant recovery of the latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Instant recovery of the state of <point_in_time> to <original_location>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to recover.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



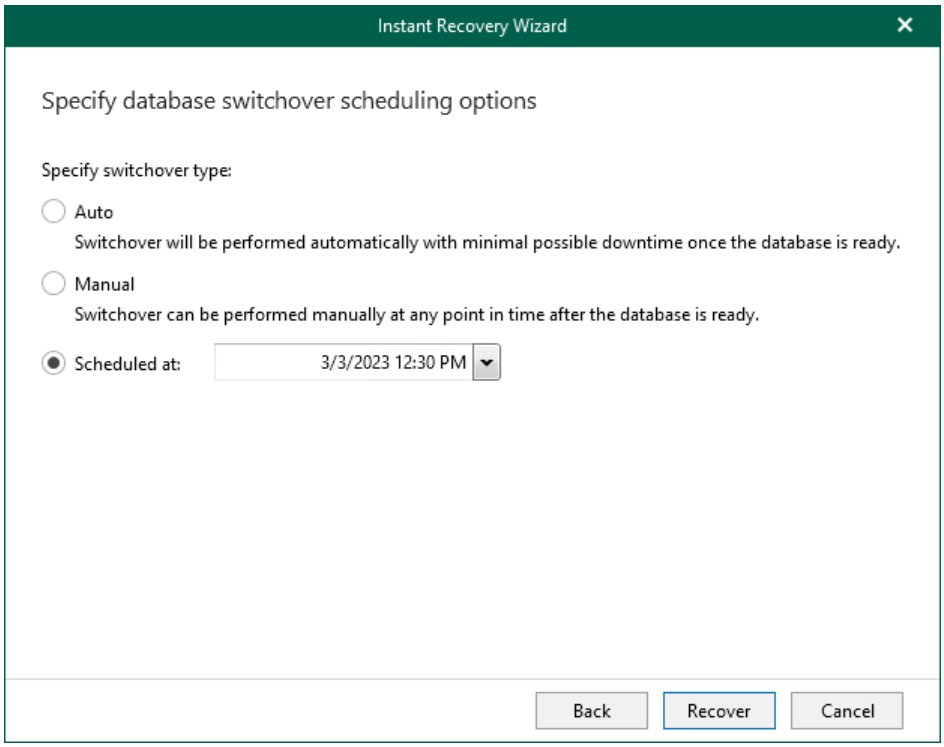
Step 3. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 4. Finalize Instant Recovery Session

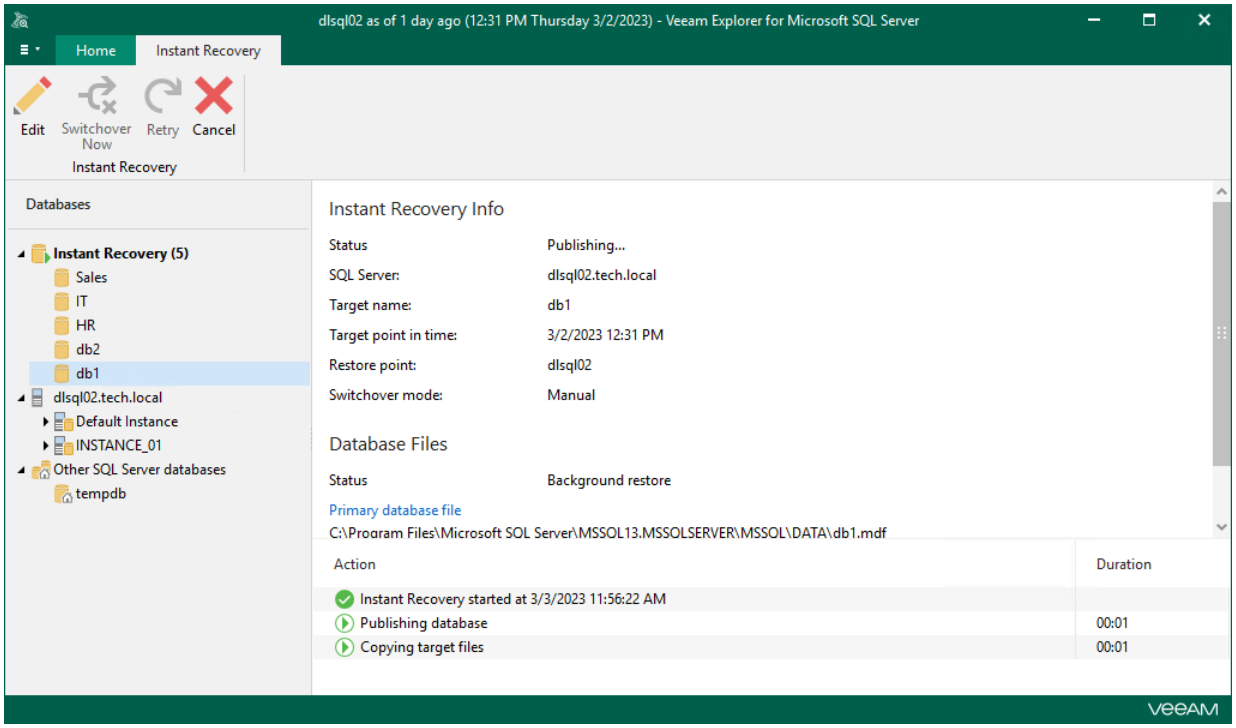
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery of Point-in-Time State

To perform instant recovery of multiple databases to a selected point-in-time state, use the **Instant Recovery** wizard.

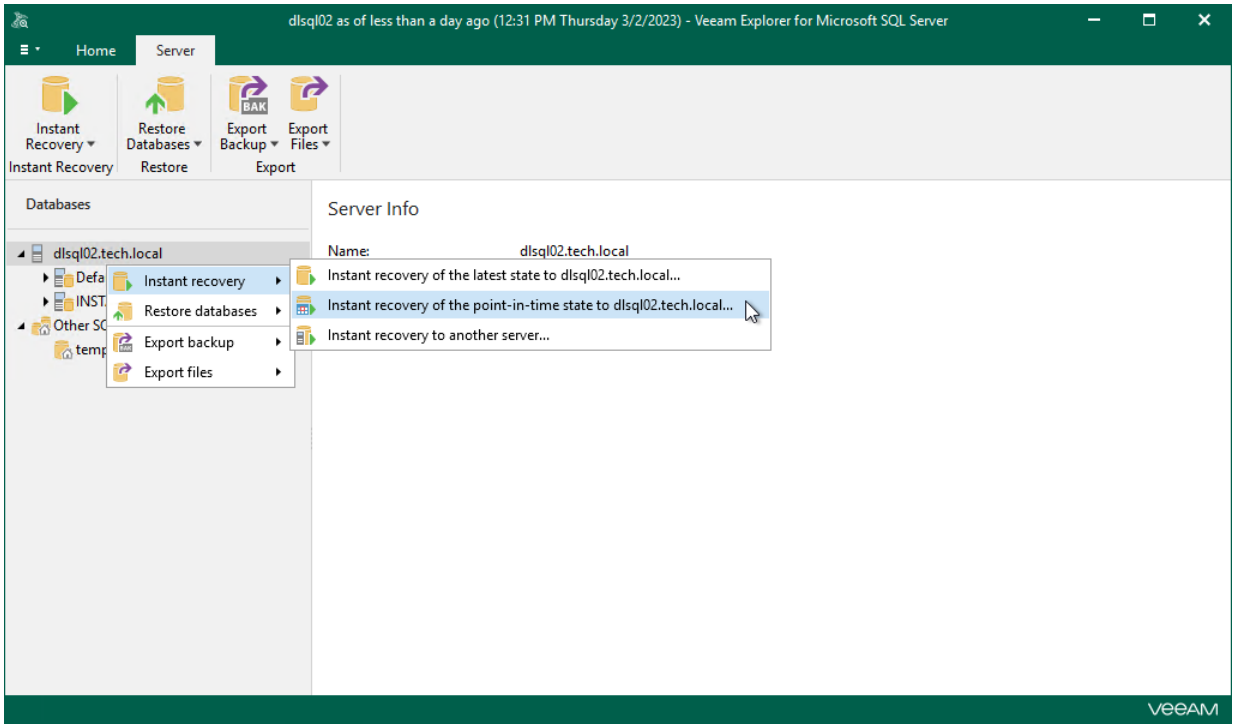
1. Launch the Instant Recovery wizard.
2. Select databases you want to recover.
3. Specify a restore point.
4. Specify switchover settings.
5. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Instant Recovery** > **Instant recovery of the point-in-time state to <original_location>**.

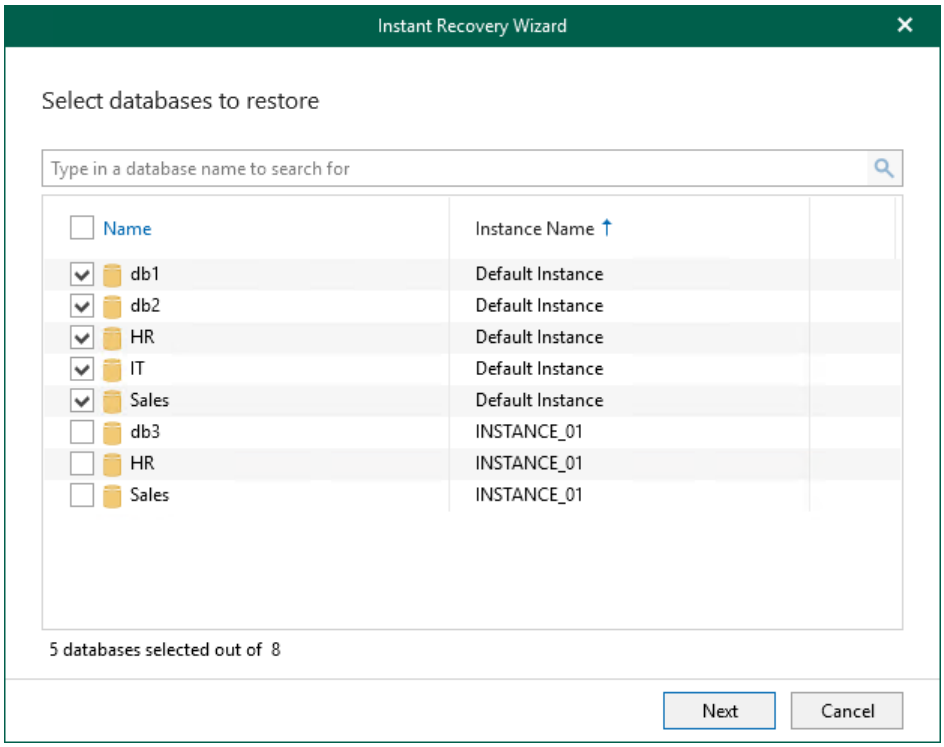
Alternatively, you can right-click an instance or the server and select **Instant recovery** > **Instant recovery of the point-in-time state to <original_location>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to recover.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



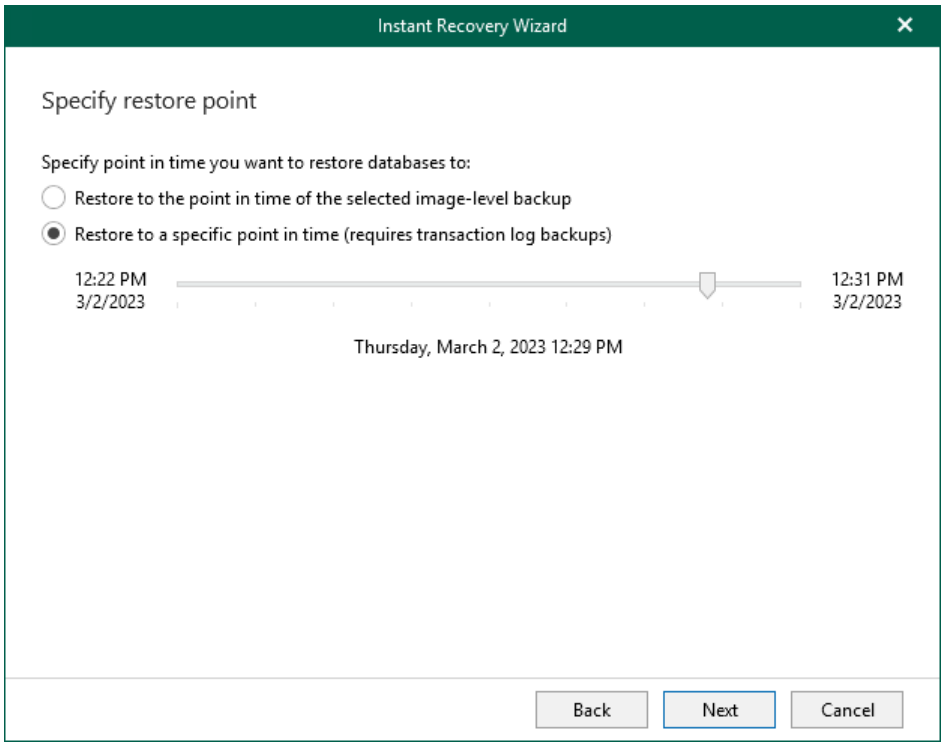
Step 3. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to recover databases:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a required point in time.

  If some of the databases do not have transaction log backups for the specified time, they will be displayed below with their own time point.



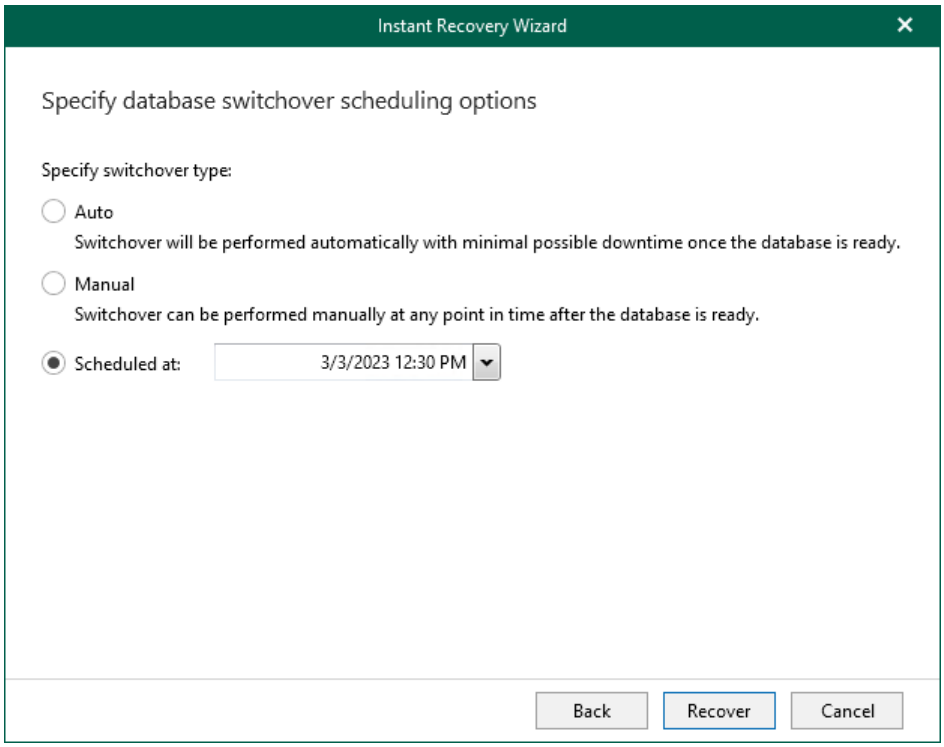
Step 4. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 5. Finalize Instant Recovery Session

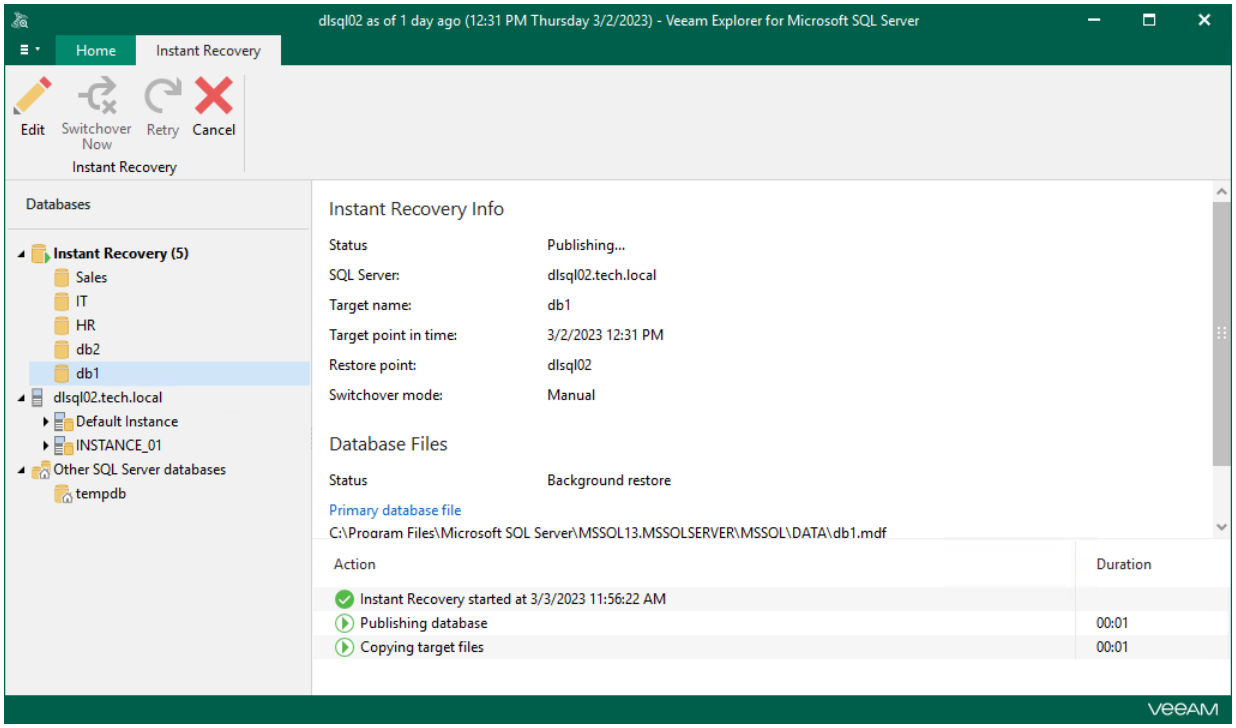
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery to Another Server

To perform instant recovery of multiple databases to another server, use the **Instant Recovery** wizard.

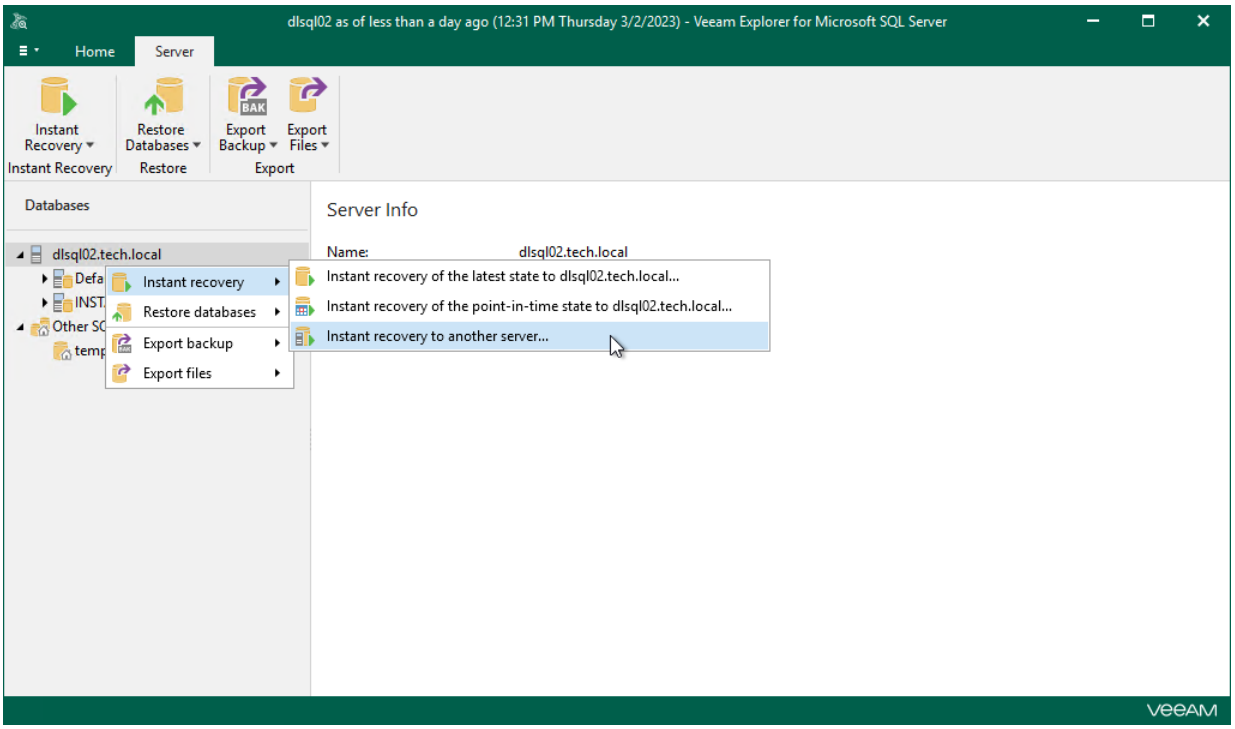
1. Launch the Instant Recovery wizard.
2. Select databases you want to recover.
3. Specify restore point.
4. Specify target server.
5. Specify switchover settings.
6. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Instant Recovery** > **Instant recovery to another server**.

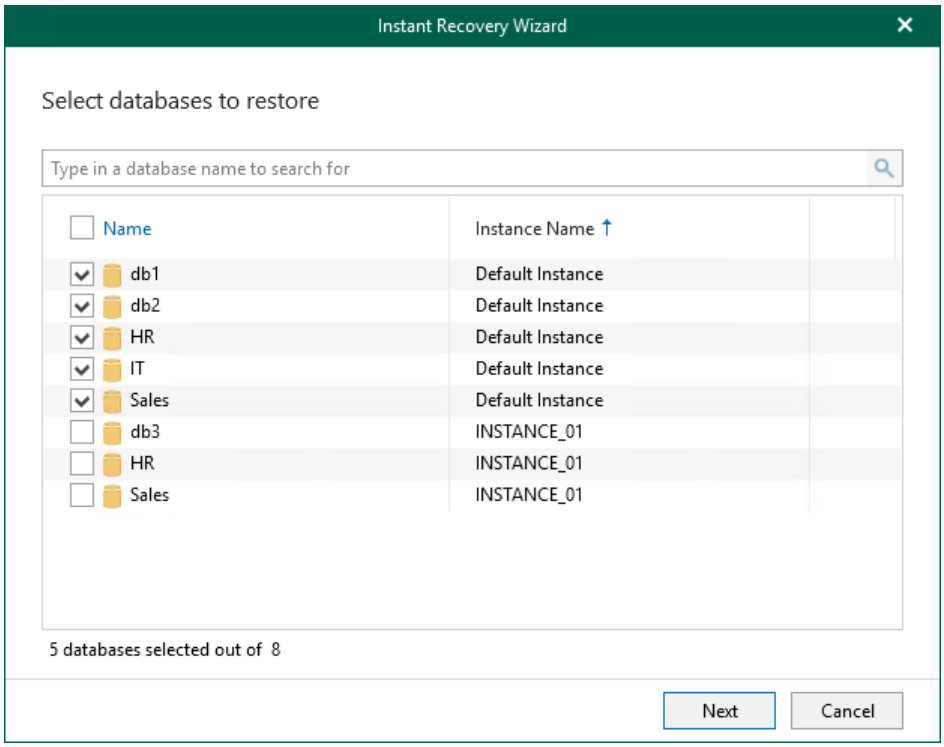
Alternatively, you can right-click an instance or the server and select **Instant recovery** > **Instant recovery to another server**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to recover.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



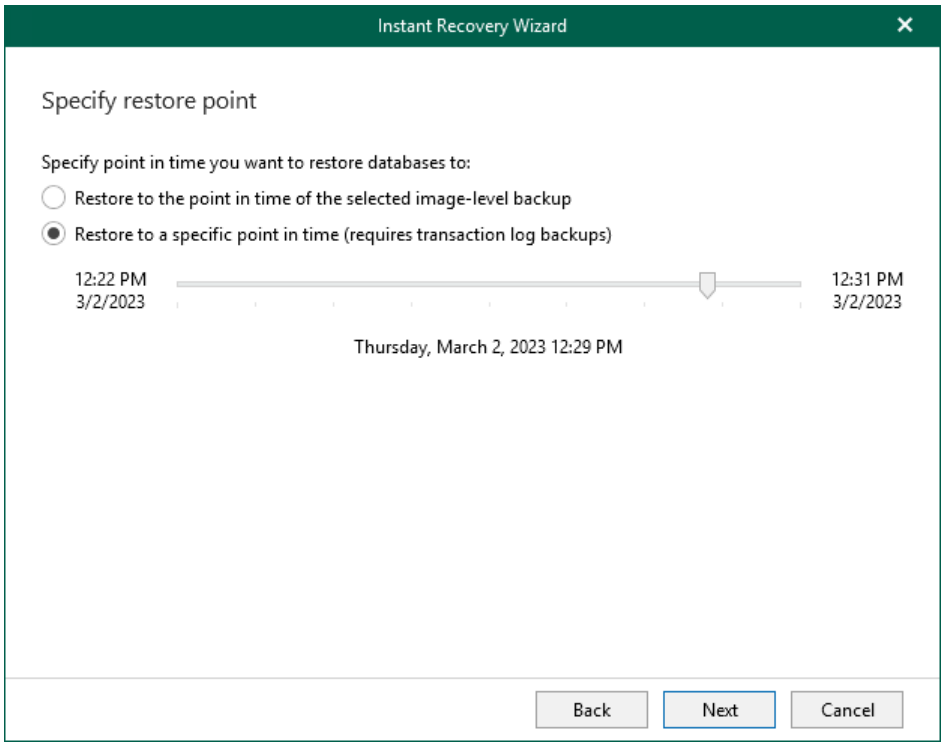
Step 3. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to recover databases:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a required point in time.

  If some of the databases do not have transaction log backups for the specified time, they will be displayed below with their own time point.



Step 4. Specify Target Server

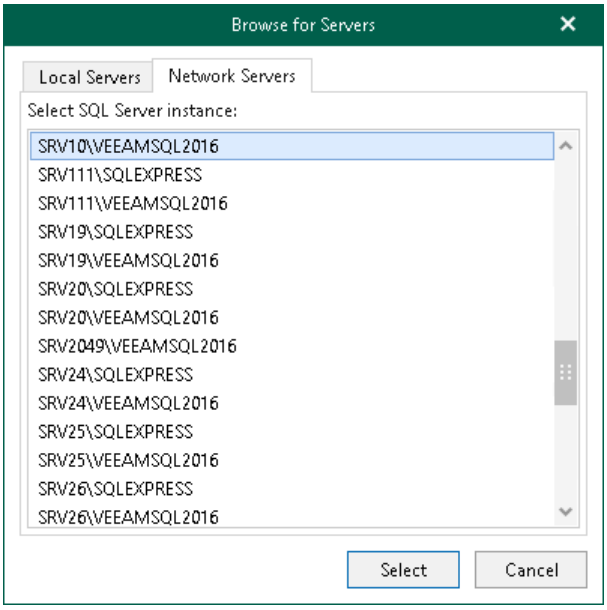
At this step of the wizard, specify credentials to access the target server.

1. In the **Server name** field, specify the target instance to which you want to restore the database. Use the `server\instance` or `IP_address\instance` format. You can select an instance from the drop-down list or use the **Browse** button on the right.

   To browse for another servers and SQL Server instances:

   a. Click the **Browse** button.

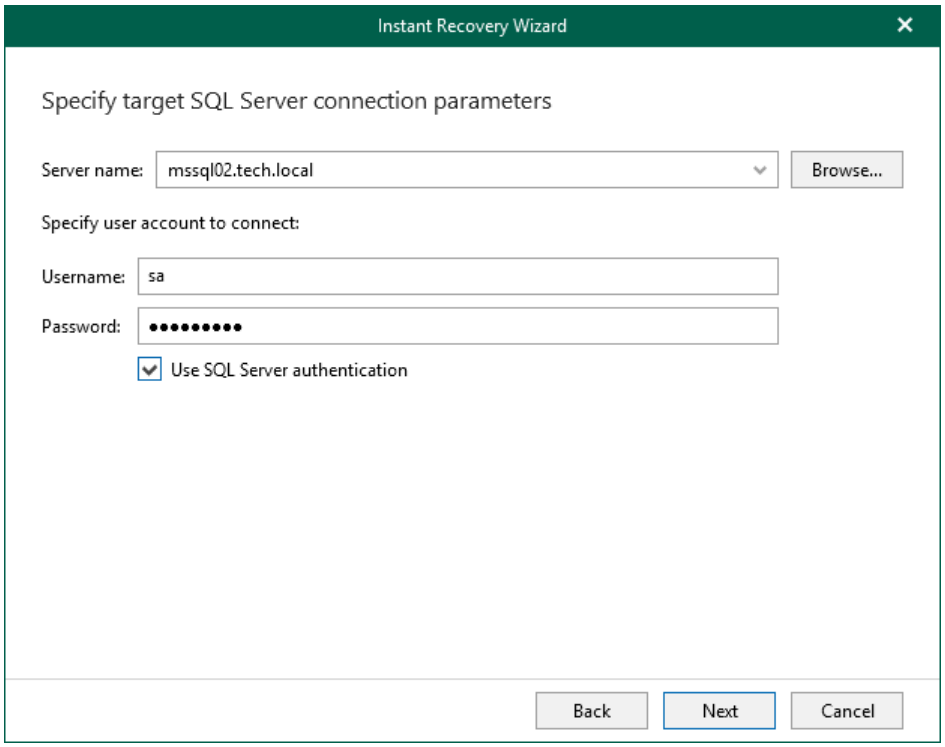
   b. You can select a SQL Server instance residing on the local machine on the **Local Servers** tab or click the **Network Servers** tab and select an instance on another server. Veeam Explorer for Microsoft SQL Server displays servers from your network where SQL Server is installed.



2. In the **Specify user account to connect** section, specify credentials which will be used to connect to the target SQL Server instance.

   - Select the **Use SQL Server authentication** check box to use SQL Server authentication. If not selected, Veeam Explorer for Microsoft SQL Server will use Windows authentication.
   - Make sure the account has been granted the sysadmin role privileges on a target SQL server.

- Make sure that the account has at least *Read* and *Write* permissions on the administrative share (for example, `\\myserver\ADMIN$`) on the target server.



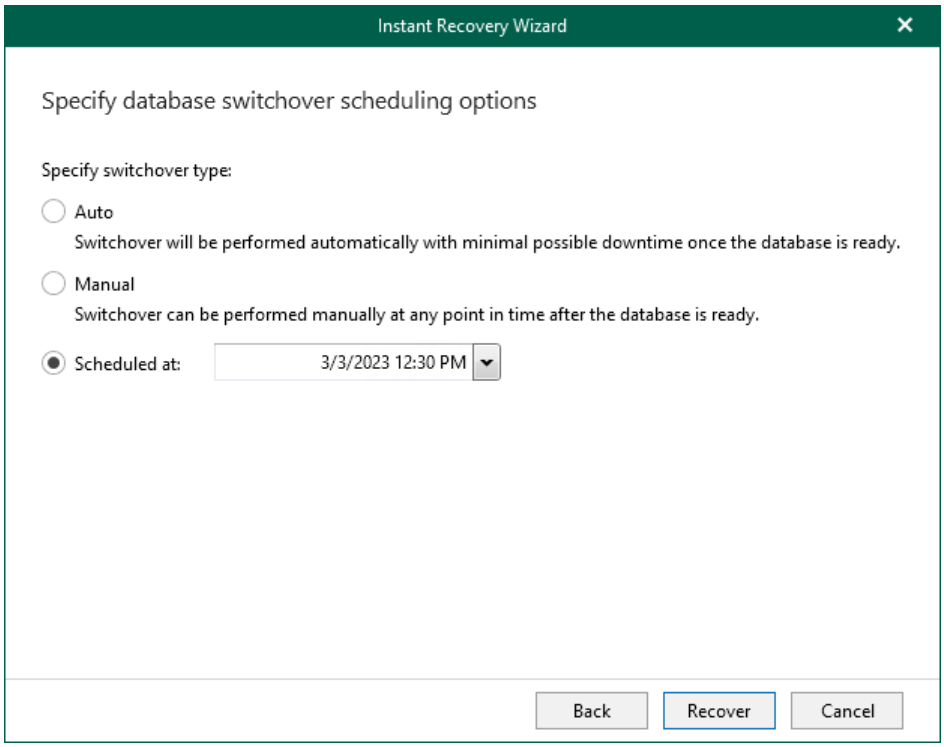
Step 5. Specify Switchover Settings

At this step of the wizard, specify a database switchover type. During switchover, the mounted database is switched to its complete copy on the target server.

To select a switchover type and start an instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Microsoft SQL Server starts publishing the database on the target server.



Step 6. Finalize Instant Recovery Session

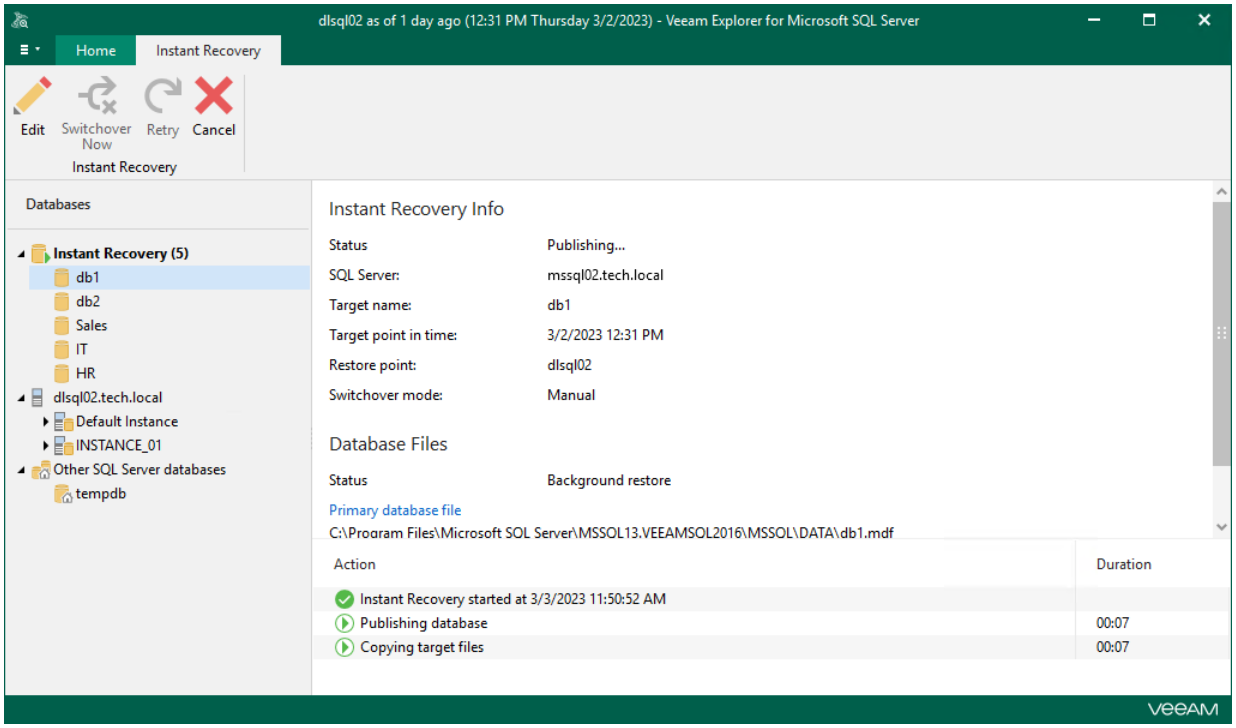
After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session.

In the **Instant Recovery** session view, you can see the progress of the recovery, edit switchover settings, cancel instant recovery, and start manual switchover (if you have selected the **Manual** switchover option in the **Instant Recovery** wizard).

Depending on the selected switchover option, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Switchover

The switchover option becomes available after all the database files are copied to the target server and all database files are synchronized. During switchover, the published mount is detached from the target SQL Server instance and the copied database is attached to this instance. Note that if you have selected to restore to the original server, the restored database will replace the original database.

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

During switchover, Veeam Explorer for Microsoft SQL Server performs the following operations:

1. Detaches the published database from the SQL Server instance.
2. Uses the cache to synchronize changes between the published database and the copied database files.
3. Drops the published database.
4. Attaches the recovered database to the SQL Server instance.

Note that the database will be offline between steps 1–4.

Auto Switchover

The Auto switchover option ensures minimal period of downtime.

As soon as database files are copied from the mount server, Veeam Explorer for Microsoft SQL Server checks the size of the cache that contains changes that have been made to the database since the publishing. Depending on the cache size, the following happens:

- If the cache size is smaller than 100 MB, Veeam Explorer for Microsoft SQL Server starts the switchover process.
- If the cache size is larger than 100 MB, Veeam Explorer for Microsoft SQL Server uses the cache to synchronize changes and checks the cache size once again. If the cache size is smaller than 100 MB, Veeam Explorer for Microsoft SQL Server starts the switchover process. If the cache size is larger than 100 MB again, another cycle of synchronization is performed. Synchronization is relaunched until the cache size is smaller than 100 MB.

Manual Switchover

After database files are copied from the mount server, Veeam Explorer for Microsoft SQL Server checks the size of the cache that contains changes that have been made to the database since the publishing. The cache size is checked every minute. If the cache size is larger than 100 MB or it has been 5 minutes since the last synchronization, Veeam Explorer for Microsoft SQL Server starts to synchronize the changes between the published database and the copied database files.

After synchronization is finished, you can launch switchover manually. For details, see Starting Switchover Manually.

If you launch switchover during the synchronization process, switchover starts only after the synchronization is finished.

Scheduled Switchover

After database files are copied from the mount server, Veeam Explorer for Microsoft SQL Server checks the size of the cache that contains changes that have been made to the database since the publishing. The cache size is checked every minute. If the cache size is larger than 100 MB or it has been 5 minutes since the last synchronization, Veeam Explorer for Microsoft SQL Server starts to synchronize the changes between the published database and the copied database files.

After synchronization is finished, Veeam Explorer for Microsoft SQL Server waits for the scheduled date and time to start switchover.

If the switchover scheduled period starts during the synchronization process, switchover starts only after the synchronization is finished.

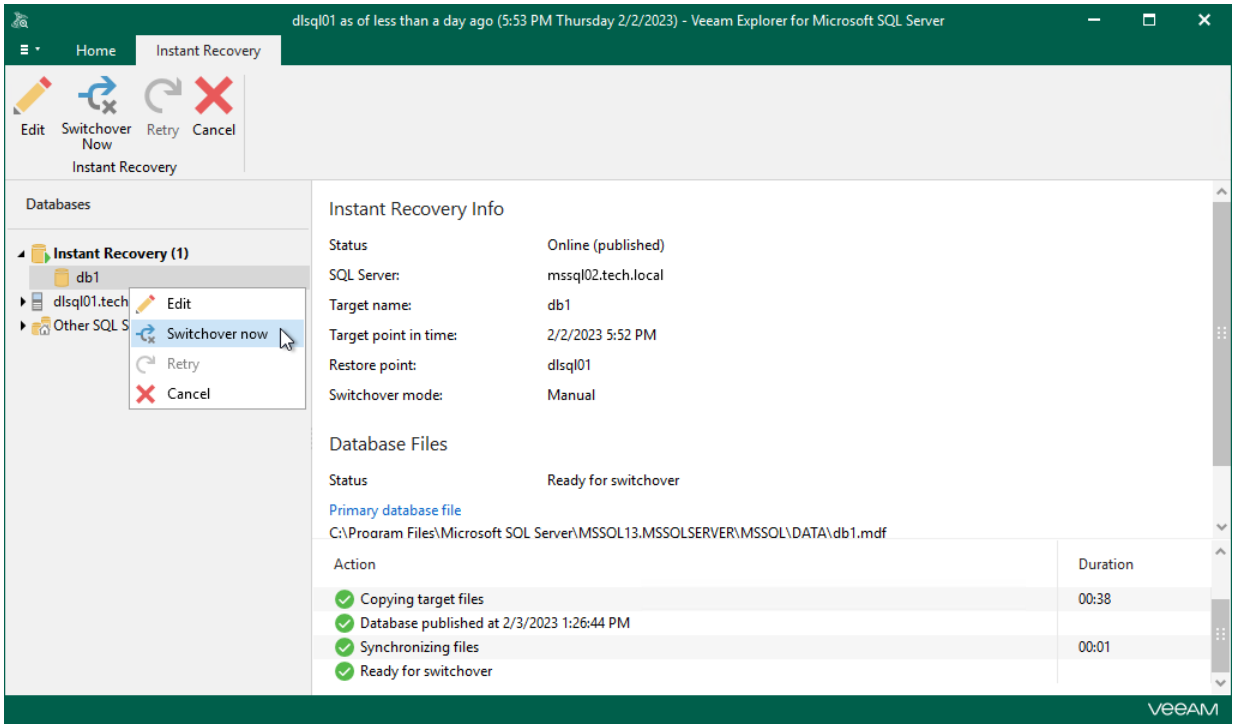
Starting Switchover Manually

If you have selected the *Manual* switchover option in the **Instant Recovery** wizard, you can start the switchover process at any time if the database is in the *Ready to switchover* state.

To start switchover manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Switchover Now**.

Alternatively, you can right-click the database and select **Switchover now**.



Managing Instant Recovery Session

After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Microsoft SQL Server starts an instant recovery session which shows the progress of the recovery process.

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

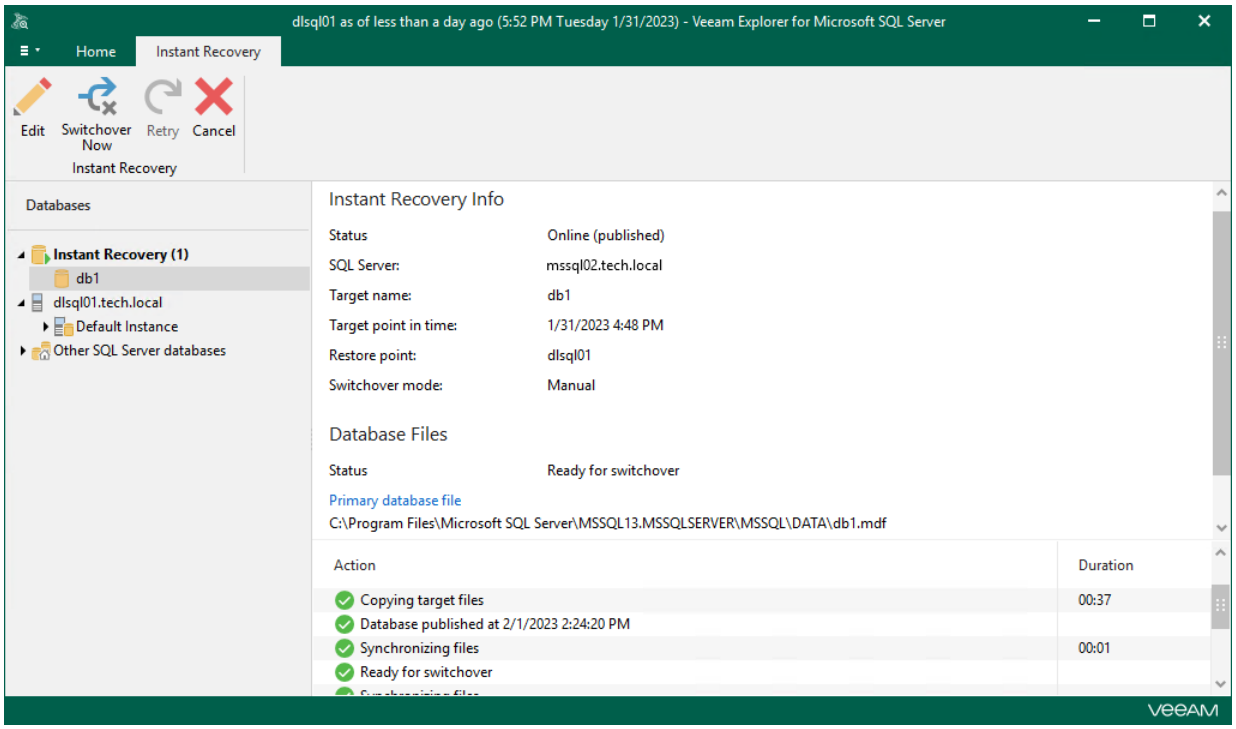
- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Also, in the **Instant Recovery** session view, you can do the following:

- Edit switchover settings.
- Retry instant recovery (in case instant recovery session fails for any reason).
- Cancel instant recovery.

> **NOTE**
>
> The instant recovery session closes automatically after switchover.

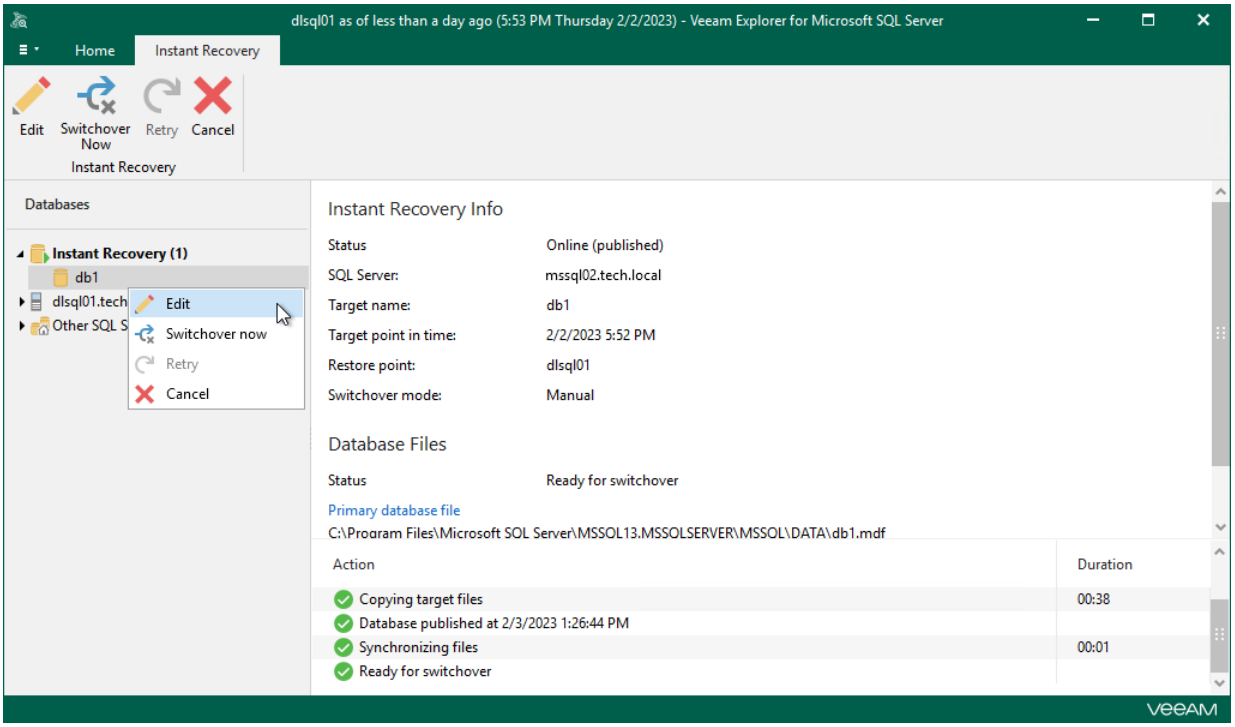


Editing Instant Recovery Settings

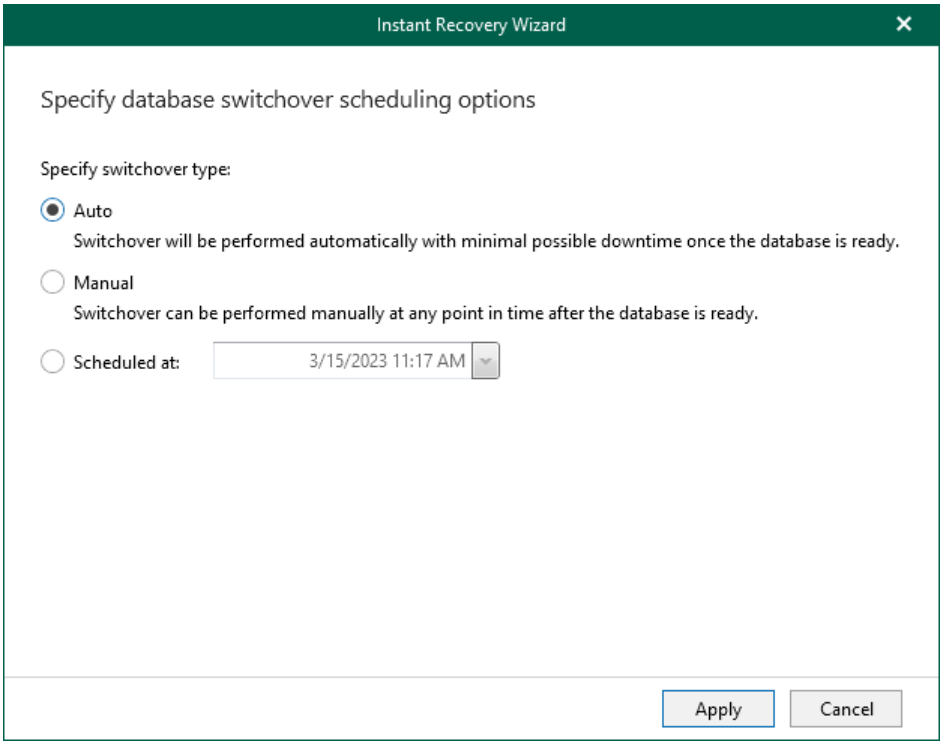
If you have started an instant recovery session and want to change switchover settings, you can edit the instant recovery settings.

To change the switchover settings of an instant recovery session, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Edit** or right-click the database or instance and select **Edit**.



3. Change the switchover option and click **Apply**.



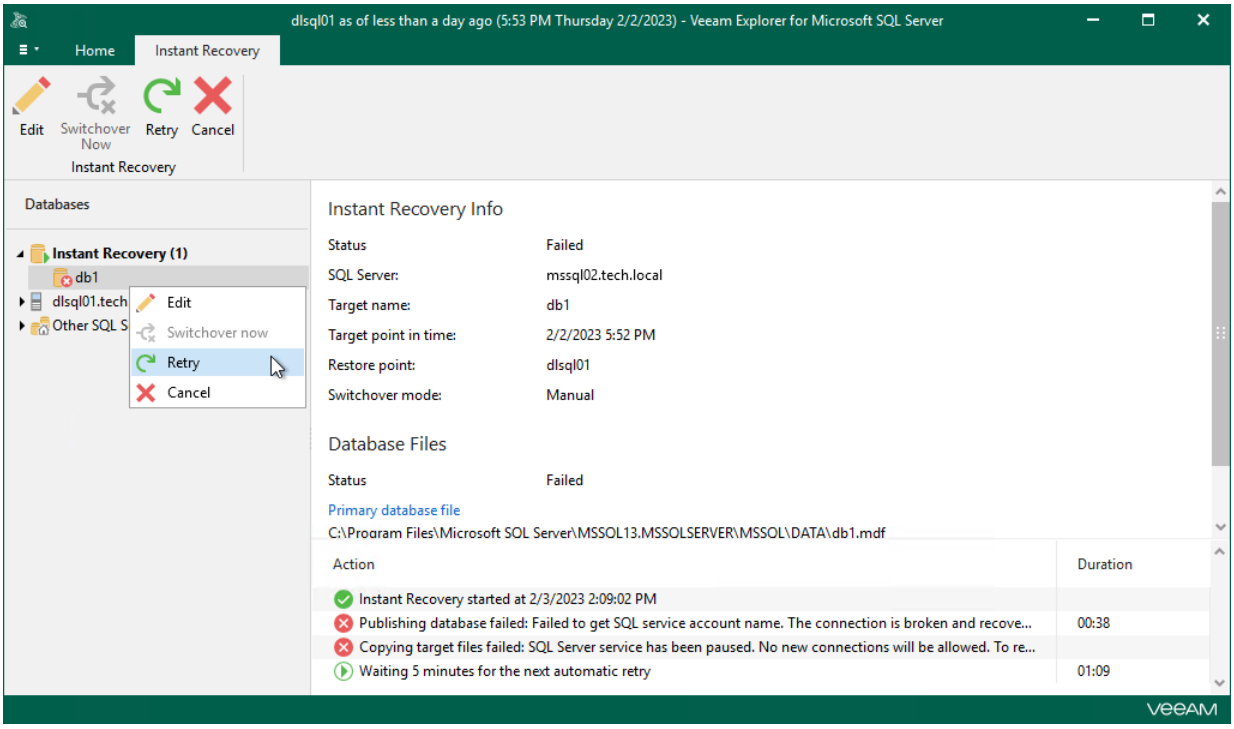
Recovery Retry

If anything disrupts the restore process (the target or mount server crashes or the network is down), the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch the retry manually after the server or network is up.

To start the retry process manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select the database.
2. On the **Instant Recovery** tab, click **Retry**.

Alternatively, you can right-click the database and select **Retry**.



Canceling Instant Recovery

If you have finished working with the published database and you do not want to switchover, you can cancel the instant recovery session.

You can do this by canceling instant recovery in either Veeam Explorer for Microsoft SQL Server or the Veeam Backup & Replication console.

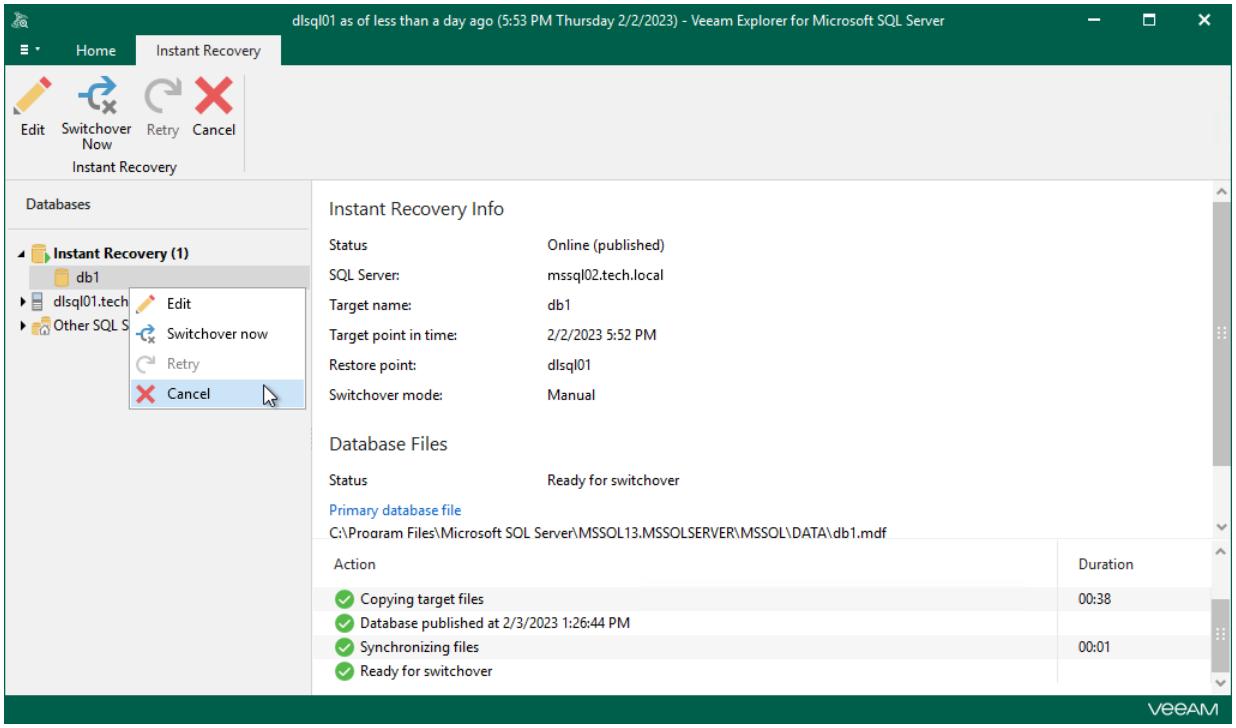
> **NOTE**
>
> Consider the following:
>
> - Closing either the Veeam Explorer for Microsoft SQL Server window or the Veeam Backup & Replication console does not cancel the instant recovery session.
> - You do not need to cancel the instant recovery session if switchover is already performed. The session closes automatically after switchover.

Canceling Instant Recovery in Veeam Explorer for Microsoft SQL Server

To cancel the instant recovery session in Veeam Explorer for Microsoft SQL Server, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Cancel**.

Alternatively, you can right-click the database and select **Cancel**.

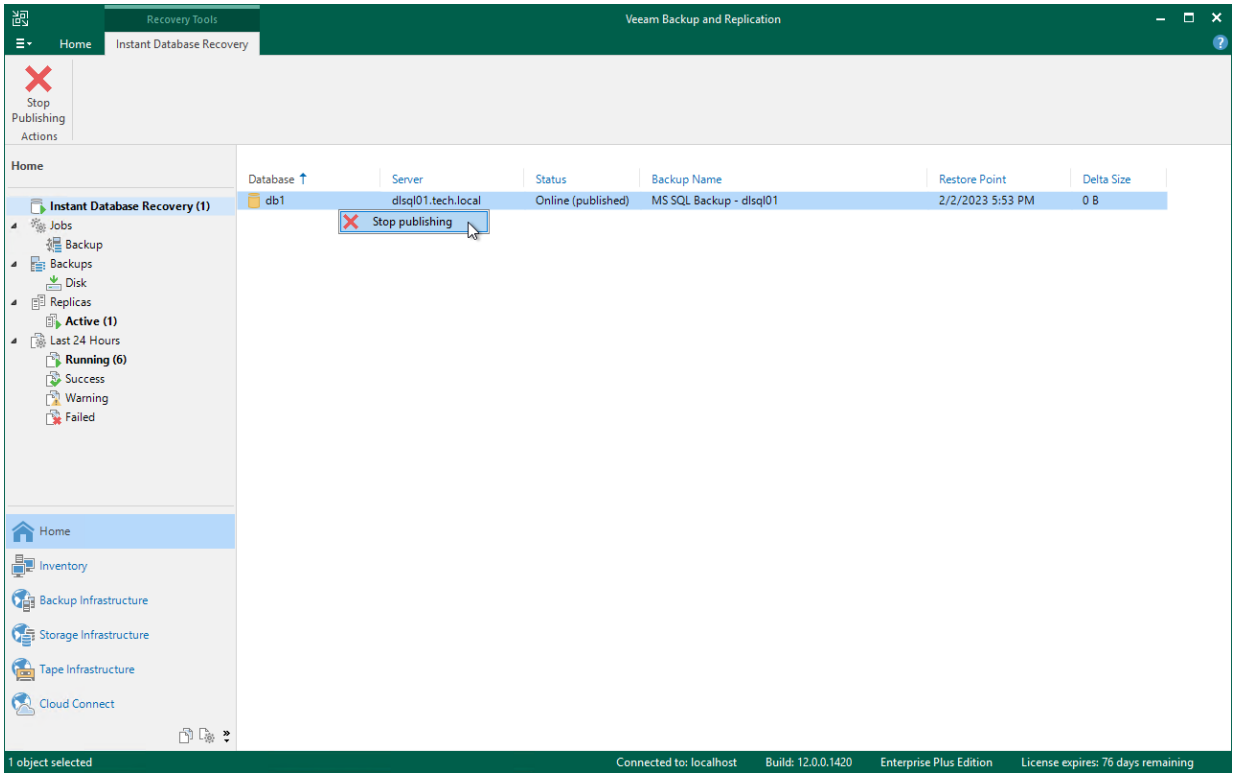


Canceling Instant Recovery in Veeam Backup & Replication Console

To cancel the instant recovery session in the Veeam Backup & Replication console, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the navigation pane, select **Instant Database Recovery**.
3. In the preview pane, select the session and in the **Instant Database Recovery** tab click **Stop Publishing**.

   Alternatively, you can right-click the session and click **Stop publishing**.



Data Export

This section contains information about the available export options for Microsoft SQL Server databases.

Exporting as MDF

This section explains how to use Veeam Explorer for Microsoft SQL Server to export database files in the MDF format.

Exporting Single Database

You can export a single Microsoft SQL Server database by following one of these scenarios:

- Exporting Latest State
- Exporting Point-in-Time State
- Exporting to Different Location

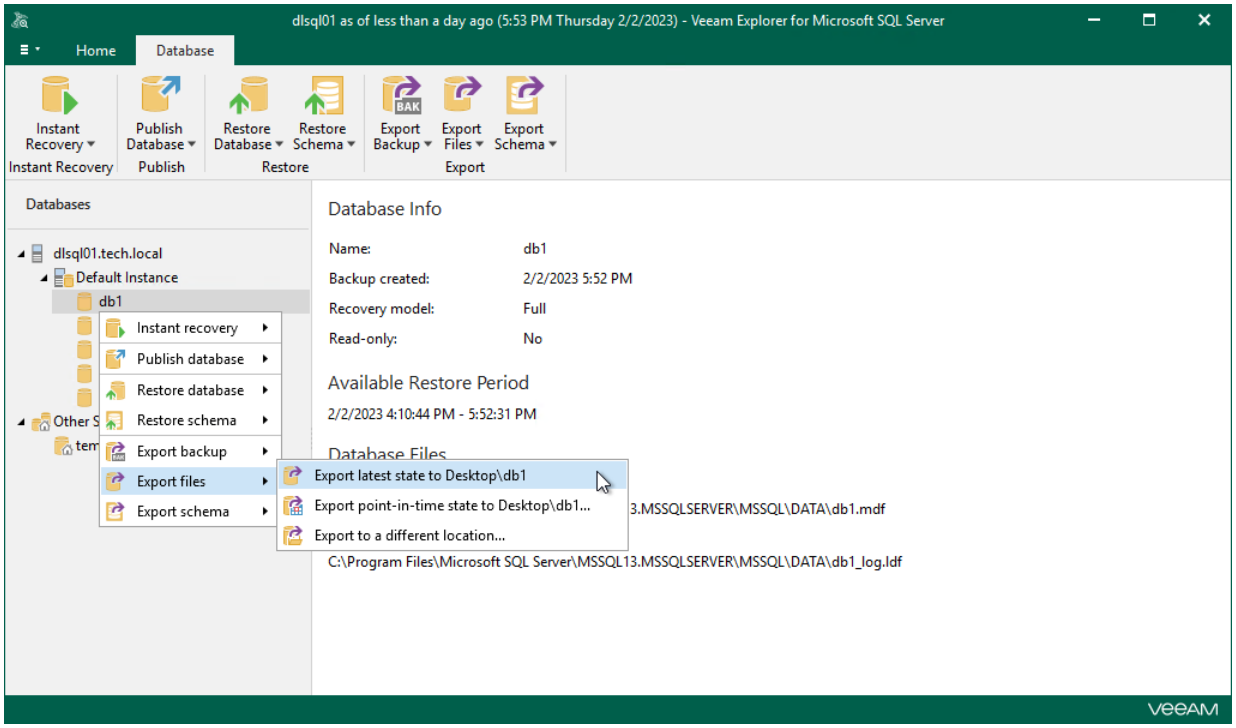
Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Files** > **Export latest state to Desktop\<db_name>**.

Alternatively, right-click a database and select **Export files** > **Export latest state to Desktop\<db_name>**.

> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export latest state to Desktop\<db_name>**.
> - If you select any other restore point, the option name is displayed as **Export state of <point_in_time> to Desktop\<db_name>**.



Exporting Point-in-Time State

To export data as of a point-in-time state, use the **Export** wizard.

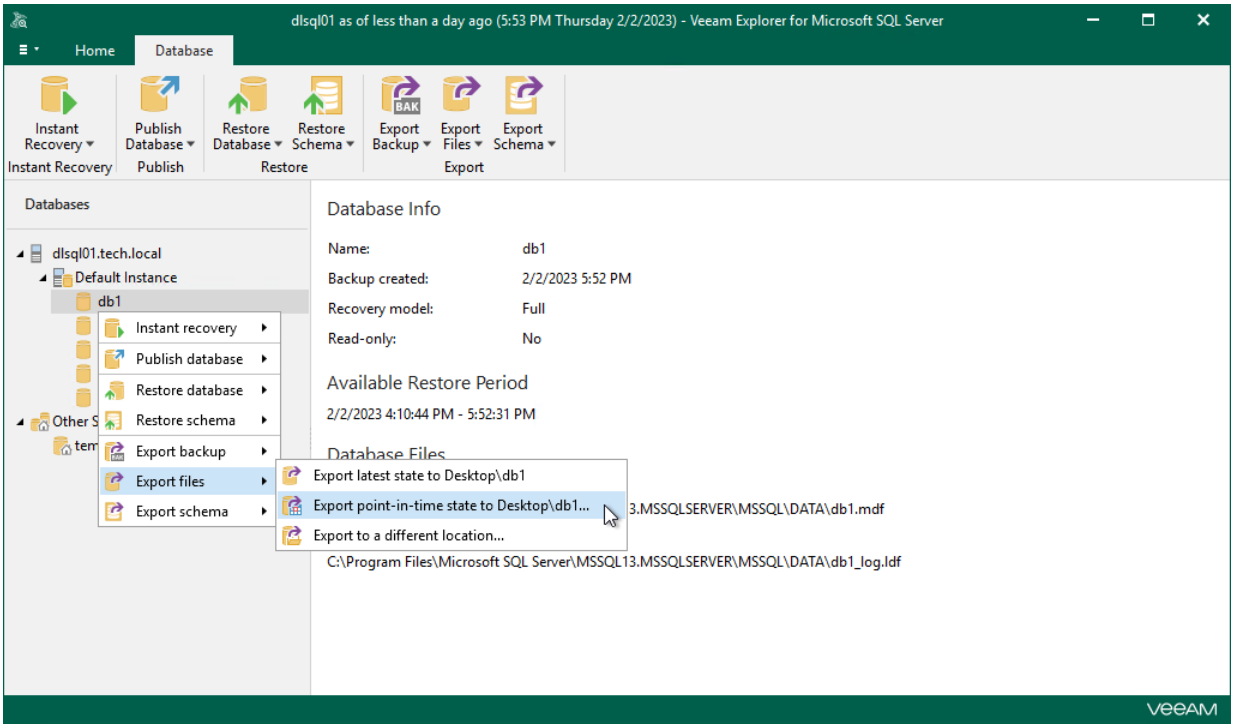
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Files** > **Export point-in-time state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export files** > **Export point-in-time state to Desktop\<db_name>**.



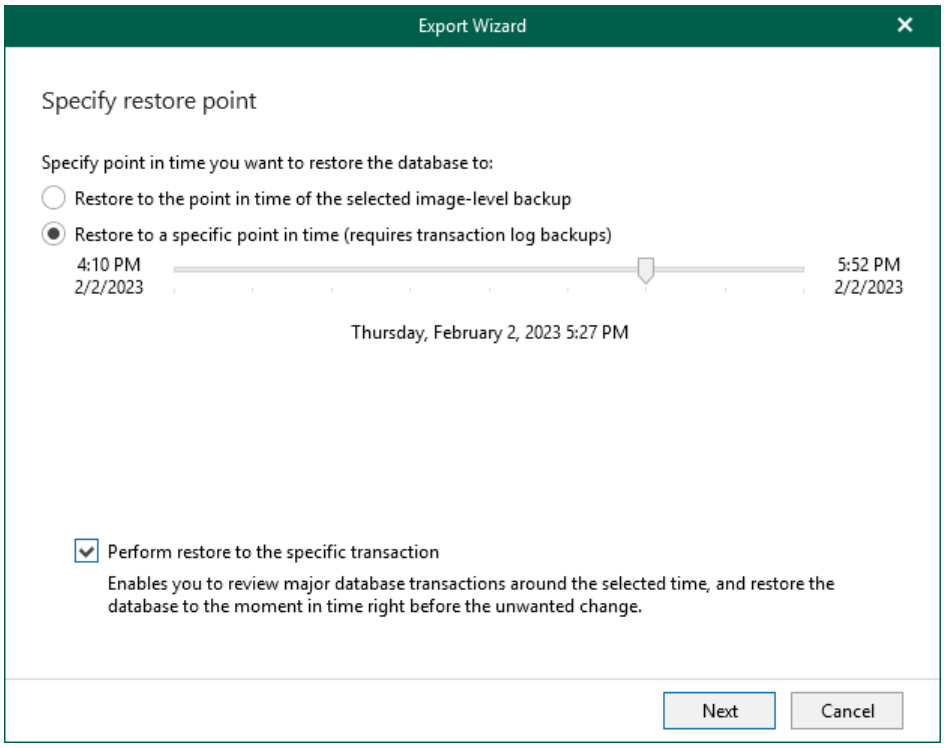
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

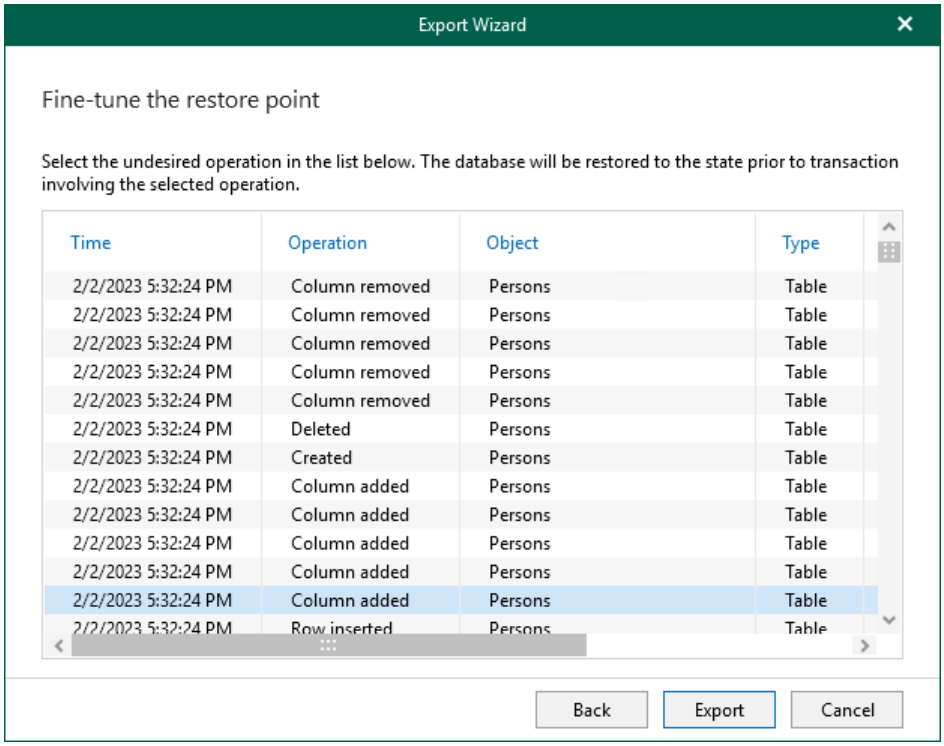


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database and click **Export**.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Exporting to Different Location

To export a single Microsoft SQL Server database to a custom location, use the **Export** wizard.

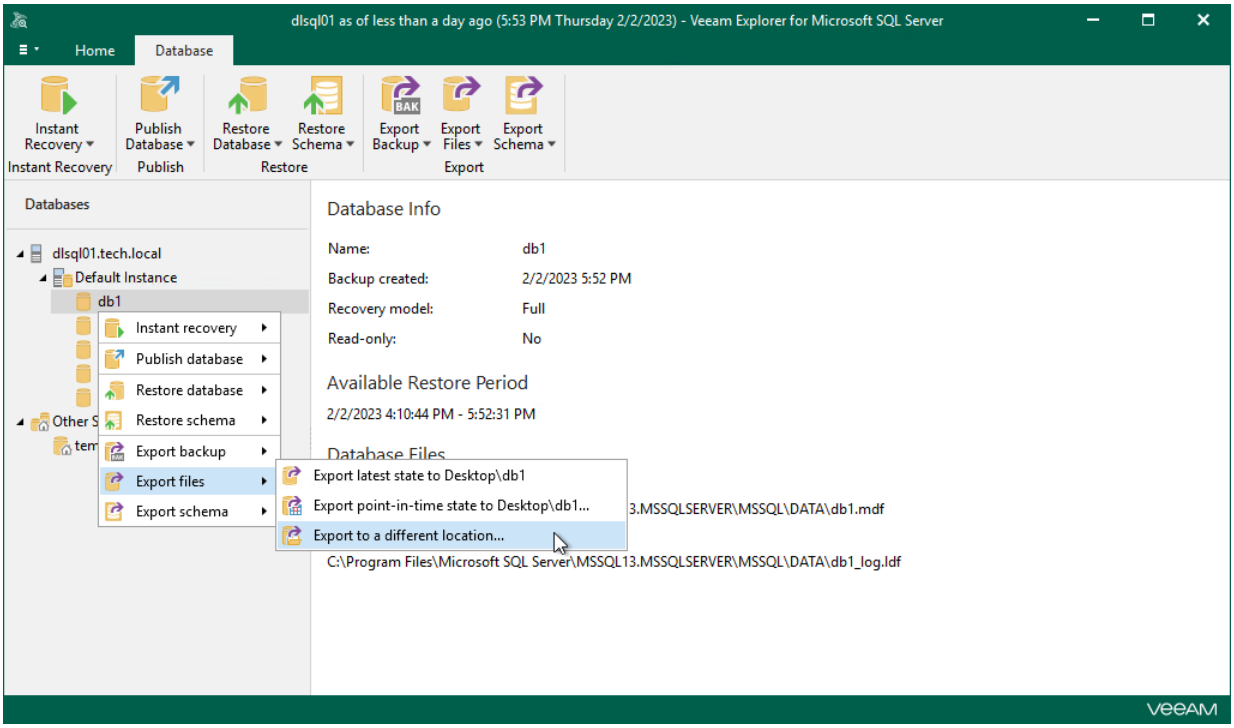
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify files location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Files** > **Export to a different location**.

Alternatively, you can right-click a database and select **Export files** > **Export to a different location**.



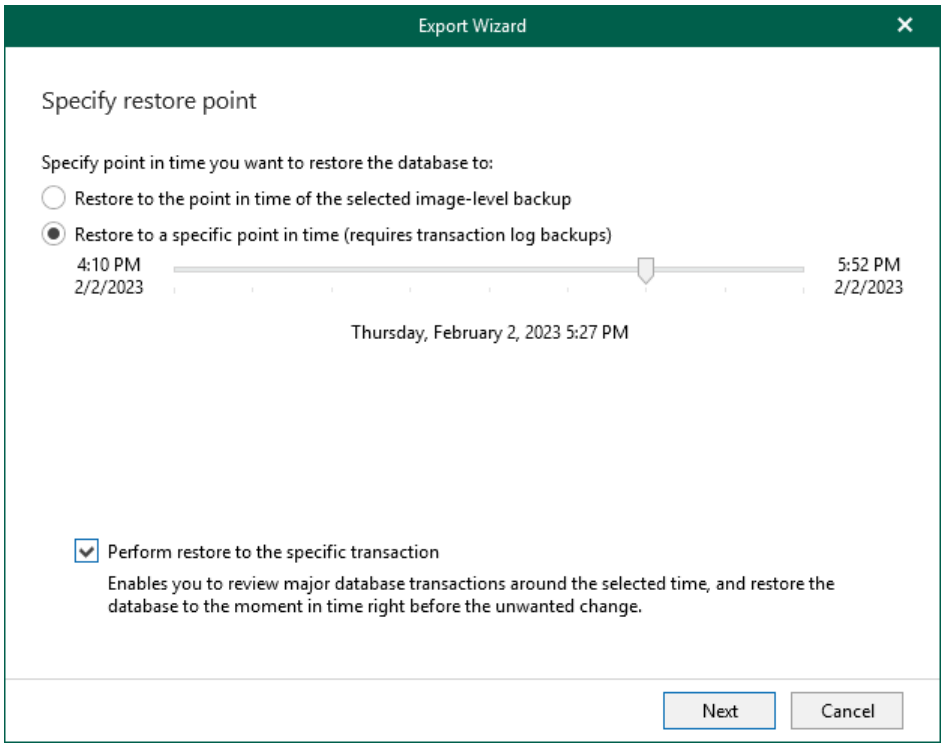
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

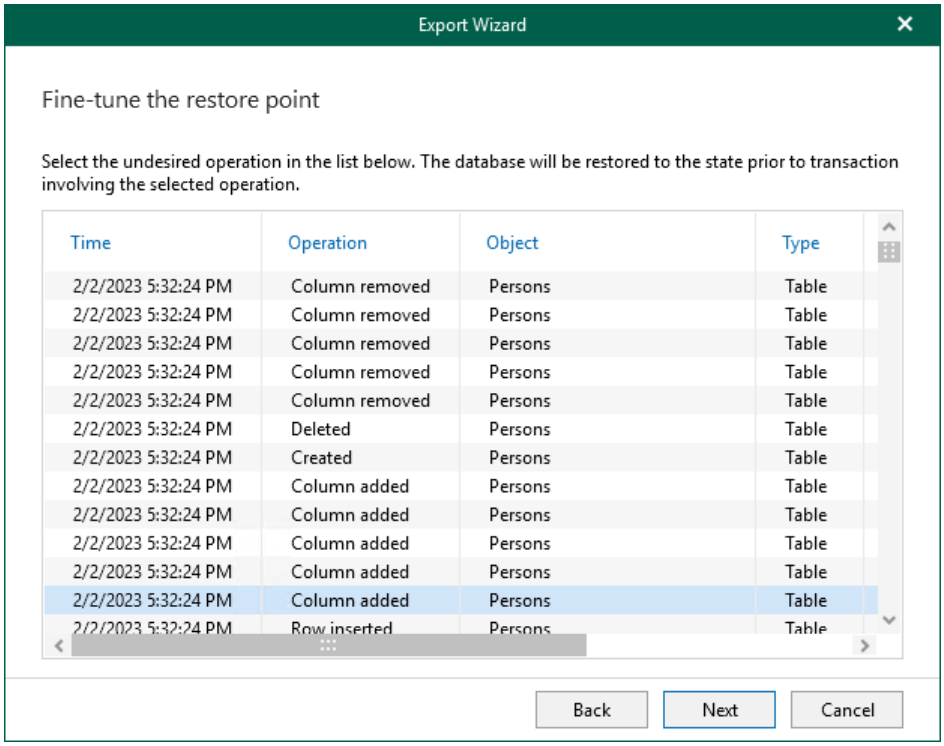


Step 3. Fine-Tune Restore Point

To fine-tune the restore point, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.

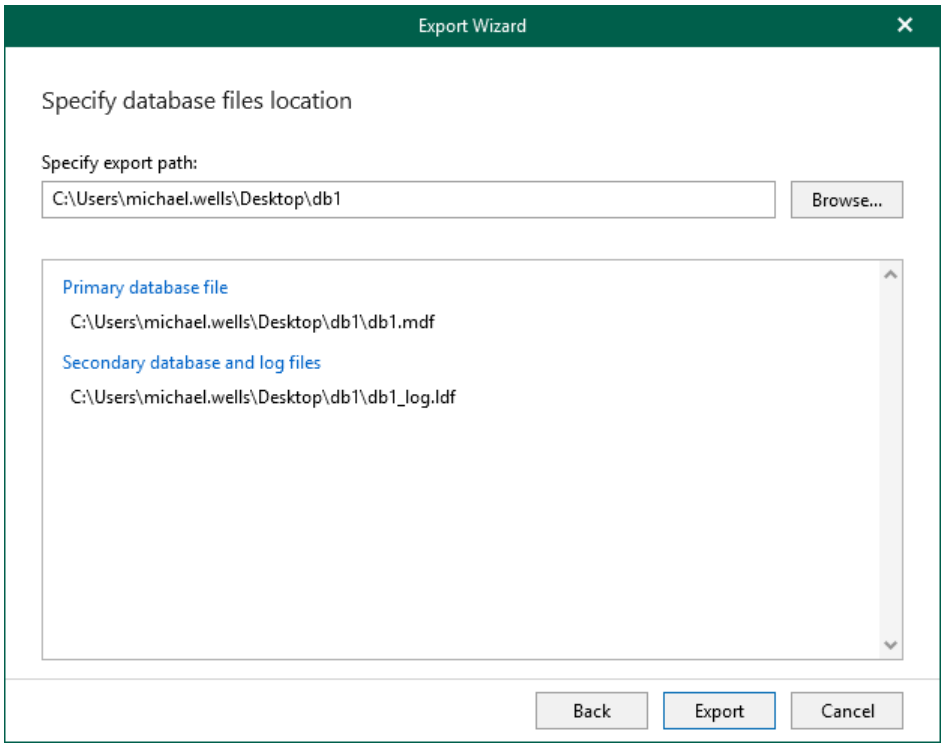


Step 4. Specify Files Location

At this step of the wizard, specify a path to the directory where you want to export database files.

Click **Browse** to specify the path manually.

> **NOTE**
>
> The account you are using must have a sufficient permission level to access the selected directory (Read and Write as minimum recommended).



Exporting Multiple Databases

You can export multiple Microsoft SQL Server databases by following one of these scenarios:

- Exporting Latest State
- Exporting Point-in-Time State
- Exporting to Different Location

Exporting Latest State

To export data as of the latest available state, use the **Export** wizard.

1. Launch the Export wizard.
2. Select databases you want to export.

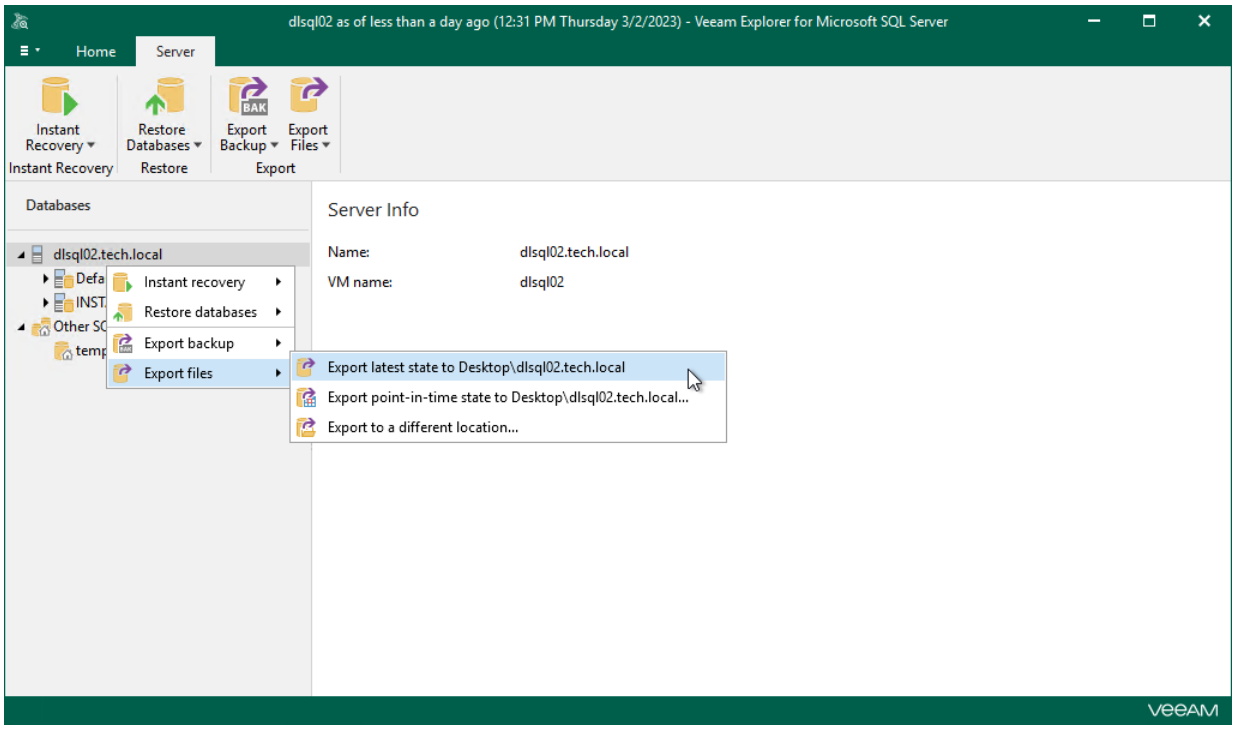
Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Export Files** > **Export latest state to Desktop\<server_name>**.

Alternatively, you can right-click an instance or the server and select **Export files** > **Export latest state to Desktop\<server_name>**.

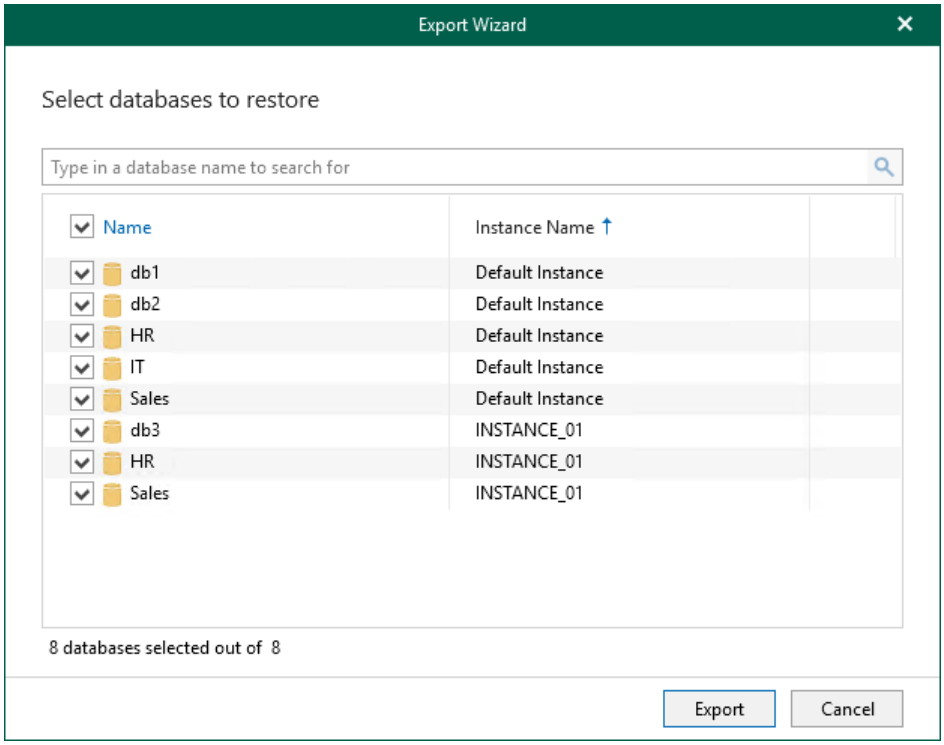
> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export latest state to Desktop\<server_name>**.
> - If you select any other restore point, the option name is displayed as **Export state of <point_in_time> to Desktop\<server_name>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



Exporting Point-in-Time State

To export data as of a point-in-time state, use the **Export** wizard.

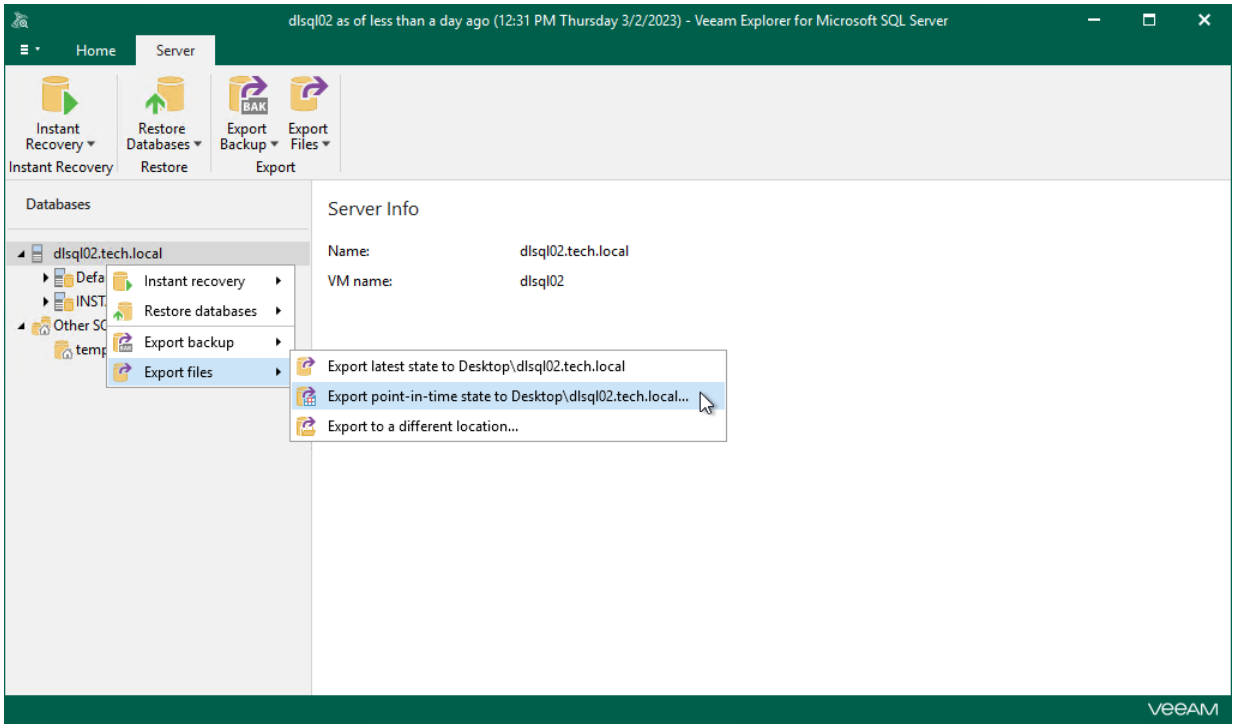
1. Launch the Export wizard.
2. Select databases you want to export.
3. Specify a restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Export Files** > **Export point-in-time state to Desktop\<db_name>**.

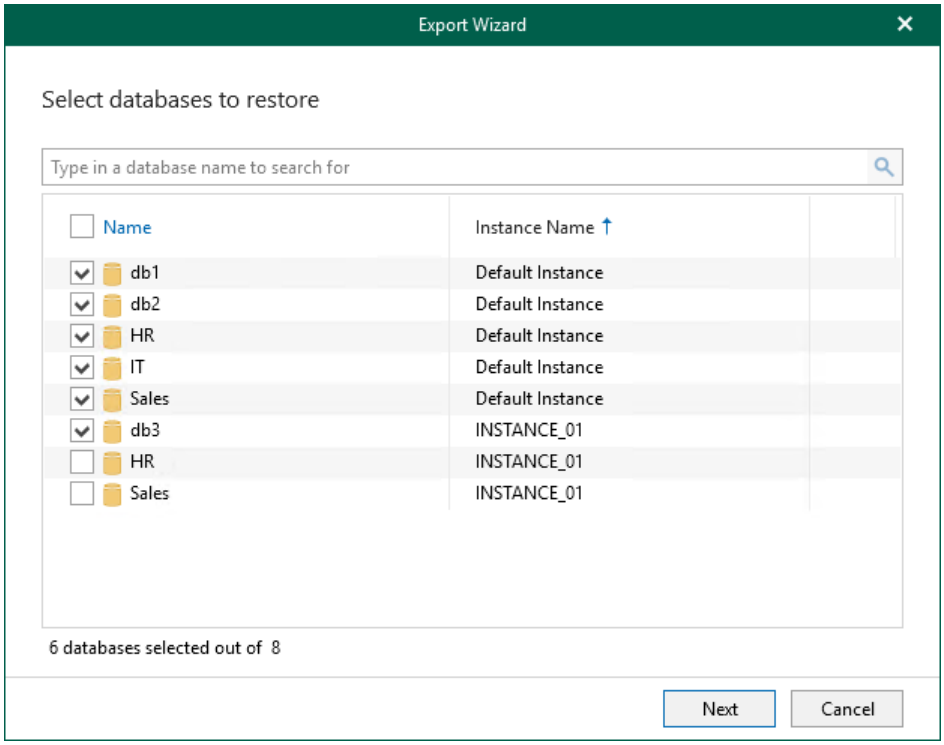
Alternatively, you can right-click an instance or the server and select **Export files** > **Export point-in-time state to Desktop\<db_name>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



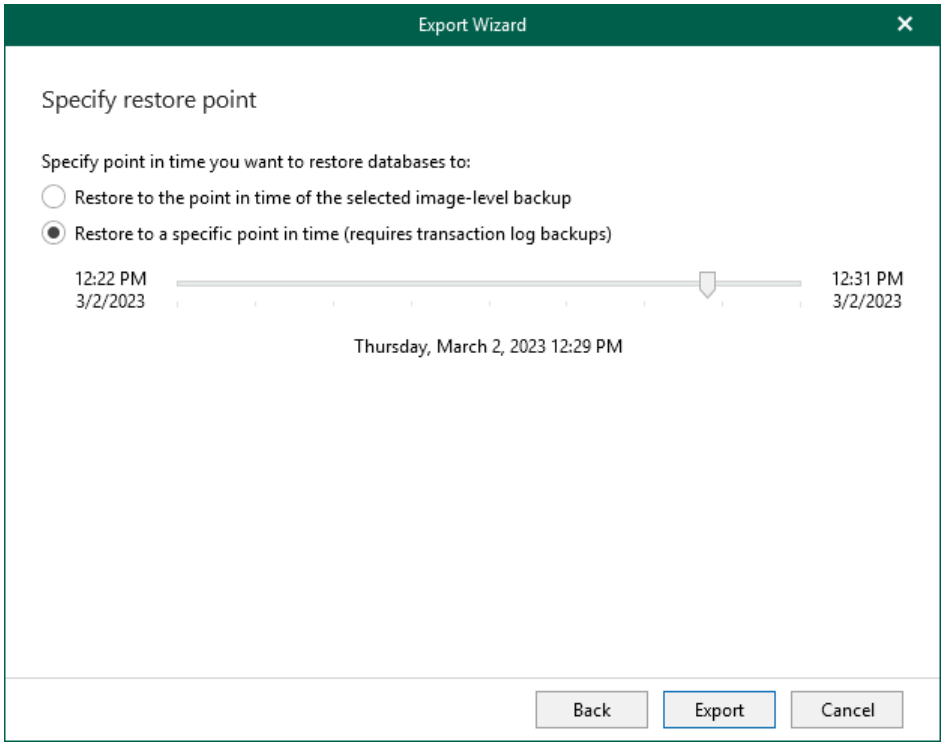
Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.



Exporting to Different Location

To export multiple Microsoft SQL Server databases to a custom location, use the **Export** wizard.

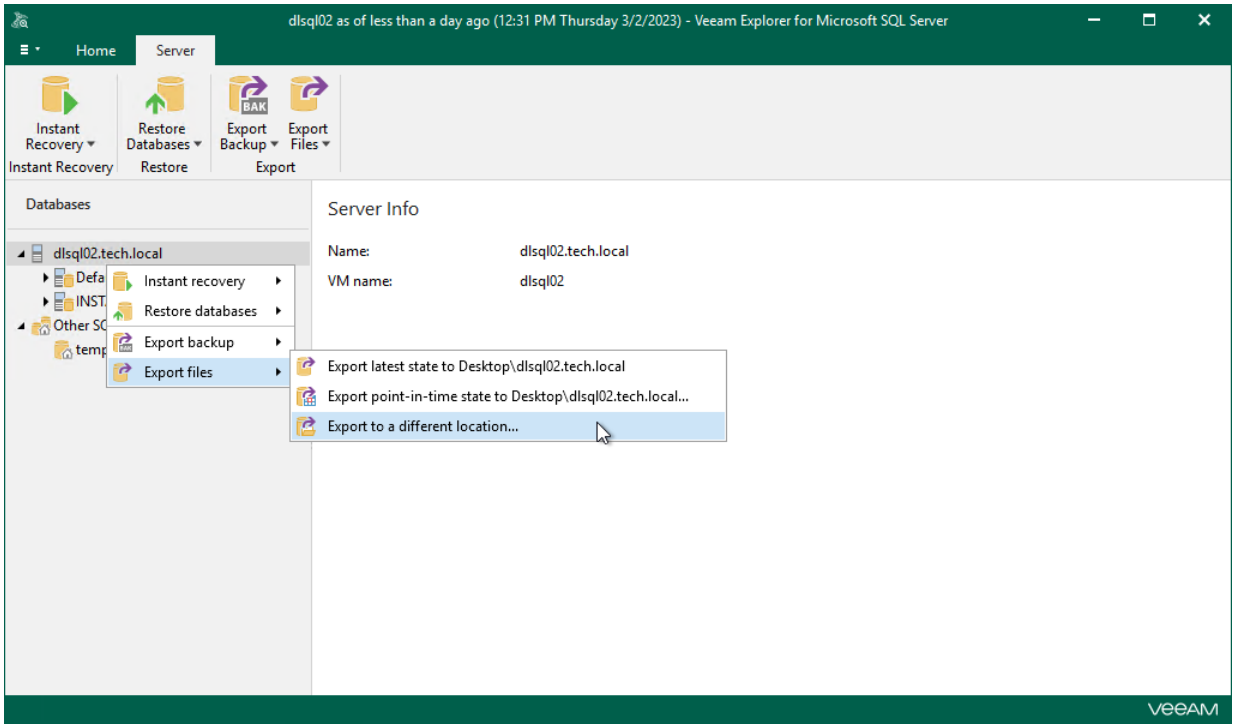
1. Launch the Export wizard.
2. Select databases you want to export.
3. Specify a restore point.
4. Specify database files location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server..
2. On the **Instance** (or **Server**) tab, select **Export Files** > **Export to a different location**.

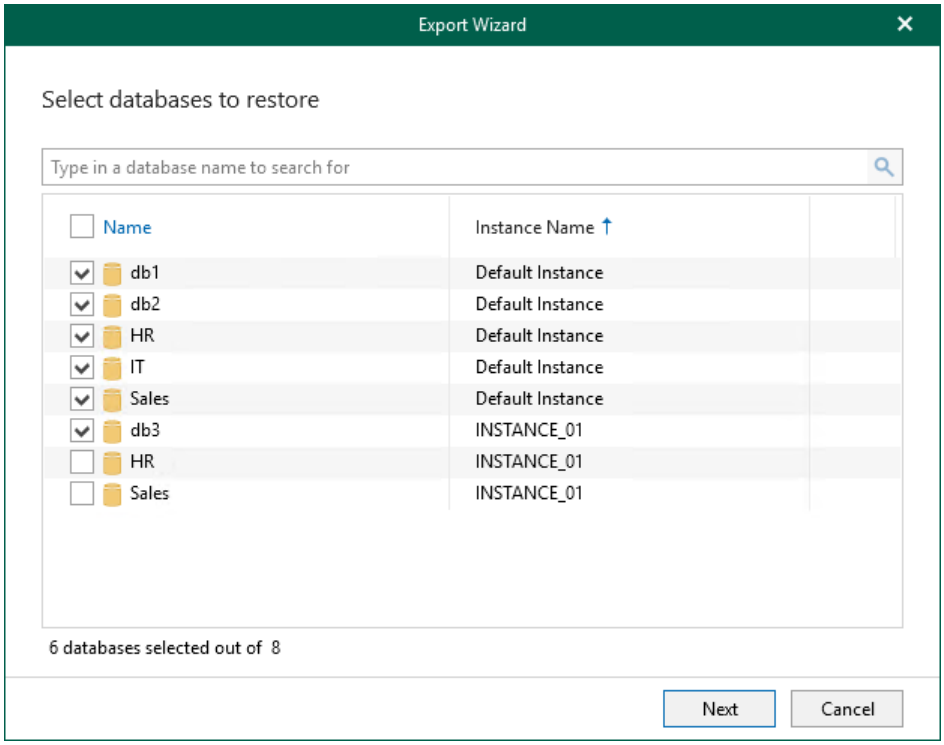
Alternatively, you can right-click an instance or the server and select **Export files** > **Export to a different location**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



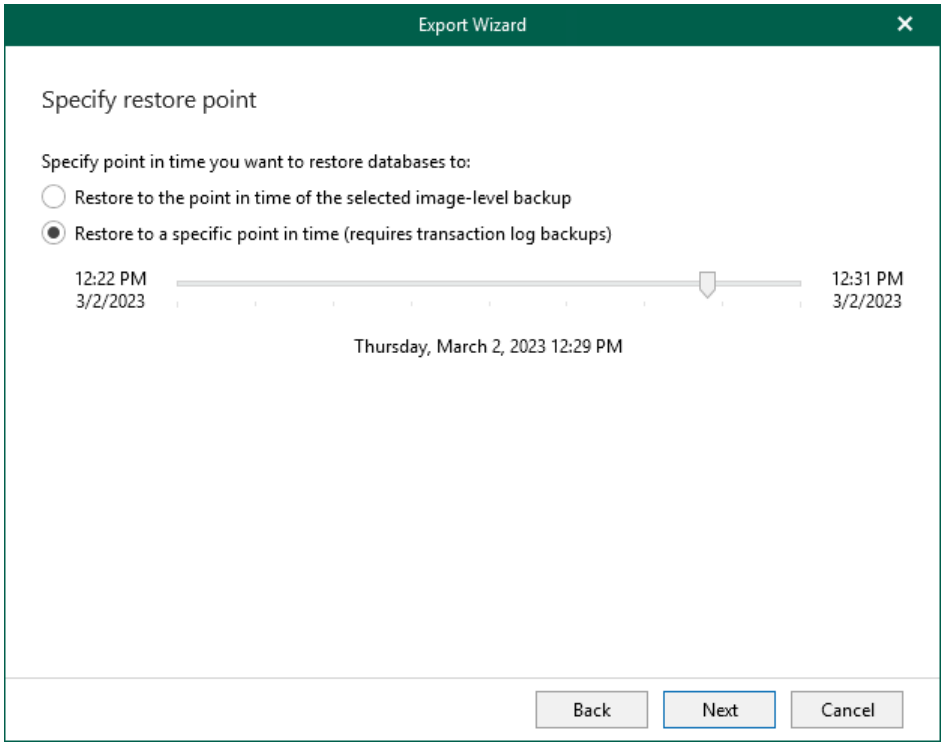
Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

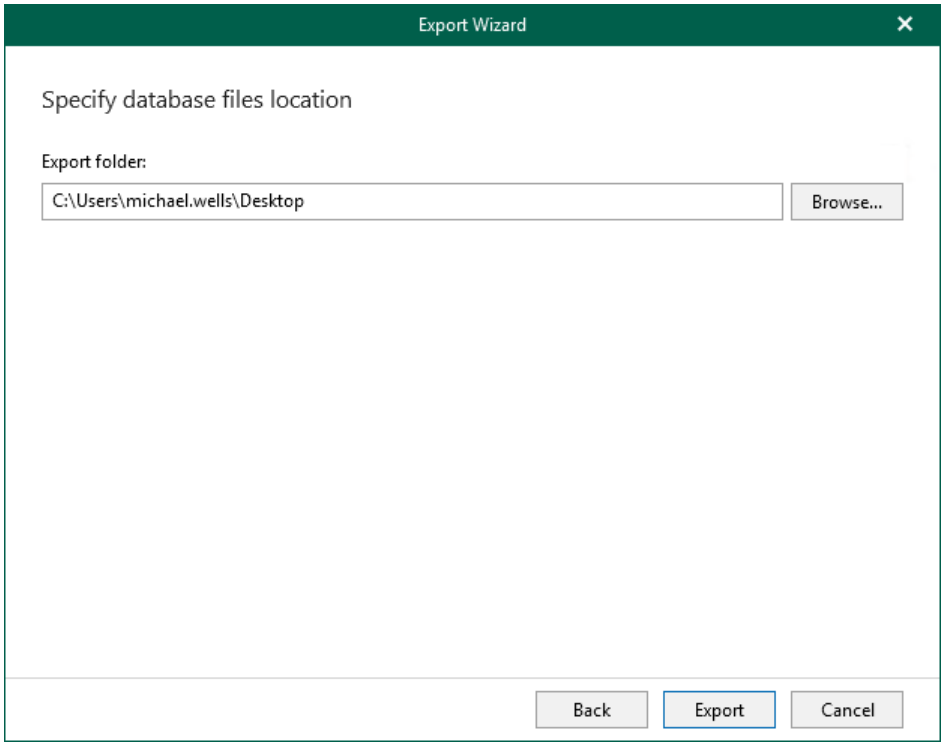
  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.



Step 4. Specify Database Files Location

At this step of the wizard, specify a path to the directory where you want to export database files.



Exporting as BAK

This section explains how to use Veeam Explorer for Microsoft SQL Server to export database files in the BAK file format.

> **IMPORTANT**
>
> To export database files as BAK, make sure to configure a staging SQL server, as described in Configuring Staging SQL Server.

Exporting Single Database

You can export a single Microsoft SQL Server database by following one of these scenarios:

- Exporting Latest State
- Exporting Point-in-Time State
- Exporting to Different Location

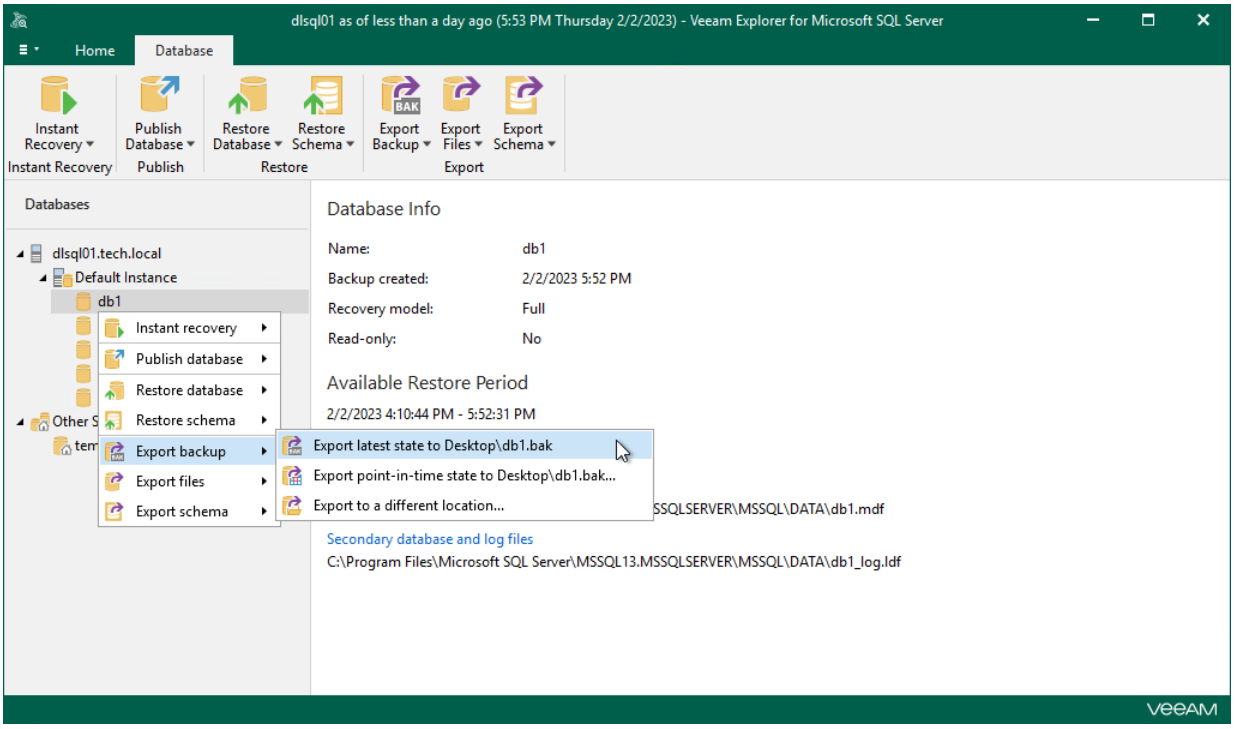
Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Backup** > **Export latest state to Desktop\<db_name>.bak**.

Alternatively, you can right-click a database and select **Export backup** > **Export latest state to Desktop\<db_name>.bak**.

> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export latest state to Desktop\<db_name>.bak**.
> - If you select any other restore point, the option name is displayed as **Export state of <point_in_time> to Desktop\<db_name>.bak**.



Exporting Point-in-Time State

To export data as of a point-in-time state, do the following:

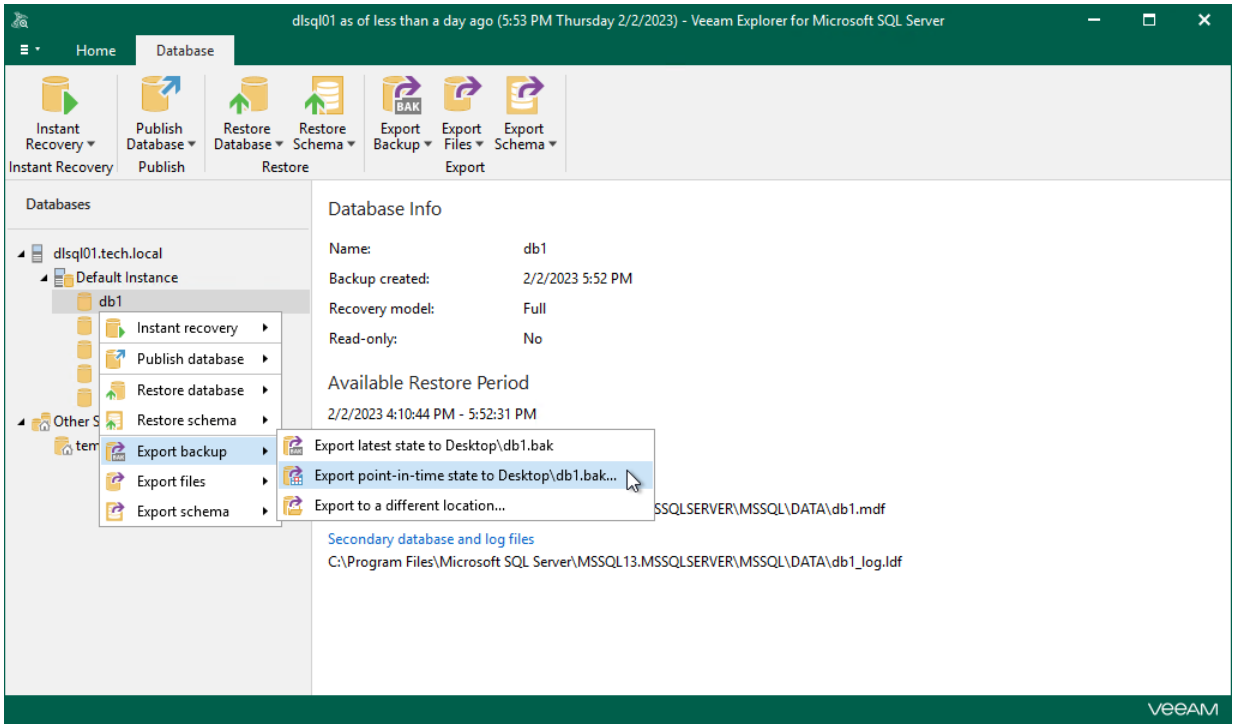
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Backup** > **Export point-in-time state to Desktop\<db_name>.bak**.

Alternatively, you can right-click a database and select **Export backup** > **Export point-in-time state to Desktop\<db_name>**.



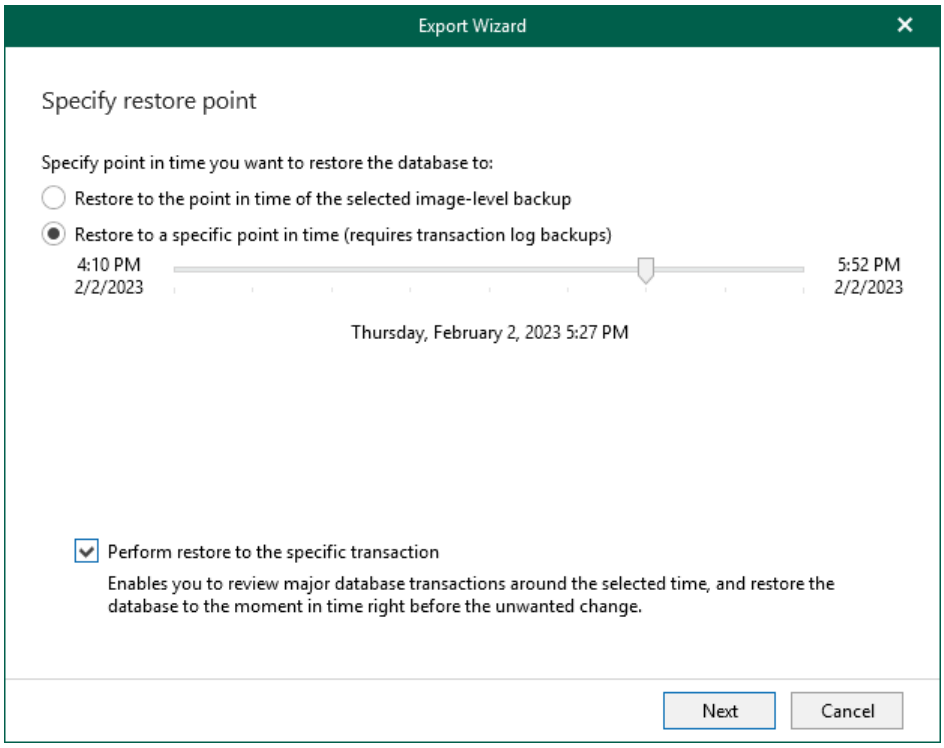
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load data as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load data as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load data exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

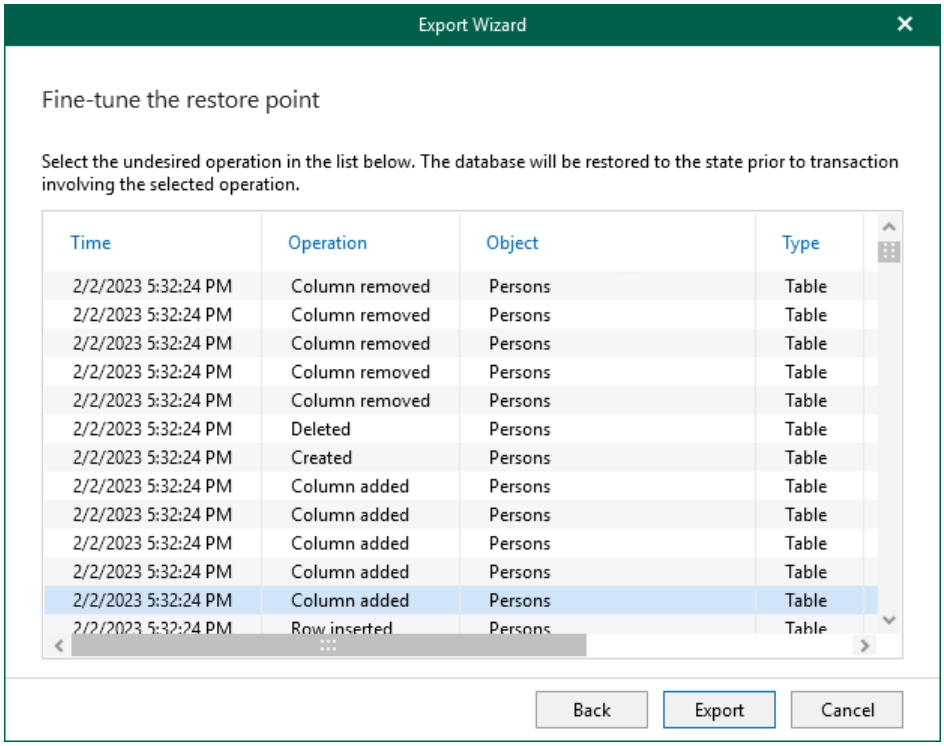


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database and click **Export**.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Exporting to Different Location

To export a single SQL database to a custom location, use the **Export** wizard.

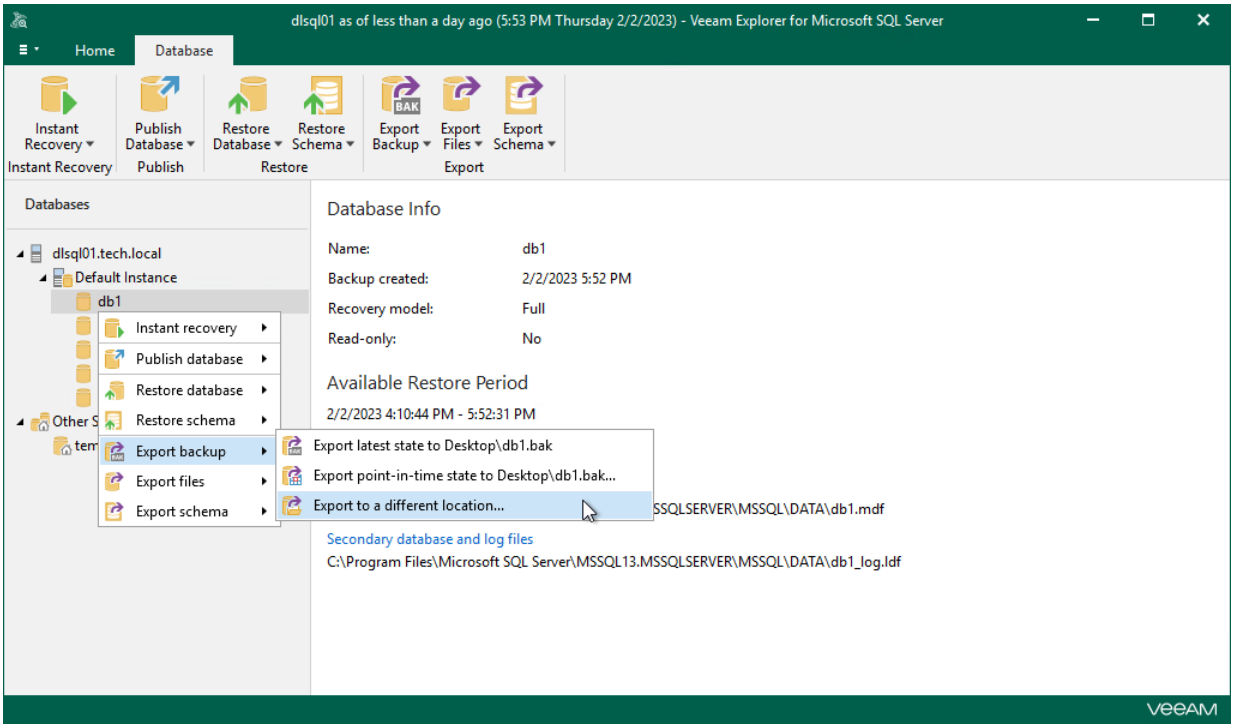
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the database export location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Backup** > **Export to a different location**.

Alternatively, you can right-click a database and select **Export backup** > **Export to a different location**.



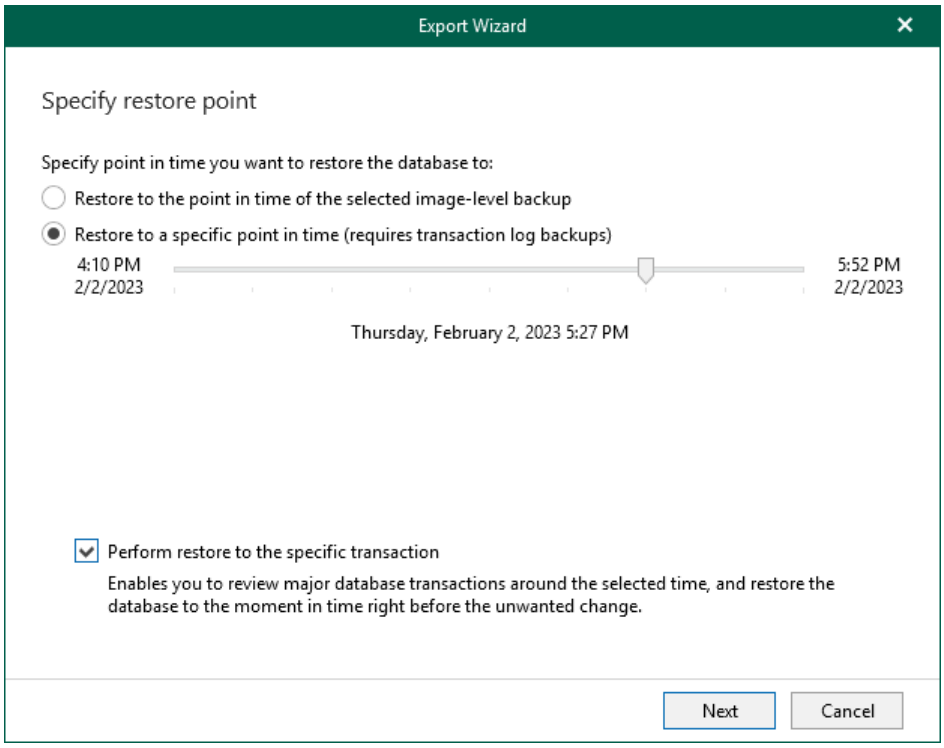
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load data as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load data as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load data exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

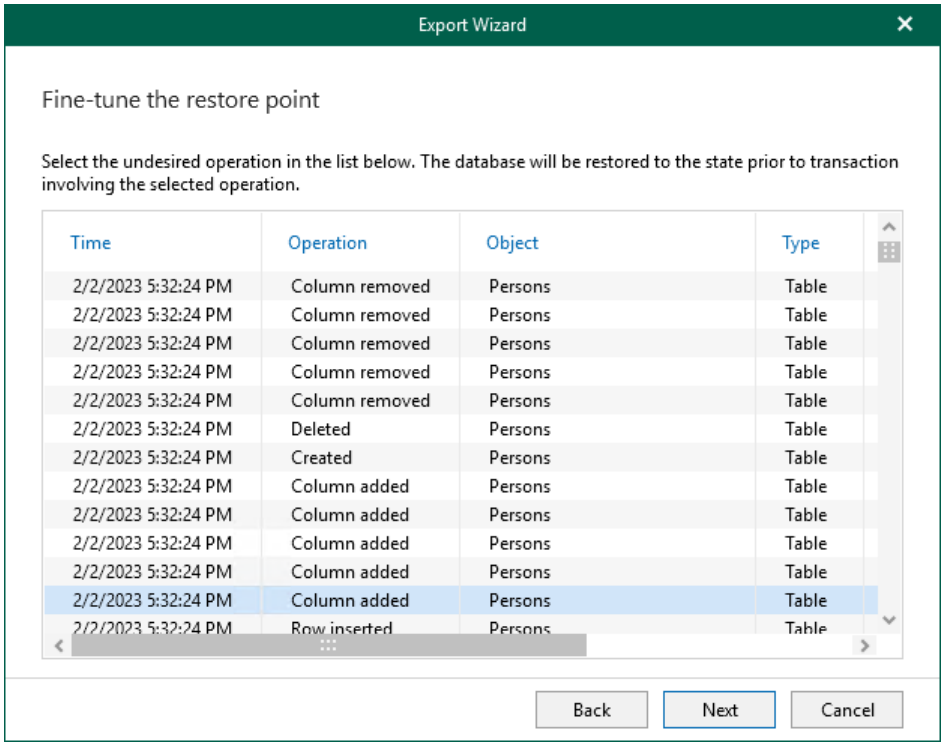


Step 3. Fine-Tune Restore Point

To fine-tune the restore point, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.

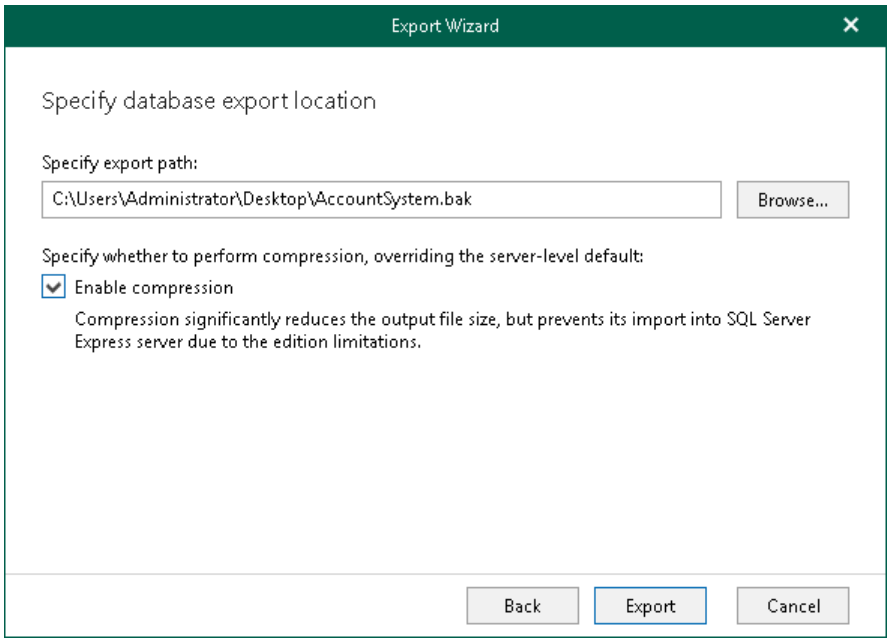


Step 4. Specify Database Export Location

At this step of the wizard, specify the path to the destination directory.

You can select **Enable compression** check box to reduce the output file size.

> **NOTE**
>
> Compression is unavailable if the staging SQL server runs Microsoft SQL Server 2005 or any Express Edition of Microsoft SQL Server.



Exporting Multiple Databases

You can export multiple Microsoft SQL Server database by following one of these scenarios:

- Exporting Latest State
- Exporting Point-in-Time State
- Exporting to Different Location

Exporting Latest State

To export data as of a point-in-time state, use the **Export** wizard.

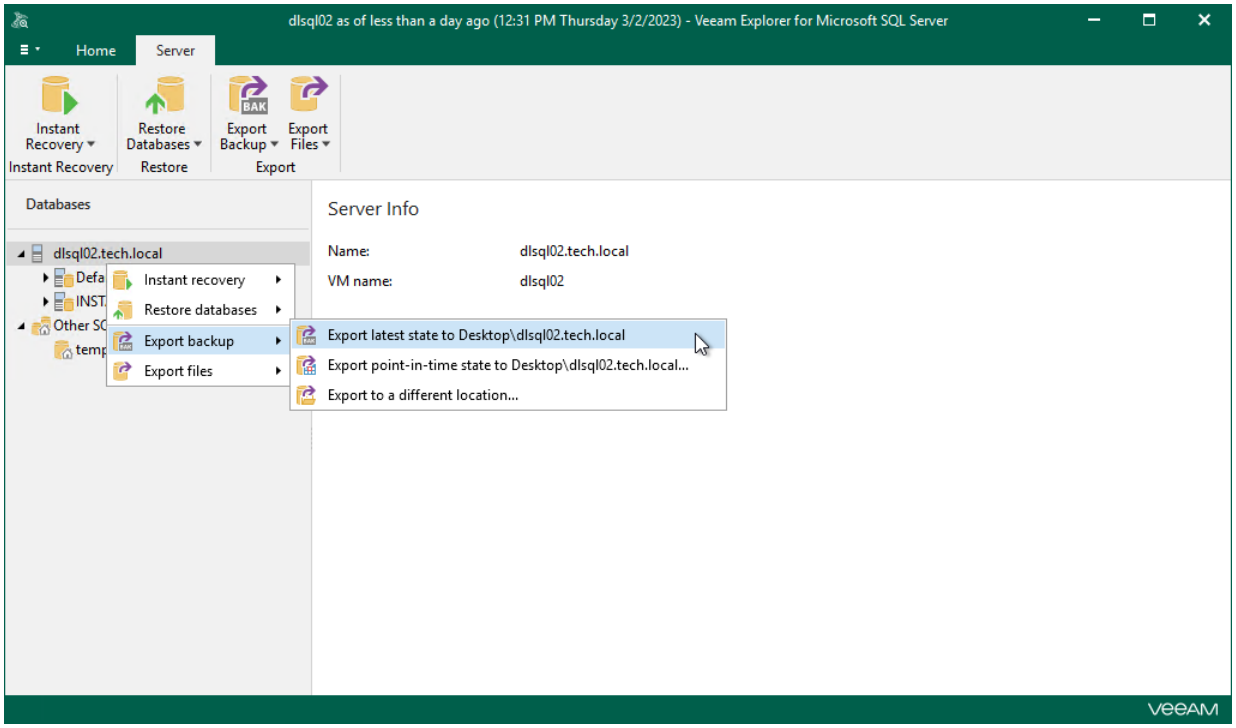
1. Launch the Export wizard.
2. Select databases you want to export.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Export Backup** > **Export latest state to Desktop\<db_name>**.

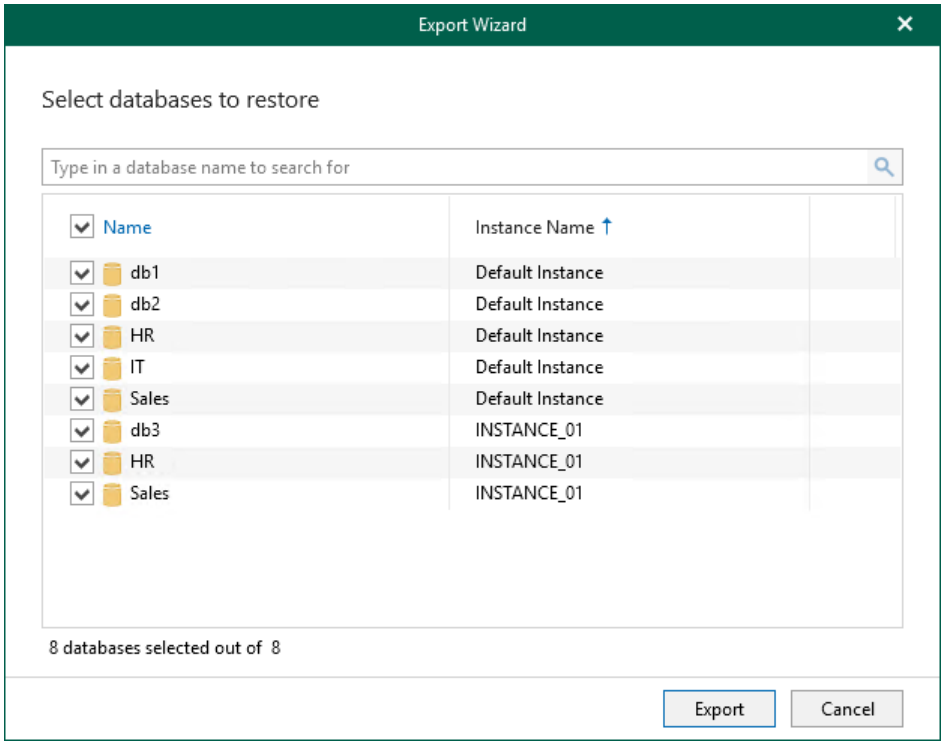
Alternatively, you can right-click an instance or the server and select **Export backup** > **Export latest state to Desktop\<db_name>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



Exporting Point-in-Time State

To export data as of a point-in-time state, use the **Export** wizard.

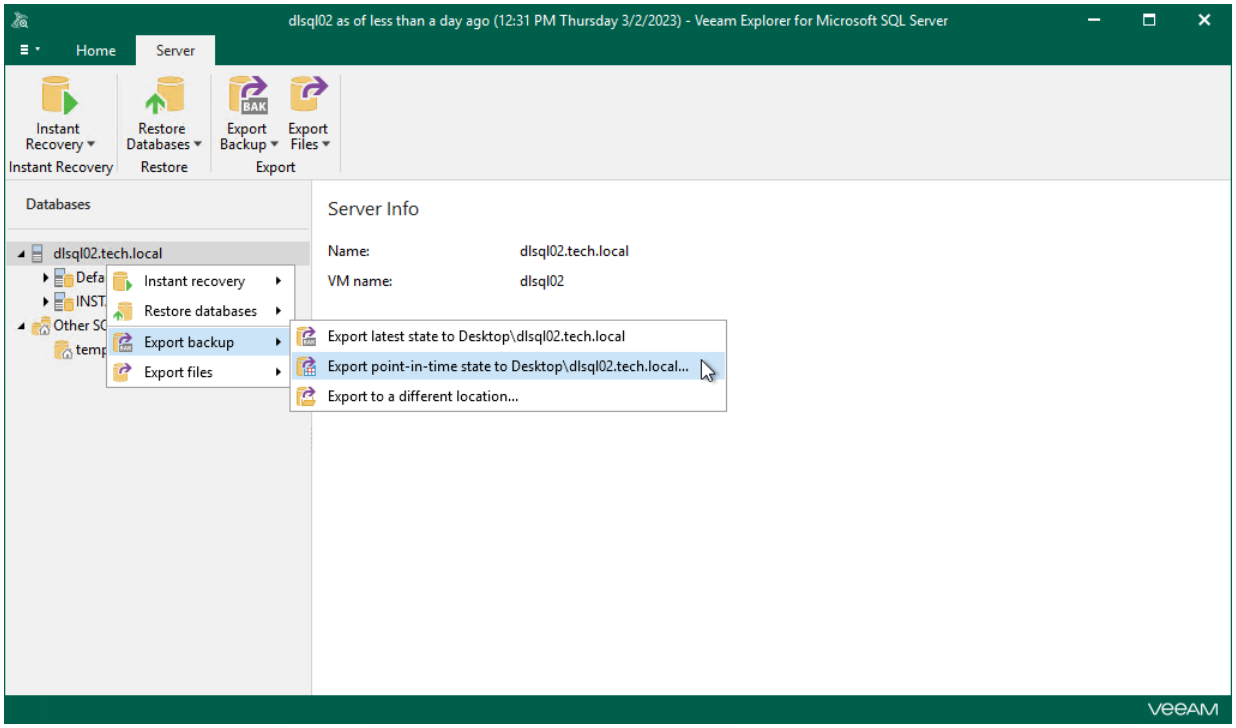
1. Launch the Export wizard.
2. Select databases you want to export.
3. Specify a restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Export Backup** > **Export point-in-time state to Desktop\<db_name>**.

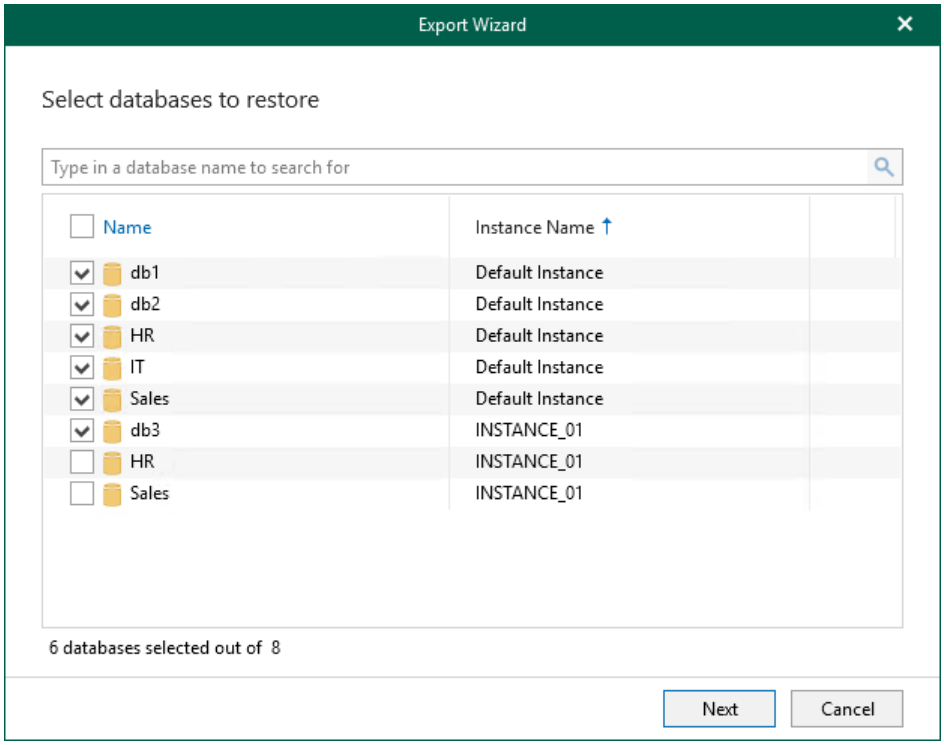
Alternatively, you can right-click an instance or the server and select **Export backup** > **Export point-in-time state to Desktop\<db_name>**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



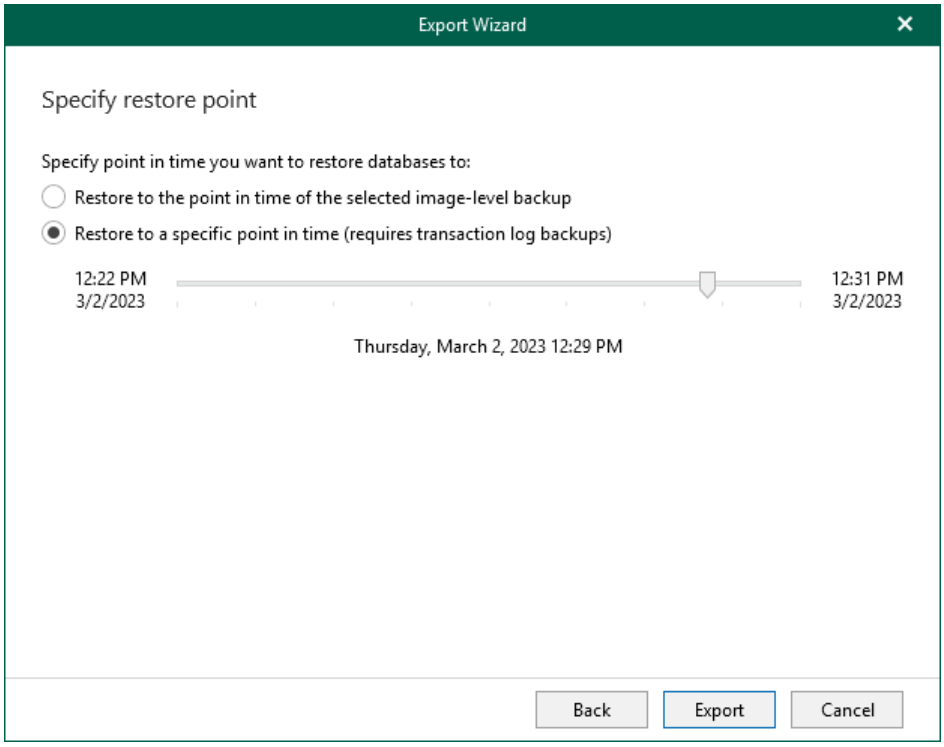
Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.



Exporting to Different Location

To export multiple Microsoft SQL Server databases as BAK to a custom location, use the **Export** wizard.

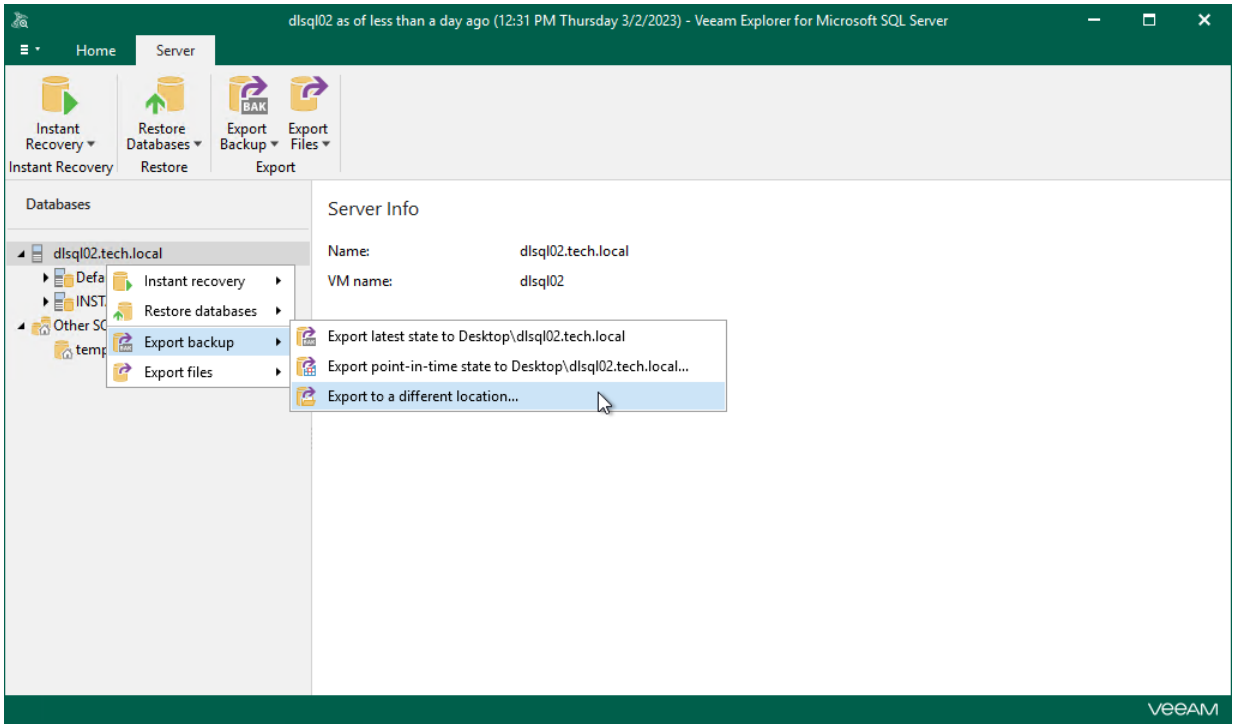
1. Launch the Export wizard.
2. Select databases you want to export.
3. Specify a restore point.
4. Specify the database export location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select an instance or the server.
2. On the **Instance** (or **Server**) tab, select **Export Backup** > **Export to a different location**.

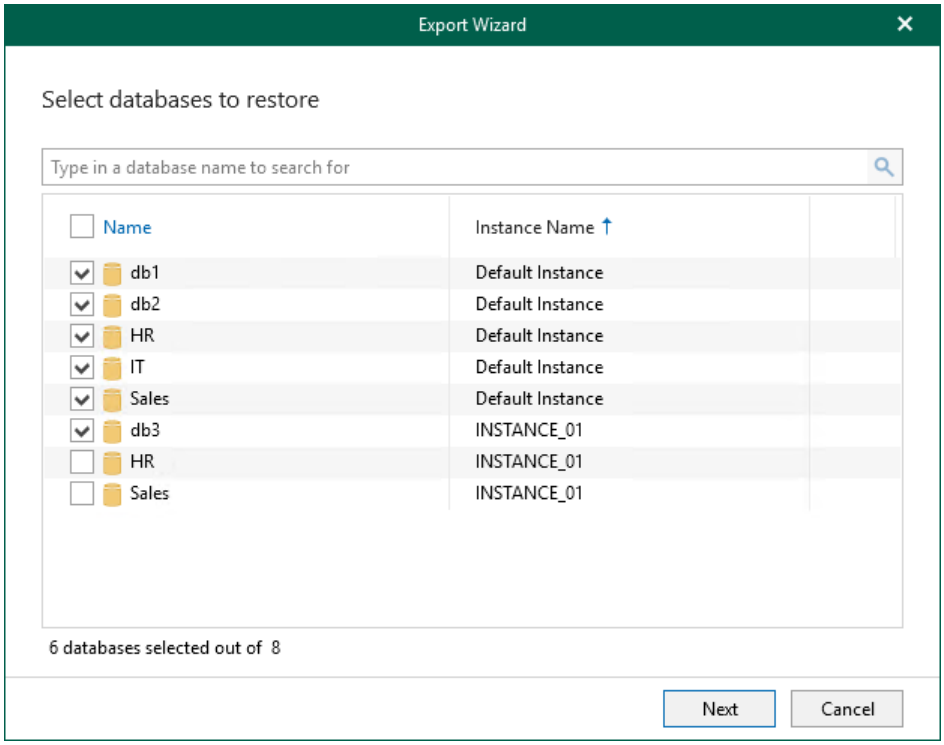
Alternatively, you can right-click an instance or the server and select **Export backup** > **Export to a different location**.



Step 2. Select Databases

At this step of the wizard, select the databases that you want to export.

To quickly find the necessary databases, use the **Search** field or sort the databases by name. If the databases belong to multiple instances, you can also sort the databases by instance name.



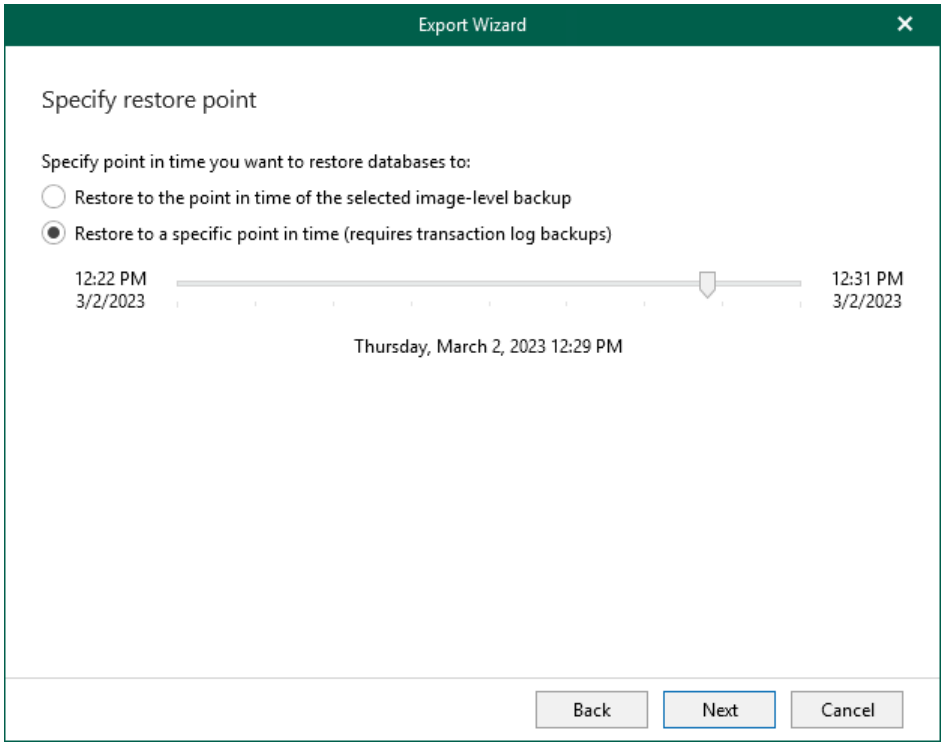
Step 3. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per moment when the current restore point of a VM was created by the backup or replication job.
- Select the **Restore to a specific point in time** option to load database files as per specified point in time.

  Use the slider control to choose a point you need.

> **NOTE**
>
> The **Perform restore to the specific transaction** option is unavailable when exporting multiple databases.

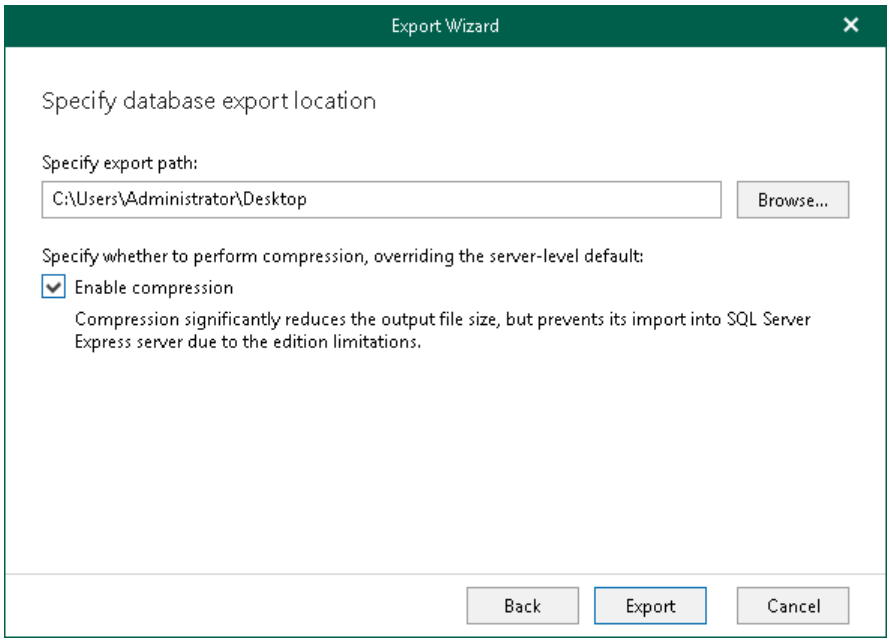


Step 4. Specify Database Export Location

At this step of the wizard, specify the path to the destination directory.

You can select **Enable compression** check box to reduce the file size.

> **NOTE**
>
> Compression is unavailable if the staging SQL server runs Microsoft SQL Server 2005 or any Express Edition of Microsoft SQL Server.



Exporting Database Schema and Data

This section explains how to use Veeam Explorer for Microsoft SQL Server to export your database schema and data.

> **NOTE**
>
> Export of schema and data for multiple databases is not supported.

Using 1-Click Export

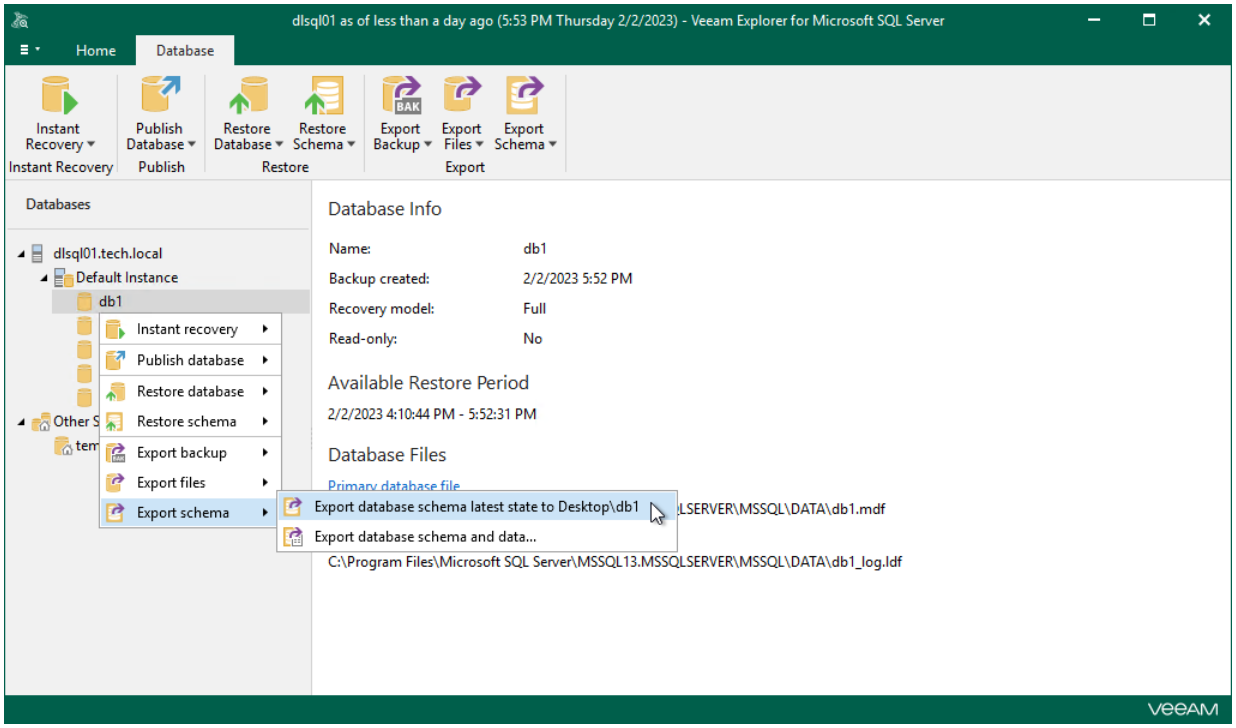
Veeam Explorer for Microsoft SQL Server allows you to quickly export database schema state as of the current restore point

To export database schema to the default location, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Schema** > **Export database schema latest state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export schema** > **Export database schema latest state to Desktop\<db_name>**.

> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export database schema latest state to Desktop\<db_name>**.
> - If you select any other restore point, the option name is displayed as **Export database schema state of <point_in_time> to Desktop\<db_name>**.



Exporting to Custom Location

To export database schema and data, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Select database objects.
5. Specify names for objects.
6. Specify the destination folder.

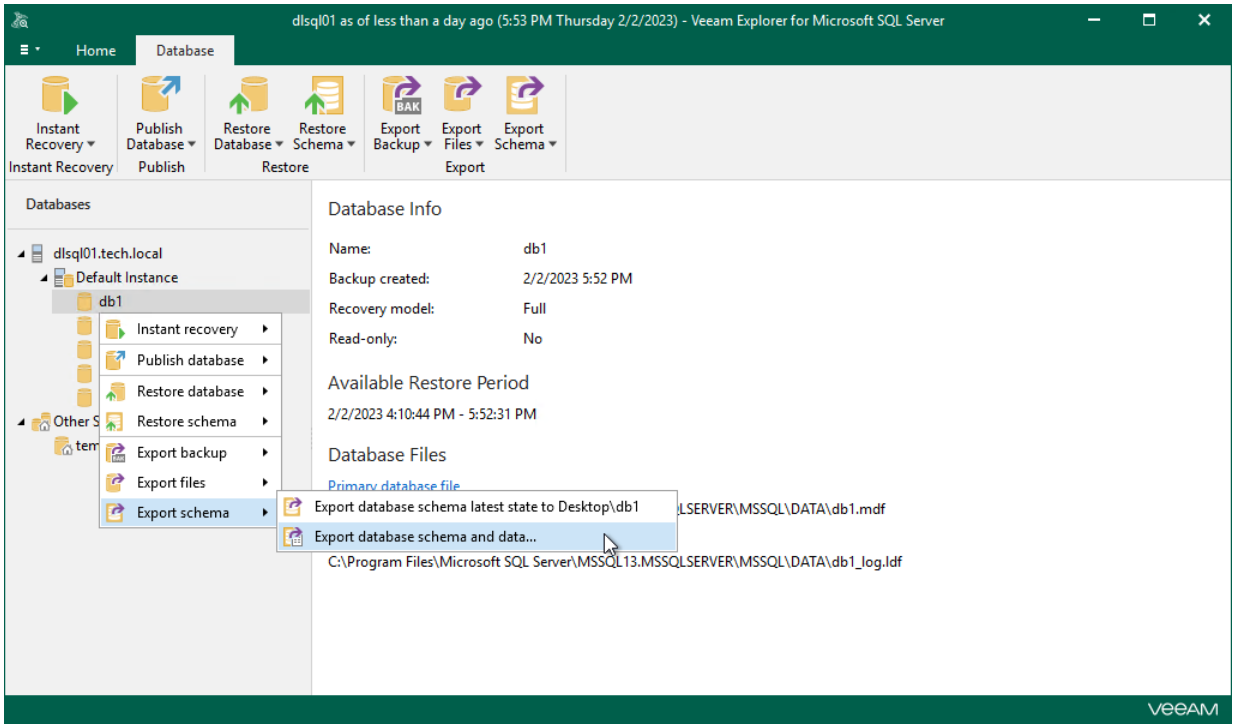
Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** (or **Server/Instance**) tab, select **Export Schema** > **Export database schema and data**.

Alternatively, you can right-click a database and select **Export schema** > **Export database schema and data**.

> **TIP**
>
> To import data tables, use the standard SQL server **bcp.exe** utility. For more information, see this Microsoft article.



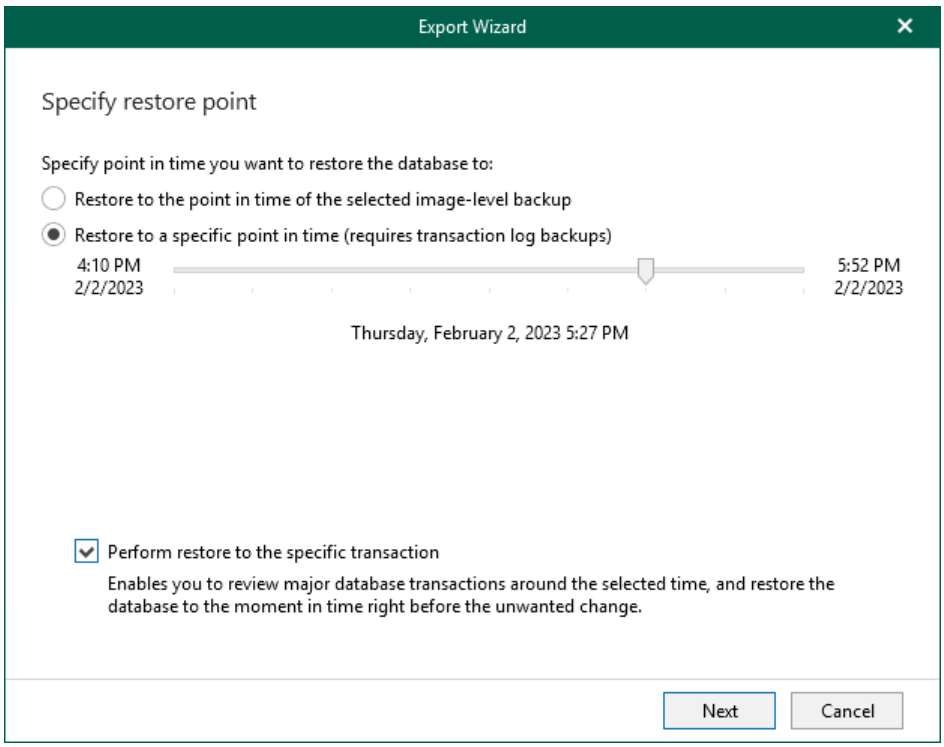
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging SQL server. For more information, see Configuring Staging SQL Server.

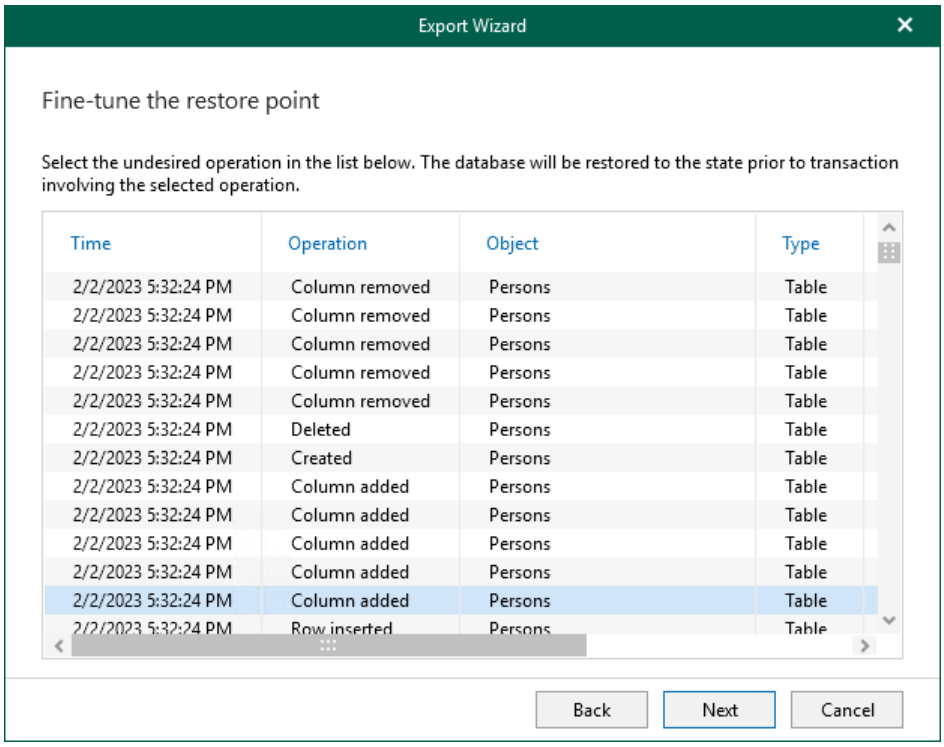


Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export your database.

Veeam Explorer for Microsoft SQL Server database operations are listed in the SQL Server Database Operation Selection section.

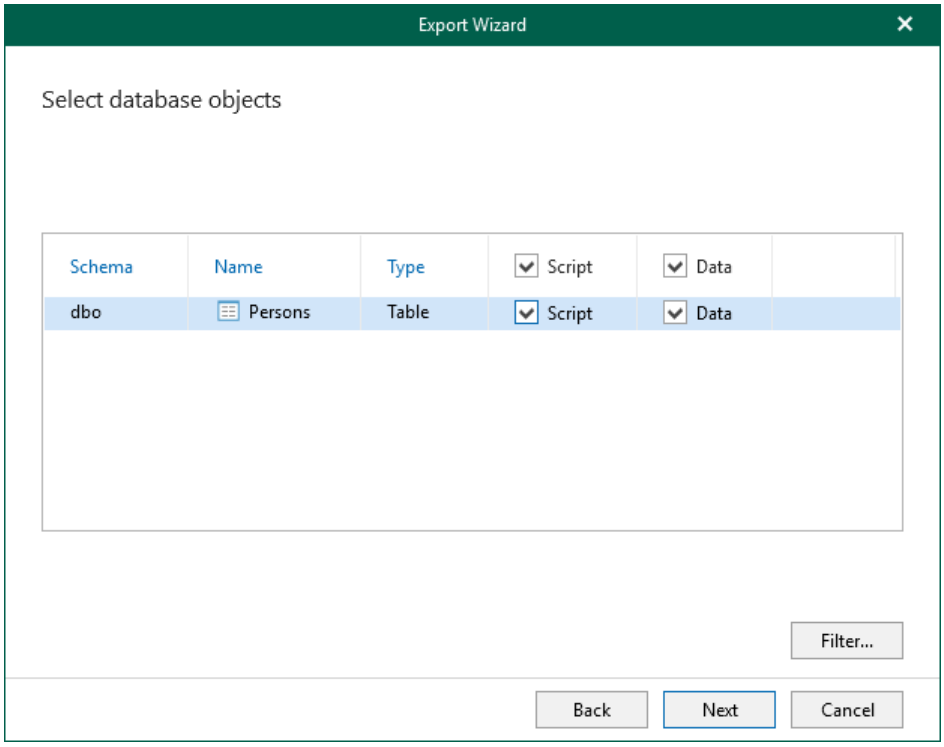
> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Select Database Objects

At this step of the wizard, select database objects to restore.

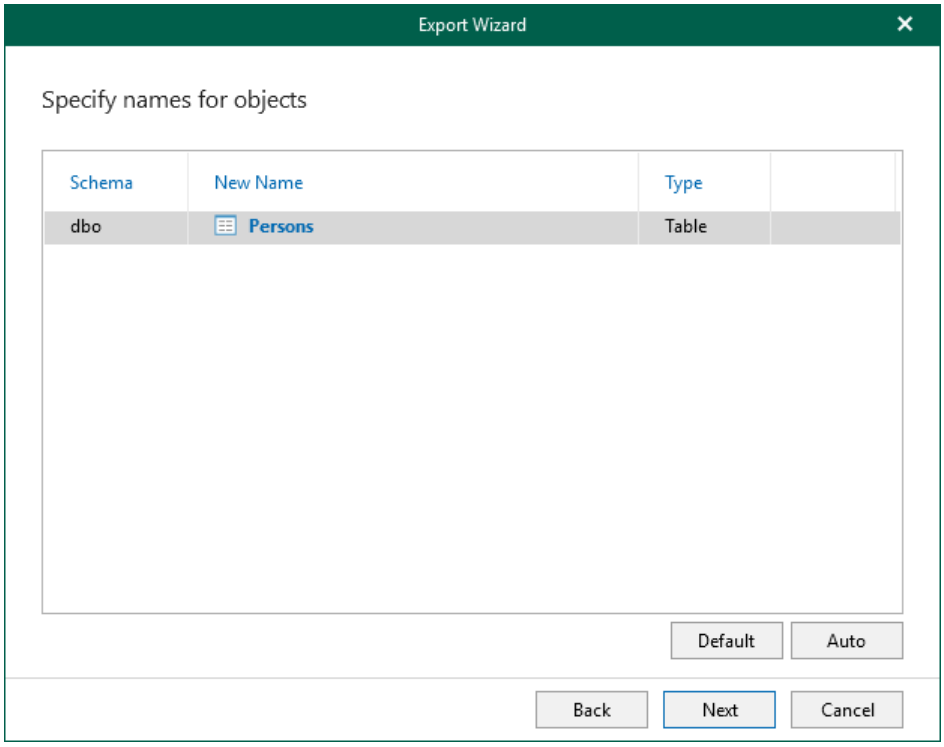
To display only specific objects, click **Filter** and select an object type you want to be shown in the list.



Step 5. Specify Names for Objects

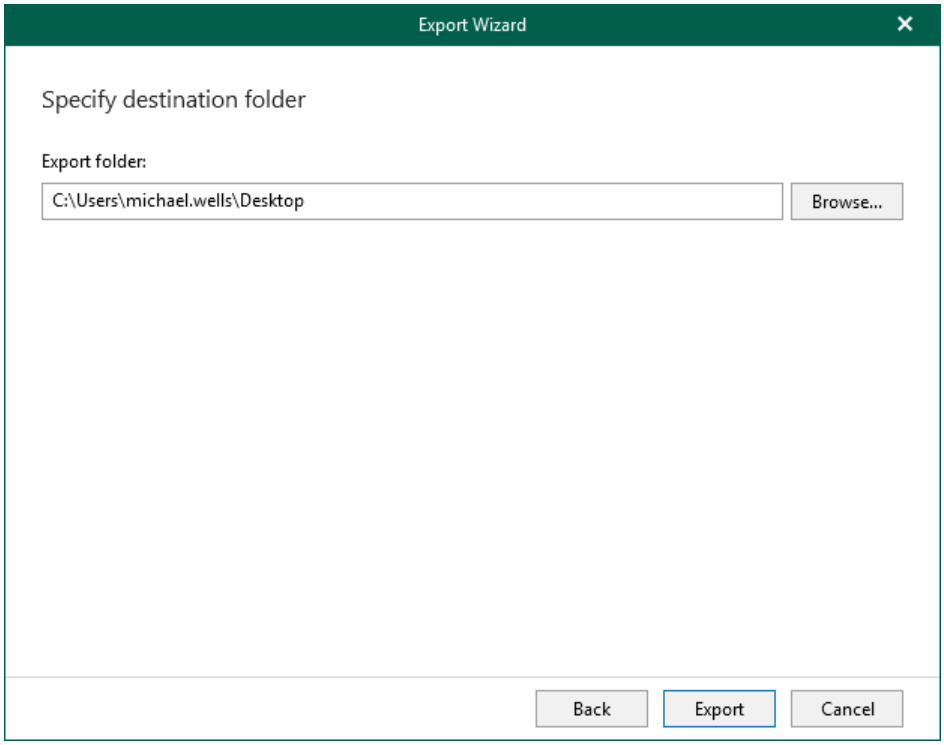
At this step of the wizard, specify the name to be assigned to the object.

- To specify a new name, select a database and provide a new name.
- To assign a default name with the *_new* suffix, click **Auto**.



Step 6. Specify Destination Folder

Specify the destination folder to which you want to export selected database schema objects.



SQL Server Database Operations

The following table lists SQL Server database operations and their display names that appear in the fine-tune dialog.

Entity	Operation	Display Format	Constraints
Table	CREATE	<date_time> Created[/Modified] <table_name> Table <table ID> <initiator>	—
	DROP	<date_time> Deleted <table_name> Table <table ID> <initiator>	—
	ALTER	<date_time> Column added <table_name> Table <table ID> <initiator>	—
	INSERT INTO	<date_time> Inserted row <table_name>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	DELETE FROM	<date_time> Deleted row <table_name>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	UPDATE	<date_time> Modified <table_name>>[/table_ID] Table <initiator>	Table name will not be displayed for deleted table, only table ID will be shown.
	TRUNCATE	<date_time> Truncated Table <initiator>	Table name and ID will not be displayed for deleted table.
	BULK INSERT	<date_time> Inserted row <table_name>[/table_ID] Table <initiator>	—
View	CREATE	<date_time> Created <view_name> View <initiator>	—
	DROP	<date_time> Deleted <view_name> Table <initiator>	—

Entity	Operation	Display Format	Constraints
	ALTER	<date_time> Modified <view_name> View <initiator>	—
Index	CREATE	<date_time> Created <index_name> Index <initiator>	—
	DROP	<date_time> Deleted <index_name> Index <initiator>	—
	ALTER	<date_time> Modified <index_name> Index <initiator>	—
Procedure	CREATE	<date_time> Created <procedure_name> Procedure <initiator>	—
	DROP	<date_time> Deleted <procedure_name> Table <initiator>	—
	ALTER	<date_time> Modified <procedure_name> Procedure <initiator>	—
Function	CREATE	<date_time> Created <function_name> Function <initiator>	—
	DROP	<date_time> Deleted <function_name> Table <initiator>	—
	ALTER	<date_time> Modified <function_name> Function <initiator>	—
Schema	CREATE	<date_time> Created <schema_name> Schema <initiator>	—
	DROP	<date_time> Deleted <schema_name> Schema <initiator>	—
	ALTER	<date_time> Modified <schema_name> Schema <initiator>	Schema cannot be detected.
User	CREATE	<date_time> Created <user_name> User <initiator>	—

Entity	Operation	Display Format	Constraints
	DROP	<date_time> Deleted <user_name> User <initiator>	—
	ALTER	<date_time> Modified <user_name> User <initiator>	—
Trigger	CREATE	<date_time> Created <trigger_name> Trigger <initiator>	—
	DROP	<date_time> Deleted <trigger_name> Trigger <initiator>	—
	ALTER	<date_time> Modified <trigger_name> Trigger <initiator>	—

Veeam Explorer for Oracle

Veeam Explorer for Oracle allows you to restore and export Oracle databases and Data Guard from backups created by Veeam Backup & Replication or Veeam Plug-in for Oracle RMAN.

Planning and Preparation

Before you start using Veeam Explorer for Oracle, make sure your backup infrastructure meets the following requirements and limitations.

System Requirements

This section lists system requirements for Veeam Explorer for Oracle.

Component	Requirement
Oracle on Windows OS / Oracle on Linux OS	For more information on supported versions of Oracle Database, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

Ports

The following tables list network ports that must be opened to manage inbound and outbound traffic.

Backup

Oracle on Windows

From	To	Protocol	Port	Notes
Backup server	Source machine with Oracle	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on the source machine.
		TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range used by the runtime coordination process that is deployed on the source machine for application-aware processing.[1] For more information, see this Microsoft article.
		TCP	6167	**For archived logs shipping** Port used by the runtime coordination process on the source machine from which archived logs are collected.
Source machine with Oracle	Backup server	TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range used by the runtime coordination process that is deployed on the source machine for application-aware processing.[1]
	Log shipping server, backup repository	TCP	2500 to 3300	**For archived logs shipping** Default range of ports used for data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Oracle on Linux

From	To	Protocol	Port	Notes
Backup server	Source machine with Oracle	TCP	6162	Default port used by Linux Management Agent.
		TCP	22	Default SSH port used as a control channel (without Linux Management Agent).
		TCP	2500 to 3300	**For archived logs shipping** Default range of ports used for managing data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.
		TCP	6167	**For archived logs shipping** Port used by the runtime process on the source machine from which archived logs are collected.
Source machine with Oracle	Log shipping server, backup repository	TCP	2500 to 3300	**For archived logs shipping** Default range of ports used for managing data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.

Restore

From	To	Protocol	Port	Notes
Backup server, Veeam Backup & Replication console, mount server associated with the backup repository (only for Instant Recovery or restore from Enterprise Manager)	Target Windows machine with Oracle	TCP	49152 to 65535	Recommended dynamic RPC port range for Microsoft Windows 2008 or later. For more information, see this Microsoft article.
		TCP	1025 to 1075	Default range of ports for the runtime component installed on the target machine to support restore operations. Port is opened only during application item restore. **Note:** You must manually open these ports for `Veeam.Oracle.Service.exe` in Microsoft Windows Firewall.
		TCP	6160, 11731	Ports used by the Veeam Installer Service for connections to the target Windows machine with Oracle.
	Target Linux machine with Oracle	TCP	22	Default SSH port used as a control channel.
Backup repository	Target Linux machine with Oracle	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) machine or another Linux machine with Oracle.
Target Linux machine with Oracle	Backup repository	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) machine or another Linux machine with Oracle.
Target Windows machine with Oracle, staging server	Mount server associated with the backup repository	TCP	3260 to 3270	Range of ports opened by Veeam Backup & Replication to manage iSCSI traffic during restore to the target machine. This port range is opened only during application item restore.

Permissions

The following table lists the required permissions for user accounts to restore Oracle data.

Operation	Required Roles and Permissions
Veeam Explorer for Oracle launch	The account used to run Veeam Explorer for Oracle must be a member of the local *Administrators* or *Users* group.
Restore / Accessing Staging Server	To restore data, make sure to configure user accounts as follows: • When restoring to a Windows-based machine, the account must be a member of the local *Administrators* group on the target machine. In addition, if *ASM* is used, then such an account must be a member of the *ORA_ASMADMIN* group (for Oracle 12 and higher). • When restoring to a Linux-based machine, the account must be a Linux user with *root* permissions on the target machine and have membership in the following groups: *OSASM* [if *ASM* is used] (typically *asmadmin*), *OSDBA* (typically dba), *Oracle Inventory group* (typically *oinstall*). Keep in mind that for restore from RMAN backups, the *root* privileges for the user account are not required.
Export as database files	The account under which Veeam Explorer for Oracle runs must be a member of the local *Administrators* group.

Required Backup Job Settings

When you create a backup job, make sure to enable the **application-aware image processing** option, as described in the Specify Guest Processing Settings section of the Veeam Backup & Replication user guide.

If your backups were created without application-aware image processing, you can still explore them, as described in Exploring non-Application Enabled Backups.

The application-specific information is retrieved according to the following:

- If the **application-aware image processing** option is enabled, Veeam Explorer for Oracle obtains application-specific Oracle database information from the Oracle VM backup metadata located in the backup server configuration database.
- If the **application-aware image processing** option is disabled, Veeam Explorer for Oracle requires a staging Oracle server to mount a selected image-level Oracle VM backup (with databases and redo logs) and collect required information using the guest scan and Oracle infrastructure analysis.

> **IMPORTANT**
>
> Make sure to have your database in the **OPEN** state during backup. Otherwise, the following warning message will appear in the backup job session: *Oracle database instance state is not valid for property collection*. Whether the backup job completes or fails depends on the selected backup job settings. For more information, see the Application-Aware Processing section of the Veeam Backup & Replication User Guide.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Oracle.

General

- When Veeam Explorer for Oracle is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.
- [Restore to Linux server] You can restore data over SSH only, restore using Linux Management Agent is not supported.
- [Restore to Linux server] Restore with Veeam Explorer for Oracle is not supported if the SQL*Plus environment on the target Oracle server is configured to use `glogin.sql` or `login.sql` profile files. For details, see the Configuring SQL*Plus section of the SQL*Plus User's Guide.
- [Restore to Linux server] Restore of databases that resided in an encrypted file system on the original server is not supported. In particular, encrypted LVM volumes are not supported.
- [For refreshable PDB] Data restore, data publishing and instant recovery are not supported for refreshable PDBs.
- [Restore from VM backups] Mount of Btrfs disks will fail if you want to perform instant recovery, data restore or data publish to the original server. The issue occurs due to restriction for mounting 2 Btrfs disks with identical IDs to the same machine.

  Note that Btrfs volumes on the backed-up Veeam Agent machine must have identifiers in the UUID format in the `fstab` configuration file.
- Mount operations with FUSE are not supported on kernel versions 4.0.0 – 4.1.33. Make sure to upgrade the kernel to version 4.1.37 or later.
- [For restore to Oracle ASM] You cannot specify paths and file names for restored database files. During restore, Oracle ASM will automatically create and name the necessary files in the specified disk group using the OMF (Oracle Managed Files) feature.

Restore from Image-Level Backups

- Veeam Explorer for Oracle does not support restore using PowerShell Direct, VIX API or vSphere Automation API.
- 1-Click restore to the original location from storage snapshots is not supported.
- A point in time restore is not supported for replicas and backups stored in the DR site by backup copy jobs, nor it is supported for backups stored in a cloud repository. Such repositories cannot be used as a destination location for archived logs.
- Restore of databases from the current restore point is only supported for backups created by Veeam backup job, replication job, VeeamZIP and for imported backup and storage snapshots.
- If OS authentication on a target Oracle server is disabled, the restore of databases with enabled ASM will not be possible.
- If OS authentication on a staging Oracle server is disabled, the restore of databases with enabled ASM as of the selected transaction state will not be possible.

- Make sure that both the backed-up Oracle machine and the target server to which you are restoring have the same OS patch version.
- Oracle Automatic Storage Management Filter Driver (Oracle ASMFD) is not supported.

Restore from RMAN Backups

> **IMPORTANT**
>
> Restore from RMAN backups is not possible if OS authentication is disabled on the target Oracle server.

Restore of Oracle Real Application Clusters (RAC)

To restore RAC databases from RMAN backups, make sure you apply the following restore settings. Otherwise, the databases will be restored as standalone databases.

- **Restore to original server**: You must perform the restore with original name and settings.
- **Restore to another server**:
  - You must perform the restore with original name and settings.
  - The Oracle home and Oracle directory structure must remain the same.
  - You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
  - For Oracle ASM, the file system structure of the restored database must remain the same.

Restore of Data Guard Databases

Data restore with Veeam Explorer for Oracle from backups of Data Guard databases created by Veeam Plug-in for Oracle RMAN has experimental support. You can restore Data Guard databases from Veeam Plug-in backups with the following limitations:

- **Restore to original server**
  - You can restore Data Guard primary databases as primary databases only to the original location with the original name and settings.
  - You can restore Data Guard standby databases as standby databases only to the original location with the original name and settings.

    A restore with different settings will fail due to Data Guard limitations.
- **Restore to another server**
  - Make sure that the copy of the original cluster already exists in the duplicated environment.
  - You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
  - You can restore Data Guard primary databases as primary databases only with the original name and settings.

- You can restore Data Guard standby databases as standby databases only to the original location with original name and settings.

  A restore with different settings will fail due to Data Guard limitations.

Restore of Oracle Databases

- When restoring to another server with the original name and settings, consider the following:
  - The Oracle home and Oracle directory structure must remain the same.
  - You must copy the original control file to the target server or recovery catalog of the database which is running in the duplicated cluster. Such a control file must contain information about backups from which the restore is being performed.
  - For Oracle ASM, the file system structure of the restored database must remain the same.
- To restore a database with different name and settings, the database must use SPFILE (server parameter file).

Publishing from Image-Level Backups

- Make sure that the target Oracle server to which you publish your databases is of the same version as the database in the backup.
- If the database that you publish is part of the ASM group, make sure that the target Oracle server also has an ASM group properly configured.

Instant Recovery

- For Oracle Database 12c, instant recovery is supported starting from version 12.2.0.1.0.211019.
- Instant recovery is supported for image-level backups only. You cannot perform instant recovery from RMAN backups.
- Make sure that both the backed-up Oracle machine and the target server to which you are restoring have the same OS patch version.
- Instant recovery of the entire Oracle Data Guard is not supported. However, you can restore individual Data Guard databases.
- Instant recovery of SAP on Oracle is not supported.
- During the instant recovery process, Veeam Explorer for Oracle requires 512 MB of RAM for each database.
- If you add a new pluggable database to the container during an instant recovery process, the instant recovery session fails.

Launching Application and Exploring Backups

To open Veeam Explorer for Oracle and load backups, you can use any of the following methods:

- The **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start** and click **Veeam Explorer for Oracle**.

If you open Veeam Explorer for Oracle from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

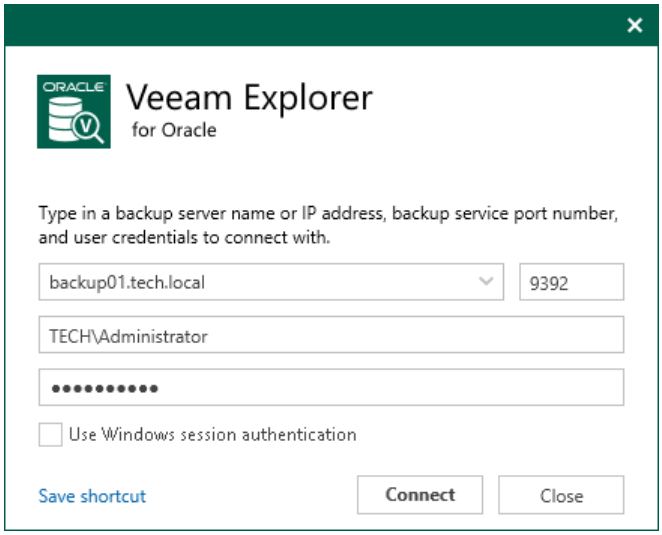
- The domain name or IP address of the backup server to which you want to connect
- The port number
- User account credentials

  Consider the following:

  - To perform recovery operations, Veeam Explorer for Oracle must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorers Suite is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Oracle is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

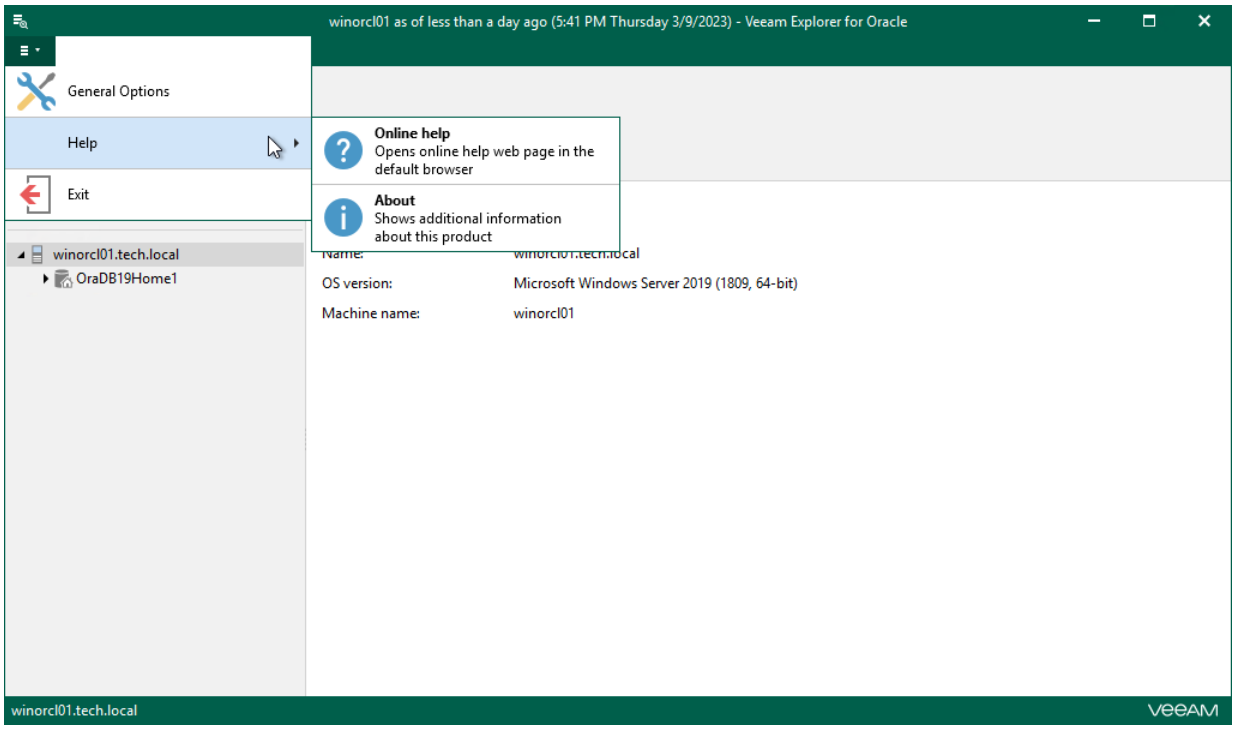
Veeam Explorer for Oracle provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Oracle window.

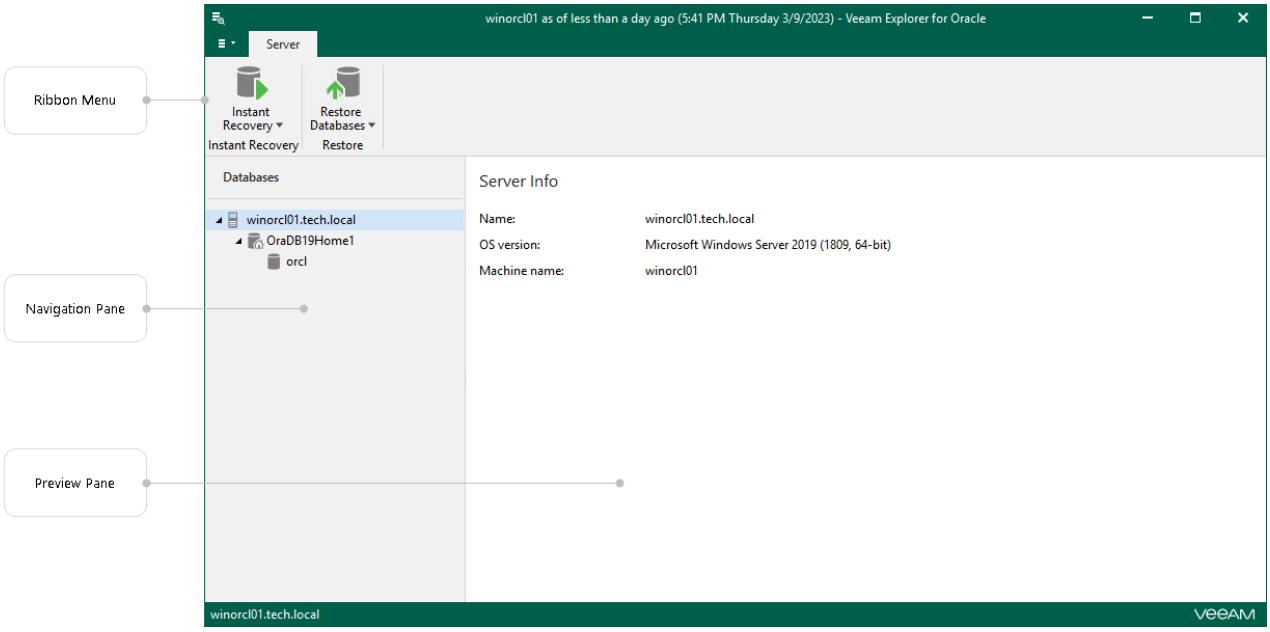
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Oracle wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



How Mounting Works

When restoring your data, Veeam Explorer for Oracle requires an additional mount point to be created to display the list of available transactions.

Mounting is performed by the *Veeam Mount Service* component which is deployed on a backup repository machine or any other machine you define in the backup repository settings. For more information on configuring mount server settings, see the Mount Server section of the Veeam Backup & Replication User Guide.

During mounting, *Veeam Mount Service* retrieves a VM file system from the backup file, attaches it to the hard drive of a target machine and creates a mount point.

Mounting is done as follows:

- To mount a VM file system on machines with the Microsoft Windows operating system, Veeam uses the iSCSI protocol.

  The original virtual machine or the staging server acts as an iSCSI initiator and the mount server that is associated with the backup repository acts as an iSCSI target. The iSCSI mount point is non-persistent and only exists during the recovery process.

- To mount a VM file system on machines with Linux, Veeam uses FUSE.

> **NOTE**
>
> When using fine-tune restore, Veeam requires a staging Oracle server to mount the VM file system.

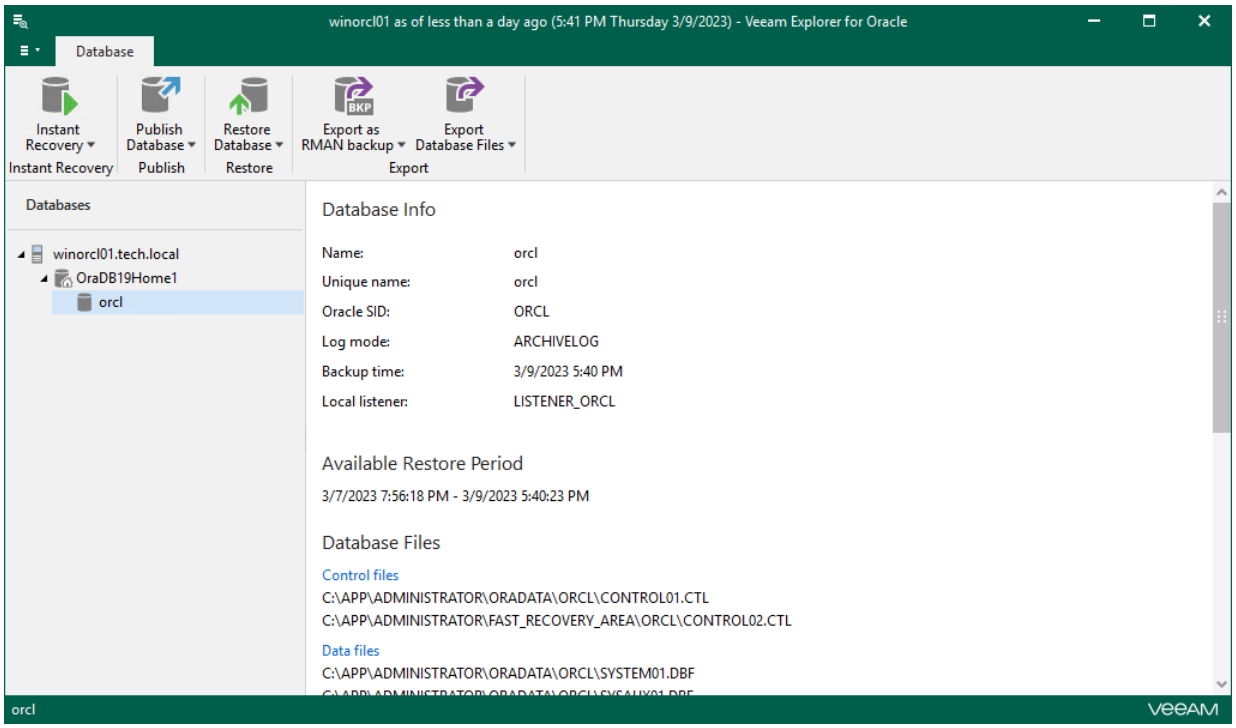
Viewing Database Information

To view Oracle database information, select a database or Data Guard in the navigation pane and review its properties in the preview pane.

Viewing Oracle Database Information

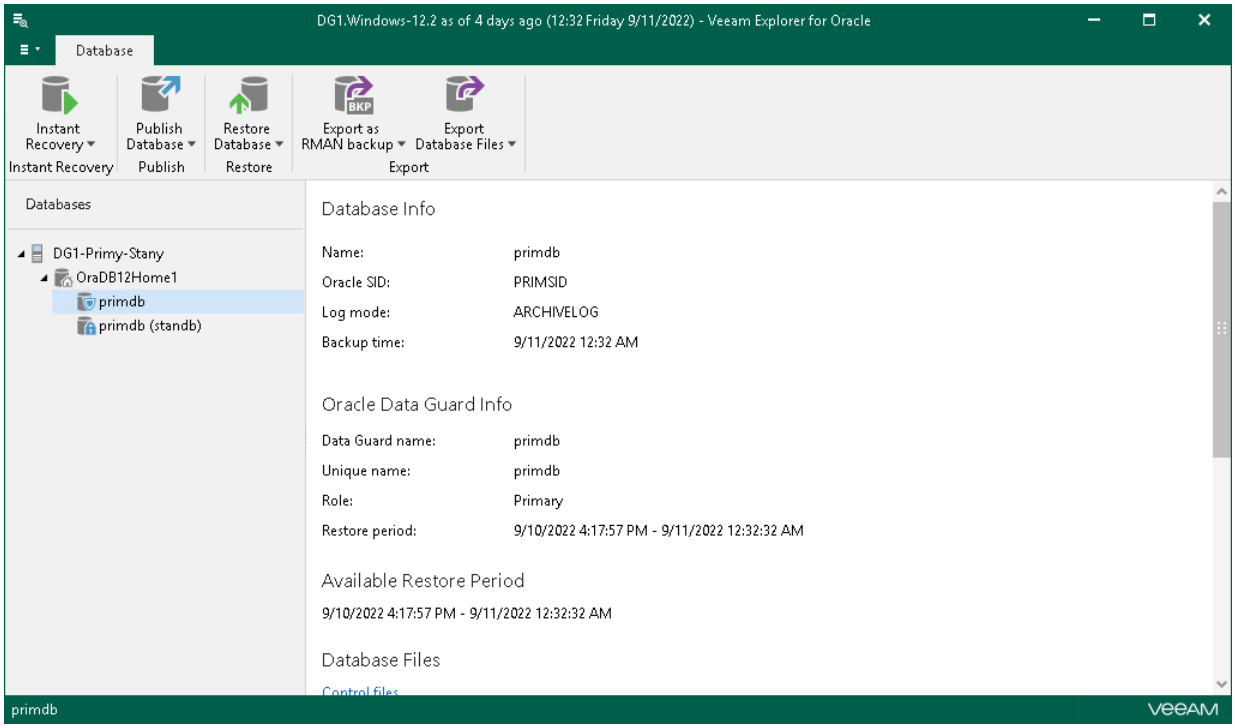
The following figure shows the standalone database information view.

If the current restore point was created with Oracle Automatic Storage Management (ASM), file paths will be displayed with the '+' prefix.



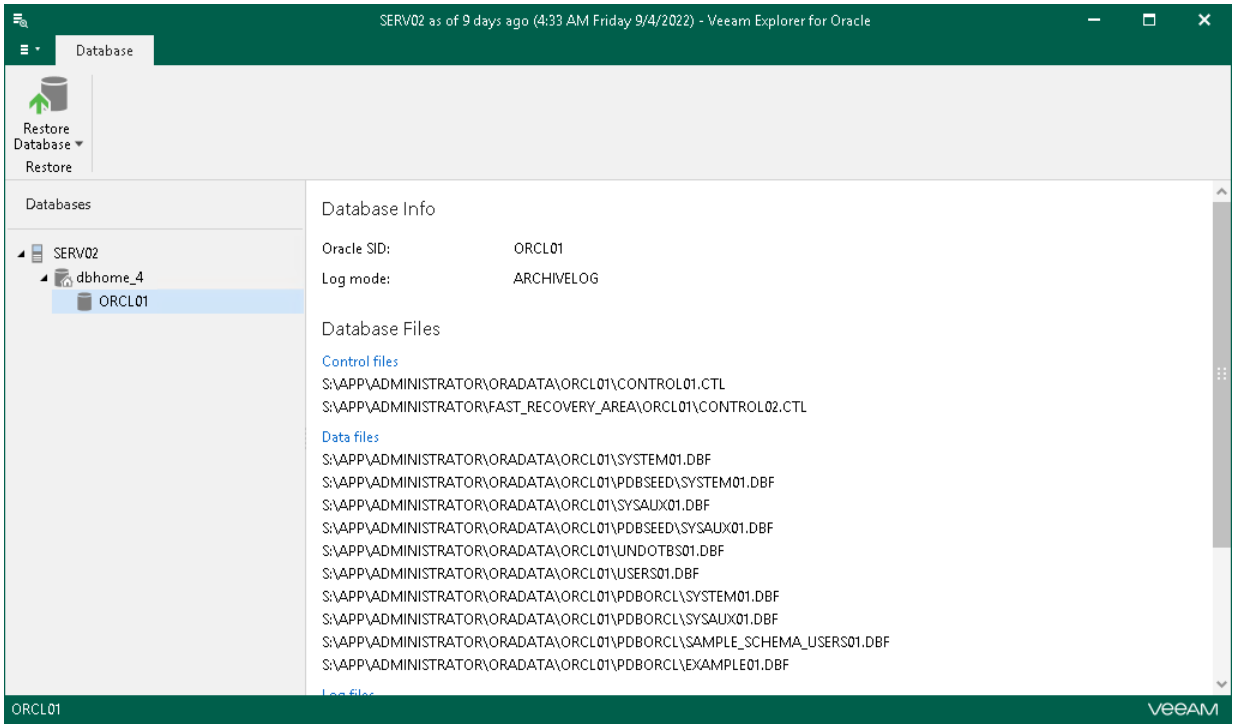
Viewing Oracle Data Guard Information

The following figure shows the Data Guard information view.



Viewing Oracle RMAN Database Information

The following figure shows the RMAN database information view.



General Application Settings

This section explains how to configure the required application settings and components of Veeam Explorer for Oracle.

Configuring Staging Oracle Server

This section explains how to configure a staging Oracle server.

A staging Oracle server is required in the following cases:

- If you use the *point-in-time state* option of databases for restore, export, publishing and instant recovery operations.
- To explore backups created without application-aware image processing. For more information, see Exploring Oracle Backups.

Consider the following:

- A staging server must be of the same Oracle version as both the source and target Oracle servers.
- If you plan to restore databases with *Automatic Storage Management* enabled, both staging and target servers must have ASM enabled.
- Oracle Database Express Edition cannot be used as a staging system.

For Windows-based VM

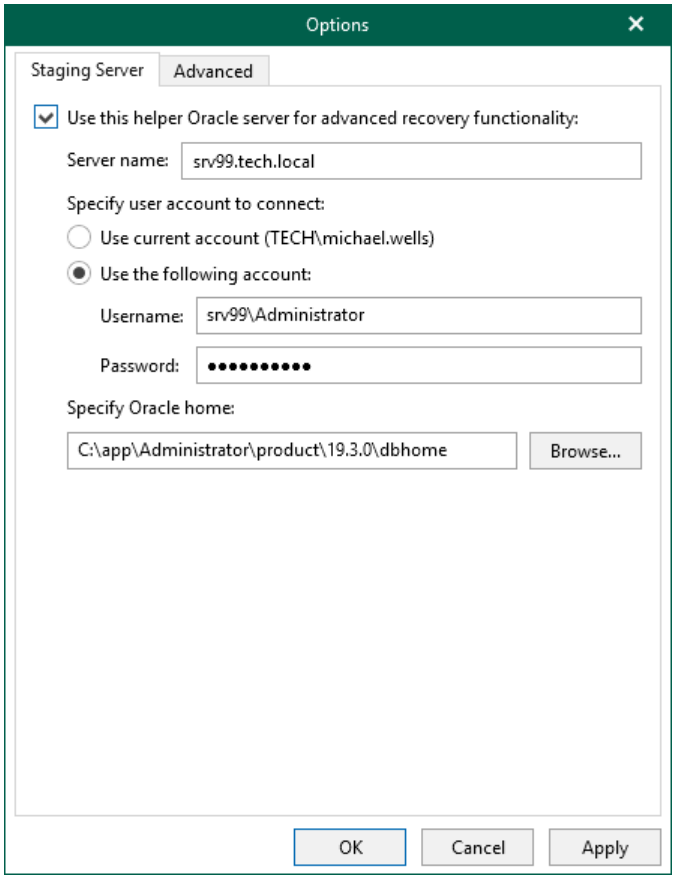
To configure a staging server for Windows-based machines, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Staging Server** tab, select the **Use this helper Oracle server for advanced recovery functionality** check box and do the following:
   a. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
   b. In the **Specify user account to connect** section, select the following:
      - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Oracle running.
      - **Use the following account**. To connect to the specified server under a custom user account.

        When using a custom account, in the **Username** field, specify a user name and in the **Password** field, provide the password.

3. Specify the path to Oracle home.

   Click **Browse** to browse for Oracle home.

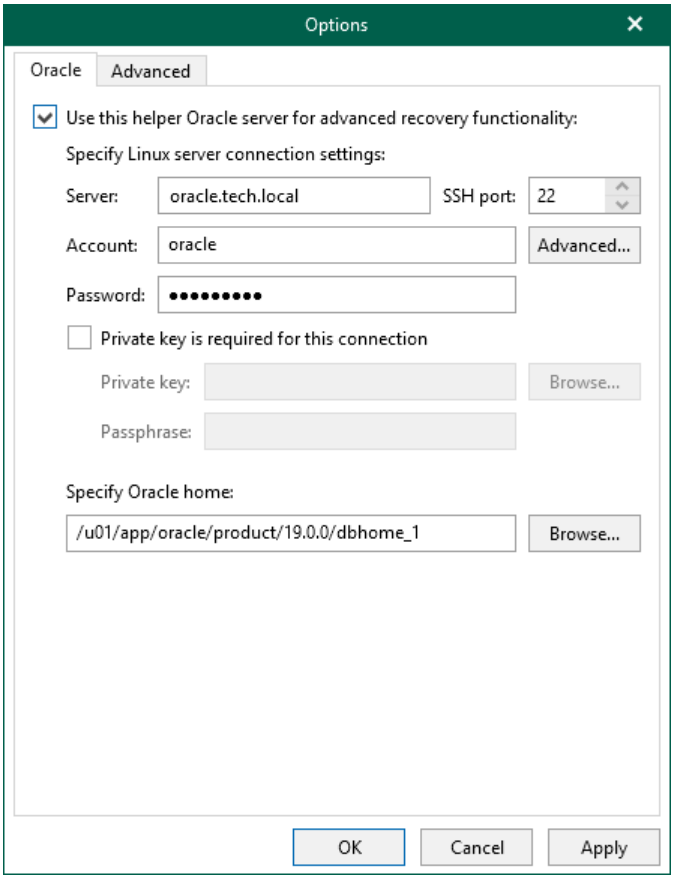


For Linux-based VM

To configure a staging server for Linux-based machines, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Oracle** tab, select the **Use this helper Oracle server for advanced recovery functionality** check box and do the following:
   a. In the **Server** field, specify the name of the Oracle server to which you want to restore data.
   b. In the **SSH-port** field, specify the port number.
   c. In the **Account** field, specify a user account under which to connect to the specified server.
   d. In the **Password** field, specify the password.
   e. If the private key is required to connect to the selected server, do the following:
      i. Select the **Private key is required for this connection** check box.
      ii. In the **Private key** filed, specify a key. To select a key, click **Browse** and select a key.
      iii. In the **Passphrase** field, enter the passphrase.

3. Specify the path to Oracle home.



4. If you specify data for a non-root account that does not have root permissions on a Linux server, click **Advanced** to grant sudo rights to this account.

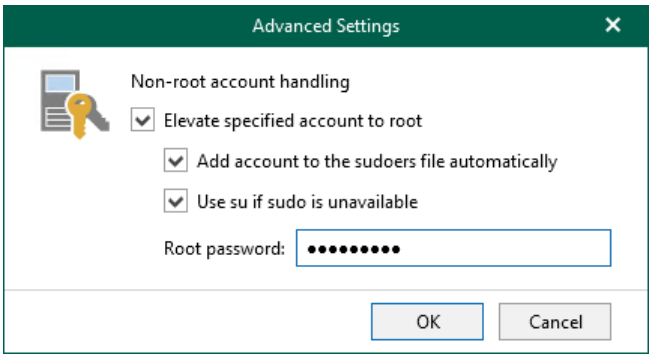
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.

   b. To add the user account to the sudoers file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the sudoers file.

   c. When registering a Linux-based VM, you have an option to failover to using the su command for distros where the sudo command is not available.

      To enable the failover, select the **Use su if sudo is unavailable** check box and in the **Root password** field, enter the password for the root account.

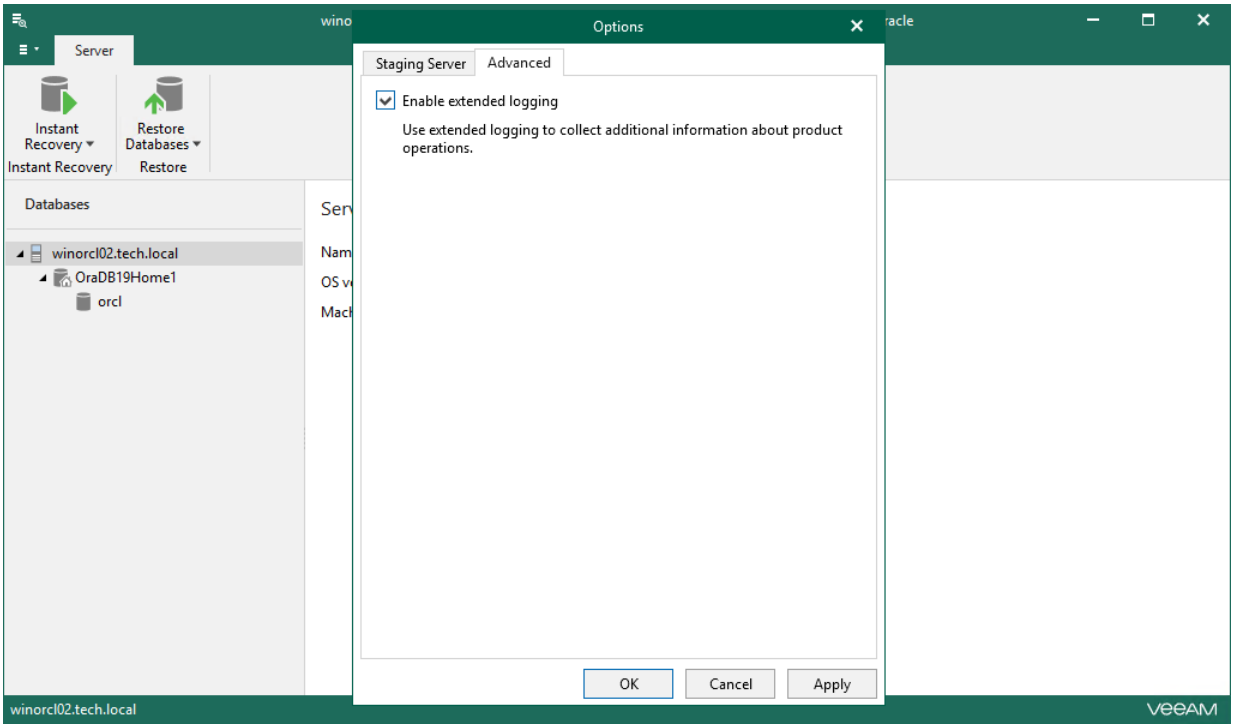


Enabling Extended Logging

Veeam Explorer for Oracle allows you to enable an extended logging mode to collect logs that contain more details on specific operations. After you enable extended logging, you can go back to the application and perform the actions for which you want to collect additional information. Then you can collect the logs.

To enable extended logging, do the following:

1. Go to the main menu and click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box and click **OK**.



Exploring Oracle Backups

This section contains information about exploring different kinds of Oracle backups.

Exploring Application-Enabled Backups

For more information about exploring backups created with application-aware image processing, see the Application Item Restore section of the Veeam Backup & Replication User Guide.

Exploring Non-Application Enabled Backups

If a backup file you are exploring has been created without application-aware image processing, you need to perform the heuristic analysis to mount the required restore points and find existing Oracle databases in these points.

> **NOTE**
>
> The heuristic analysis requires a staging Oracle server to be configured in advance. For more information, see Configuring Staging Oracle Server.

To explore backups created without application-aware image processing, do the following:

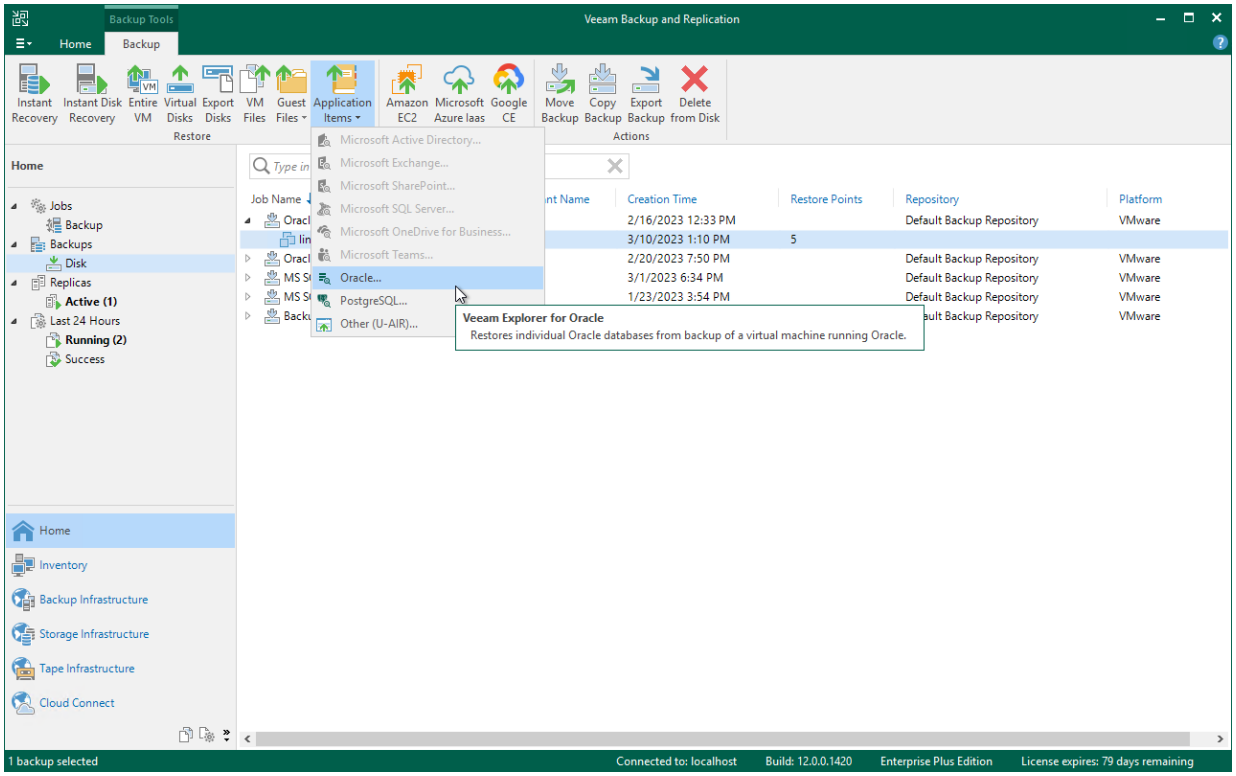
1. Launch the Heuristic Analysis wizard.
2. Specify the target server.
3. Specify heuristic settings.

Step 1. Launch Heuristic Analysis Wizard

To launch the **Heuristic Analysis** wizard, do the following:

1. In the Veeam Backup & Replication console, select the necessary backup and click **Application Items** > **Oracle** (or **Windows**) on the ribbon.
2. At the **Restore Point** step of the **Oracle Database Restore** wizard, select a restore point to explore.
3. Complete subsequent steps of the wizard and click **Browse**.

Veeam Backup & Replication will launch Veeam Explorer for Oracle and display the **Heuristic Analysis** wizard.



Step 2. Specify Target Server

At this step of the **Heuristic Analysis** wizard, specify 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.

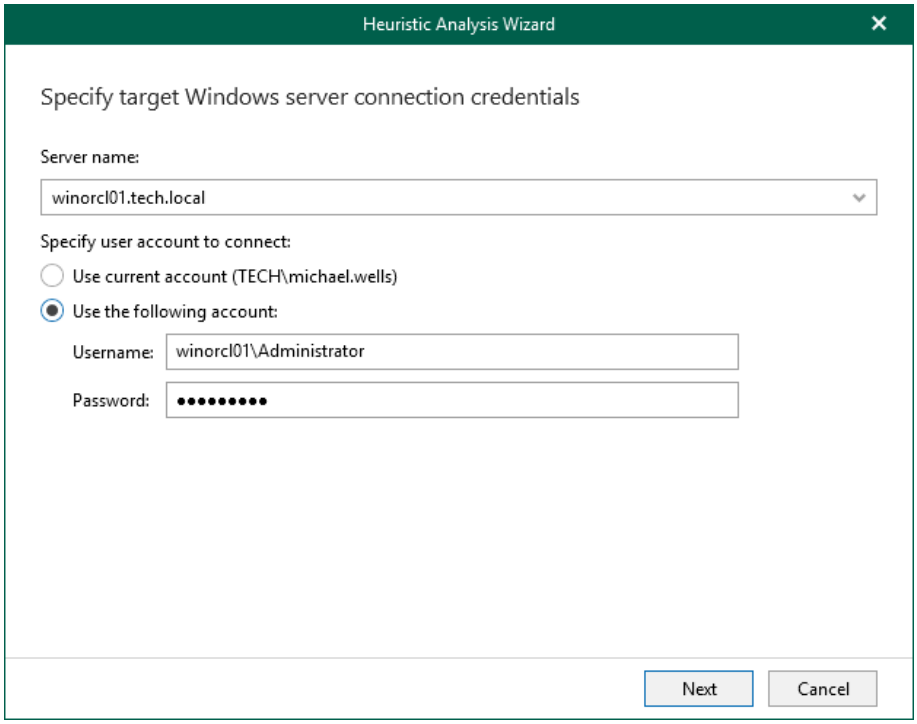
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify a server name to which you want to restore data.
2. In the **Specify user account to connect to server** section, select one of the following:
   - **Use current account**. To connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**. To connect to the specified server under a custom user account.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.



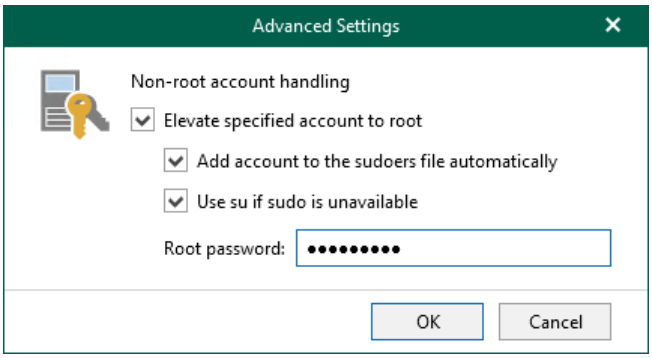
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

3. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
4. In the **SSH port** field, specify the port number of the selected Oracle server.
5. In the **Account** filed, specify an account under which to connect to the specified server.

6. In the **Password** field, enter the password.
7. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

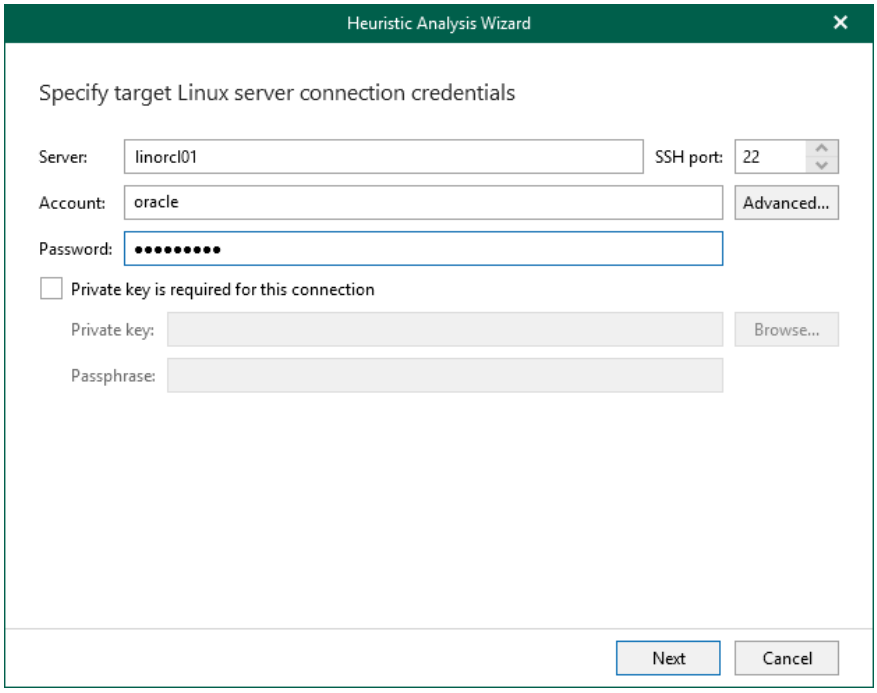
      If you do not enable this option, you will have to manually add the user account to the sudoers file.
   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use su if sudo is unavailable** check box and enter the password for the root account in the **Root password** field.



8. 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.

Consider that the user account must be a member of the **dba** group.



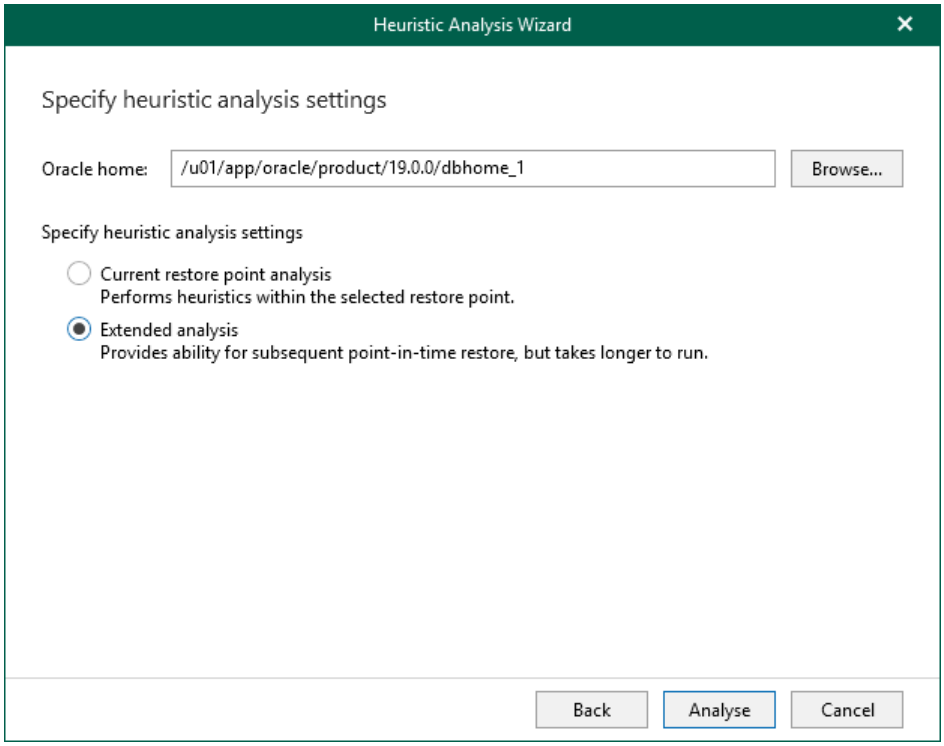
Step 3. Specify Heuristic Settings

At this step of the wizard, specify the following:

- **Oracle home**. To attach a database, apply log files (if required) and make a consistency check of the database.
- **Heuristic analysis settings**:
  - **Current restore point analysis**. To search for available Oracle databases within the selected restore point only.
  - **Extended analysis**. To search for available Oracle databases within multiple restore points.

    Typically, Veeam Explorer for Oracle scans three restore points; the current restore point that you select when opening Veeam Explorer for Oracle, and two other restore points that come before and after the current restore point.

Once analysis is complete, Veeam Explorer for Oracle will load available Oracle databases to the program scope automatically.

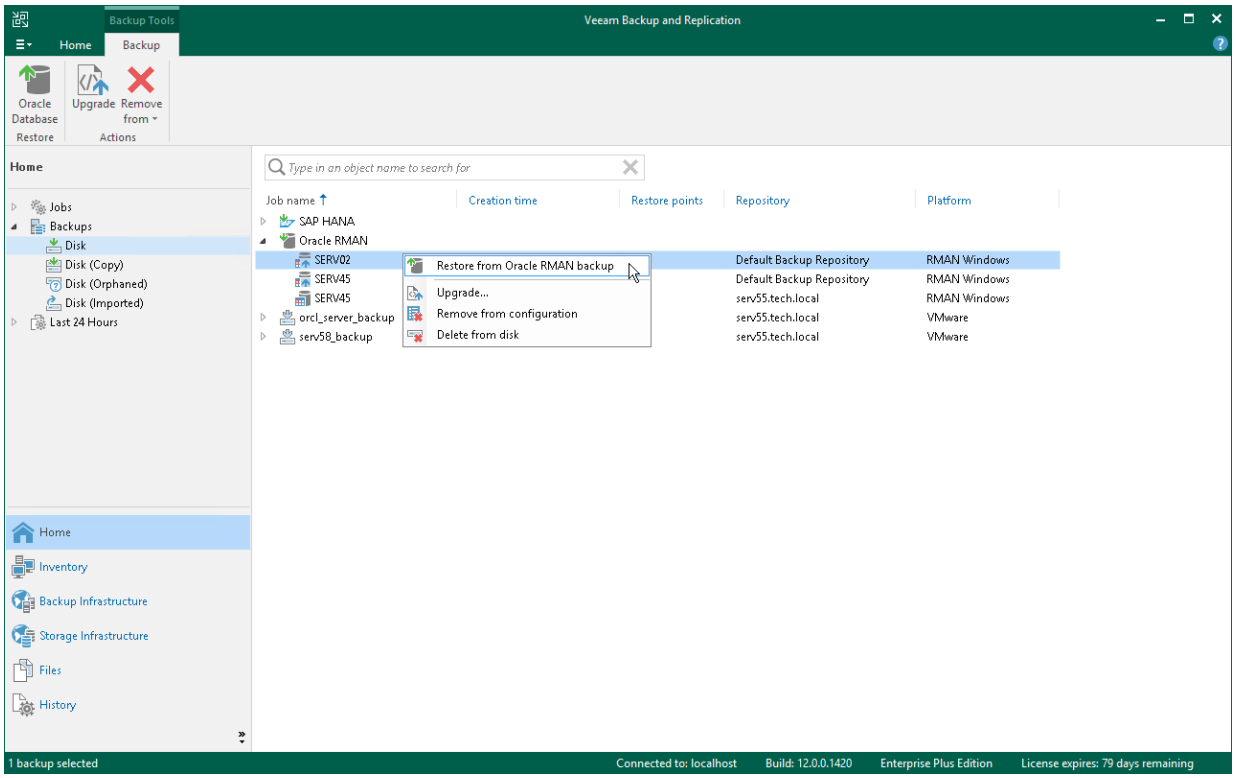


Exploring RMAN Backups

This section explains how to explore backups created with the Oracle RMAN Plug-in. For more information, see Veeam Plug-in for Oracle RMAN.

To load RMAN backups, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Go to the **Backups** > **Disk** node.
3. Right-click an RMAN backup and select **Restore from Oracle RMAN backup**.



Data Restore

This section contains information about the available restore operations in Veeam Explorer for Oracle.

Before restoring data, read the Considerations and Limitations section.

> **IMPORTANT**
>
> Make sure to install a bash shell on a target Oracle server to perform a restore.

Restoring Single Database and Data Guard

This section explains how to restore Oracle databases and Oracle Data Guard back to the production environment.

Consider that when restoring Data Guard to another server as described in this section, databases from Data Guard will be restored as standalone Oracle databases preserving no Data Guard infrastructure. To restore Data Guard infrastructure altogether, use either a latest state restore, or point-in-time restore. For more information, see Restoring Latest State and Restoring Point-in-Time State.

To restore data, take the following steps:

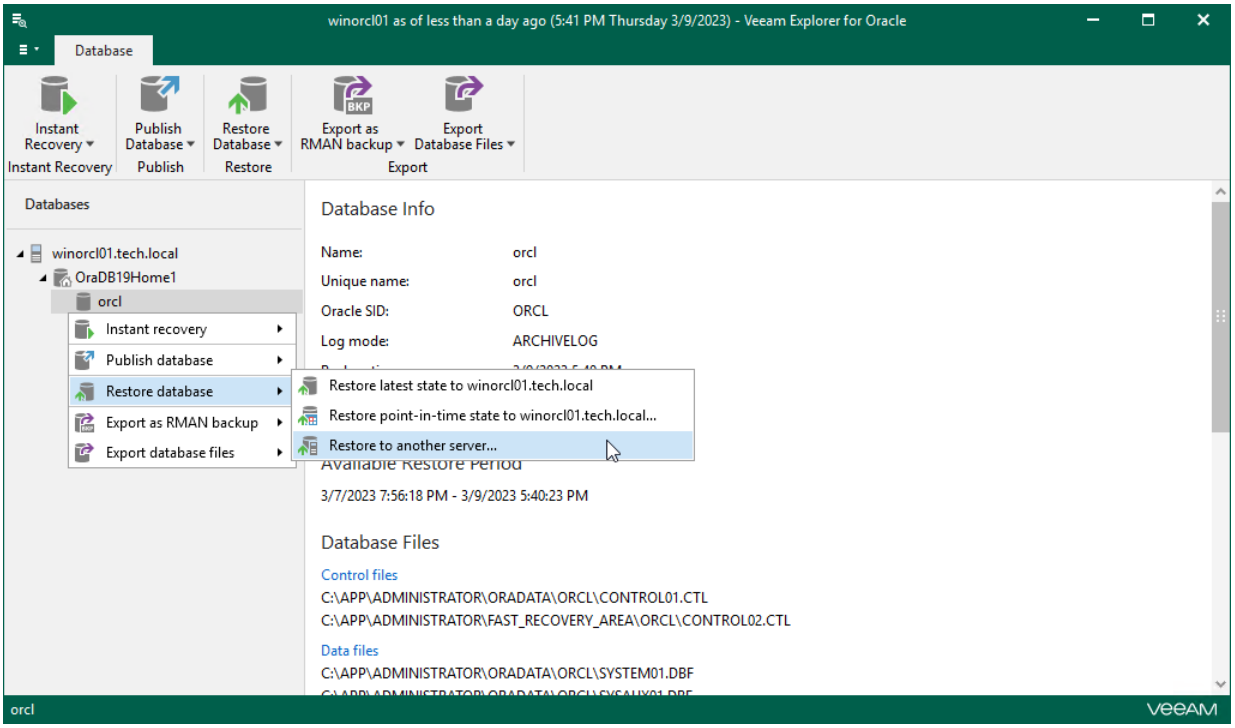
1. Launch the Restore wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target server.
5. Specify Oracle settings.
6. Specify database files location.

Step 1. Launch Restore Wizard

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

1. In the navigation tree, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore to another server**.

Alternatively, you can right-click a database or Data Guard and select **Restore database** > **Restore to another server**.



Step 2. Specify Restore Point

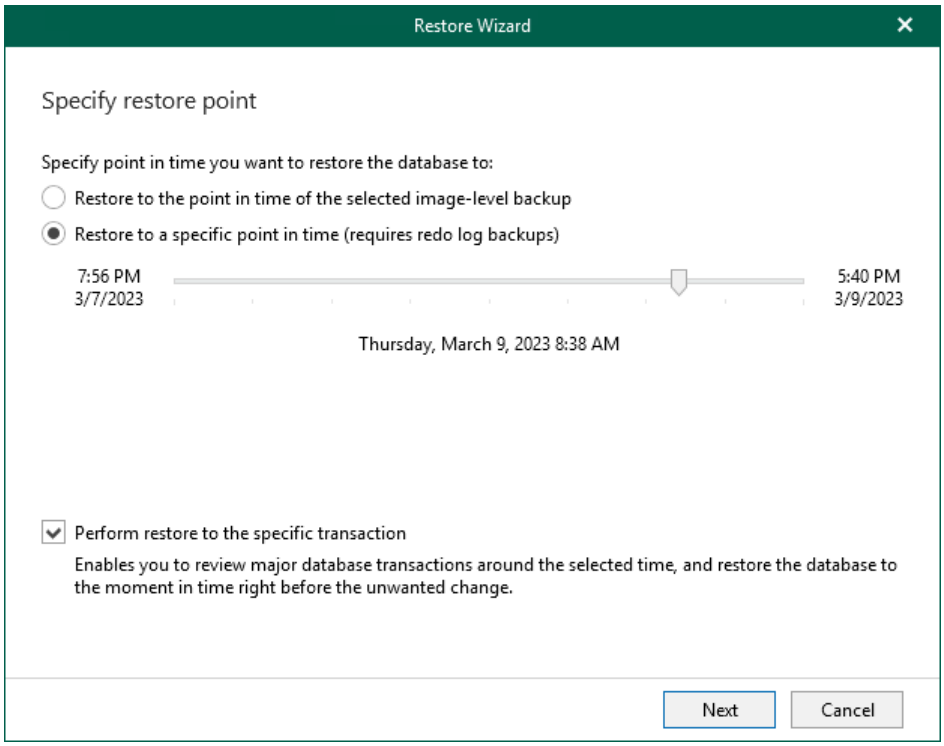
At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

Consider the following:

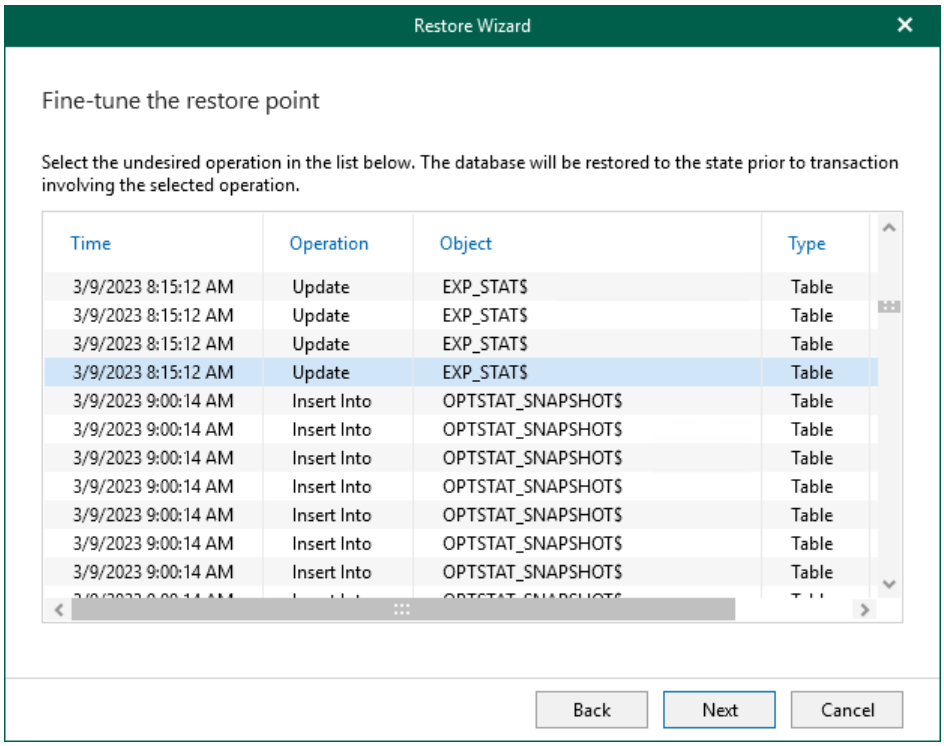
- The **Restore to a specific point in time** option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
- The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore your database.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Server

At this 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

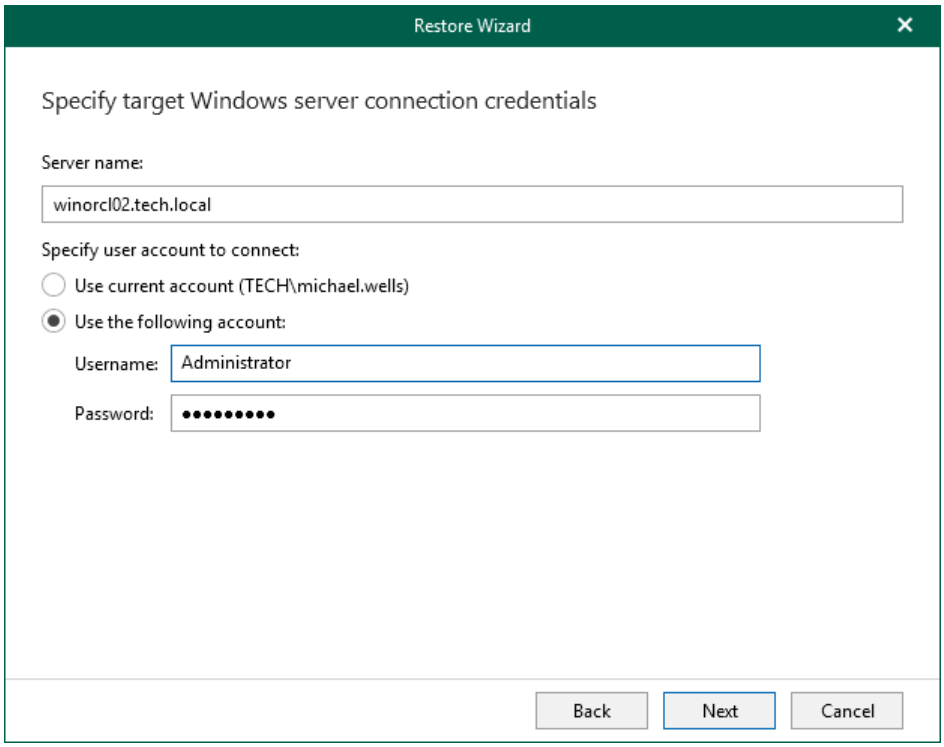
For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the target Oracle server.
2. In the **Specify user account to connect** section, select either of the following options:
   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Oracle is running.

     You cannot use this option if Veeam Explorer for Oracle and mount server are located on separate machines.
   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.

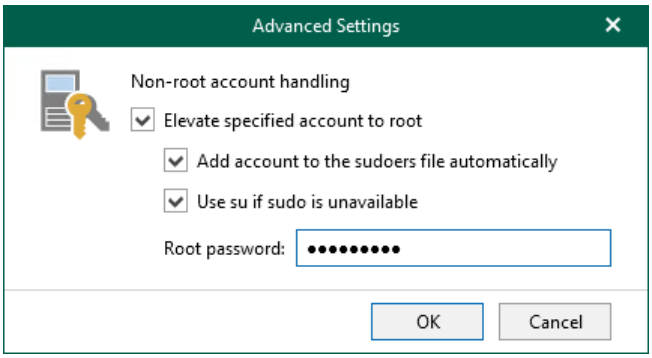


Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

1. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

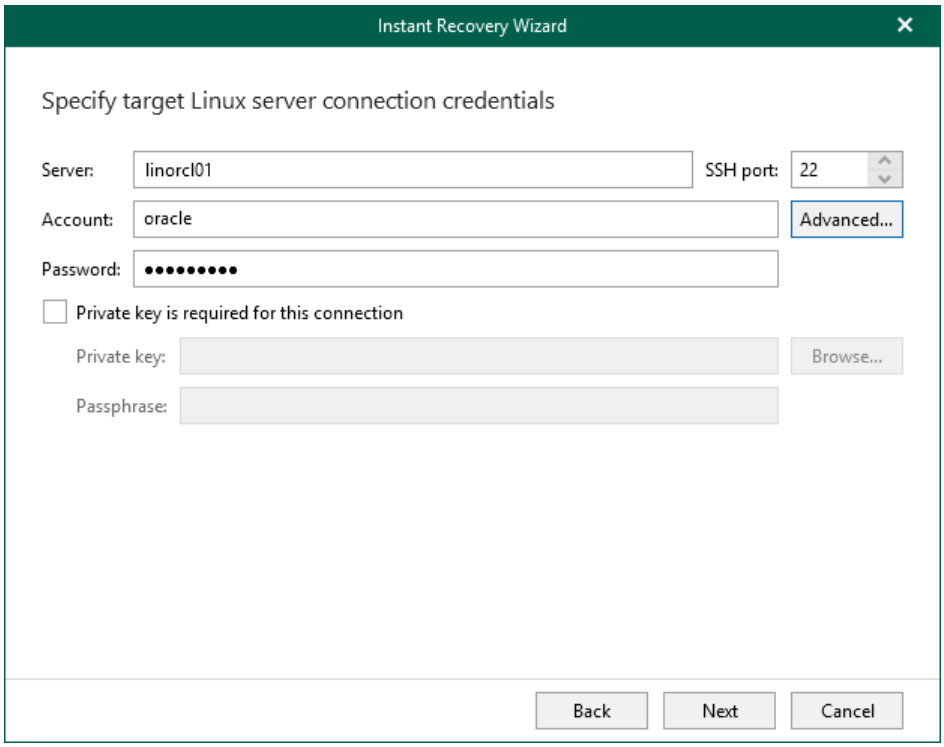
      If you do not enable this option, you will have to manually add the user account to the sudoers file.
   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use su if sudo is unavailable** check box and enter the password for the root account in the **Root password** field.



6. 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.

Consider that the user account must be a member of the **dba** group.



Step 5. Specify Oracle Settings

At this step of the wizard, specify the location to which you want to restore the database.

- Select **Restore to the original location** to restore the database back to the original location.
- Select **Restore to a different location** to restore the database to a custom location.

  a. In the **Oracle home field**, specify the Oracle home directory. To locate the Oracle home directory, click **Browse** and select the folder you want to use.

  b. In the **Global database name** field, specify the global database name as *DB_NAME.DB_DOMAIN*, where:

  - *DB_NAME* is the database name. Oracle limits the length of the database name to 8 characters. If the database name you specify exceeds this limit, Veeam Explorer for Oracle will automatically shorten the database name, and hence the global database name, during the restore process.

    The value you specify is also used for the unique database name (*DB_UNIQUE_NAME*). The unique database name can contain up to 30 characters.

  - *DB_DOMAIN* is the domain name of the database. It does not count towards any character limits and Veeam Explorer for Oracle does not shorten it during the restore process.

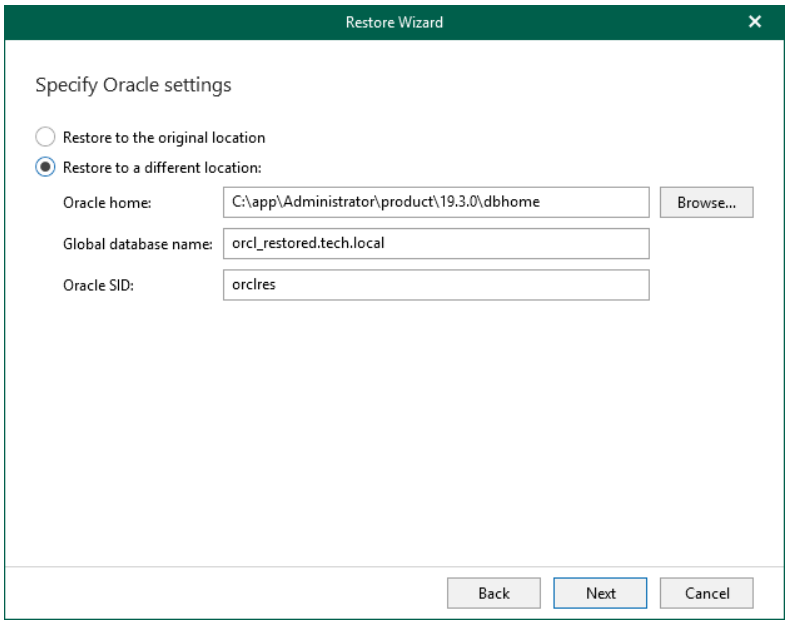
  For example, if you specify the global database name as *orcl_restored.tech.local*, Veeam Explorer for Oracle will shorten it to *orcl_res.tech.local*. The database name will be *orcl_res*, while the unique database name will be *orcl_restored.*

  c. In the **Oracle SID** field, specify the database system identifier. The **Oracle SID** field is automatically filled with the value entered in the **Global database name** field, but you can also assign a different value.

  The maximum length of the Oracle SID is 12 characters and it can only contain alphanumeric characters (a-z, A-Z and 0-9).

NOTE

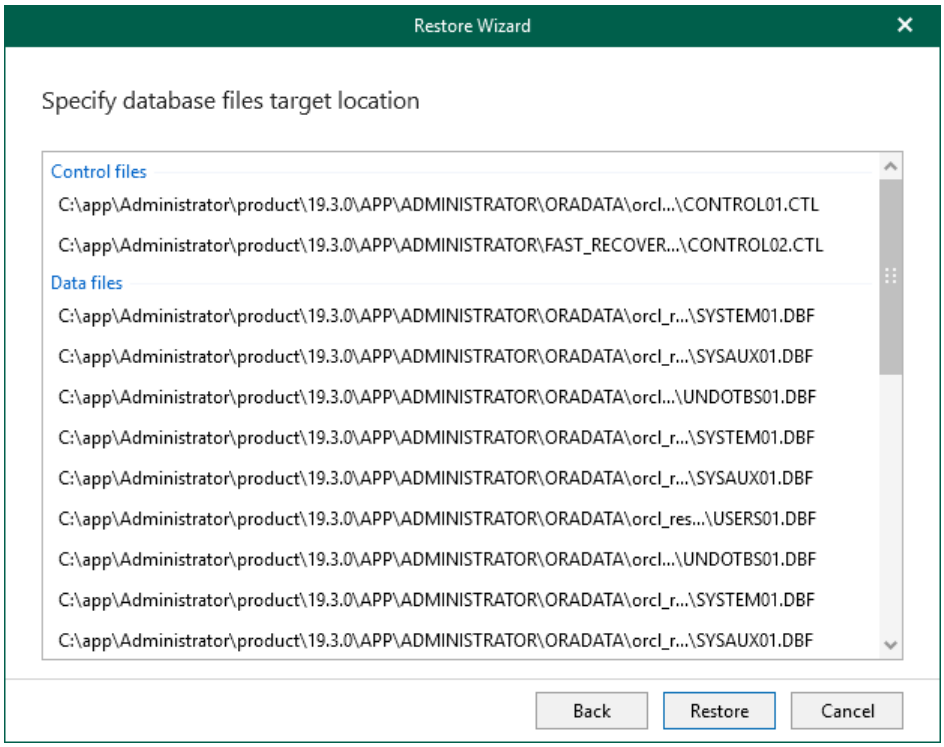
If the account specified in the previous step is not the Oracle home user, you will be asked to provide a password to access the target Oracle home. Applicable to Oracle 12c and later versions.



Step 6. Specify Database Files Location

At this step of the wizard, specify the location for database files.

To edit the path, click the path row and provide the location you want to use.



Restoring Latest or Point-in-Time State

This section explains how to select a state as of which to restore Oracle databases or Data Guard, including a point-in-time restore — to revert the database to a state before an undesired transaction or before a point of failure.

The behavior in case of a latest or point-in-time state restore is as follows:

- Data Guard will be restored starting from the primary node. Once the primary node is restored, Veeam Explorer for Oracle will use it to restore standby nodes.
- Database files will be copied to the original location and then mounted to the original Oracle home.
- Databases from the backed-up ASM group will be restored back to the original ASM group.
- All existing databases on the target Oracle server will be replaced with databases from the backup files.

Consider that restoring a latest or point-in-time state to the original Oracle server from storage snapshots is not supported. Use the **Restore to another server** command, as described in Restoring Database and Data Guard.

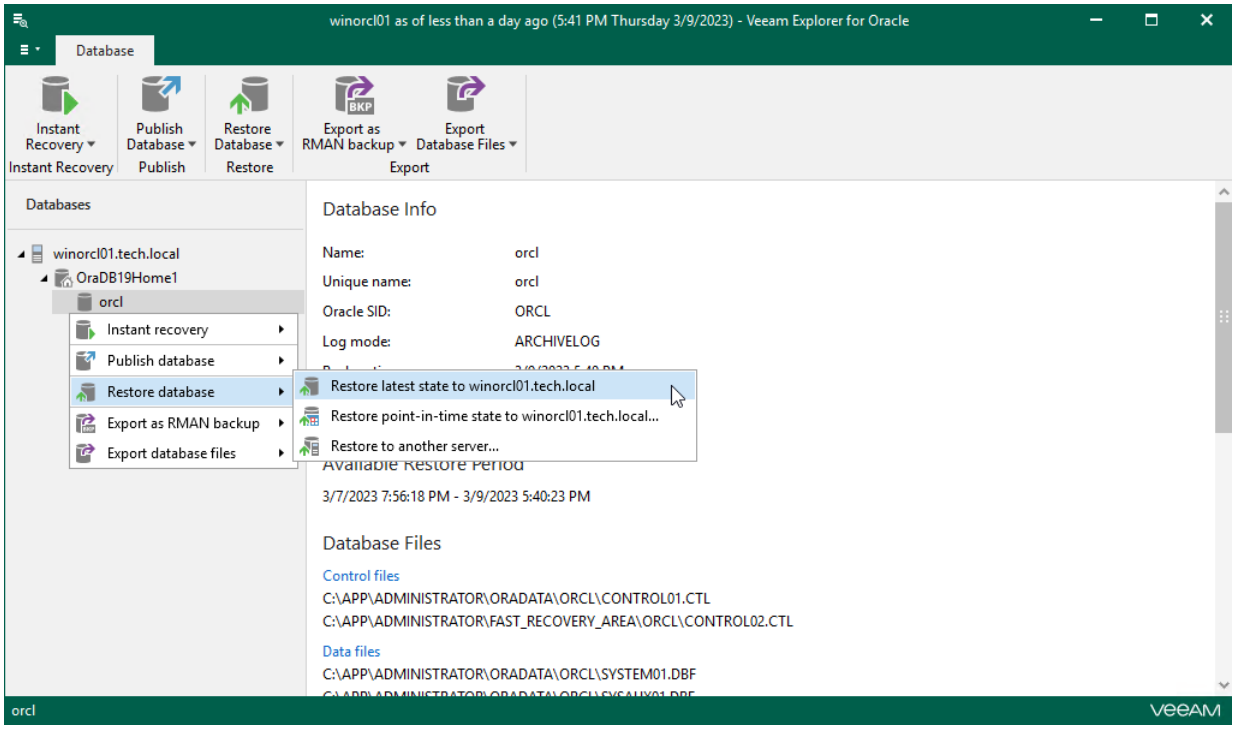
Restoring Latest State

To restore Oracle databases or Data Guard as of the latest available state, do the following:

1. In the navigation pane, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore latest state to <original_location>**.

Alternatively, you can right-click a database or Data Guard and select **Restore database > Restore latest state to <original_location>**.

> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Restoring Point-in-Time State

To restore Oracle databases or Data Guard as of the selected point-in-time state, do the following:

1. Launch Restore Wizard.
2. Specify Restore Point.
3. Fine-tune Restore Point.

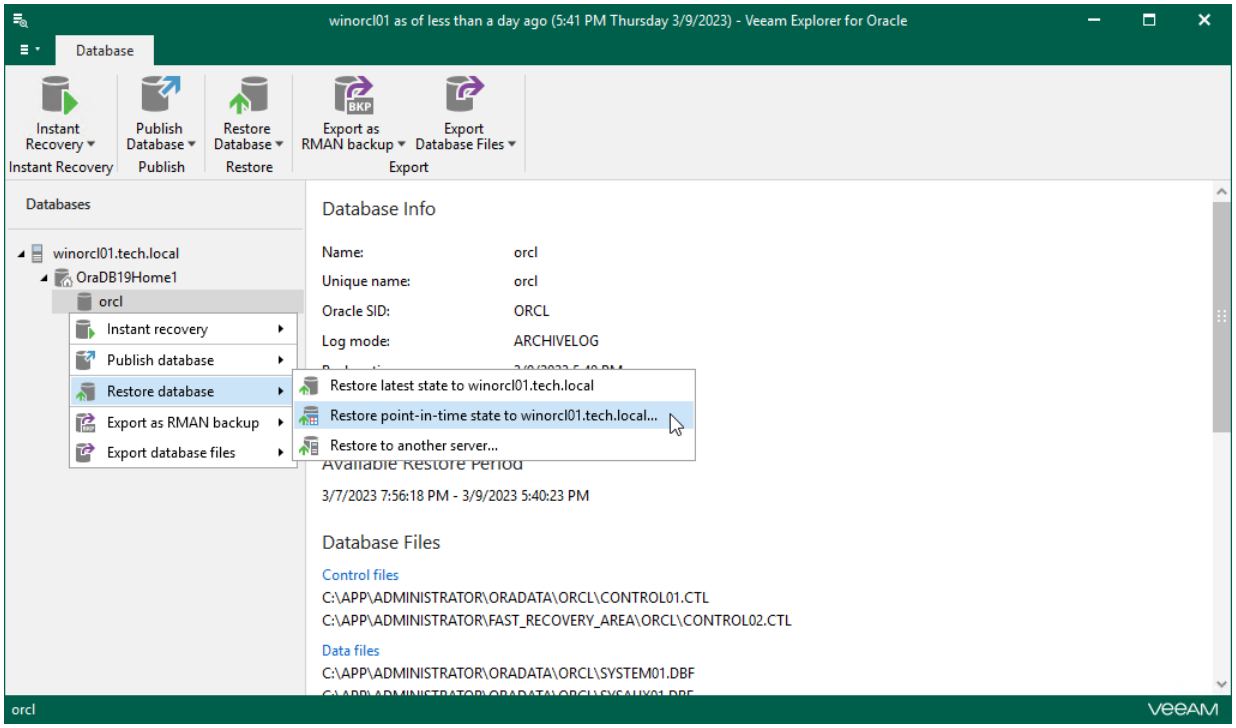
Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a database or Data Guard.
2. On the **Database** tab, select **Restore Database** > **Restore point-in-time state**.

Alternatively, you can right-click a database or Data Guard and select **Restore database** > **Restore point-in-time state**.

> **IMPORTANT**
>
> A point in time restore is only possible if the *ARCHIVELOG* mode is enabled.



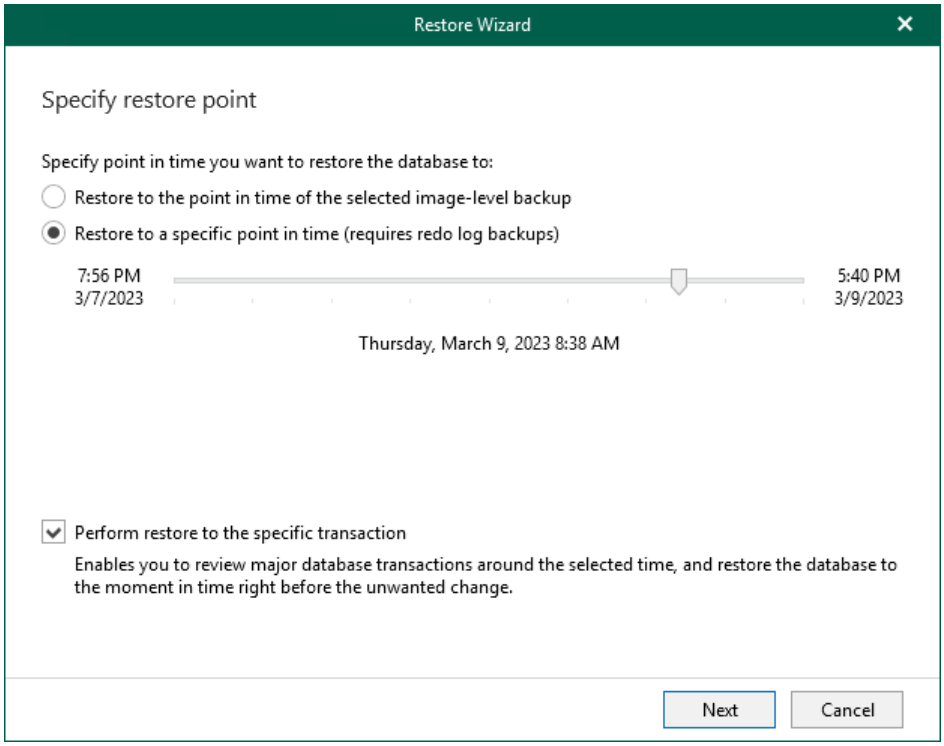
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain selected database files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

Consider the following:

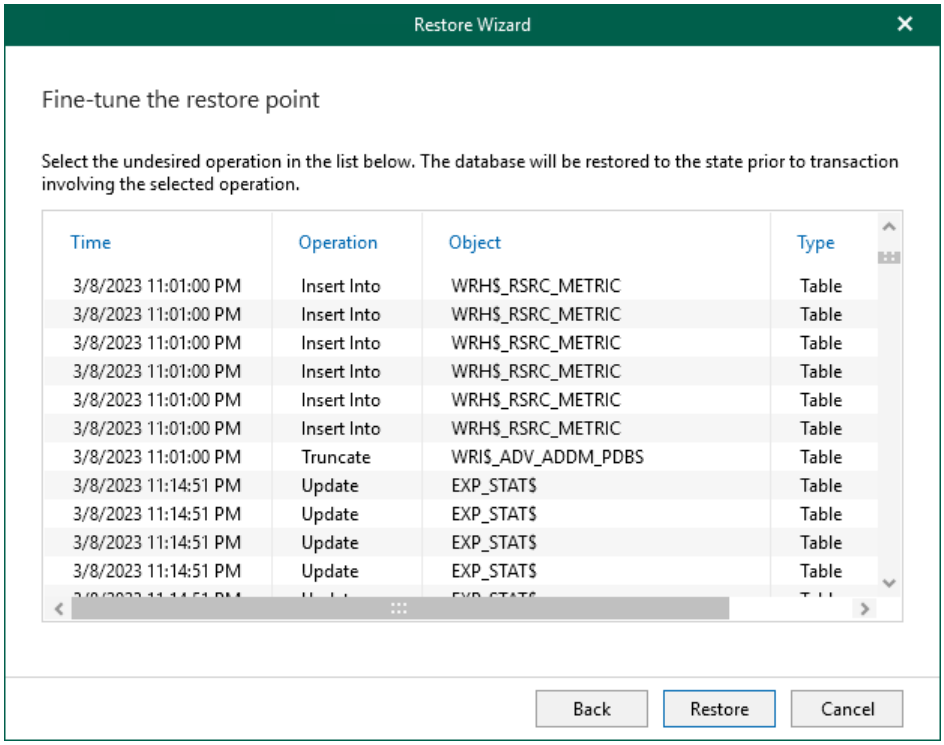
- The **Restore to a specific point in time** option is available only if archived log backups exist. For more information, see Required Backup Job Settings.
- The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore your database and click **Restore**.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Restoring Multiple Databases

With Veeam Explorer for Oracle, you can restore multiple databases of the Oracle home or the server to the original server or to another server with different settings. For instructions, see:

- Restoring Databases to Latest or Point-in-Time State
- Restoring Databases to Another Server

Restoring Databases to Latest or Point-in-Time State

With Veeam Explorer for Oracle, you can restore the latest or point-in-time state of multiple Oracle databases. In this scenario, all selected databases on the original Oracle server will be replaced with databases from the latest or earlier backup files.

Consider the following:

- Data Guard will be restored starting from the primary node. Once the primary node is restored, Veeam Explorer for Oracle will use it to restore standby nodes.
- Database files will be copied to the original location and then mounted to the original Oracle home.
- Databases from the backed-up ASM group will be restored back to the original ASM group.

Consider that restoring a latest or point-in-time state to the original Oracle server from storage snapshots is not supported. Use the **Restore to another server** command, as described in Restoring Databases to Another Server.

For instructions, see the following sections:

- Restoring Databases to Latest State
- Restoring Databases to Point-in-Time State

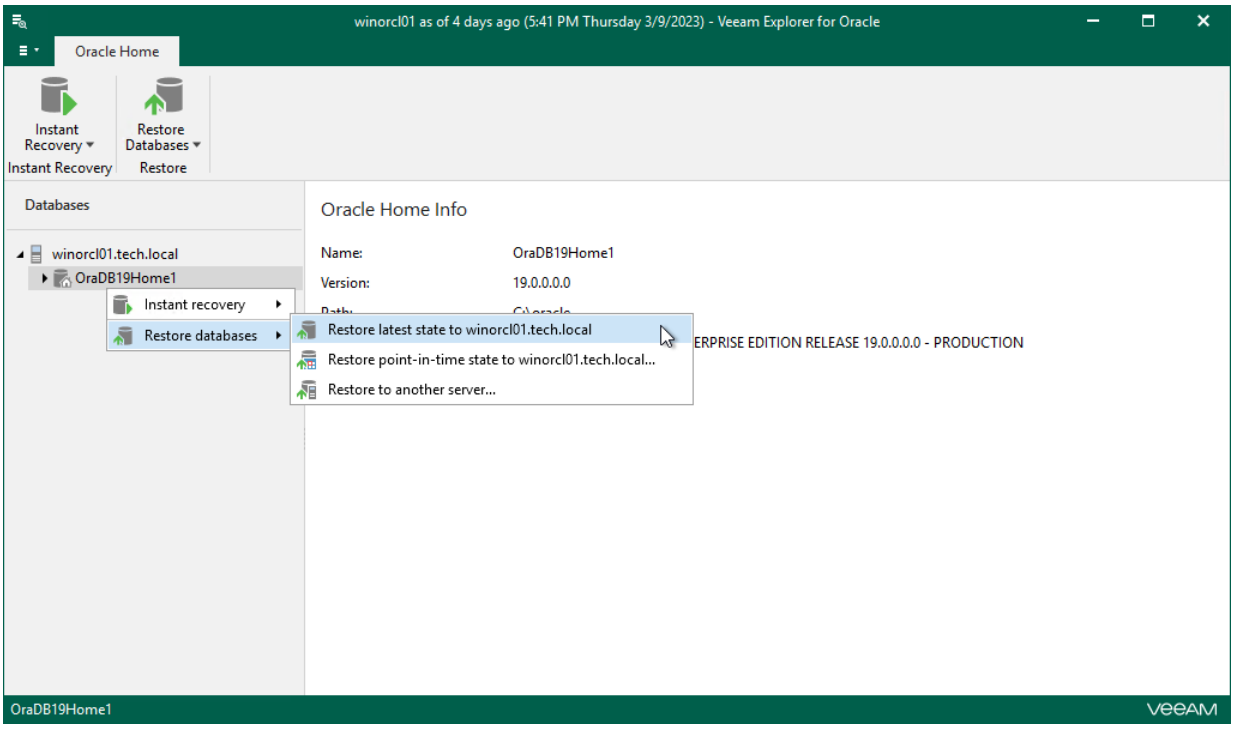
Restoring Databases to Latest State

To restore multiple databases to the latest state to the original server, do the following:

1. In the navigation pane, select the Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Database** > **Restore latest state to <original_location>**.

Alternatively, you can right-click the Oracle server or Oracle home and select **Restore databases** > **Restore latest state to <original_location>**.

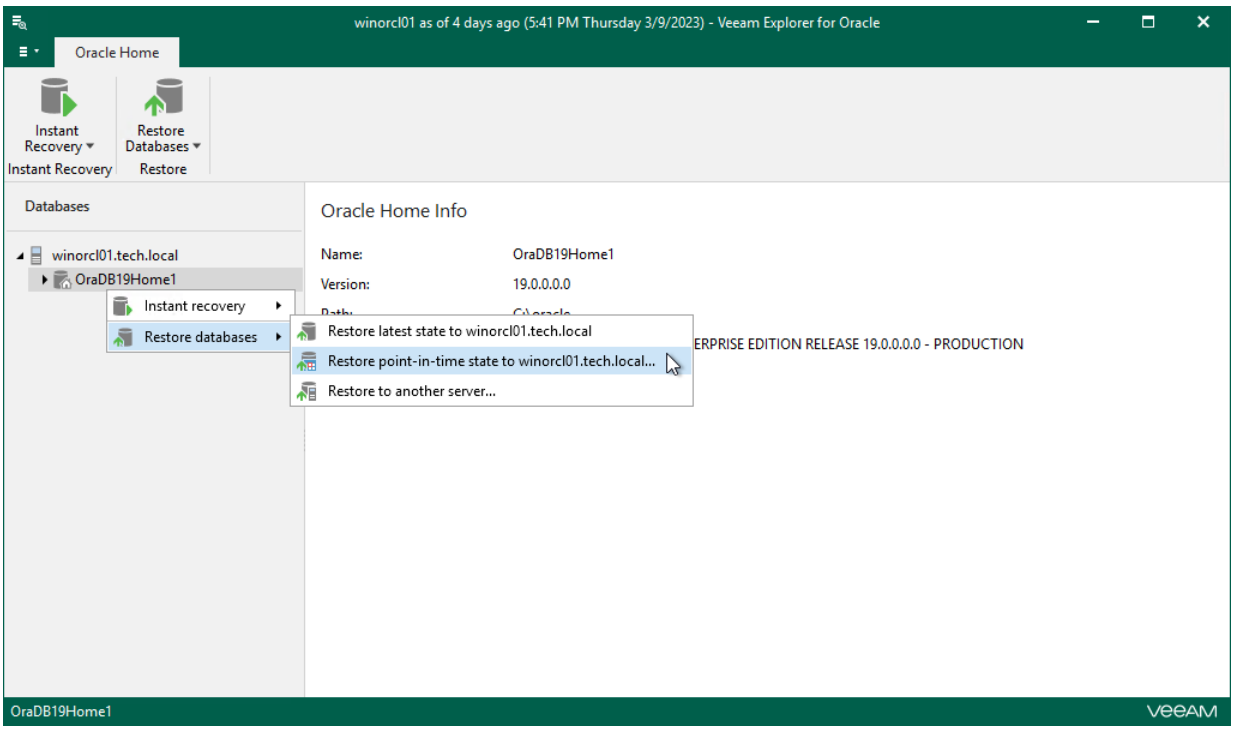
> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Restoring Databases to Point-in-Time State

To restore multiple databases to a point-in-time state to original server, do the following:

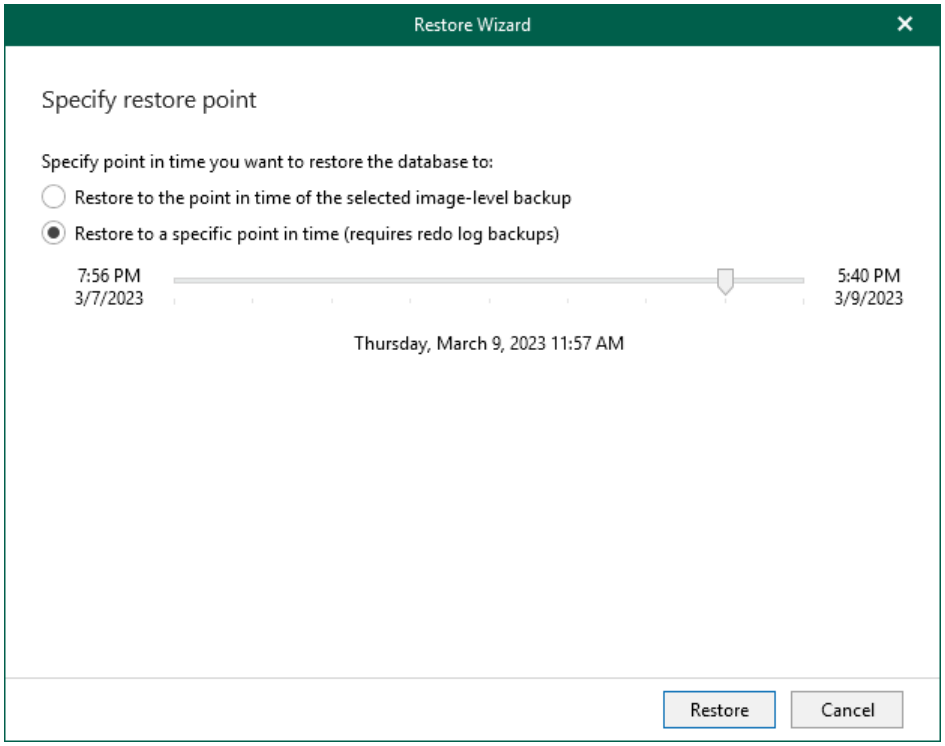
1. In the navigation pane, select the Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Database** > **Restore state of <point_in_time>** or right-click a database and select **Restore databases** > **Restore point-in-time state**.



3. At this step of the **Restore** wizard, select a state as of which you want to restore the databases:
   - Select the **Restore to the point in time** of the selected image-level backup option to load database files as per date when the current restore point was created.

- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a necessary point in time.



Restoring Databases to Another Server

To restore multiple Oracle databases, do the following:

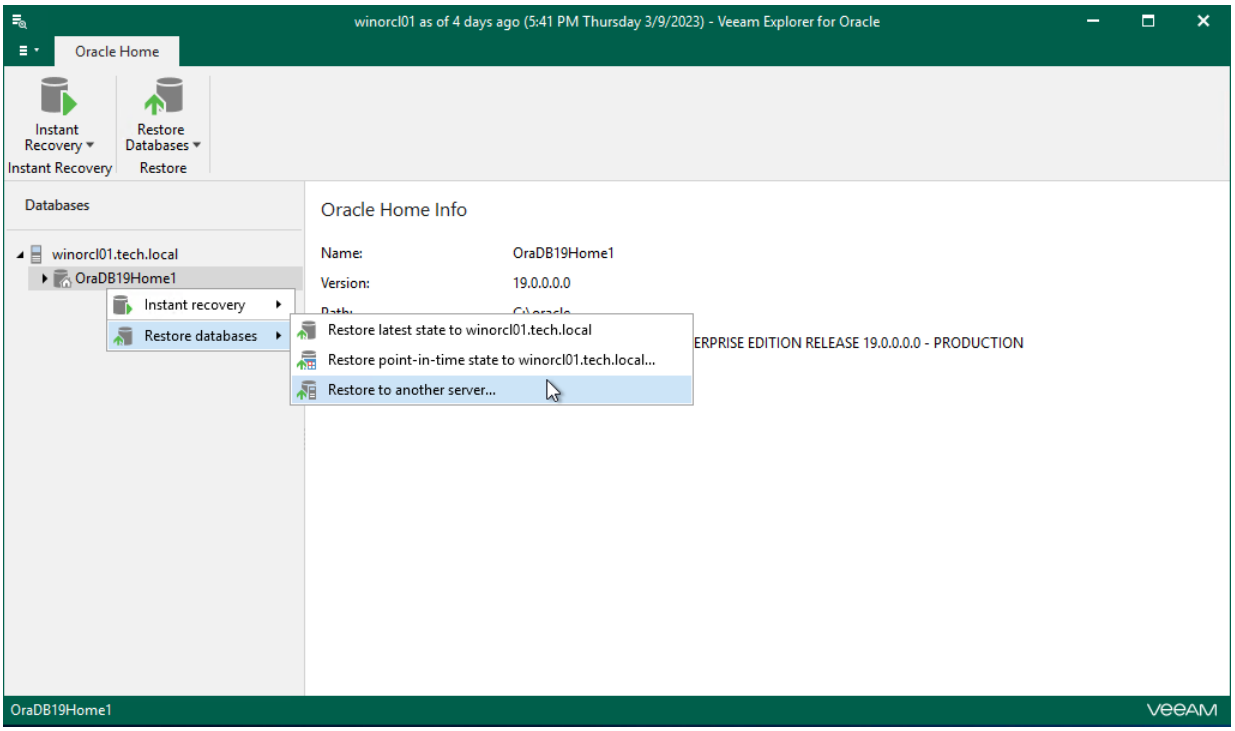
1. Launch the Restore wizard.
2. Specify a restore point.
3. Specify a target server.
4. Specify Oracle settings.

Step 1. Launch Restore Wizard

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

1. In the navigation tree, select an Oracle server or Oracle home.
2. On the **Server** or **Oracle Home** tab, select **Restore Databases** > **Restore to another server**.

Alternatively, you can right-click the Oracle server or Oracle home and select **Restore databases** > **Restore to another server**.

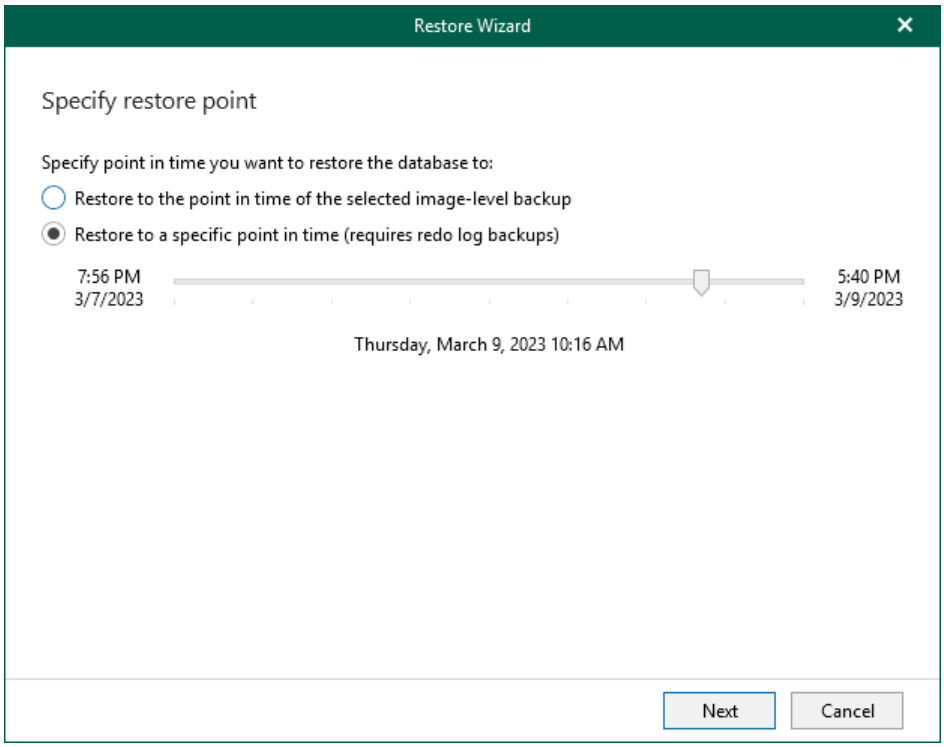


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore the databases:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a necessary point in time.



Step 3. Specify Target Server

At this step of the wizard, specify 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

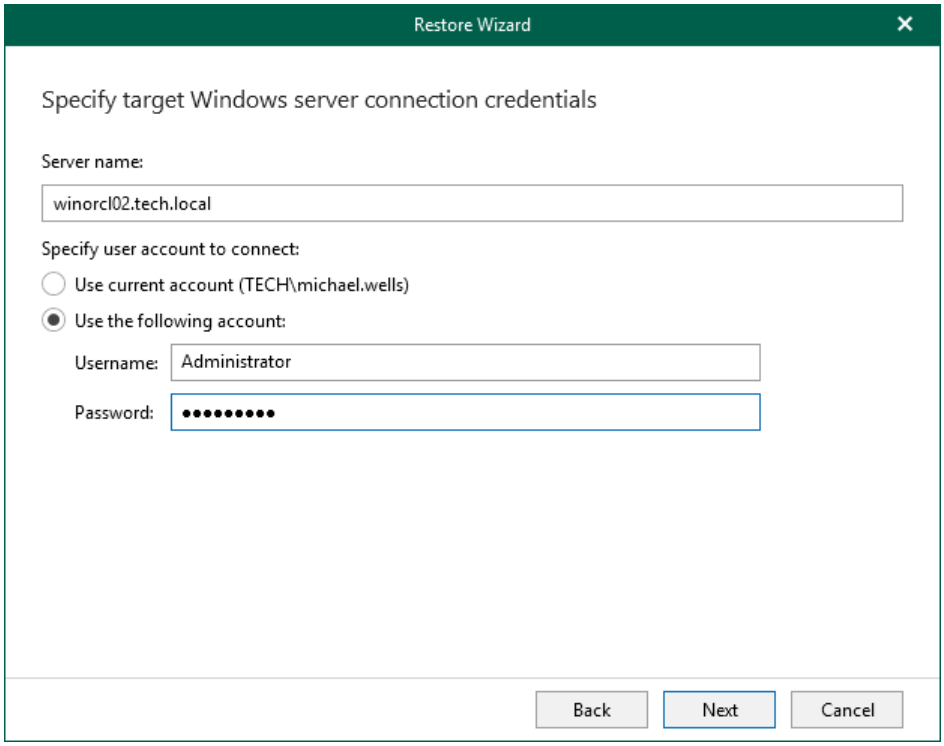
For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the target Oracle server.
2. In the **Specify user account to connect** section, select either of the following options:
   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Oracle is running.

     You cannot use this option if Veeam Explorer for Oracle and mount server are located on separate machines.
   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.

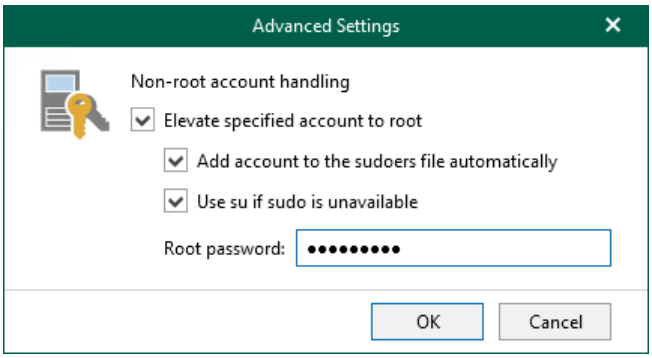


Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

1. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

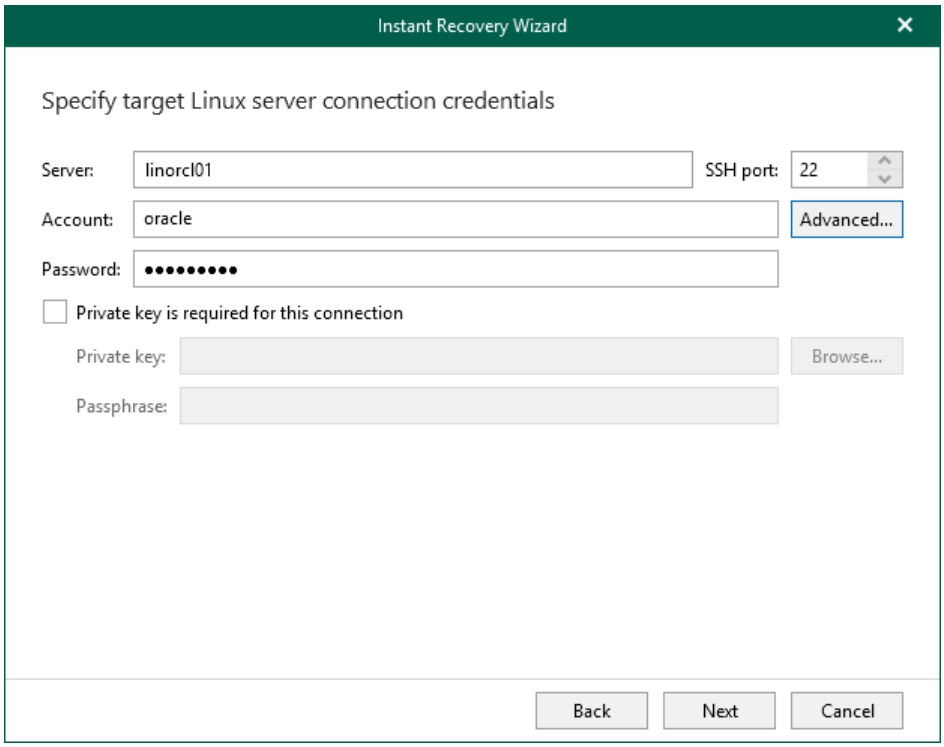
      If you do not enable this option, you will have to manually add the user account to the sudoers file.
   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use su if sudo is unavailable** check box and enter the password for the root account in the **Root password** field.



6. 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.

Consider that the user account must be a member of the **dba** group.

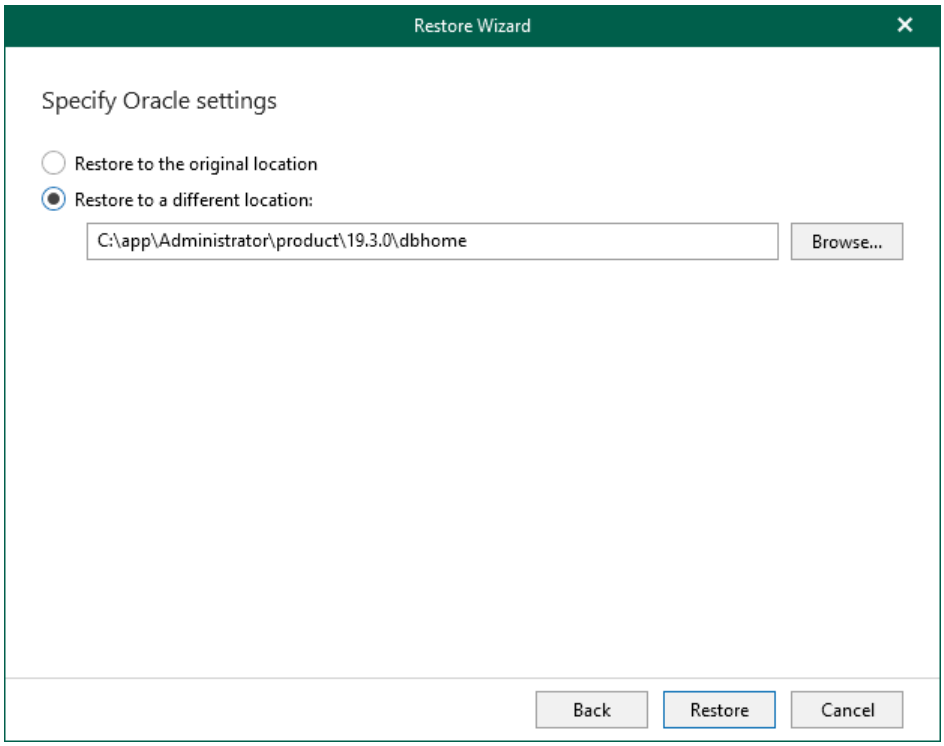


Step 4. Specify Oracle Settings

At this step of the wizard, select a location to which you want to restore databases and launch the restore.

1. At the **Specify Oracle settings** field, select one of the following:
   - **Restore to the original location:** Veeam Explorer for Oracle checks if there are suitable Oracle home directories. If yes, the databases are restored to these home directories. If no, the databases are not restored, and Veeam Explorer for Oracle issues an error that suitable home directories have not been found.
   - **Restore to a different location**: Veeam Explorer for Oracle restores all databases to the custom location. To specify the Oracle home directory, click **Browse** and select a folder that you want to use.
2. Click **Restore**.

> **NOTE**
>
> If the account specified in the previous step is not an Oracle home user, you will be asked to provide a password to access the target Oracle home. Applicable to Oracle 12c and later versions.



Restoring RMAN Backups

This section explains how to restore backups created with Veeam Plug-in for Oracle RMAN. For more information, see the Veeam Plug-in for Oracle RMAN section of the Veeam Plug-ins for Enterprise Applications User Guide.

To restore RMAN backups, do the following:

1. Launch the Restore wizard.
2. Specify the recovery type.
3. Specify the target server.
4. Specify Oracle settings.
5. Specify home user password.
6. Specify point in time.
7. Specify database files location.
8. Configure channel allocation.

Before You Begin

If you want to restore Oracle Real Application Clusters (RAC) or Data Guard databases, consider the following limitations.

Restore of Oracle RAC

To restore RAC databases from RMAN backups, make sure you apply the following restore settings. Otherwise, the databases will be restored as standalone databases.

- **Restore to original server**: You must perform the restore with original name and settings.
- **Restore to another server**:
  - You must perform the restore with original name and settings.
  - Oracle home and Oracle directory structure must remain the same.
  - You must copy the original control file to the target server.
  - For Oracle ASM, the file system structure of the restored database must remain the same.

Restore of Data Guard Databases

In Veeam Backup & Replication 10, Veeam Plug-in for Oracle RMAN has experimental support of Data Guard databases. You can restore Data Guard databases from Veeam Plug-in backups with the following limitations.

- You can restore Data Guard primary databases as primary databases only to original location.

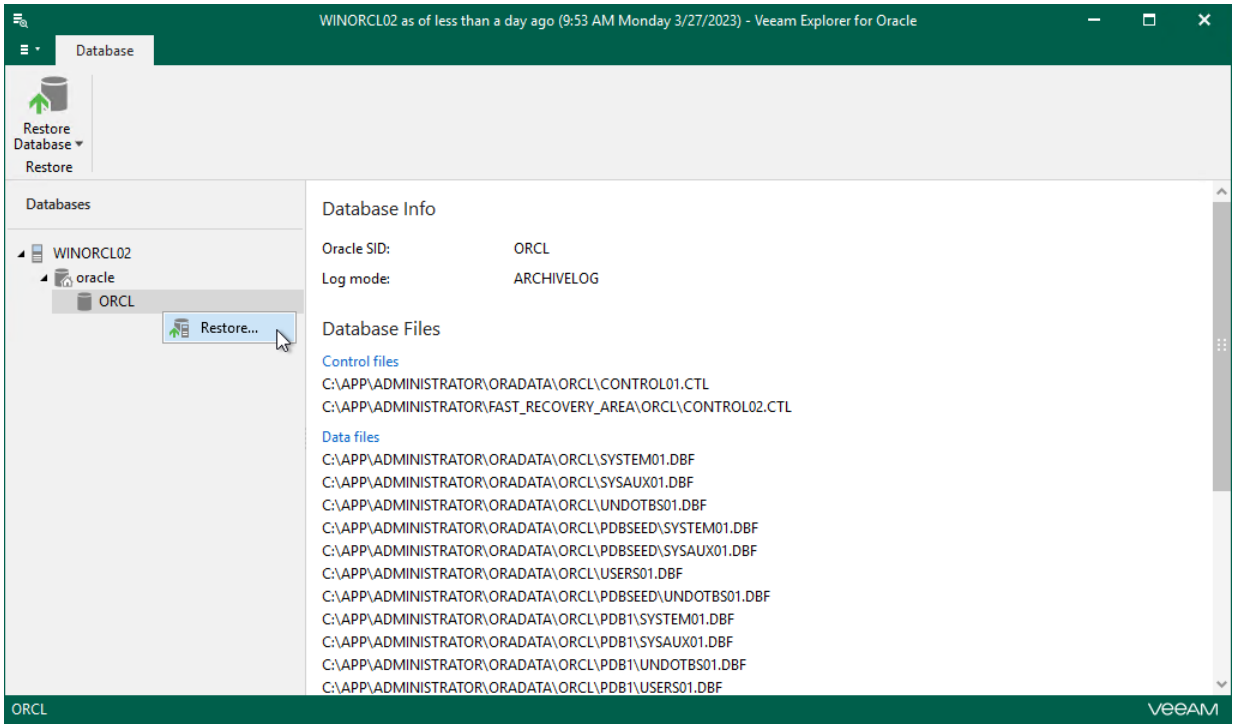
  If you restore primary databases to another server, they will be restored as standalone databases. To convert the standalone database to Data Guard primary database, you can the configuration manually.

- You can restore Data Guard standby databases as standby databases only to original location.

Step 1. Launch Restore Wizard

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

1. Open an RMAN backup, as described in Exploring RMAN Backups.
2. In the navigation pane, select a database.
3. On the **Database** tab, select **Restore Database** > **Restore** or right-click a database and select **Restore**.



Step 2. Specify Recovery Type

At this step of the wizard, select a recovery type:

- **Recover database to specific point in time**

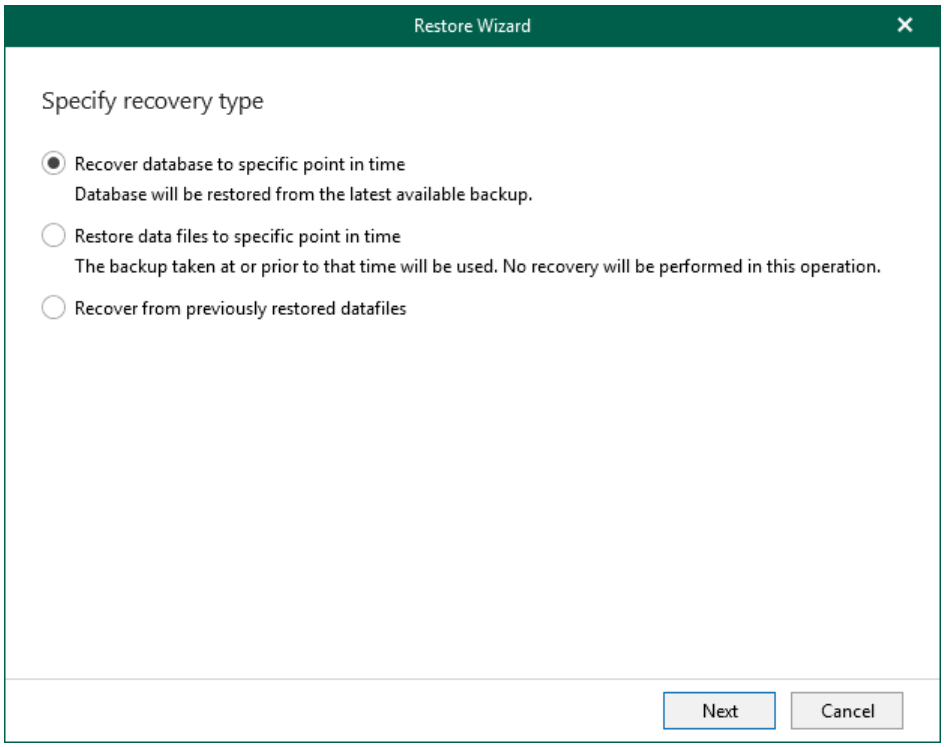
  Select this option to restore databases as of the latest available state.

- **Restore data files to specific point in time**

  Select this option to restore only datafiles as of the specific point-in-time state without applying log files.

- **Recover from previously restored datafiles**

  Select this option to apply log files to restored datafiles.



Step 3. Specify Target Server

At this step of the wizard, specify 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 a Windows-based Oracle server, do the following:

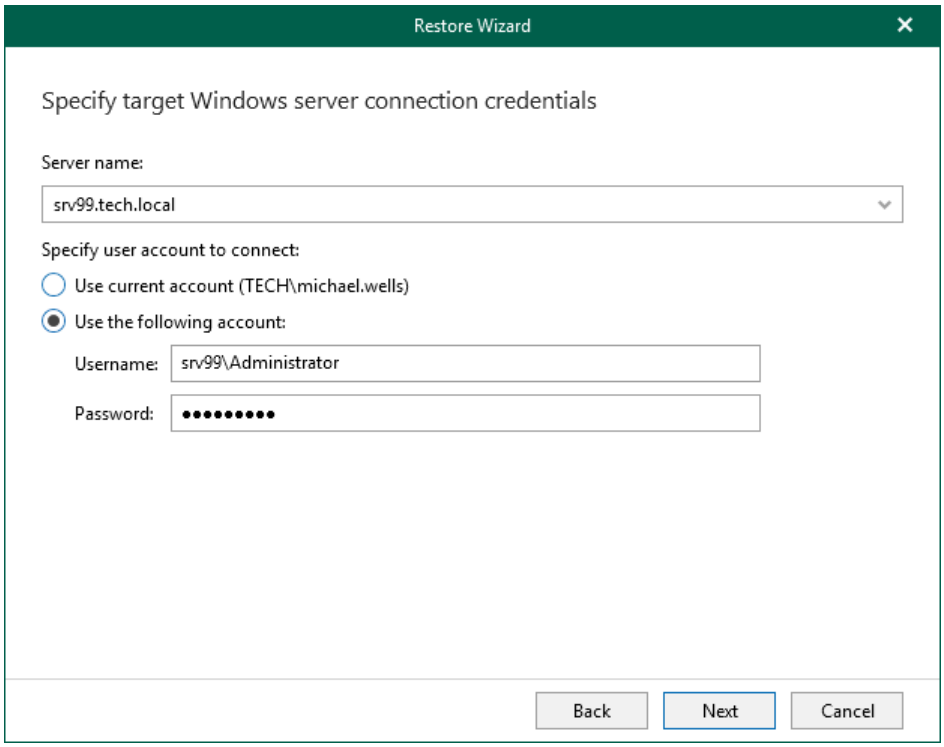
1. In the **Server name** field, specify the name of the Oracle server to which you want to restore data.
2. In the **Specify user account to connect to server** section, select either of the following options:
   - **Use current account**

     Select this option to connect to the specified server using the current user account under which Veeam Explorer for Oracle is running.
   - **Use the following account**

     Select this option to connect to the specified server using a custom user account.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.



Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

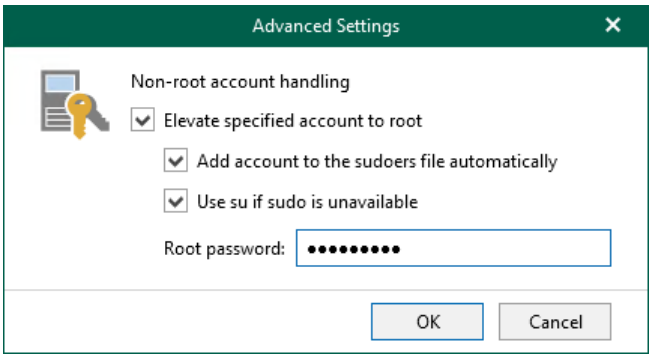
1. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.

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

    d. 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.

    e. 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 is unavailable** check box and enter the password for the root account in the **Root password** field.



6. If a private key is required to connect to the selected server, do the following:

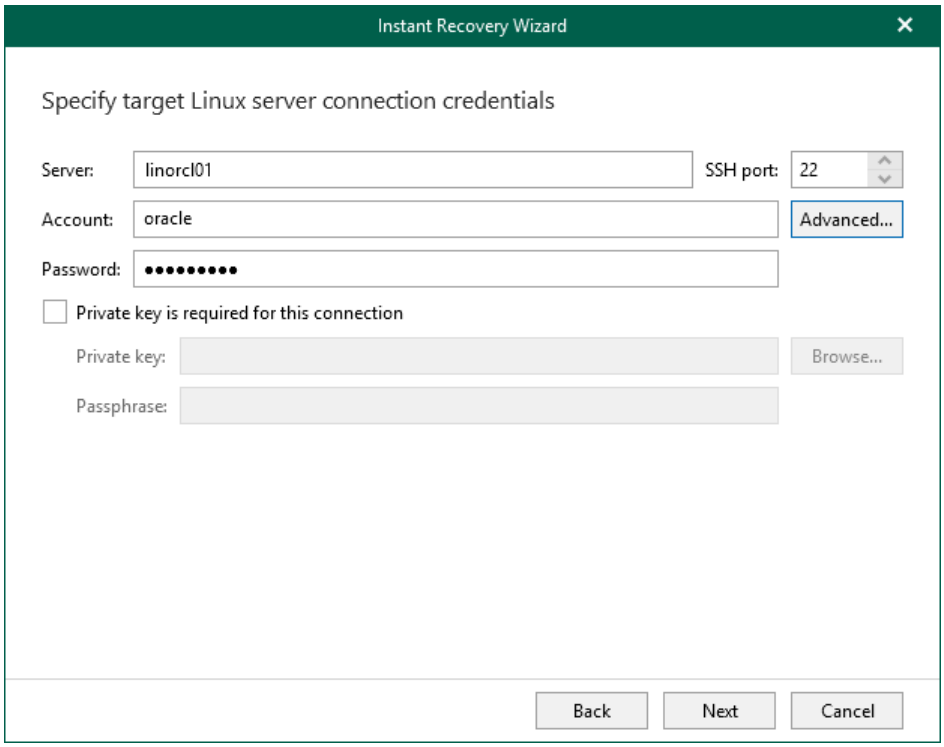
    a. Select the **Private key is required for this connection** check box.

    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.

Consider that the user account must be a member of the **dba** group.



Step 4. Specify Oracle Settings

At this step of the wizard, specify the location to which you want to restore the database.

- Select **Restore with the original name and settings** to restore data using the original name and settings.
- Select **Restore with different name and settings** to choose custom settings:
  a. In the **Oracle home** field, specify the Oracle home directory.

     You can click **Browse** to select a folder.

  b. In the **Global database name** field, specify the global database name as *DB_NAME.DB_DOMAIN*, where:

     - *DB_NAME* is the database name. Oracle limits the length of the database name to 8 characters. If the database name you specify exceeds this limit, Veeam Explorer for Oracle will automatically shorten the database name, and hence the global database name, during the restore process.

       The value you specify is also used for the unique database name (*DB_UNIQUE_NAME*). The unique database name can contain up to 30 characters.

     - *DB_DOMAIN* is the domain name of the database. It does not count towards any character limits and Veeam Explorer for Oracle does not shorten it during the restore process.

     For example, if you specify the global database name as *orcl_restored.tech.local*, Veeam Explorer for Oracle will shorten it to *orcl_res.tech.local*. The database name will be *orcl_res*, while the unique database name will be *orcl_restored.*

     The **Global database name** field is available only if you have selected the **Recover database to specific point in time** option at the Specify Recovery Type step.

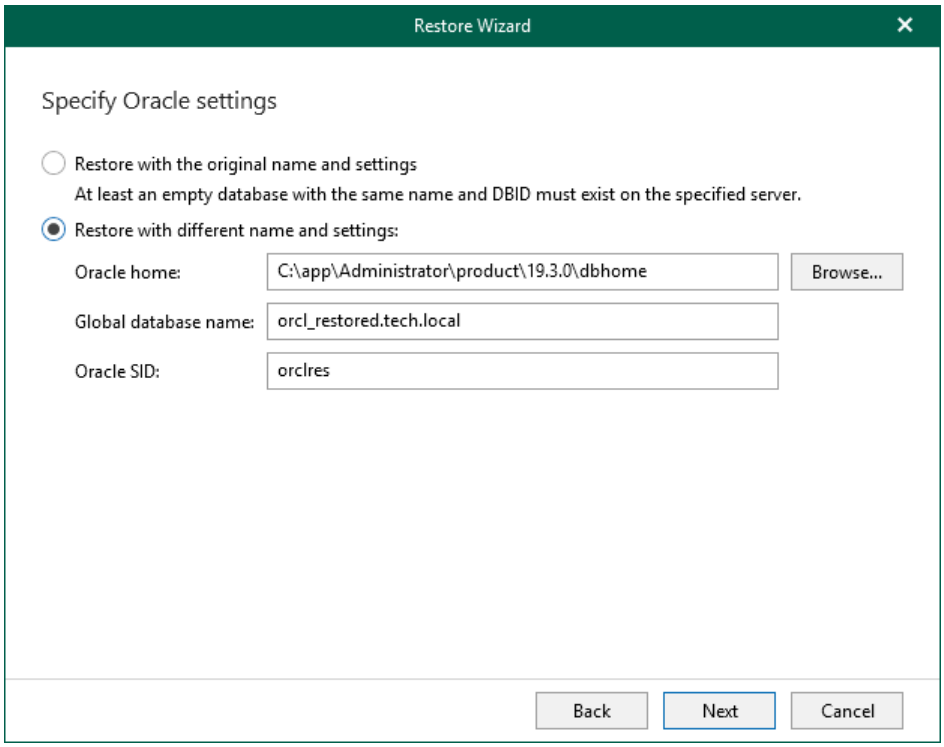
  c. In the **Oracle SID** field, specify the database system identifier. The **Oracle SID** field is automatically filled with the value entered in the **Global database name** field, but you can also assign a different value.

     The maximum length of the Oracle SID is 12 characters and it can only contain alphanumeric characters (a-z, A-Z and 0-9).

NOTE

Consider the following:

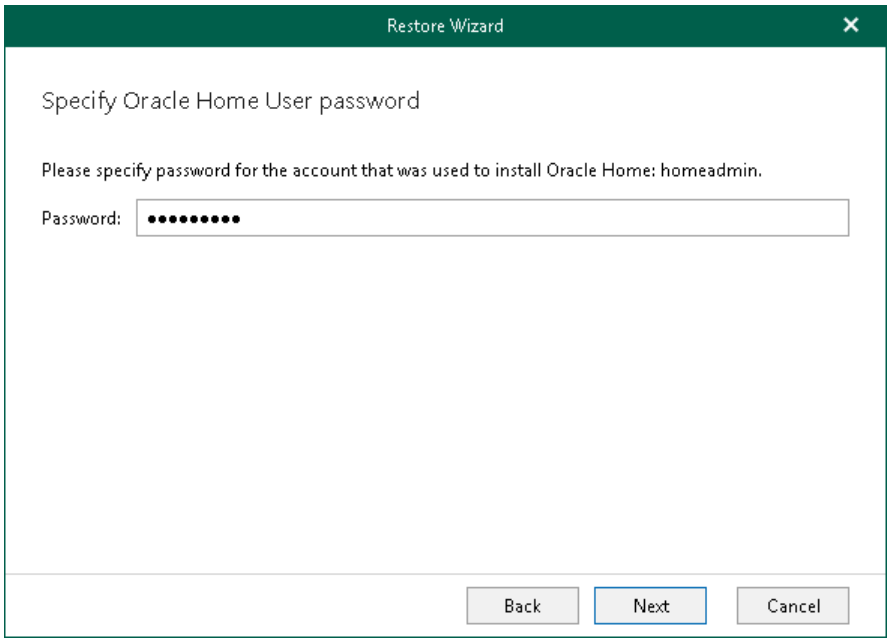
- To use the **Restore with different name and settings** option, make sure that *Controlfile Autobackup* is enabled. For more information, see the Oracle Environment Planning section of the Veeam Plug-in for Oracle RMAN User Guide.
- An existing Oracle SID (if any) will be replaced with that from the backup when selecting the **Restore with different name and settings** option.



Step 5. Specify Home User Password

This step of the wizard is available if the account specified in Specify Target Server is not the Oracle home user.

At this step of the wizard, specify the password for the *Oracle home* user.



Step 6. Specify Point in Time

At this step of the wizard, do the following:

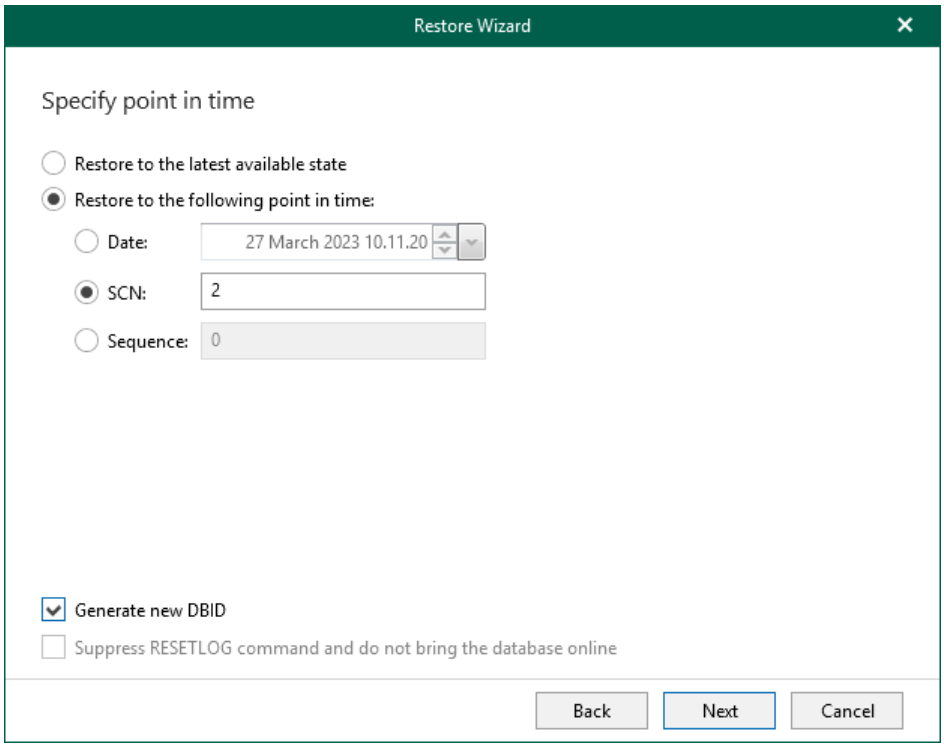
- Select the **Restore to the latest available** option to restore data as of the latest available state.
- Select the **Restore to the following point in time** option to select a state as of which you want to restore data:
  - **Date**. Select a date as of which you want to restore data.
  - **SCN**. Specify SCN (System Change Number).
  - **Sequence**. Specify the sequence.
- Select the **Generate new DBID** check box to generate a new DBID in addition to the new database name.

  This check box is available only when using the **Restore with different name and settings** option at the Specify Oracle Settings step.
- Select the **Suppress RESETLOG command and do not bring the database online** check box to skip the OPEN RESETLOGS operation if it was required by the database. The database in this case remains in the *mount* state.

  This check box is available only when using the **Restore with the original name and settings** option at the Specify Oracle Settings step.

TIP

For more information, see the Oracle documentation.



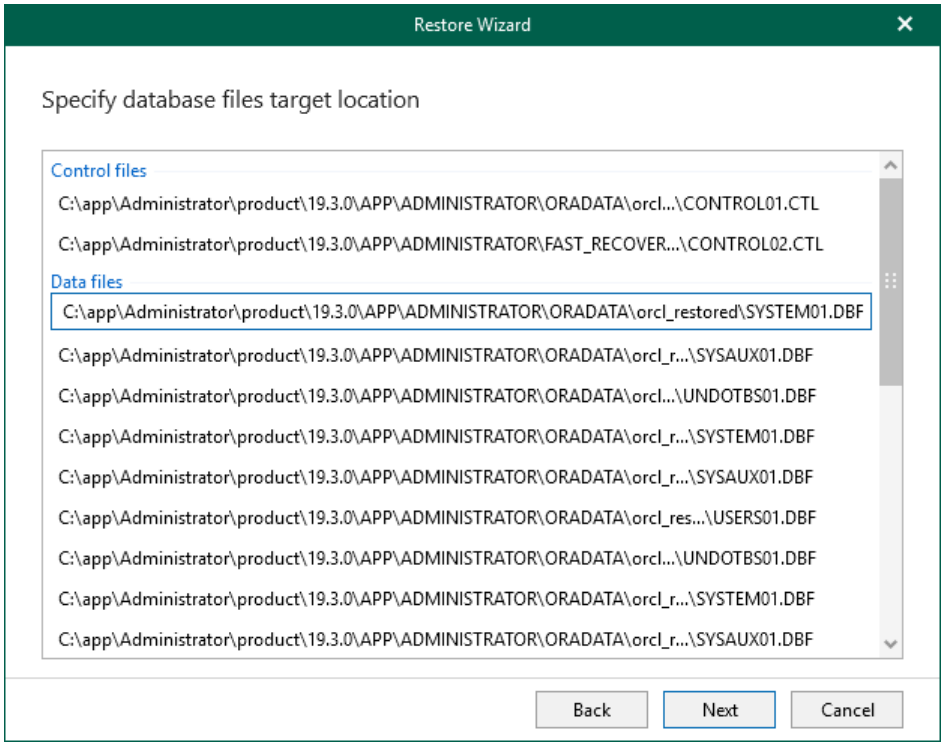
Step 7. Specify Database Files Location

At this step of the wizard, specify the location to which you want to restore data files.

Consider the following:

- When restoring with the **Restore with the original name and settings** option, only the location for *Data files* will be available for editing.
- When restoring with the **Restore with different name and settings** option, the location for the following files will be available for editing:
  - *Control files*
  - *Data files*
  - *Log files*
  - *Temp files*

To change the location, click the path row and specify the path.



Step 8. Configure Channel Allocation

At this step of the wizard, specify channels allocation.

Channels are used to restore data in multiple threads per session. Using multiple threads allows Veeam Explorer for Oracle to reduce the amount of time needed to complete restore sessions. For more information about allocating channels, see the Oracle documentation.

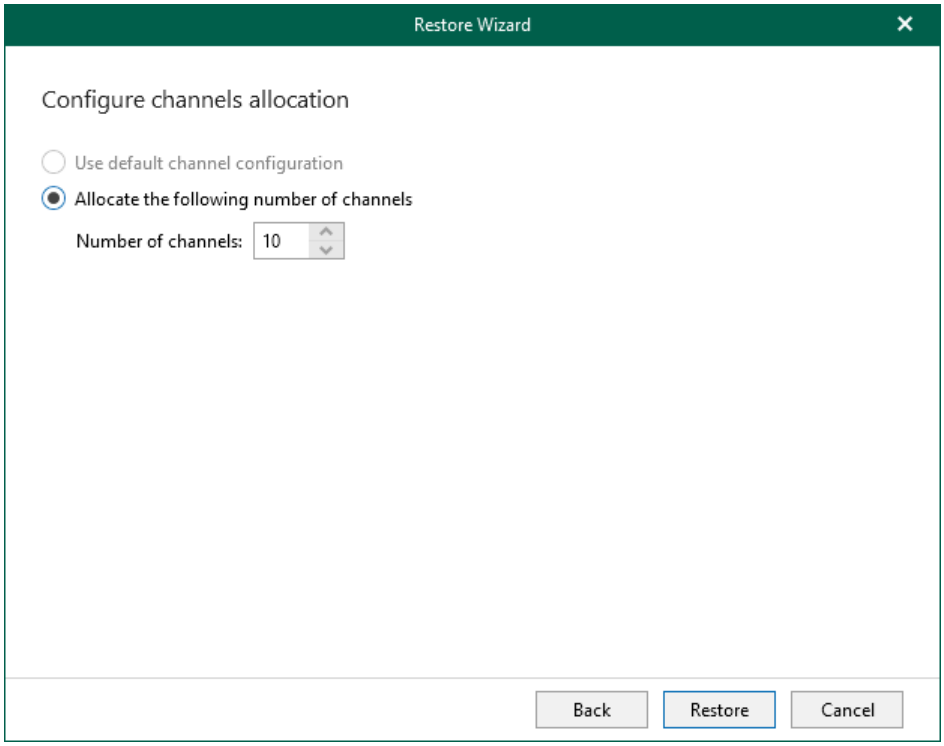
The following options are available:

- **Use default channel configuration**

  Select this option to use the default channel configuration defined in the RMAN plug-in settings.

- **Allocate the following number of channels**

  Select this option to specify the number of channels to be used when restoring your data.



Data Publishing

Publishing an Oracle database allows you to temporarily attach the databases to the target Oracle server without launching restore. Publishing typically occurs faster than using standard restore features and could be convenient when, for example, your time to perform disaster-recovery operations is limited.

After you have launched a publishing operation to an Oracle server, you can quickly republish the latest or point-in-time state of the database to the same server.

During publishing, Veeam Explorer for Oracle takes the following actions:

1. Mounts VM disks from the backup file to the target Oracle server.

   Mounting is done to the `C:\VeeamFLR` directory for Windows-based servers and the `/tmp` directory for Linux-based servers.

2. Retrieves required database files.

3. Attaches associated databases directly to the target Oracle server so that you can perform required operations using Oracle tools.

Before publishing data, read the Considerations and Limitations section.

Publishing to Specified Server

To publish a database to the specified Oracle server, do the following:

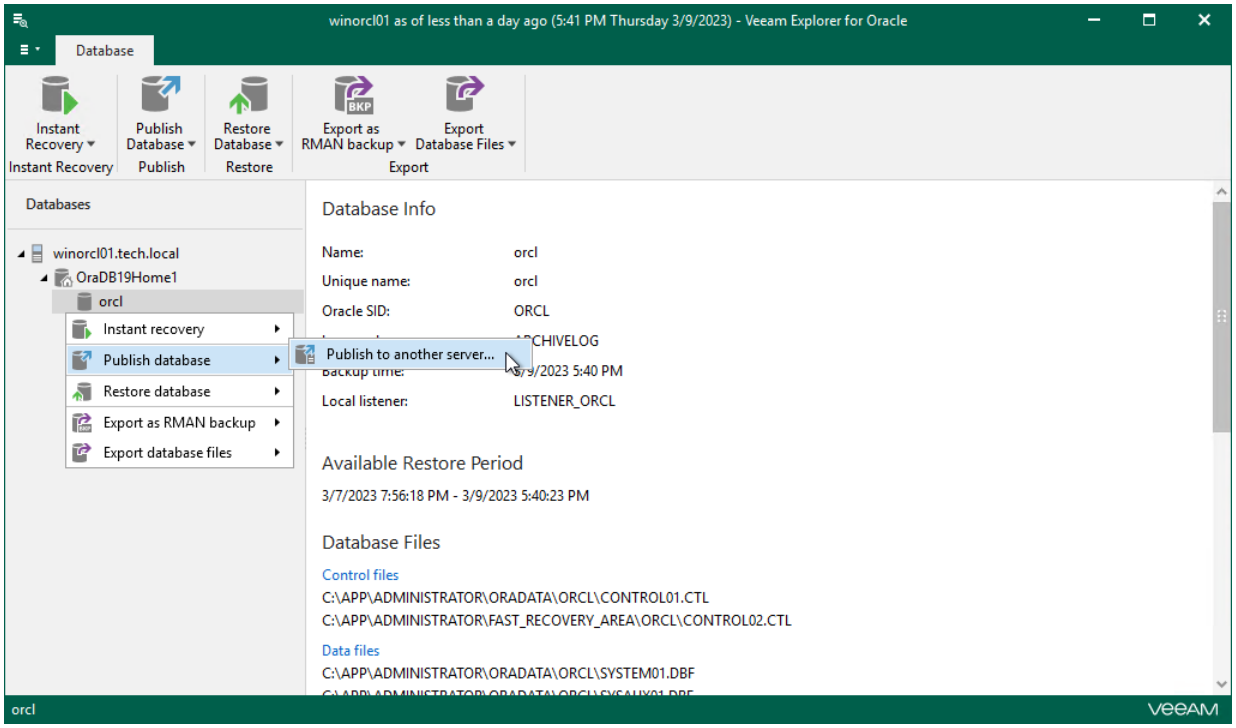
1. Launch the Publish wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target Oracle server.
5. Specify Oracle settings.

Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish to another server**.

Alternatively, you can right-click a database and select **Publish database** > **Publish to another server**.



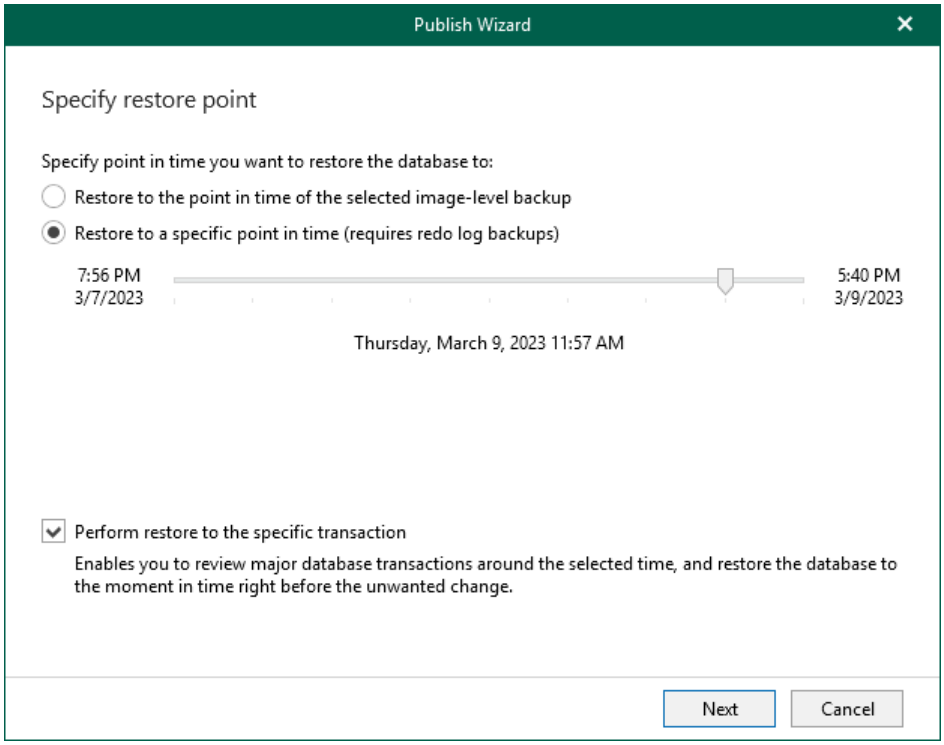
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

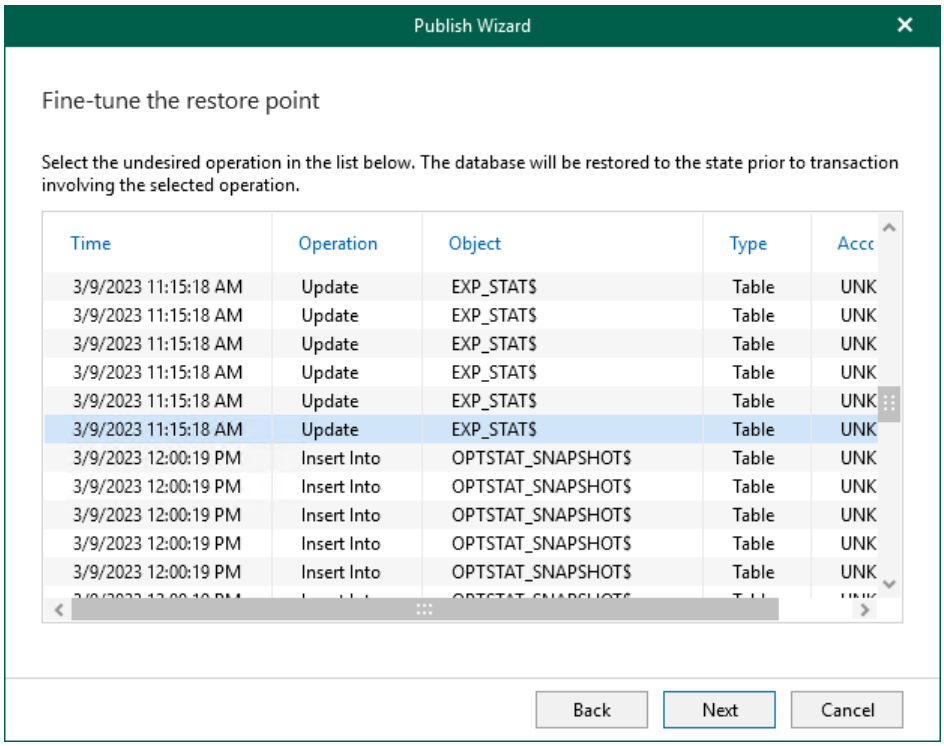
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Oracle Server

At this 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

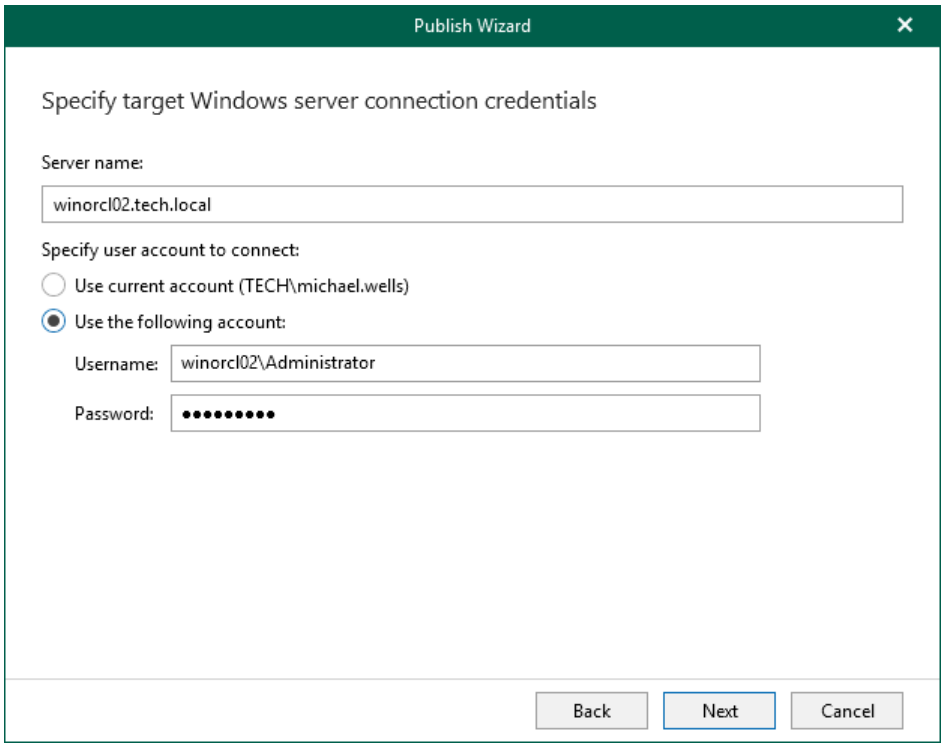
For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the target Oracle server.
2. In the **Specify user account to connect** section, select either of the following options:
   - **Use current account**. Select this option to connect to the specified server using the account under which Veeam Explorer for Oracle is running.

     You cannot use this option if Veeam Explorer for Oracle and mount server are located on separate machines.
   - **Use the following account**. Select this option to connect to the specified server using a custom user account. Then provide a user name and password for the account.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.

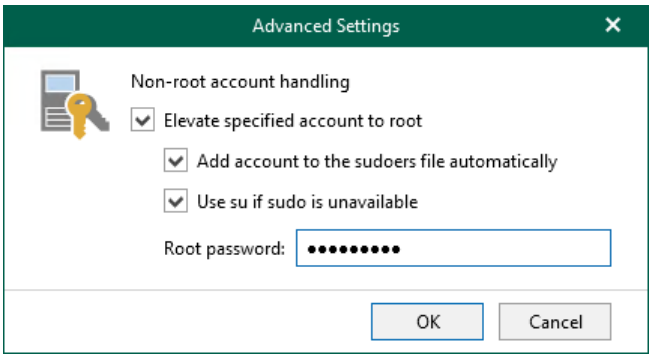


Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

1. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
2. In the **SSH port** field, specify the port number of the selected Oracle server.
3. In the **Account** filed, specify an account under which to connect to the specified server.
4. In the **Password** field, enter the password.
5. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

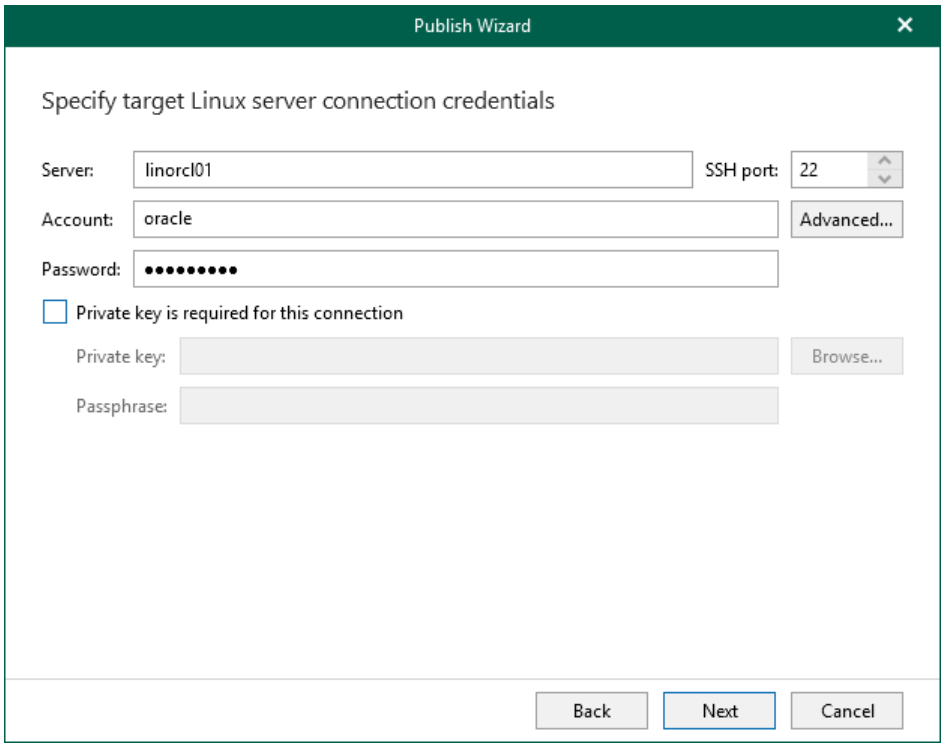
      If you do not enable this option, you will have to manually add the user account to the sudoers file.
   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use su if sudo is unavailable** check box and enter the password for the root account in the **Root password** field.



6. 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.

Consider that the user account must be a member of the **dba** group.



Step 5. Specify Oracle Settings

At this step of the wizard, specify the location to which you want to restore the database.

- Select **Restore to the original location** to publish the database to the original location.
- Select **Restore to a different location** to publish the database to a custom location.

  a. **In the Oracle home field, specify the Oracle home directory**. To locate the Oracle home directory, click **Browse** and select the folder you want to use.

  b. In the **Global database name** field, specify the global database name as *DB_NAME.DB_DOMAIN*, where:

     - *DB_NAME* is the database name. Oracle limits the length of the database name to 8 characters. If the database name you specify exceeds this limit, Veeam Explorer for Oracle will automatically shorten the database name, and hence the global database name, during the publishing process.

       The value you specify is also used for the unique database name (*DB_UNIQUE_NAME*) of the published database. The unique database name can contain up to 30 characters.

     - *DB_DOMAIN* is the domain name of the database. It does not count towards any character limits and Veeam Explorer for Oracle does not shorten it during the publishing process.

     For example, if you specify the global database name as *orcl_published.tech.local*, Veeam Explorer for Oracle will shorten it to *orcl_pub.tech.local*. The database name of the published database will be *orcl_pub*, while the unique database name of the published database will be *orcl_published.*

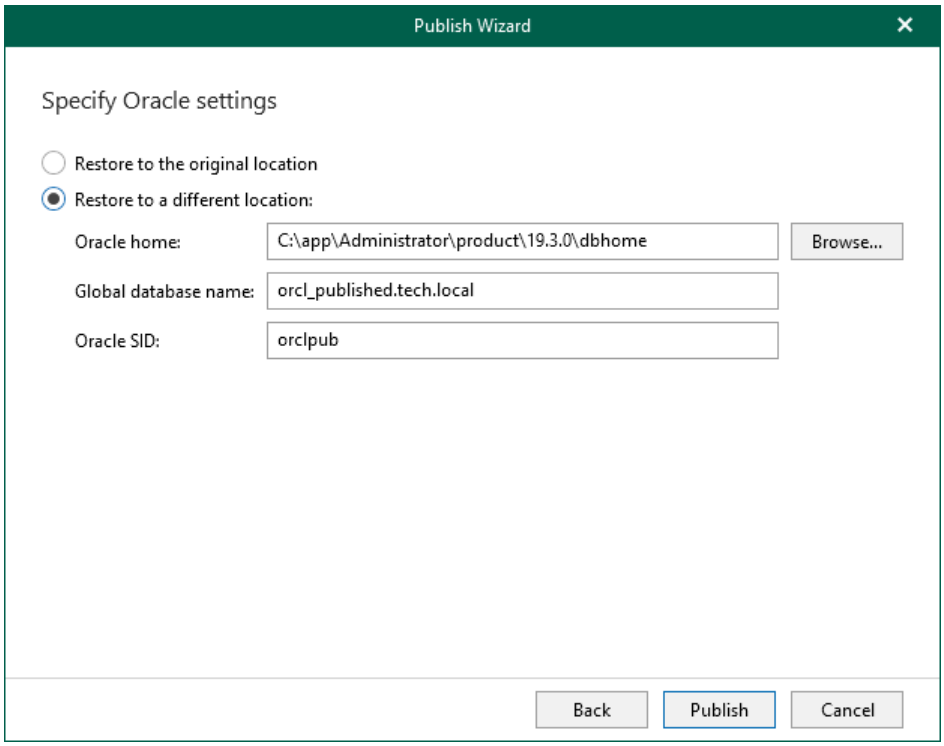
  c. In the **Oracle SID** field, specify the database system identifier. The **Oracle SID** field is automatically filled with the value entered in the **Global database name** field, but you can also assign a different value.

     The maximum length of the Oracle SID is 12 characters and it can only contain alphanumeric characters (a-z, A-Z and 0-9).

After you complete this step, a new **Published databases** node appears at the top of the navigation pane in Veeam Explorer for Oracle. Under this node you can find the databases that have been published during the current session.

NOTE

If the account specified in Specify Target Oracle Server is not the Oracle home user, you will be asked to provide a password to access the target Oracle home. Applicable to Oracle 12c and later versions.



Publishing Latest or Point-in-Time State

After you have launched a publishing operation to an Oracle server (as described in Publishing to Specified Server), you can quickly republish a state of the Oracle database to the same server.

You can republish either of the following states:

- The latest available state — to publish data as of the latest state in the backup file.
- A point-in-time state — to publish data as of the selected point-in-time state. This option is available only if backups of Oracle archive logs exist. For more information, see Required Backup Job Settings.

When you unpublish a database, both options continue to remain until you close the application so that you can quickly republish a database if required.

Publishing Latest State

Veeam Explorer for Oracle allows you to republish an unpublished database anew. When republishing a database, it will be attached to the target Oracle server as of the latest available state.

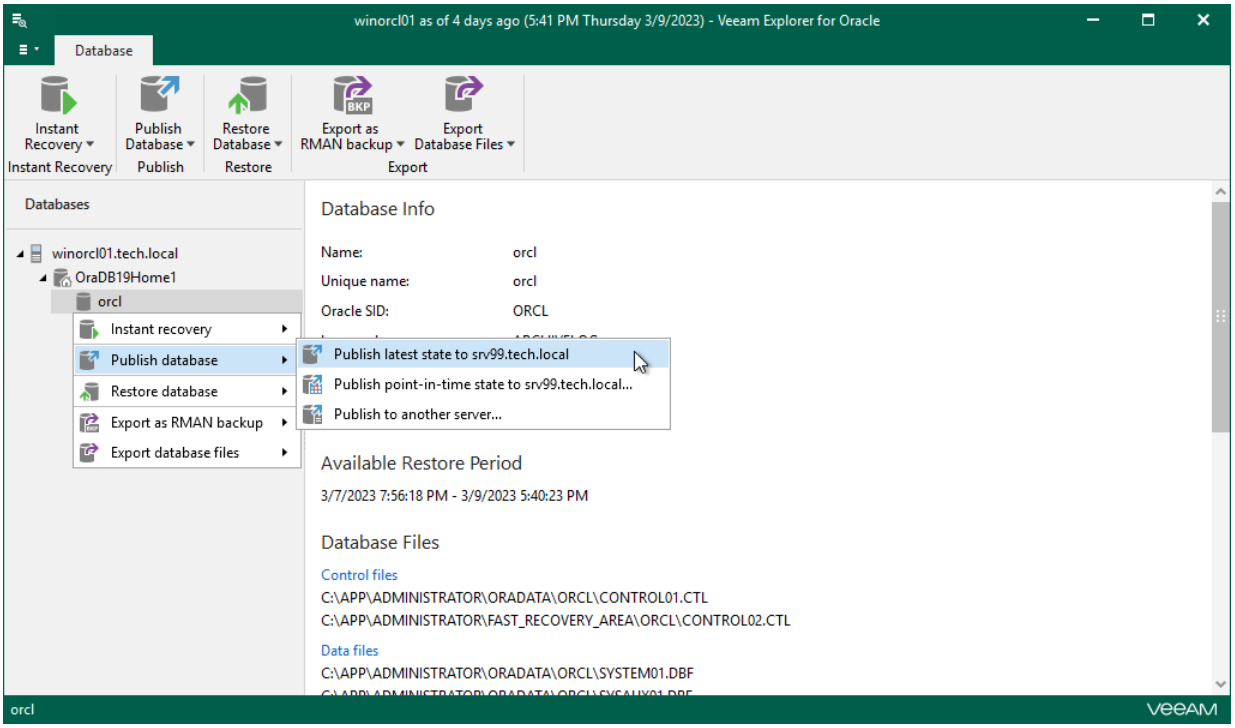
To republish a database as of the latest state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish latest state to <target_server>**.

Alternatively, you can right-click a database and select **Publish database** > **Publish latest state to <target_server>**.

> **NOTE**
>
> The name of the publish option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Publish latest state to <target_server>**.
> - If you select any other restore point, the option name is displayed as **Publish state of <point_in_time> to <target_server>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



Publishing Point-in-Time State

Publishing a point-in-time state allows you to load a required database state and unroll specified transactions if needed.

To publish a database as of the point-in-time state, do the following:

1. Launch the Publish wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

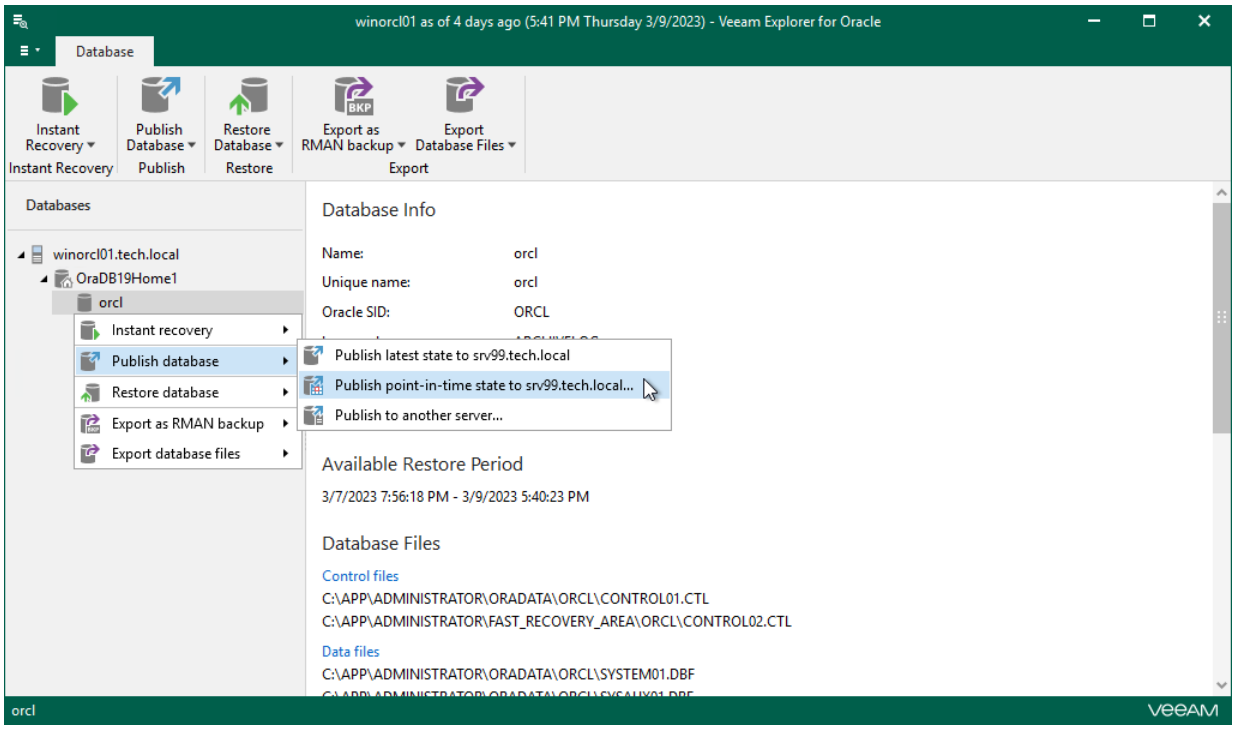
Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Publish Database** > **Publish point-in-time state to <server_name>**.

Alternatively, you can right-click a database and select **Publish database** > **Publish point-in-time state to <server_name>**.

Once completed, the database will be published with the same name as it was during the initial publishing session.



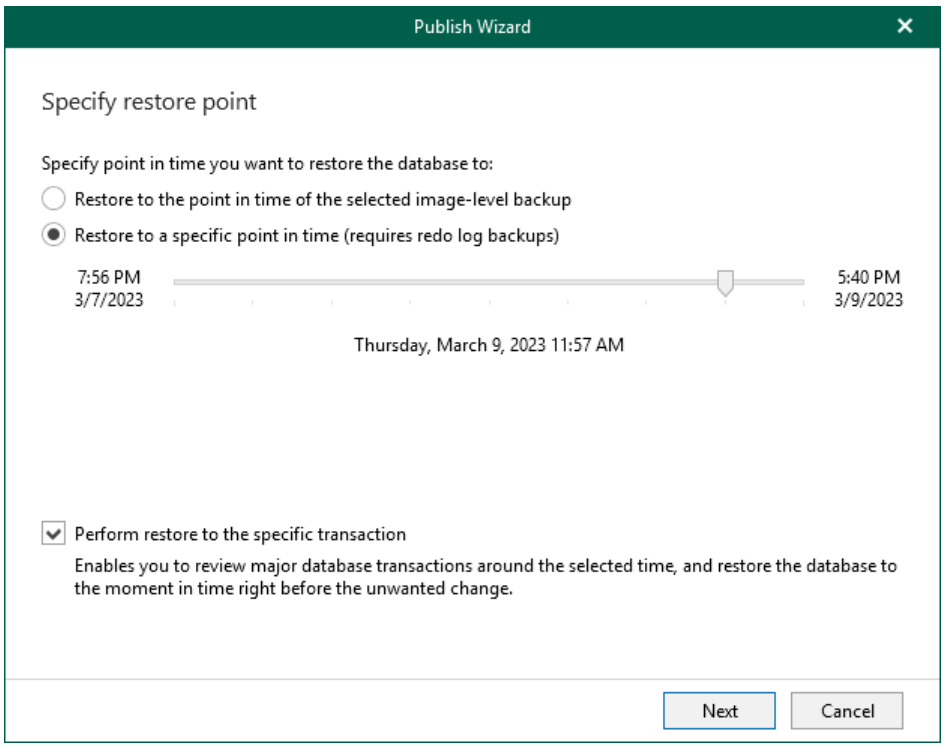
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to publish your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

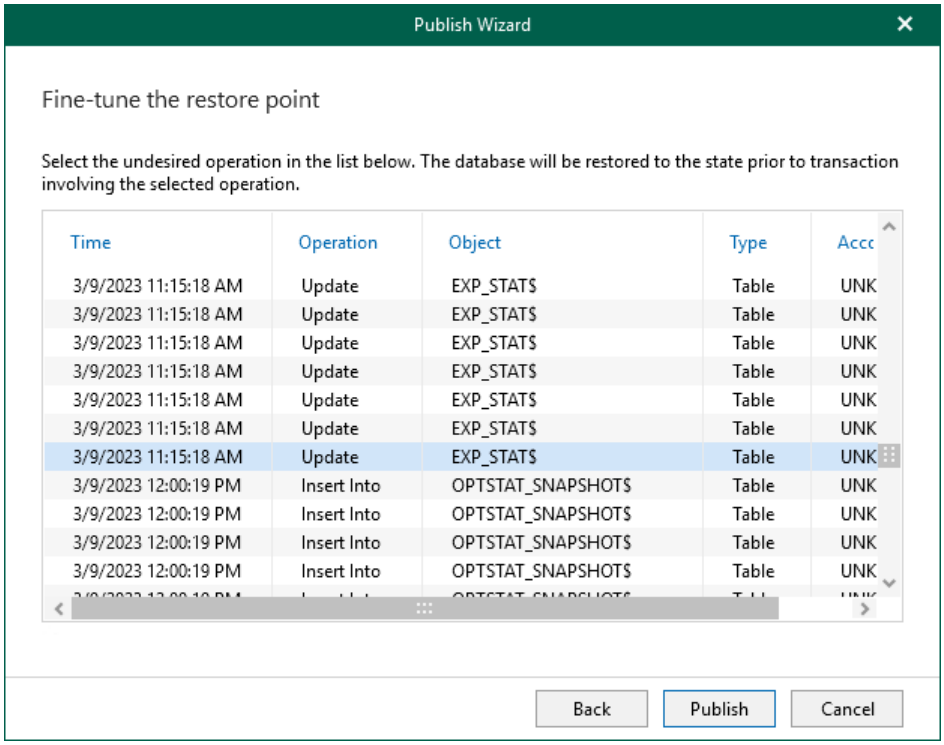
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to publish your database and click **Publish**.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Unpublishing Databases

Once you are finished working with published databases, you may want to unpublish (detach) these databases from the target Oracle server.

Detachment occurs in the following manner:

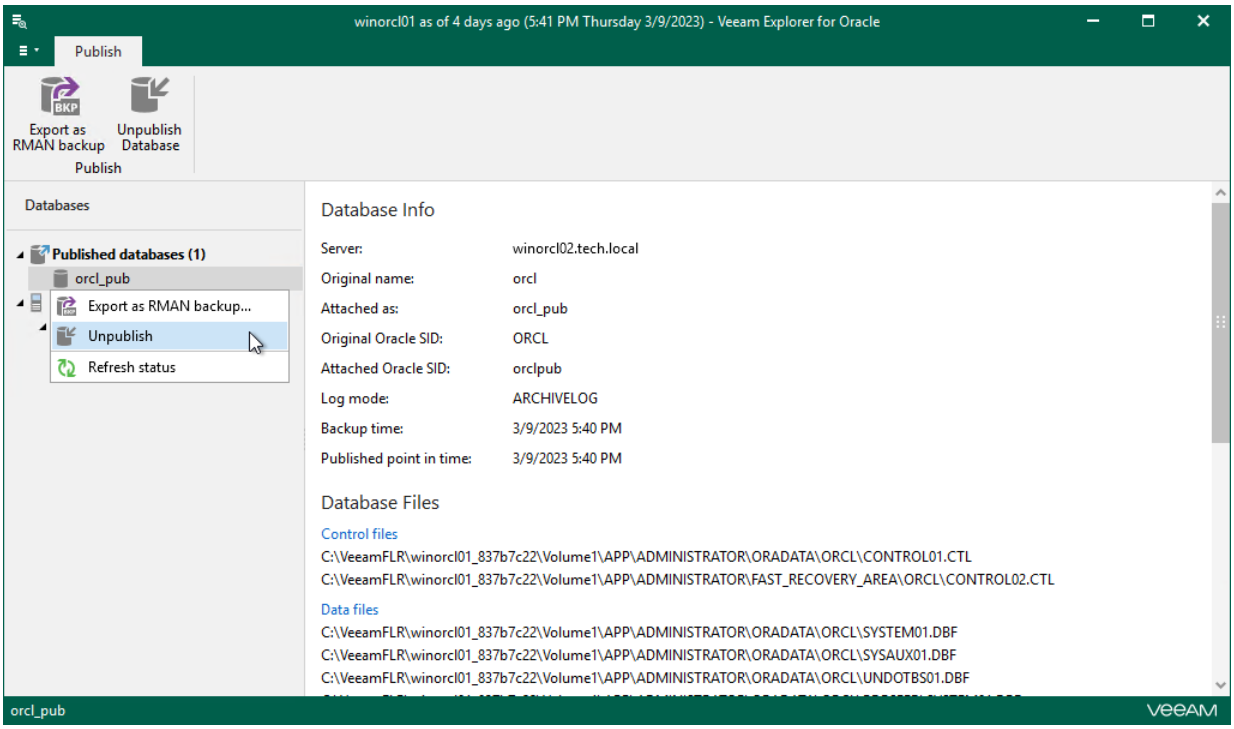
- Upon closing the Veeam Explorer for Oracle console, all published databases will be detached from the target Oracle server automatically. Mount points will be also dismounted from under the `C:\VeeamFLR` directory for Windows-based servers and the `/tmp` directory for Linux-based servers.
- On manual unpublishing, databases will be detached at once but the restore point will remain mounted on the target server for the next 15 minutes.

To unpublish a database manually, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Unpublish Database**.

Alternatively, in the navigation pane, right-click a published database and select **Unpublish**.

To detach more than one published database simultaneously, right-click the root **Published databases** node and select **Unpublish databases** or select the root **Published databases** node and click **Unpublish Databases** on the **Publish** tab.



Exporting as RMAN Backup

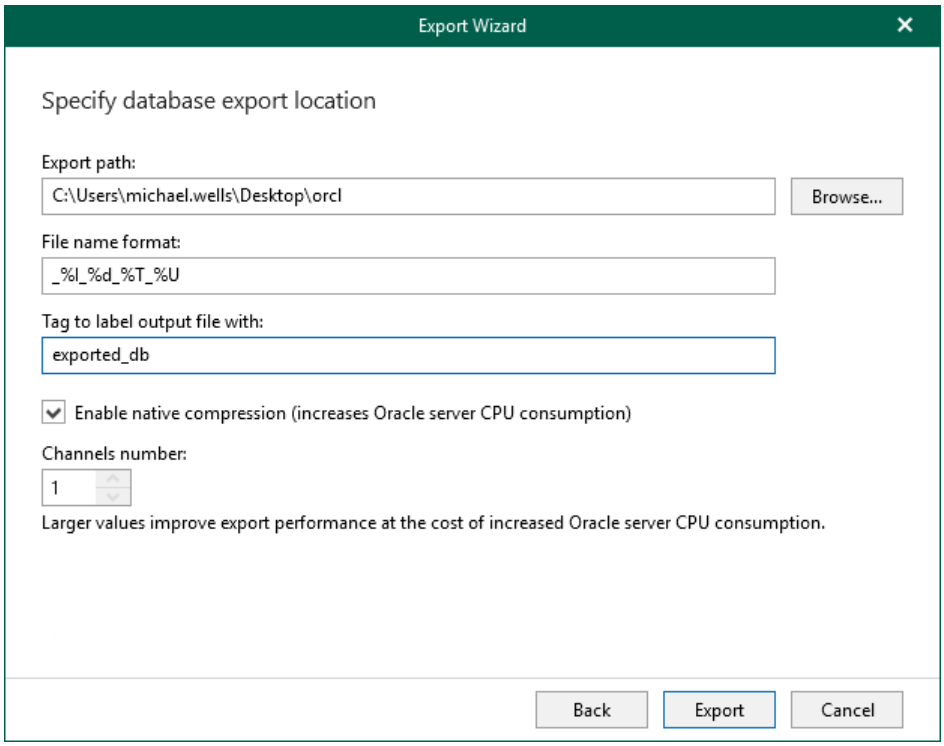
Once published, the database can be exported as an RMAN backup so that you can save the changes you may have made on the target server. For example, after publishing a database, you may have added a column or alter some values. To save these modifications before you unpublish the database, you can use the export feature.

To export a database, do the following:

1. In the navigation pane, under the **Published databases** node, select a published database.
2. On the **Publish** tab, select **Export as RMAN backup** or right-click a published database and select **Export as RMAN backup**.
3. In the **Export** wizard, in the **Export path** field, specify the location to which you want to export database files.

   If the folder you are specifying does not exist, it will be created.
4. In the **File name format** field, specify the format according to which your files will be named after the export.

   For more information, see this Oracle article.
5. In the **Tag to label output file with** field, specify a new tag name.
6. To compress files using native Oracle compression, select the **Enable native compression** check box.
7. In the **Channels number** numeric field, specify the number of channels to be used when retrieving Oracle databases from the backup.
8. Click **Export**.

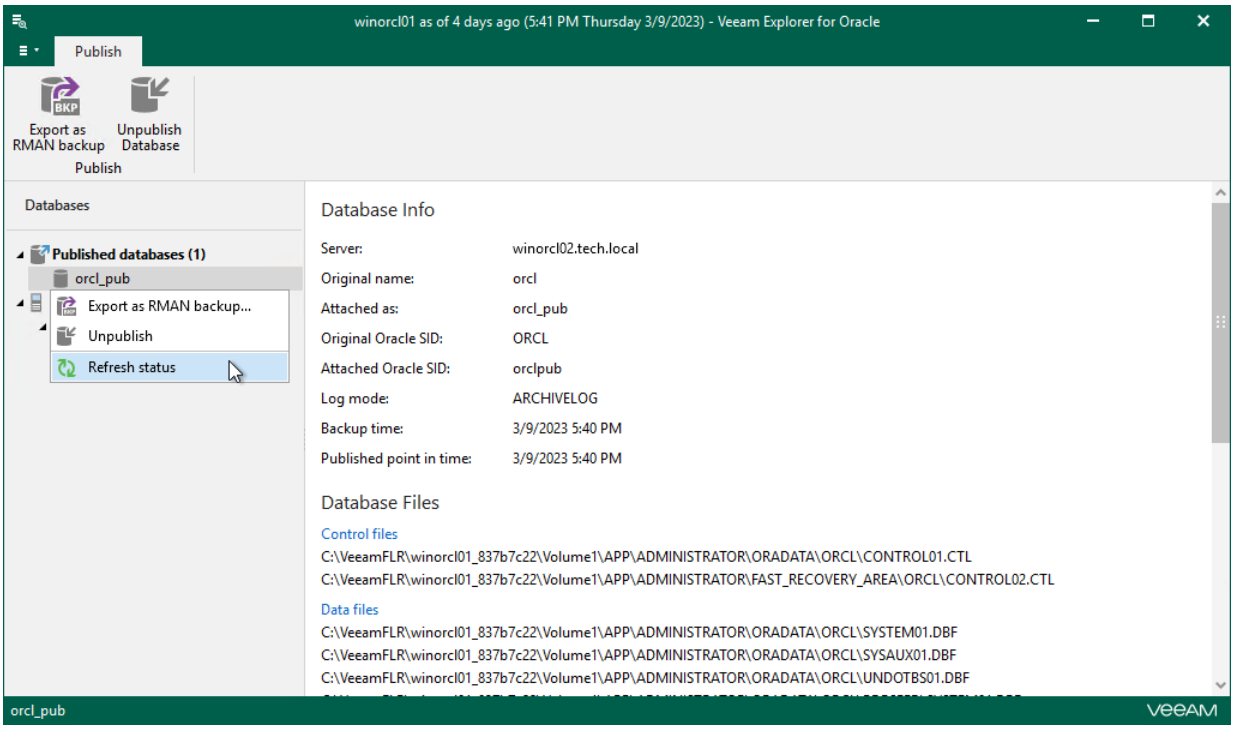


Refreshing Database Status

While databases are attached to the target Oracle server, Veeam Explorer for Oracle synchronizes each published database state to verify its availability. By default, synchronization occurs every five seconds.

If something went wrong with any of the published databases, the question mark appears next to each of such databases indicating the database unavailability. In the **Database Info** section, you will also see the notification message describing the problem.

To refresh a published database state manually, in the navigation pane, under the **Published databases** node, right-click a published database and select **Refresh status**.



Instant Recovery

Instant recovery combines capabilities of the data restore and data publishing features. If you want the database to be online as quickly as possible, you can use the **Instant Recovery** option and restore it in the background.

Before performing instant recovery, read the Considerations and Limitations section.

How It Works

To perform instant recovery, Veeam Explorer for Oracle uses the *Veeam Explorers Recovery Service*. The service is installed on the backup server and every mount server deployed in the backup infrastructure, and runs in the background. During instant recovery, Veeam Explorer for Oracle uses the service running on the mount server associated with the backup repository. This removes the necessity to keep Veeam Explorer for Oracle running during an entire instant recovery session. Once you have started an instant recovery session, you can close Veeam Explorer for Oracle and then launch it later when necessary.

When you start the instant recovery session in Veeam Explorer for Oracle, the following happens:

1. Veeam Explorer for Oracle uses backup files to publish the database on the target production server directly from backup.
2. While the published database is online, Veeam Explorer for Oracle starts to create a copy of the database on the target Oracle server.
3. All changes in database files that occur after publishing are saved in cache.

   [For Windows-Based Oracle server] The instant recovery write cache is stored on the mount server. You can view and change the write cache location in the mount server settings. For more information, see the Specify Mount Server Settings section of the Veeam Backup & Replication User Guide.

   [For Linux-Based Oracle server] The instant recovery write cache is stored on the target server.
4. After all database files are copied to the target server, Veeam Explorer for Oracle uses archived redo logs to synchronize changes in database files.
5. After synchronization, you can switch over to the up-to-date copy of the database on the production server. Depending on the option you choose, switchover starts in one of the following ways:
   - Automatically, immediately after synchronization
   - Automatically, according to a specified schedule
   - Manually

   During switchover, Veeam Explorer for Oracle does the following:

   a. Stops the published database.

   b. Uses redo logs to synchronize differences between the published database and the copied database files.

   c. Drops the published database.

   d. Starts the recovered database.

Instant recovery session is resilient to network disruption, backup server or mount server crash. If anything disrupts the restore process, the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch retry after the server or network is up.

Instant Recovery of Multiple Databases

You can you Veeam Explorer for Oracle to perform instant recovery of multiple databases hosted on a server or a certain Oracle server. You can perform instant recovery to the original server or to any other server in your network where Oracle Database is installed.

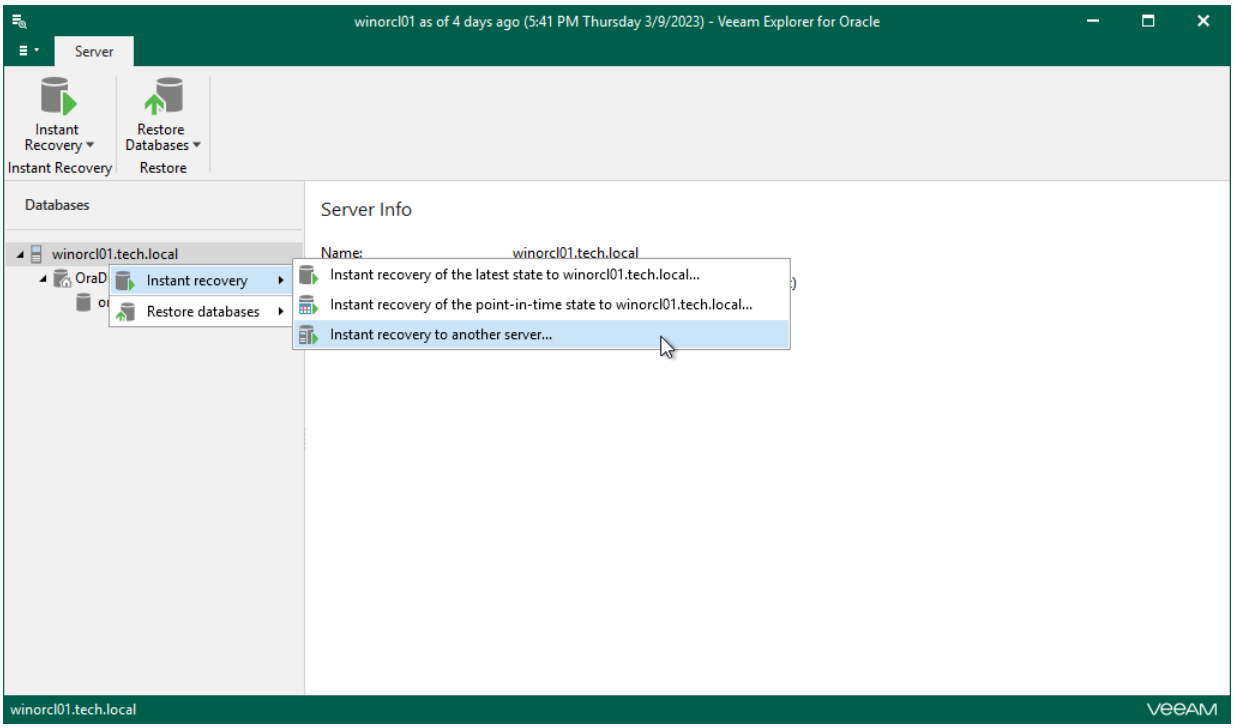
To perform instant recovery of multiple databases, do the following:

1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Specify the target server.
4. Specify Oracle settings.
5. Specify switchover settings.
6. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

To perform instant recovery of multiple databases, do the following:

1. In the navigation tree of Veeam Explorer for Oracle, select a server or Oracle home.
2. On the **Server** or the **Oracle Home** tab, select one of the following options:
   - **Instant Recovery** > **Instant Recovery of the latest state to** ***<original server>*** or right-click the server or Oracle home and select **Instant recovery** > **Instant recovery of the latest state to** ***<original server>***.
   - **Instant Recovery** > **Instant Recovery of the point-in-time state to** ***<original server>*** or right-click a server or Oracle home and select **Instant recovery** > **Instant recovery of the point-in-time state to** ***<original server>***.
   - **Instant Recovery** > **Instant Recovery to another server** or right-click a server or Oracle home and select **Instant recovery** > **Instant recovery to another server**.



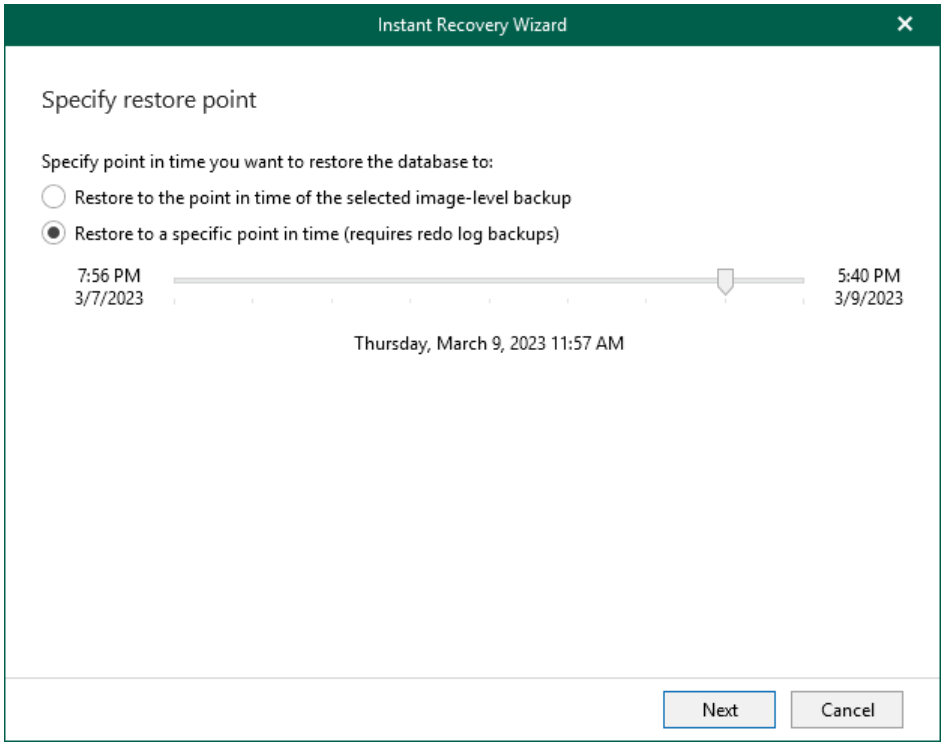
Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  Use the slider to choose a required point in time.

> **NOTE**
>
> If you have selected to perform instant recovery of databases latest state to original server, skip this step and go to Specify Switchover Settings.



Step 3. Specify Target Server

The **Specify Target Server** step of the wizard is available if you select the instant recovery to another server option.

At this step, 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.

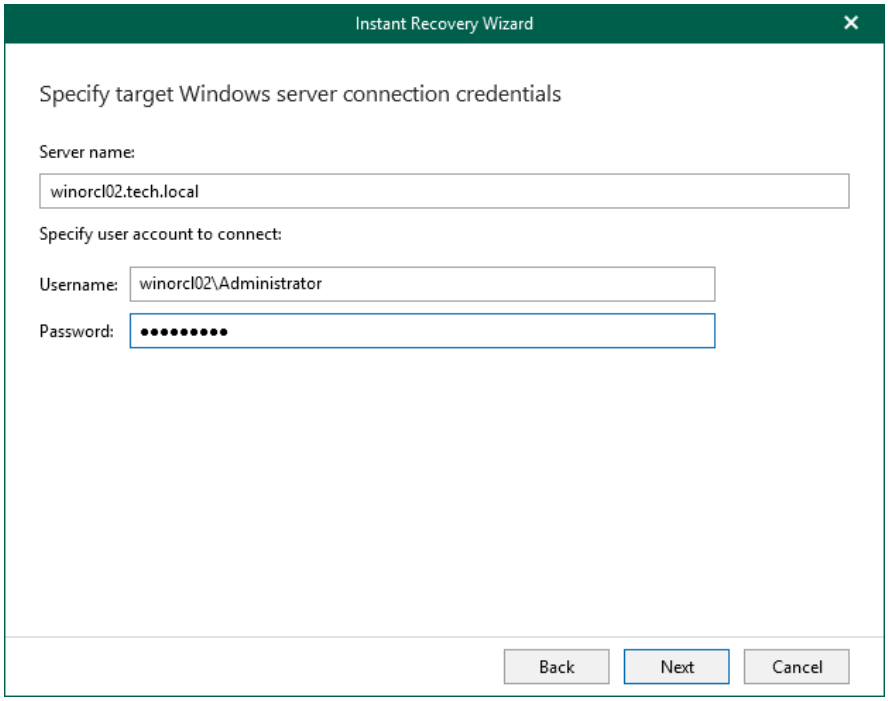
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the target Oracle server.
2. In the **Specify user account to connect** section, enter credentials to connect to the target Oracle server.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



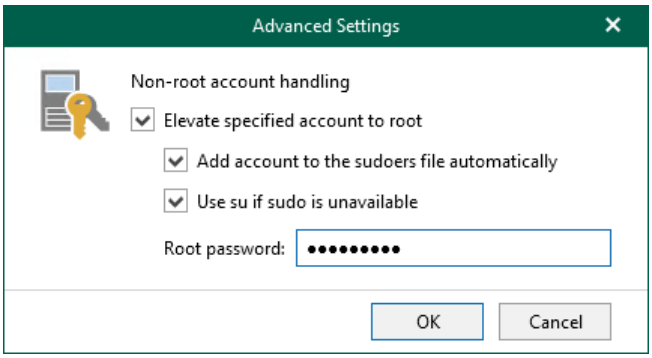
Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

3. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
4. In the **SSH port** field, specify the port number of the selected Oracle server.
5. In the **Account** filed, specify an account under which to connect to the specified server.

6. In the **Password** field, enter the password.
7. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.
   a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

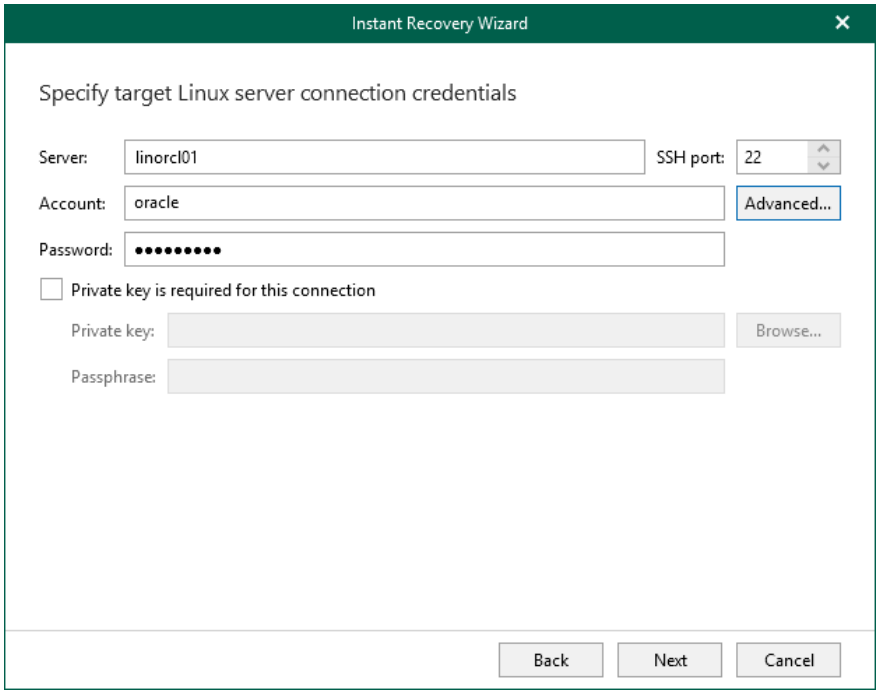
      If you do not enable this option, you will have to manually add the user account to the sudoers file.
   c. If the `sudo` command is not available or may fail on the target Linux server, you have an option to use the `su` command instead. To enable the `su` command, select the **Use su if sudo is unavailable** check box and enter the password for the root account in the **Root password** field.



8. 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.

Consider that the user account must be a member of the **dba** group.



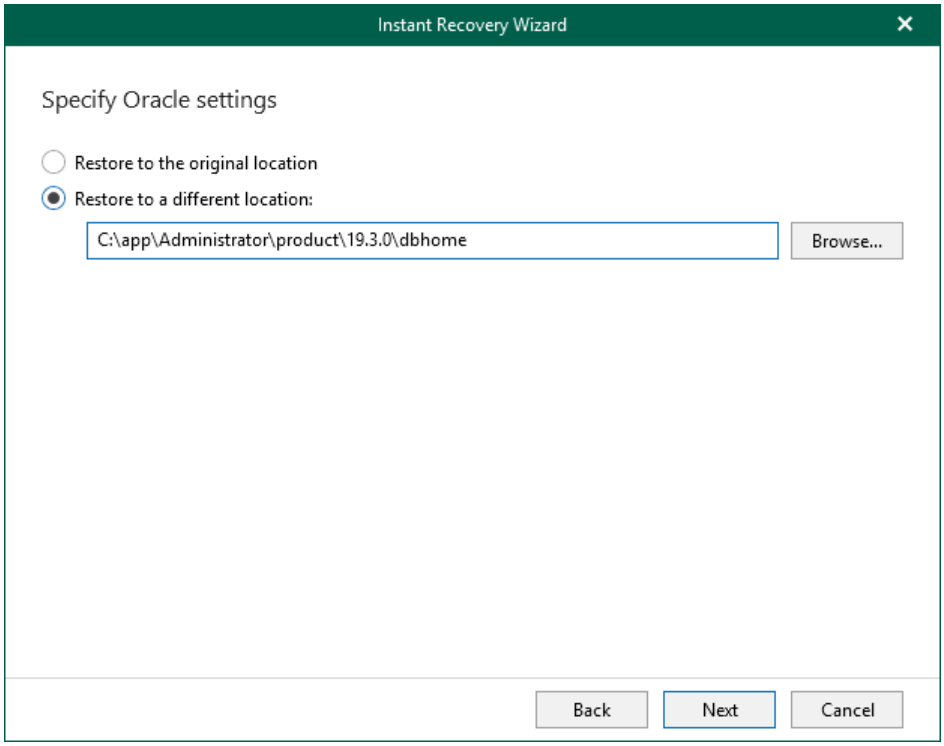
Step 4. Specify Oracle Settings

The **Specify Oracle settings** step of the wizard is available if you select the instant recovery to another server option.

At this step of the wizard, select a location to which you want to restore databases:

- **Restore to the original location** — to restore databases back to the original location.
- **Restore to a different location** — to restore databases to a custom location. To locate an Oracle home directory for restored databases, click Browse and select a folder you want to use.

> **NOTE**
>
> If the account specified in Specify Target Server is not the Oracle home user, you will be asked to provide a password to access the target Oracle home. Applicable to Oracle 12c and later versions.



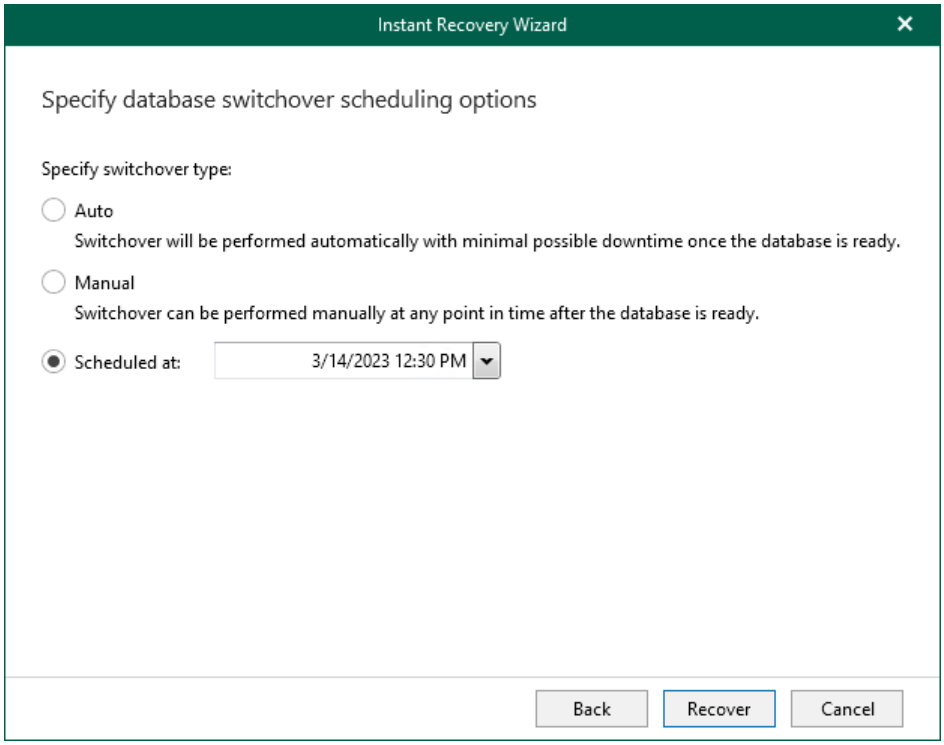
Step 5. Specify Switchover Settings

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.



Step 6. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Instant Recovery of Latest State

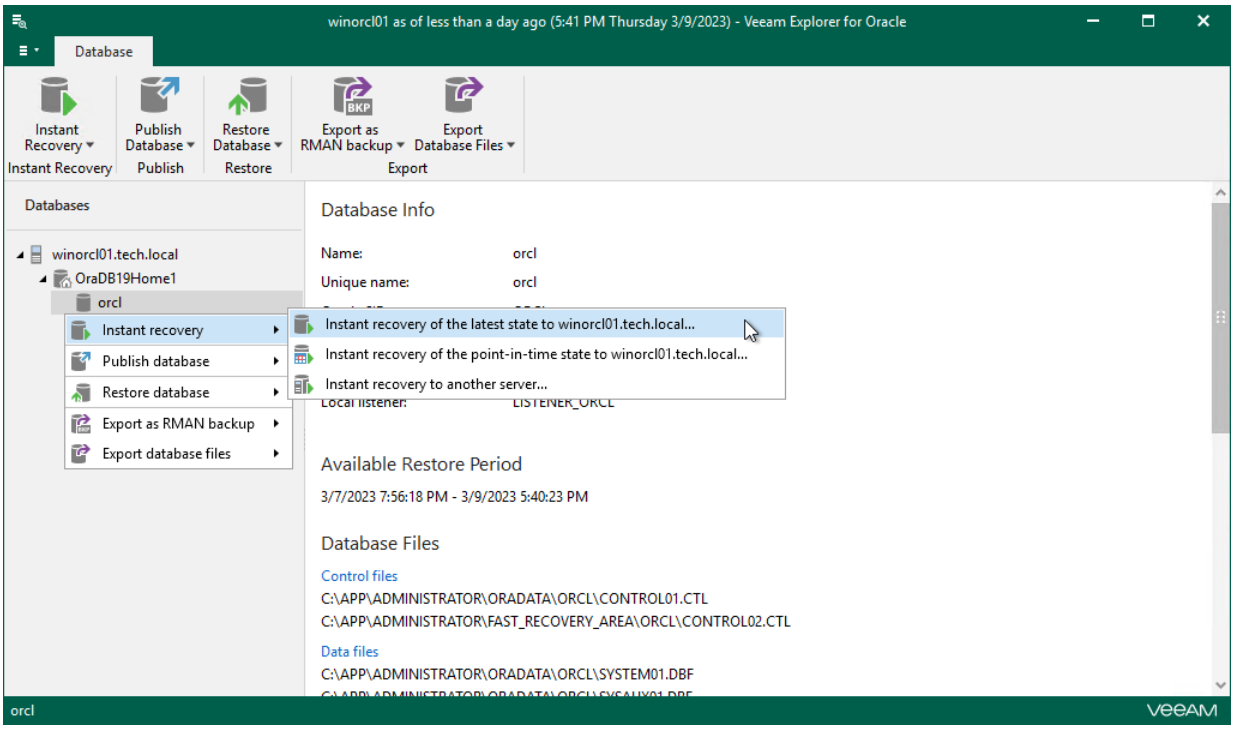
To perform instant recovery of a single database to the latest state, do the following:

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant Recovery of the latest state to <original_location>**, or you can right-click a database and select **Instant Recovery** > **Instant recovery of the latest state to <original_location>**.

NOTE

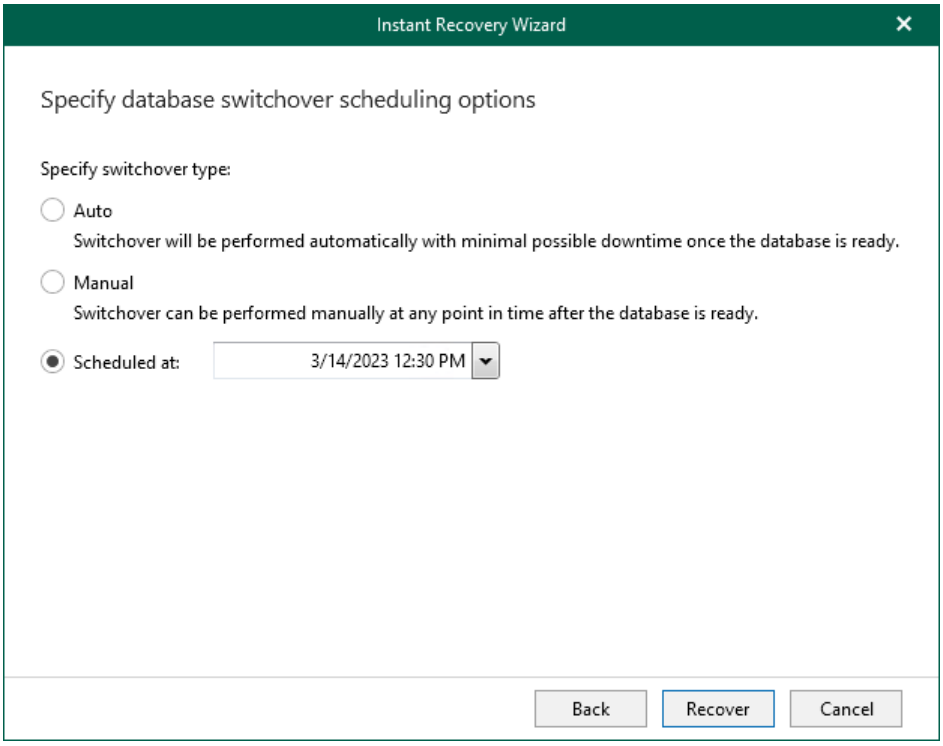
The name of the instant recovery option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.

- If you select the most recent available restore point, the option name is displayed as **Instant recovery of the latest state to <original_location>**.
- If you select any other restore point, the option name is displayed as **Instant recovery of the state of <point_in_time> to <original_location>**.



3. In the **Instant Recovery** wizard, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.

- **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.



4. Click **Recover**.

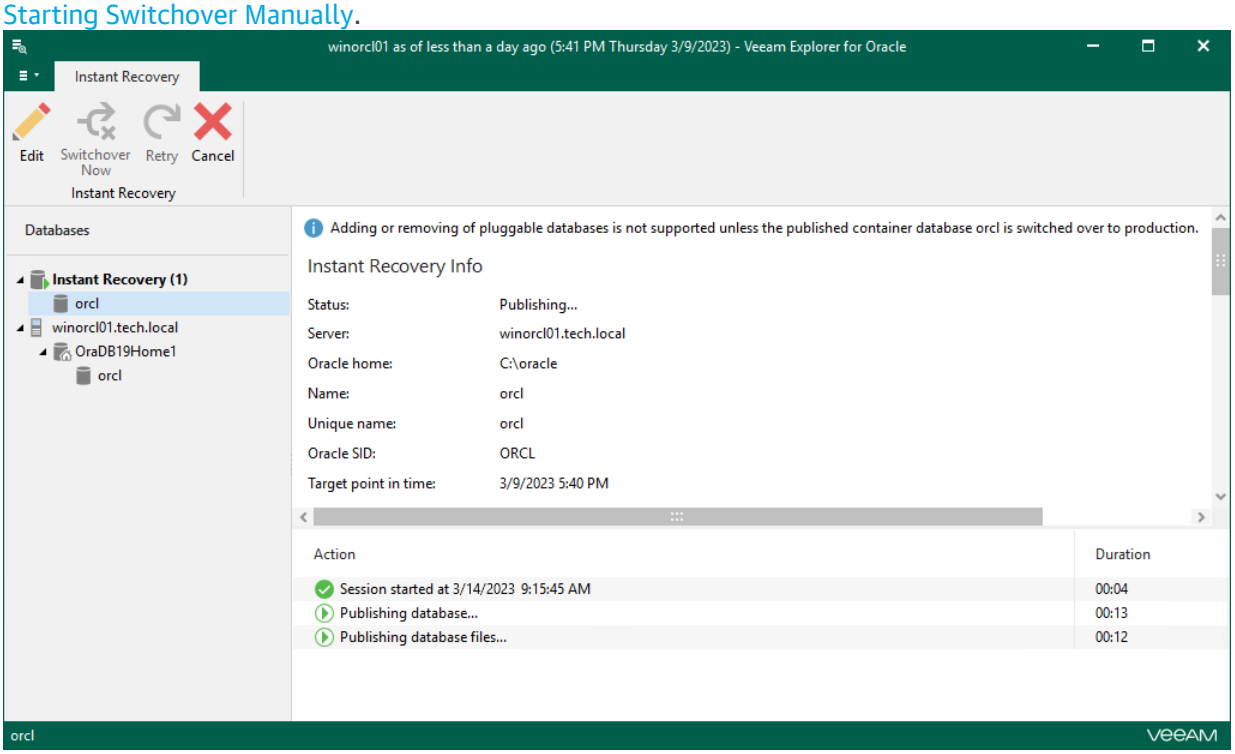
   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.

5. Depending on the option you choose in the Instant Recovery wizard, switchover starts in one of the following ways:

   - Automatically, immediately after synchronization
   - Automatically, according to a specified schedule

- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery of Point-in-Time State

To perform instant recovery of a database to a selected point-in-time state, perform the following steps:

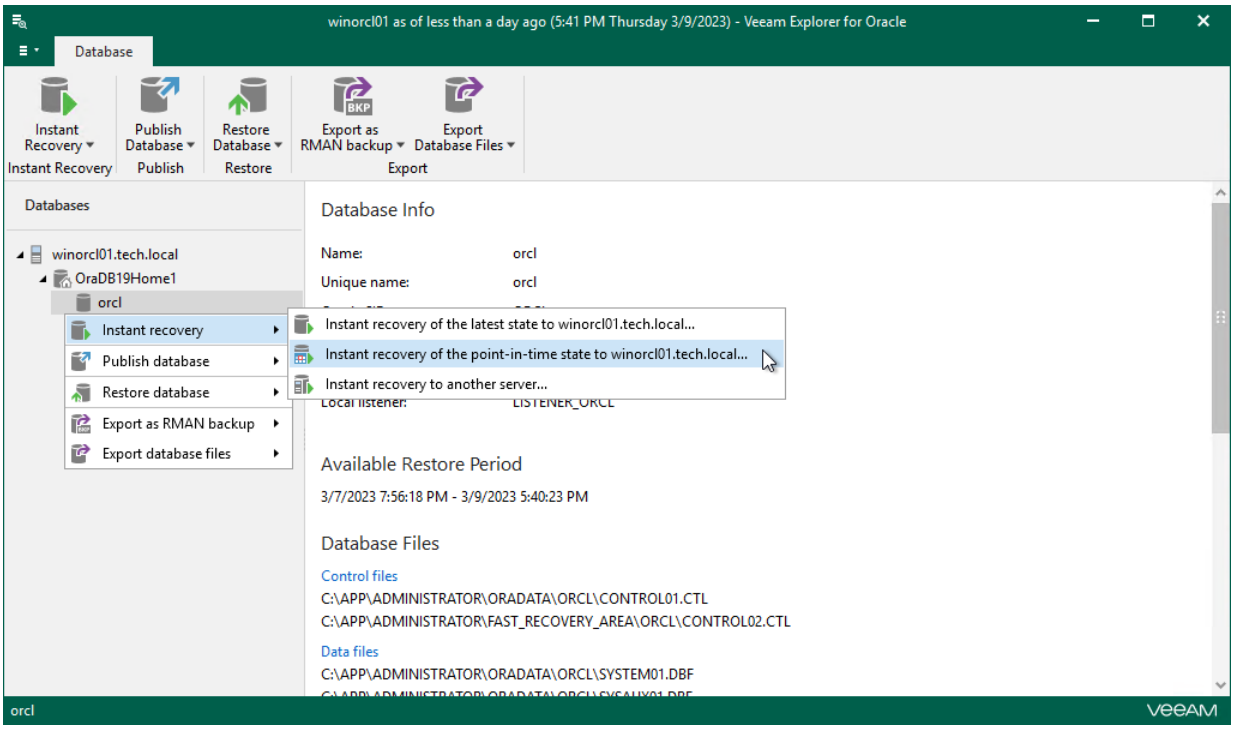
1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify switchover settings.
5. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant recovery of point-in-time state to <original server>**.

Alternatively, you can right-click a database and select **Instant recovery** > **Instant recovery of point-in-time state to <original server>**.



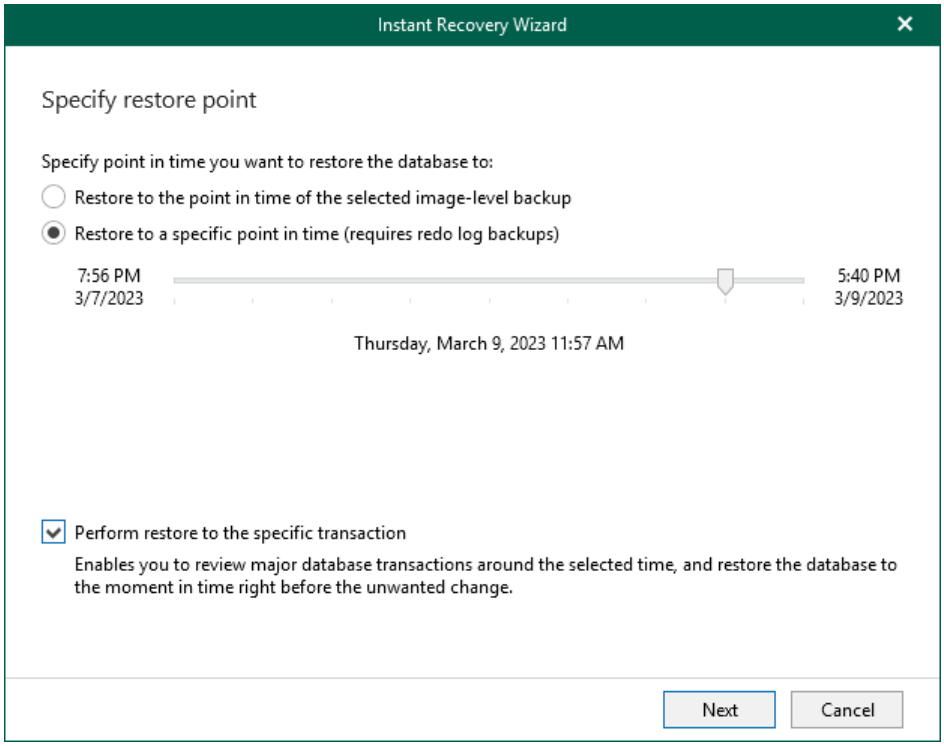
Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. This option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  a. Use the slider to choose a required point in time.

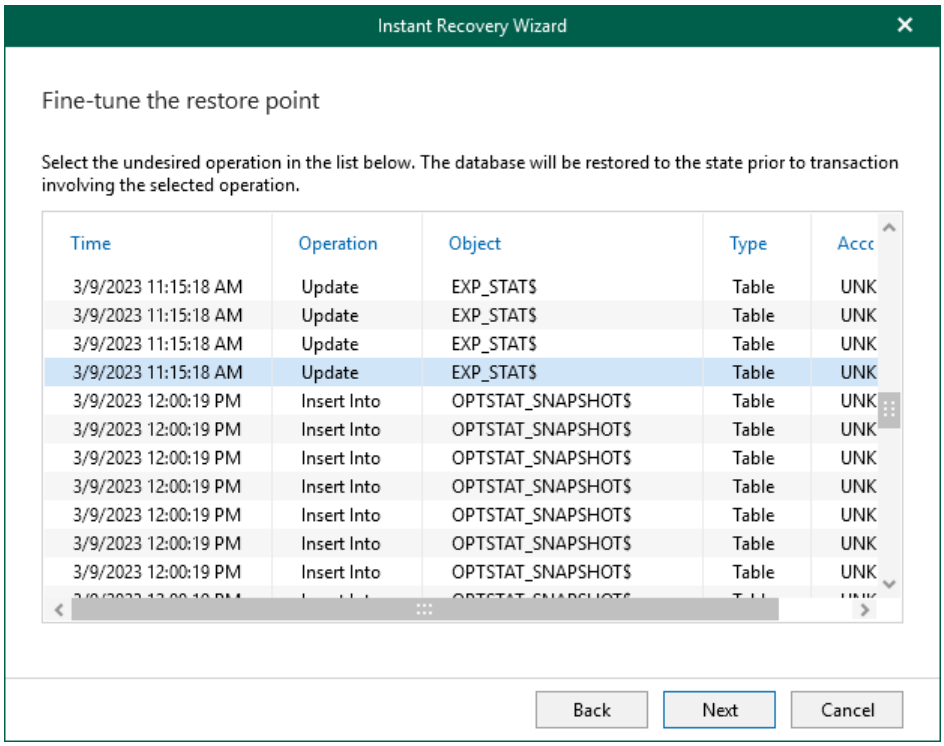
  b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



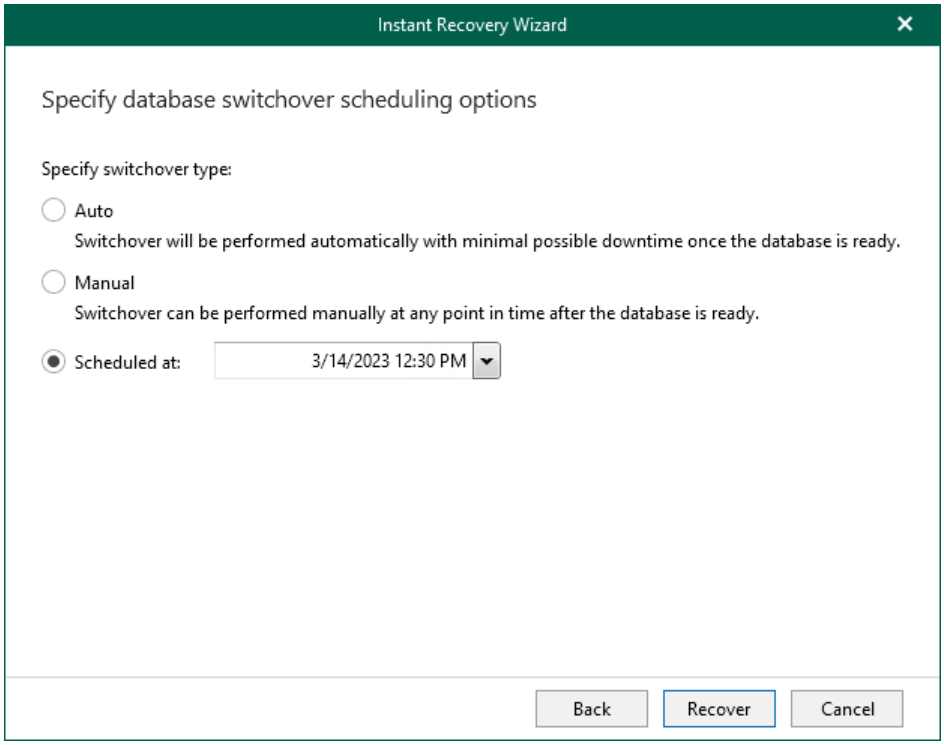
Step 4. Specify Switchover Settings

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.

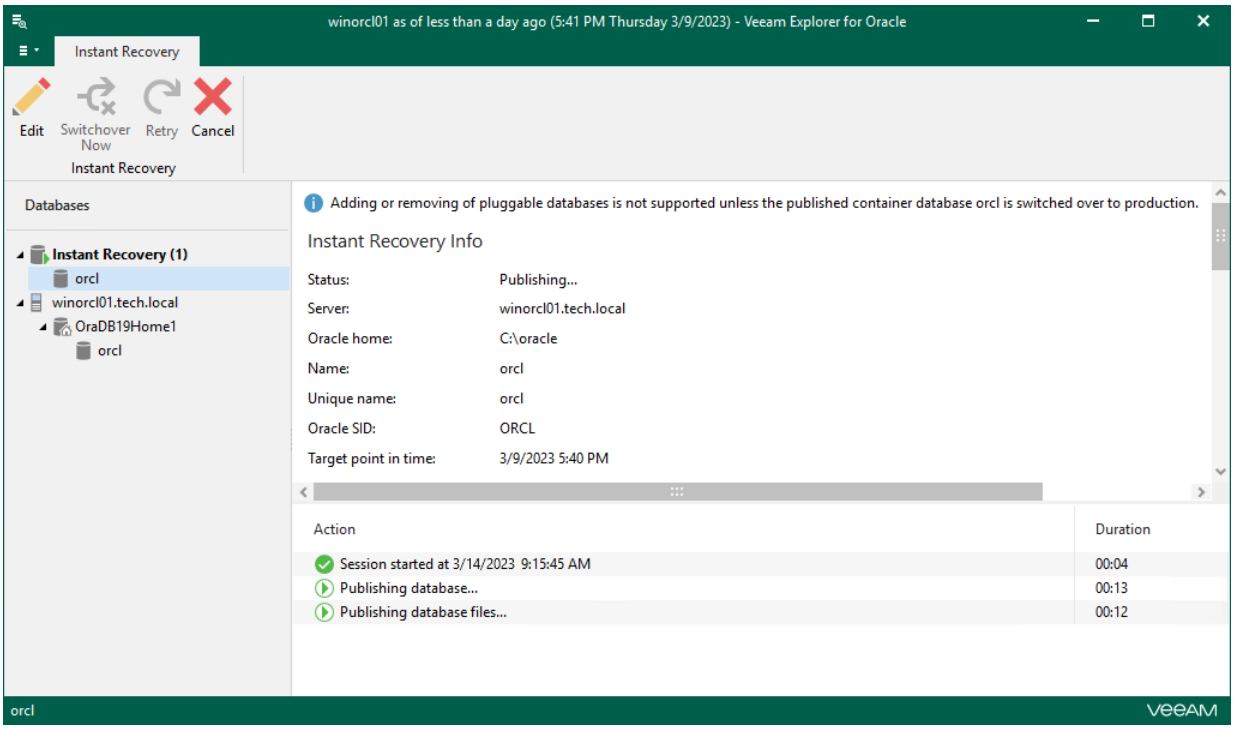


Step 5. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Instant Recovery to Another Server

To perform instant recovery of a database to another server, perform the following steps:

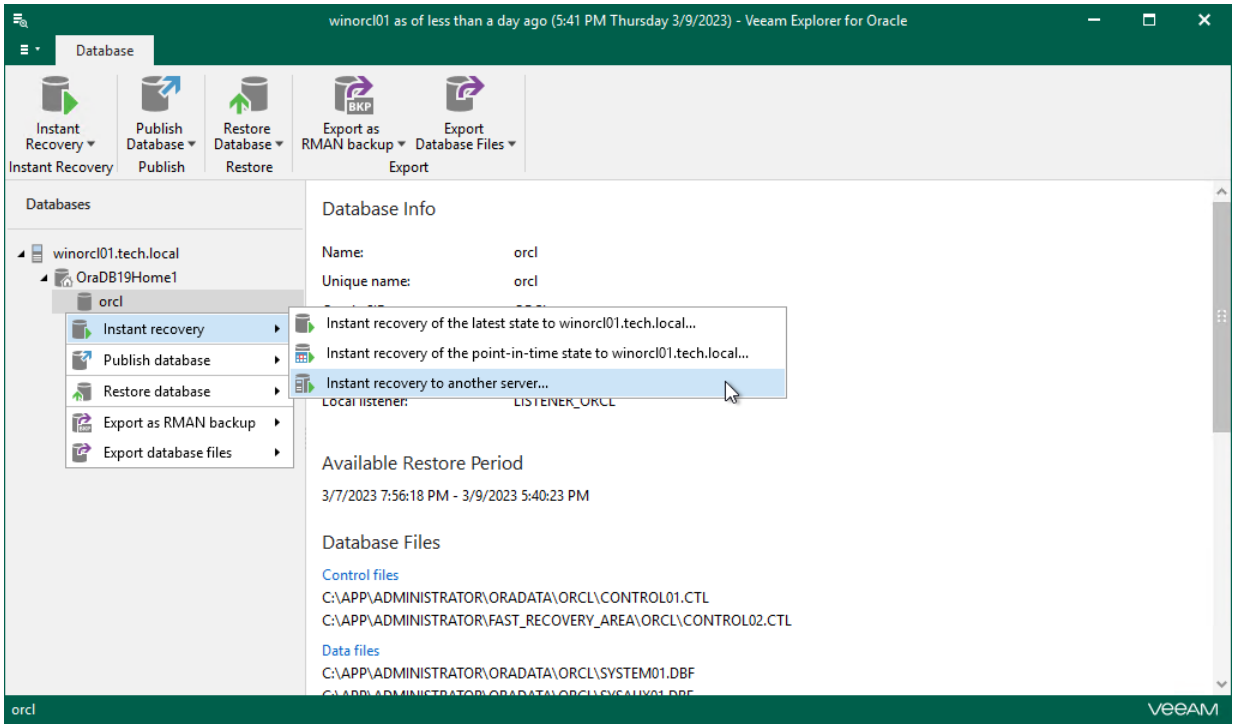
1. Launch the Instant Recovery wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target Oracle server.
5. Specify Oracle settings.
6. Specify database files location.
7. Specify switchover settings.
8. Finalize the Instant Recovery session.

Step 1. Launch Instant Recovery Wizard

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

1. In the navigation tree, select a database.
2. On the **Database** tab, select **Instant Recovery** > **Instant Recovery to another server**.

Alternatively, you can right-click a database and select **Instant recovery** > **Instant recovery to another server**.



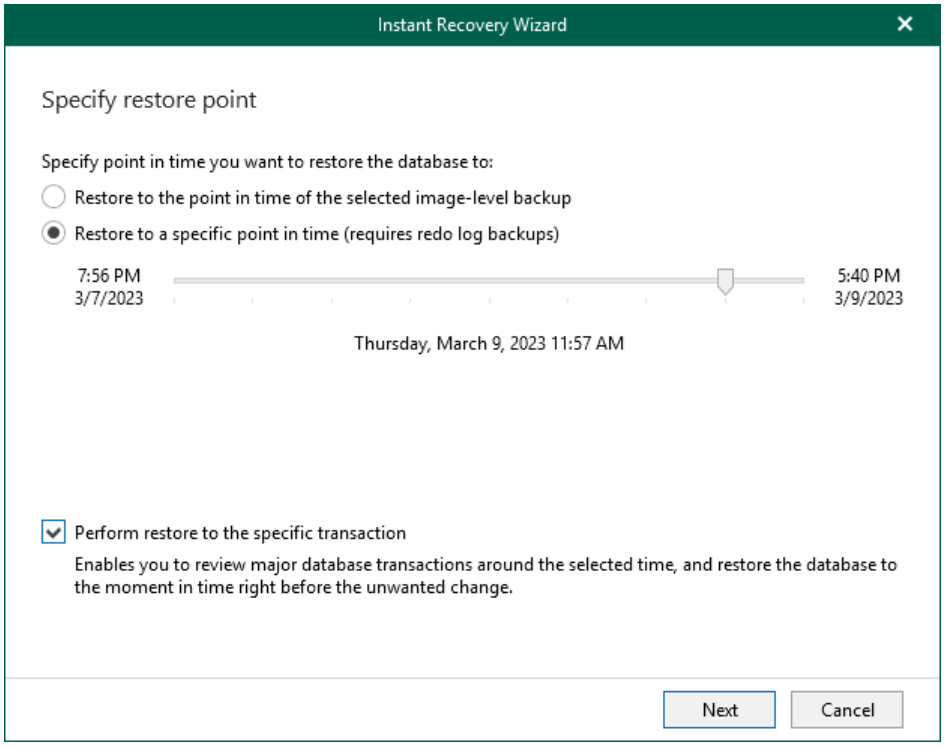
Step 2. Specify Restore Point

At this step of the **Instant Recovery** wizard, select a state as of which you want to restore the database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time. Note that this option is available only if archived log backups exist. For more information, see Required Backup Job Settings.

  a. Use the slider to choose a required point in time.

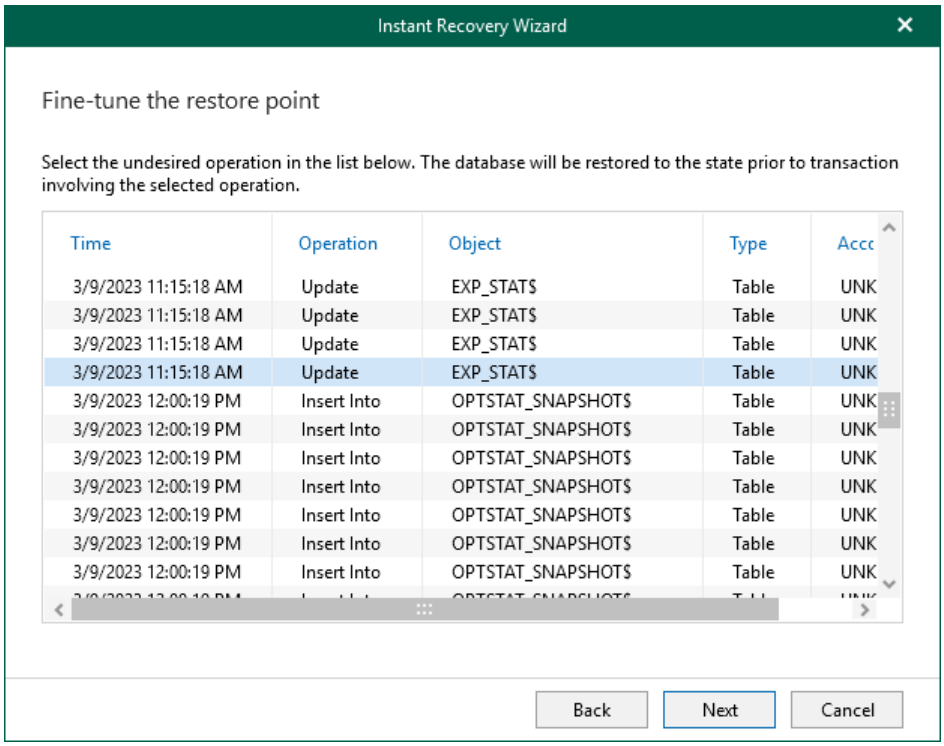
  b. If you want to load database files exactly as of the moment before undesired transactions, select the **Perform restore to the specific transaction** check box. Note that this option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to restore the database.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Oracle Server

At this 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.

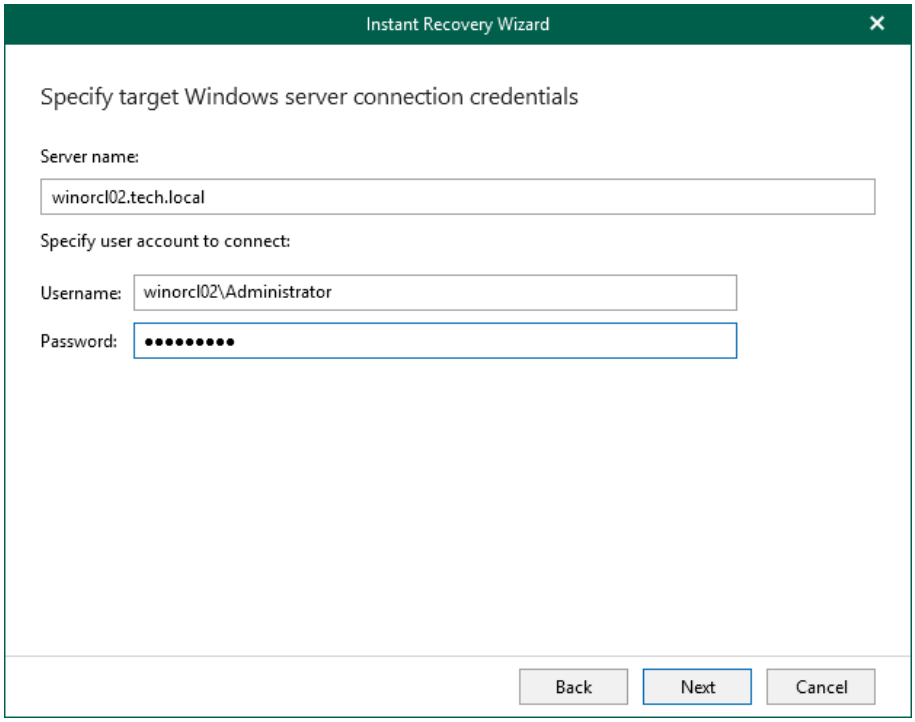
Windows-Based Oracle Server

For a Windows-based Oracle server, do the following:

1. In the **Server name** field, specify the name of the target Oracle server.
2. In the **Specify user account to connect** section, enter credentials to connect to the target Oracle server.

Consider the following:

- The user account must be a member of the local Administrators group and have **sysdba** privileges.
- The user account must be granted appropriate permissions to access Oracle databases; **Read** and **Write** are minimum required, **Full Control** is recommended.
- To copy archived logs to the specified server, the user account must be granted sufficient permissions to access the administrative share.



Linux-Based Oracle Server

For a Linux-based Oracle server, do the following:

3. In the **Server** drop-down list, specify a target Oracle server. You can select an Oracle server from the list or enter a DNS name of the target Oracle server.
4. In the **SSH port** field, specify the port number of the selected Oracle server.
5. In the **Account** filed, specify an account under which to connect to the specified server.
6. In the **Password** field, enter the password.

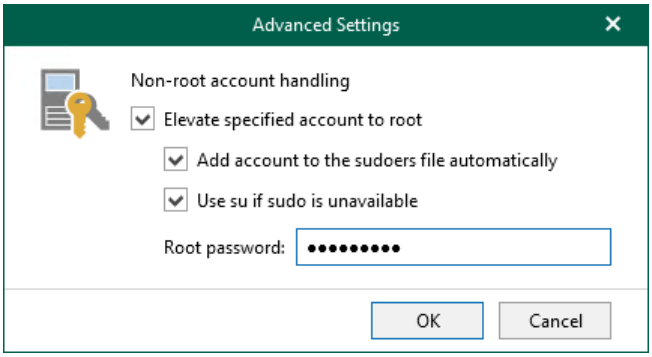
7. If you have specified a non-root account that does not have root permissions on the target server, click **Advanced** to grant sudo rights to this account.

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

   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the sudoers file.

   c. 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 is unavailable** check box and enter the password for the root account in the **Root password** field.



8. If a private key is required to connect to the selected server, do the following:

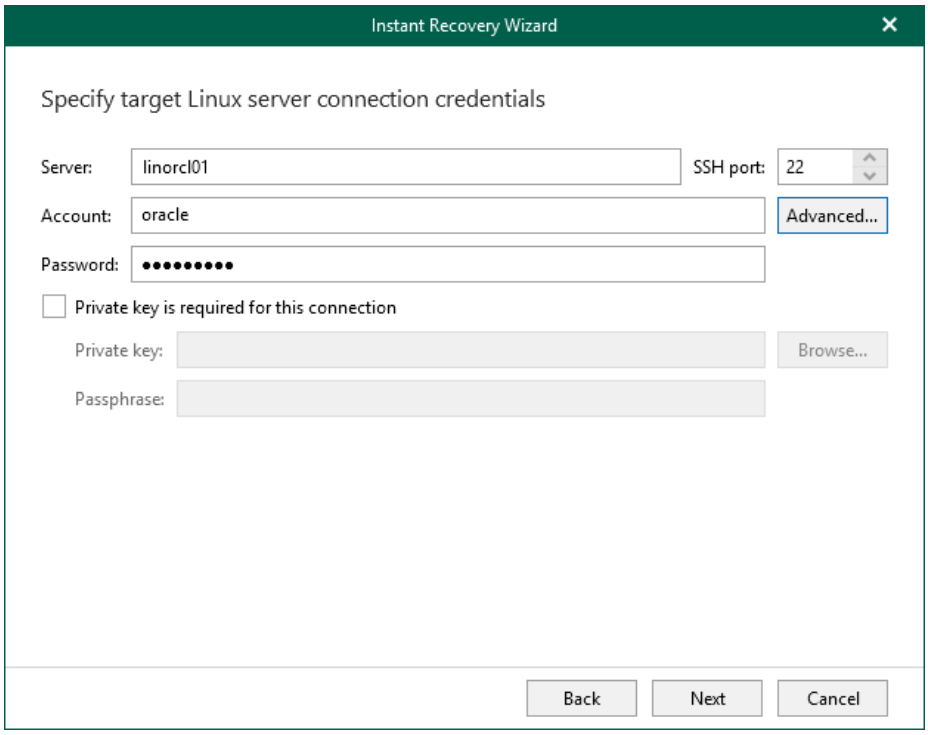
   a. Select the **Private key is required for this connection** check box.

   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.

Consider that the user account must be a member of the **dba** group.



Step 5. Specify Oracle Settings

At this step of the wizard, specify the location to which you want to restore the database.

- Select **Restore to the original location** to restore the database back to the original location.
- Select **Restore to a different location** to restore the database to a custom location.

  a. In the **Oracle home** field, specify the Oracle home directory. To locate the Oracle home directory, click **Browse** and select the folder you want to use.

  b. In the **Global database name** field, specify the global database name as *DB_NAME.DB_DOMAIN*, where:

     - *DB_NAME* is the database name. Oracle limits the length of the database name to 8 characters. If the database name you specify exceeds this limit, Veeam Explorer for Oracle will automatically shorten the database name, and hence the global database name, during the publishing process.

       The value you specify is also used for the unique database name (*DB_UNIQUE_NAME*) of the published database. The unique database name can contain up to 30 characters.

     - *DB_DOMAIN* is the domain name of the database. It does not count towards any character limits and Veeam Explorer for Oracle does not shorten it during the publishing process.

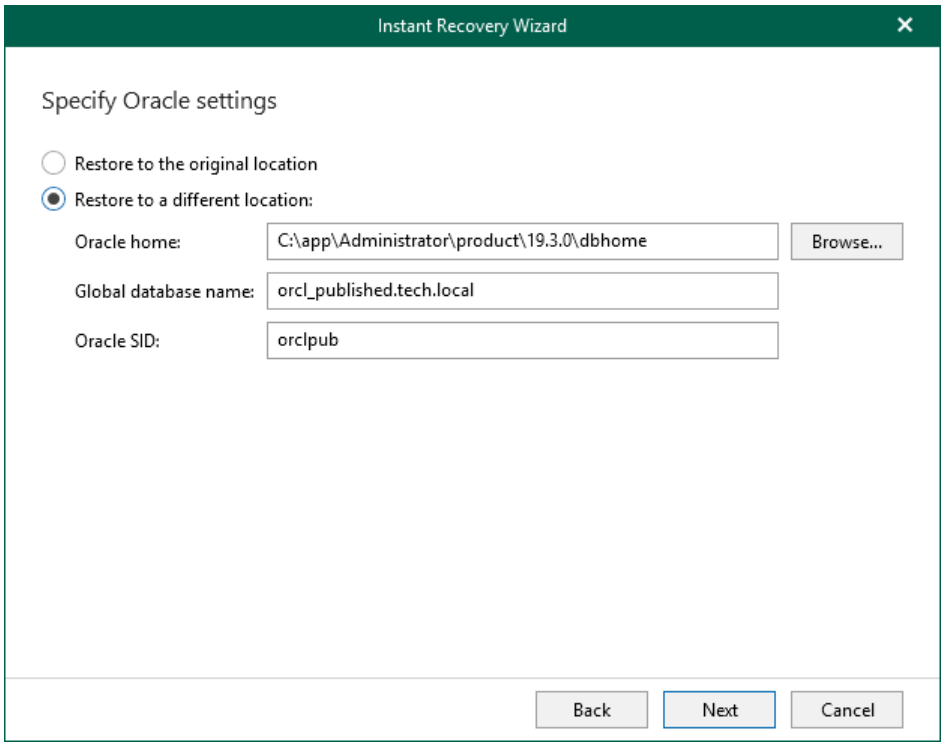
     For example, if you specify the global database name as *orcl_published.tech.local*, Veeam Explorer for Oracle will shorten it to *orcl_pub.tech.local*. The database name of the published database will be *orcl_pub*, while the unique database name of the published database will be *orcl_published.*

  c. In the **Oracle SID** field, specify the database system identifier. The **Oracle SID** field is automatically filled with the value entered in the **Global database name** field, but you can also assign a different value.

     The maximum length of the Oracle SID is 12 characters and it can only contain alphanumeric characters (a-z, A-Z and 0-9).

NOTE

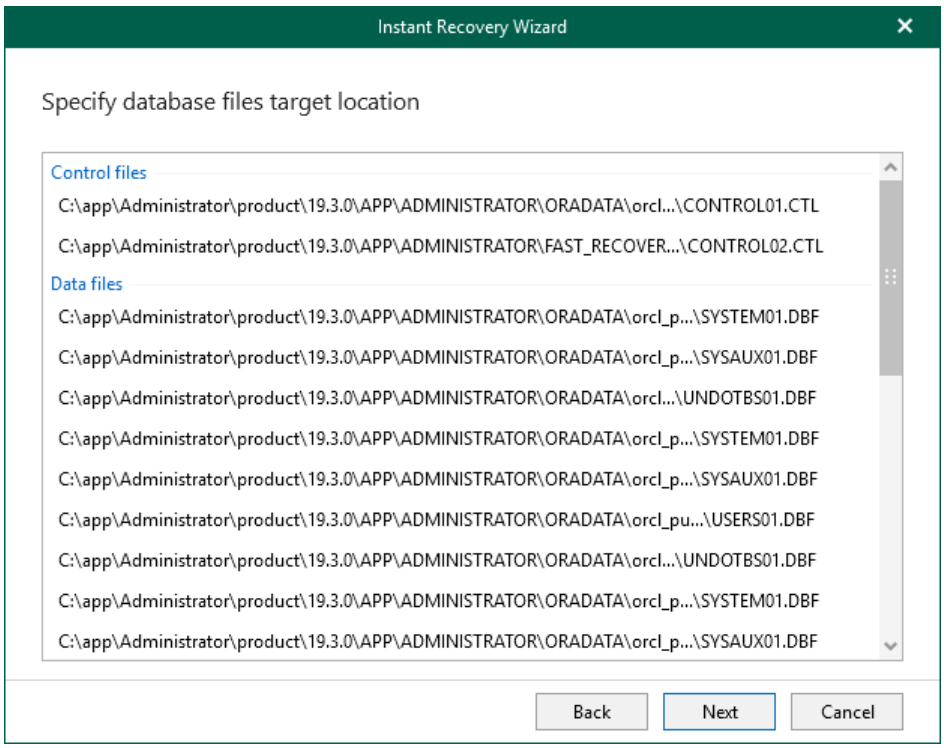
If the account specified in Specify Target Oracle Server is not the Oracle home user, you will be asked to provide a password to access the target Oracle home. Applicable to Oracle 12c and later versions.



Step 6. Specify Database File Location

At this step of the wizard, specify the location for database files (control files, data files, log files and temp files).

To edit the path, click the path row and provide the location you want to use. If specified folders do not exist, Veeam Explorer for Oracle will create these folders.



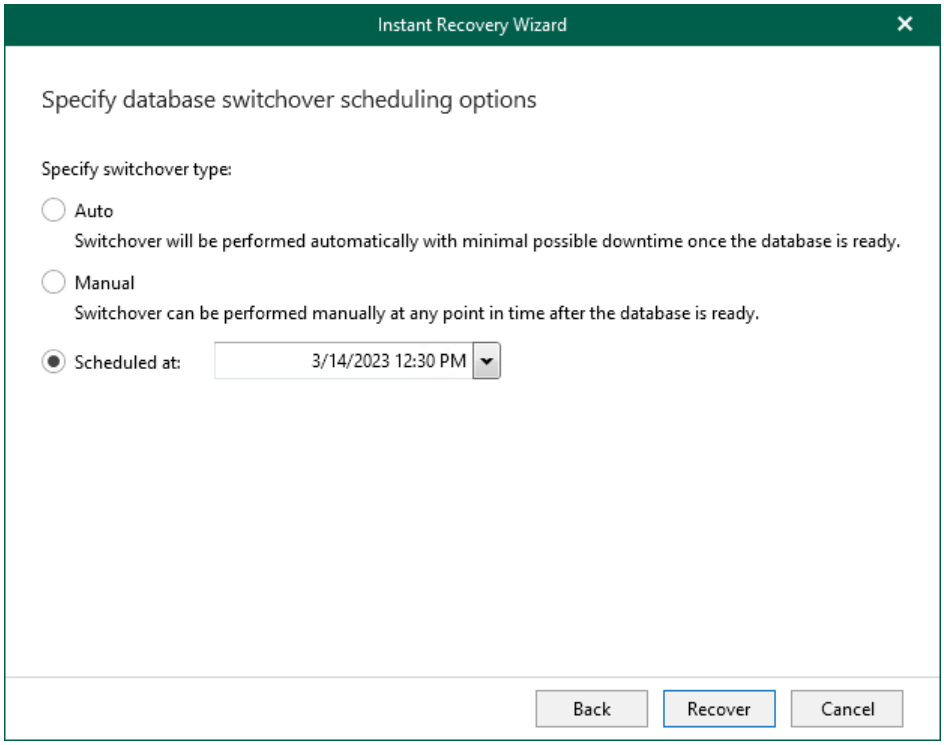
Step 7. Specify Switchover Settings

At this step of the wizard, specify database switchover options.

To select a switchover option and start the instant recovery session, do the following:

1. At the **Specify switchover type** field, select one of the following switchover options:
   - **Auto**: switchover is performed automatically after all database files are copied and synchronized.
   - **Manual**: switchover is started manually by user at any time after all database files are copied and synchronized.
   - **Scheduled**: switchover is performed at a specified date and time. Use the drop-down calendar to specify the date and time.
2. Click **Recover**.

   After you click **Recover**, Veeam Explorer for Oracle starts publishing the database on the target server.

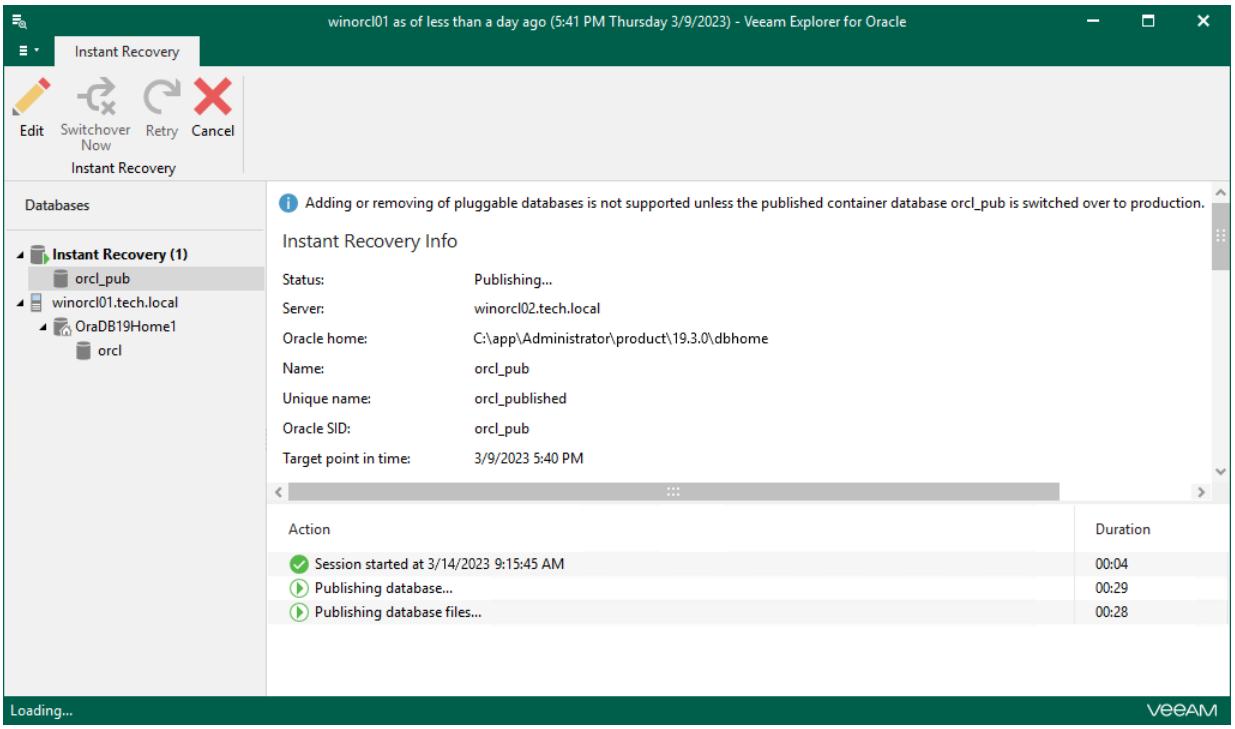


Step 8. Finalize Instant Recovery Session

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.



Switchover

The switchover option becomes available after all the database files are copied to the target server. During switchover, the mounted database is switched to its complete copy on the target server. Note that if you have selected to restore to the original server, the restored database will replace the original database.

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in on of the following ways:

- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

During switchover, Veeam Explorer for Oracle performs the following operations:

1. Detaches the published database from the Oracle server.
2. Uses archived redo logs to synchronize changes between the published database and the copied database files.
3. Drops the published database.
4. Attaches the recovered database to the Oracle server.

Note that the database will be offline between the steps 1–4.

Auto Switchover

The *Auto* switchover option ensures minimal period of downtime.

As soon as database files are copied from backup files, Veeam Explorer for Oracle uses archived redo logs to find differences between the published database and the recovered database. Depending on the size of differences in archived redo logs, the following happens:

- If the size of differences in archived redo logs is smaller than 10 MB, Veeam Explorer for Oracle starts the switchover process. In this case, the databases are synchronized during switchover.
- If the size of differences in archived redo logs is larger than 10 MB, Veeam Explorer for Oracle uses redo logs to synchronize the changes.

  After synchronizations, checks the size of differences in archived redo logs once again. If the size is smaller than 10 MB, Veeam Explorer for Oracle starts the switchover process. If the size is larger than 10 MB again, another cycle of synchronization is performed. Synchronization is relaunched until the size of differences in logs is smaller than 10 MB.

Scheduled Switchover

After database files are copied from backup files, Veeam Explorer for Oracle uses archived redo logs to find differences between the published database and the recovered database. Veeam Explorer for Oracle checks the size of differences every minute. If the size is larger than 10 MB or it has been 5 minutes since the last synchronization, Veeam Explorer for Oracle starts to synchronize the changes between the published database and the copied database files.

After synchronization is finished, Veeam Explorer for Oracle waits for the scheduled date and time to start switchover.

If the switchover scheduled period starts during the synchronization process, switchover starts only after the synchronization is finished.

Manual Switchover

After database files are copied from backup files, Veeam Explorer for Oracle uses archived redo logs to find differences between the published database and the recovered database. Veeam Explorer for Oracle checks the size of differences every minute. If the size is larger than 10 MB or it has been 5 minutes since the last synchronization, Veeam Explorer for Oracle starts to synchronize the changes between the published database and the copied database files.

After synchronization is finished, you can launch switchover manually. For details, see Starting Switchover Manually.

If you launch switchover during the synchronization process, switchover starts only after the synchronization is finished.

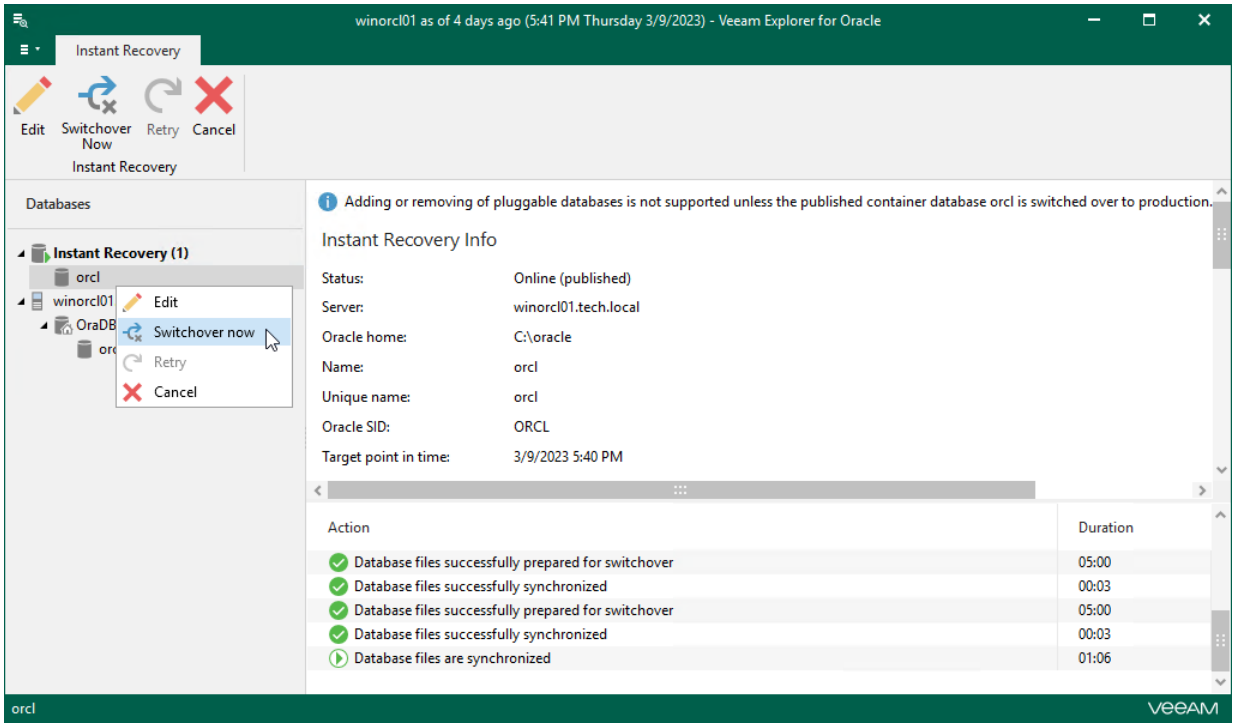
Starting Switchover Manually

If you have selected the *Manual* switchover option in the **Instant Recovery** wizard, you can start the switchover process at any time if the database is in the *Ready to switchover* state.

To start switchover manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Switchover Now**.

Alternatively, you can right-click the database and select **Switchover now**.



Managing Instant Recovery Session

After you finish steps of the **Instant Recovery** wizard, Veeam Explorer for Oracle starts an instant recovery session which shows the progress of the recovery process.

Depending on the option you choose in the **Instant Recovery** wizard, switchover starts in one of the following ways:

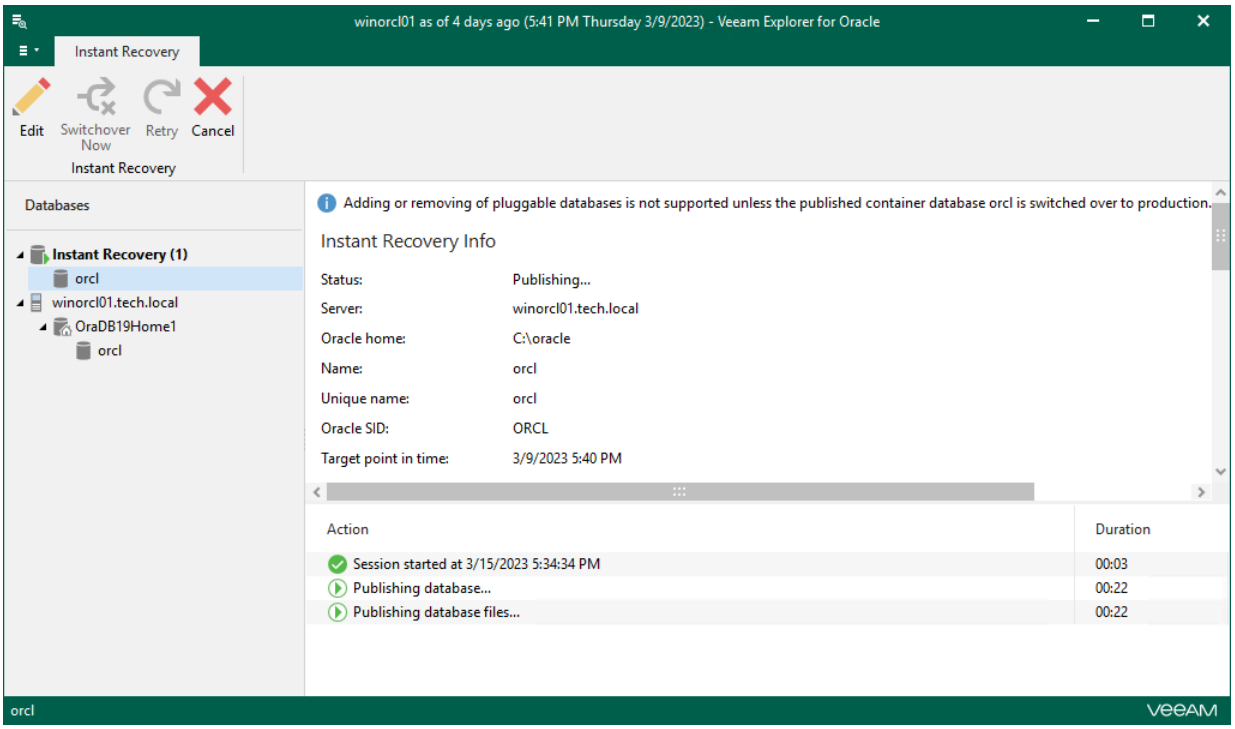
- Automatically, immediately after synchronization
- Automatically, according to a specified schedule
- Manually

If you have selected the **Manual** switchover option, you must perform switchover manually as described in Starting Switchover Manually.

Also, in the **Instant Recovery** session view, you can do the following:

- Edit switchover settings.
- Retry instant recovery (in case instant recovery session fails for any reason).
- Cancel instant recovery.

> **NOTE**
>
> The instant recovery session closes automatically after switchover.

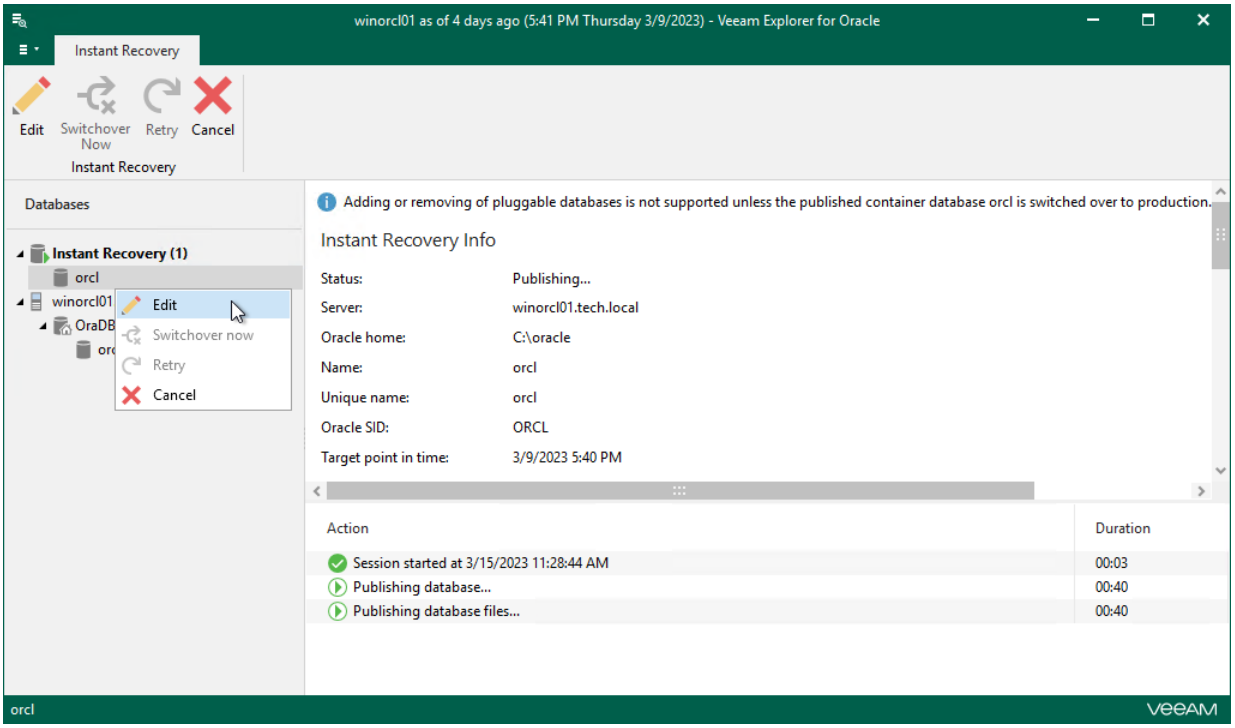


Editing Instant Recovery Settings

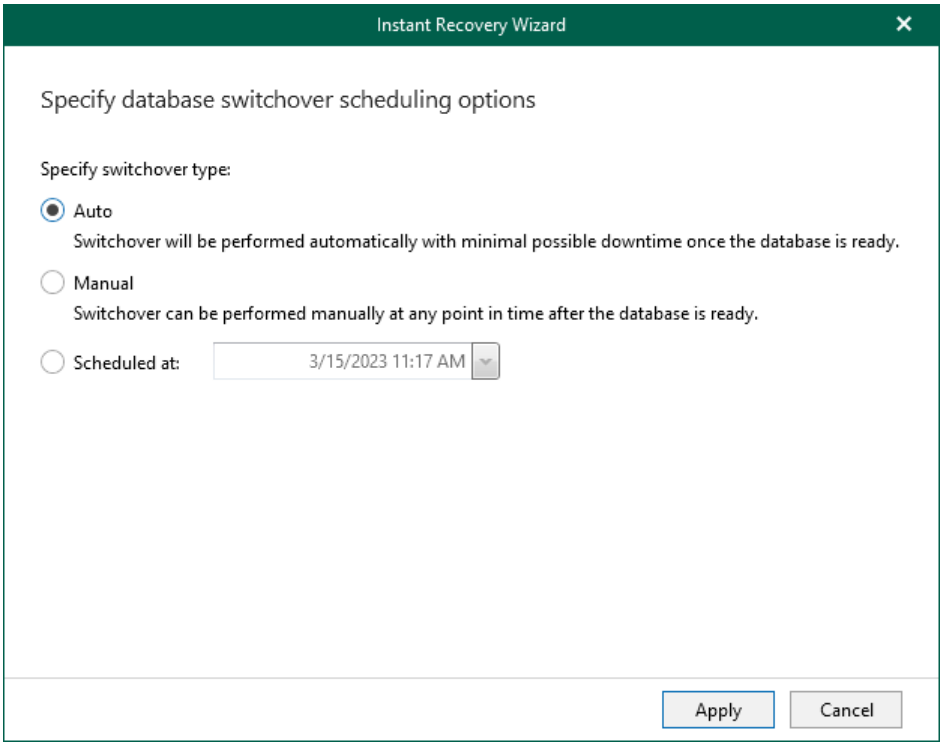
If you have started an instant recovery session and want to change switchover settings, you can edit instant recovery settings.

To change switchover settings of an instant recovery session, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Edit** or right-click the database or instance and select **Edit**.



3. Change the switchover option and click **Apply**.



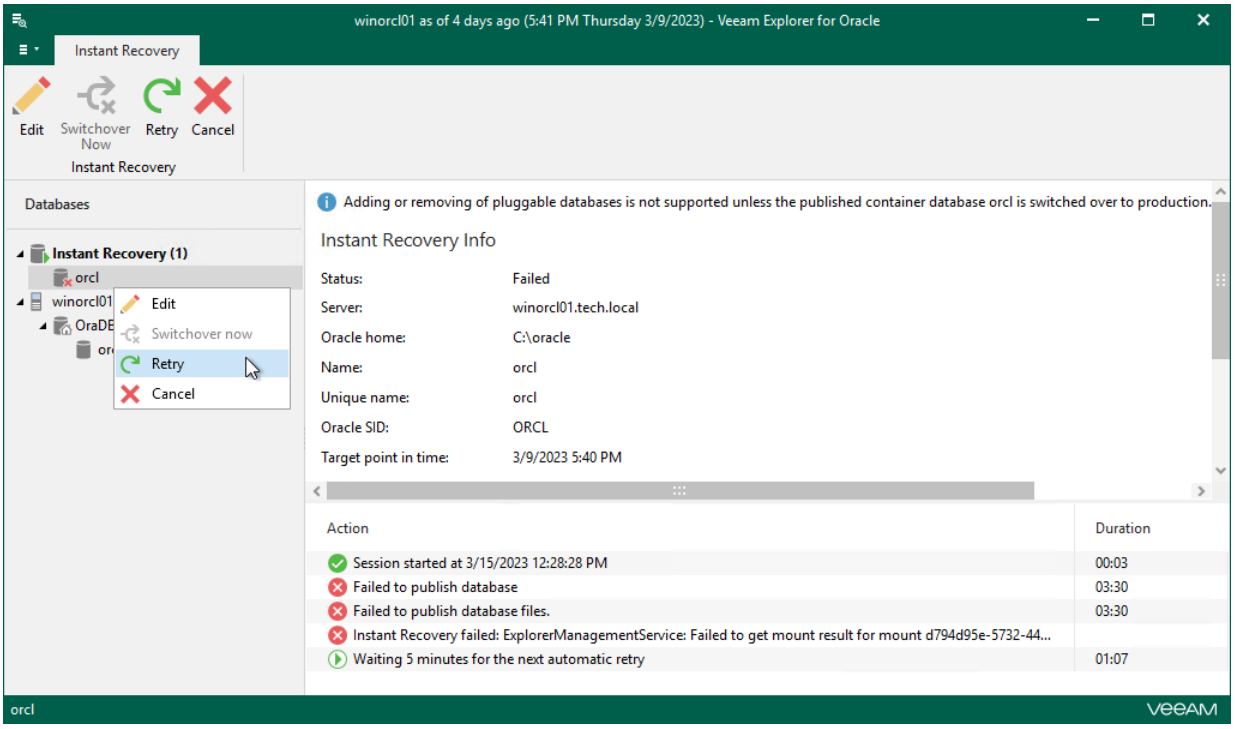
Recovery Retry

If anything disrupts the restore process (the target or mount server crashes or the network is down), the restore process stays in the waiting mode and performs 10 automatic retries every 5 minutes. If the retries fail, you can launch the retry manually after the server or network is up.

To start the retry process manually, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select the database.
2. On the **Instant Recovery** tab, click **Retry.**

Alternatively, you can right-click the database and select **Retry**.



Canceling Instant Recovery

If you have finished working with the published database and you do not want to switchover, you can cancel the instant recovery session.

You can do this by canceling instant recovery in either Veeam Explorer for Oracle or the Veeam Backup & Replication console.

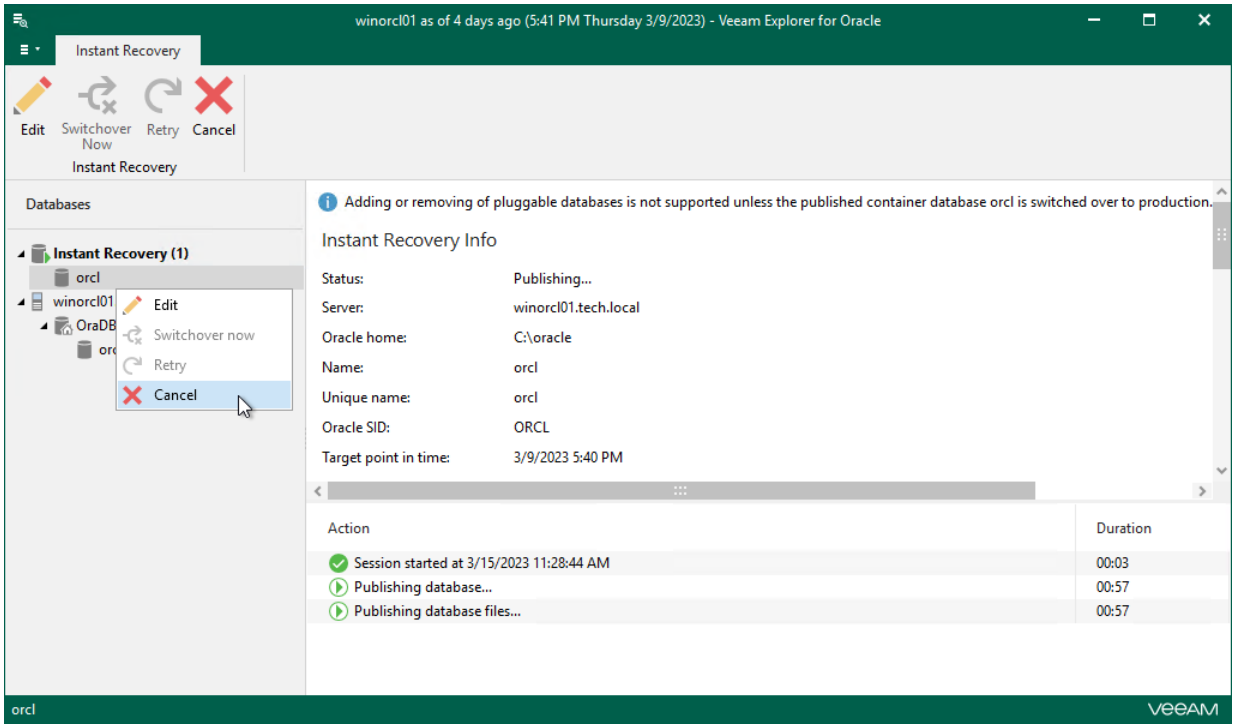
> **NOTE**
>
> Consider the following:
>
> - Closing either the Veeam Explorer for Oracle window or the Veeam Backup & Replication console does not cancel the instant recovery session.
> - You do not need to cancel the instant recovery session if switchover is already performed. The session closes automatically after switchover.

Canceling Instant Recovery in Veeam Explorer for Oracle

To cancel the instant recovery session in Veeam Explorer for Oracle, do the following:

1. In the navigation pane, under the **Instant Recovery** node, select a published database.
2. On the **Instant Recovery** tab, select **Cancel**.

Alternatively, you can right-click the database and select **Cancel**.

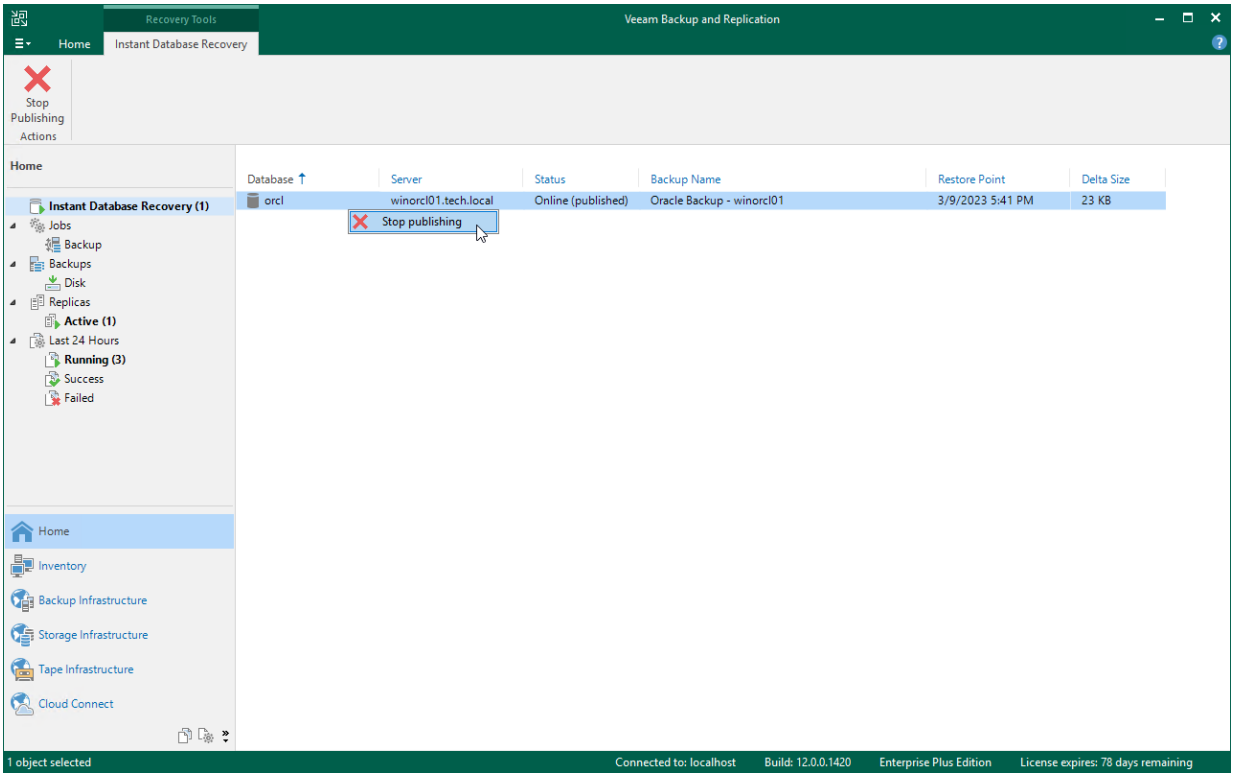


Canceling Instant Recovery in Veeam Backup & Replication Console

To cancel the instant recovery session in the Veeam Backup & Replication console, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the navigation pane, select **Instant Database Recovery**.
3. In the preview pane, select the session and in the **Instant Database Recovery** tab click **Stop Publishing**.

   Alternatively, you can right-click the session and click **Stop publishing**.



Data Export

This section explains how to export Oracle data using Veeam Explorer for Oracle.

Export as RMAN Backup

In Veeam Explorer for Oracle, you can export Oracle databases as RMAN backups.

During the export, Veeam Explorer for Oracle does the following:

- Uses native Oracle RMAN to retrieve Oracle databases from the backup that is being explored.

  The retrieved databases are then saved onto a staging server as RMAN backups.

  When exporting published databases, then such databases are saved directly to the server onto which they are published.

- Copies the saved RMAN backups to the target location.

Exporting Latest State

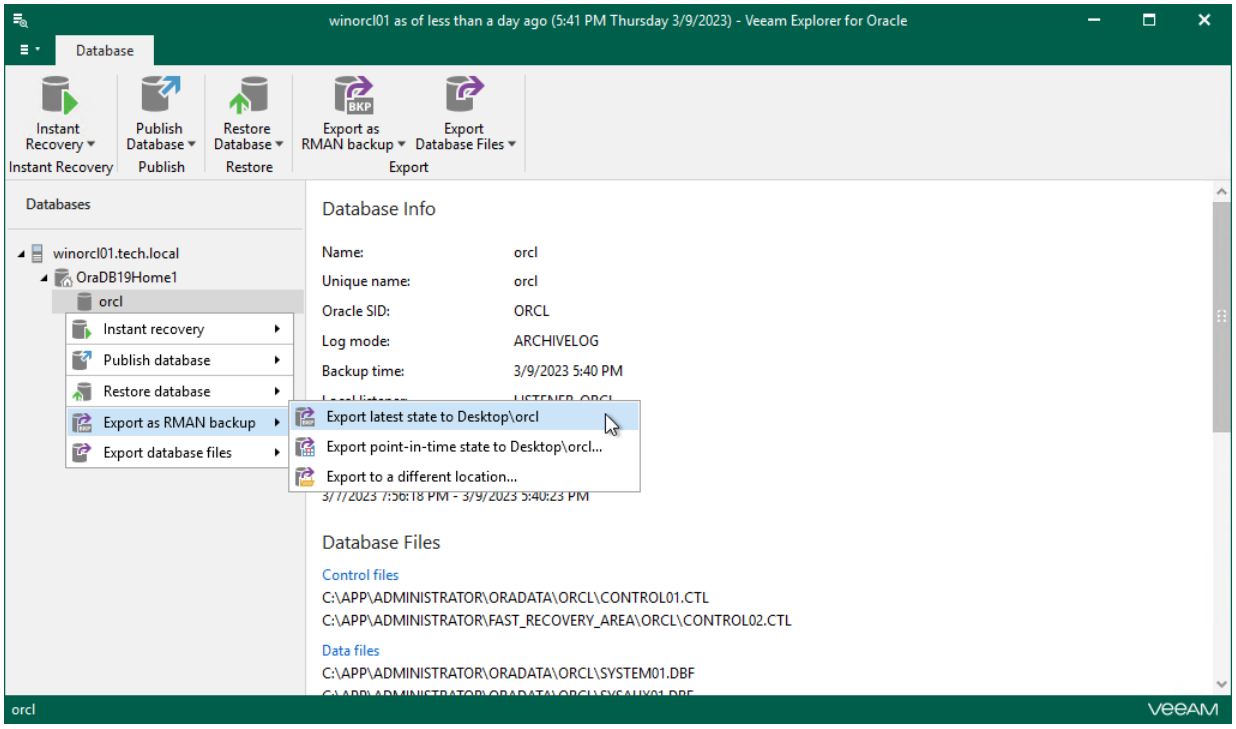
To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup > Export latest state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export as RMAN backup** > **Export latest state to Desktop\<db_name>**.

> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export latest state to Desktop\<db_name>**.
> - If you select any other restore point, the option name is displayed as **Export state of <point_in_time> to Desktop\<db_name>**.

Consider that Veeam Explorer for Oracle exports files in the following format: *_%I_%d_%T_%U*. For more information, see this Oracle article. To set a different export format, use Exporting to Custom Location.



Exporting Point-in-Time State

To export data as of the point-in-time state, do the following:

1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

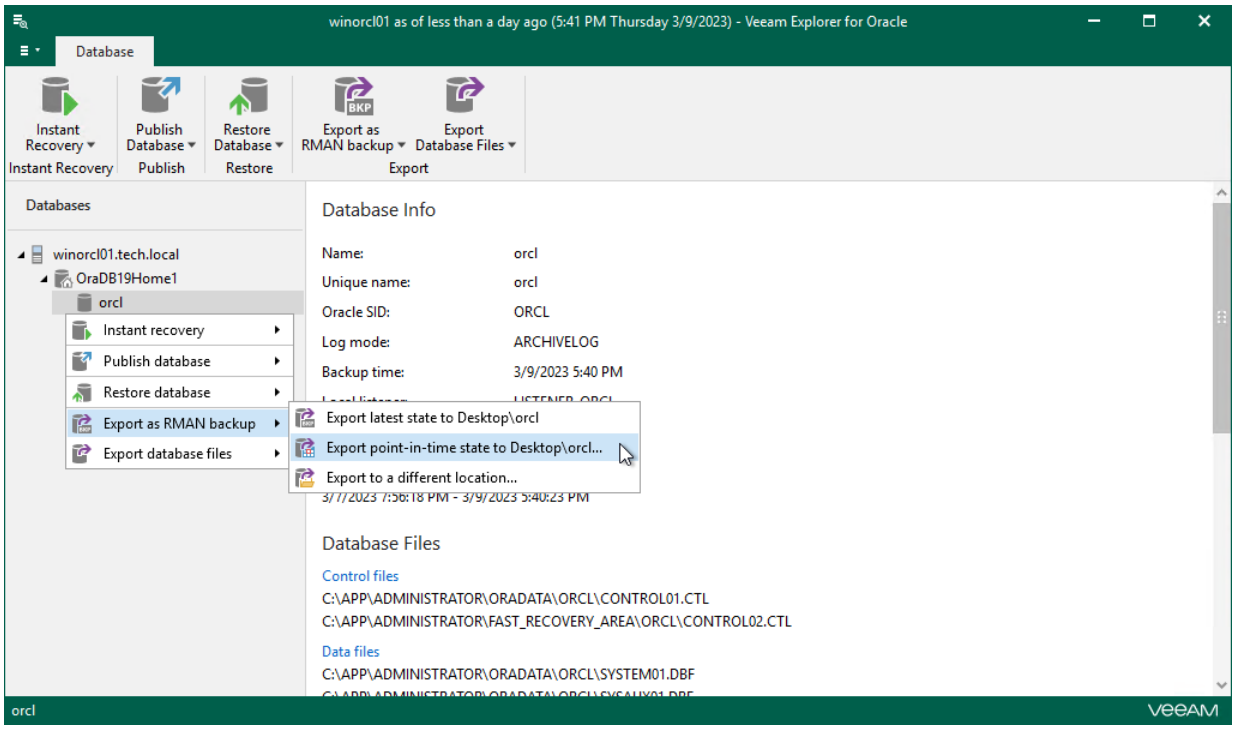
Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup** > **Export point-in-time state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export as RMAN backup** > **Export point-in-time state to Desktop\<db_name>**.

Consider that Veeam Explorer for Oracle exports files in the following format: *_%I_%d_%T_%U*. For more information, see this Oracle article. To set a different export format, use Exporting to Custom Location.



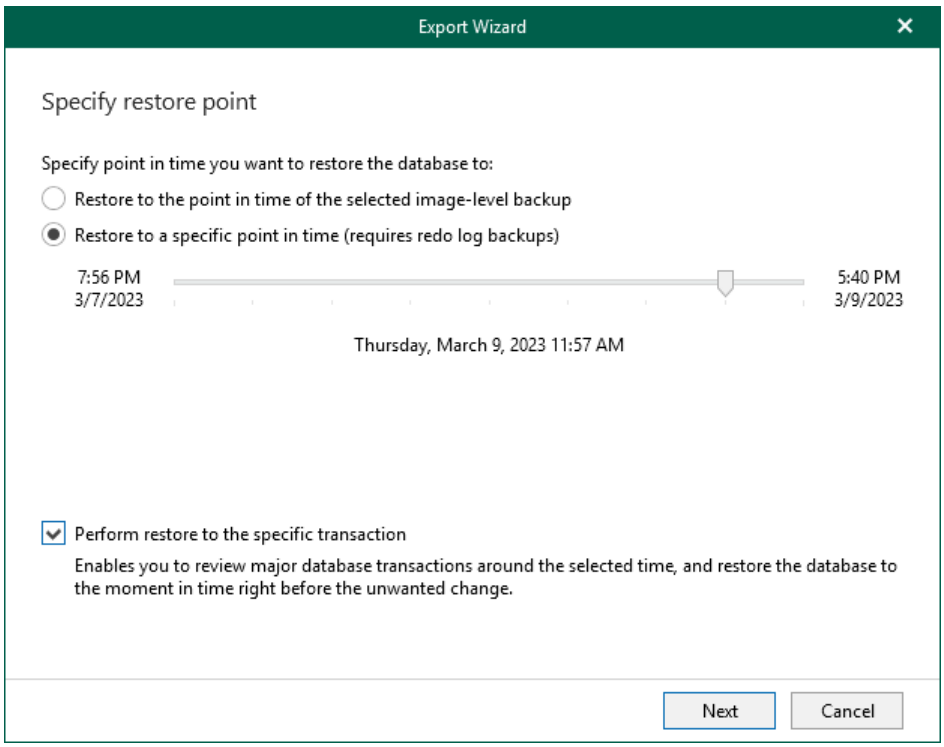
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

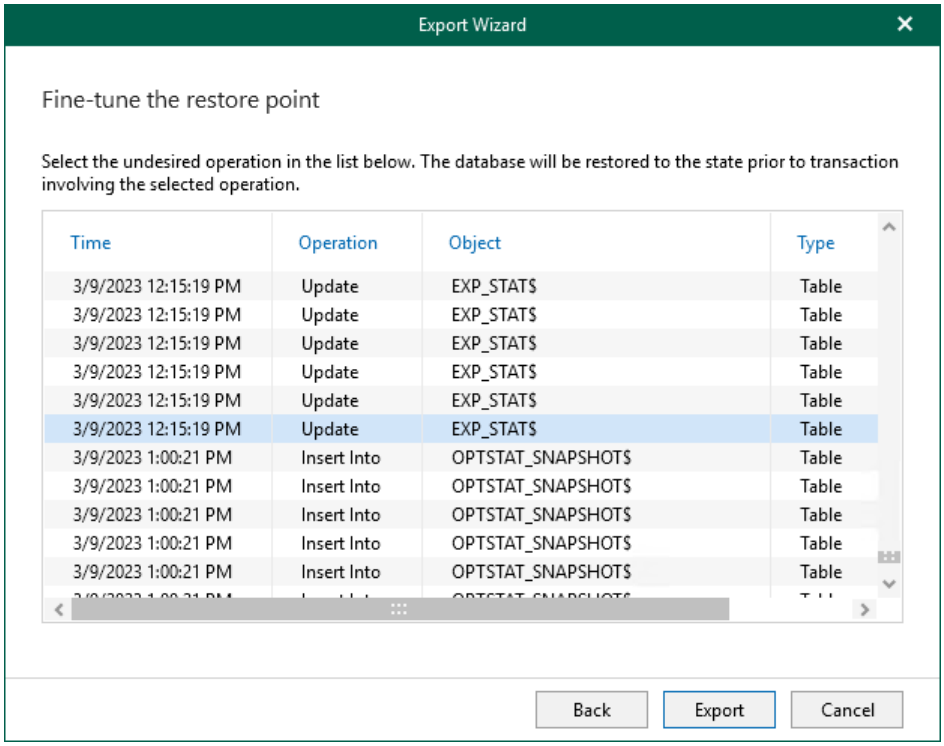
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data and click **Export**.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Exporting to Custom Location

To export a database to a custom location, do the following:

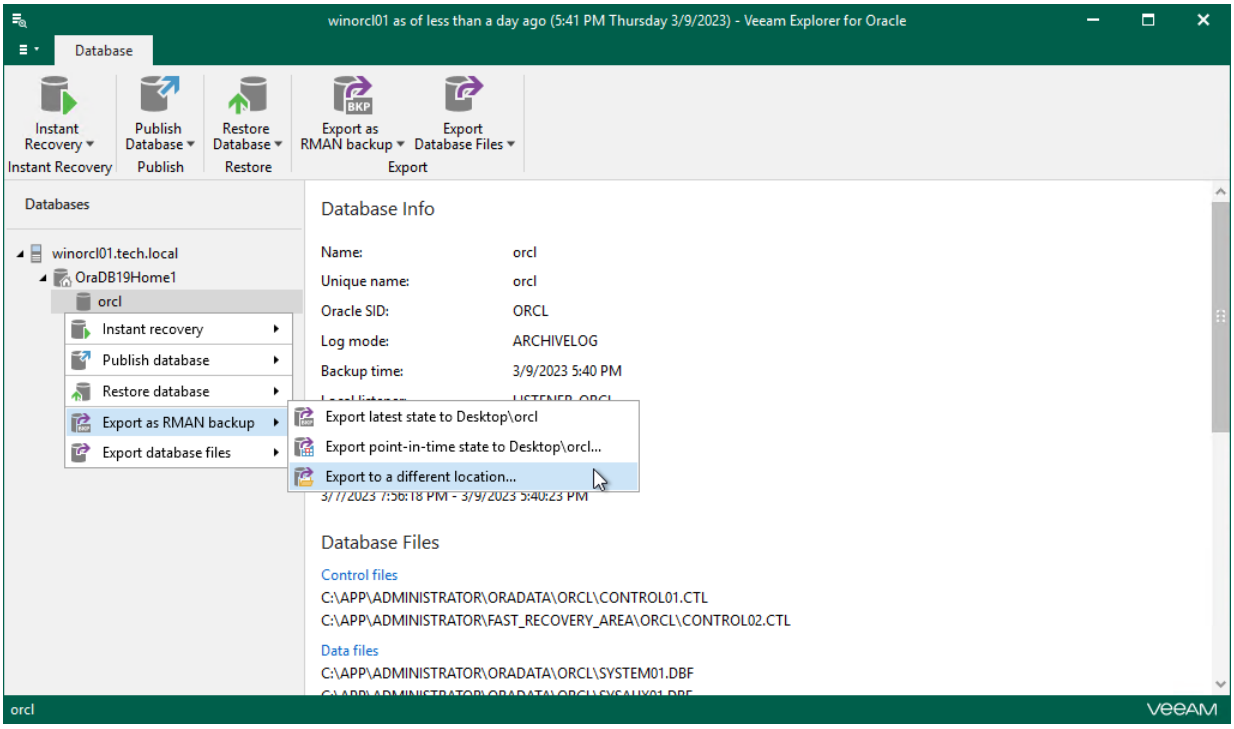
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export as RMAN backup** > **Export to a different location**.

Alternatively, you can right-click a database and select **Export as RMAN backup** > **Export to a different location**.



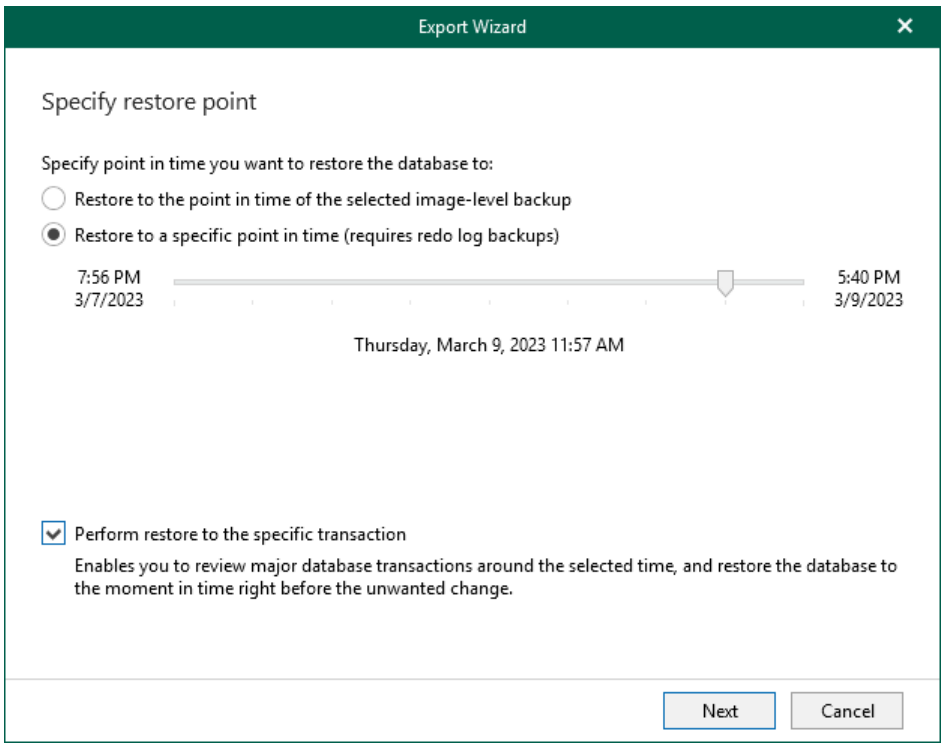
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

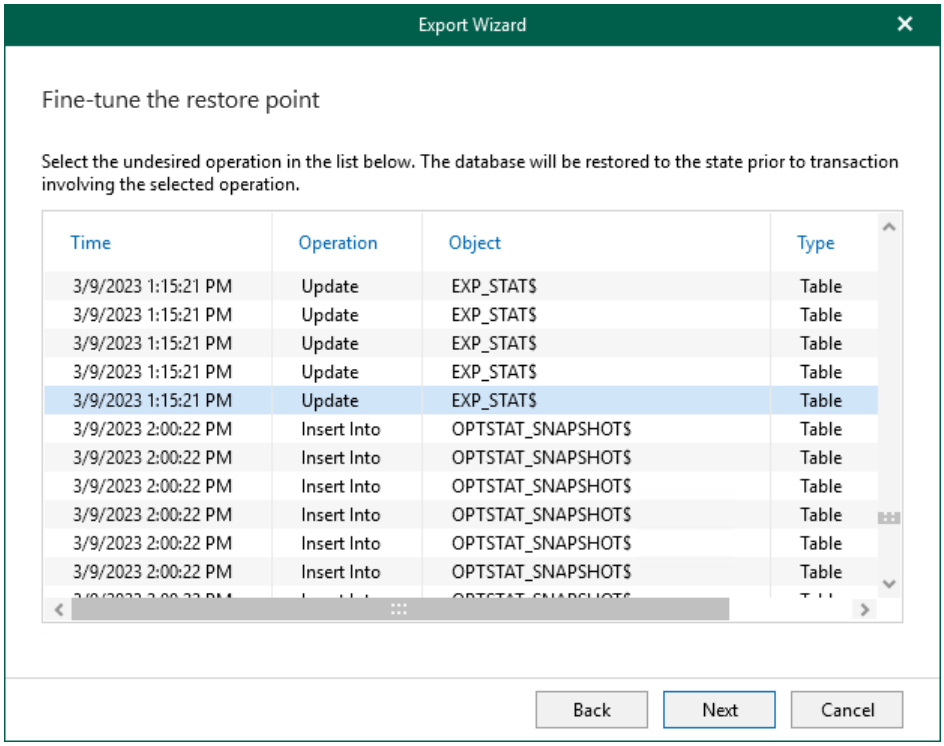
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Location

At this step of the wizard, do the following:

1. In the **Export path** field, specify the location to which you want to export database files.

   If the folder you are specifying does not exist, it will be created.

2. In the **File name format** field, specify the format according to which your files will be named after the export.

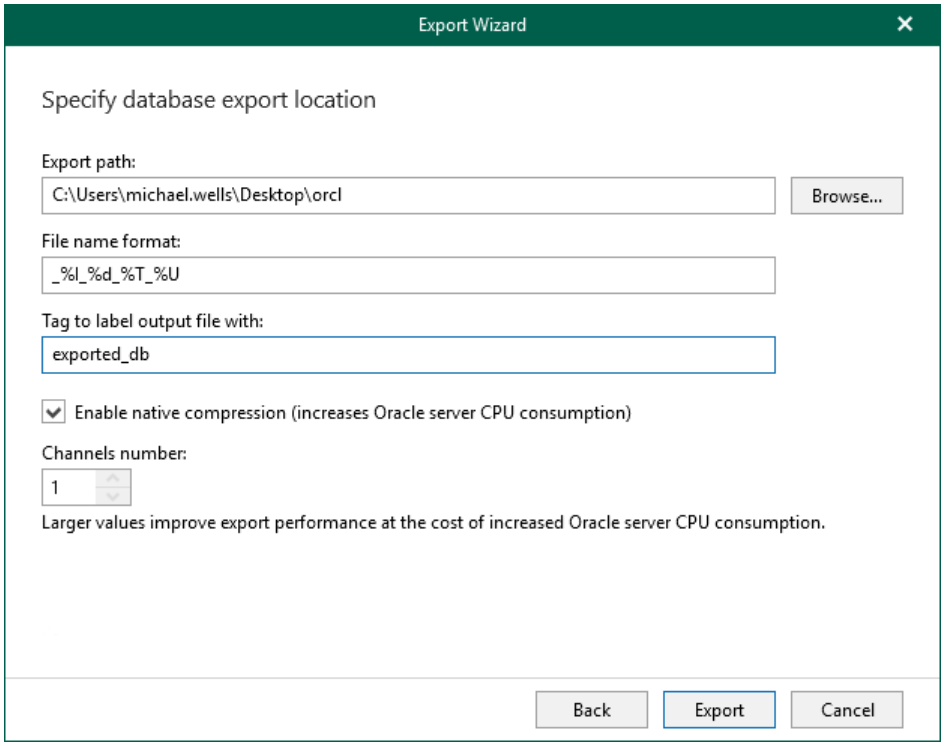
   For more information, see this Oracle article.

3. In the **Tag to label output file with** field, specify a new tag name.

4. To compress files using native Oracle compression, select the **Enable native compression** check box.

5. In the **Channels number** numeric field, specify the number of channels to be used when retrieving Oracle databases from the backup.

6. Click **Export**.



Export Database Files

This section contains information about the available export options for Oracle databases.

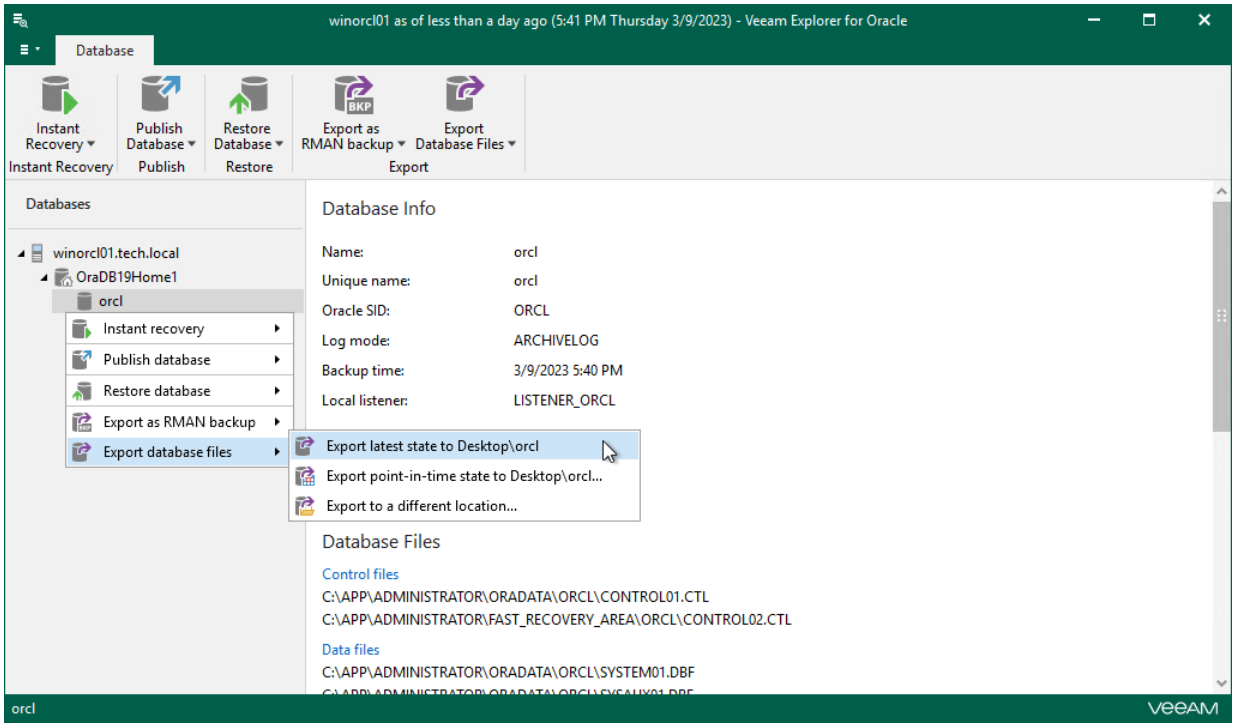
Exporting Latest State

To export data as of the latest available state, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export latest state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export database files** > **Export latest state to Desktop\<db_name>**.

> **NOTE**
>
> The name of the export option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Export latest state to Desktop\<db_name>**.
> - If you select any other restore point, the option name is displayed as **Export state of <point_in_time> to Desktop\<db_name>**.



Exporting Point-in-Time State

This section explains how to export data as of a point-in-time state.

To export data as of a point-in-time state, do the following:

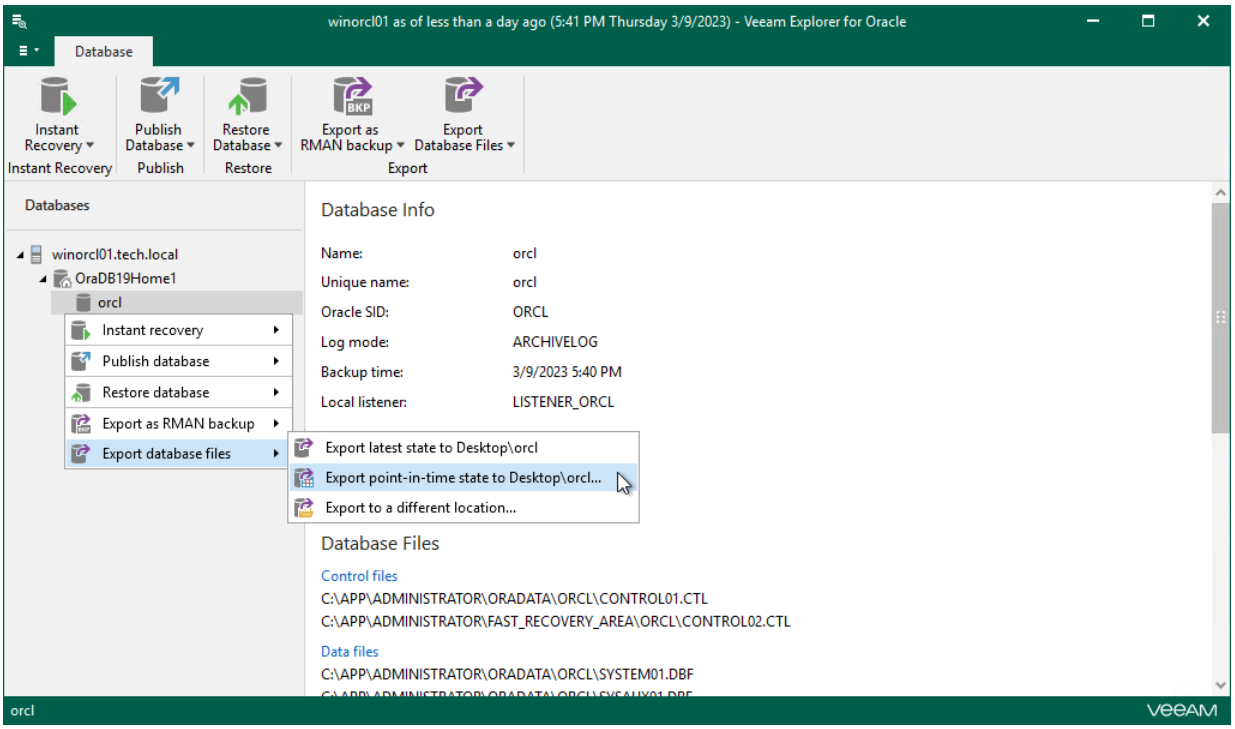
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export point-in-time state to Desktop\<db_name>**.

Alternatively, you can right-click a database and select **Export database files** > **Export point-in-time state to Desktop\<db_name>**.



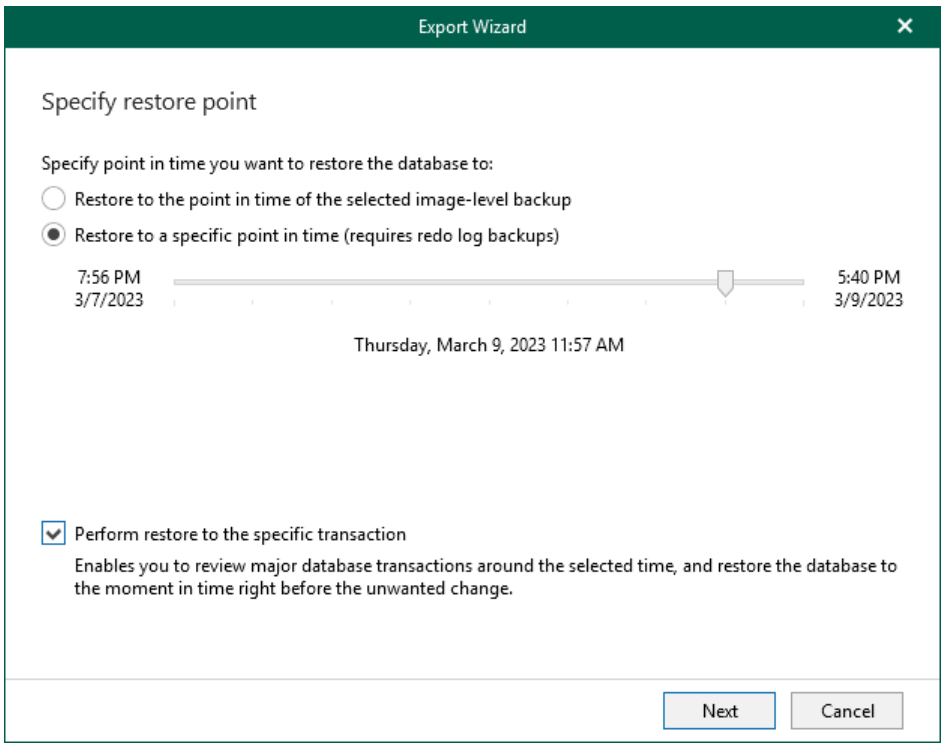
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

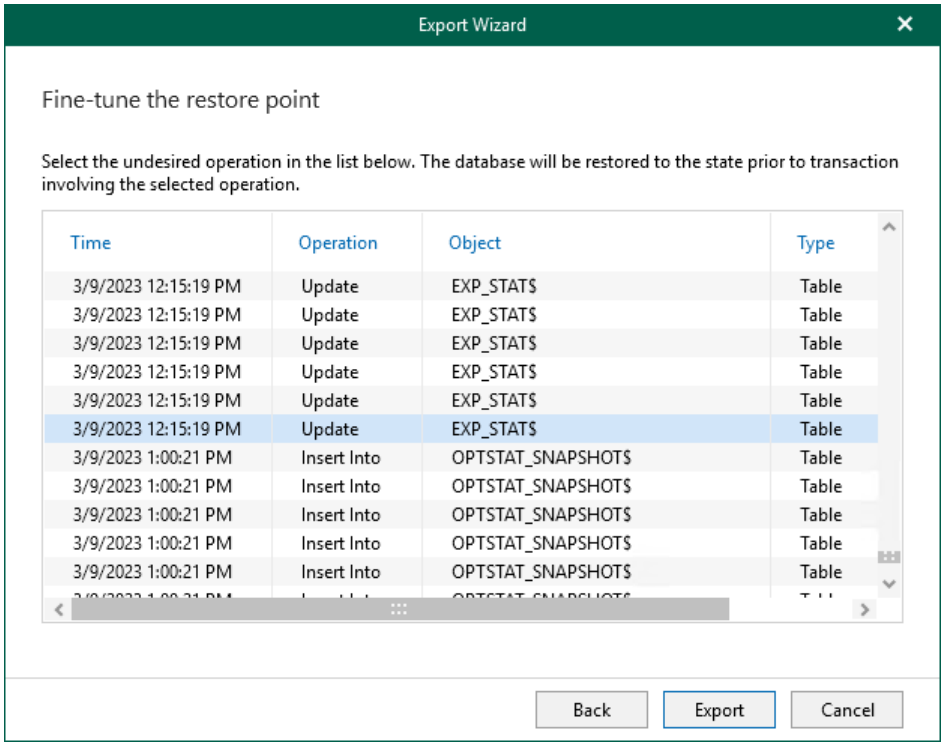
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

At this step of the wizard, select an operation prior to which you want to export data and click **Export**.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Exporting to Custom Location

This section explains how to export a database to a custom location.

To export a database to a custom location, do the following:

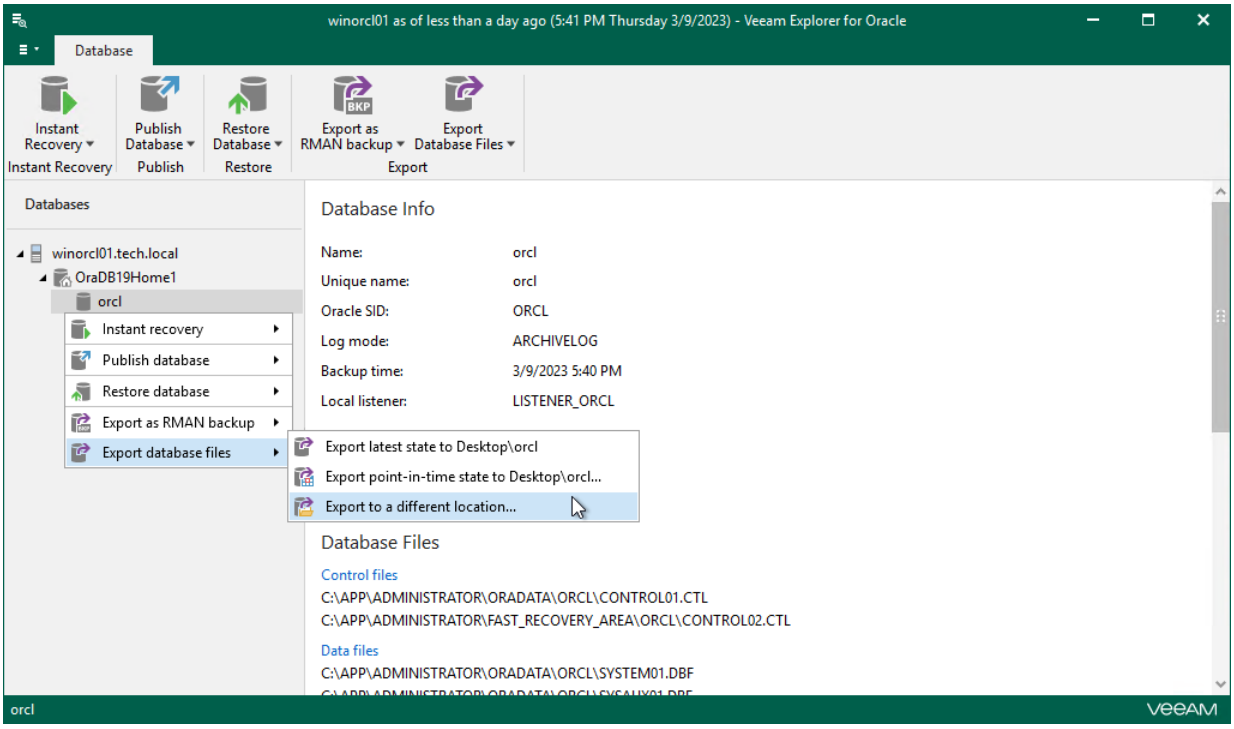
1. Launch the Export wizard.
2. Specify a restore point.
3. Fine-tune the restore point.
4. Specify the target location.

Step 1. Launch Export Wizard

To launch the **Export** wizard, do the following:

1. In the navigation pane, select a database.
2. On the **Database** tab, select **Export Database Files** > **Export to a different location**.

Alternatively, you can right-click a database and select **Export database files** > **Export to a different location**.



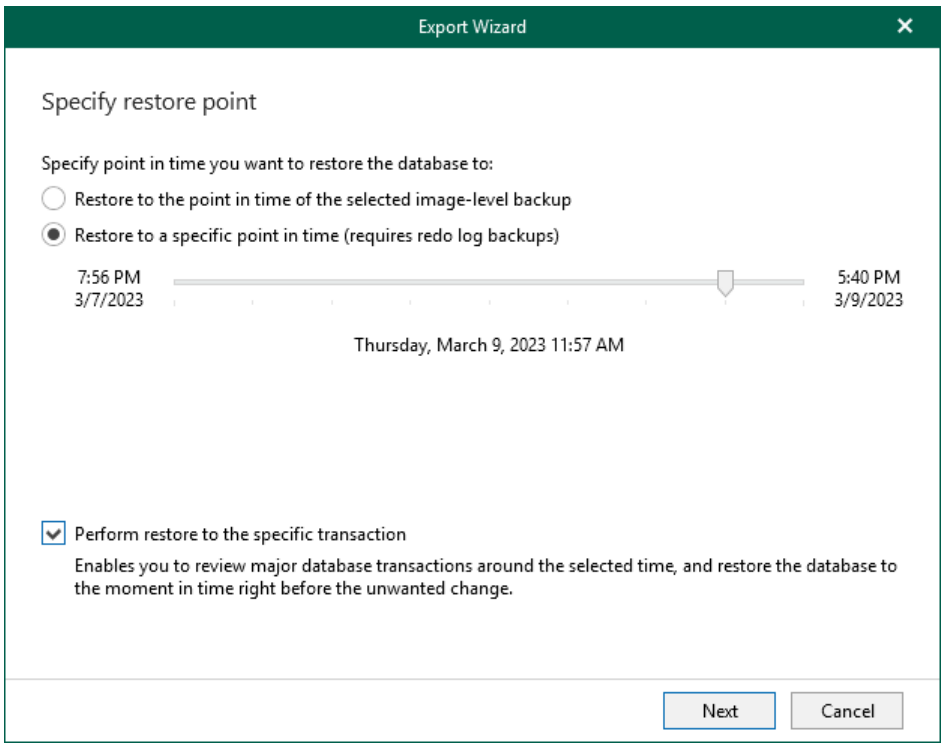
Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your database:

- Select the **Restore to the point in time of the selected image-level backup** option to load database files as per date of the current restore point.
- Select the **Restore to a specific point in time** option to load database files as per selected point in time.

  Use the slider control to choose a point you need.
- Select the **Perform restore to the specific transaction** check box to load database files exactly as of the moment before undesired transactions.

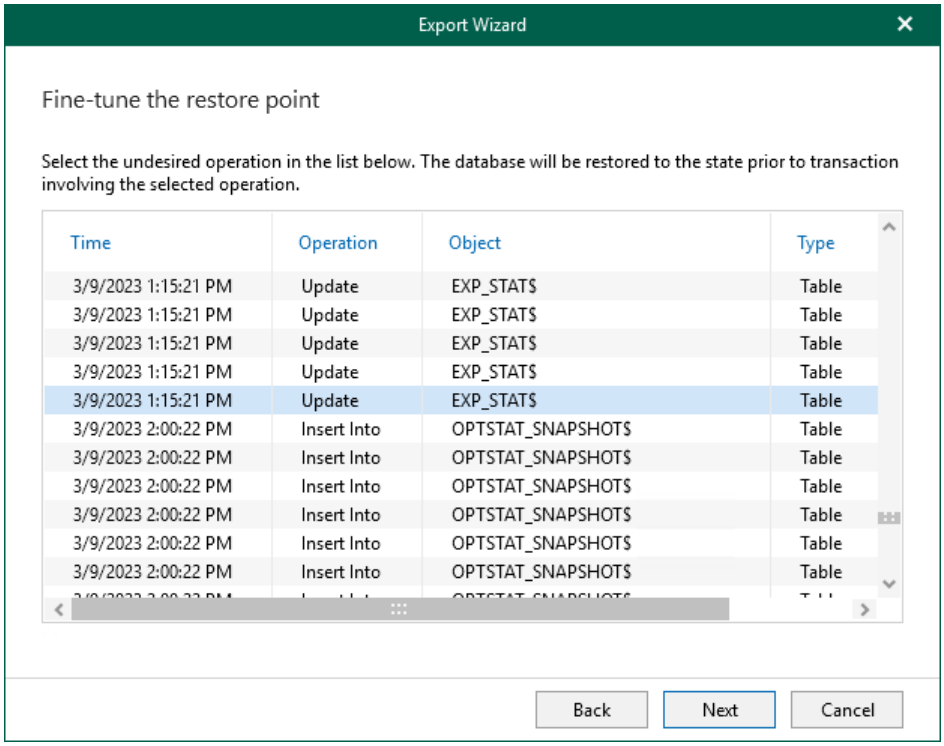
> **NOTE**
>
> The **Perform restore to the specific transaction** option requires a staging Oracle server. For more information, see Configuring Staging Oracle Server.



Step 3. Fine-Tune Restore Point

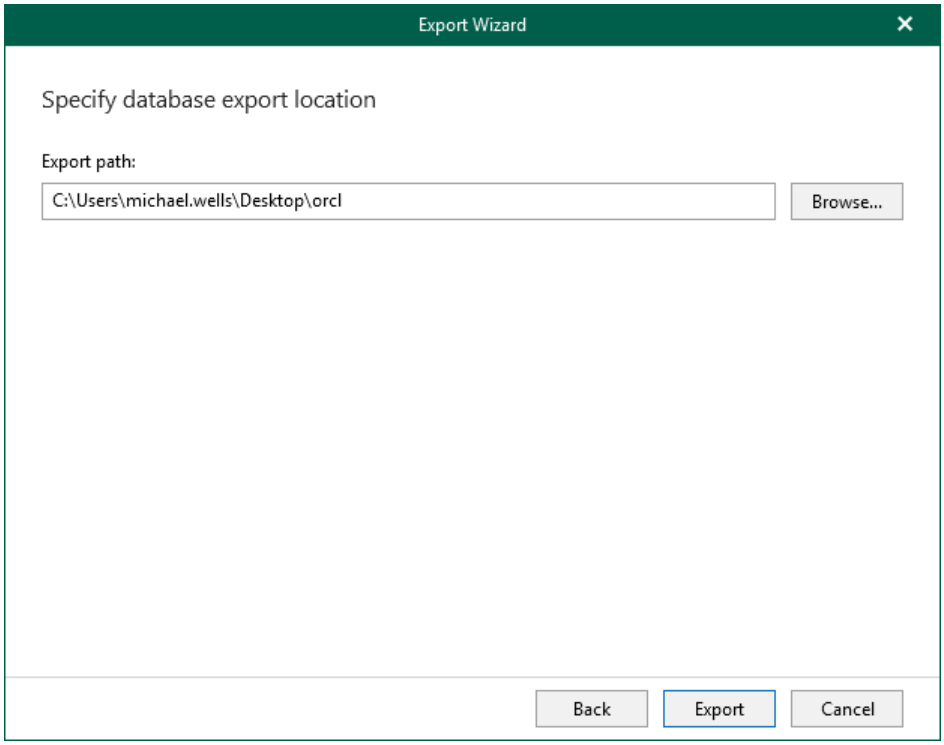
At this step of the wizard, select an operation prior to which you want to export data.

> **NOTE**
>
> This step is available only if you have selected the **Perform restore to the specific transaction** check box at the Specify Restore Point step of the wizard.



Step 4. Specify Target Location

At this step of the wizard, in the **Export path** field, specify the location to export data.



Veeam Explorer for PostgreSQL

Veeam Explorer for PostgreSQL allows you to restore and publish PostgreSQL instances from backups created by Veeam Backup & Replication.

Planning and Preparation

Before you start using Veeam Explorer for PostgreSQL, make sure your backup infrastructure meets the following requirements and limitations.

System Requirements

This section lists system requirements for Veeam Explorer for PostgreSQL.

Component	Requirement
PostgreSQL on Linux	For more information on supported versions of PostgreSQL, see the Supported Applications subsection of the Veeam Backup & Replication User Guide.

Ports

The following tables list network ports that must be opened to manage inbound and outbound traffic.

Backup

From	To	Protocol	Port	Notes
Backup server	Source Linux machine with PostgreSQL	TCP	6162	Default port used by Linux Management Agent.
		TCP	22	Default SSH port used as a control channel (without Linux Management Agent).
		TCP	2500 to 3300	**For archive logs shipping** Default range of ports used for managing data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.
Source Linux machine with PostgreSQL	Log shipping server, backup repository	TCP	2500 to 3300	**For archive logs shipping** Default range of ports used for managing data transfer over the network. Log shipping server is used in case the direct connection to the backup repository is not possible. For more information, see Log Shipping Servers.

Restore

From	To	Protocol	Port	Notes
Backup server, Veeam Backup & Replication console	Mount server	TCP	6170	Port used for connections to the mount service.
Backup repository	Target Linux machine with PostgreSQL	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) machine or another Linux machine with PostgreSQL.
Target Linux machine with PostgreSQL	Backup repository	TCP	2500 to 3300	Default range of ports used for managing data transfer during restore to the original (remote) machine or another Linux machine with PostgreSQL.
Mount server	Target Linux machine with PostgreSQL	TCP	22	Default SSH port used as a control channel.

Permissions

The following table lists the required permissions for user accounts to restore PostgreSQL data.

Operation	Required Roles and Permissions
Veeam Explorer for PostgreSQL launch	The account used to run Veeam Explorer for PostgreSQL must be a member of the local *Administrators* or *Users* group.
Restore	The account used for PostgreSQL data recovery must be a Linux user with root privileges on the target machine. Root privileges are required to mount the backed-up file system to the target server and to communicate with PostgreSQL.

Required Backup Job Settings

This requirement applies to backup jobs created by Veeam Backup & Replication.

When you create a backup job, make sure to enable the **application-aware image processing** option. For more information, see the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for PostgreSQL.

- With Veeam Explorer for PostgreSQL, you can restore and publish entire PostgreSQL instances; restore and publishing of individual databases is not supported.
- Veeam Explorer for PostgreSQL does not support restore over VIX API or vSphere Automation API.
- High availability cluster configurations and replication setups of PostgreSQL servers are not supported.
- Restore of databases that reside in an encrypted file system on the source machine is not supported. In particular, encrypted LVM volumes are not supported.
- You can restore a PostgreSQL instance over SSH only, restore using Linux Management Agent is not supported.
- If you specify another data directory for the restored PostgreSQL instance, services will not be created automatically (including systemd).
- Mount of Btrfs disks will fail if you perform data restore or data publish to the original server. The issue occurs due to restriction for mounting 2 Btrfs disks with identical IDs to the same machine.
- Before you restore a PostgreSQL instance to another server, make sure PostgreSQL is installed on the target machine.
- Veeam Explorer for PostgreSQL does not support configuration sub-files (include files such as `include_if_exist`, `include_dir` and so on). All PostgreSQL configurations, instance ports in particular, must be specified in a single `postgresql.conf` file.
- PostgreSQL on the target machine must be of the same major version as PostgreSQL on the original machine. For example, you can restore a PostgreSQL instance based on PostgreSQL 14.1 to a machine with PostgreSQL 14.3.
- The account that you use to connect to the target server must have root privileges to mount the backed-up file system to the target server and to communicate with PostgreSQL.
- To restore or publish a specific point-in-time state of a PostgreSQL instance, backups of PostgreSQL WAL archive logs must exist. To enable PostgreSQL WAL log archiving, PostgreSQL instances must have the *replica* WAL logging level or higher. The *minimal* logging level does not write information about database transactions and it allows you to create a crash-consistent backup only.
- [For Debian] When you restore a PostgreSQL instance to a new data directory, Veeam Explorer for PostgreSQL saves PostgreSQL configuration files to the specified data directory (not to the `/etc/postgresql` directory). In this case, you will not be able to discover the recovered PostgreSQL instance with the `pg_lsclusters` utility.

Launching Application

To open Veeam Explorer for PostgreSQL, you can use any of the following methods:

- The **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start** and select **Veeam Explorer for PostgreSQL**.

  If you open Veeam Explorer for PostgreSQL on a machine that is not a backup server but runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following settings for connection to the backup server:

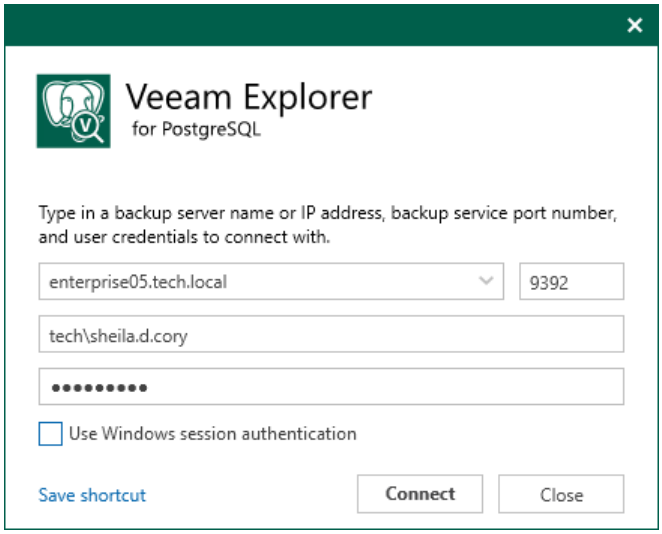
  - Domain name or IP address of the backup server to which you want to connect
  - Port number
  - User account credentials

    To use the account under which Veeam Explorer for PostgreSQL is running, select **Use Windows session authentication**.

    Consider the following:

    - To perform recovery operations, run Veeam Explorer for PostgreSQL with elevated permissions. The user account must be a member of the local Administrators group on the machine where Veeam Explorers are installed.
    - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

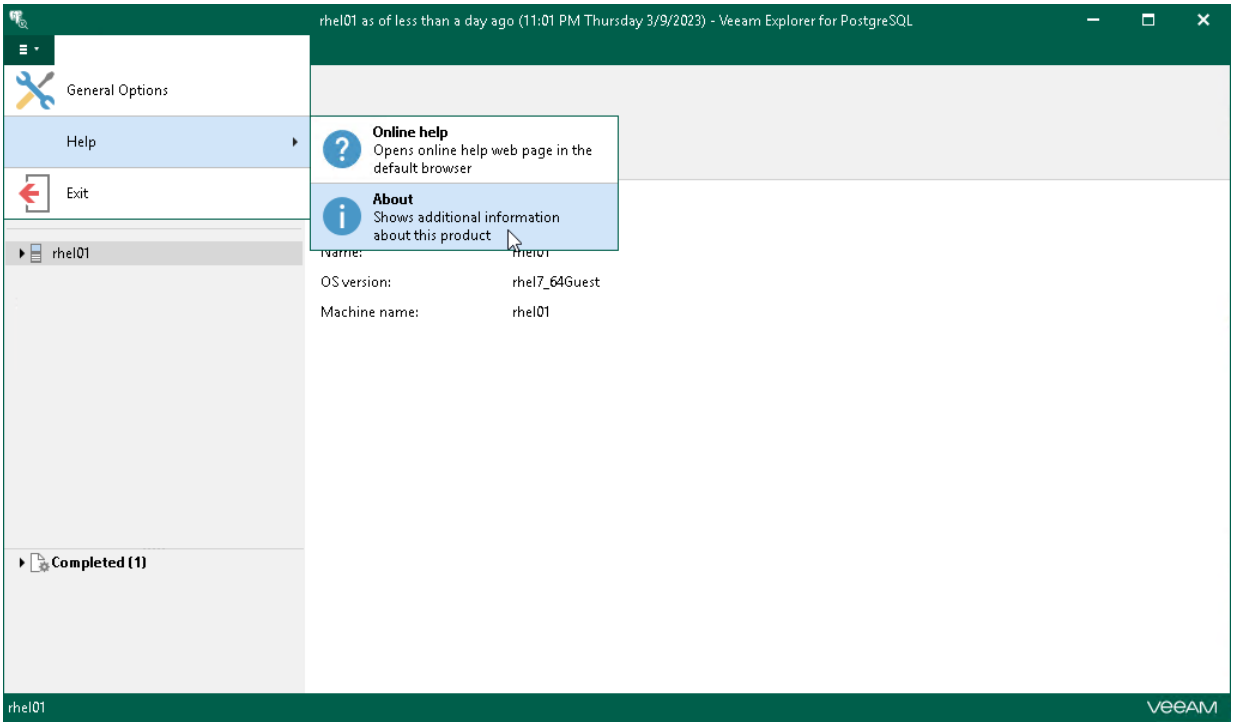
The user interface of Veeam Explorer for PostgreSQL is designed to let you quickly find commands that you need to restore PostgreSQL instances from backups.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to enable extended logging. For more information, see Enabling Extended Logging.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for PostgreSQL window.

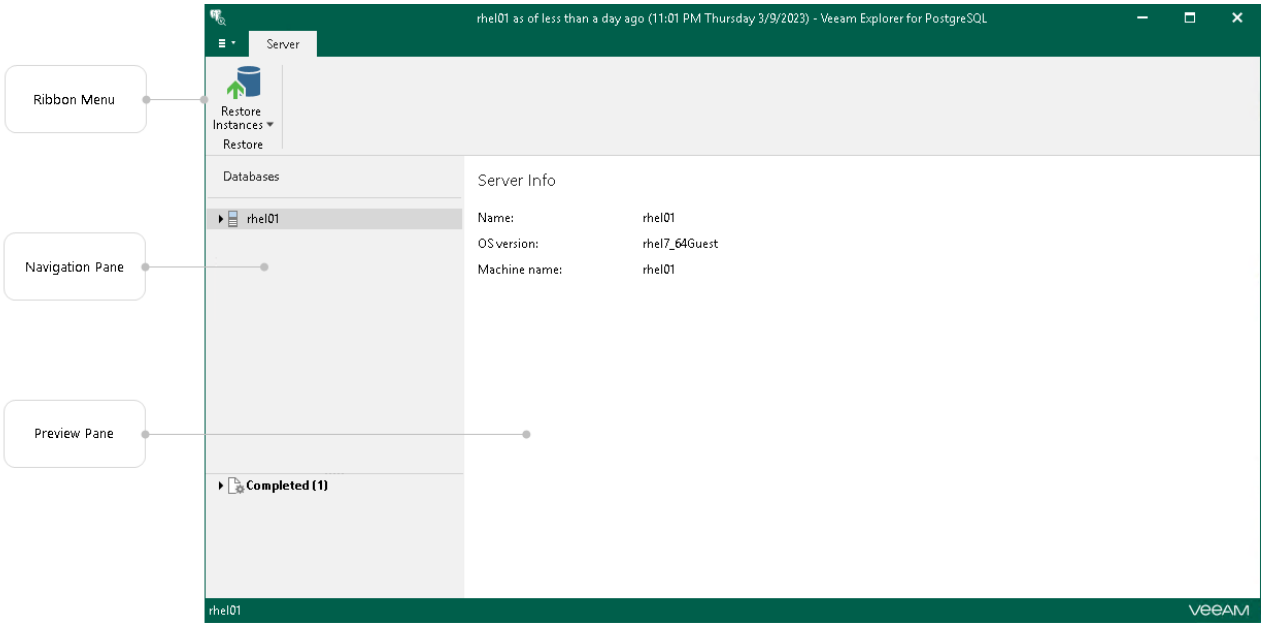
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for PostgreSQL wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.
- The navigation pane that allows you to browse through the hierarchy of folders with backed-up data.
- The preview pane that allows you to view details about items that are contained in a folder you have selected in the navigation pane.



How Mounting Works

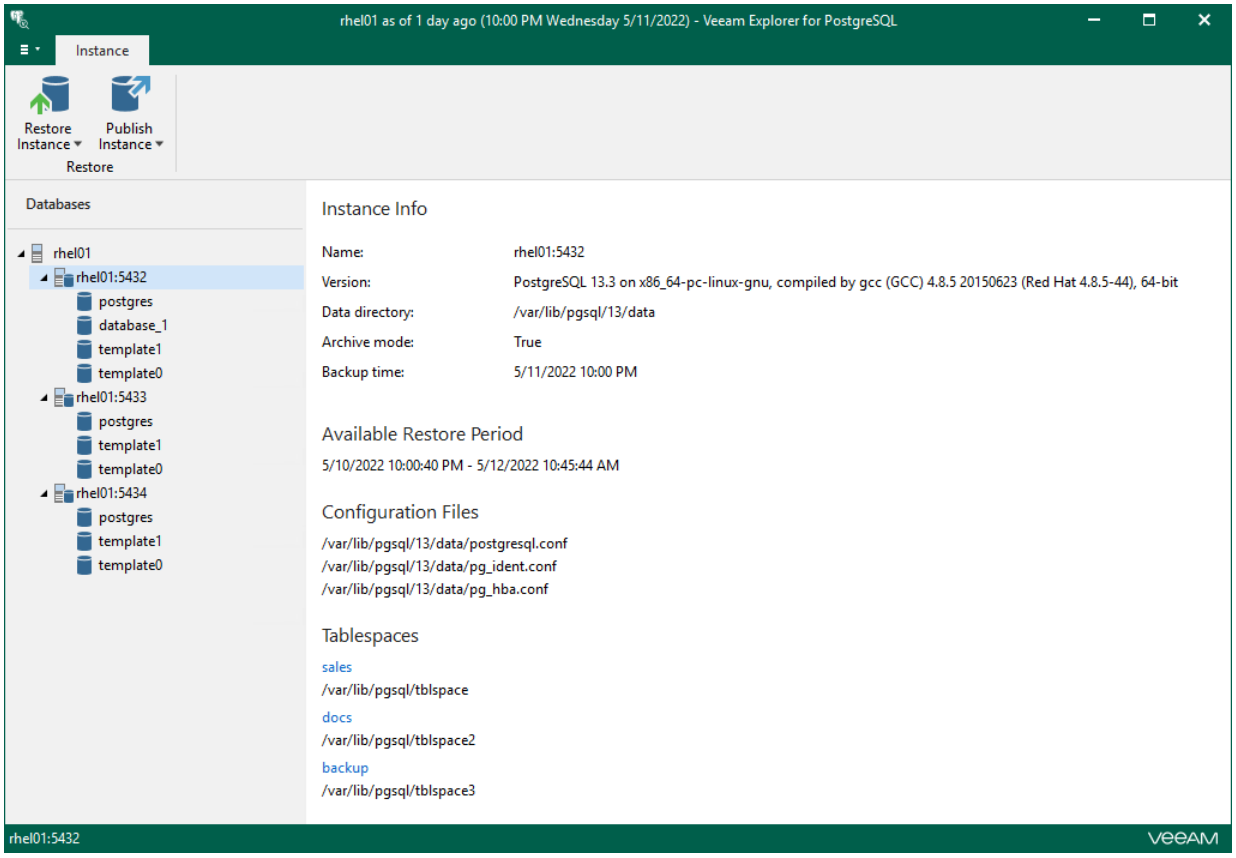
When restoring your data, Veeam Explorer for PostgreSQL requires an additional mount point to be created to display the list of available transactions.

Mounting is performed by the *Veeam Mount Service* component which is deployed on a backup repository machine or any other machine you define in the backup repository settings. For more information on configuring mount server settings, see the Mount Server section of the Veeam Backup & Replication User Guide.

During mounting, *Veeam Mount Service* retrieves a VM file system from the backup file, attaches it to the hard drive of a target machine and creates a mount point. To mount a VM file system to the target VM, Veeam Backup & Replication uses FUSE.

Viewing Instance Information

To view PostgreSQL instance information, select an instance in the navigation pane and review its properties in the preview pane.

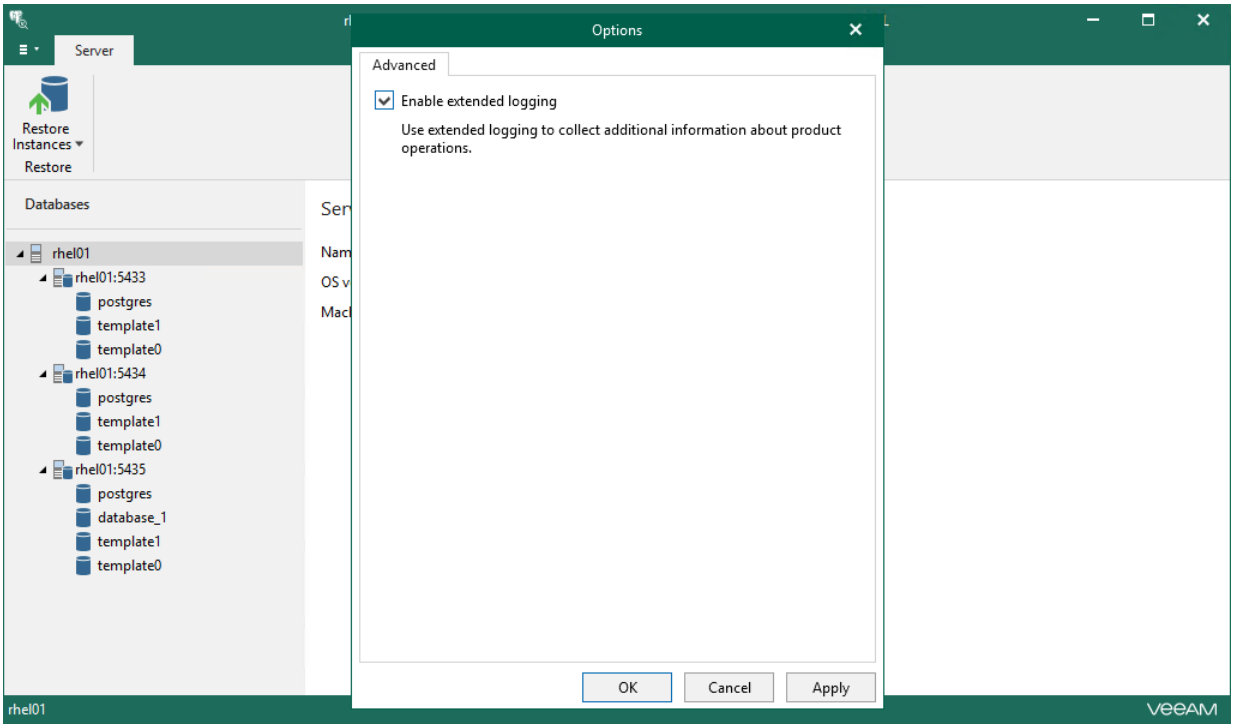


Enabling Extended Logging

Veeam Explorer for PostgreSQL allows you to enable an extended logging mode to collect logs that contain more details on specific operations. After you enable extended logging, you can go back to the application and perform the actions for which you want to collect additional information. Then you can collect the logs.

To enable extended logging, do the following:

1. In the main menu, click **General Options**.
2. On the **Advanced** tab, select the **Enable extended logging** check box and click **OK**.



Data Restore

You can restore a single PostgreSQL instance or multiple PostgreSQL instances at a time.

Before restoring data, read the Considerations and Limitations section.

Restoring Single Instance

You can restore a PostgreSQL instance by following one of the scenarios:

- Restoring Latest State
- Restoring Point-in-Time State
- Restoring to Another Server

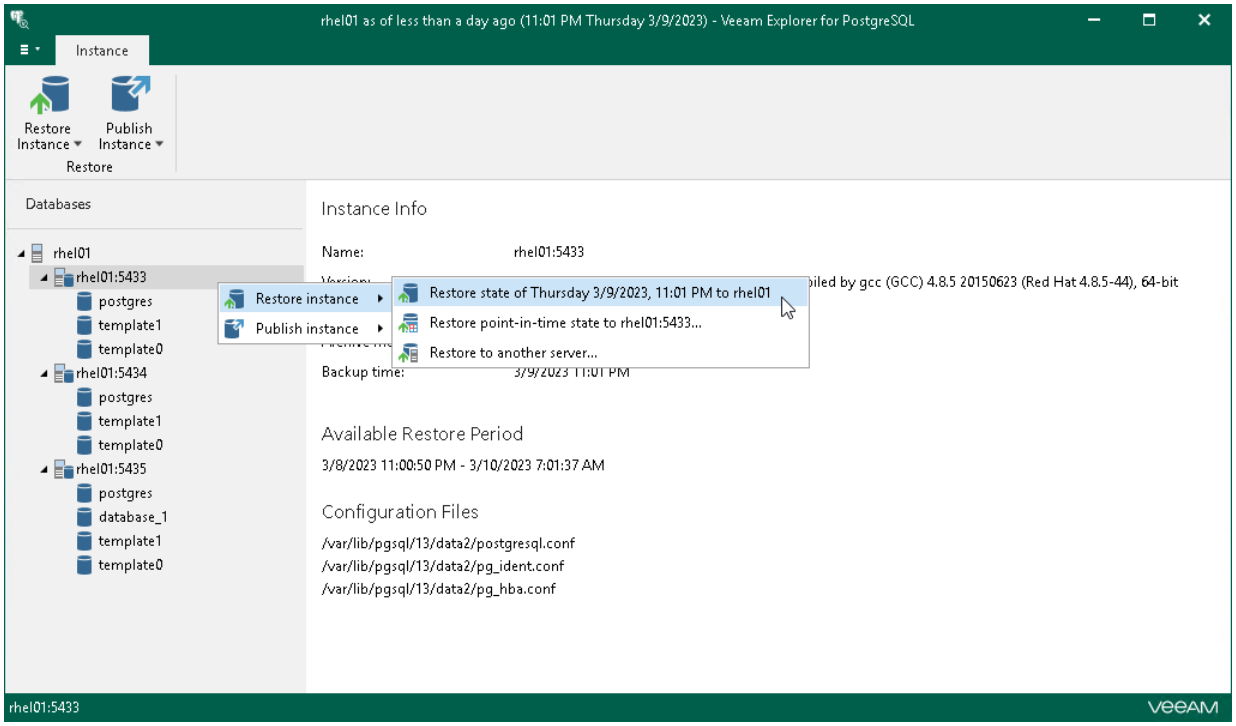
Restoring Latest State

To restore the latest state of a PostgreSQL instance, do the following:

1. In the navigation pane, select a PostgreSQL instance you want to restore.
2. On the **Instance** tab, select **Restore Instance** > **Restore latest state to <original_location>**.

Alternatively, you can right-click an instance and select **Restore instance** > **Restore latest state to <original_location>**.

> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Restoring Point-in-Time State

To restore a point-in-time state of a PostgreSQL instance, use the **Restore** wizard.

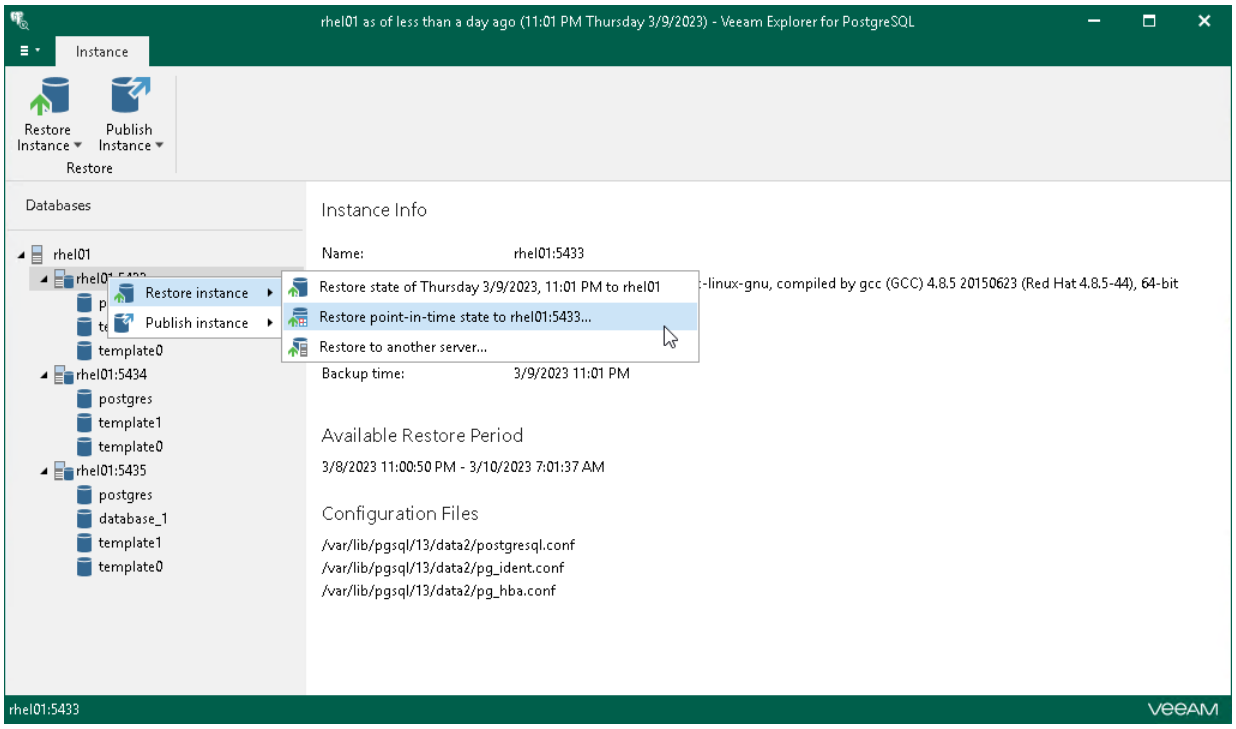
1. Launch the Restore wizard.
2. Specify a restore point.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a PostgreSQL instance you want to restore.
2. On the **Instance** tab, select **Restore Instance** > **Restore point-in-time state to <server_name>**.

Alternatively, you can right-click an instance and select **Restore Instance** > **Restore point-in-time state to <server_name>**.

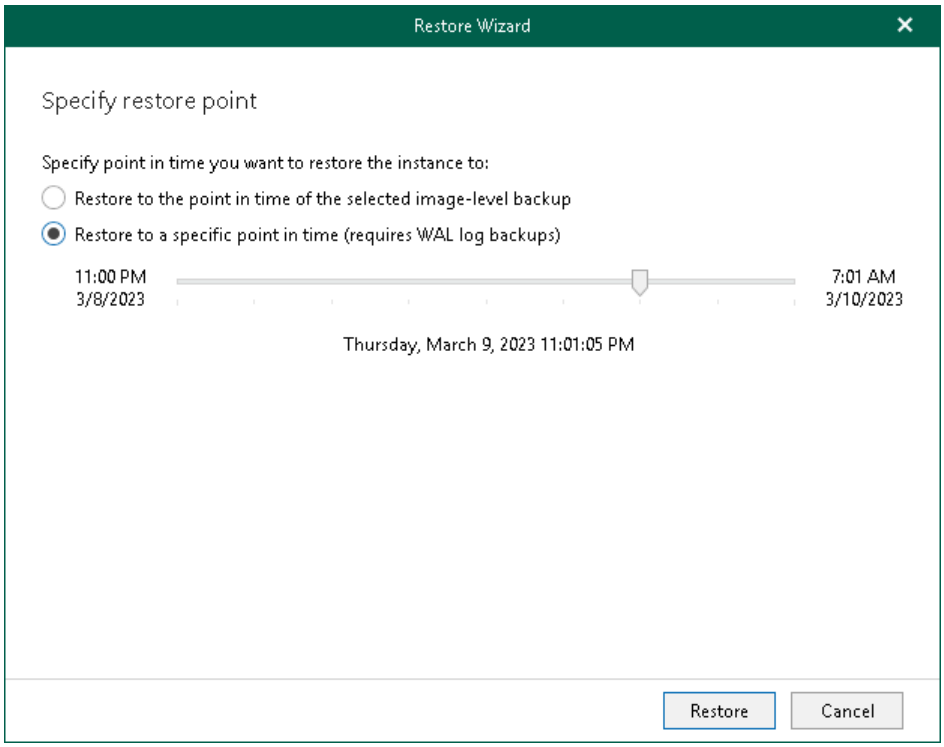


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.

  The **Restore to a specific point in time** option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.



Restoring to Another Server

You can restore a PostgreSQL instance to another server or to the same server but with different settings.

To restore a PostgreSQL instance, use the **Restore** wizard.

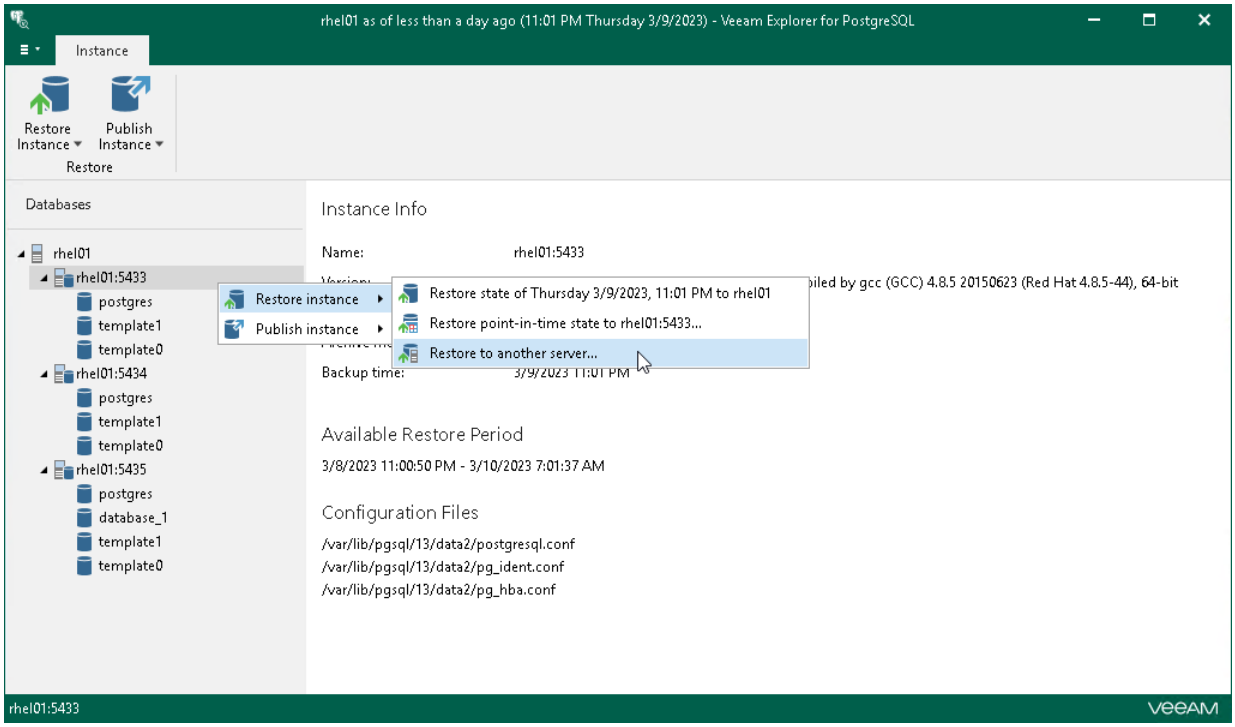
1. Launch the Restore wizard.
2. Specify a restore point.
3. Specify a target server.
4. Specify PostgreSQL settings.
5. Specify tablespaces.
6. Specify a post-restore action.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a PostgreSQL instance you want to restore.
2. On the **Instance** tab, select **Restore Instance** > **Restore to another server**.

Alternatively, you can right-click an instance and select **Restore Instance** > **Restore to another server**.

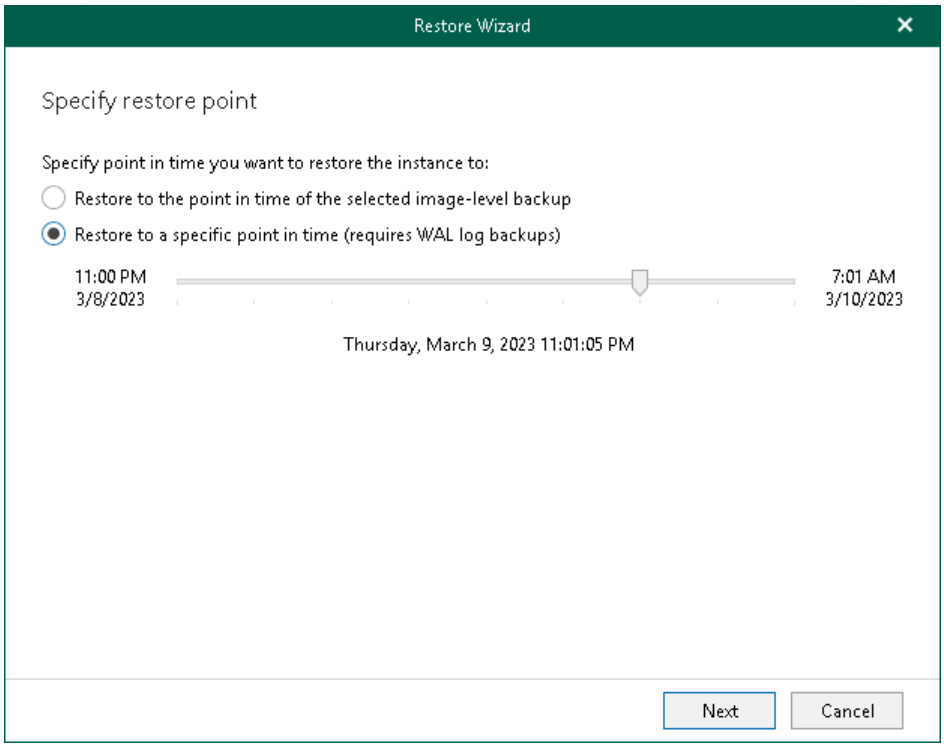


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.

  The **Restore to a specific point in time** option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.



Step 3. Specify Target Server

At this step of the wizard, specify credentials to access the target PostgreSQL server.

1. In the **Server** field, enter a DNS name or IP address of the target server.
2. In the **SSH port** field, specify an SSH port (by default, port 22 is used).
3. In the **Account** filed, specify a Linux system account name under which to connect to the specified server.
4. If you have specified a non-root account that does not have root privileges on the target server, click **Advanced**:
   a. Select the **Elevate specified account to root** check box.

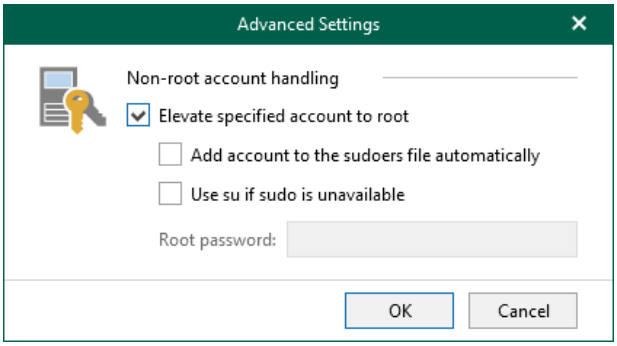
      The account must have root privileges to mount the backed-up file system to the target server and to communicate with PostgreSQL.

   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

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

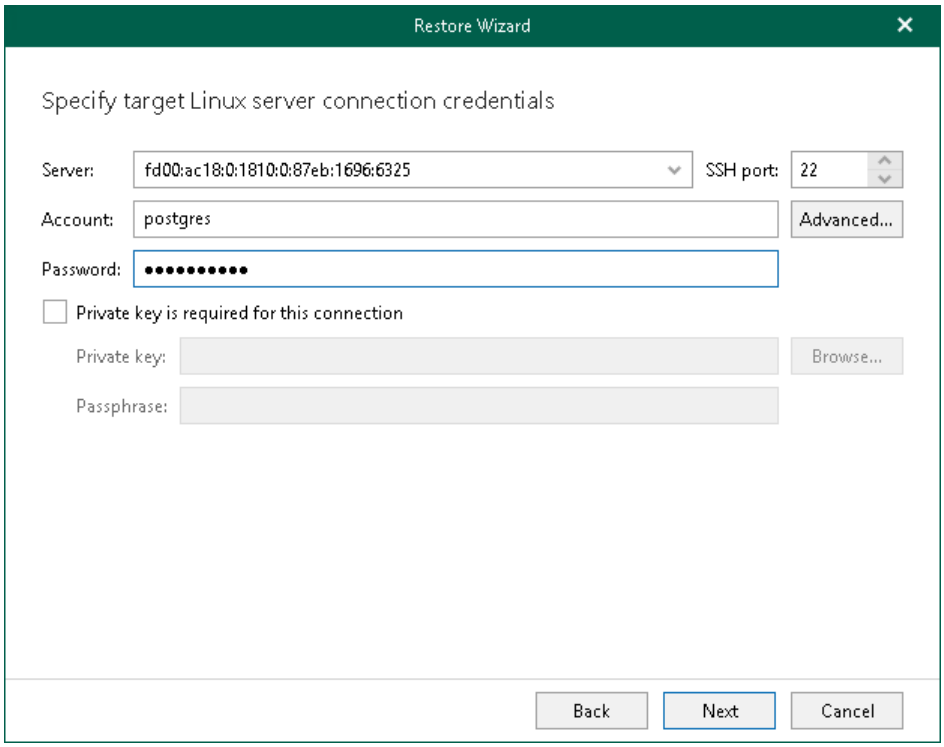
      Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.



5. In the **Password** field, enter the account password.
6. If a private key is required to connect to the server, do the following:
   b. Select the **Private key is required for this connection** check box.
   c. In the **Private key** filed, specify a file that contains a private key.

      To locate a file, click **Browse** and select a key.

d. In the **Passphrase** field, enter the passphrase used to decrypt the private key.



Step 4. Specify PostgreSQL Settings

At this step of the wizard, specify the following PostgreSQL settings:

1. Specify a location to which you want to restore the PostgreSQL instance:
   - Select **Restore to the original location** to restore the PostgreSQL instance to the original data directory.
   - Select **Restore to a different location** and specify a path in the **Data directory path** field to restore the PostgreSQL instance to another directory. To locate a new directory, click **Browse** and select a folder you want to use.
2. In the **Instance port** field, specify an instance port, which will also serve as an instance identifier. The port must be free. If the specified port is occupied, the recovered PostgreSQL will be shut down.

   To start the PostgreSQL instance manually, do the following:

   a. Change the port number in the `postgresql.conf` file.

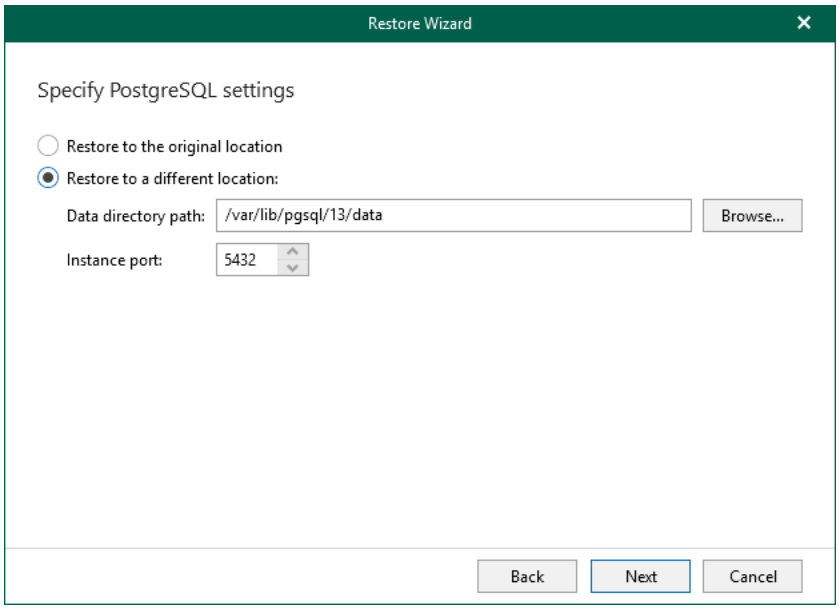
   b. Launch the PostgreSQL instance with the `pg_ctl` command:

   ```
   $ pg_ctl start -D <data_directory>
   ```

   where `<data_directory>` is a data directory of the PostgreSQL instance.

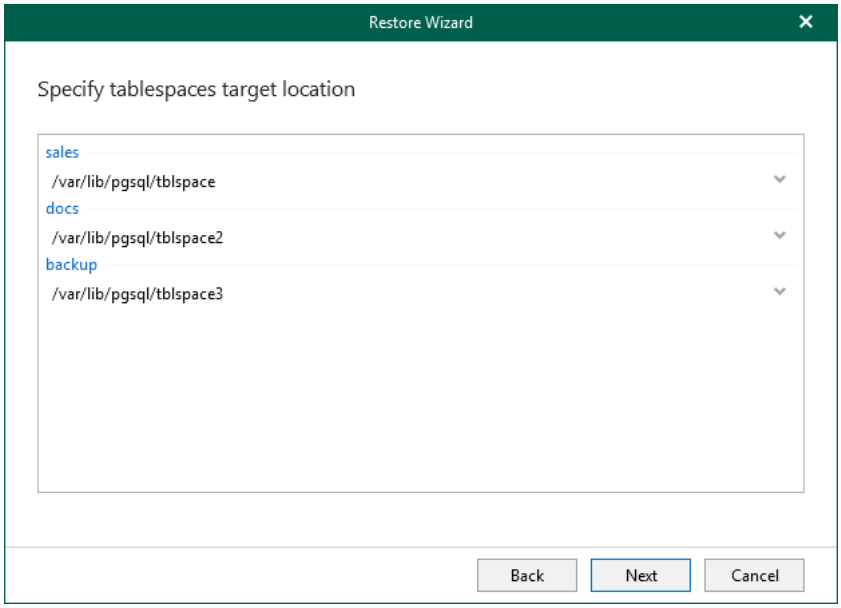
   For example:

   ```
   $ pg_ctl start -D /var/lib/pgsql/13/data
   ```



Step 5. Specify Tablespaces

At this step of the wizard, specify paths of directories where database tables will be stored.



Step 6. Specify Post-Restore Action

This step is available only if you have selected the **Restore to a specific point in time option** at the Specify restore point step of the wizard.

At this step of the wizard, select one of the following post-restore actions that the PostgreSQL instance must take after the instance is restored:

- Select **Promote the PostgreSQL server to accept connections once recovery is finished** to make the PostgreSQL instance available for connections.
- Select **Pause recovery process and keep the PostgreSQL server in recovery mode** to make the PostgreSQL instance run but not accepting incoming remote TCP connections.

  To resume the paused state, use the `pg_wal_replay_resume()` command:

  ```
  psql -p <port> -c "SELECT pg_wal_replay_resume();"
  ```

  where `<port>` is a port number of the PostgreSQL instance.
- Select **Shut down the PostgreSQL server once recovery process is completed** to make the PostgreSQL instance stop upon recovery.

  In this case, you will need to start the PostgreSQL instance manually:

  a. Change or remove the `recovery.signal` configuration file.

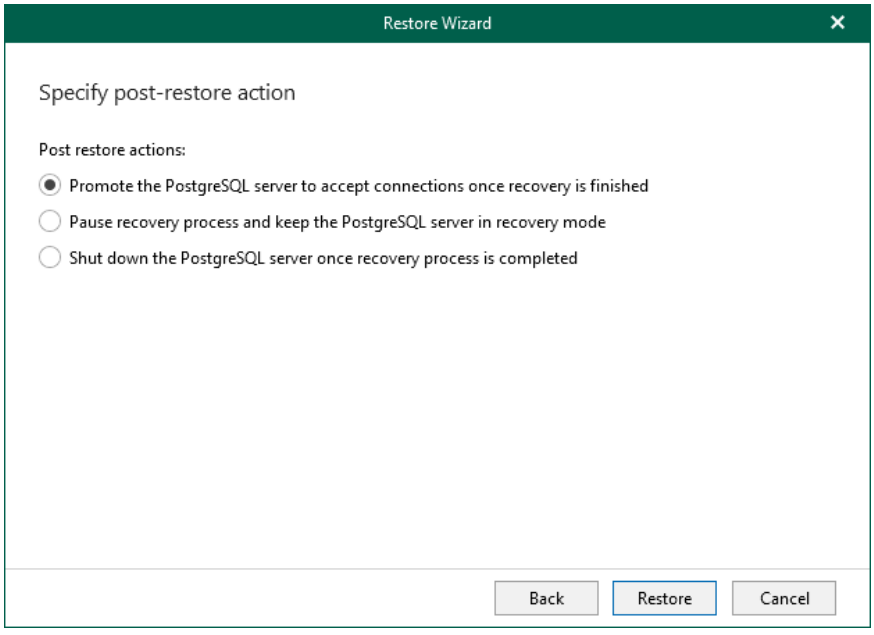
  b. Launch the PostgreSQL instance with the `pg_ctl` command:

  ```
  $ pg_ctl start -D <data_directory>
  ```

  where `<data_directory>` is a data directory of the PostgreSQL instance.

  For example:

  ```
  $ pg_ctl start -D /var/lib/pgsql/13/data
  ```



Restoring Multiple Instances

You can restore multiple PostgreSQL instances by following one of the scenarios:

- Restoring Latest State
- Restoring Point-in-Time State
- Restoring to Another Server

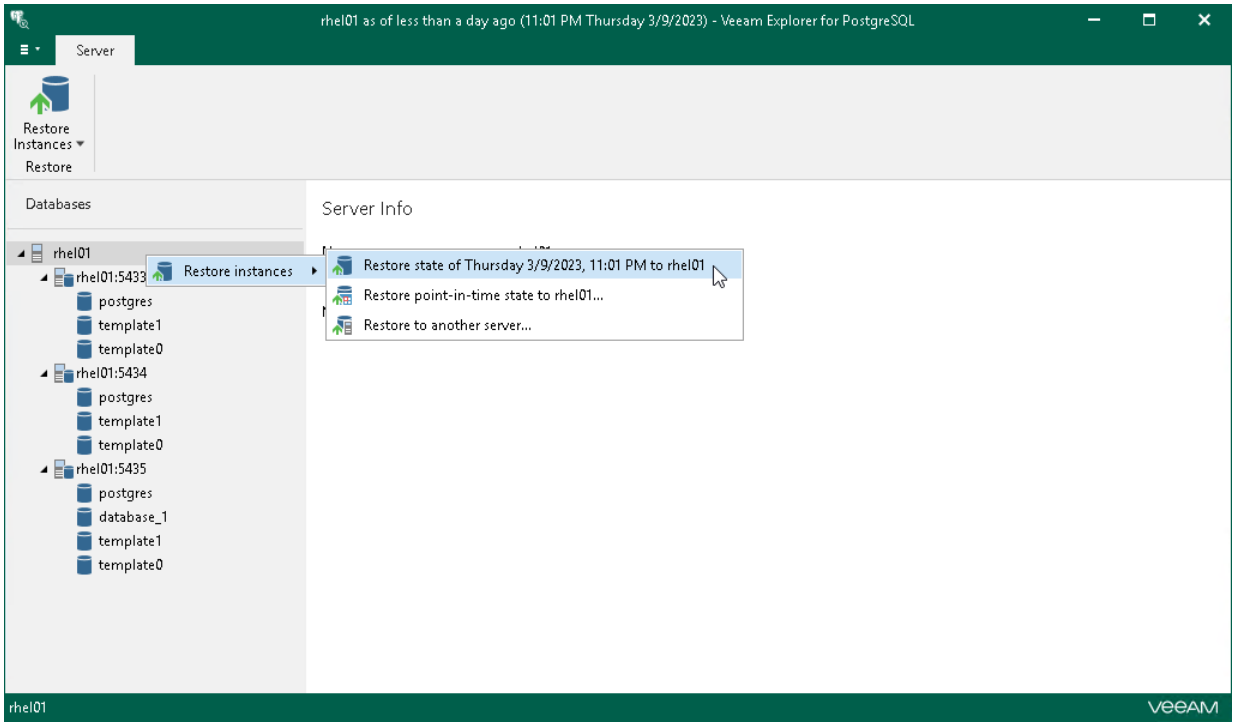
Restoring Latest State

To restore the latest state of the PostgreSQL server, do the following:

1. In the navigation pane, select the PostgreSQL server.
2. On the **Server** tab, select **Restore Instances** > **Restore latest state to <original_location>**.

Alternatively, you can right-click the server and select **Restore instances** > **Restore latest state to <original_location>**.

> **NOTE**
>
> The name of the restore option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Restore latest state to <original_location>**.
> - If you select any other restore point, the option name is displayed as **Restore state of <point_in_time> to <original_location>**.



Restoring Point-in-Time State

To restore a point-in-time state of the PostgreSQL server, use the **Restore** wizard.

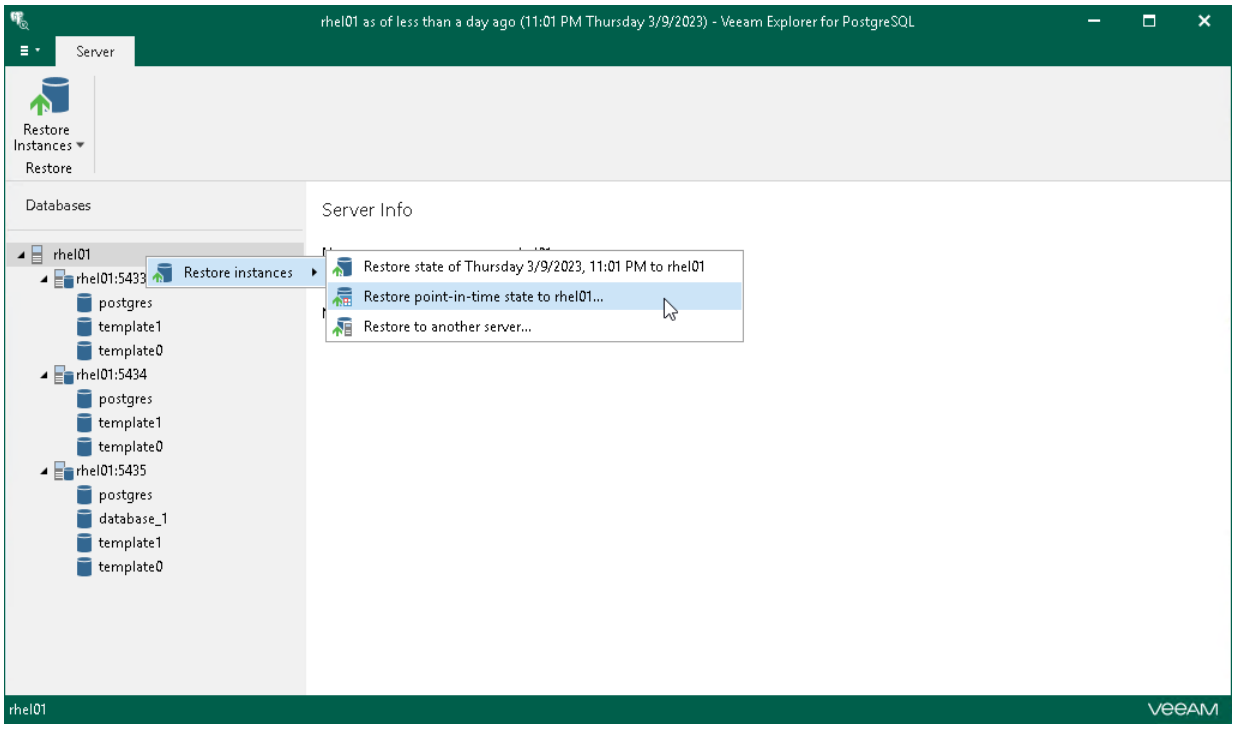
1. Launch the Restore wizard.
2. Specify a restore point.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a PostgreSQL instance you want to restore.
2. On the **Server** tab, select **Restore Instances** > **Restore point-in-time state to <server_name>**.

Alternatively, you can right-click an instance and select **Restore Instances** > **Restore point-in-time state to <server_name>**.

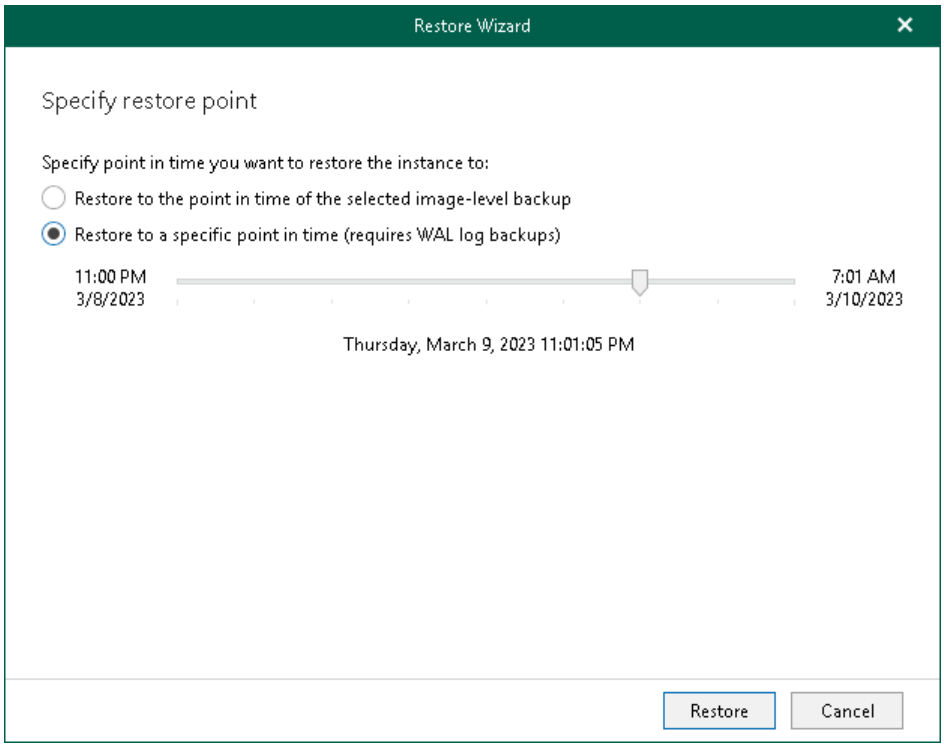


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.

  The **Restore to a specific point in time** option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.



Restoring to Another Server

You can restore multiple PostgreSQL instances to another server or to the same server but with different settings.

To restore PostgreSQL instances, use the **Restore** wizard.

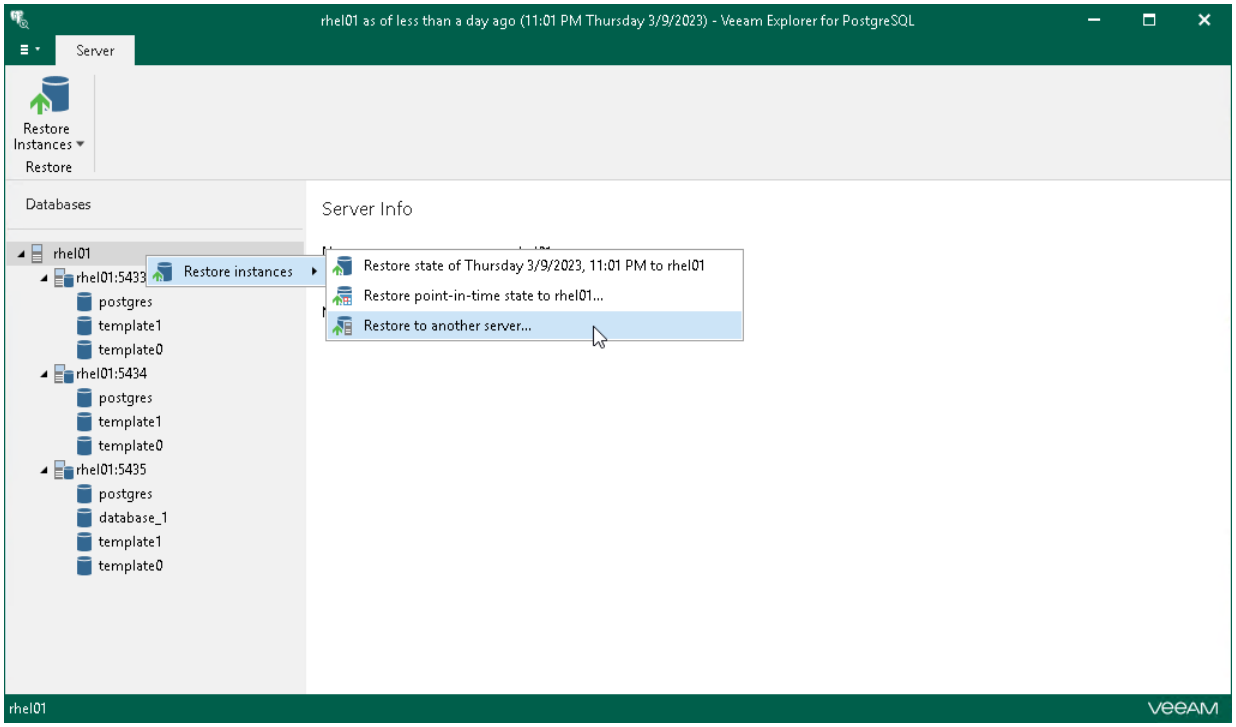
1. Launch the Restore wizard.
2. Specify a restore point.
3. Specify a target server.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select the PostgreSQL server.
2. On the **Server** tab, select **Restore Instances** > **Restore to another server**.

Alternatively, you can right-click an instance and select **Restore Instances** > **Restore to another server**.

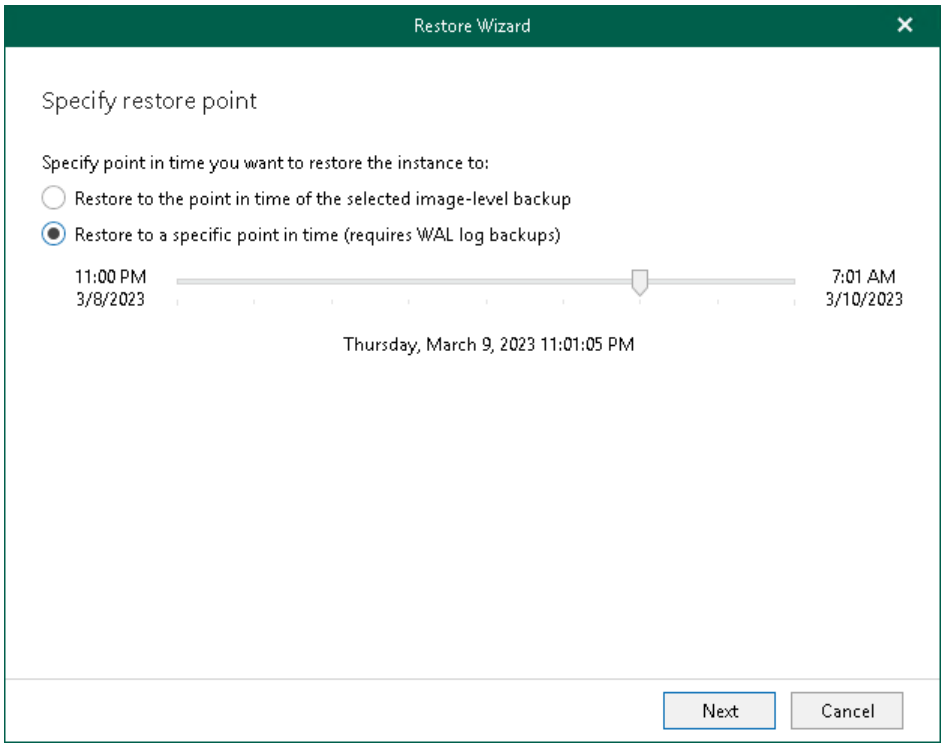


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore your data:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.

  The **Restore to a specific point in time** option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.



Step 3. Specify Target Server

At this step of the wizard, specify credentials to access the target PostgreSQL server.

1. In the **Server** field, enter a DNS name or IP address of the target server.
2. In the **SSH port** field, specify an SSH port (by default, port 22 is used).
3. In the **Account** filed, specify a Linux system account name under which to connect to the specified server.
4. If you have specified a non-root account that does not have root privileges on the target server, click **Advanced**:
   a. Select the **Elevate specified account to root** check box.

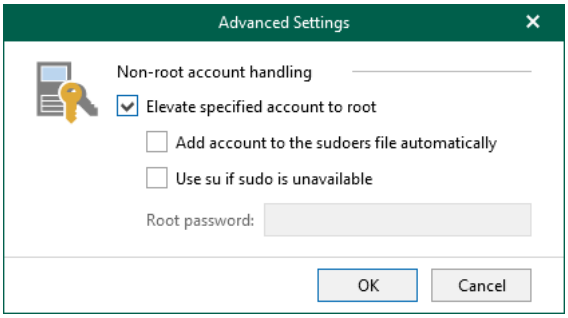
      The account must have root privileges to mount the backed-up file system to the target server and to communicate with PostgreSQL.

   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

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

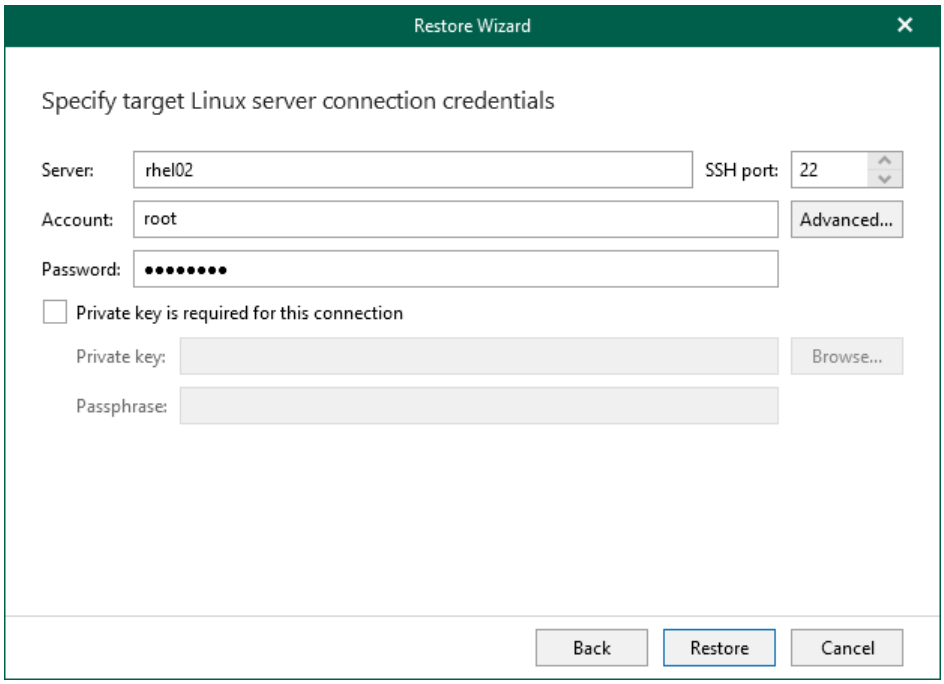
      Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.



5. In the **Password** field, enter the account password.
6. If a private key is required to connect to the server, do the following:
   b. Select the **Private key is required for this connection** check box.
   c. In the **Private key** filed, specify a file that contains a private key.

      To locate a file, click **Browse** and select a key.

d. In the **Passphrase** field, enter the passphrase used to decrypt the private key.



Data Publishing

Publishing a PostgreSQL instance allows you to temporarily attach the instance to the target PostgreSQL server without launching restore. Publishing typically occurs faster than using standard restore features and could be convenient when, for example, your time to perform disaster-recovery operations is limited.

After you have launched a publishing operation to a PostgreSQL server, you can quickly republish the latest or point-in-time state of the PostgreSQL instance to the same server.

During publishing, Veeam Explorer for PostgreSQL takes the following actions:

1. Mounts VM disks from the backup file to the `/tmp` directory on the target PostgreSQL machine.
2. Retrieves required instance files.
3. Attaches the associated instance directly to the target PostgreSQL server so that you can perform required operations using PostgreSQL tools.

The publishing session is resilient to network disruption, backup server or mount server crash. All changes in database files that occur after publishing are saved in the publishing write cache, which is stored on the target server. If anything disrupts the publishing process (the target or mount server crashes, or the network is down), you can launch the retry manually after the server or network is up.

Before publishing an instance, read the Considerations and Limitations section.

Publishing to Specified Server

To publish a PostgreSQL instance to the specified PostgreSQL server, use the **Publish** wizard.

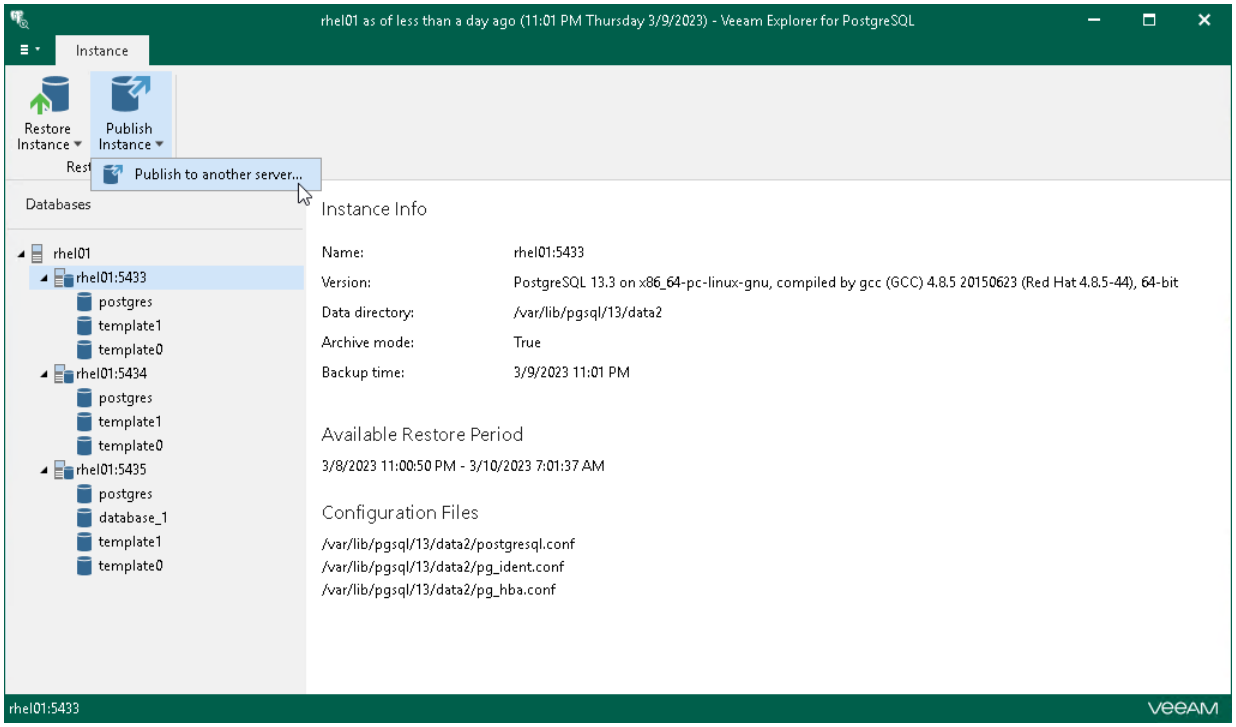
1. Launch the Publish wizard.
2. Specify a restore point.
3. Specify the target PostgreSQL server.
4. Specify PostgreSQL settings.

Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, select a PostgreSQL instance you want to publish.
2. On the **Instance** tab, select **Publish Instance** > **Publish to another server**.

Alternatively, you can right-click an instance and select **Publish Instance** > **Publish to another server**.

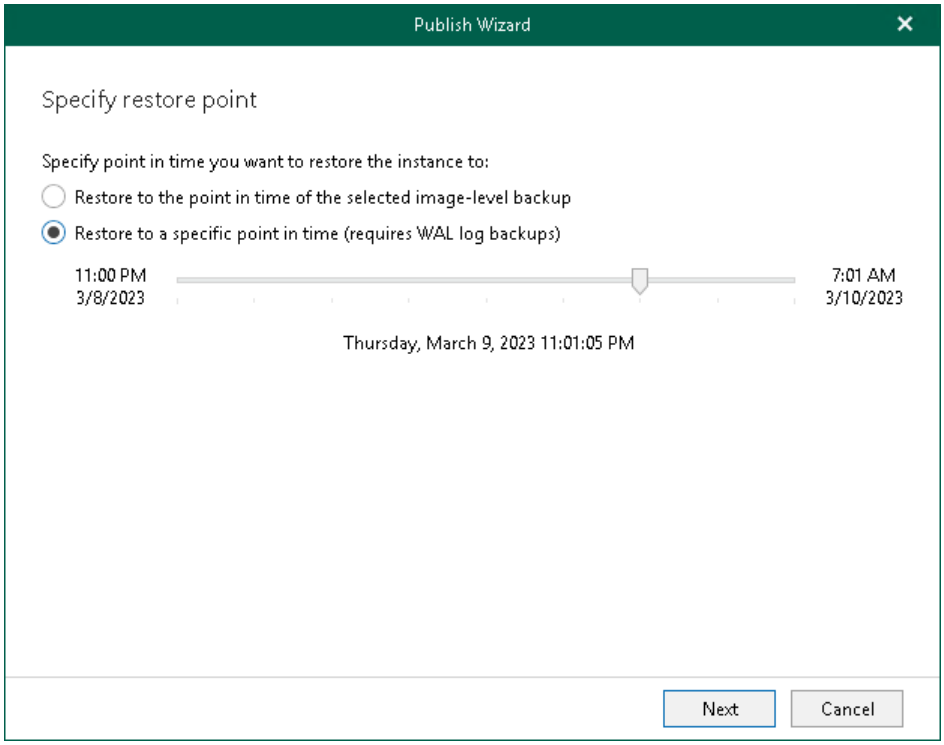


Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore the PostgreSQL instance:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.

  The **Restore to a specific point in time** option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.



Step 3. Specify Target Server

At this step of the wizard, specify credentials to access the target PostgreSQL server.

1. In the **Server** field, enter a DNS name or IP address of the target server.
2. In the **SSH port** field, specify an SSH port (by default, port 22 is used).
3. In the **Account** filed, specify a Linux system account name under which to connect to the specified server.
4. If you have specified a non-root account that does not have root privileges on the target server, click **Advanced**:
   a. Select the **Elevate specified account to root** check box.

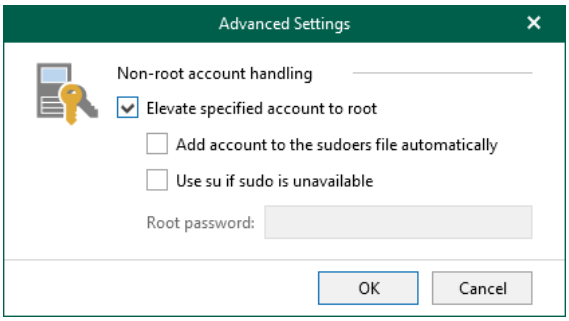
      The account must have root privileges to mount the backed-up file system to the target server and to communicate with PostgreSQL.

   b. To add the user account to the `sudoers` file, select the **Add account to the sudoers file automatically** check box. In the **Root password** field, enter the password for the root account.

      If you do not enable this option, you will have to manually add the user account to the `sudoers` file.

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

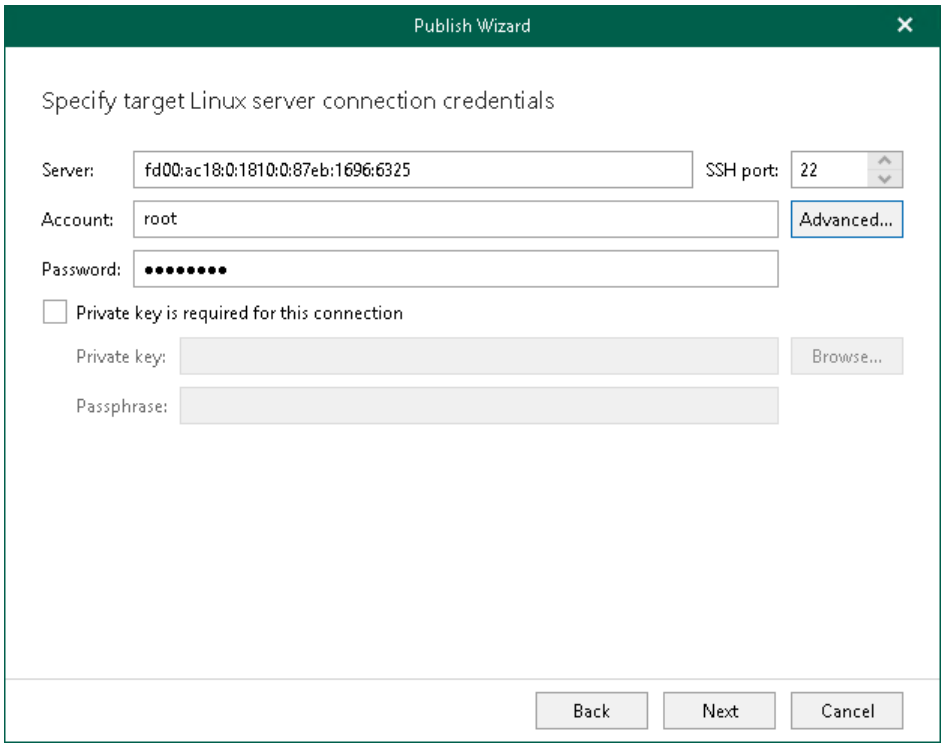
      Veeam Backup & Replication will first try to use the `sudo` command. If the attempt fails, Veeam Backup & Replication will use the `su` command.



5. In the **Password** field, enter the account password.
6. If a private key is required to connect to the server, do the following:
   b. Select the **Private key is required for this connection** check box.
   c. In the **Private key** filed, specify a file that contains a private key.

      To locate a file, click **Browse** and select a key.

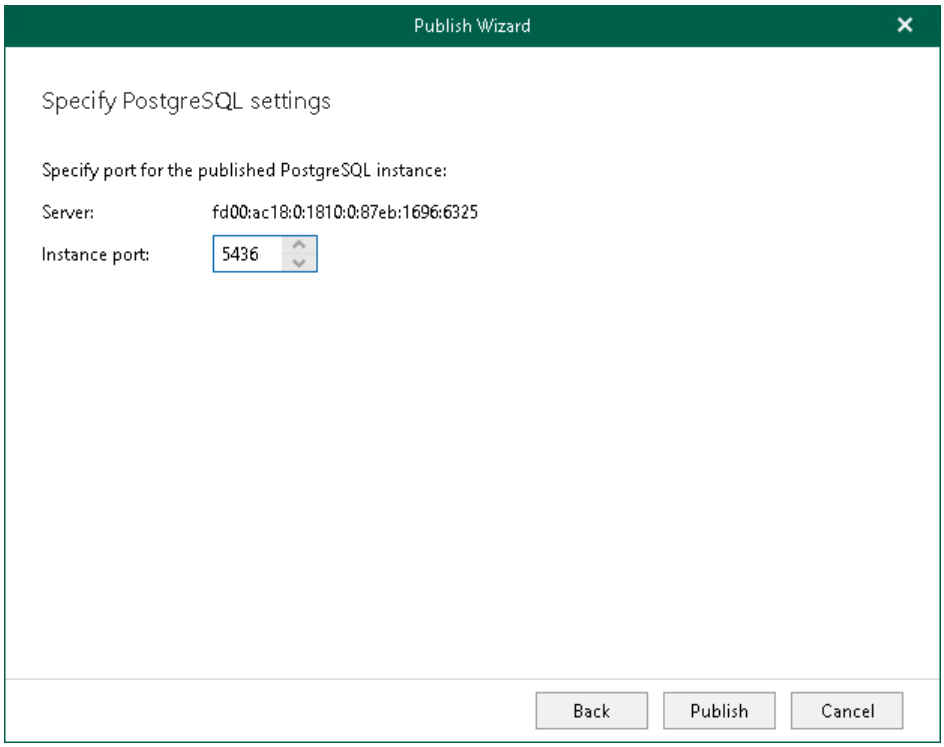
d. In the **Passphrase** field, enter the passphrase used to decrypt the private key.



Step 4. Specify PostgreSQL Settings

At this step of the wizard, specify a free PostgreSQL instance port in the **Instance port** field.

The specified port must be free. If the port is occupied, Veeam Explorer for PostgreSQL will display an error.



Publishing Latest or Point-in-Time State

After you have launched a publishing operation to a PostgreSQL instance (as described in Publishing to Specified Server), you can quickly republish a state of the PostgreSQL instance to the same server.

You can republish either of the following states:

- The latest available state — to publish data as of the latest state in the backup file.
- A point-in-time state — to publish data as of the selected point-in-time state. This option is available only if backups of PostgreSQL archive logs exist. For more information, see Required Backup Job Settings.

When you unpublish an instance, both options continue to remain until you close the application so that you can quickly republish a database if required.

Publishing Latest State

You can republish an unpublished instance anew. When republishing an instance, it will be attached to the target PostgreSQL server as of the latest available state.

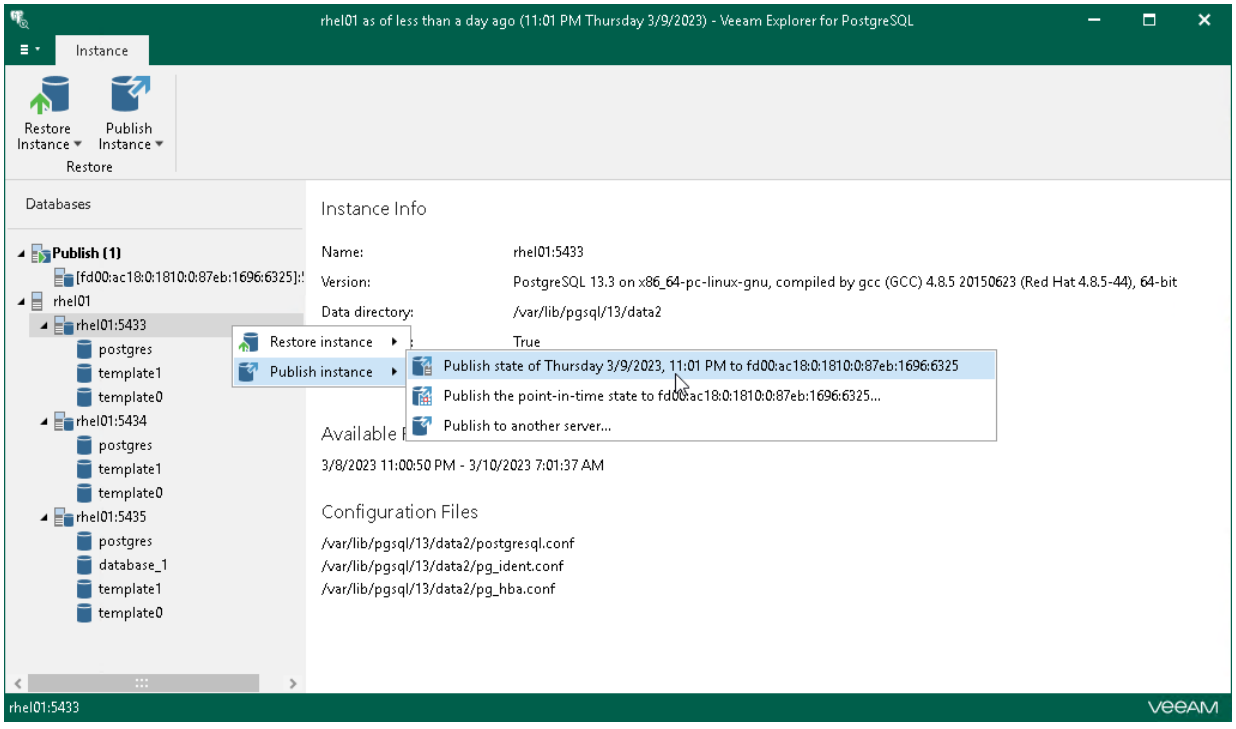
To republish an instance as of the latest state, do the following:

1. In the navigation pane, select a PostgreSQL instance you want to republish.
2. On the **Instance** tab, select **Publish Instance** > **Publish latest state to <target_server>**.

Alternatively, you can right-click an instance and select **Publish instance** > **Publish latest state to <target_server>**.

> **NOTE**
>
> The name of the publish option depends on the restore point you select during the application item restore process in the Veeam Backup & Replication console.
>
> - If you select the most recent available restore point, the option name is displayed as **Publish latest state to <target_server>**.
> - If you select any other restore point, the option name is displayed as **Publish state of <point_in_time> to <target_server>**.

Once completed, the instance will be published with the same settings as you specified during the initial publishing session.



Publishing Point-in-Time State

After you have launched a publishing operation to a PostgreSQL server (as described in Publishing to Specified Server), you can quickly publish another point-in-time state of the PostgreSQL instance to the same server.

To publish a PostgreSQL instance as of the point-in-time state, use the **Publish** wizard.

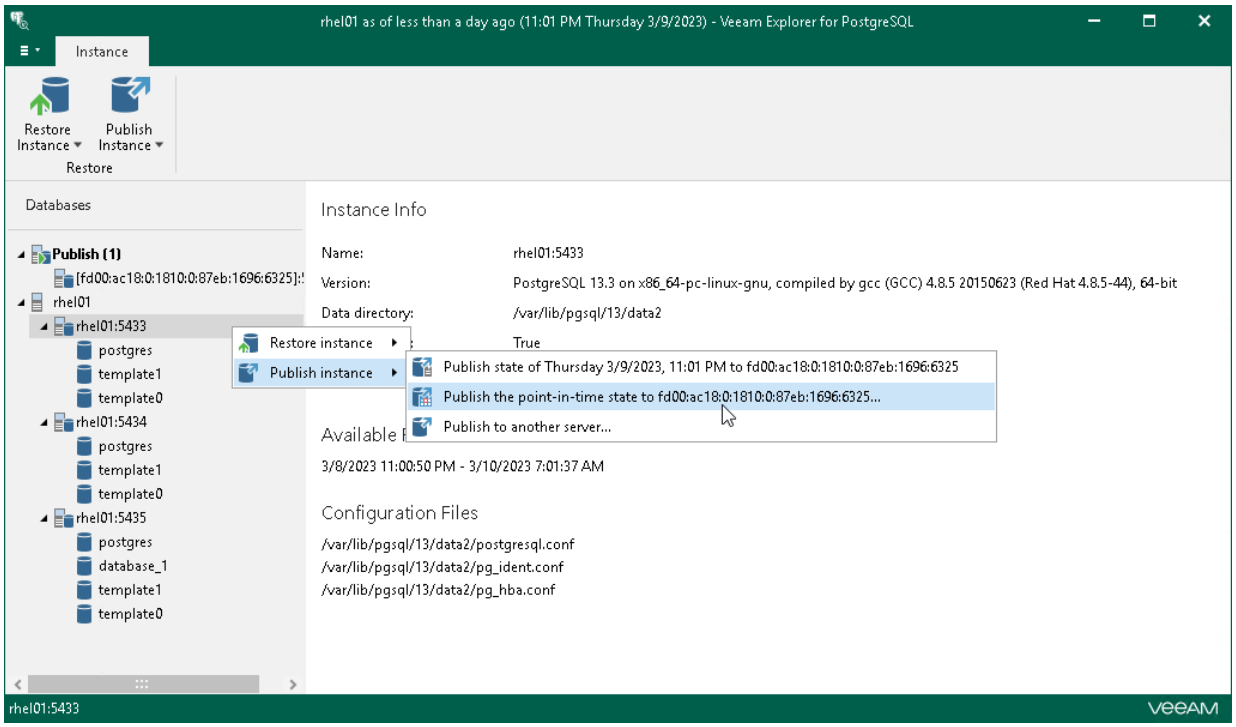
1. Launch the Publish wizard.
2. Specify a restore point.

Step 1. Launch Publish Wizard

To launch the **Publish** wizard, do the following:

1. In the navigation pane, select a PostgreSQL instance you want to republish.
2. On the **Instance** tab, select **Publish Instance** > **Publish point-in-time state to <server_name>**.

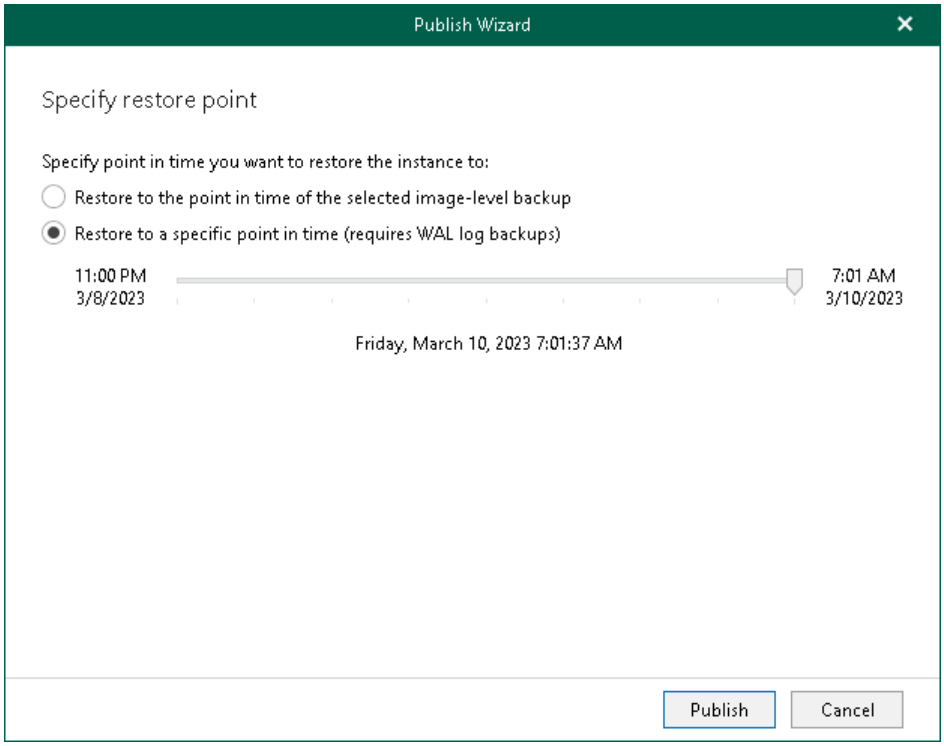
Alternatively, you can right-click an instance and select **Publish Instance** > **Publish point-in-time state to <server_name>**.



Step 2. Specify Restore Point

At this step of the wizard, select a state as of which you want to restore PostgreSQL instance:

- Select the **Restore to the point in time of the selected image-level backup** option to load instance files as per date when the current restore point was created.
- Select the **Restore to a specific point in time** option to obtain instance files as per selected time interval of the current restore point. Use the slider control to choose a time interval you need.



Unpublishing Instances

Once you have finished working with published instances, you may want to unpublish (detach) these instances from the target server.

Detachment occurs in the following manner:

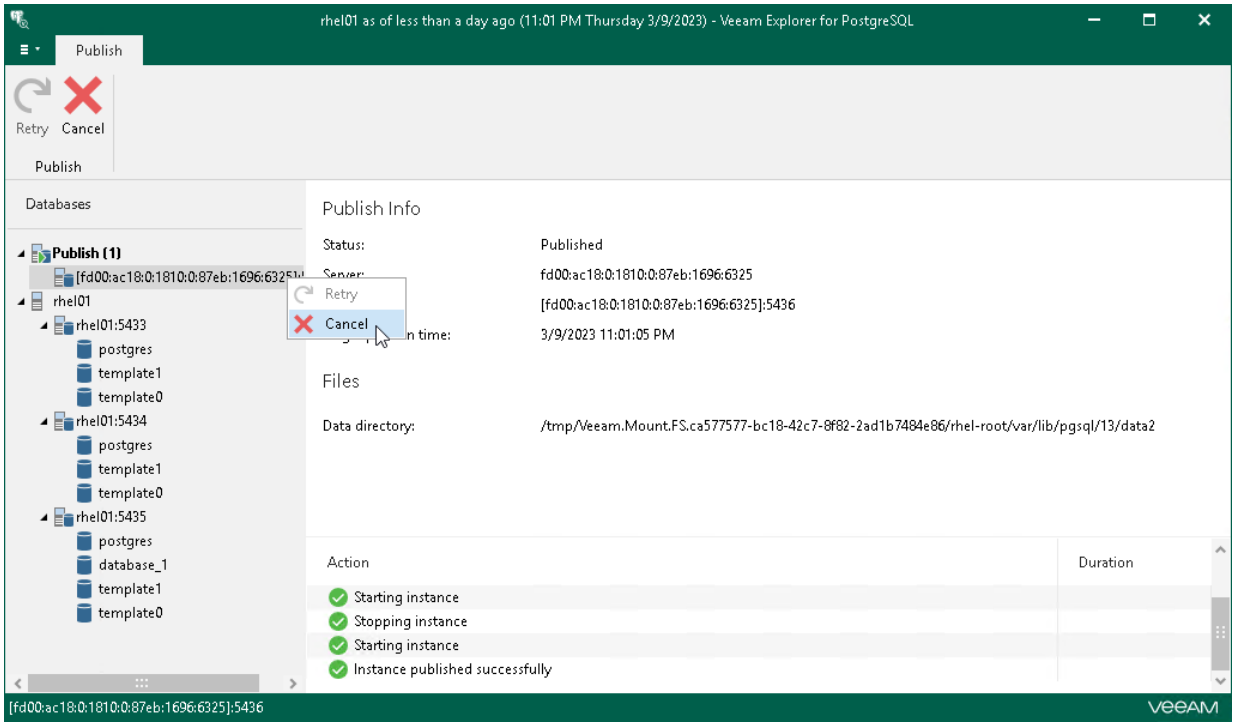
- Upon closing the Veeam Explorer for PostgreSQL console, all published instances will be detached from target servers automatically. Mount points will be also dismounted from under the `/tmp` directory.
- On manual unpublishing, instances will be detached at once but the restore point will remain mounted on the target server for the next 15 minutes.

To unpublish an instance manually, do the following:

1. In the navigation pane, under the **Published instances** node, select a published instance.
2. On the **Publish** tab, select **Cancel**.

Alternatively, in the navigation pane, right-click a published database and select **Cancel**.

To detach more than one published instance simultaneously, right-click the root **Published instances** node and select **Cancel** or select the root **Published instances** node and click **Cancel** on the **Publish** tab.



Veeam Explorer for Microsoft Exchange

Veeam Explorer for Microsoft Exchange allows you to restore and export Microsoft Exchange data from backups created by Veeam Backup for Microsoft 365 and Veeam Backup & Replication.

Planning and Preparation

You can configure your environment before you start using Veeam Explorer for Microsoft Exchange.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft Exchange.

Component	Requirement
Microsoft Exchange	For more information about supported versions of Microsoft Exchange, see: • The Supported Applications subsection of the Veeam Backup & Replication User Guide. • The System Requirements section of the Veeam Backup for Microsoft 365 User Guide.

Consider the following:

- To work with database files, Veeam Explorer for Microsoft Exchange requires a dynamic link library *ese.dll* supplied with Microsoft Exchange. The *ese.dll* file must be of the same version as that of Microsoft Exchange in which database files were created.
- To restore mailbox items from a server running Microsoft Windows ReFS, the backup server or Veeam Backup & Replication console must be installed on a machine that runs Microsoft Windows Server 2012 or later.
- To restore mailbox items from a server running Microsoft Windows ReFS 3.x, the backup server or Veeam Backup & Replication console must be installed on a machine that runs Microsoft Windows Server 2016 or later, and the ReFS version must be supported on this machine.
- To restore data that was backed up by Veeam Backup for Microsoft 365 v1.5 using PowerShell, make sure to install Windows PowerShell 2.0 or later.
- Restore of mailbox datastore from backups created by Veeam Agent for Microsoft Windows 2.0 or later requires integration with Veeam Backup & Replication to be set up. For more information, see the Using with Veeam Backup & Replication section of the Veeam Agent for Microsoft Windows User Guide.

Ports

The following tables list network ports that must be opened to manage inbound and outbound traffic.

Backup

From	To	Protocol	Port	Notes
Backup server, guest interaction proxy (Enterprise and Enterprise Plus editions)	Source Windows machine with Microsoft Exchange	TCP, UDP	135, 137 to 139, 445	Ports used to deploy the runtime coordination process on the source machine.
		TCP	6005 to 65535	The dynamic RPC range that is used by the runtime coordination process which is deployed on the source machine for application-aware processing (when working over the network). **Note**: Microsoft Exchange (in particular, Client Access) expands standard Windows dynamic RPC port range to provide better scalability. For more information, see this Microsoft article.
Source Windows machine with Microsoft Exchange	Backup server, guest interaction proxy (Enterprise and Enterprise Plus editions)	TCP	6005 to 65535	The dynamic RPC range that is used by the runtime coordination process which is deployed on the source machine for application-aware processing (when working over the network). **Note**: Microsoft Exchange (in particular, Client Access) expands standard Windows dynamic RPC port range to provide better scalability. For more information, see this Microsoft article.

NOTE

Configuring dynamic RPC range is not required when using default Microsoft Windows firewall settings as Veeam Backup & Replication automatically creates an associated firewall rule for the runtime process during installation. When using custom firewall settings or if application-aware processing fails with the *RPC function call failed* error, make sure to configure dynamic RPC ports manually. For more information, see this Microsoft article.

Restore

From	To	Protocol	Port	Notes
Backup server, Veeam Backup & Replication console	Target Microsoft Exchange 2013/2016/2019 CAS server	TCP	443	Port used for Microsoft Exchange web services connections.

Permissions

The following table lists required permissions for data restore and data compare.

Operation	Required Roles and Permissions
Restore to Microsoft 365 and on-premises Microsoft Exchange	To restore data to Microsoft 365 and on-premises Microsoft Exchange organizations, you must grant the following roles and permissions to user accounts: **Restore to Public Folder Using Basic Authentication Method** • The account must own a mailbox on a target Microsoft Exchange server. • The account must be a member of the *Organization Management* role group on a target Microsoft Exchange server. See Adding User Account to Organization Management Role Group. • [For restore of *In-Place Hold Items* to the original location] If the *In-Place Hold Items* folder already exists, make sure the account being used can create, modify and delete items. If the *In-Place Hold Items* folder does not exist, the account being used must be able to create folders under the *All Public Folders* root node. **Restore to Mailbox Using Basic Authentication Method** • If the account owns a mailbox, make sure it has *Full Access*. • If the account does not own a mailbox, then access must be granted through impersonation. See Granting Full Access. **Restore Using Modern Authentication Method** The account used to log in to Microsoft 365 must be assigned the following roles: • *ApplicationImpersonation* role. For more information, see this Microsoft article. • *Global Administrator* or *Exchange Administrator* role. Also make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.
Compare Data with Production Environment	The Veeam Backup account must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.

Examples

Adding User Account to Organization Management Role Group

To add user account to the *Organization Management* role group, use the following cmdlet:

```
Add-RoleGroupMember "Organization Management" –Member "<user_account>"
```

For more information about the *Add-RoleGroupMember* cmdlet, see this Microsoft article.

Granting Full Access

To grant *Full Access* to the account that owns a mailbox, use the following cmdlet:

```
Add-MailboxPermission –Identity "<target_mailbox>" -User "<user_account>" -Acce
ssRights FullAccess –InheritanceType All
```

For more information about the *Add-MailboxPermission* cmdlet, see this Microsoft article.

To grant *Full Access* to the account that does not own a mailbox (in particular, through impersonation), use the following cmdlet:

```
New-ManagementRoleAssignment -Name "<role_name>" -Role ApplicationImpersonation
-User "<user_account>"
```

For more information about the *New-ManagementRoleAssignment* cmdlet, see this Microsoft article.

Recalling Given Permissions

To recall given access level, run one of the following cmdlets:

```
Remove-ManagementRoleAssignment "<role_name>"
```

```
Remove-ManagementRoleAssignment -Identity "<role_name>"
```

Required Backup Job Settings

This requirement applies to backup jobs created by Veeam Backup & Replication.

When you create a backup job, make sure to enable the **application-aware image processing** option. For more information, see the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

> **NOTE**
>
> By default, Exchange transaction logs will be truncated upon successful backup. To keep transaction logs for further processing by a third-party application, select the Exchange server VM from the list, click **Edit** and on the **General** tab select **Perform copy only**.

Support for Database Availability Groups (DAG)

Veeam Backup & Replication supports any configuration of DAGs. In particular, having all the databases active on a single node or with the active databases on each node. Transaction logs will be truncated on all DAG members.

For more information and recommendations, see the following articles:

- How to virtualize and protect Exchange 2016
- Veeam Knowledge Base article

Considerations and Limitations

This section lists considerations and limitations of Veeam Explorer for Microsoft Exchange.

General

When Veeam Explorer for Microsoft Exchange is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft Exchange does not support restore using PowerShell Direct, VIX API or vSphere Automation API.
- Sending objects that exceed 3 MB in size may fail. To fix this issue, install this Microsoft update.
- Bulk restore (restore of multiple objects) is not supported for public folder mailboxes. Use the regular per-object restore instead.
- Mailboxes can be restored only to mailboxes of the same type. For example, a user mailbox to a user mailbox, an archive mailbox to an archive mailbox.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location, consider the following:
  - *In-Place Hold Items* restore is not supported for On-Premises Exchange Server 2013 due to EWS limitations.
  - To restore *In-Place Hold Items* of Exchange 2016 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with *DiscoveryHolds* system folder creation. Otherwise, restore will fail with the following error:

    "*Failed to restore In-Place Hold Items. Restore of In-Place Hold Items into Exchange 2013 is not supported*".

    For information on enabling *In-Place Hold* and *Litigation Hold*, see this Microsoft article.
- [For Veeam Explorer for Microsoft Exchange that comes with Veeam Backup & Replication] Restore of an entire mailbox or selected mailbox items to the original location is available with Veeam Universal License. When using a legacy socket-based license, the *Enterprise* or *Enterprise Plus* editions of Veeam Backup & Replication is required.

NOTE

To use an internet proxy server to restore backups created by Veeam Backup for Microsoft 365, make sure to provide appropriate proxy server address and the port number. To do this,go to the **Control Panel** > **Internet Options Connections** tab, click **LAN Settings**, select the **Use a proxy server for your LAN** check box and specify a proxy server you want to use. Credentials for such a proxy (if needed) will be taken from the **Control Panel** > **Credential Manager** > **Windows Credentials** console.

Consider that this functionality is only available in Veeam Explorer for Microsoft Exchange that comes as part of the Veeam Backup for Microsoft 365 installation package.

Export

- Export is available if you have a 64-bit version of Microsoft Outlook 2010 or later installed on a computer with Veeam Explorer for Microsoft Exchange.

  > **NOTE**
  >
  > For Outlook for Microsoft 365, only the *Semi-Annual Enterprise Channel* is supported. For more information, see this Microsoft article.

- To avoid conflicts during export, make sure to exclude PST files from the indexing scope. Oftentimes conflicts may occur due to a file you are exporting is being indexed at the same time. When exporting to shared folders, exclude Outlook files or disable Windows search on the destination computer.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Exchange and load backups, you can use any of the following methods:

- The **Explore** option to load backups created by Veeam Backup for Microsoft 365. For more information, see the Data Restore section of the Veeam Backup for Microsoft 365 User Guide.

  When loading backups located in object storage, Veeam Explorer for Microsoft Exchange will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To disable these notifications, clear the **Show pop-up notifications on startup** check box. For more information, see Advanced Settings.

- The **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start**, click **Veeam Explorer for Microsoft Exchange** and manually open Microsoft Exchange databases. For more information, see Standalone Databases and External Servers.

  When you open Veeam Explorer for Microsoft Exchange from the **Start** menu, all backed-up databases will be loaded automatically.

If you open Veeam Explorer for Microsoft Exchange from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

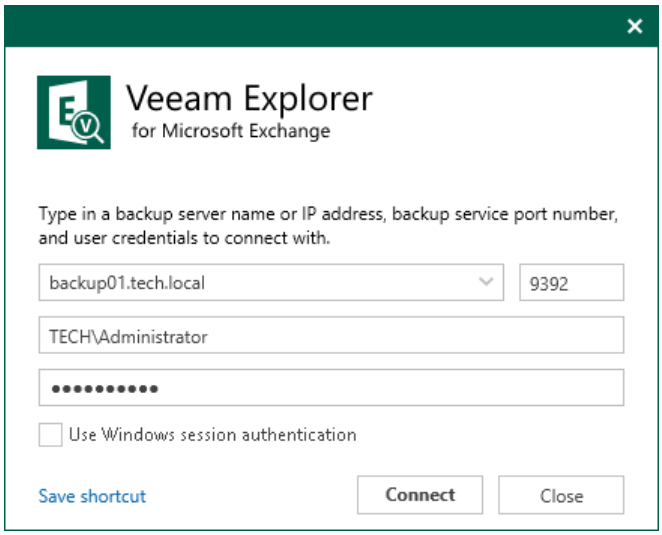
- The domain name or IP address of a server to which you want to connect.
- The port number.
- User account credentials.

  Consider the following:

  - To perform restore operations, Veeam Explorer for Microsoft Exchange must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorer for Microsoft Exchange is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft Exchange is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

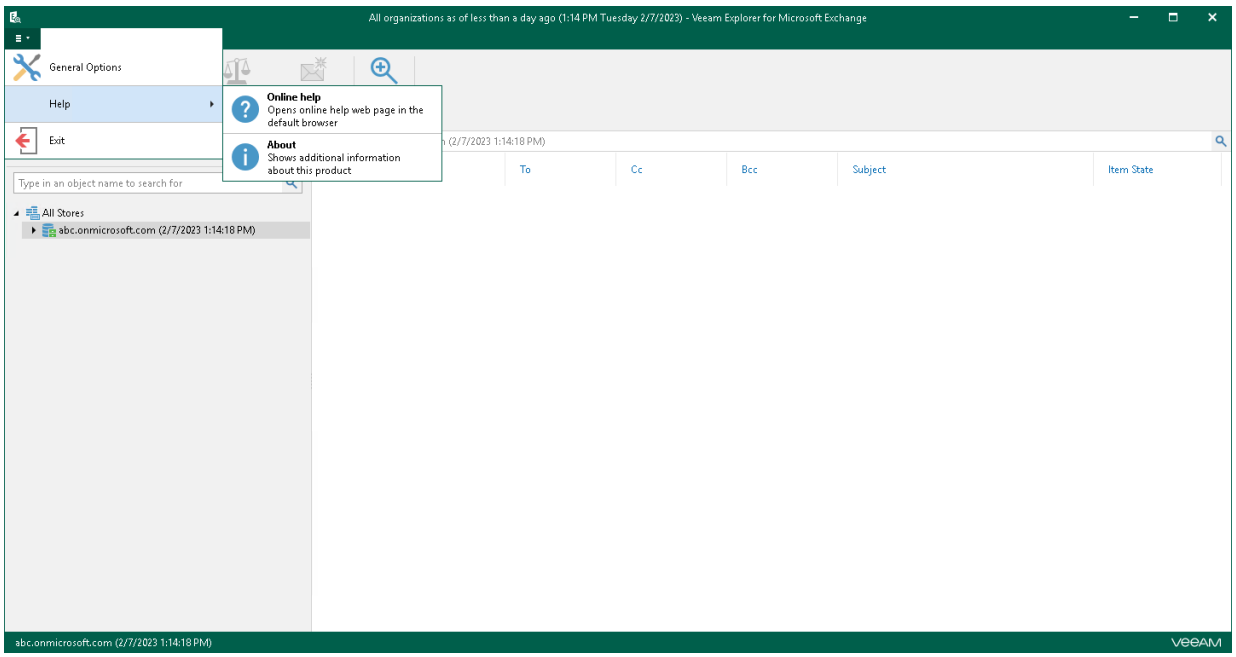
The user interface of Veeam Explorer for Microsoft Exchange is designed to let you quickly find commands that you need to restore and export Microsoft Exchange data from backups created by Veeam Backup for Microsoft 365 and Veeam Backup & Replication.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings. For more information, see General Application Settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft Exchange window.

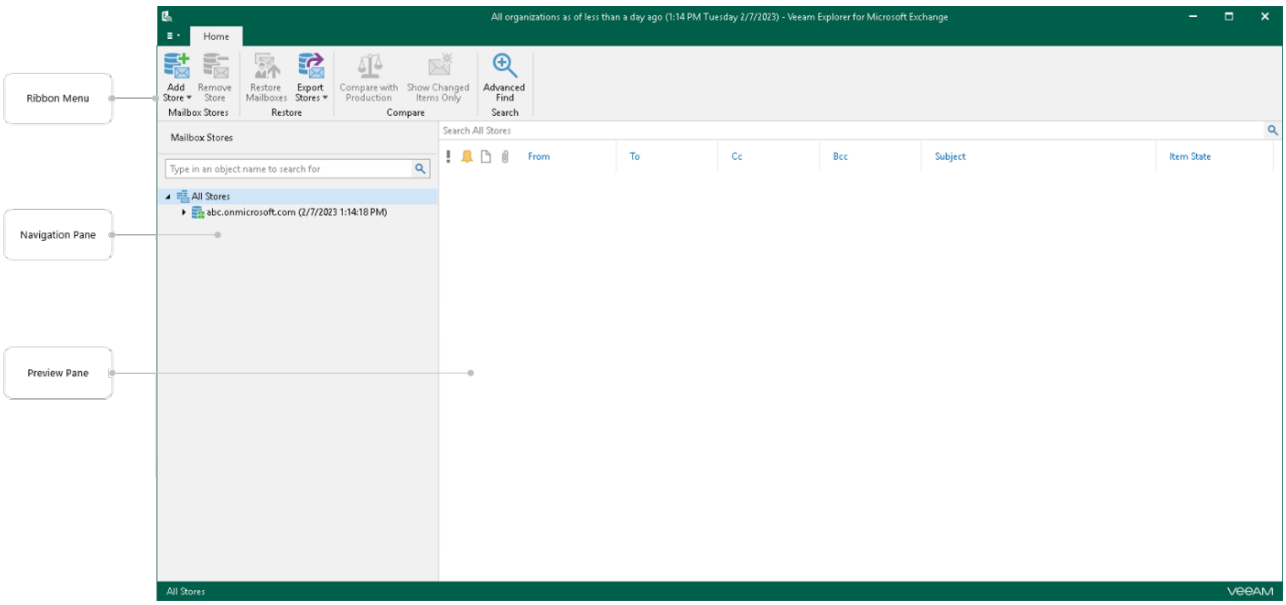
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft Exchange wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.
- The navigation pane that allows you to browse through the hierarchy of folders with backed-up data. Also, it allows you to search for mailboxes using keywords.
- The preview pane that provides search capabilities and allows you to view details about items that are contained in a folder you have selected in the navigation pane.



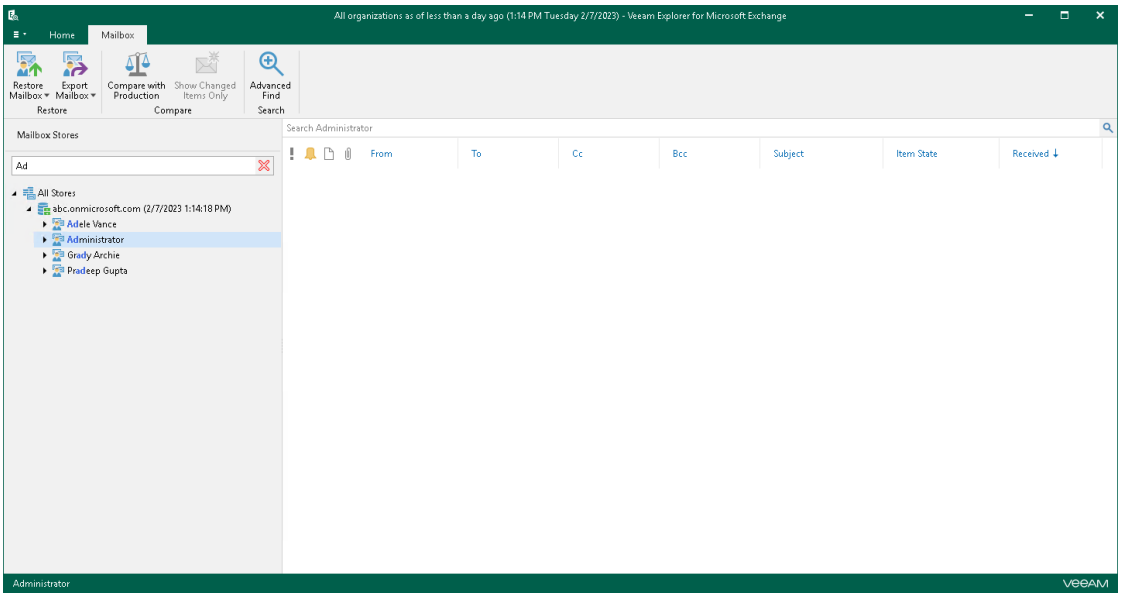
Browsing, Searching and Viewing Items

You can use Veeam Explorer for Microsoft Exchange to view the contents of a backup file, open messages, search for mailboxes and for items in a backup file as well as customize criteria of your search.

Searching for Mailboxes

You can use keywords to search for mailboxes in the database structure containing your Exchange objects. To do this, enter a search query in the search field at the top of the navigation pane.

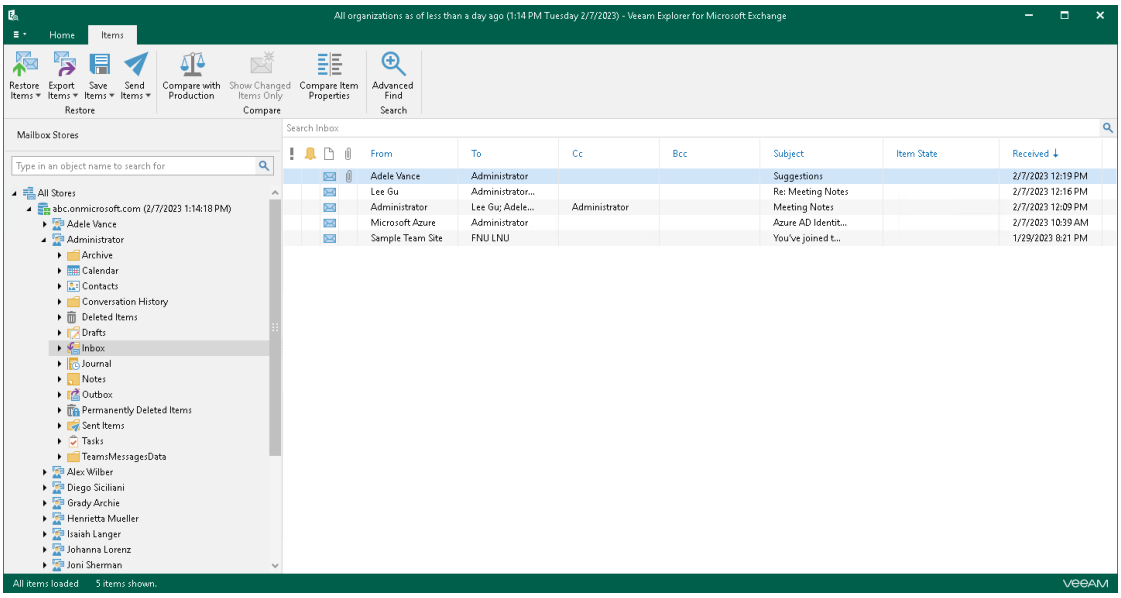
To remove a keyword, click the cross mark.



Browsing Backup Content

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your Exchange objects.

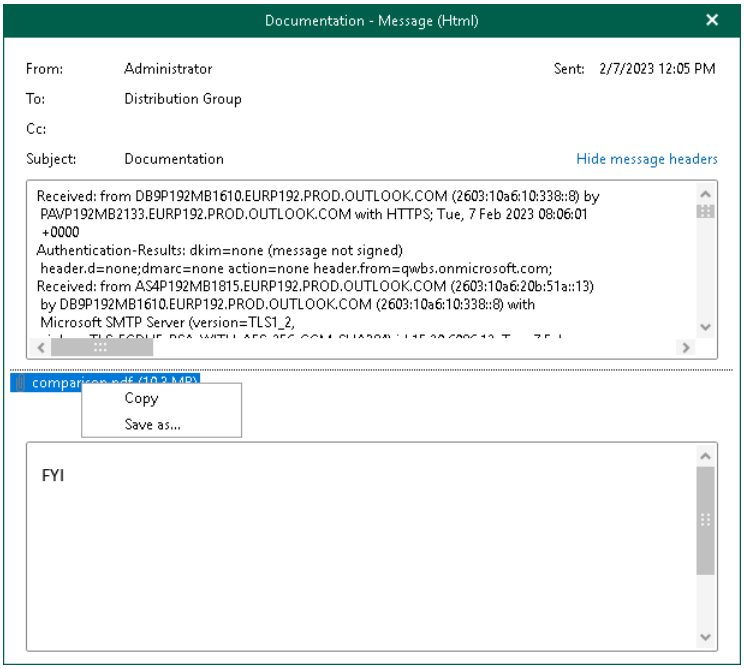
After you select an object in the navigation pane, you can see its content in the preview pane.



Opening Messages

To open a message, right-click a message in the preview pane and select **Open**. You can also double-click a message:

- To show message headers, click **Show message headers**.
- To open attachments, double-click an attachment.
- To save attachments, right-click an attachment and select **Save as**.



Searching for Objects in Backup File

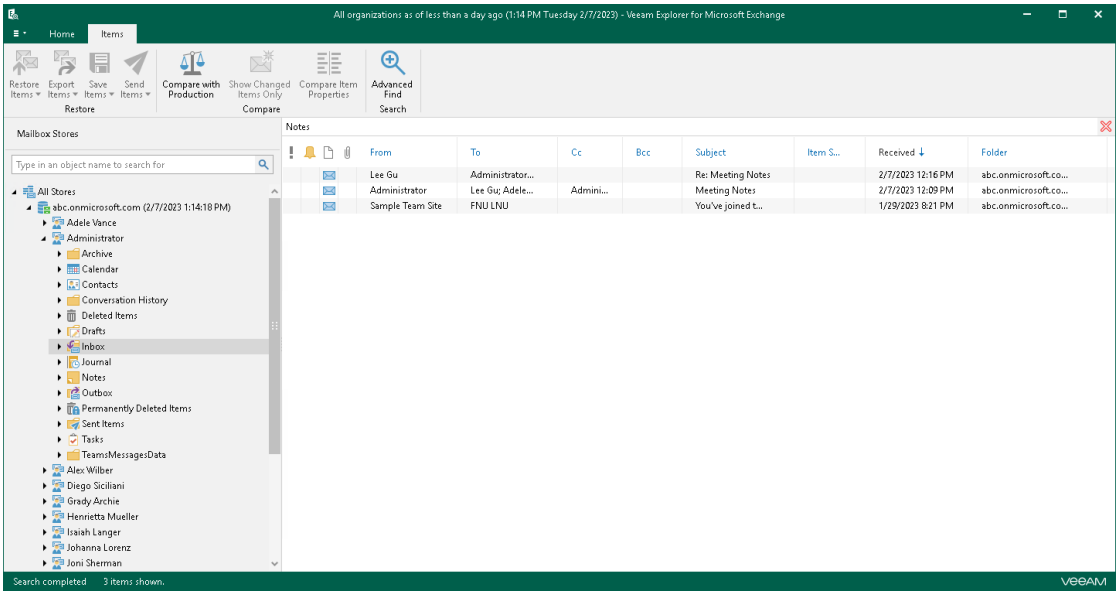
The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find data.
2. Enter a search query in the search field at the top of the preview pane.

> **NOTE**
>
> To find the exact phrase, use double quotes. For example, "*Microsoft 365*".

You can narrow search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



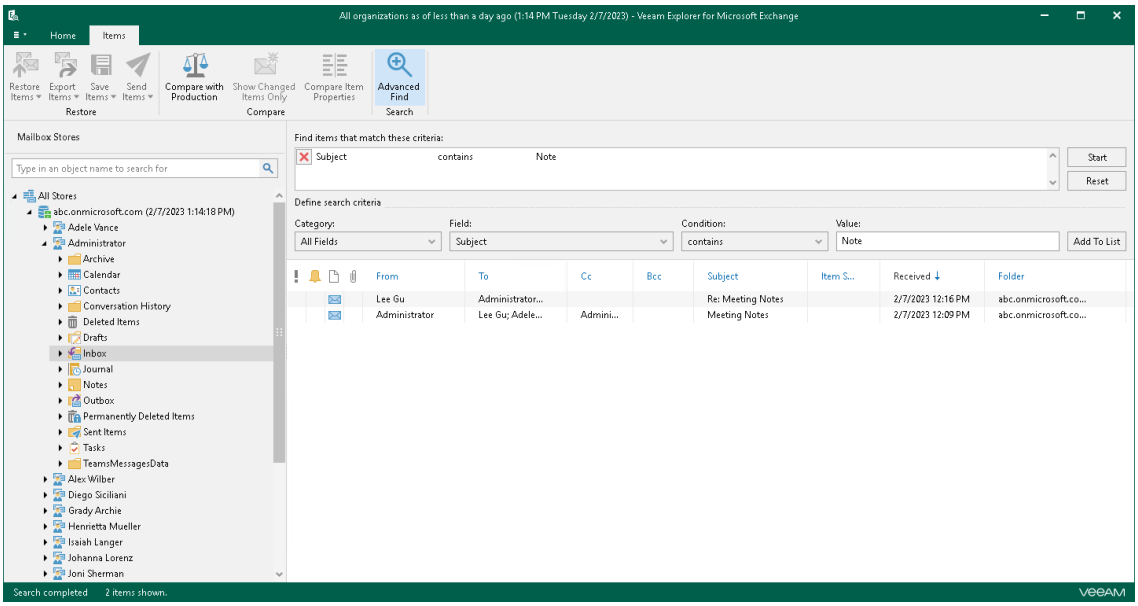
Using Advanced Find

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find messages with the subject *Report*, do the following:

1. In the preview pane, select a node and click **Advanced Find** on the ribbon.
2. In the **Define search criteria** section, select **Category** > **All fields**.
3. In the **Field** list, select **Subject**.
4. In the **Condition** list, select **contains**.
5. In the **Value** field, specify a substring to look for.
6. Click **Add to List** and then click **Start**.

To remove a filter, click the cross mark on the left. To remove all configured filters, click **Reset**.



General Application Settings

You can configure general settings for Veeam Explorer for Microsoft Exchange.

Extensible Storage Engine

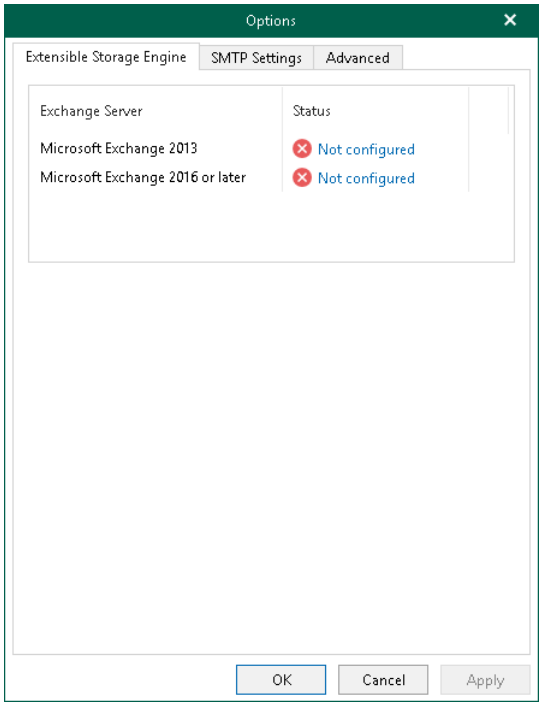
To work with database files, Veeam Explorer for Microsoft Exchange requires a dynamic link library `ese.dll` which is distributed with Microsoft Exchange.

The `ese.dll` file must be of the same version as the Microsoft Exchange application that was used to create a database. When restoring a VM that was backed up with application-aware image processing, the `ese.dll` file will be located automatically.

To specify the path to the `ese.dll` file, do the following:

1. In the main menu, click **General Options**.
2. Open the **Extensible Storage Engine** tab.
3. Click the link next to the Microsoft Exchange version and specify the path to the `ese.dll` file.

   This file can be found on the Microsoft Exchange server distribution CD in the *X:|Setup|ServerRoles|Common|ese.dll* directory or in the installation directory of the Microsoft Exchange server.
4. Click **OK**.



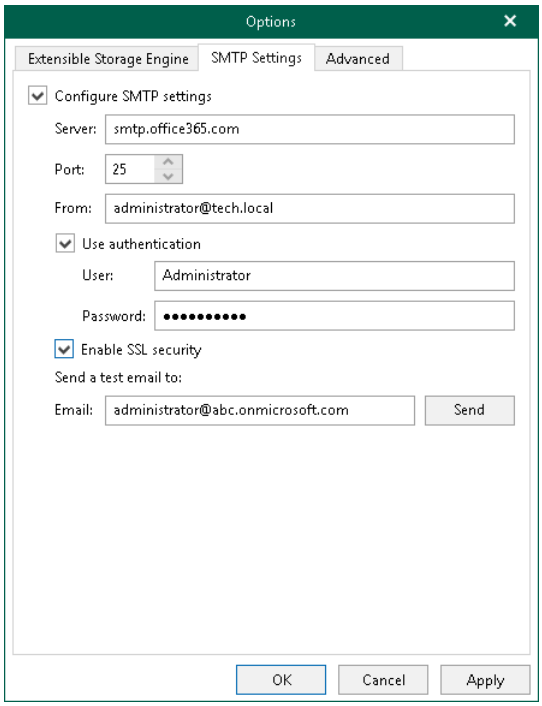
SMTP Settings

Veeam Explorer for Microsoft Exchange allows you to send Exchange items that are located in a backup through email and deliver export reports. To do this, you must configure an SMTP server which you want to use for sending emails.

To configure SMTP settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
   a. In the **Server** field, specify a DNS name or IP address of the SMTP server.
   b. In the **Port** field, specify a port number of the specified SMTP server.

      The default port number is *25*. If you want to use SSL data encryption, specify port *587*.
   c. In the **From** field, specify the sender email address.
   d. If the specified SMTP server requires an authentication for outgoing mail, select the **Use authentication** check box and provide valid credentials.
   e. Select the **Enable SSL security** check box to enable SSL data encryption.
4. Click **Send** to send a test email message.
5. Click **OK**.



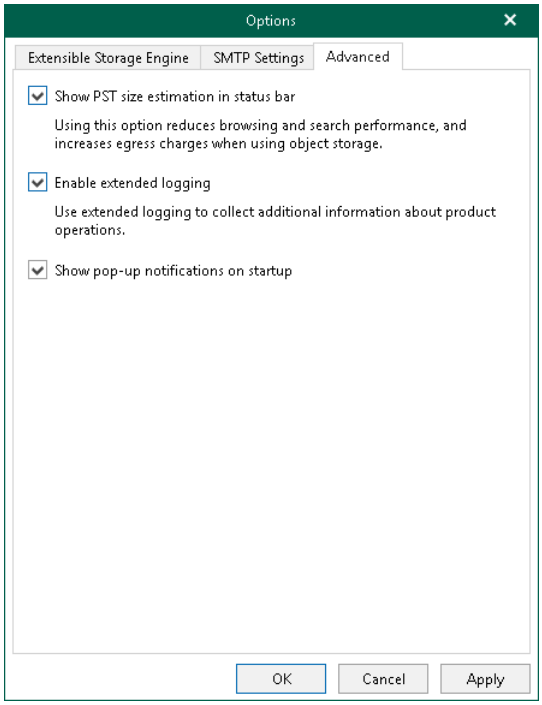
Advanced Settings

Veeam Explorer for Microsoft Exchange allows you to configure advanced settings such as extended logging mode, pop-up notifications and PST size availability.

To configure advanced settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Advanced** tab.
3. If you want to see the estimated size of the Outlook database file in the status bar, select the **Show PST size estimation in status bar** check box.
4. If you want to enable extended logging mode to collect logs that contain additional information on specific operations, select the **Enable extended logging** check box.

   After enabling extended logging mode, you can go back to the application and perform actions for which you want to collect additional information. Then you can collect logs.
5. By default, Veeam Explorer for Microsoft Exchange displays notifications when loading backups created by Veeam Backup for Microsoft 365 from object storage. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.
6. Click **OK**.



Standalone Databases and External Servers

You can add standalone databases to the Veeam Explorer for Microsoft Exchange scope as well as connect to a Veeam Backup for Microsoft 365 server or service provider server to view backups located on these servers.

Veeam Explorer for Microsoft Exchange supports adding databases created with the following Microsoft Exchange versions:

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013

Adding Microsoft Exchange Databases

You can add Microsoft Exchange databases to the application scope manually.

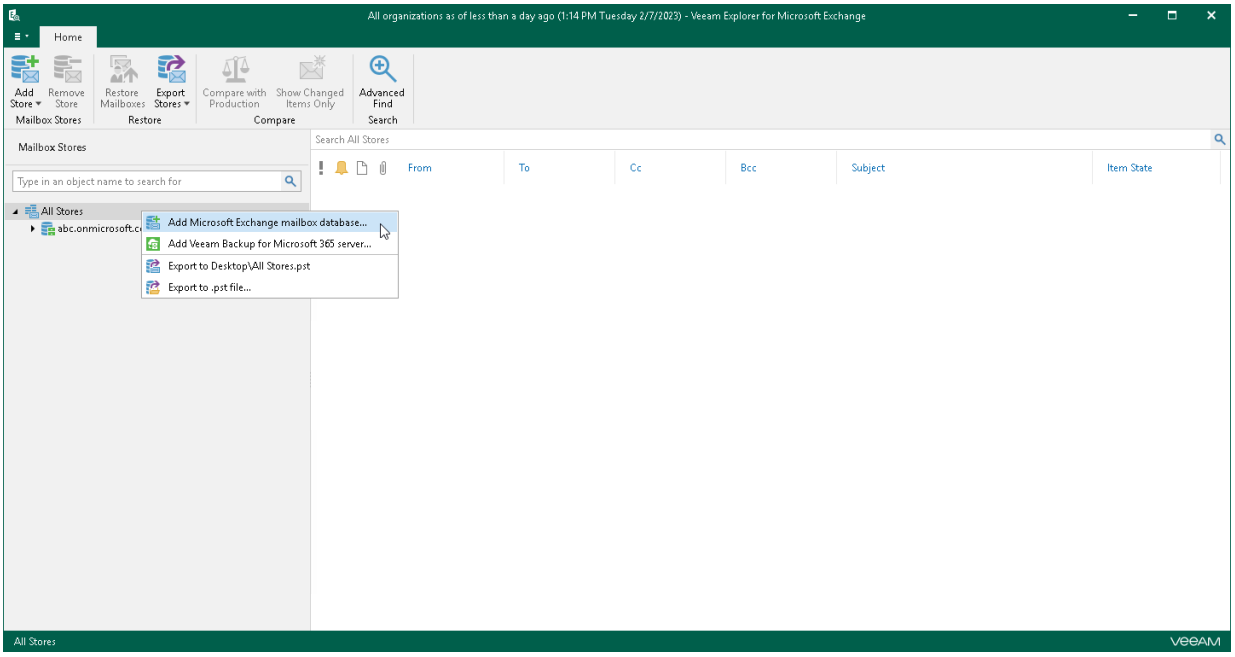
Veeam Explorer for Microsoft Exchange supports adding databases created with the following Microsoft Exchange versions:

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013

> **NOTE**
>
> Consider the following:
>
> - Before adding databases, make sure that Veeam Explorer for Microsoft Exchange has access to the `ese.dll` file. For more information, see Extensible Storage Engine.
> - If a database is in *Dirty State*, you will need to recover it by applying log files. Click **Recover** and wait until log files are applied, then re-add the database. Make sure that the **Write** permission is granted to the account being used.
> - Make sure you have disabled the *Veeam Backup Proxy for Microsoft Office 365* service when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will not be able to access the database due to database lock.

To manually add a Microsoft Exchange database, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Store** > **Microsoft Exchange mailbox database** on the ribbon.
   - Right-click the **All Stores** node and select **Add Microsoft Exchange mailbox database**.
2. Click **Browse** to specify the path to the `.edb` or `.adb` file and Exchange logs folder.



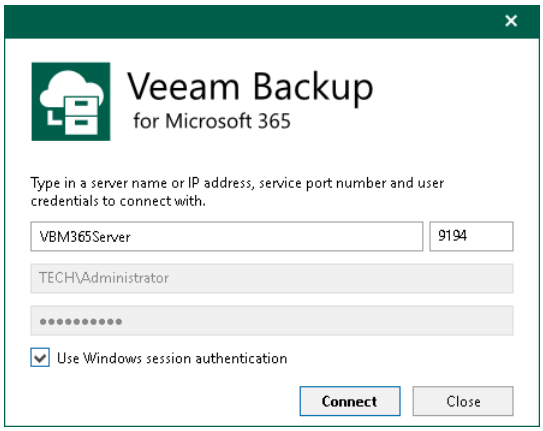
Adding Veeam Backup for Microsoft 365 Server

In Veeam Explorer for Microsoft Exchange, you can connect to a Veeam Backup for Microsoft 365 server to view backups located on this server.

To connect to a Veeam Backup for Microsoft 365 server, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Store** > **Veeam Backup for Microsoft 365 server** on the ribbon.
   - Right-click the **All Stores** node and select **Add Veeam Backup for Microsoft 365 server**.
2. Specify a server name or IP address and enter credentials to access the specified server.

   Select the **Use Windows session authentication** check box to connect with the user account under which you are currently logged in.
3. Click **Connect**.



Adding Veeam Backup for Microsoft 365 Service Provider

In Veeam Explorer for Microsoft Exchange, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.

> **NOTE**
>
> Make sure that both Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication. For more information, see the Connecting to Service Providers section of the Veeam Cloud Connect Guide.

To add Veeam Backup for Microsoft 365 service providers, do the following:

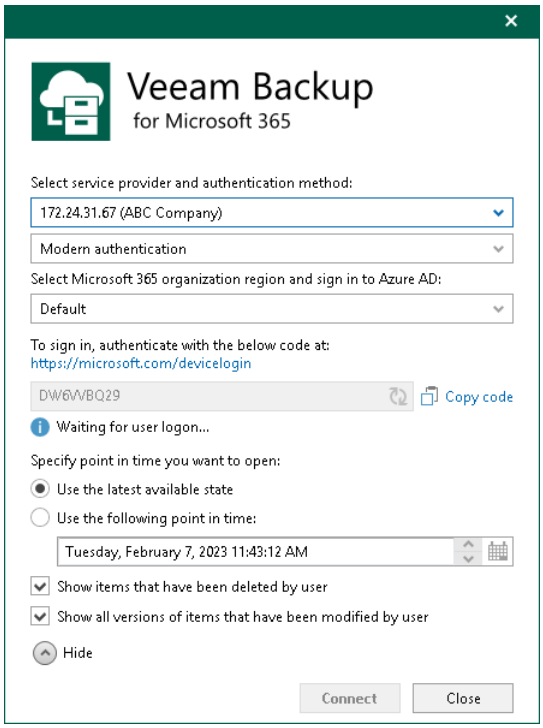
1. Do one of the following:
   - On the **Home** tab, click **Add Store** > **Veeam Backup for Microsoft 365 service provider** on the ribbon.
   - Right-click the **All Stores** node and select **Add Veeam Backup for Microsoft 365 service provider**.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and select an authentication method that can be either *Modern authentication* or *Basic authentication*.
3. [For *Modern authentication*] Select a region to which a Microsoft 365 organization of the selected service provider belongs.
4. [For *Modern authentication*] Copy the device code and use it to sign in to Azure Active Directory.

   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.

   > **NOTE**
   >
   > You cannot use *Basic authentication* to load backups if a Microsoft 365 organization has been added to the service provider infrastructure using *Modern authentication*.
5. Select a point-in-time state as of which you want to load Microsoft 365 backups.

   To select a point in time, use the calendar control.
6. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
7. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.

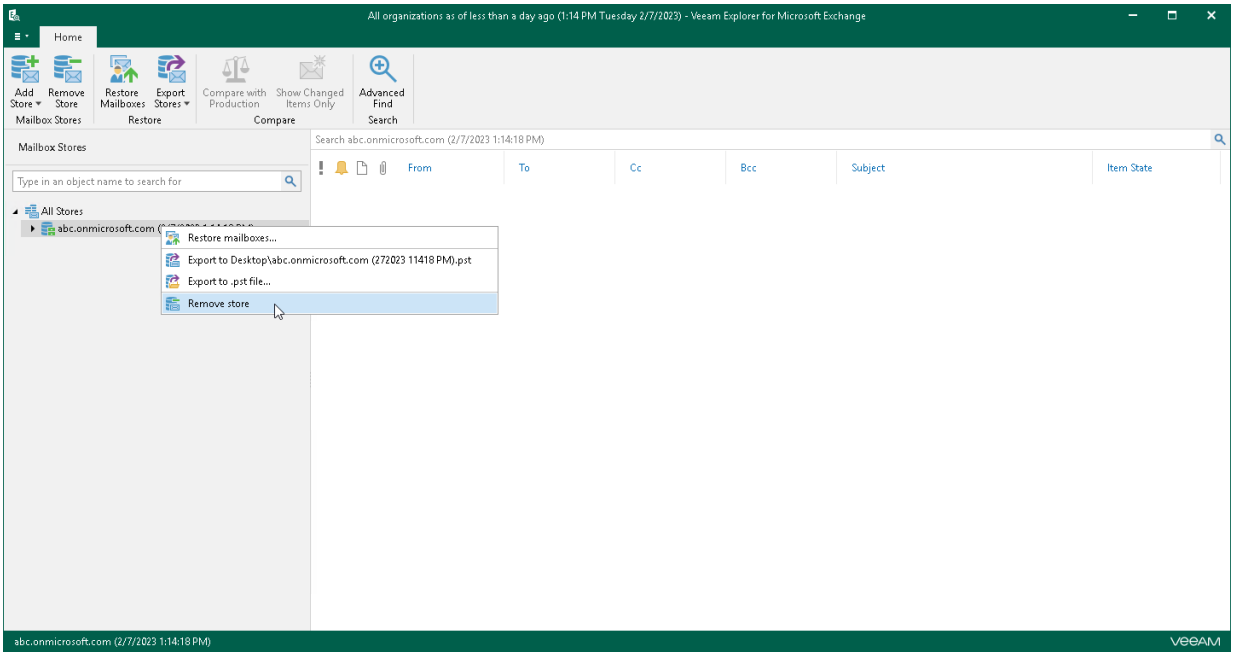
8. Click **Connect**.



Removing Stores

Veeam Explorer for Microsoft Exchange allows you to remove an Exchange store from the application scope when you no longer need it.

To remove a store from the application scope, right-click a store in the navigation pane and select **Remove store**.



Data Restore

You can use Veeam Explorer for Microsoft Exchange to restore data to Microsoft 365 organizations and on-premises Microsoft organizations.

Veeam Explorer for Microsoft Exchange allows you to perform granular restore of Microsoft Exchange data. You can restore data of mailboxes and mailbox folders as well as specific emails, calendar items, contacts, tasks, notes, journal items, and so on.

Before restoring data, read the Considerations and Limitations section.

Restore to Microsoft 365 Organizations

You can restore data to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and security defaults.

When you perform a restore, you can specify a target mailbox, select an authentication method that you want to use for data restore, specify a target folder to which you want to restore data and configure restore options.

You can also use 1-Click Restore if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folder or Item

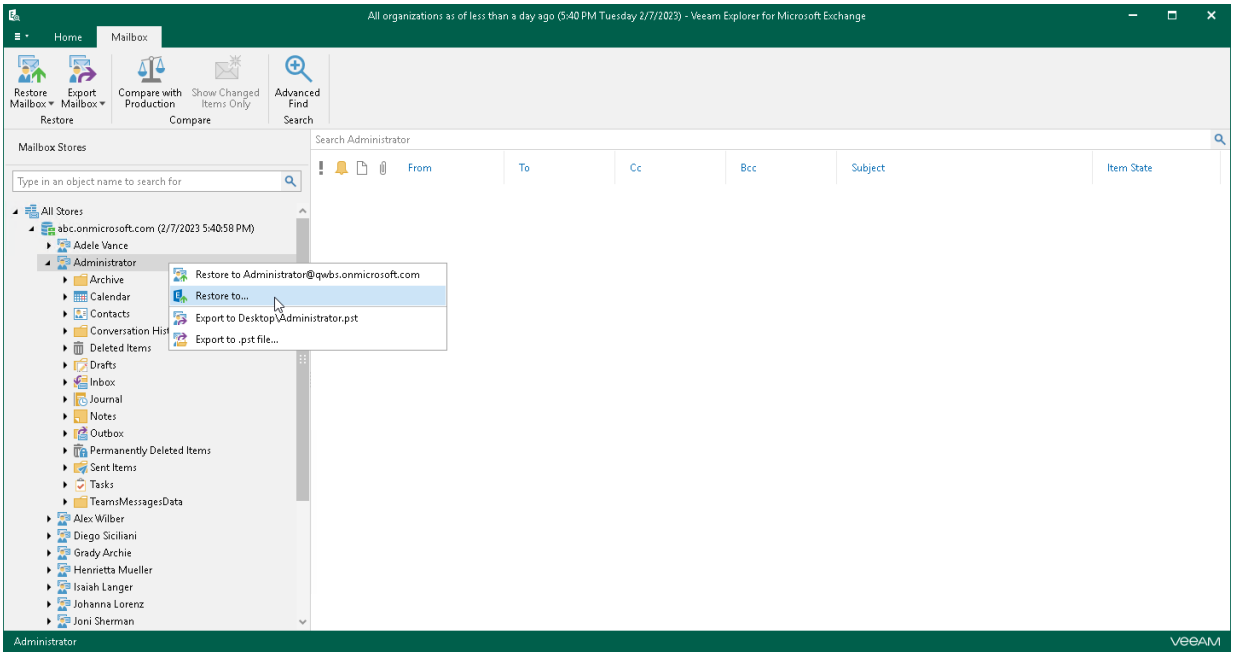
To restore a single mailbox, folder or item, do the following:

1. Launch the Restore wizard.
2. Specify a target mailbox.
3. Select an authentication method.
4. Log in to Microsoft 365.
5. Specify a CAS server.
6. Specify a target folder.
7. Specify restore options.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. Do one of the following:
   - On the **Mailbox/Folder/Items** tab, click **Restore Mailbox/Restore Folder/Restore Item** > **Restore to** on the ribbon.
   - Right-click a mailbox, folder or an item and select **Restore to**.



Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

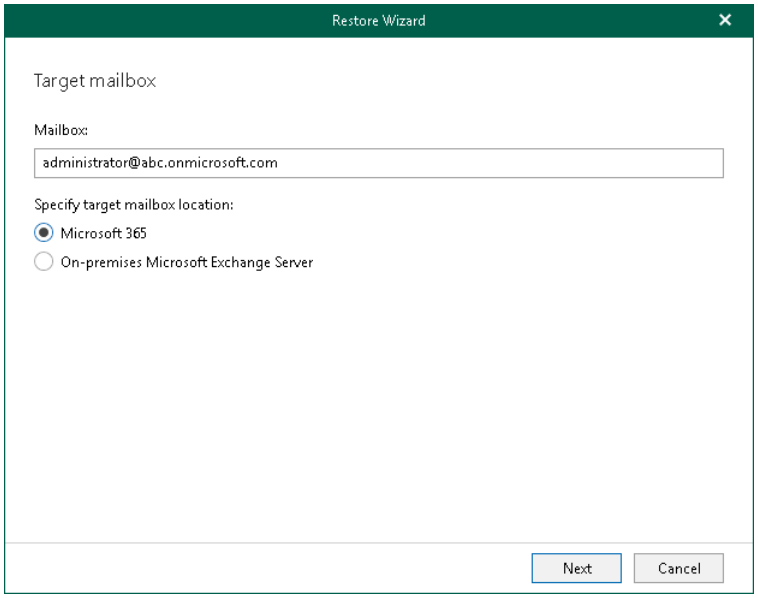
To specify mailbox settings, do the following:

1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.

   You can specify any name that you want. You can also restore a mailbox to a different organization. For example, you have backed up a mailbox *administrator@abc.onmicrosoft.com*. To restore such a mailbox to a different organization, you can specify, for example, *administrator@xyz.onmicrosoft.com* to restore a mailbox to the *xyz.onmicrosoft.com* organization.

2. Select **Microsoft 365** to restore the specified mailbox to an Exchange Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

   You can also perform a restore of backups created for Exchange Online organizations to on-premises Microsoft Exchange servers and vice versa. For more information, see Restore to On-Premises Microsoft Servers.



Step 3. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified mailbox back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

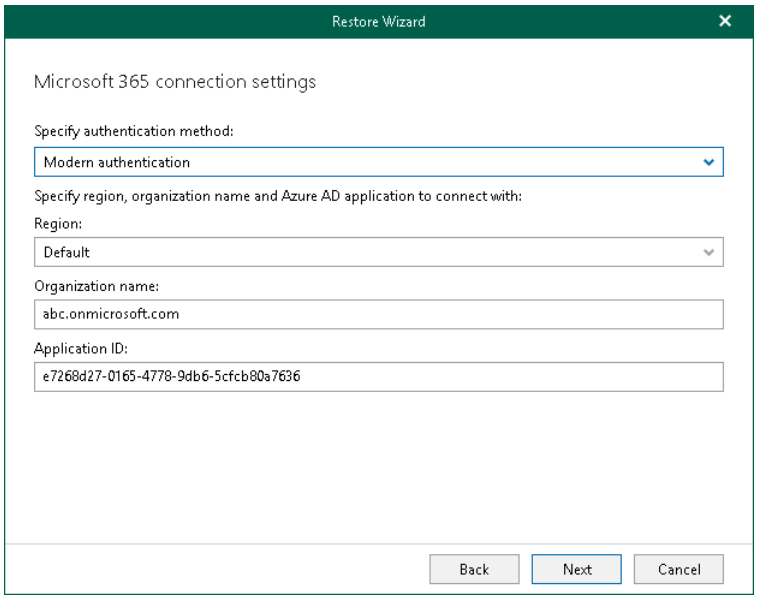
2. From the **Region** drop-down list, select a region to which your Exchange Online organization belongs.

3. In the **Organization name** field, enter a name of your Exchange Online organization.

   Make sure that the organization name matches the name specified at the previous step of the wizard.

4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.

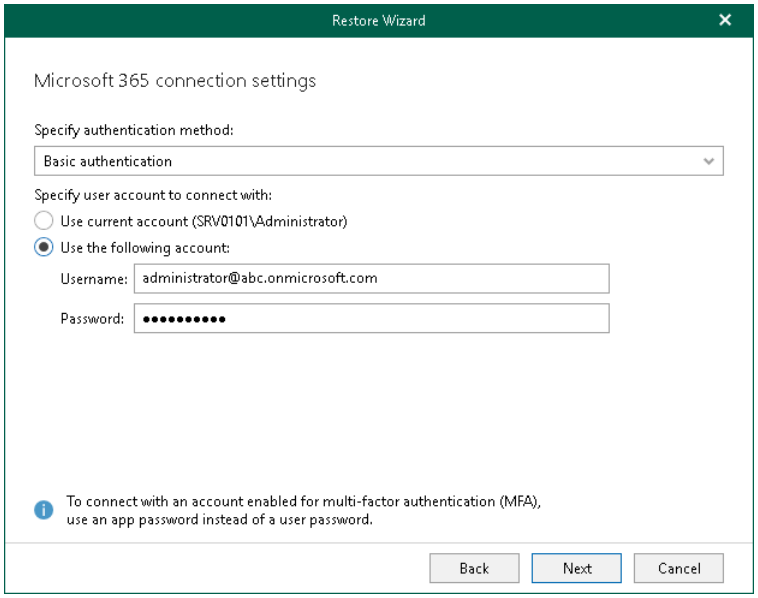


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the Exchange organization.

   Make sure that the account that you use has both the *Exchange Administrator* and the *Global Administrator* roles.



Step 4. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

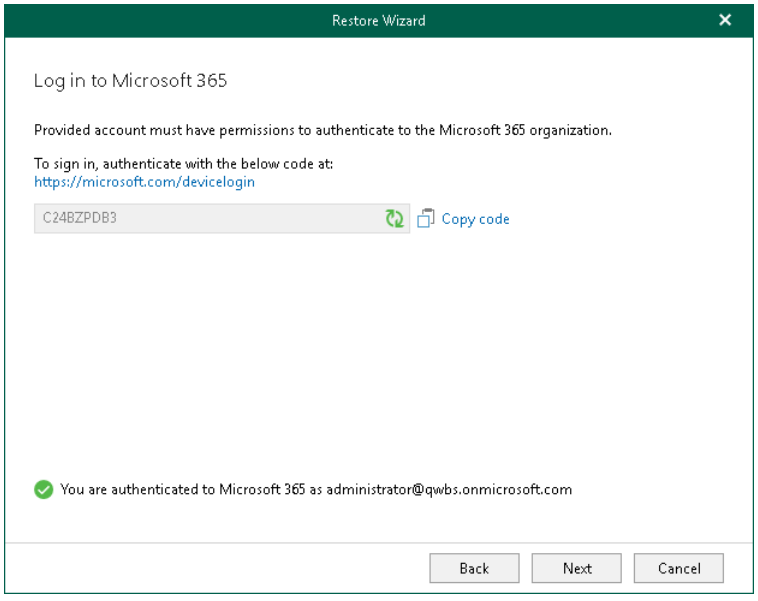
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



Step 5. Specify CAS Server and Target Folder

This step is only available if you have selected the *Basic Authentication* option at the Select Authentication Method step.

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

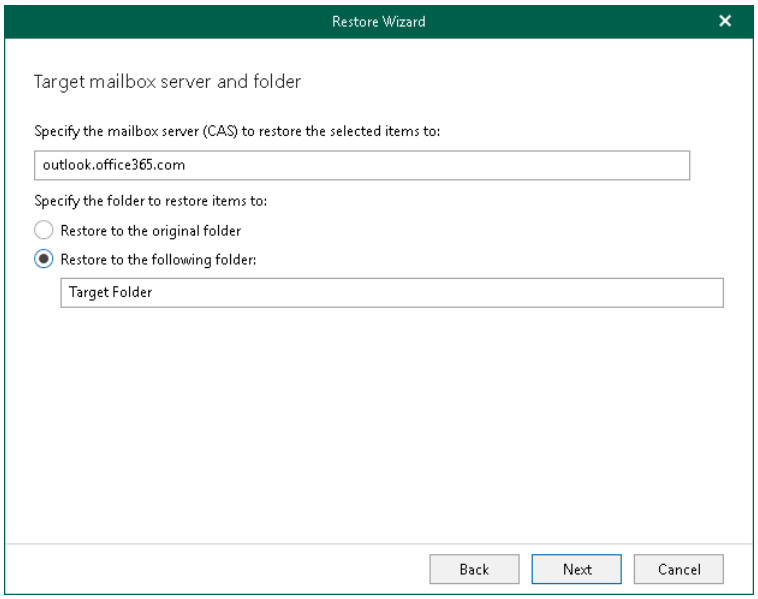
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or IP address.

   This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.

2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

   When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Explorer for Microsoft Exchange will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.

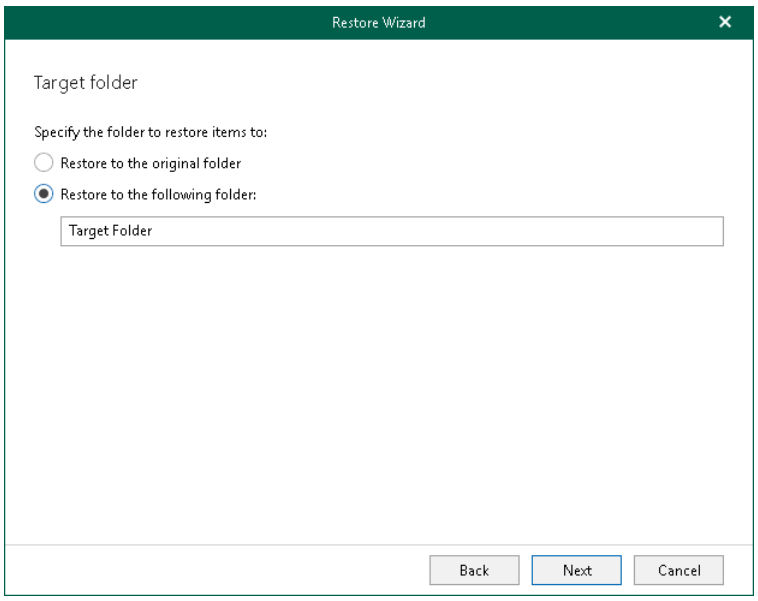


Step 6. Specify Target Folder

This step is only available if you have selected the *Modern Authentication* option at the Select Authentication Method step.

At this step of the wizard, select a target folder to which you want to restore the specified mailbox. You can perform a restore to the original folder or specify a custom folder.

When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.



Step 7. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

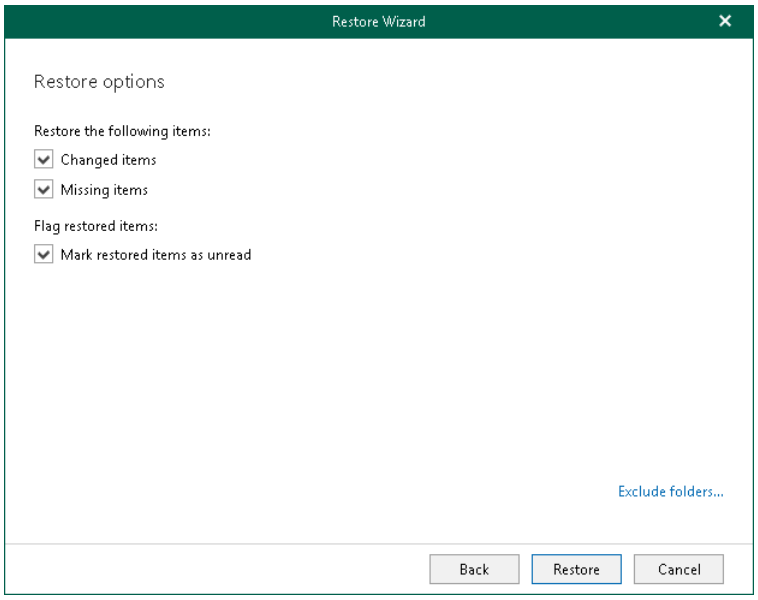
  Select this check box if you want to restore items that are missing in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

If you restore a mailbox, to prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.

> **NOTE**
>
> The **Exclude folders** link is not available when restoring folders and items.



Restoring Multiple Mailboxes

This scenario is only available for data restore from backups created by Veeam Backup for Microsoft 365.

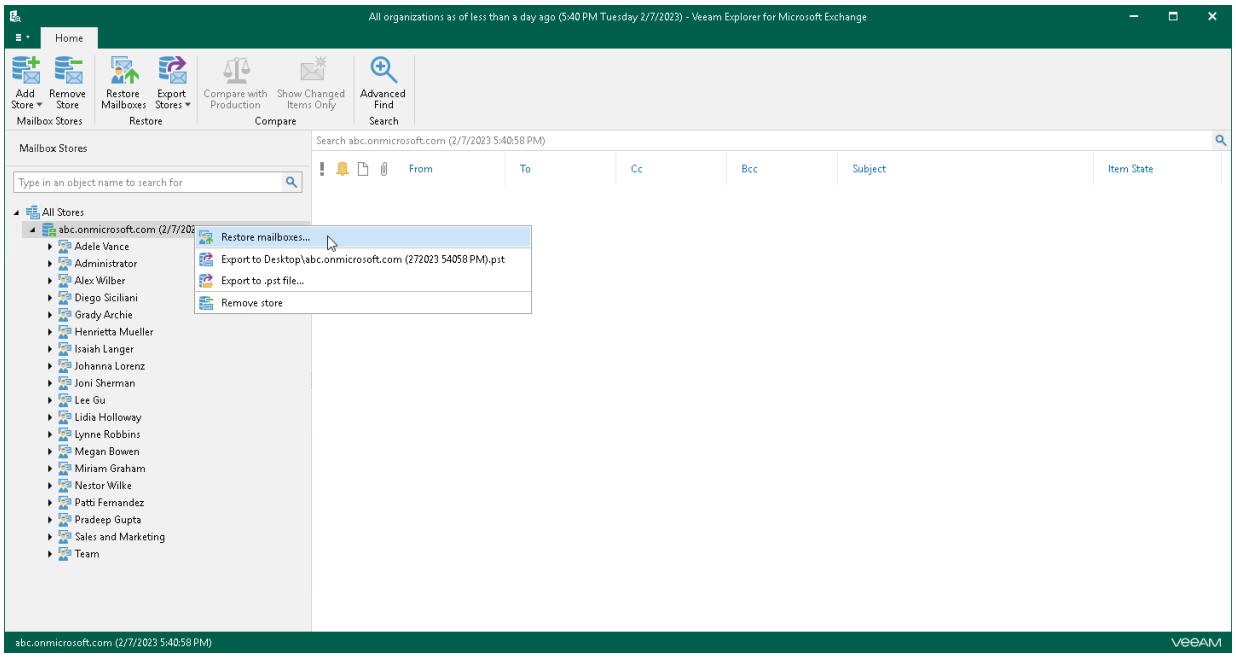
To restore multiple Exchange mailboxes, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Select mailboxes to restore.
5. Select restore options.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select an organization whose mailboxes you want to restore.
2. Do one of the following:
   - On the **Home** tab, click **Restore Mailboxes** on the ribbon.
   - Right-click a mailbox store and select **Restore mailboxes**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

To use modern authentication, do the following:

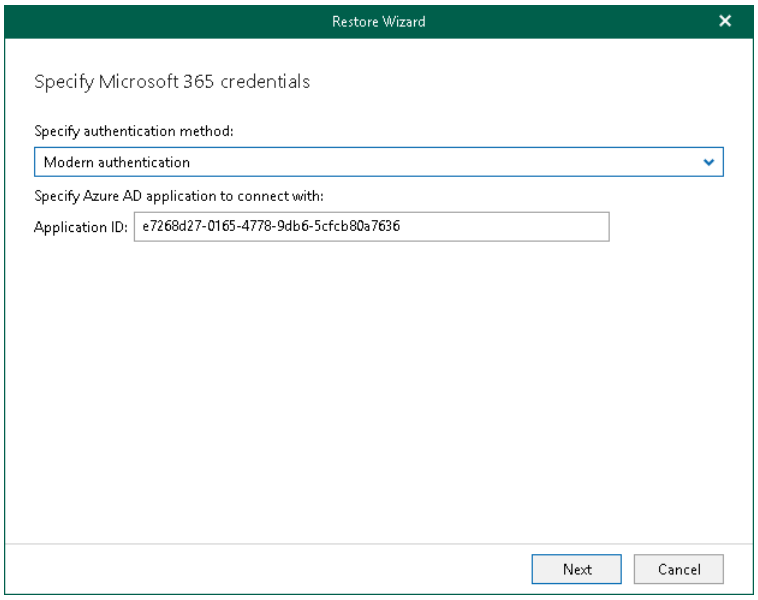
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified mailbox back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

   For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.

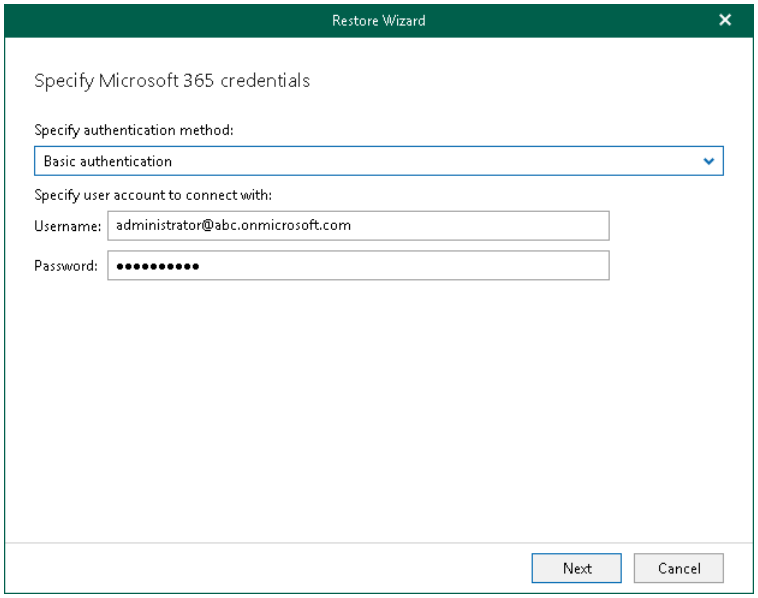


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Exchange organization.

   Make sure that the account that you use has both the *Exchange Administrator* and the *Global Administrator* roles.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

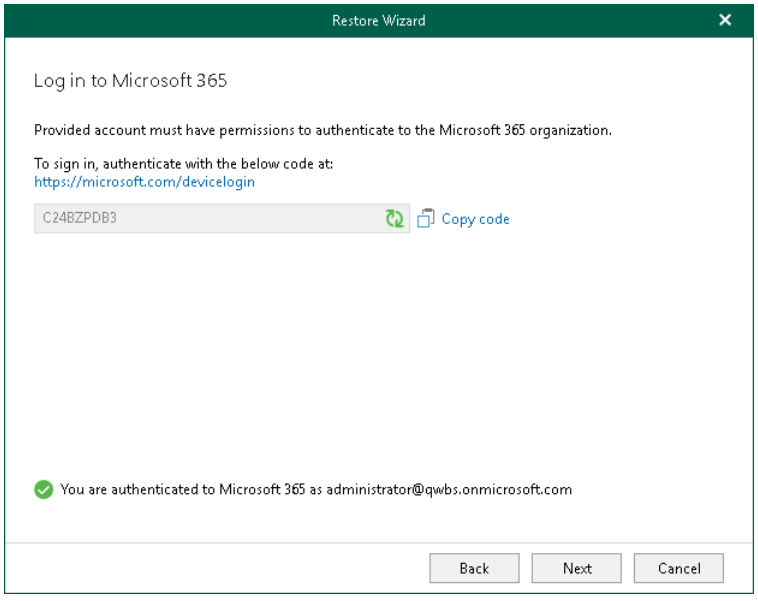
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

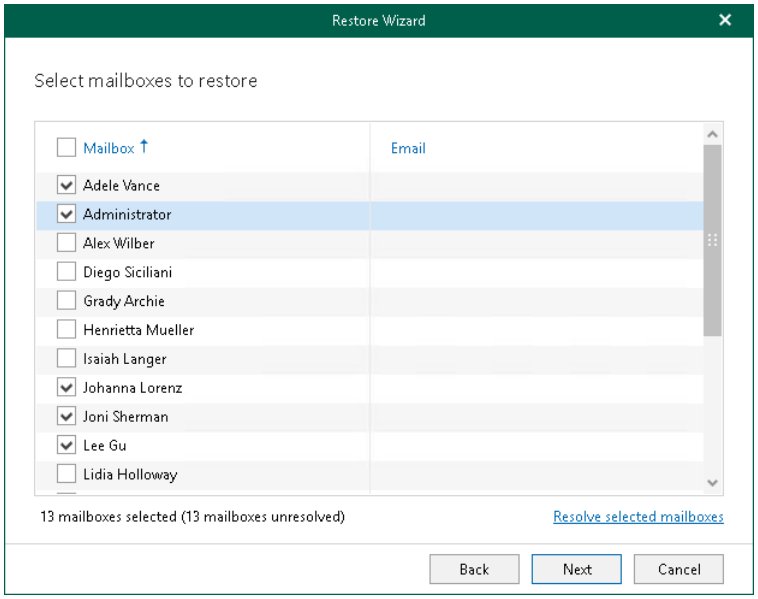
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Select Mailboxes to Restore

At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **Email** column, click **Resolve selected mailboxes**.



Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

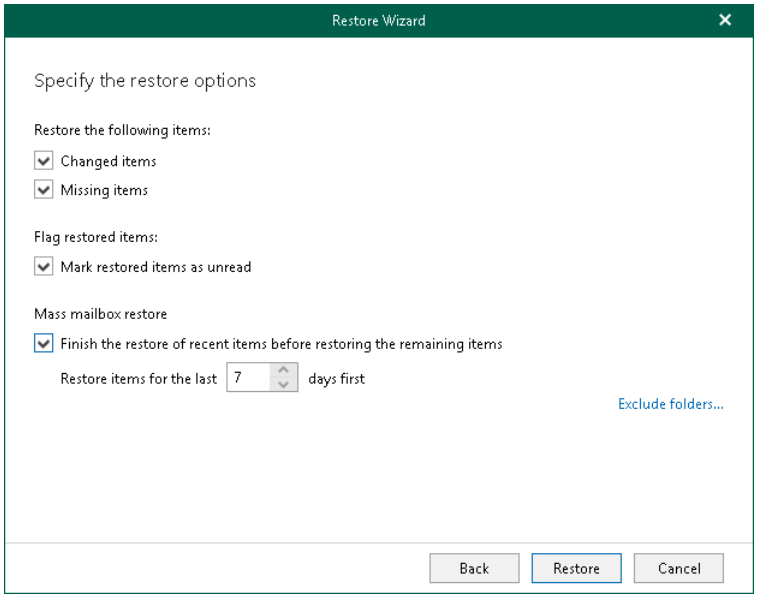
  Select this check box if you want to restore items that are missing in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.



Restore to On-Premises Microsoft Servers

You can restore data to on-premises Microsoft Exchange servers.

When you perform a restore, you can specify a target mailbox, select an authentication method that you want to use for data restore, specify a target folder to which you want to restore data and configure restore options.

You can also use 1-Click Restore if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folder or Item

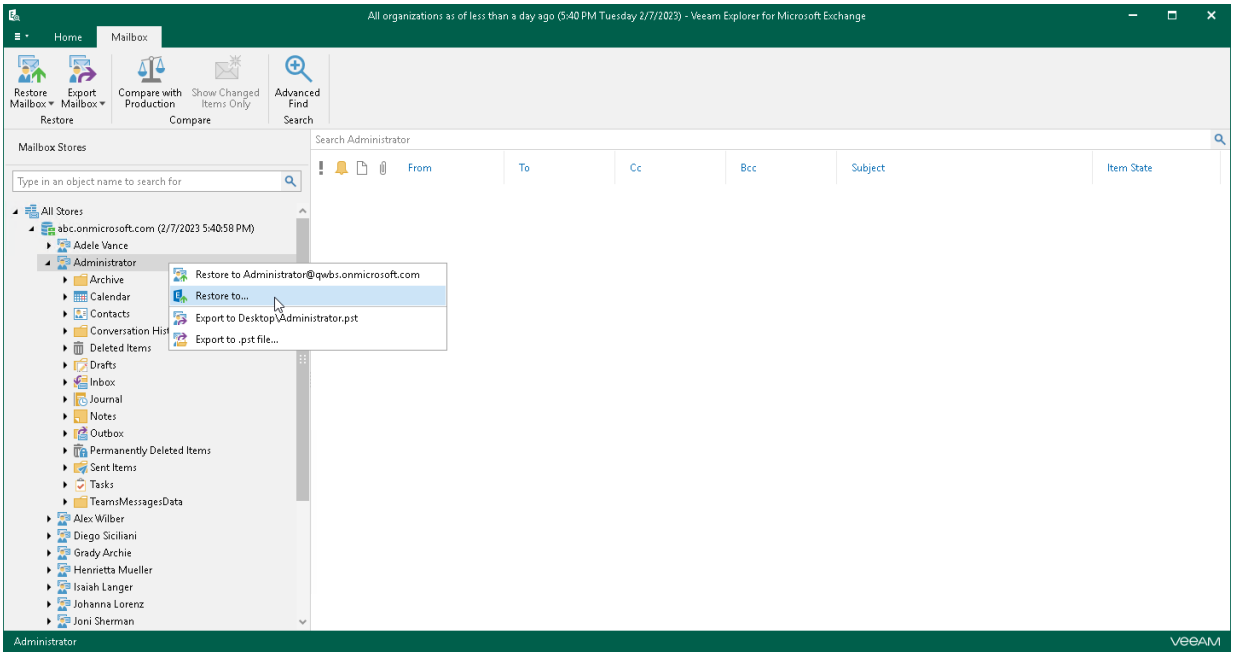
To restore a single mailbox, folder or item, do the following:

1. Launch the Restore wizard.
2. Specify a target mailbox.
3. Specify a user account.
4. Specify a CAS server and target folder.
5. Specify restore options.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. Do one of the following:
   - On the **Mailbox/Folder/Items** tab, click **Restore Mailbox/Restore Folder/Restore Item** > **Restore to** on the ribbon.
   - Right-click a mailbox, folder or an item and select **Restore to**.



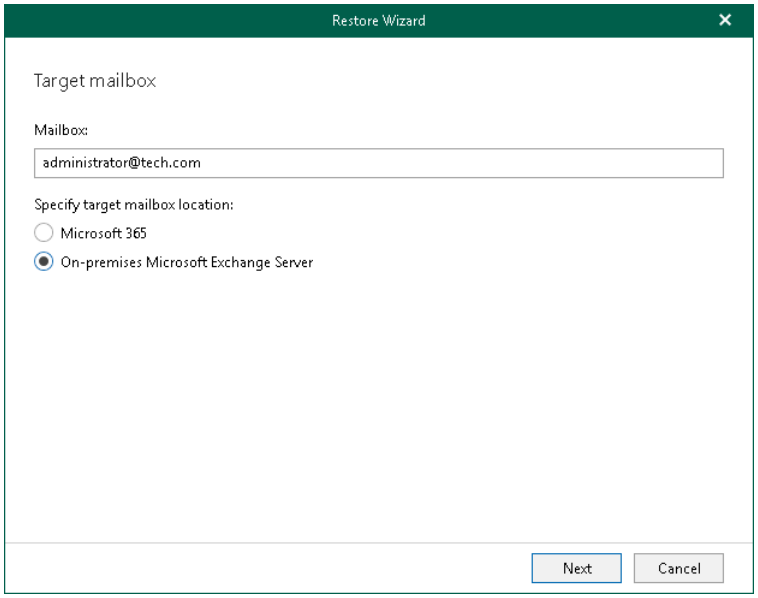
Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

To specify mailbox settings, do the following:

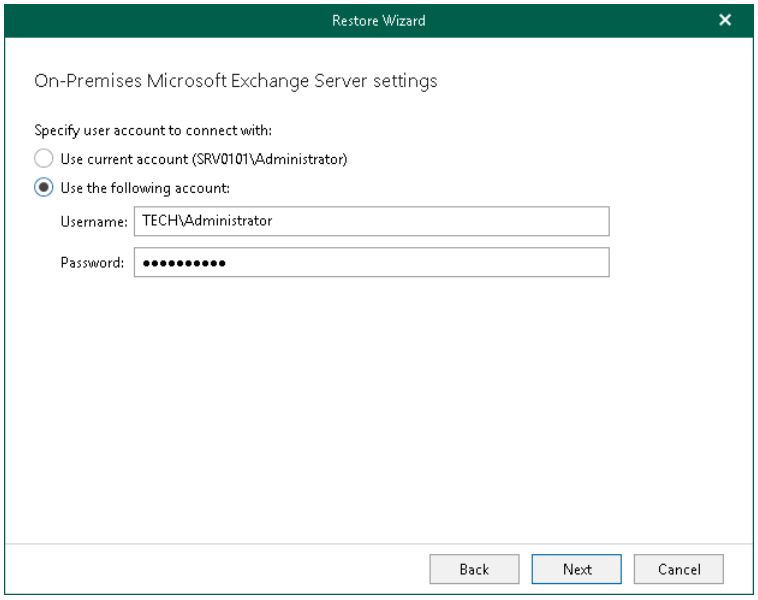
1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.
2. Select **On-premises Microsoft Exchange Server** to restore the specified mailbox to an on-premises Microsoft Exchange organization. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.

   You can also perform a restore of backups created for on-premises Microsoft Exchange organizations to Exchange Online organizations and vice versa. For more information, see Restore to Microsoft 365 Organizations.



Step 3. Specify User Account

At this step of the wizard, specify an account that you want to use to connect to the Exchange server in your domain.



Step 4. Specify CAS Server and Target Folder

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

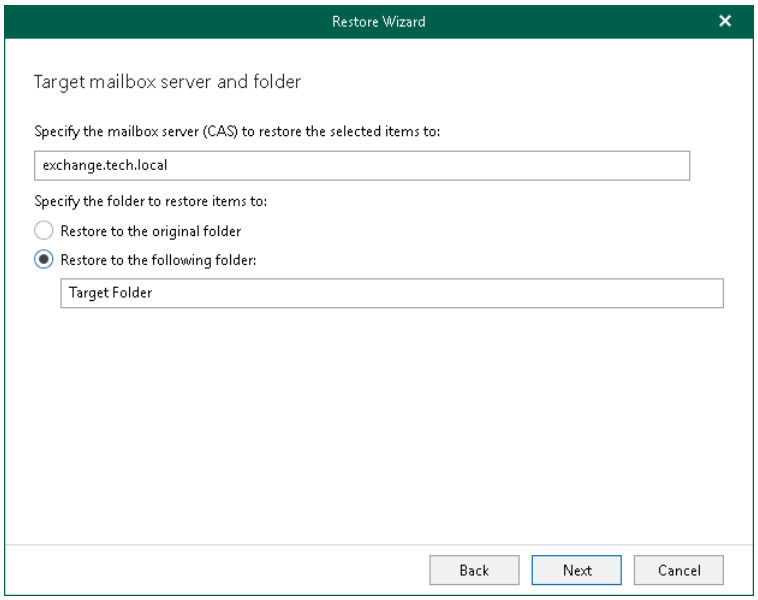
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or IP address.

   This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.

2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

   When you select to restore to a custom folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Explorer for Microsoft Exchange will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.



Step 5. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

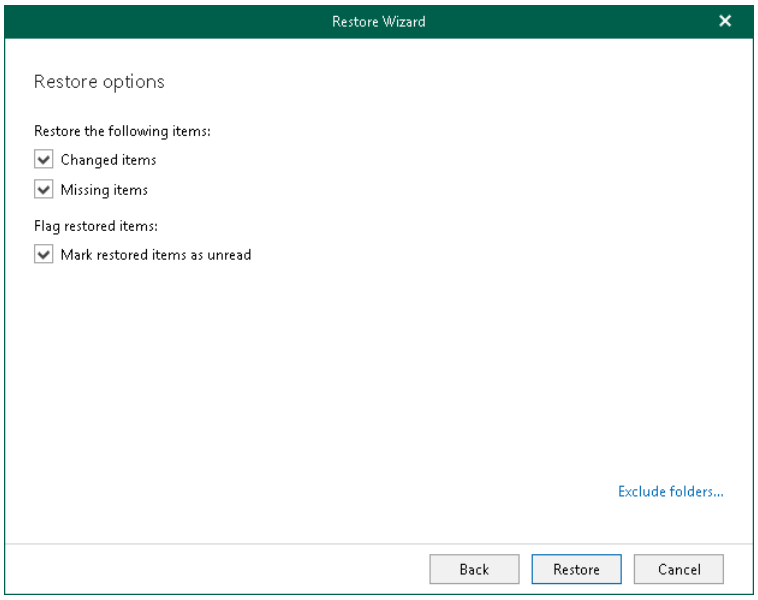
  Select this check box if you want to restore items that are missing in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

If you restore a mailbox, to prevent certain folders from being restored, click **Exclude folders** and select folders to exclude.

> **NOTE**
>
> The **Exclude folders** link is not available when restoring folders and items.



Restoring Multiple Mailboxes

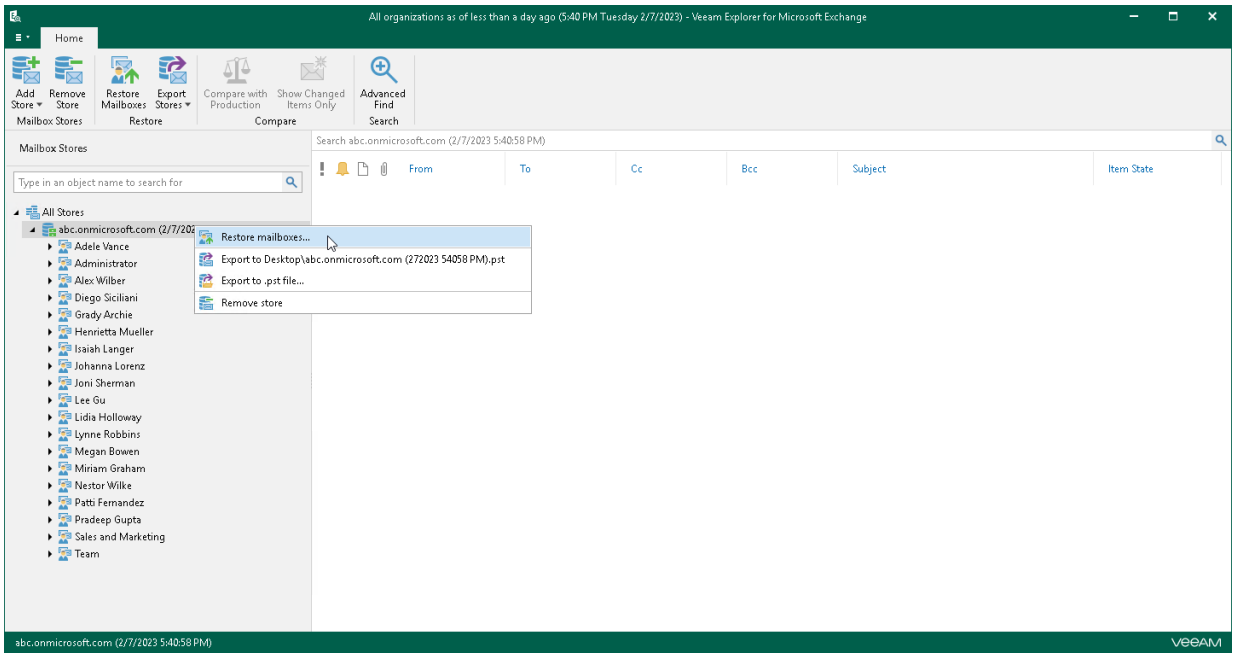
To restore multiple Exchange mailboxes, do the following:

1. Launch the Restore wizard.
2. Specify a domain and credentials.
3. Select mailboxes to restore.
4. Specify a target mailbox server.
5. Select restore options.

Step 1. Launch Restore Wizard

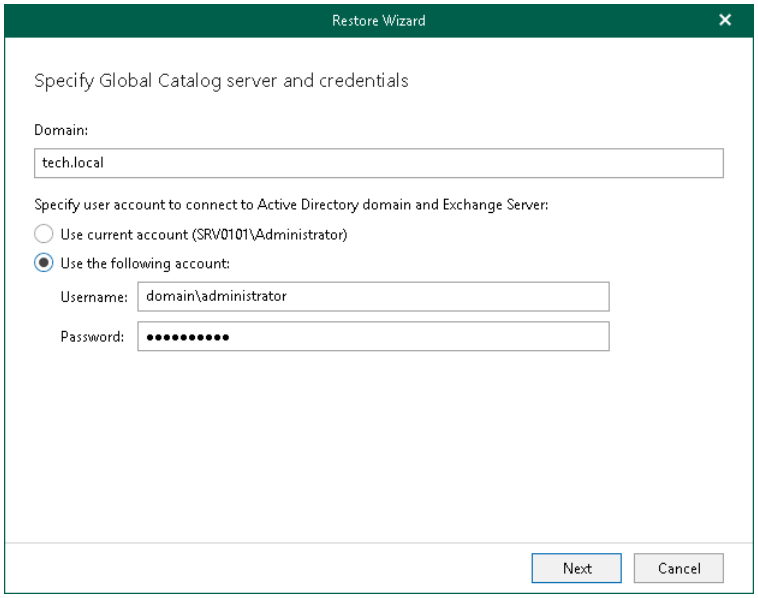
To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox store whose mailboxes you want to restore.
2. Do one of the following:
   - On the **Home** tab, click **Restore Mailboxes** on the ribbon.
   - Right-click a mailbox store and select **Restore mailboxes**.



Step 2. Specify Domain and Credentials

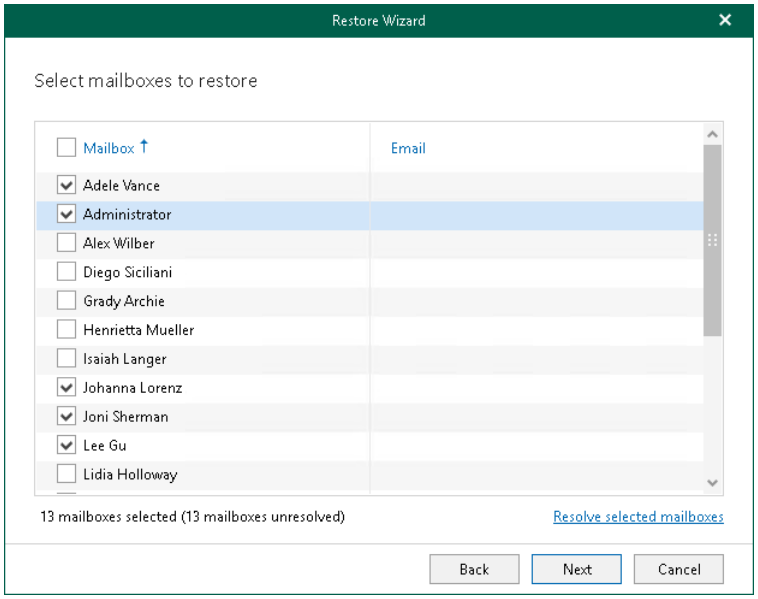
At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.



Step 3. Select Mailboxes to Restore

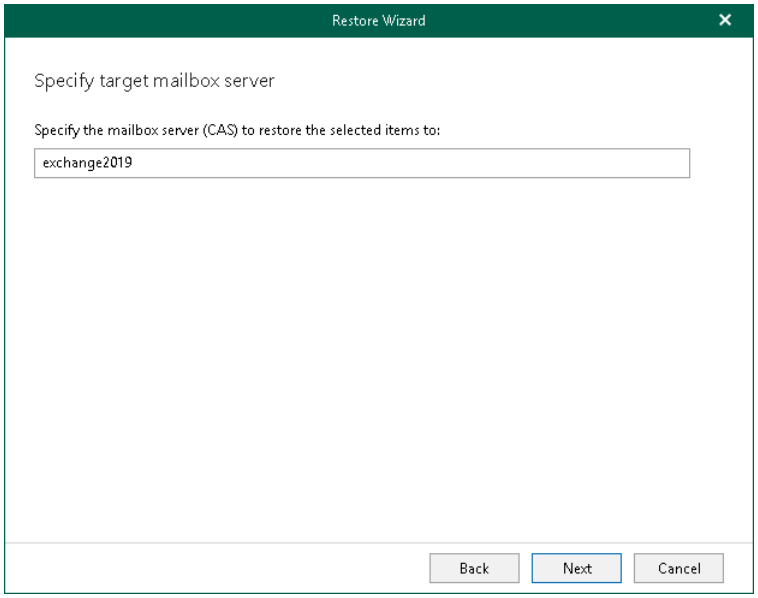
At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **Email** column, click **Resolve selected mailboxes**.



Step 4. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes.



Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

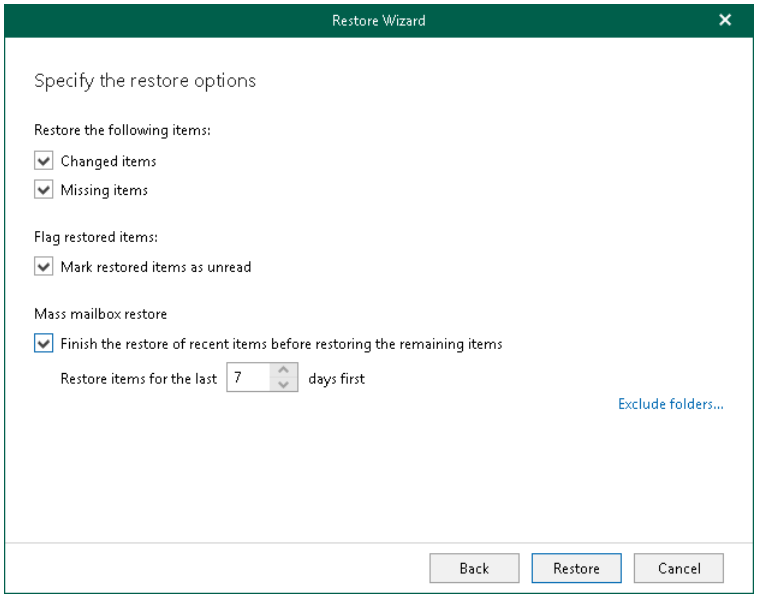
  Select this check box if you want to restore items that are missing in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.



1-Click Restore

The *1-Click Restore* feature allows you to quickly restore Exchange mailboxes, folders and items according to the following:

- The original Exchange server, original folder and the original mailbox name are restored.
- Both changed and missing items are restored.
- Restored items are marked as unread.
- No folders are excluded.

You can use *1-Click Restore* when you do not want to configure a restore session and prefer to restore data with the default settings.

Restoring to Microsoft 365 Organizations

This scenario is only available for data restore from backups created by Veeam Backup for Microsoft 365.

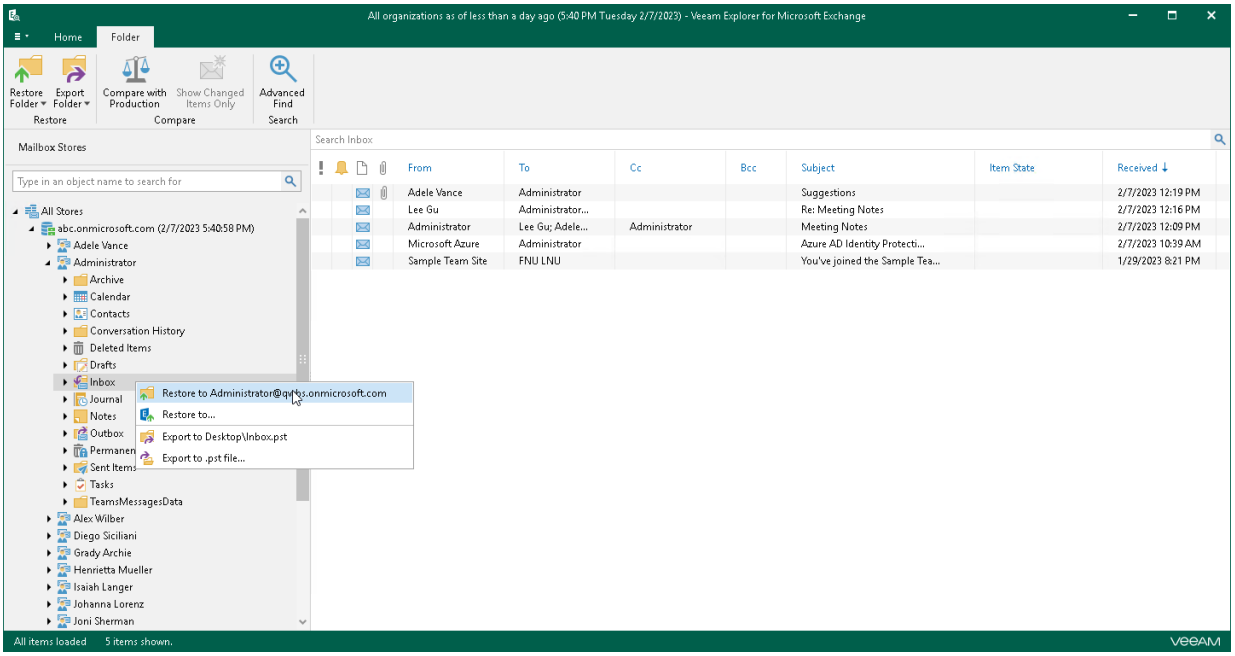
To perform *1-Click Restore* to Microsoft 365 organizations, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. Do one of the following:
   - On the **Mailbox/Folder/Items** tab, click **Restore Mailbox/Restore Folder/Restore Item** > **Restore to <mailbox_name>** on the ribbon.
   - Right-click a mailbox, folder or an item and select **Restore to <mailbox_name>**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

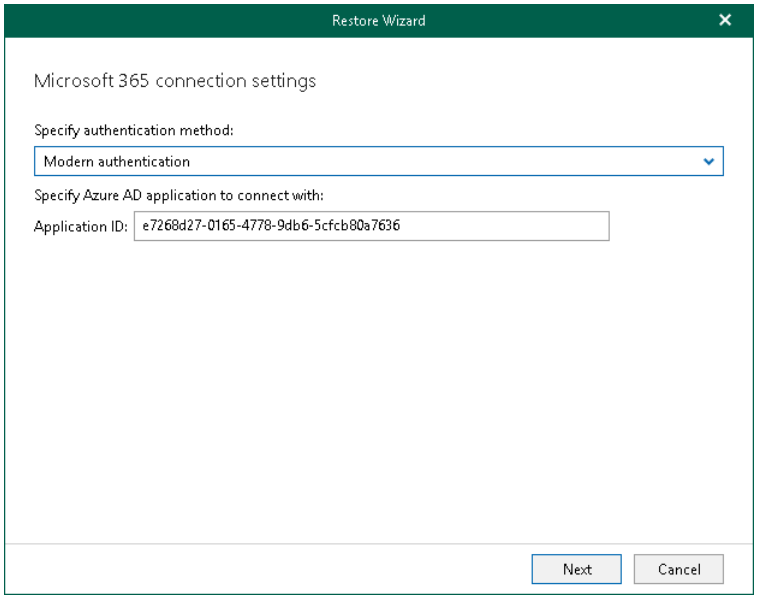
To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified mailbox back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.

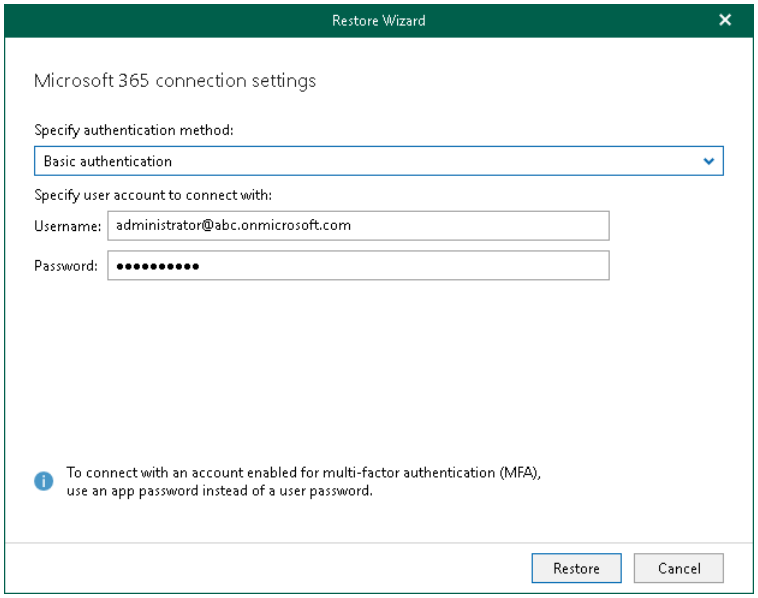


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the Exchange organization and click **Restore**.

   Make sure that the account that you use has both the *Exchange Administrator* and the *Global Administrator* roles.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

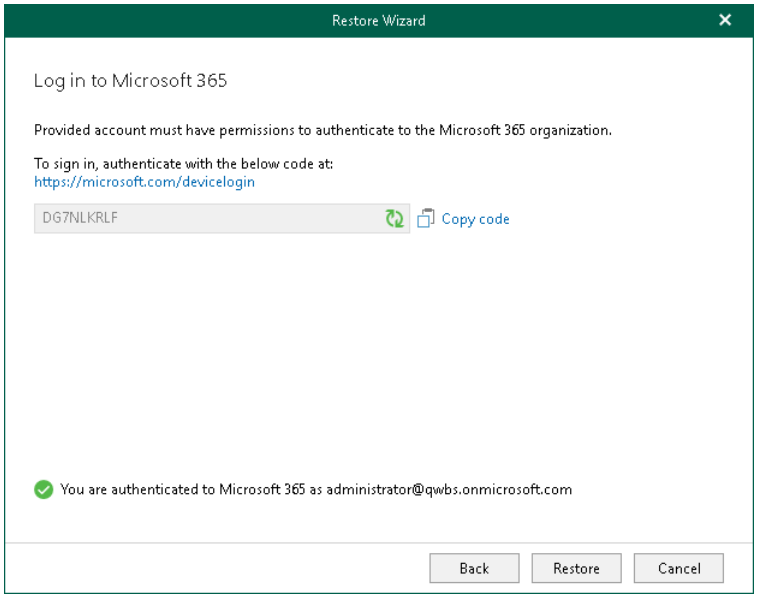
2. Click the Microsoft authentication portal link.

   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has both the *ApplicationImpersonation* and the *Exchange Administrator* roles. For more information, see this Microsoft article.

4. Return to the **Restore Wizard** window and click **Restore**.



Restoring to On-Premises Microsoft Servers

To perform *1-Click Restore* to on-premises Microsoft servers, do the following:

1. Launch the Restore wizard.
2. Specify a user account.

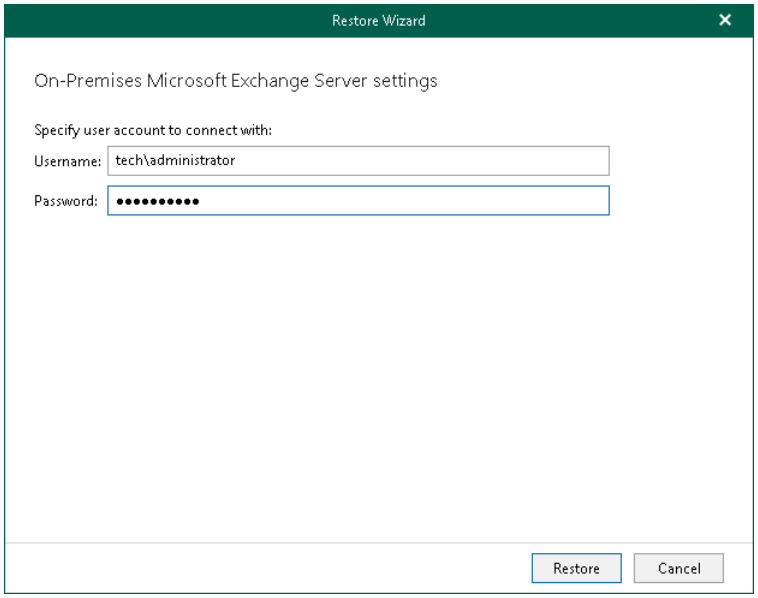
Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a mailbox, folder or item that you want to restore.
2. Do one of the following:
   - On the **Mailbox/Folder/Items** tab, click **Restore Mailbox/Restore Folder/Restore Item** > **Restore to <mailbox_name>** on the ribbon.
   - Right-click a mailbox, folder or an item and select **Restore to <mailbox_name>**.

Step 2. Specify User Account

At this step of the wizard, specify an account that you want to use to connect to the Exchange server.



Data Export

You can use Veeam Explorer for Microsoft Exchange to export Microsoft Exchange data.

Before exporting data, read the Considerations and Limitations section.

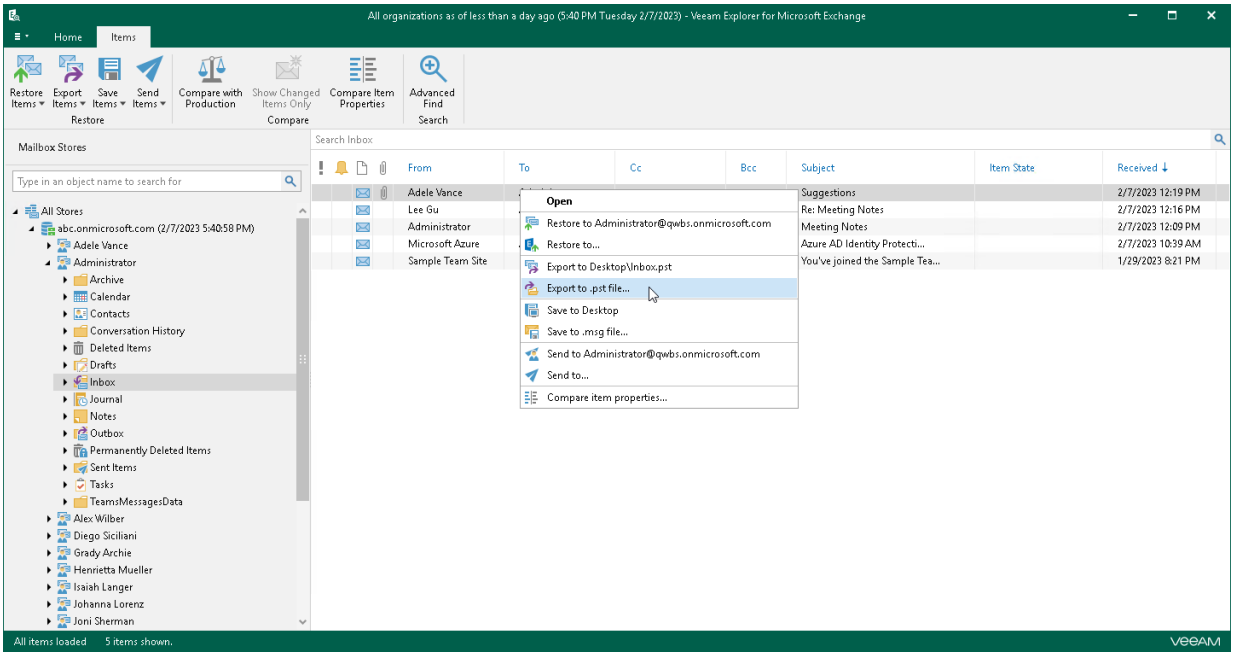
Exporting to Custom Location

Veeam Explorer for Microsoft Exchange allows you to export mailbox store data to a custom location as PST files.

> **NOTE**
>
> Export operations require Microsoft Outlook to be installed on a computer running Veeam Explorer for Microsoft Exchange.

To export objects to a custom location, do the following:

1. Do one of the following:
   - In the navigation pane, select a folder, a mailbox, a mailbox store or all stores added to the scope.
   - In the preview pane, select an item.
2. Do one of the following:
   - On the **Home/Mailbox/Folder/Items** tab, click **Export Stores/Export Mailbox/Export Folder/Export Items** > **Export to .pst file** on the ribbon.
   - Right-click an object and select **Export to .pst file**.



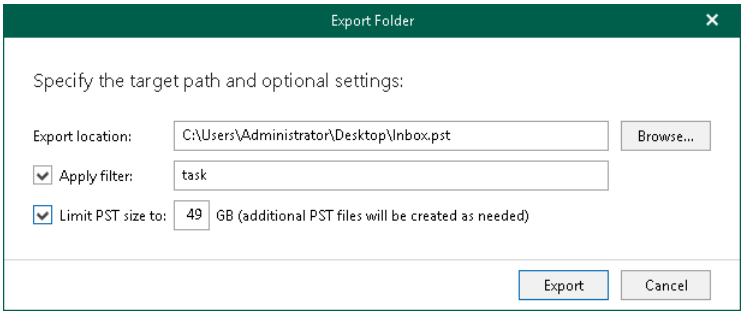
3. In the **Export Folder**/**Export Mail Items** window, do the following:
   a. In the **Export location** field, specify the name and location for the new PST file.
   b. Select the **Apply filter** check box and enter keywords to export only those items that match specified criteria. To provide multiple keywords, use the *OR* logical operator as the delimiter.

      Veeam Explorer for Microsoft Exchange will check for the specified keywords in all fields such as **From**, **To**, **Subject** and **Body**.

      The **Apply filter** option is only available when exporting folders and mailboxes, not items.

c. Select the **Limit PST size to** check box and specify the size of which to export PST files.

With this option, Veeam Explorer for Microsoft Exchange will create multiple PST files as of the specified size.



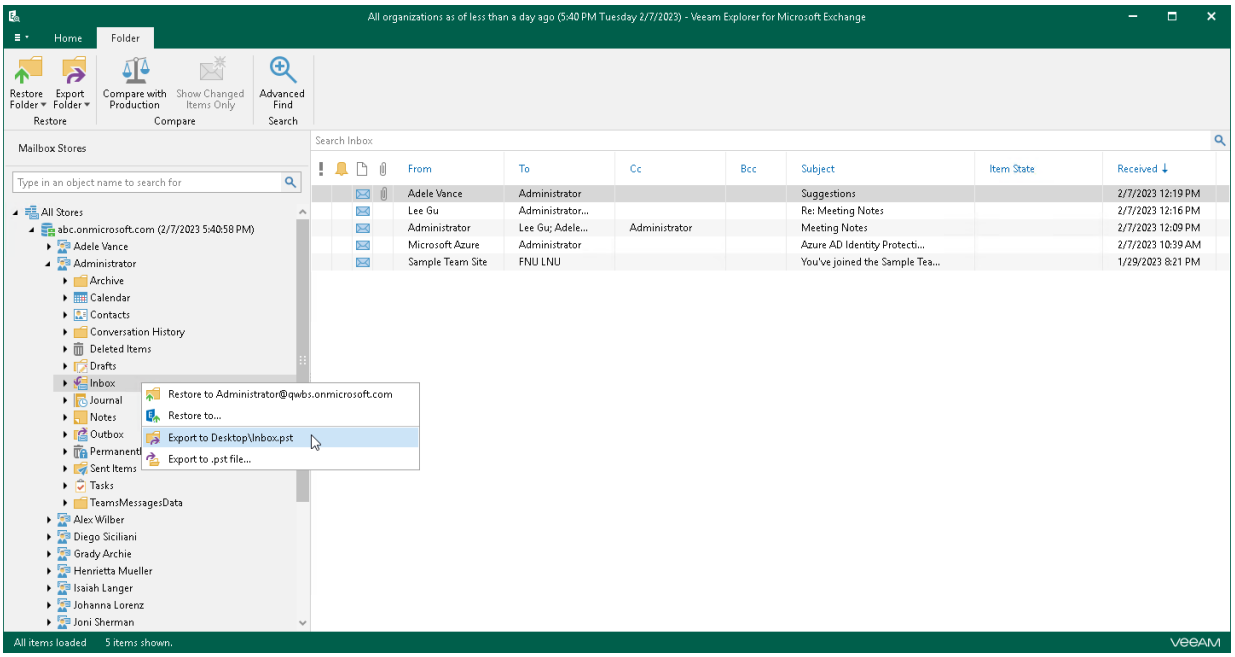
Using 1-Click Export

Veeam Explorer for Microsoft Exchange allows you to quickly export mailbox store data as PST files.

> **NOTE**
>
> Export operations require Microsoft Outlook to be installed on a computer running Veeam Explorer for Microsoft Exchange.

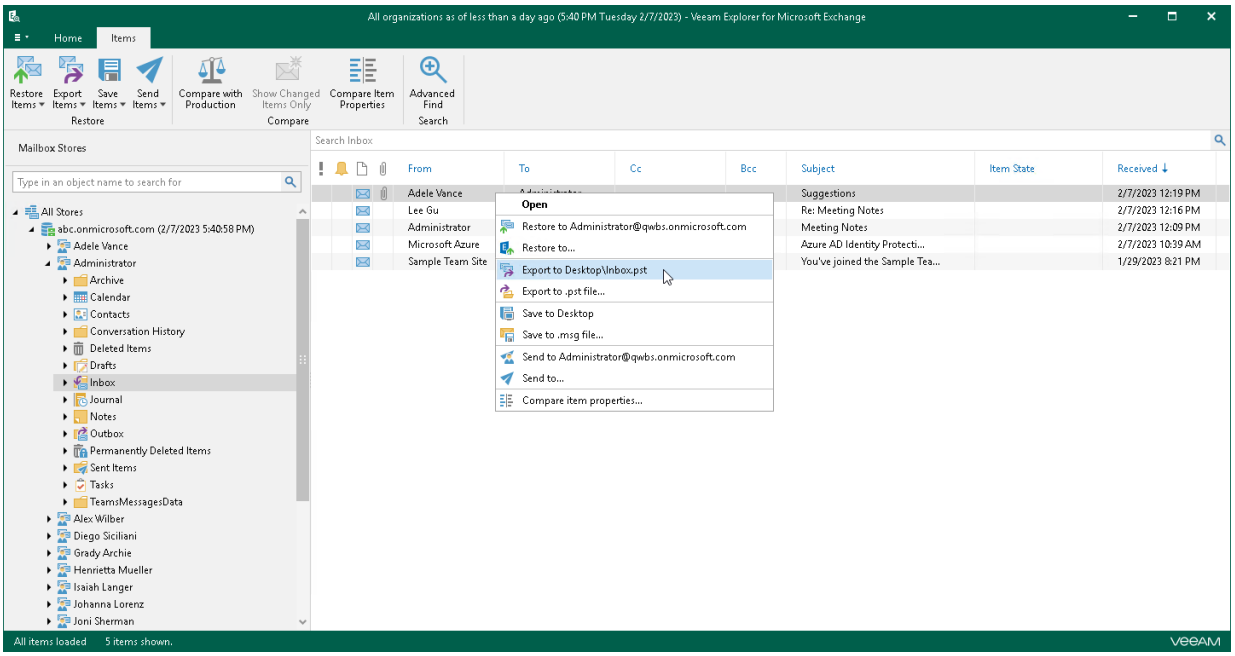
Depending on the object type you want to export, do the following:

- To export a folder, in the navigation pane, do one of the following:
  - Select a folder and on the **Folder** tab, click **Export Folder** > **Export to <default_location>\<original_folder_name>.pst** on the ribbon.
  - Right-click a folder and select **Export to <default_location>\<original_folder_name>.pst**.

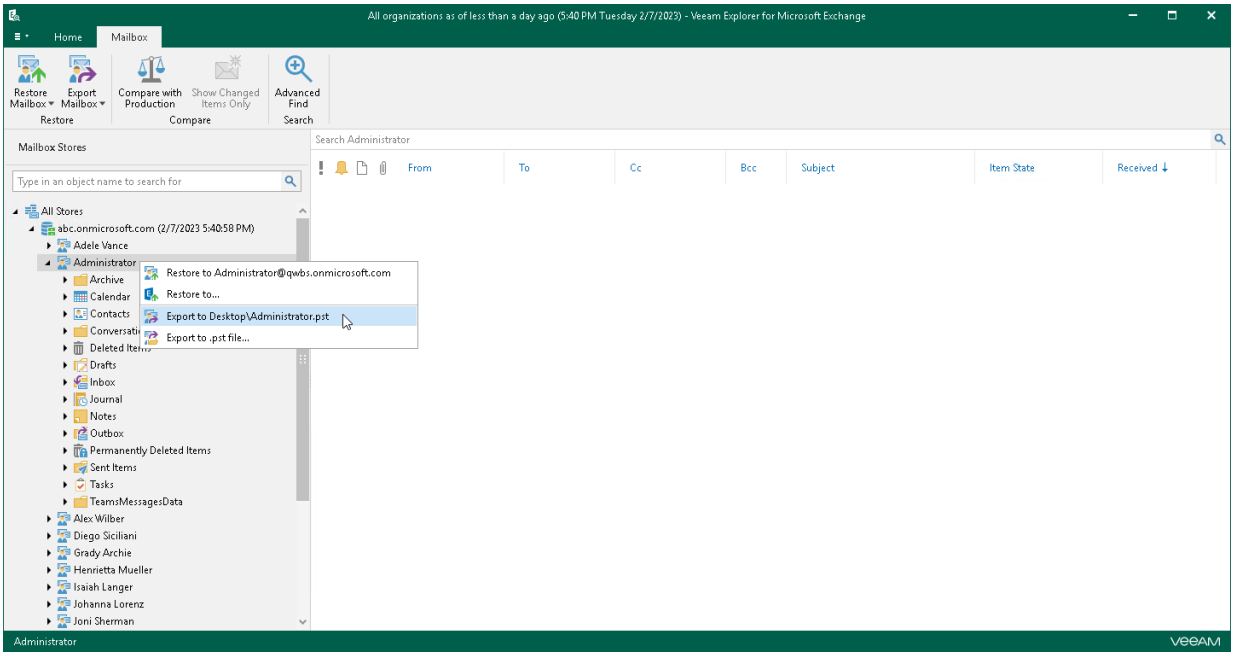


- To export an item, in the preview pane, do one of the following:
  - Select an item and on the **Items** tab, click **Export Items** > **Export to <default_location>\<original_folder_name>.pst** on the ribbon.

- Right-click an item and select **Export to <default_location>\<original_folder_name>.pst**.

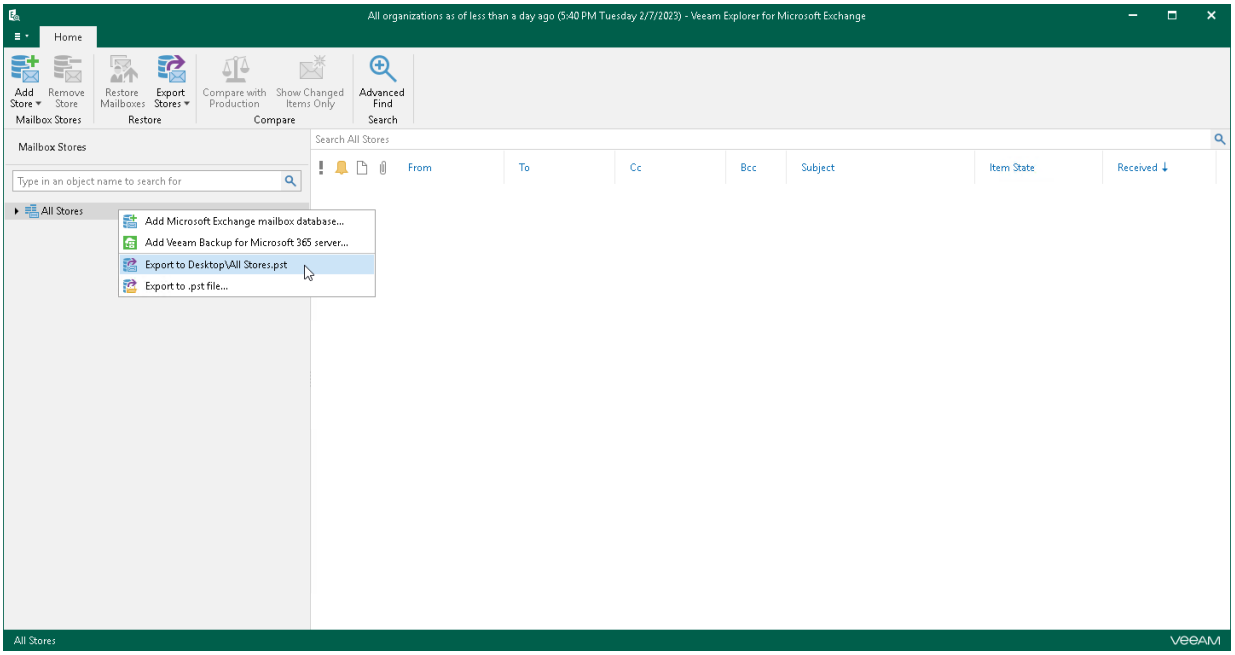


- To export a mailbox, in the navigation pane, do one of the following:
  - Select a mailbox and on the **Mailbox** tab, click **Export Mailbox** > **Export to <default_location>\<original_mailbox_name>.pst** on the ribbon.
  - Right-click a mailbox and select **Export to <default_location>\<original_folder_name>.pst**.



- To export a mailbox store or all stores added to the scope, in the navigation pane, do one of the following:
  - Select a store or the **All Stores** node and on the **Home** tab, click **Export Stores** > **Export to <default_location>\<original_store_name>.pst** on the ribbon.

- Right-click a store or the **All Stores** node and select **Export to <default_location>\<original_store_name>.pst**.



Receiving Export Reports

Veeam Explorer for Microsoft Exchange can deliver reports that show summary information about export operations.

Consider the following:

- If you want export reports to be delivered, make sure to configure an SMTP server in Veeam Explorer for Microsoft Exchange or Veeam Backup & Replication notification settings.

  For more information, see the SMTP Settings section of this guide and the Configuring Global Email Notification Settings section of the Veeam Backup & Replication User Guide.

- A server with Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication must be in a domain.

- Export reports are delivered automatically upon each export session.

  You can use Exporting to Custom Location or Using 1-Click Export.

- Keep in mind the following when specifying recipients of the report:

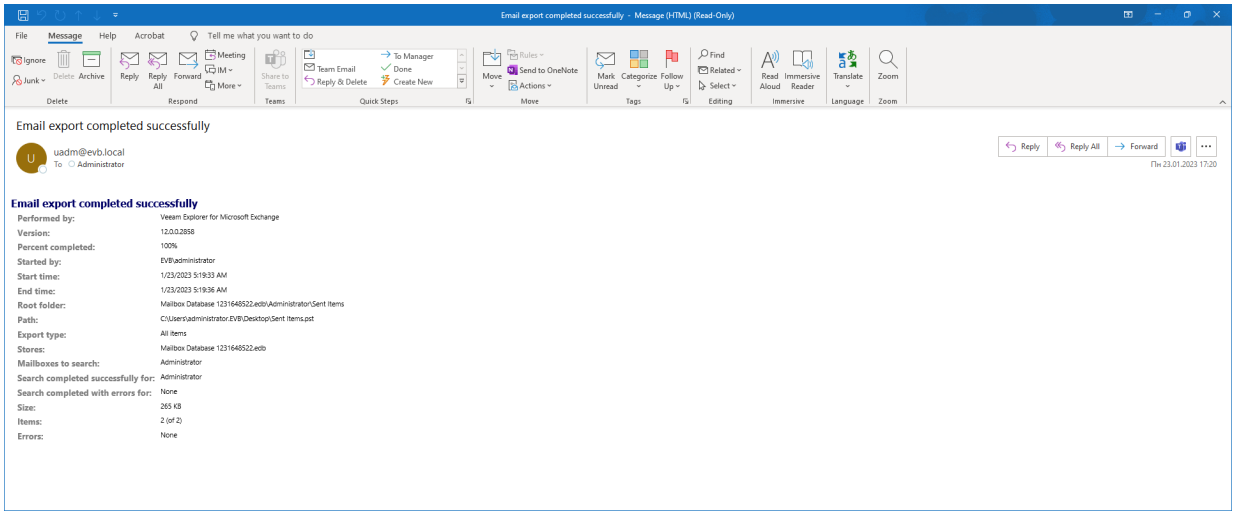
  - The recipient is always the current user account under which Veeam Explorer for Microsoft Exchange is running when using only Veeam Explorer for Microsoft Exchange notification settings.
  - The recipient is always the user account provided in Veeam Backup & Replication notification settings when using only Veeam Backup & Replication settings.
  - If you have configured both Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication notification settings, the report will be sent to both recipients.

    > **NOTE**
    >
    > If you export Microsoft Exchange data using PowerShell cmdlets and you have a restore session started for Veeam Backup for Microsoft 365, the report will only be sent to the user account provided in Veeam Explorer for Microsoft Exchange notification settings.

The following table lists fields that are shown in the report.

Report field	Description
Performed by	Veeam Explorer for Microsoft Exchange
Version	Shows the Veeam Explorer for Microsoft Exchange build number.
Percent completed	Shows the number of items included in the PST file.
Started by	Shows the user account generated the report.
Start time, End time	Shows the creation time of a report.
Root folder	Shows the object path.

Report field	Description
Path	Shows the path to the database file.
Export type	Shows the export type.
Stores	Shows a datastore name from which items have been exported.
Mailboxes to search	Shows a mailbox name from which items have been exported.
Search completed successfully for, Search completed with errors for	Shows results for mailboxes to search.
Size	Shows the total size of exported items.
Items	Shows the number of exported items.
Errors	Shows errors that occurred during export.



Data Compare

You can use Veeam Explorer for Microsoft Exchange to compare data in a backup file with that of the production state.

> **NOTE**
>
> The Veeam Backup account you want to use for data compare, must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization. For more information about the required permissions, see Permissions.

To compare backed-up data with production environment, do the following:

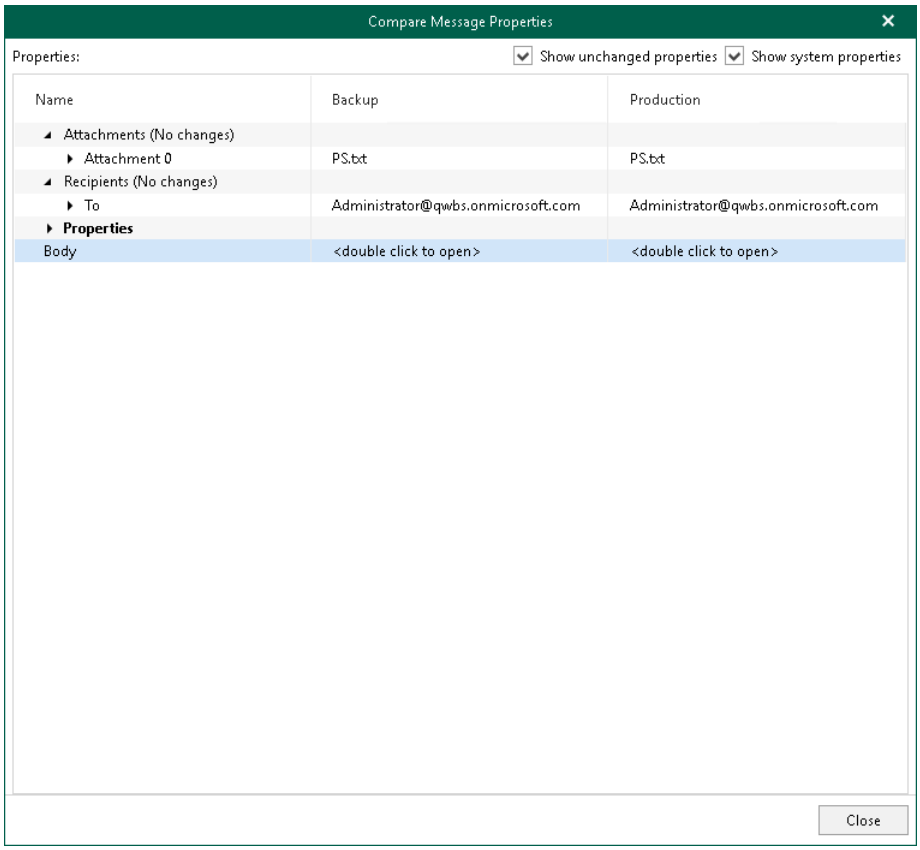
1. In the navigation pane, select an object and click **Compare with Production** on the ribbon.
2. Proceed to either Compare to Microsoft 365 Organizations or Compare to On-Premises Microsoft Servers.
3. After the authorization process is complete, click **Show Changed Items Only** on the ribbon to view only those items that have been changed.

To view the details on what exactly has changed since the last backup, right-click an item and select **Compare item properties**. The discrepancies will be shown in the **Compare Message Properties** window. If both objects are equal, nothing will be displayed.

To show unchanged objects, select **Show unchanged properties** in the top-right corner. To show system properties, select **Show system properties**.

Double-click **Body** to see the body message.

To compare a single item, right-click an item and select **Compare item properties**.



Compare to Microsoft 365 Organizations

This scenario is only available for backups created by Veeam Backup for Microsoft 365.

To compare data with your production Microsoft 365 organizations, do the following:

1. Select an authentication method.
2. Log in to Microsoft 365.

Step 1. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

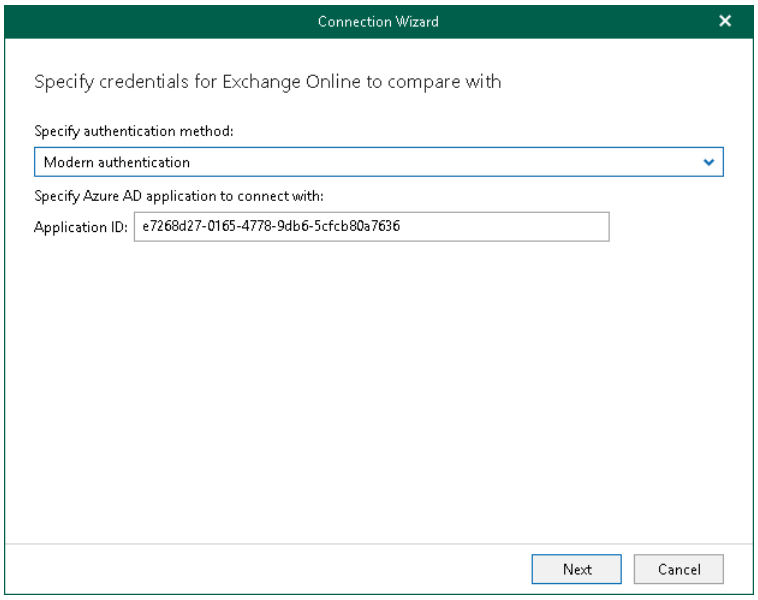
To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified mailbox back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

   By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.

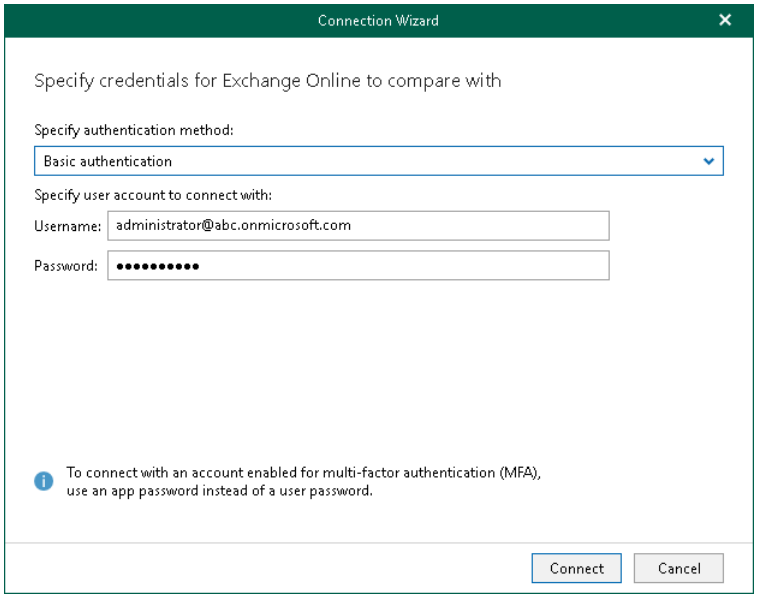


Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the Exchange organization and click **Connect**.

   Make that the account that you use has both the *Exchange Administrator* and the *Global Administrator* roles.



Step 2. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

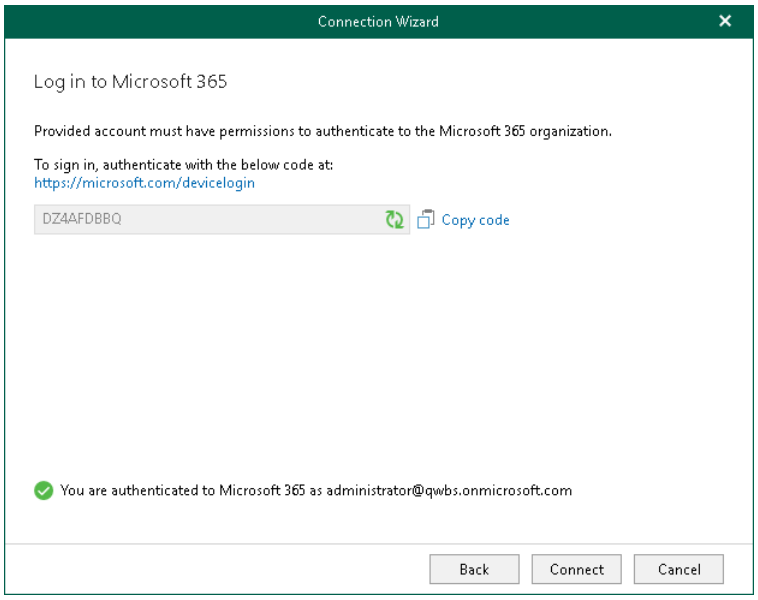
2. Click the Microsoft authentication portal link.

   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has both the *ApplicationImpersonation* and the *Exchange Administrator* roles. For more information, see this Microsoft article.

4. Return to the **Connection Wizard** window and click **Connect**.



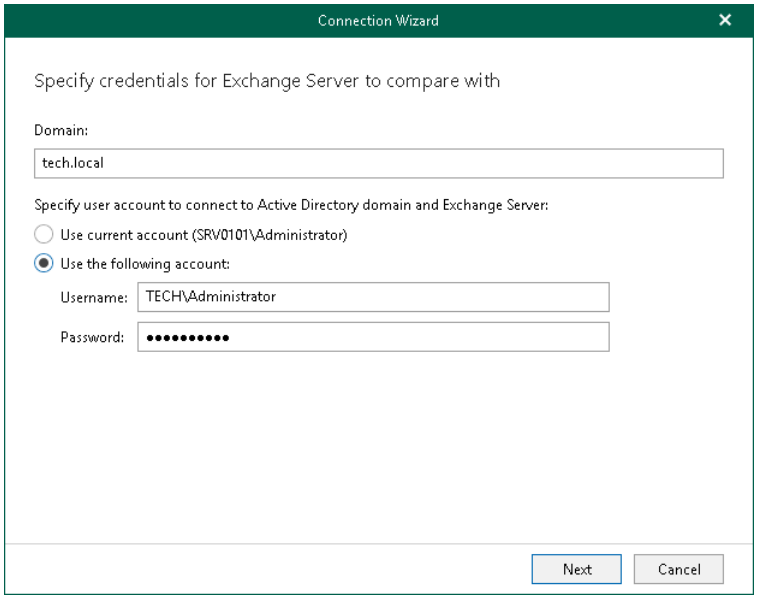
Compare to On-Premises Microsoft Servers

To compare data with your production on-premises Microsoft Exchange, do the following:

1. Specify a domain and credentials.
2. Specify a target mailbox server.

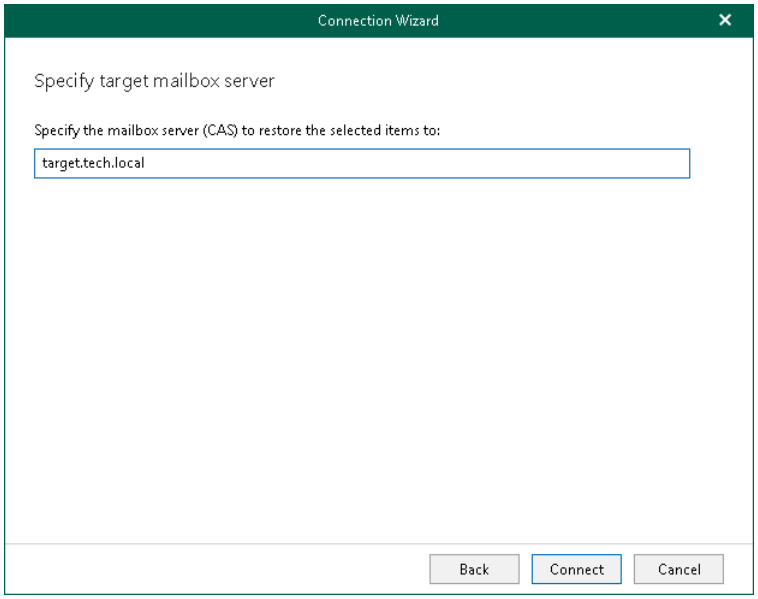
Step 1. Specify Domain and Credentials

At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.



Step 2. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes and click **Connect**.



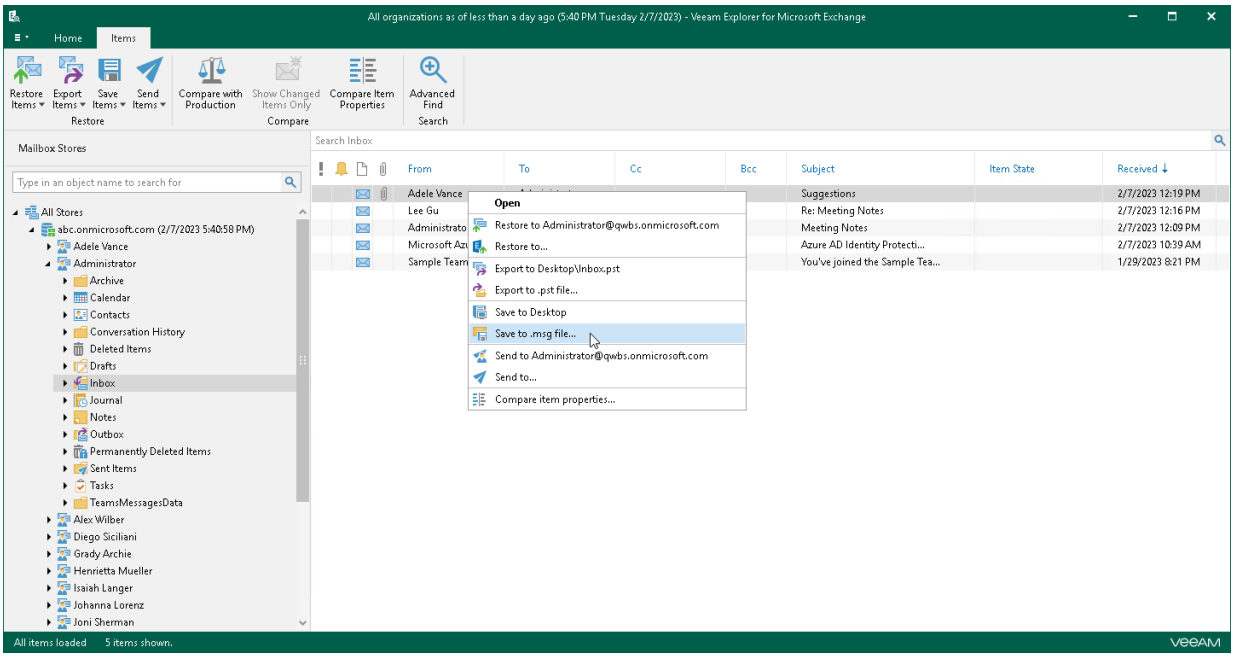
Saving Microsoft Exchange Items

Veeam Explorer for Microsoft Exchange allows you to save any item as *Microsoft Exchange Mail Document* (*.msg*) files.

Saving to Custom Location

To save items to a custom location, do the following:

1. In the navigation pane, select a folder and then in the preview pane, select an item.
2. Do one of the following:
   - On the **Items** tab, click **Save Items** > **Save to .msg file** on the ribbon.
   - Right-click an item and select **Save to .msg file**.



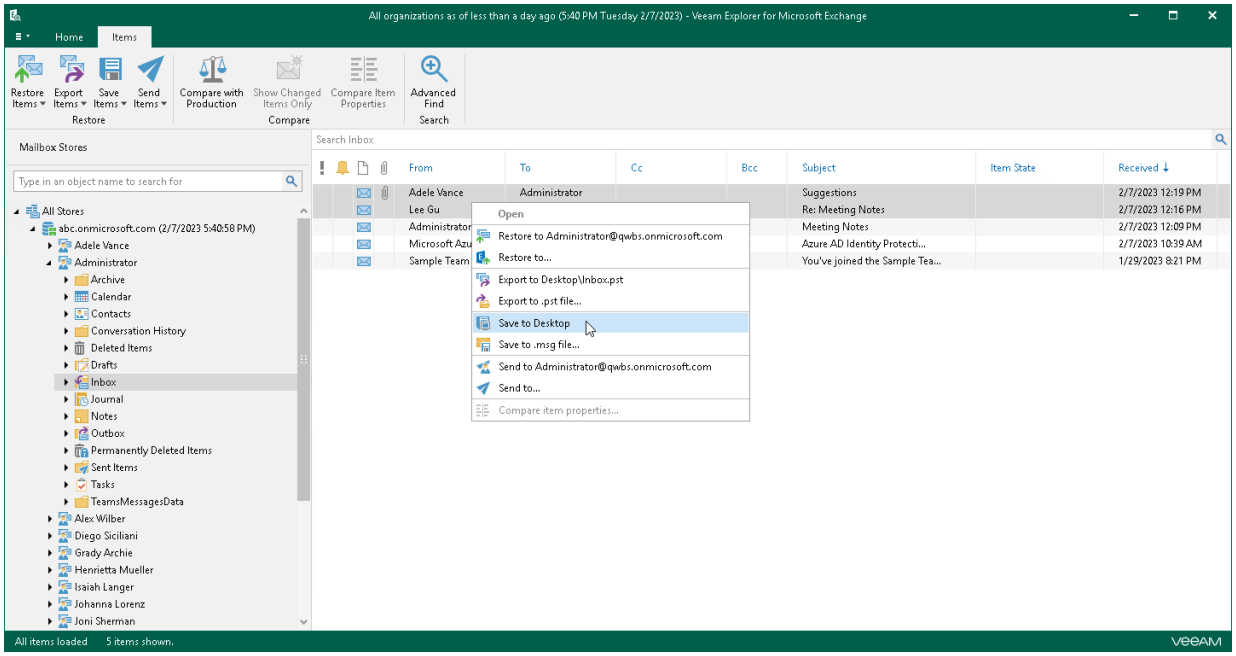
1-Click Save

To save your Exchange data, do the following:

1. In the navigation pane select a folder containing required items.
2. In the preview pane, select items that you want to save.

   Use the **Search** field to find particular items.
3. Do one of the following:
   - On the **Items** tab, click **Save Items** > **Save to <folder_name>** on the ribbon.
   - Right-click an item and select **Save to <folder_name>**.

   A **<folder_name>** name depends on the latest location that was used when saving items.



Sending Microsoft Exchange Items

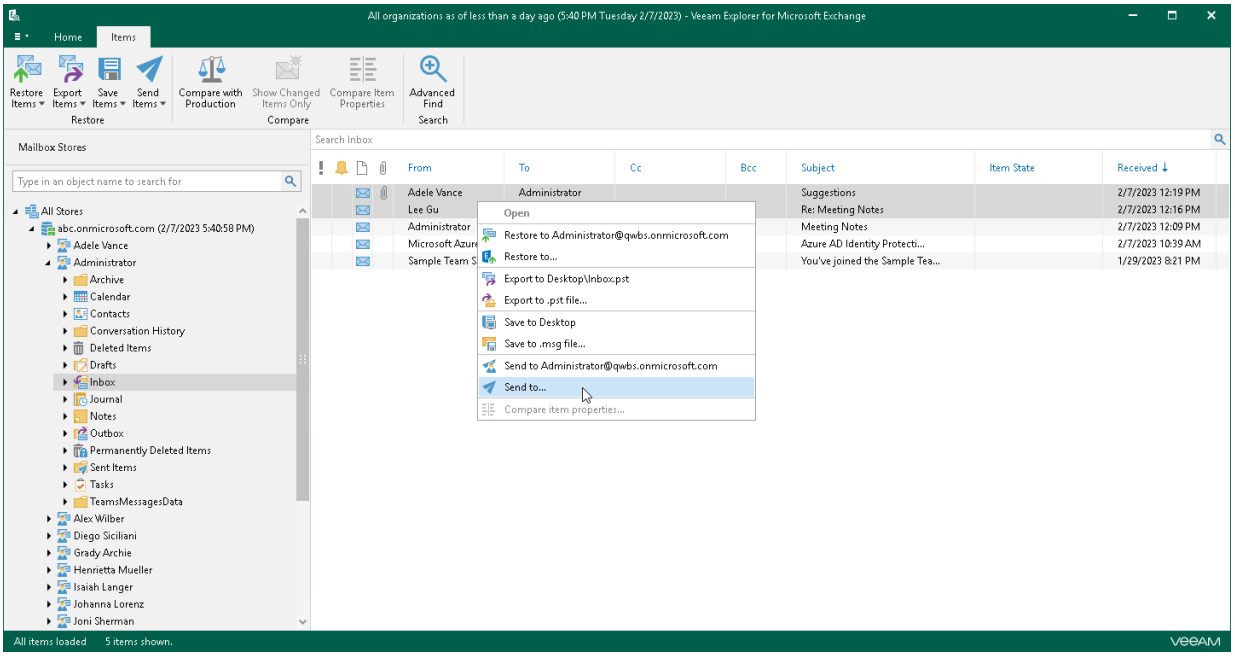
Veeam Explorer for Microsoft Exchange allows you to send Exchange items through email.

> **TIP**
>
> Before sending documents, make sure to configure SMTP settings. The amount of data you can send at a time depends on your SMTP server configuration. For more information about configuring SMTP settings, see SMTP Settings.

To send items, do the following:

1. In the navigation pane select a folder containing required items.
2. In the preview pane, select items to send.

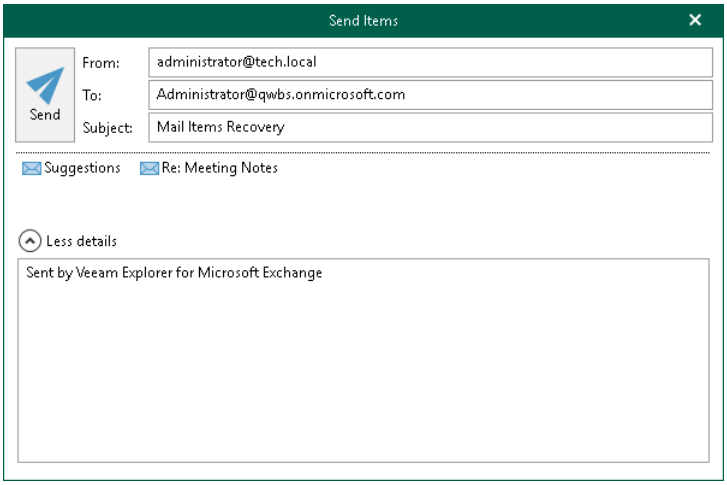
   Use the **Search** field to find particular items.
3. Do one of the following:
   - On the **Items** tab, click **Send Items > Send to** on the ribbon.
   - Right-click an item and select **Send to**.



4. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

You can also edit the message subject and body. To edit the message body, click **More details**.



Veeam Explorer for Microsoft SharePoint

Veeam Explorer for Microsoft SharePoint allows you to restore and export Microsoft SharePoint data from backups created by Veeam Backup for Microsoft 365 and Veeam Backup & Replication.

Planning and Preparation

You can configure your environment before you start using Veeam Explorer for Microsoft SharePoint.

System Requirements

This section lists system requirements for Veeam Explorer for Microsoft SharePoint.

Component	Requirement
Microsoft SharePoint	For more information about supported versions of Microsoft SharePoint, see: • The Supported Applications subsection of the Veeam Backup & Replication User Guide. • The System Requirements section of the Veeam Backup for Microsoft 365 User Guide.

NOTE

Consider the following:

- To restore SharePoint content database items from a server running Microsoft Windows ReFS, the backup server or Veeam Backup & Replication console must be installed on the Microsoft Windows Server 2012 or later.
- To restore from a server running Microsoft Windows ReFS 3.x, Veeam backup server or a management console must be installed on the Microsoft Windows Server 2016.

Ports

The following tables list network ports that must be opened to manage inbound and outbound traffic.

General

From	To	Protocol	Port	Notes
Veeam Explorer for Microsoft SharePoint	SharePoint web application	As recommended by Microsoft	As recommended by Microsoft	For more information on recommended port numbers and protocols for SharePoint web application, see this Microsoft article. To discover ports currently used by your SharePoint web application, follow the steps described in this Microsoft article.
Backup server, Veeam Backup & Replication console, mount server associated with the backup repository	Staging server	TCP, UDP	135, 445	Ports used to deploy the runtime coordination process on the target machine.
		TCP	49152 to 65535 (for Microsoft Windows 2008 or later)	Dynamic RPC range used by the runtime coordination process that is deployed on the target machine.[1] For more information, see this Microsoft article.
		TCP	6160	Port used to communicate with the installer service.
Backup server, Veeam Backup & Replication console	Staging server	TCP	1433, 1434 and other	Ports used to communicate with Microsoft SQL servers hosting content databases. Exact port numbers depend on the configuration of the Microsoft SQL server. For more information, see this Microsoft article.

From	To	Protocol	Port	Notes
		UDP	1434	Port used by the Microsoft SQL Server Browser service. For more information, see this Microsoft article.

[1] If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *RPC function call failed* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

> **NOTE**
>
> To restore database items or lists to a server that is running in a DMZ, the SharePoint web application ports will be used.

iSCSI Traffic

From	To	Protocol	Port	Notes
Staging server	Mount server associated with the backup repository	TCP	3260 to 3270	Ports used by iSCSI initiator to connect to the iSCSI target.

Permissions

The following table lists required permissions for data restore.

Operation	Required Roles and Permissions
Restore to on-premises Microsoft SharePoint	To restore data to on-premises Microsoft SharePoint organizations, you must grant the following roles and permissions to user accounts: • The account must be granted *Full Control* to connect to the target SharePoint server. • The account must be assigned either the *Site Administrator* or *System Account* role to restore user permissions. • If permissions of items being restored are inherited from the parent one, the account must be granted *Full Control*. • If permissions of items being restored are not inherited from the parent one and items being restored replace the existing ones, the account must be granted *Contribute* and *Full Control*.

Operation	Required Roles and Permissions
Restore to Microsoft Office 365	To restore data to SharePoint Online organizations, you must grant the following roles and permissions to user accounts: **Restore Using Basic Authentication Method** • The account used to log in to Microsoft Office 365 must have the *Global Administrator* or *SharePoint Administrator* role assigned. • For restore of personal SharePoint sites, make sure to select the **Allow users to run custom script on personal sites** option in the SharePoint admin center. For more information, see this Microsoft article. • During restore, Veeam Backup for Microsoft 365 automatically assigns the *Site Collection Administrator* role to the user account. **Restore Using Modern Authentication Method** • The account used to log in to Microsoft Office 365 must have the *Global Administrator* or *SharePoint Administrator* role assigned. • For restore of personal SharePoint sites, make sure to select the **Allow users to run custom script on personal sites** option in the SharePoint admin center. For more information, see this Microsoft article. • During restore, Veeam Backup for Microsoft 365 automatically assigns the *Site Collection Administrator* role to the user account. • Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide. • If you restore data with Azure AD applications using a certificate, make sure that your Azure AD application is granted the required permissions. For more information, see the Permissions for Modern App-Only Authentication section of the Veeam Backup for Microsoft 365 User Guide.

Consider the following:

- The current account can only be used to access a *local* staging server. To connect to a *remote* server, use appropriate authentication credentials to access that server.
- The account requires the *sysadmin* fixed server role on a staging Microsoft SQL server.
- For ADFS as an authentication provider:
  - When using *Windows Authentication*, you can use both your current account or provide another account.
  - When using *Forms Authentication*, the current account cannot be used.

Required Backup Job Settings

This requirement applies to backup jobs created by Veeam Backup & Replication.

When you create a backup job, make sure to enable the **application-aware image processing** option. For more information, see the Specify Guest Processing Settings section of the Veeam Backup & Replication User Guide.

Staging SQL Server

To perform Microsoft SharePoint items restore, Veeam Explorer for Microsoft SharePoint requires a Microsoft SQL server to be used as a staging system.

The server you plan to use as a staging system must conform to the following requirements:

- A staging system must have the same or later version of Microsoft SQL Server that hosts restored Microsoft SharePoint databases.
- Microsoft SQL Server that is included in Microsoft SQL Server Failover Cluster cannot be used as a staging system.
- Nodes participating in AlwaysOn Availability Groups are supported. However, you should not use Availability Group Listeners as staging servers.

> **NOTE**
>
> You can use Microsoft SQL Server 2012/2016 Express editions which are shipped with the Veeam Backup & Replication distribution package. Consider that due to Express edition limitations, the maximum database size that can be attached is 10 GB. For more information, see this Microsoft article.

Remote BLOB Stores Support

A BLOB store must be either included in the SharePoint backup created by Veeam Backup & Replication or Veeam Agent for Microsoft Windows (for automated discovery) or stored on a local machine running Veeam Explorer for Microsoft SharePoint (for manual discovery).

> **IMPORTANT**
>
> RBS FILESTREAM is the only provider that is supported in the current version.

Make sure the staging Microsoft SQL Server configuration meets the following requirements:

1. **FILESTREAM** is enabled on a database server. For more information, see the following articles:
   - For SQL Server 2017 for Windows, see this Microsoft article.
   - For SQL Server 2016, see this Microsoft article.
   - For SQL Server 2014, see this Microsoft article.
   - For SQL Server 2012, see this Microsoft article.
   - For SQL Server 2008 R2, see this Microsoft article.
2. **RBS Client Library** is installed on the database server.

   For Microsoft SQL Server 2014 and later, the Remote Blob Store setup is included in the installation media. For other versions, you can use the Microsoft SQL Server Remote Blob Store installation package. For more information on how to install the package, see this Microsoft article.

Considerations and Limitations

This section lists considerations and limitations of Veeam Explorer for Microsoft SharePoint.

General

Consider the following:

- When Veeam Explorer for Microsoft SharePoint is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.
- Restore using PowerShell Direct, VIX API or vSphere Automation API is not supported.
- Restore of backed-up Microsoft SharePoint data to another Microsoft organization cannot be performed to a target Microsoft SharePoint organization whose version is earlier than the version of the restored backups.
- To use an internet proxy server to restore backups created by Veeam Backup for Microsoft 365, make sure to provide appropriate proxy server address and the port number. To do this, go to the **Control Panel** > **Internet Options Connections** tab, click **LAN Settings**, select the **Use a proxy server for your LAN** check box and specify a proxy server you want to use. Credentials for such a proxy (if needed) will be taken from the **Control Panel** > **Credential Manager** > **Windows Credentials** console.

  Using an internet proxy server is only possible in Veeam Explorer for Microsoft SharePoint that comes as part of the Veeam Backup for Microsoft 365 distribution package.
- For VMs that run Microsoft SQL Server backed up by Veeam Agent for Microsoft Windows and Microsoft SharePoint backed up by Veeam Backup & Replication, to perform SharePoint item restore, you must start Veeam Explorer for Microsoft SharePoint from the Veeam Backup Browser. To do this, start File Level Recovery for the backup of the required SQL Server VM, and then launch Veeam Explorer for Microsoft SharePoint from the toolbar in the Veeam Backup Browser.

  If you start item-level recovery directly for the backup of the SharePoint VM, mapping of a SharePoint site to a content database in the Restore wizard will fail, and Veeam Backup & Replication will display the following error: "*Unable to find SQL Server VM hosting the content database for the selected SharePoint site*".

  Backup of the same VM by both Veeam Backup & Replication and Veeam Agent for Microsoft Windows may be required, for example, if Microsoft SQL Server running on the VM operates as part of a failover cluster.

Status Restore Limitations

Consider the following when planning documents/list items restore:

- If a document/item was in *Check Out* state when the backup was created, the last version of the item will not be restored to the target SharePoint and will be available for viewing only. Previous versions (if any) will be restored.
- If the *Declare this item as a record* action was originally applied to list item, the relevant status will not be preserved. Instead, the restored item status will be set in accordance with the target list/library content approval workflow.
- Original status *On Hold* will not be restored.

Restore of Documents, Libraries and Lists

Consider the following:

- Versioning settings of SharePoint lists are not preserved during restore.
- Restoring Generic List and Pages Library may fail with the "*No content type 'XXX' found in web YYY*" error.
- The *Created By* field of restored documents is updated with the account performing restore.
- Some *Rating Settings of Discussion* lists values are not restored.
- Make sure to view information about unsupported Microsoft SharePoint lists before restoring them. In particular, hidden lists are not displayed in Veeam Explorer for Microsoft SharePoint after a site backup. Thus, such lists cannot be exported. For more information, see Unsupported SharePoint Lists.

Restore of List Items

Consider that when restoring a list item, Veeam Explorer for Microsoft SharePoint works in the following way:

- Deletes an existing item.
- Creates the latest version of the item anew using data from the backup.
- Checks whether it is declared as a record.
- If the check is a success, the process finishes.
- If not, the created version is deleted and item versions are restored sequentially.

This logic leads to the following peculiarities of list item restore:

- If a list or list items column is used as a lookup column in the dependent list, consider that restoring an item from the source list causes the relevant items deletion in the dependent list.
- If a lookup column in the dependent list has the enforced relationship behavior set to **Cascade Delete**, then restoring an item from the source list may cause item deletion in the dependent list due to Microsoft implementation. For more information, see this Microsoft article.

To prevent this issue, you should turn off enforced relationship behavior. As a work-around, you can roll-back the SharePoint database using Veeam Explorer for Microsoft SQL Server (see this section) or roll-back the whole SharePoint server VM to the desired state using any Veeam Backup & Replication recovery option.

The following limitations should also be considered:

- If a lookup column in the dependent list has the enforced relationship behavior set to **Restrict Delete**, then item restore with Veeam Explorer for Microsoft SharePoint will fail.
- If an .ASPX page references an item using *ItemID*, this reference may fail to restore (as the item will be created anew with a different *ItemID*).
- If a list item cannot be deleted (for example, the *Welcome* page of the site), consider that restore process will restore all versions of the item sequentially without deletions, adding them to *Version History*.
- *Restored Issue* list items are assigned new *IssueID*.
- Restore of *Time Card* list is not supported.

Restore of List Items with Links (Attachments)

Consider the following when planning for the restore of list items with links (attachments):

- If the retention policy for target list/document library was configured to **Declare record** automatically, only the last version of the item will be restored to target list/library. Target retention policy settings will be applied to restored item (**Declare record**). However, links (attachments) will not be restored.
- Alternatively (with different retention policy settings), all versions of the original item will be restored to target list/library; item links (attachments) will be restored only if such item does not exist on target SharePoint.
- If *Declare this item as a record* action was originally applied to list item, such item will not be restored.

Restore of Items with Custom Content Type

For item restore, Veeam Explorer for Microsoft SharePoint uses content types that exist in the target library or list. If you restore an item with a custom content type, and the target location does not contain this content type, the restore process will fail with the following error: "*Cannot find corresponding Content-Type for: 15_.000. Original ContentTypeID: 'XXX'*".

Restore of Surveys

Consider the following limitations when planning for the restore of surveys, survey questions and responses:

- Survey items can be restored to a new survey, created automatically by Veeam Explorer for Microsoft SharePoint in the specified destination instead of the previously deleted survey. However, if a new survey is created by user from scratch (not replacing a deleted one) – items cannot be restored to such a survey.
- A survey can be restored to an existing target survey only if that target survey includes at least one item (question) same as survey questions stored in the content database.
- If a survey question was not answered completely in the source survey, after restore the response status in the target survey will be set to *Completed*, anyway.
- When restoring a single response to a survey, target response item with the same number will be deleted and restored item will be placed in the target survey after the last numbered response.

  For example, if the target survey has responses #1-15 and you try to restore a response that used to be #6 on source – then target response #6 will be deleted and restored response will be assigned #16.

Restore of Sites

Consider the following:

- When restoring site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.
- If you plan to restore SharePoint site pages, consider that Veeam Explorer for Microsoft SharePoint does not support restore of items which are not stored in the SharePoint content database (in particular, pages, page references and items based on default templates). Such items cannot be restored (neither by **Restore** nor by **Save** menu option), except for data from Wiki Content (text and images) which is stored in the database. Thus, site pages containing only text and images can be restored and displayed properly.

> **NOTE**
>
> Consider the following:
>
> - In case you attempt to restore such items, the following error message will be logged: "*Item <item> is skipped: restoration of items based on SharePoint default template is not supported*."
> - In case you attempt to save such items, the following error message will be logged: "*Unable to save document <item>. Document content is not available*."

Export and Import

Consider the following:

- In on-premises Microsoft SharePoint organizations, importing exported Picture Library may result in IDs changed for some items.
- Importing exported Project Tasks list does not preserve column order.
- Importing exported SharePoint list does not preserve Validation Settings.
- Export is unavailable for backups created by Veeam Backup for Microsoft 365. The operation is available only for backups created by Veeam Backup & Replication.
- Make sure to view information about unsupported Microsoft SharePoint lists before exporting them. In particular, hidden lists are not displayed in Veeam Explorer for Microsoft SharePoint after a site backup. Thus, such lists cannot be exported. For more information, see Unsupported SharePoint Lists.
- Export of empty SharePoint folders is not supported.

Data Type Limitations

Consider the column (field) data type when planning for the restore of your SharePoint libraries/lists:

- If source column (field) data type was set to *Lookup*, but the referenced list/library was deleted, such columns (fields) will not be restored even if you restore that referenced list. The reason is that if referenced list is deleted, the reference (link) to that list is no longer valid.
- If source column (field) data type was set to *Managed Metadata*, such columns (fields) will not be restored.

Workflow-Related Considerations

You may need to restore the items originally belonging to a list with no content approval required, to another list. If you try to restore such items to a list that requires content approval, item version and status will be modified in the following way:

- If a target list is configured to include major versions only, then all versions of restored item will become major (despite the original versioning); item status will be set to *Pending*.
- If a target list is configured to include both major and minor versions, then all versions of restored item will become minor (despite the original versioning); item status will be set in the following way:
  - If the last version (original) was major — status will be set to *Pending*.
  - If the last version was minor — status will be set to *Draft*.

Also, consider the following when planning for the restore of list items (with or without content approval originally required):

- If the retention policy for target list/document library is configured to **Declare record** automatically, only the last version of the item will be restored to target list/library. Target retention policy settings will be applied to restored item (**Declare record**). Besides, if **Require content approval for submitted items** was enabled for the original list, then after restore item status will be set to *Pending*.
- Alternatively (with different retention policy settings), all versions of the original item will be restored to target list/library. Besides, if **Require content approval for submitted items** was enabled for the original list, then after restore item status in the content approval workflow will be also restored, except for the states listed. For more information, see Status Restore Limitations.

Unsupported SharePoint Lists

The following table contains all unsupported Microsoft SharePoint lists. Veeam Explorer for Microsoft SharePoint does not restore data from these lists.

Due to Veeam Explorer for Microsoft SharePoint that is distributed as a part of Veeam Backup & Replication does not process hidden lists, such lists are also included in the following table.

List Template ID[1]	List Name	Microsoft SharePoint Server Version
101	SearchConfigListTemplate	2013/2016/2019/SE
110	datasrcs	2010/2013/2016/2019/SE
111	webtemp	2010/2013/2016/2019/SE
112	users	2010/2013/2016/2019/SE
113	wplib	2010/2013/2016/2019/SE
114	listtemp	2010/2013/2016/2019/SE
116	mplib	2010
117	nocodewf	2010/2013/2016/2019/SE
118	workflowProcess	2010/2013/2016/2019/SE
121	solutions	2010/2013/2016/2019/SE
122	nocodepublicwf	2010/2013/2016/2019/SE
123	themes	2010/2013/2016/2019/SE

List Template ID[1]	List Name	Microsoft SharePoint Server Version
124	designs	2013/2016/2019/SE
125	appdata	2013/2016/2019/SE
126	appfiles	2019/SE
160	accessrequests	2013/2016/2019/SE
175	MaintenanceLogs	2013/2016/2019/SE
200	meetings	2010/2013/2016/2019/SE
212	wkspglib	2010/2013/2016/2019/SE
331	ComponentManifests	2019/SE
334	ClientSideAssets	2019/SE
335	SiteCollectionAppCatalogs	2019/SE
336	WebApiPermissionRequests	2019/SE
401	fcgroups	2010/2013/2016/2019/SE
401	MonitoredAppsList	2013/2016/2019/SE
420	timecard	2013/2016/2019/SE
425	whatsnew	2010/2013/2016/2019/SE
530	ContentFollowingList	2013/2016/2019/SE
544	MicroBlogList	2013/2016/2019/SE
550	SocialDataStoreList	2013/2016/2019/SE
563	AnnouncementTilesList	2016/2019/SE

List Template ID[1]	List Name	Microsoft SharePoint Server Version
600	extlist	2010/2013/2016/2019/SE
880	members	2013/2016/2019/SE
925	abusereports	2013/2016/2019/SE
1221	healthreports	2010/2013/2016/2019/SE
1305	EDiscoverySources	2016/2019/SE
1306	EDiscoverySourceInstances	2013/2016/2019/SE
1309	DlpEDiscoveryQueries	2016/2019/SE
1310	PreservationListTemplate	2013/2016/2019/SE
2000	PNSubscribers	2013/2016/2019/SE
2001	ExternalSubscriptions	2013/2016/2019/SE
3100	AccSrvAddApp	2013/2016/2019/SE
3300	SharingLinks	2016/2019/SE
3400	HashtagStore	2019/SE
3401	BlockedHashtags	2019/SE
3412	HubSites	2019/SE
3415	WebTemplateExtensions	2019/SE
3500	IRCollection	2019/SE
3501	IRReference	2019/SE
3502	IRReferenceCollection	2019/SE

List Template ID[1]	List Name	Microsoft SharePoint Server Version
4501	wfsvc	2013/2016/2019/SE
10000	Academic Library	N/A
10001	eduentity"	2013/2016/2019/SE
10007	EduWorkItem	2013/2016/2019/SE
10008	EduQuiz	2013/2016/2019/SE
10051	eduentity	2013/2016/2019/SE
10060	eduusersetting	2013/2016/2019/SE
10061	eduexternalsyncsetting	2013/2016/2019/SE
10099	AcquisitionHistoryList	2013/2016/2019/SE
10101	edudocument	2013/2016/2019/SE
10102	IWConvertedForms	2010/2013/2016/2019/SE
10401	eduannouncement	2013/2016/2019/SE
10631	educalendar	2013/2016/2019/SE

[1]For more information, see this Microsoft article.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft SharePoint and load backups, you can use any of the following methods:

- The **Explore** option to load backups created by Veeam Backup for Microsoft 365. For more information, see the Data Restore section of the Veeam Backup for Microsoft 365 User Guide.

  When loading backups located in object storage, Veeam Explorer for Microsoft SharePoint will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To disable these notifications, clear the **Show pop-up notifications on startup** check box. For more information, see Advanced Settings.

- The **Restore application item** option to load backups created by Veeam Backup & Replication.

  For more information, see the Application Items Restore section of the Veeam Backup & Replication User Guide.

- Go to **Start**, click **Veeam Explorer for Microsoft SharePoint** and manually open Microsoft SharePoint databases. For more information, see Standalone Databases.

  When you open Veeam Explorer for Microsoft SharePoint from the **Start** menu, all backed-up databases will be loaded automatically.

If you open Veeam Explorer for Microsoft SharePoint from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

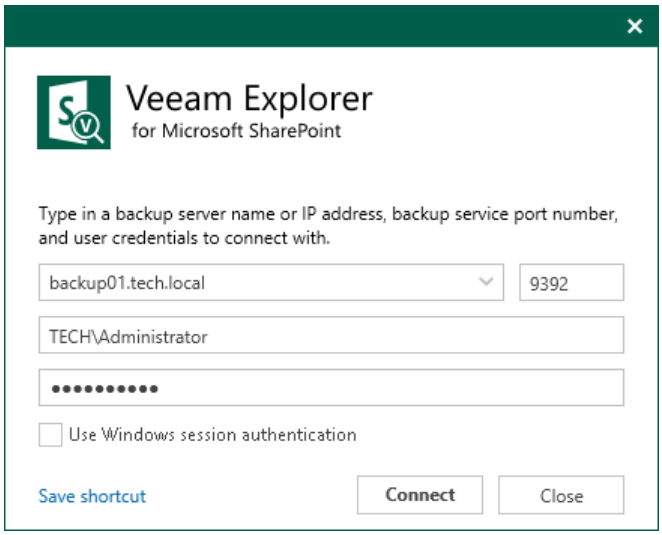
- The domain name or IP address of a server to which you want to connect.
- The port number.
- User account credentials.

  Consider the following:

  - To perform restore operations, Veeam Explorer for Microsoft SharePoint must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorer for Microsoft SharePoint is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft SharePoint is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Getting to Know User Interface

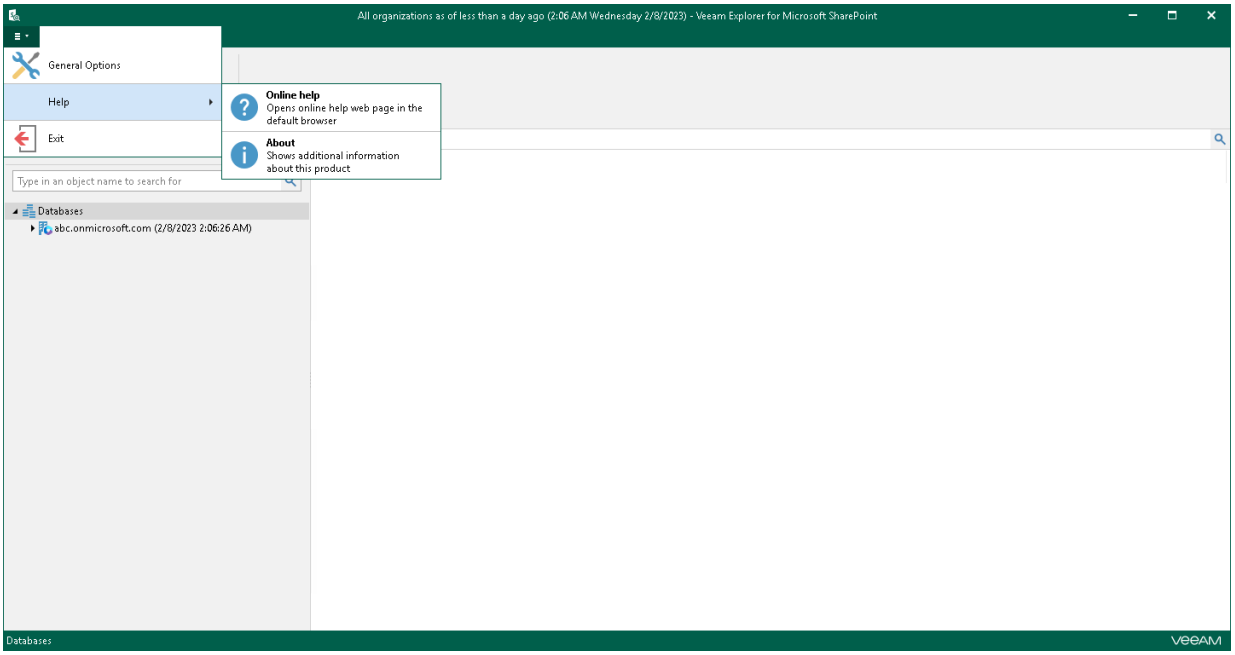
The user interface of Veeam Explorer for Microsoft SharePoint is designed to let you quickly find commands that you need to restore and export Microsoft SharePoint data from backups created by Veeam Backup for Microsoft 365 and Veeam Backup & Replication.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings. For more information, see General Application Settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft SharePoint window.

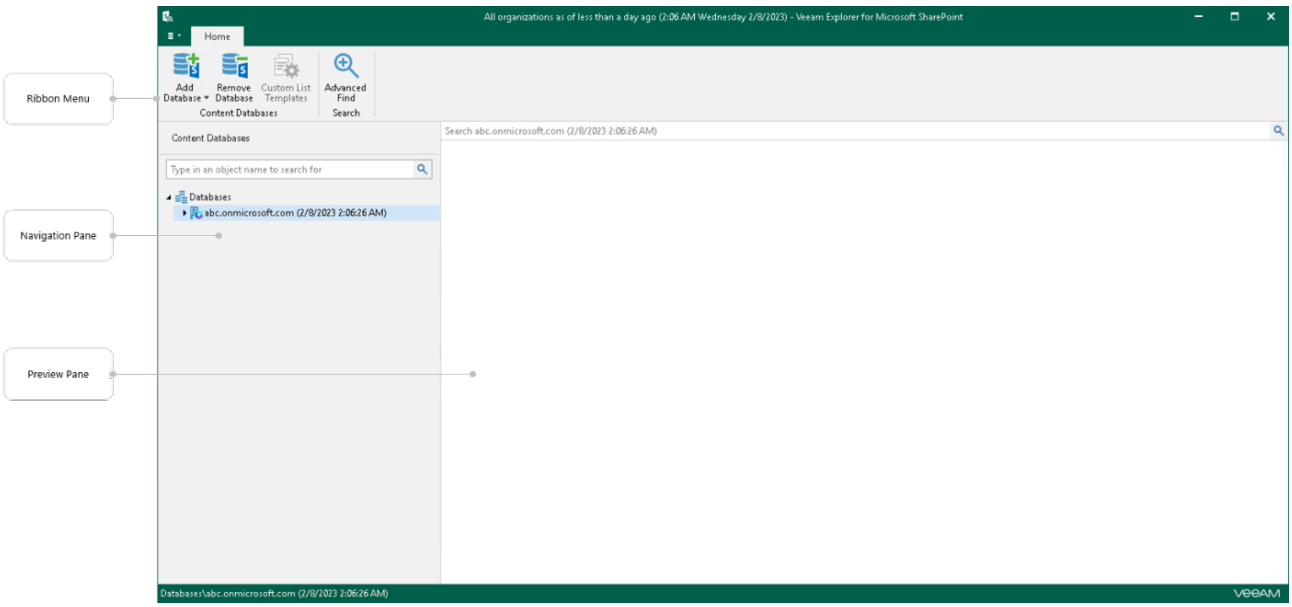
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft SharePoint wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.
- The navigation pane that allows you to browse through the hierarchy of folders with backed-up data. Also, it allows you to search for sites using keywords.
- The preview pane that provides search capabilities and allows you to view details about items that are contained in a folder you have selected in the navigation pane.



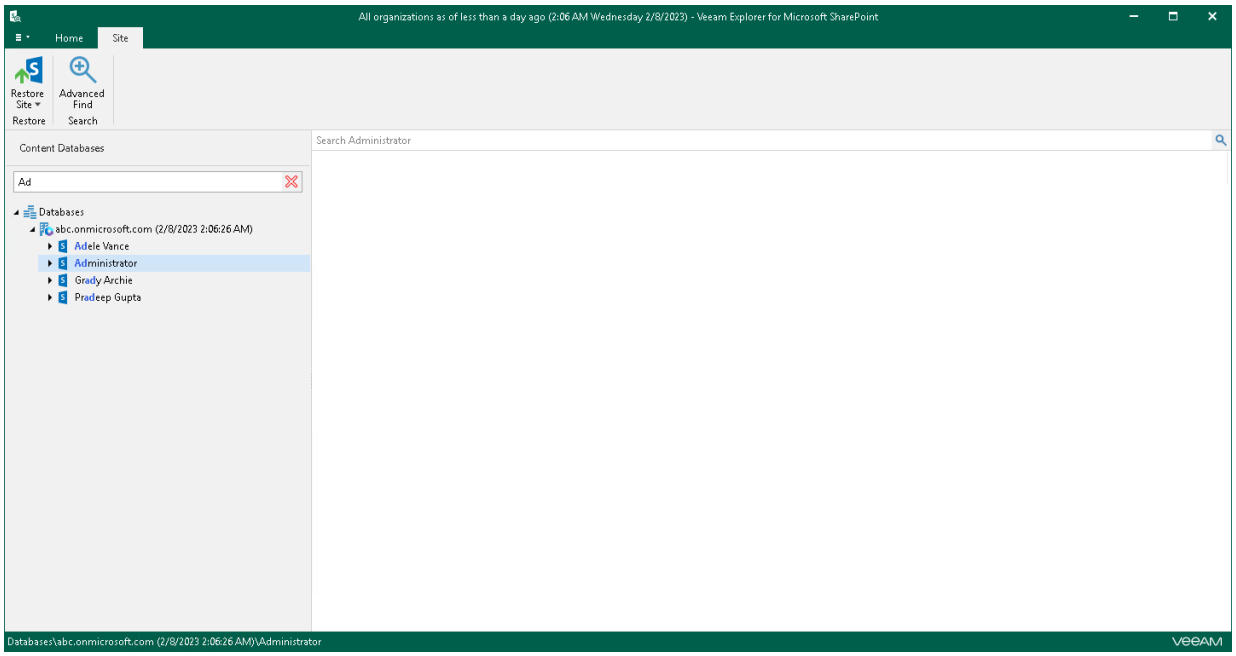
Browsing, Searching and Viewing Items

You can use Veeam Explorer for Microsoft SharePoint to view the contents of a backup file, view object properties, open files, search for sites and for items in a backup file as well as customize criteria of your search.

Searching for Sites

You can use keywords to search for sites in the database structure containing your SharePoint objects. To do this, enter a search query in the search field at the top of the navigation pane.

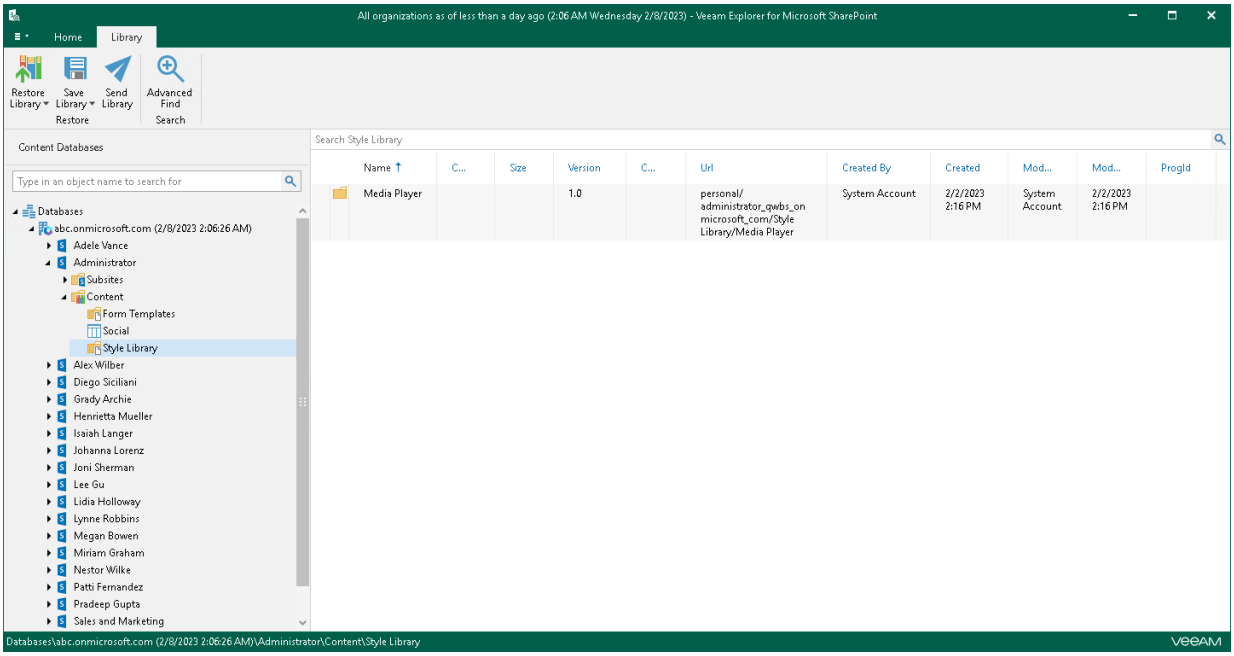
To remove a keyword, click the cross mark.



Browsing Backup Content

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your site items such as libraries and subsites.

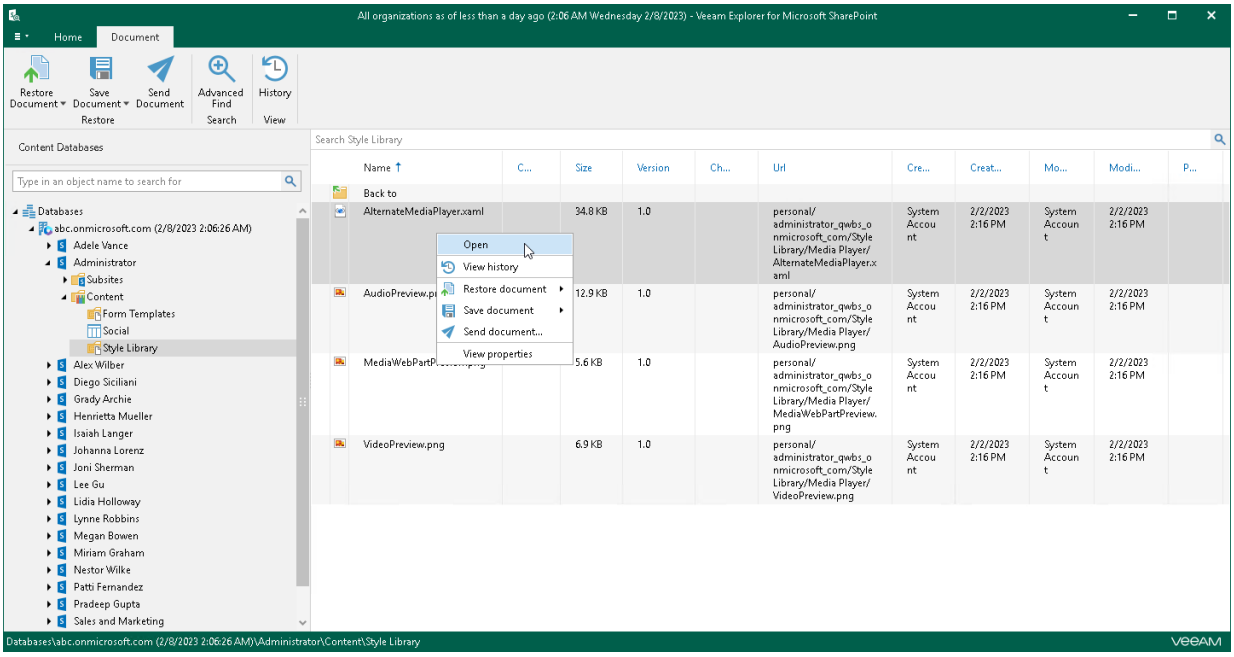
After you select an object in the navigation pane, you can see its content in the preview pane.



Viewing Objects Properties and Opening Files

To view object properties, right-click an object in the preview pane and select **View properties**.

To open a document using an associated application, right-click a document in the preview pane and select **Open**.



Searching for Objects in Backup File

The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

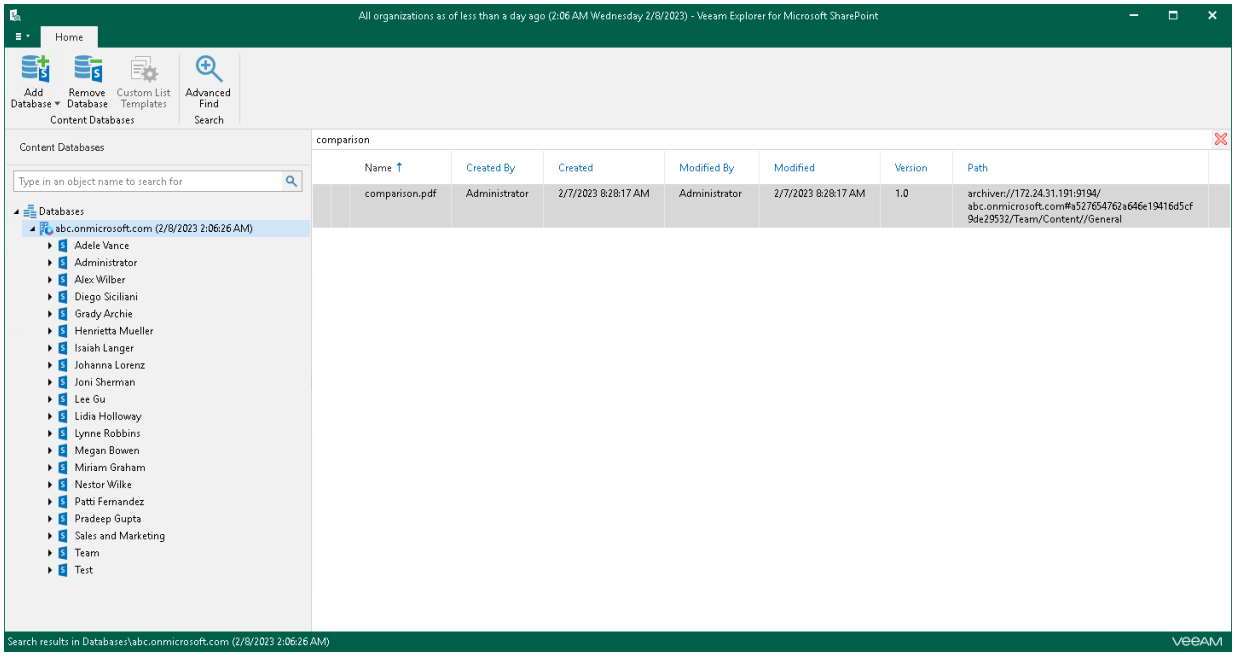
1. In the navigation pane, select an object in which you want to find data.
2. Enter a search query in the search field at the top of the preview pane.

> **NOTE**
>
> To find the exact phrase, use double quotes. For example, "*media player*".

You can narrow your search results by specifying various search criteria using the *criteria:value* format.

For example, you can use *status:pending approval* to find all items that require approval in the list of decisions.

You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*. The search criteria are similar to those used for searching in Microsoft SharePoint. For more information, see this Microsoft article.



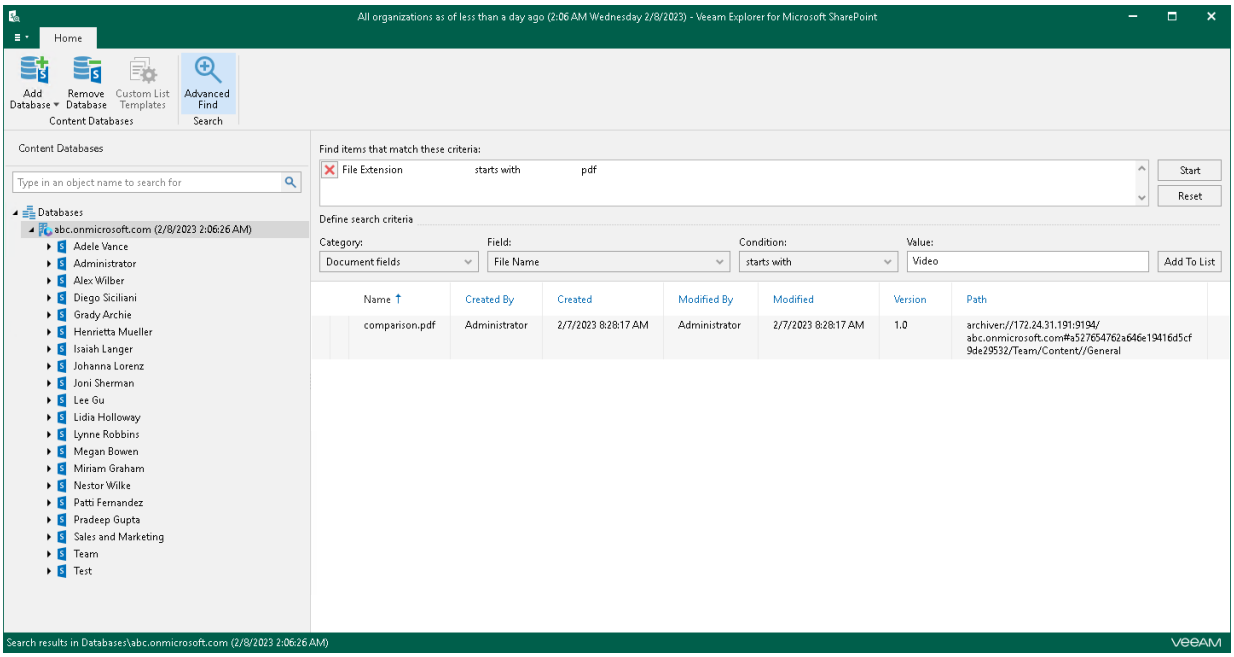
Using Advanced Find

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find an object that starts with the word *Media*, do the following:

1. In the preview pane, select a node and click **Advanced Find** on the ribbon.
2. In the **Define search criteria** section, select **Category** > **Document fields**.
3. In the **Field** list, select **File Name**.
4. In the **Condition** list, select **starts with**.
5. In the **Value** field, specify a file name.
6. Click **Add to List** and then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



General Application Settings

You can configure general settings for Veeam Explorer for Microsoft SharePoint.

Staging SQL Server

To perform Microsoft SharePoint items restore, Veeam Explorer for Microsoft SharePoint requires a Microsoft SQL server to be used as a staging system.

> **NOTE**
>
> Configuring the staging SQL server settings is only required to restore SharePoint data from the following sources:
>
> - Backups created by Veeam Backup & Replication.
> - Microsoft SharePoint databases manually added to the application scope. For more information, see Adding Microsoft SharePoint Databases.

Consider the following when configuring a staging SQL server:

- If an SQL server belongs to an untrusted domain, connection will not be possible.
- If an SQL server belongs to a trusted domain, only the *SQL Server authentication* method is available.
- If both an SQL server and the machine running Veeam Explorer for Microsoft SharePoint belong to the same domain, then both *Windows* and *SQL Server authentication* methods are possible.

  To use *Windows authentication*, make sure to configure the following delegation settings:

  a. In **Active Directory Users and Computers**, select the necessary staging SQL server.

  b. Open the server properties and select the **Delegation** tab. Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol** options for the **cifs** service on a computer with Veeam Explorer for Microsoft SharePoint.

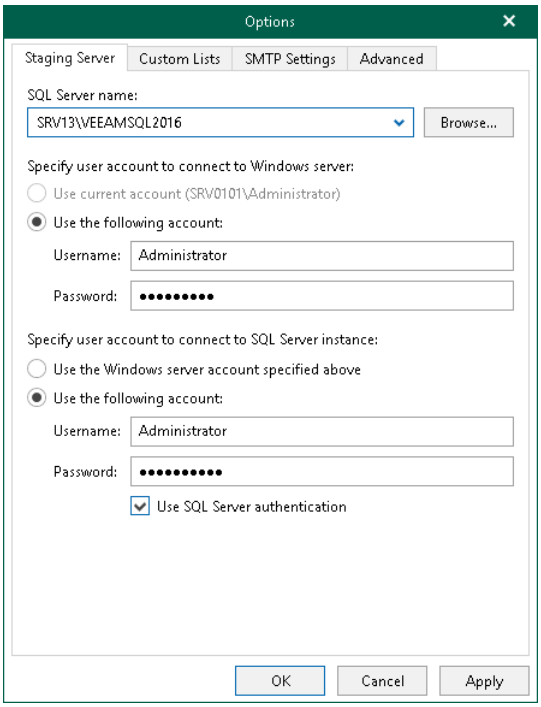
  c. Restart the staging SQL Server.

  d. Select a user account to connect to the staging SQL server. Also, select its properties on the **Account** tab and make sure the **Account is sensitive and cannot be delegated** check box is cleared.

To configure a staging server, do the following:

1. In the main menu, click **General Options**.
2. Open the **Staging Server** tab.
3. Click **Browse** to specify an SQL server that you want to use as a staging system. Do one of the following:
   - On the **Local Servers** tab, select a local SQL server that is located on a machine with Veeam Explorer for Microsoft SharePoint.
   - On the **Network Server** tab, select an SQL server over the network.
4. Specify the account to access the selected SQL server.
5. Specify the account to access a SQL server instance.

6. Click **OK**.


Options
Staging Server
Custom Lists
SMTP Settings
Advanced
SQL Server name:
SRV13\VEEAMSQL2016
Browse...
Specify user account to connect to Windows server:
Use current account (SRV0101\Administrator)
Use the following account:
Username:
Administrator
Password:
Specify user account to connect to SQL Server instance:
Use the Windows server account specified above
Use the following account:
Username:
Administrator
Password:
Use SQL Server authentication
OK
Cancel
Apply

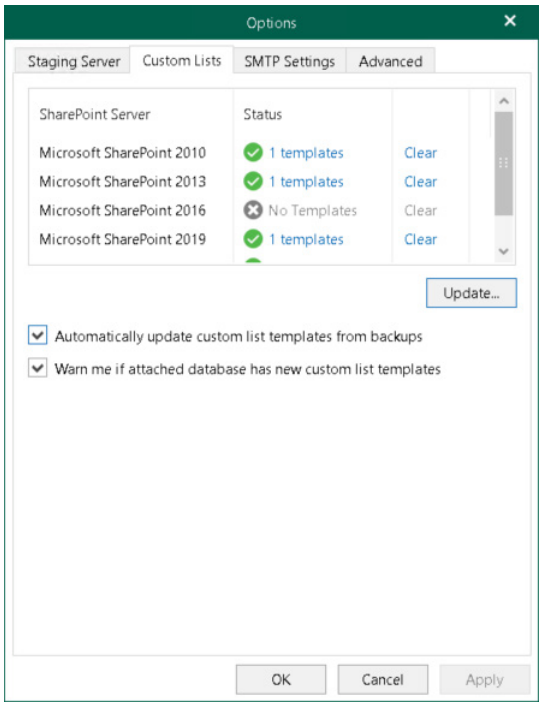
Custom Lists

Veeam Explorer for Microsoft SharePoint supports obtaining custom list templates from backups created by Veeam Backup & Replication. The actual information about templates is stored directly in a backup file and obtained automatically so that you can view the custom list data without having to perform any additional operations.

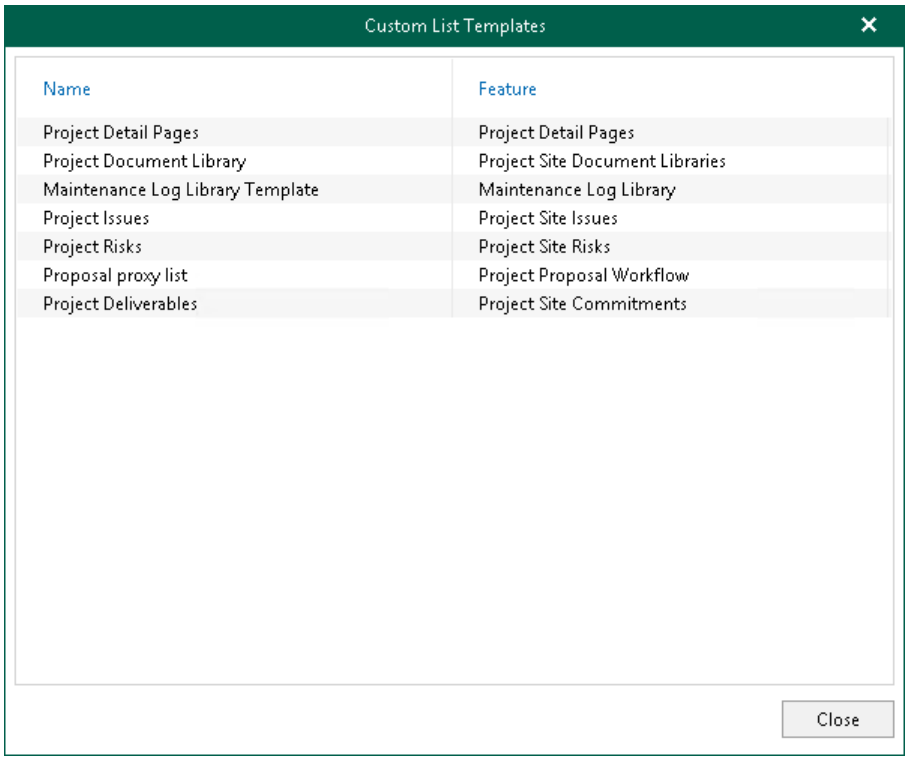
> **NOTE**
>
> Configuring custom lists is not required when working with backups created by Veeam Backup for Microsoft 365.

To see templates with their names and features, do the following:

1. In the main menu, click **General Options**.
2. Open the **Custom Lists** tab.
3. Click the link under the **Status** column which also comprises the total number of available templates.
4. If you want to automatically update existing templates, select the **Automatically update custom list templates from backups** check box.
5. If you want to be notified whether the database contains new templates other than those you already have, select the **Warn me if attached database has new custom list templates** check box.
6. Click **OK**.



See the next figure showing you what custom list templates are available.

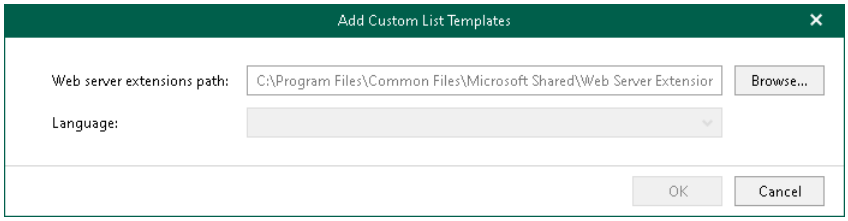


To remove templates, click **Clear**.

Importing Templates Manually

To import existing templates from the Microsoft SharePoint server manually, do the following:

1. In the main menu, click **General Options**.
2. Open the **Custom Lists** tab.
3. Click **Update**.
4. Specify the path to Microsoft SharePoint templates, select the language and click **OK**. The language set in the drop-down list depends on the installed language packages on a SharePoint server.

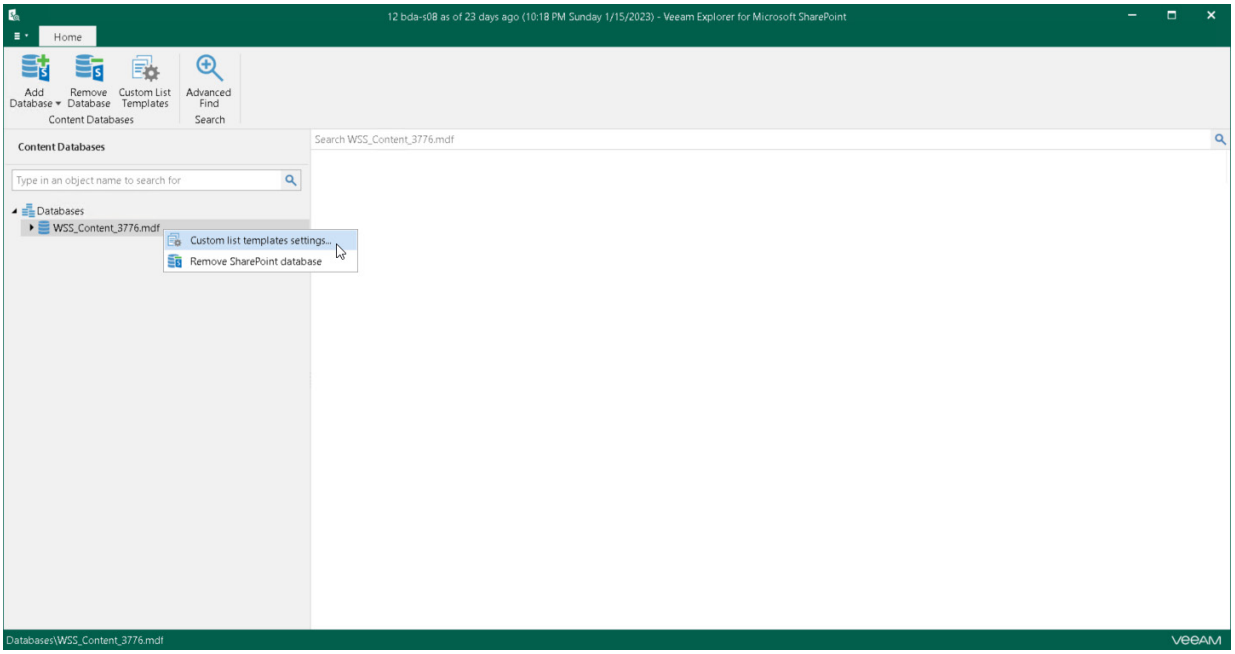


Importing Templates Using Ribbon Menu

> **NOTE**
>
> Available only for Microsoft SQL Server databases and requires a staging SQL server. For more information on configuring a staging server, see Staging SQL Server.

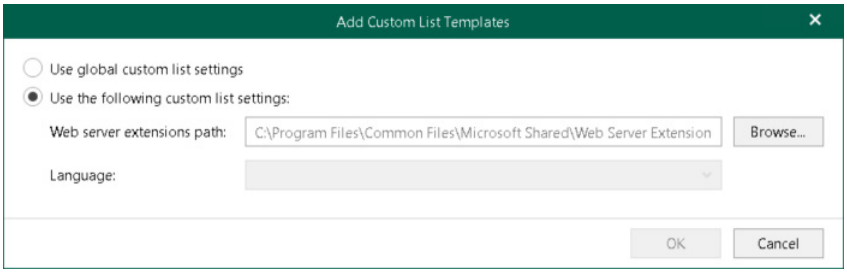
To import existing templates from the Microsoft SharePoint server using the ribbon menu, do the following:

1. In the navigation pane, select a SQL database.
2. Do one of the following:
   - Click **Custom List Templates** on the ribbon.
   - Right-click a SQL database and select **Custom list templates settings**.



3. Select how you want your templates to be applied:
   - Select **Use global custom list settings** to apply global list templates to the select database.
   - Select **Use the following custom list settings** to apply the templates to the selected database only.

     When using the latter option, specify the path to the Microsoft SharePoint templates, select the language and click **OK**. The language set in the drop-down list depends on the installed language packages on a SharePoint server.



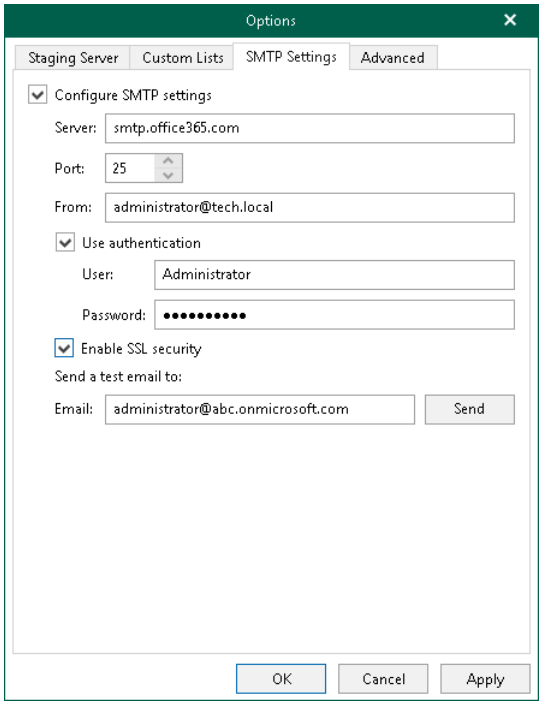
SMTP Settings

To send Microsoft SharePoint items as attachments, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
   a. In the **Server** field, specify a DNS name or IP address of the SMTP server.
   b. In the **Port** field, specify a port number of the specified SMTP server.

      The default port number is *25*. If you want to use SSL data encryption, specify port *587*.
   c. In the **From** field, specify the sender email address. This address will appear in the **From** field when sending SharePoint items.
   d. If the specified SMTP server requires an authentication for outgoing mail, select the **Use authentication** check box and provide valid credentials.
   e. Select the **Enable SSL security** check box to enable SSL data encryption.
4. Click **Send** to send a test email message.
5. Click **OK**.



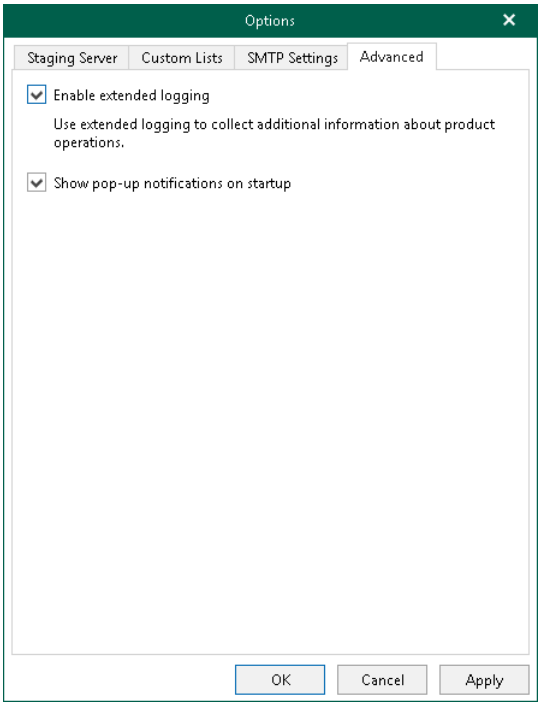
Advanced Settings

Veeam Explorer for Microsoft SharePoint allows you to configure advanced settings such as extended logging mode and pop-up notifications.

To configure advanced settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Advanced** tab.
3. If you want to enable extended logging mode to collect logs that contain additional information on specific operations, select the **Enable extended logging** check box.

   After enabling extended logging mode, you can go back to the application and perform actions for which you want to collect additional information. Then you can collect logs.
4. By default, Veeam Explorer for Microsoft SharePoint displays notifications when loading backups created by Veeam Backup for Microsoft 365 from object storage. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.
5. Click **OK**.



Standalone Databases

You can add standalone databases to the Veeam Explorer for Microsoft SharePoint scope and connect to a Veeam Backup for Microsoft 365 server and service provider server to view backups located on these servers.

Adding Microsoft SharePoint Databases

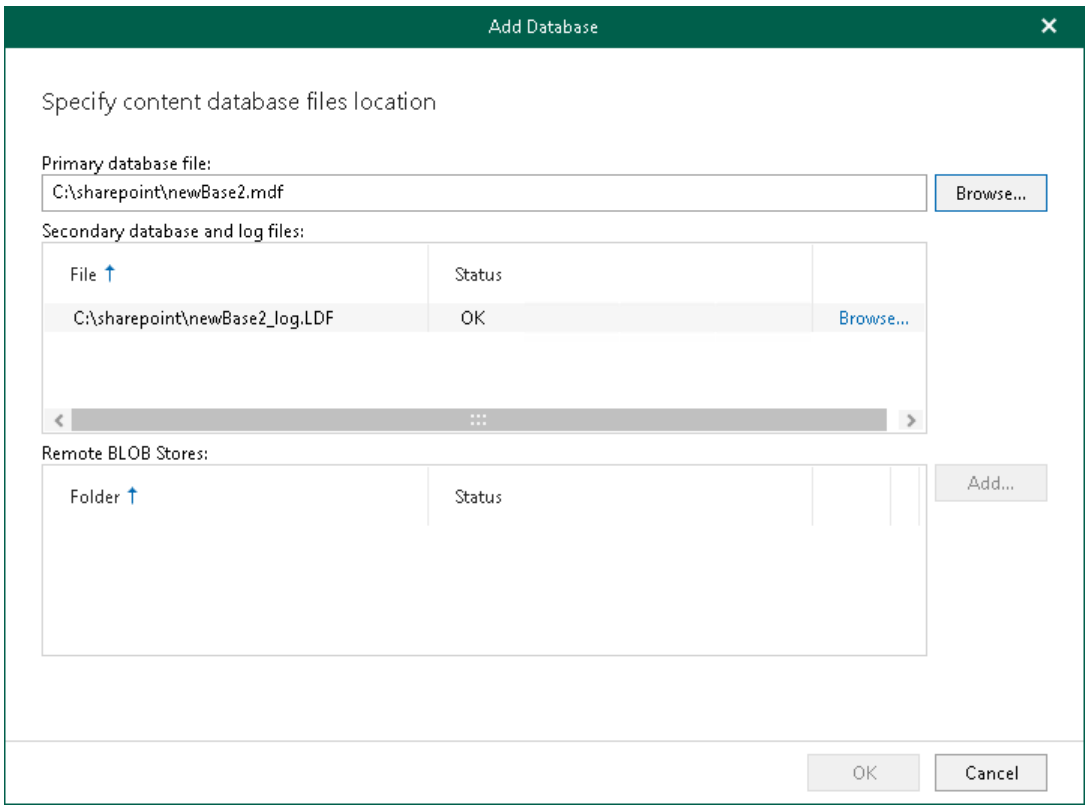
You can add Microsoft SharePoint databases to the application scope manually. For example, you may want to do this to restore items from a Microsoft SharePoint database exported earlier using Veeam Explorer for Microsoft SQL Server. For more information, see Export as MDF.

When you add standalone Microsoft SharePoint databases to the application scope, Veeam Explorer for Microsoft SharePoint attaches such a database to the staging SQL server, creating a temporary Microsoft SharePoint content database from which you can restore your items.

To manually add new Microsoft SharePoint databases to the application scope, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Database** > **Microsoft SharePoint database** on the ribbon.
   - Right-click the **Databases** node and select **Add database**.
2. Specify the location of the Microsoft SharePoint primary content database file (`.mdf`). The secondary database and the transaction log file (`.ldf`) will be added as well. Keep in mind that shared folders and mapped network drives are not supported as a location for Microsoft SharePoint content database files.

   To add remote BLOB stores, click **Add** next to the **Remote BLOB Stores** section.
3. Click **OK**.



Adding Veeam Backup for Microsoft 365 Databases

To manually add databases that store Microsoft 365 organization data, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Database** > **Veeam Backup for Microsoft 365 database** on the ribbon.
   - Right-click the **Databases** node and select **Veeam Backup for Microsoft 365 database**.
2. Specify the database file location and log directory.
3. Click **Open**.

> **NOTE**
>
> Make sure you have disabled the *Veeam Backup Proxy for Microsoft 365 Service* when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will not be able to access the database due to database lock.

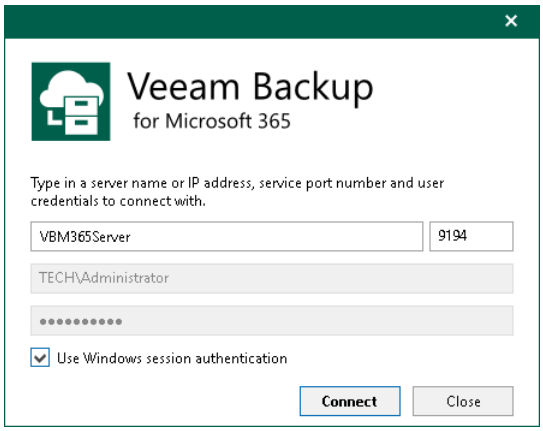
Adding Veeam Backup for Microsoft 365 Server

You can use the built-in Veeam Explorer for Microsoft SharePoint abilities to connect to another Veeam Backup for Microsoft 365 server and add its databases to the Veeam Explorer for Microsoft SharePoint scope.

To connect to another Veeam Backup for Microsoft 365 server remotely, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Database** > **Veeam Backup for Microsoft 365 server** on the ribbon.
   - Right-click the **Databases** node and select **Veeam Backup for Microsoft 365 server**.
2. Specify a server name or IP address and enter credentials to access the specified server.

   Select the **Use Windows session authentication** check box to connect with the user account under which you are currently logged in.
3. Click **Connect**.



Adding Veeam Backup for Microsoft 365 Service Provider

In Veeam Explorer for Microsoft SharePoint, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.

> **NOTE**
>
> Make sure that both Veeam Explorer for Microsoft SharePoint and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication. For more information, see the Connecting to Service Providers section of the Veeam Cloud Connect Guide.

To add Veeam Backup for Microsoft 365 service providers, do the following:

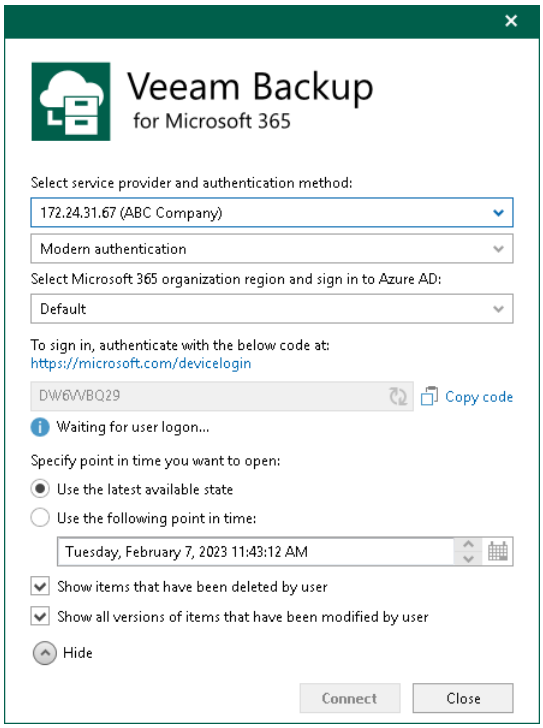
1. Do one of the following:
   - On the **Home** tab, click **Add Database** > **Veeam Backup for Microsoft 365 service provider** on the ribbon.
   - Right-click the **Databases** node and select **Veeam Backup for Microsoft 365 service provider**.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and select an authentication method that can be either *Modern authentication* or *Basic authentication*.
3. [For *Modern authentication*] Select a region to which a Microsoft 365 organization of the selected service provider belongs.
4. [For *Modern authentication*] Copy the device code and use it to sign in to Azure Active Directory.

   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.

   > **NOTE**
   >
   > You cannot use *Basic authentication* to load backups if a Microsoft 365 organization has been added to the service provider infrastructure using *Modern authentication*.
5. Select a point-in-time state as of which you want to load Microsoft 365 backups.

   To select a point in time, use the calendar control.
6. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
7. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.

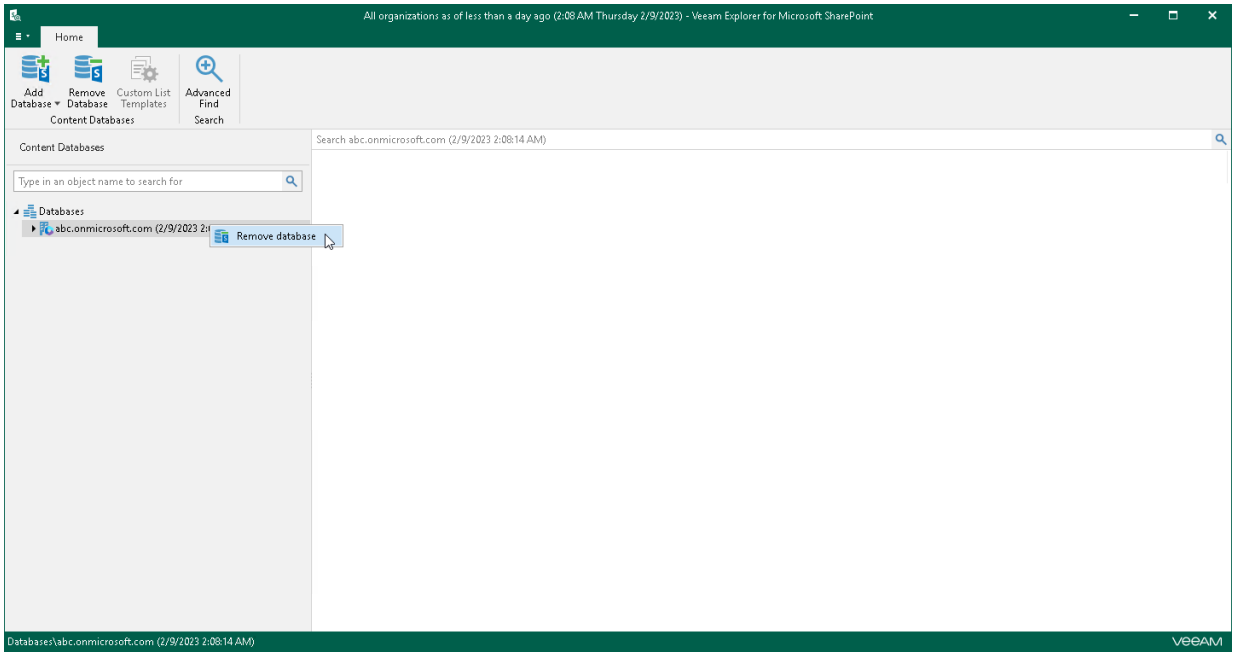
8. Click **Connect**.



Removing Databases

Veeam Explorer for Microsoft SharePoint allows you to remove Microsoft SharePoint databases from the application scope when you no longer need it.

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove database**.



Data Restore

You can use Veeam Explorer for Microsoft SharePoint to restore backed-up Microsoft SharePoint data to the original location or other Microsoft 365 organizations and on-premises Microsoft organizations.

Before restoring data, read the Considerations and Limitations section.

Restoring Sites

Veeam Explorer for Microsoft SharePoint allows you to restore Microsoft SharePoint sites to the original location or other Microsoft 365 organizations and on-premises Microsoft organizations.

Restoring Sites to Original Location

To restore Microsoft SharePoint sites to the original location, do the following:

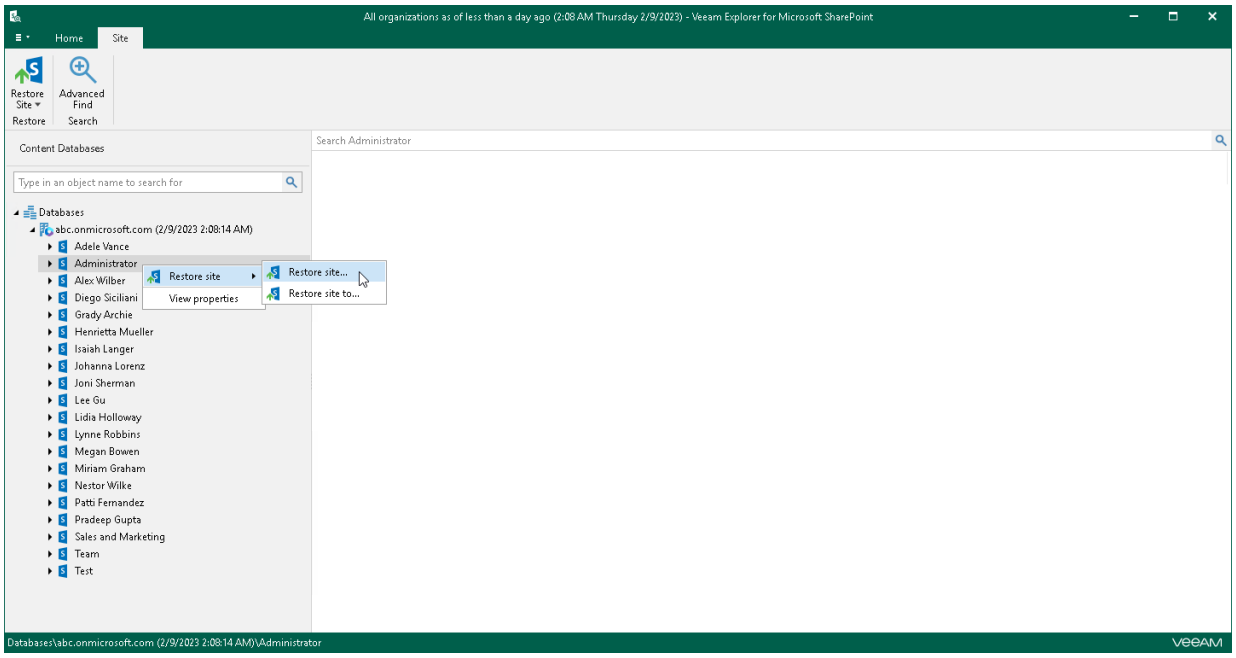
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify a target site alias.
5. Specify restore options.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a site that you want to restore.
2. Do one of the following:
   - On the **Site** tab, click **Restore Site** > **Restore site to <site_name>** on the ribbon.
   - Right-click a site and select **Restore site** > **Restore site**.

> **NOTE**
>
> When restoring sites to site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server, and specify authentication settings.

Modern Authentication

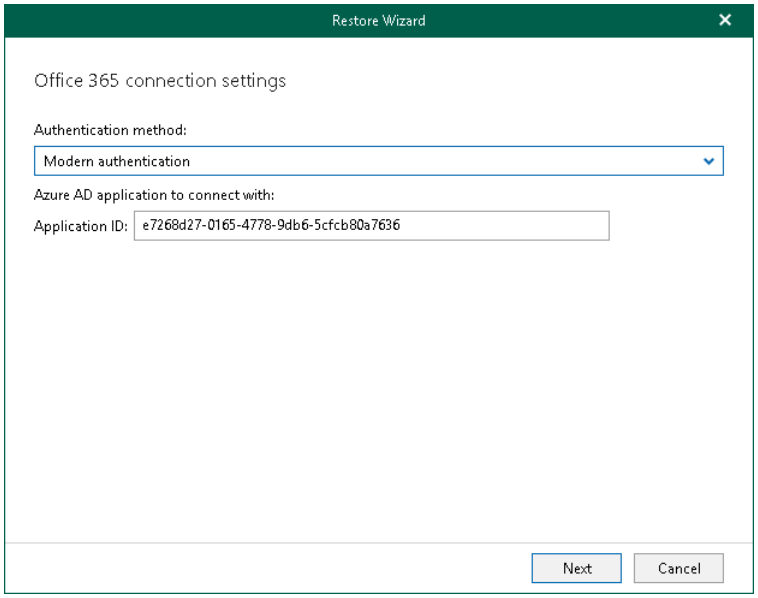
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

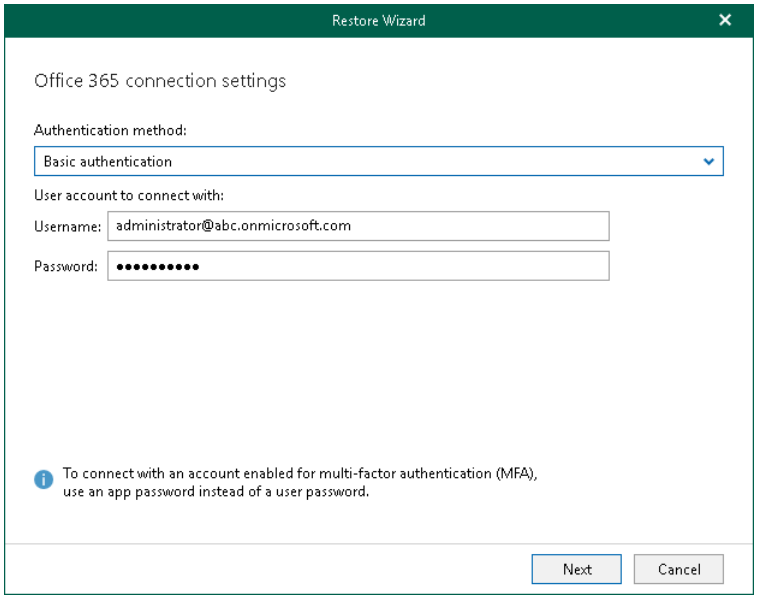
   By default, Veeam Explorer for Microsoft SharePoint populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

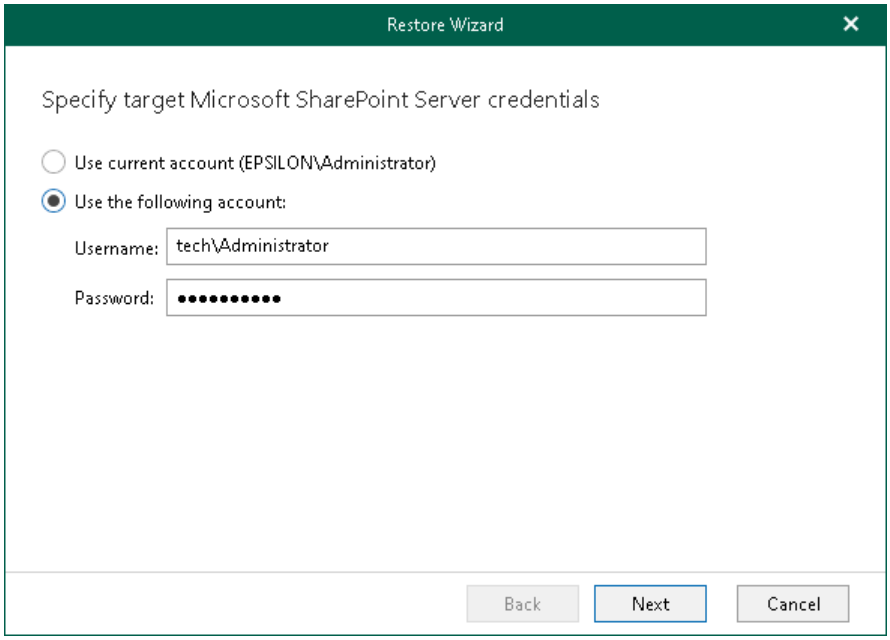
To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, use an account that you are currently logged in to or provide a user name and password.

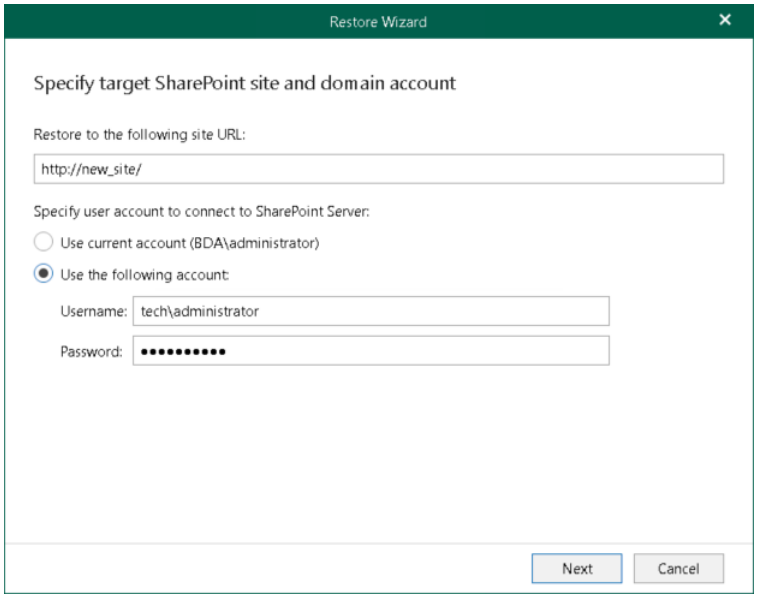


Restoring from Microsoft SQL Database

When restoring from a Microsoft SQL database, provide the following:

- The site URL to which you want to restore your site.
- Authentication credentials.

> **NOTE**
>
> When restoring Microsoft SharePoint sites from a Microsoft SQL database, you will proceed directly to the Specify Restore Options step of the wizard.



Step 3. Log In to Microsoft 365

This step is only available for data restore from backups created by Veeam Backup for Microsoft 365 and if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

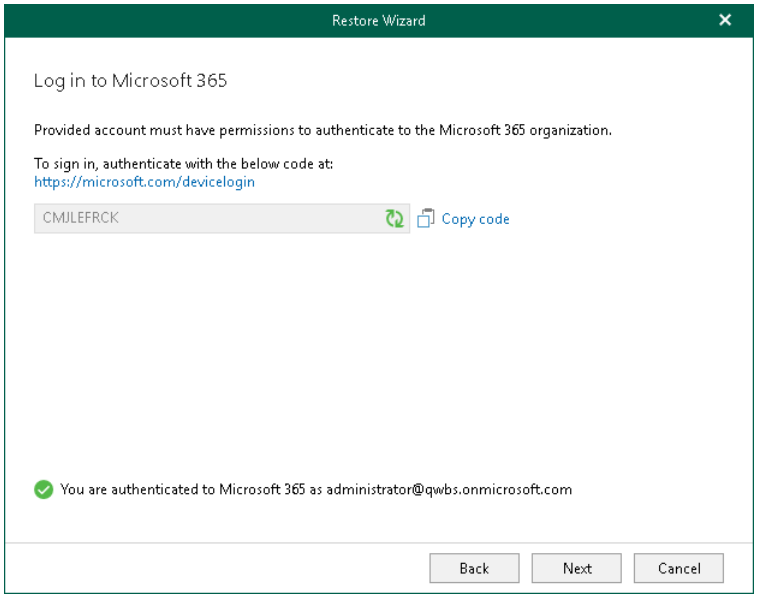
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.

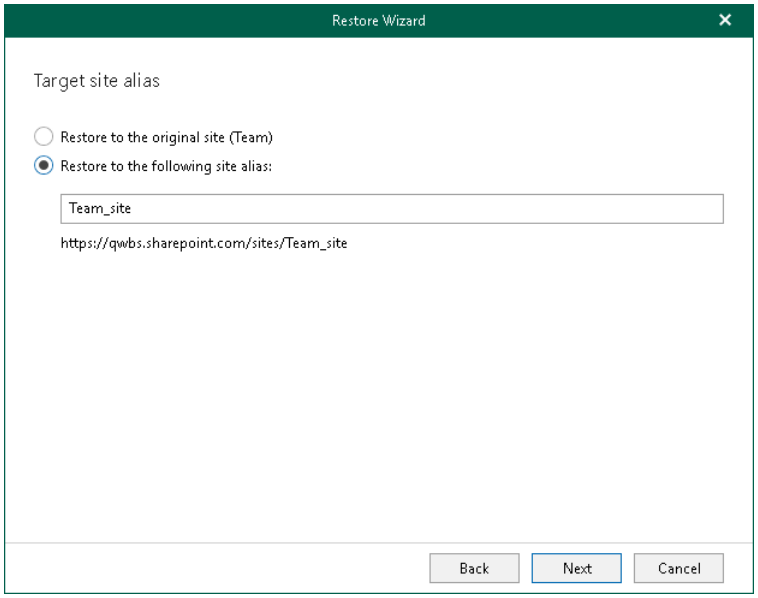


Step 4. Specify Target Site Alias

This step is only available if you restore subsites or site collections from backups created by Veeam Backup for Microsoft 365 with the *Group#0* or *SITEPAGEPUBLISHING#0* template. These are subsites, team sites with modern authentication or communication sites with modern authentication. For sites with different template, such as personal sites or other sites, this step is unavailable. You proceed to the Specify Restore Options step.

At this step of the wizard, specify a target site alias that you want to use for data restore.

> **NOTE**
>
> When restoring site collections other than site collections with the *Group#0* or *SITEPAGEPUBLISHING#0* template, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



Step 5. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

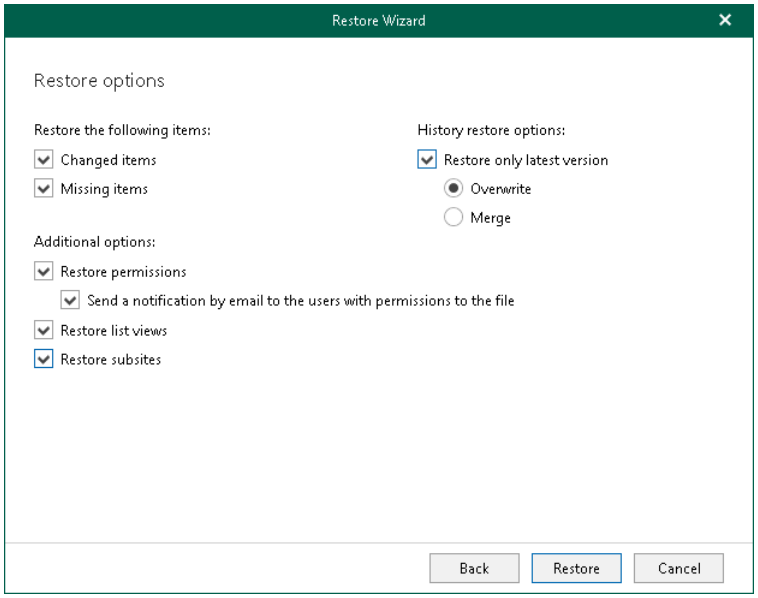
- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items. If this check box is selected, you can select one of the following options:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore permissions**. Allows you to restore permissions. If not selected, the permissions for the restored document library or list will be set in the following way:
  - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
  - If the library (or list) already exists on target, permissions will be preserved.
- **Send a notification by email to the users with permissions to the file**. Select this check box if you want to notify users about items restore. Veeam Explorer for Microsoft SharePoint will notify users with whom items have been shared. You can select this check box only if the **Restore permissions** check box is selected.

  > NOTE
  >
  > The **Send a notification by email to the users with permissions to the file** check box is only available when restoring data from backups created by Veeam Backup for Microsoft 365 for Microsoft 365 organizations.

- **Restore list views.** Allows you to restore your list views.

- **Restore subsites.** Allows you to restore your subsites.



Restoring Sites to Another Location

You can restore Microsoft SharePoint sites to other Microsoft 365 organizations and on-premises Microsoft organizations.

Restore to Microsoft 365 Organizations

You can restore backed-up data to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

To restore Microsoft SharePoint sites to another Microsoft 365 organization, do the following:

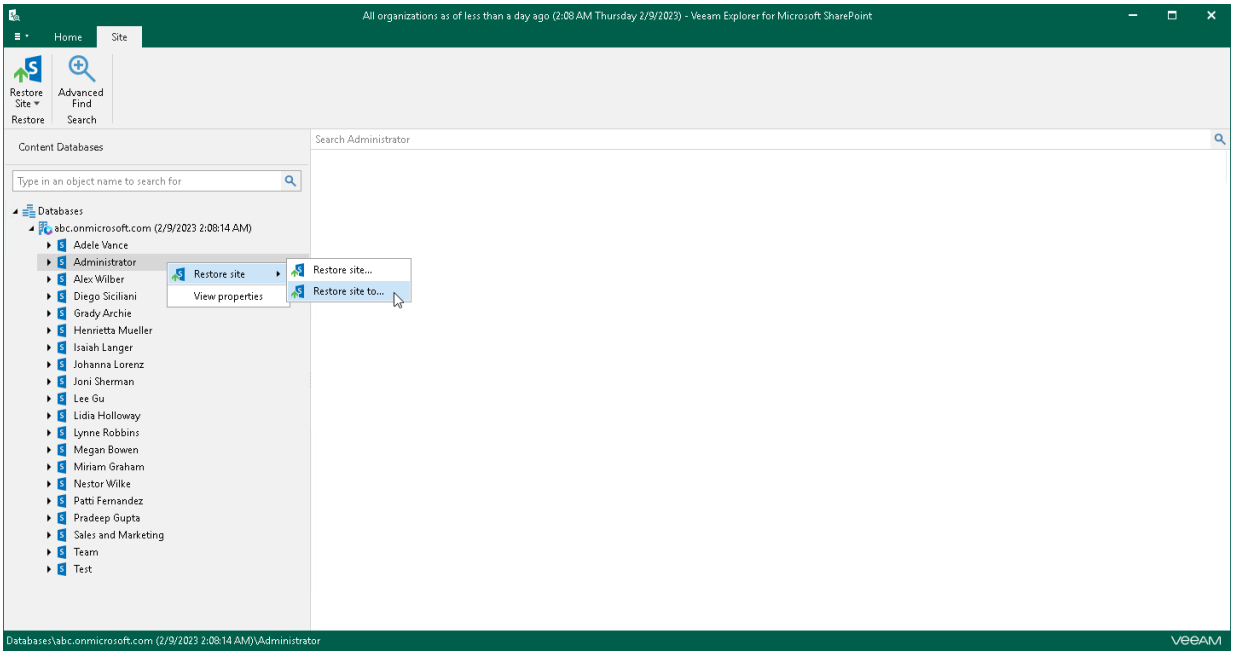
1. Launch the Restore wizard.
2. Select a target site location.
3. Select an authentication method.
4. Log in to Microsoft 365.
5. Specify a target site web address.
6. Specify restore options.

Step 1. Launch Restore Wizard

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

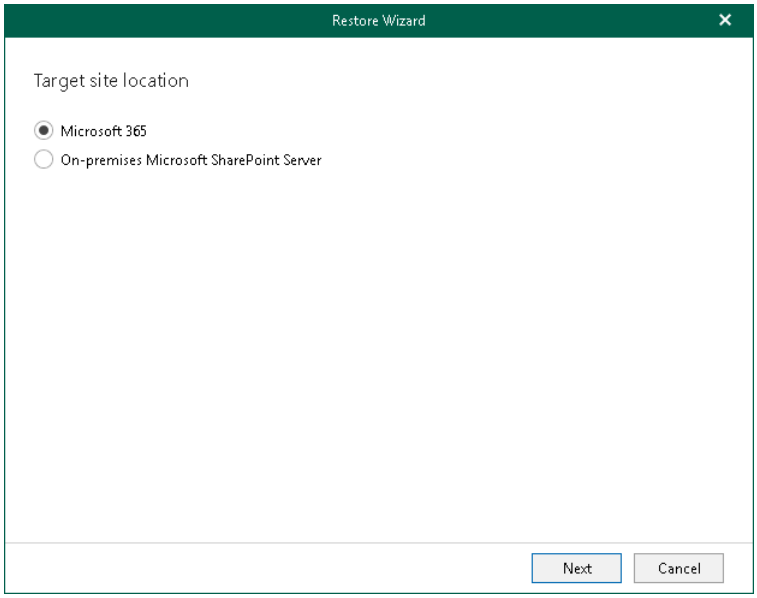
1. In the navigation pane, select a site that you want to restore.
2. Do one of the following:
   - On the **Site** tab, click **Restore Site** > **Restore site to** on the ribbon.
   - Right-click a site and select **Restore site** > **Restore site to**.

> **NOTE**
>
> When restoring sites to site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



Step 2. Select Target Site Location

At this step of the wizard, select **Microsoft 365** to restore the SharePoint site to a SharePoint Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.



Step 3. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

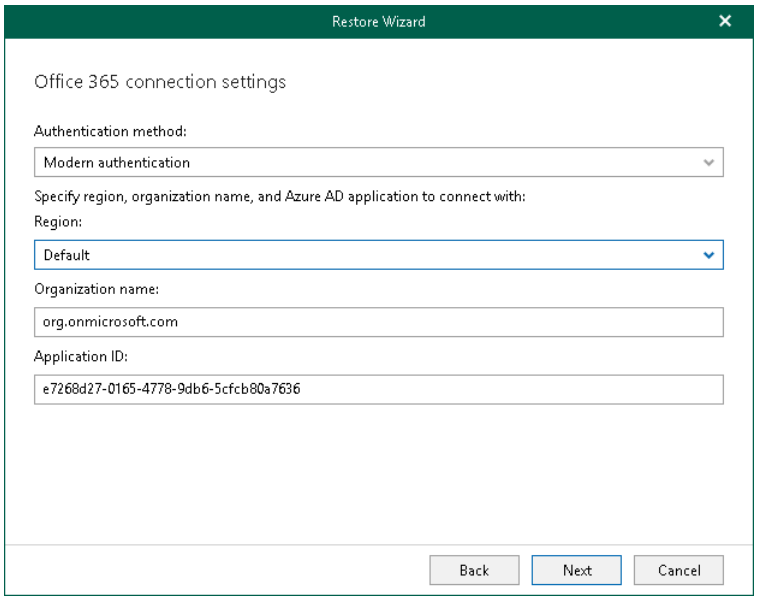
   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.

3. In the **Organization name** field, enter a name of your target SharePoint Online organization.

4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

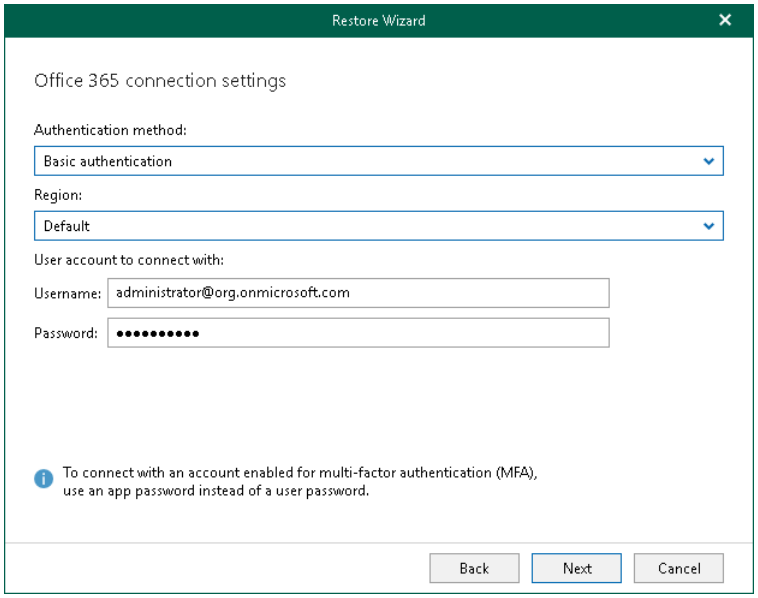
   By default, Veeam Explorer for Microsoft SharePoint populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.
3. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 4. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

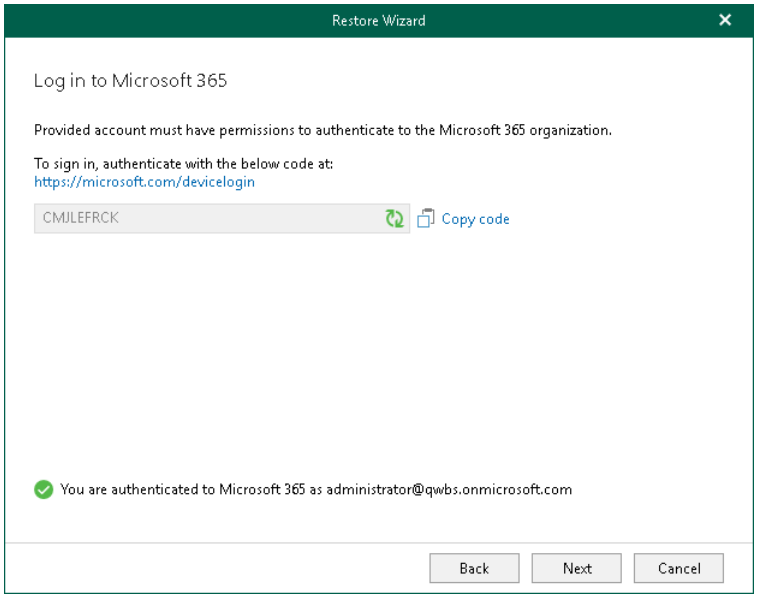
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

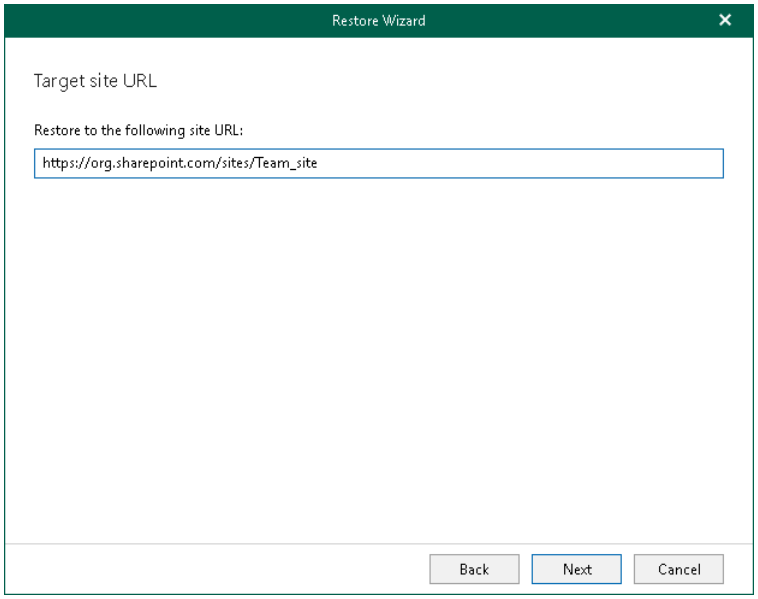
4. Return to the **Restore Wizard** window and click **Next**.



Step 5. Specify Target Site Web Address

At this step of the wizard, specify web address of a target SharePoint site.

> **NOTE**
>
> When restoring site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



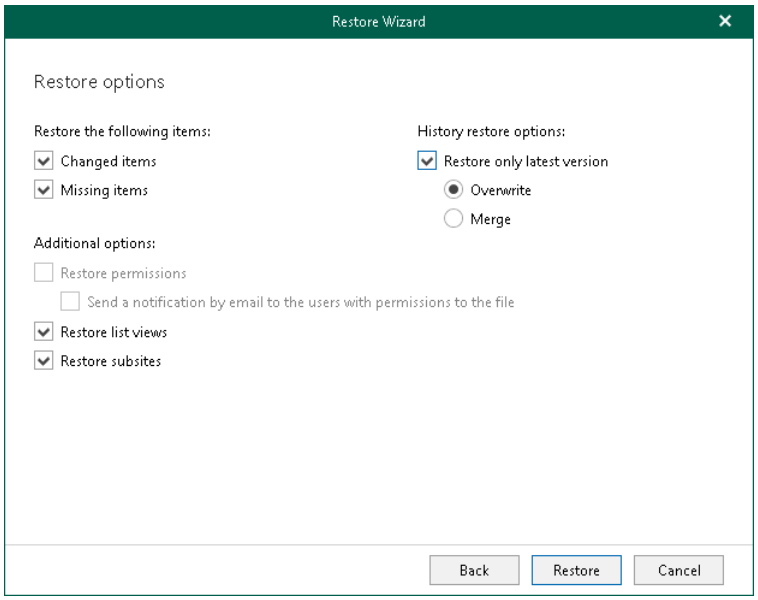
Step 6. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore list views.** Allows you to restore your list views.
- **Restore subsites.** Allows you to restore your subsites.



Restore to On-Premises Microsoft Servers

You can restore backed-up data to on-premises Microsoft SharePoint servers. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.

To restore Microsoft SharePoint sites to an on-premises Microsoft SharePoint server, do the following:

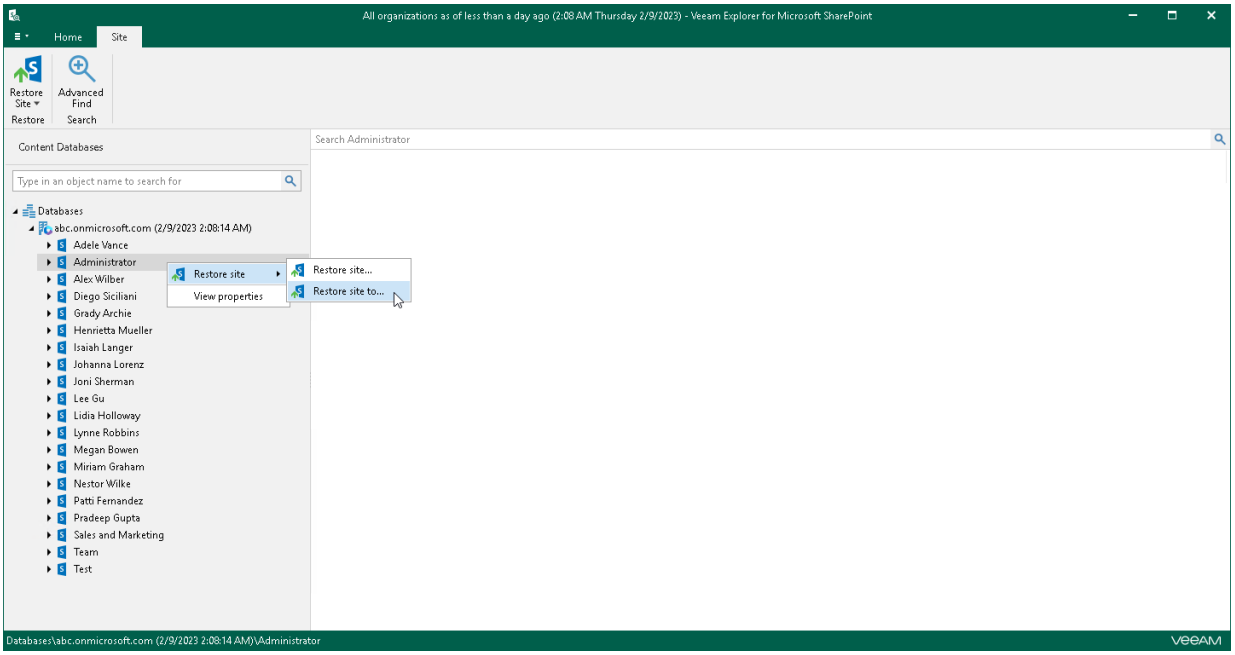
1. Launch the Restore wizard.
2. Select a target site location.
3. Specify a target site web address and credentials.
4. Specify restore options.

Step 1. Launch Restore Wizard

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

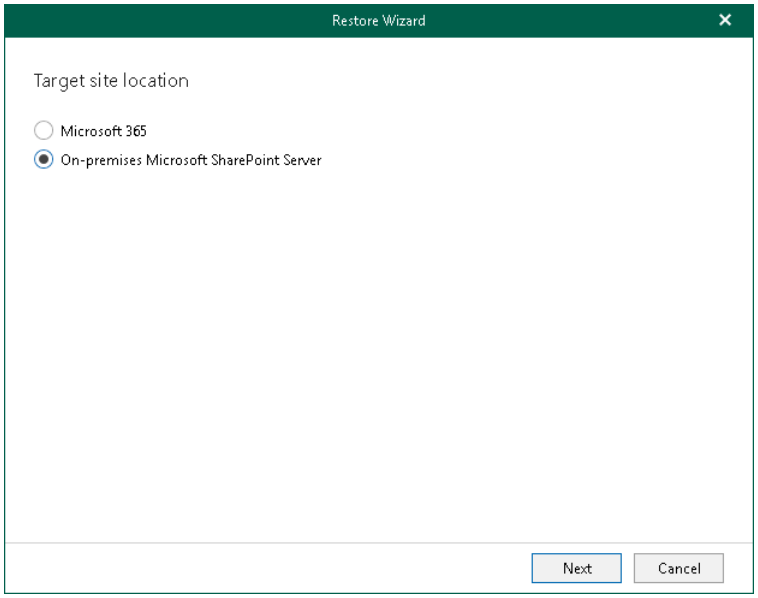
1. In the navigation pane, select a site that you want to restore.
2. Do one of the following:
   - On the **Site** tab, click **Restore Site** > **Restore site to** on the ribbon.
   - Right-click a site and select **Restore site** > **Restore site to**.

> **NOTE**
>
> When restoring sites to site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



Step 2. Select Target Site Location

At this step of the wizard, select **On-premises Microsoft SharePoint Server** to restore the SharePoint site to an on-premises Microsoft SharePoint organization. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.



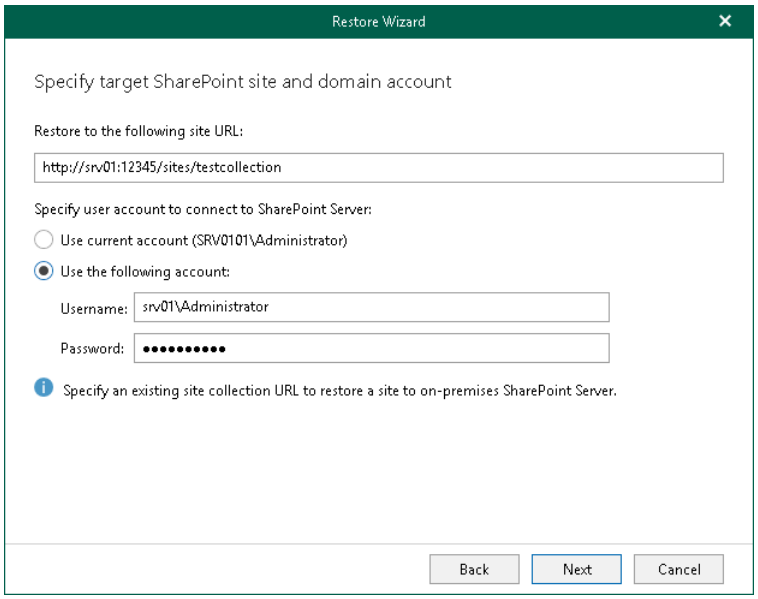
Step 3. Specify Target Site Web Address and Credentials

At this step of the wizard, specify web address of a target SharePoint site and provide credentials to connect to the Microsoft SharePoint server.

> **NOTE**
>
> Make sure that you restore to site collection that exists in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.

To specify web address of a target site and credentials to connect to SharePoint server, do the following:

1. In the **Restore to the following site URL** field, specify web address of a target site.
2. In the **Specify user account to connect to SharePoint Server** section, use an account that you are currently logged in to or provide a user name and password to connect to the on-premises Microsoft SharePoint server.



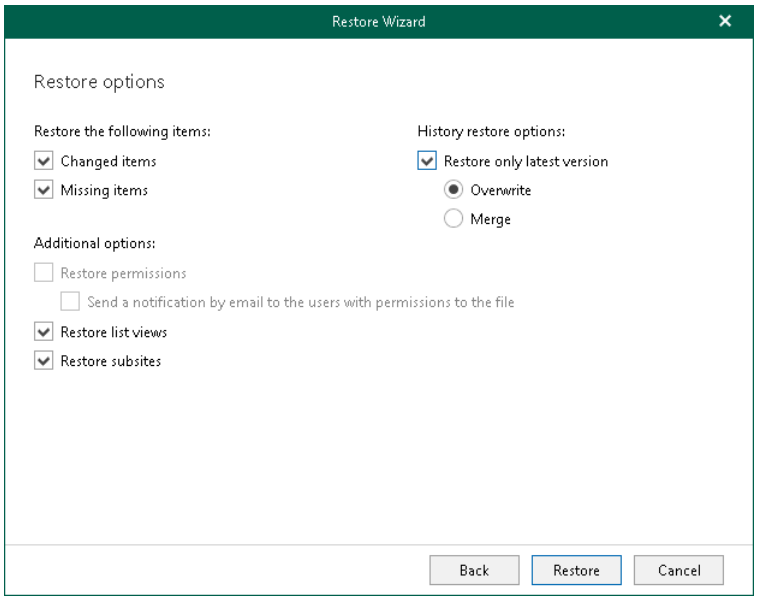
Step 4. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore list views.** Allows you to restore your list views.
- **Restore subsites.** Allows you to restore your subsites.



Restoring Document Libraries and Lists

Veeam Explorer for Microsoft SharePoint allows you to restore Microsoft SharePoint document libraries and lists to the original location or other Microsoft 365 organizations and on-premises Microsoft organizations.

Restoring Document Libraries and Lists to Original Location

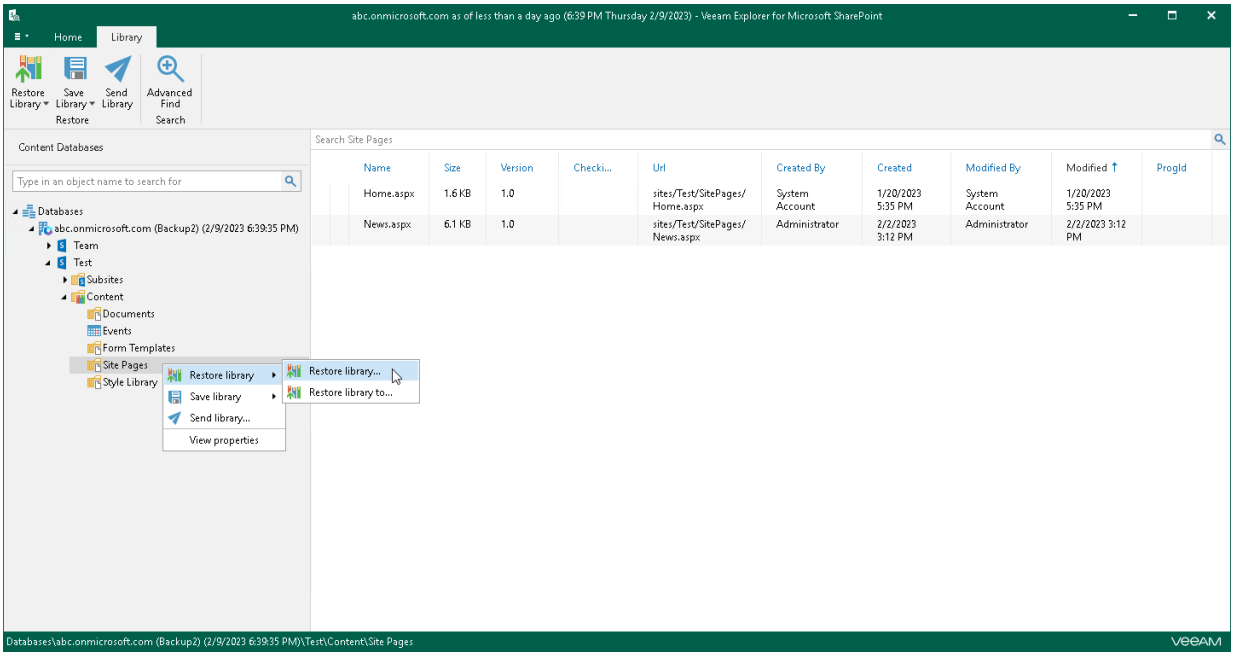
To restore Microsoft SharePoint document libraries and lists to the original location, do the following:

1. Launch the restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select a document library or a list that you want to restore.
2. Do one of the following:
   - On the **Library** tab, click **Restore Library** > **Restore library to <library_name>** on the ribbon.
   - Right-click a library and select **Restore library** > **Restore library**.
   - On the **List** tab, click **Restore List** > **Restore list to <list_name>** on the ribbon.
   - Right-click a list and select **Restore list** > **Restore list**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server, and specify authentication settings.

Modern Authentication

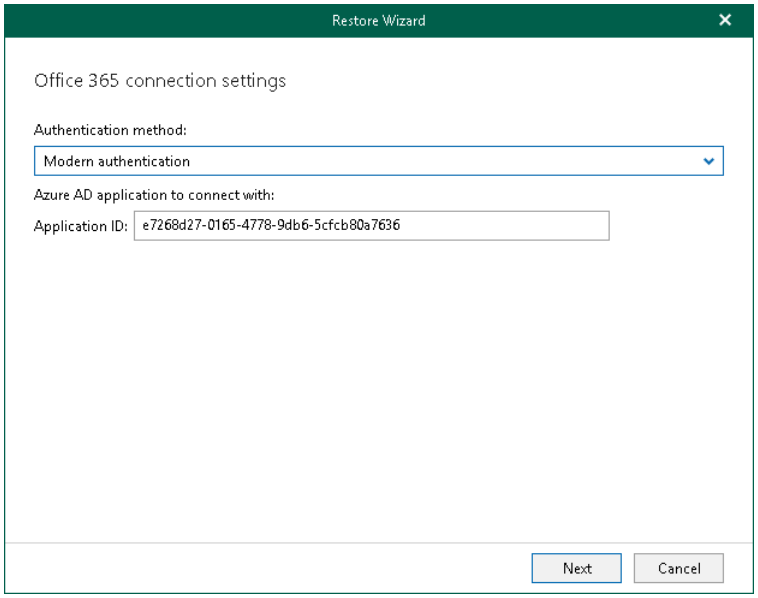
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

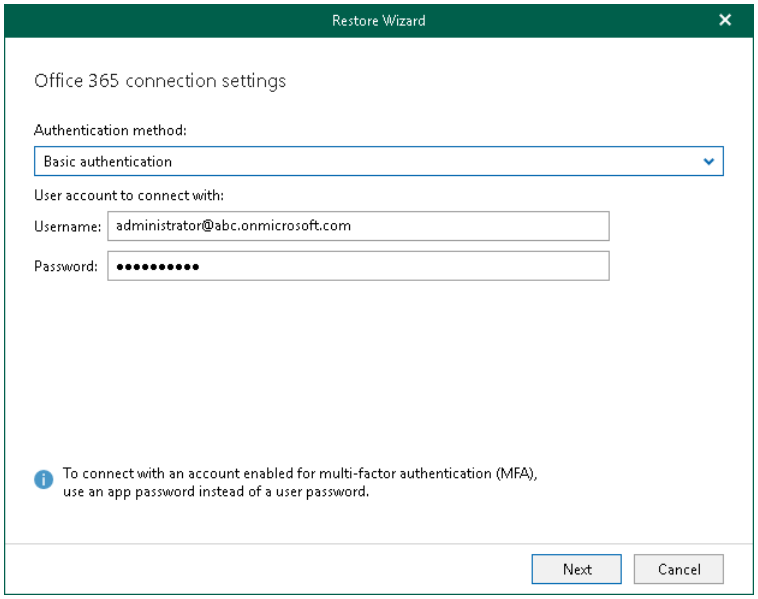
   By default, Veeam Explorer for Microsoft SharePoint populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

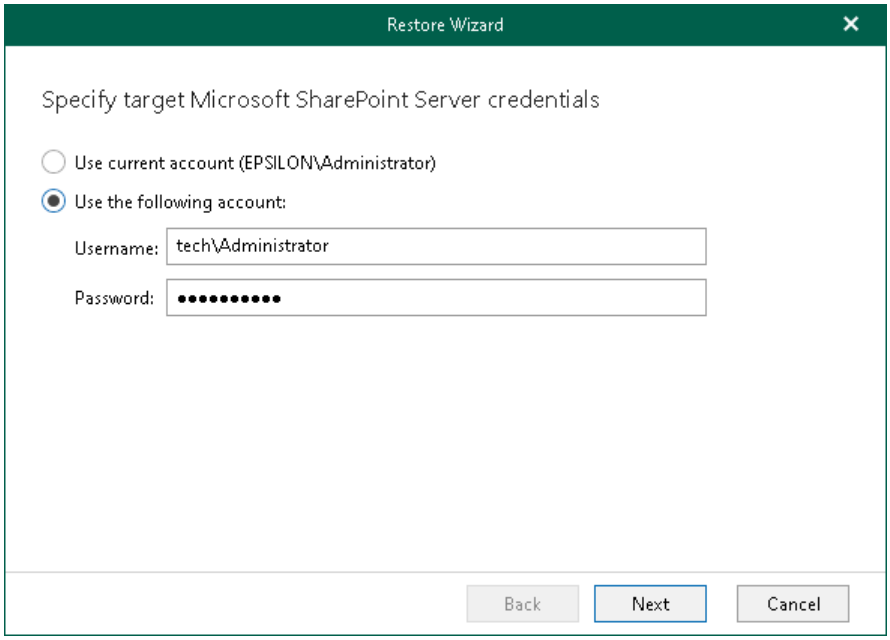
To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, use an account that you are currently logged in to or provide a user name and password.

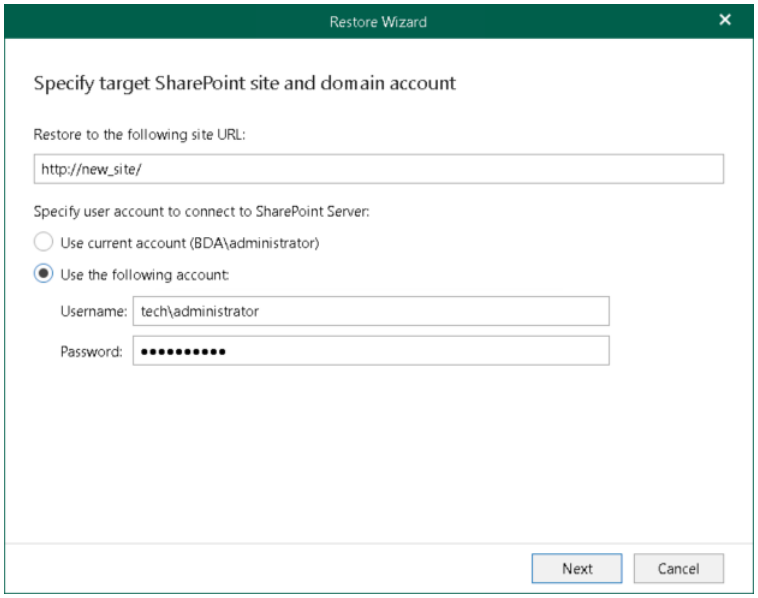


Restoring from Microsoft SQL Database

When restoring from a Microsoft SQL database, provide the following:

- The site URL to which you want to restore your site.
- Authentication credentials.

> **NOTE**
>
> When restoring Microsoft SharePoint document libraries and lists from a Microsoft SQL database, you will proceed directly to the Specify Restore Options step of the wizard.



Step 3. Log In to Microsoft 365

This step is only available for data restore from backups created by Veeam Backup for Microsoft 365 and if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

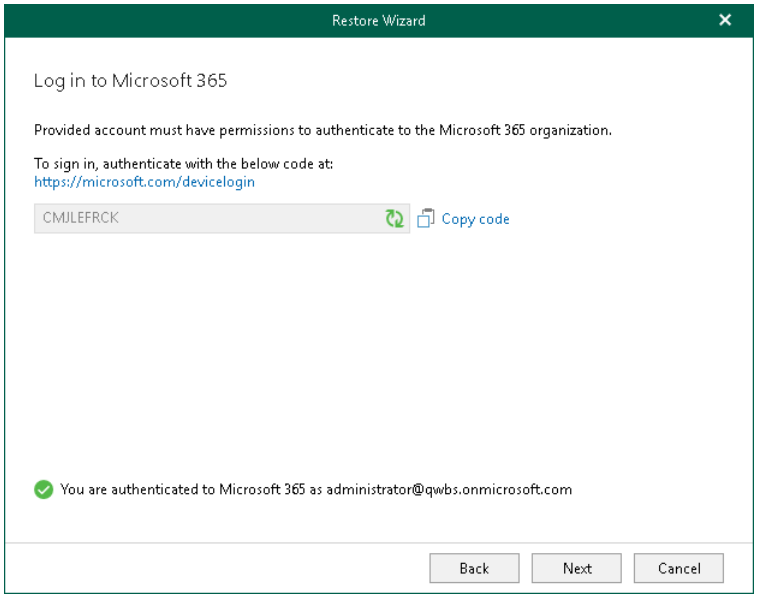
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



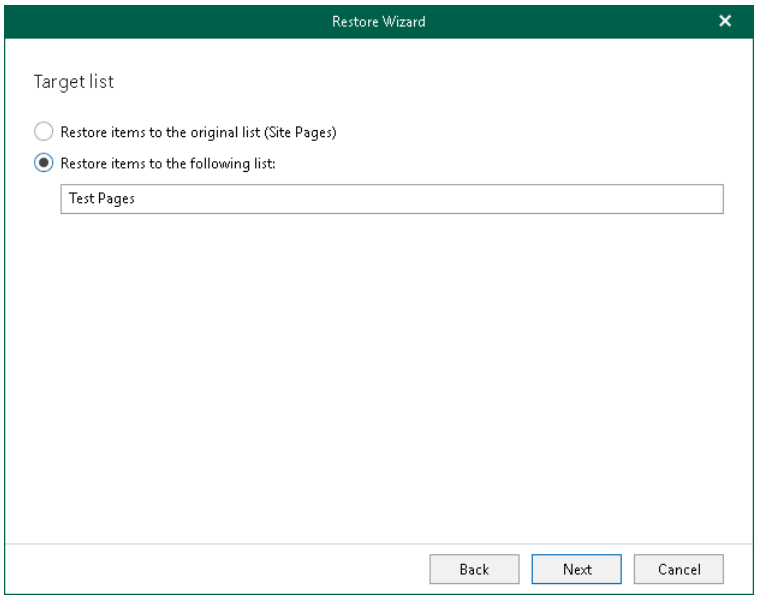
Step 4. Specify Target List

At this step of the wizard, select whether you want to restore backed-up data to the original list or specify a custom list.

You can select one of the following options:

- **Restore items to the original list**. To restore the document library or list back to the original list.
- **Restore items to the following list**. To restore the document library or list to the specified list.

  If the specified list does not exist, Veeam Explorer for Microsoft SharePoint will create it automatically.



Step 5. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

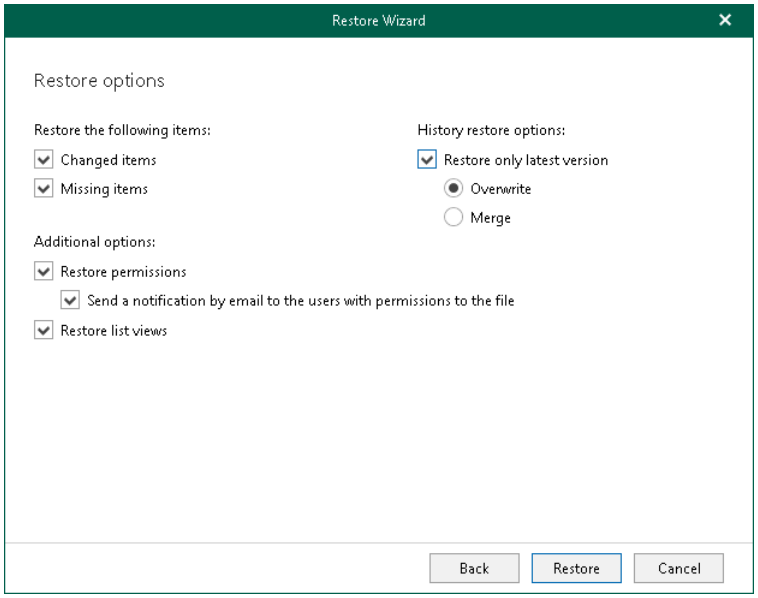
You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items. If this check box is selected, you can select one of the following options:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore permissions**. Allows you to restore permissions. If not selected, the permissions for the restored document library or list will be set in the following way:
  - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
  - If the library (or list) already exists on target, permissions will be preserved.
- **Send a notification by email to the users with permissions to the file**. Select this check box if you want to notify users about items restore. Veeam Explorer for Microsoft SharePoint will notify users with whom items have been shared. You can select this check box only if the **Restore permissions** check box is selected.

  > **NOTE**
  >
  > The **Send a notification by email to the users with permissions to the file** check box is only available when restoring data from backups created by Veeam Backup for Microsoft 365 for Microsoft 365 organizations.

- **Restore list views.** Allows you to restore your list views.



Restoring Document Libraries and Lists to Another Location

You can restore Microsoft SharePoint document libraries and lists to other Microsoft 365 organizations and on-premises Microsoft organizations.

Restore to Microsoft 365 Organizations

You can restore backed-up data to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

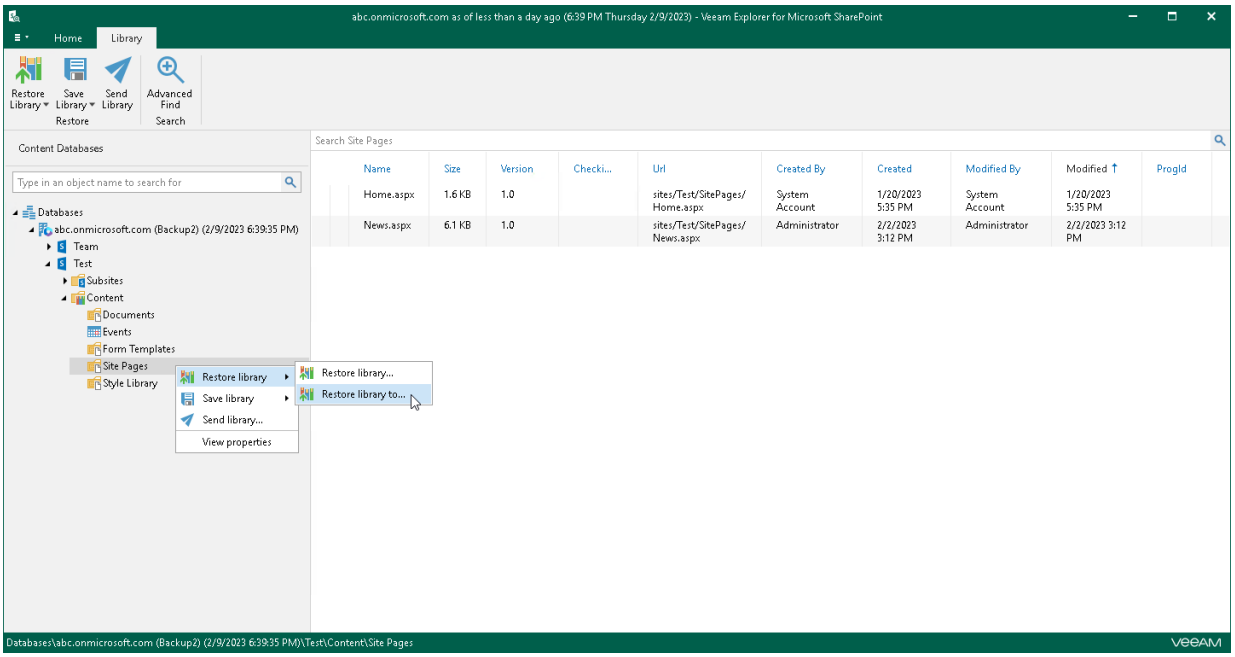
To restore Microsoft SharePoint document libraries and lists to another Microsoft 365 organization, do the following:

1. Launch the Restore wizard.
2. Select a target site location.
3. Select an authentication method.
4. Log in to Microsoft 365.
5. Specify a target site web address and a target list.
6. Specify restore options.

Step 1. Launch Restore Wizard

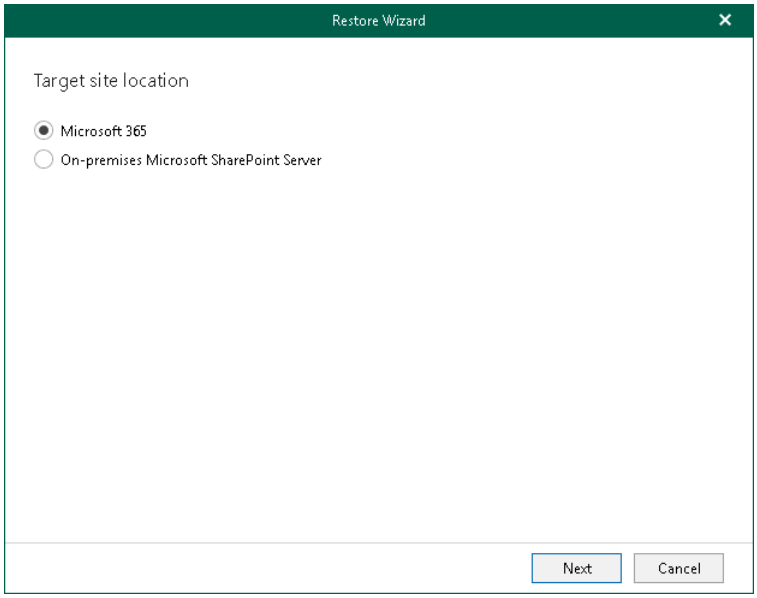
To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a document library or a list that you want to restore.
2. Do one of the following:
   - On the **Library** tab, click **Restore Library** > **Restore library to** on the ribbon.
   - Right-click a library and select **Restore library** > **Restore library to**.
   - On the **List** tab, click **Restore List** > **Restore list to** on the ribbon.
   - Right-click a list and select **Restore list** > **Restore list to**.



Step 2. Select Target Site Location

At this step of the wizard, select **Microsoft 365** to restore the document library or list to a SharePoint Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.



Step 3. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

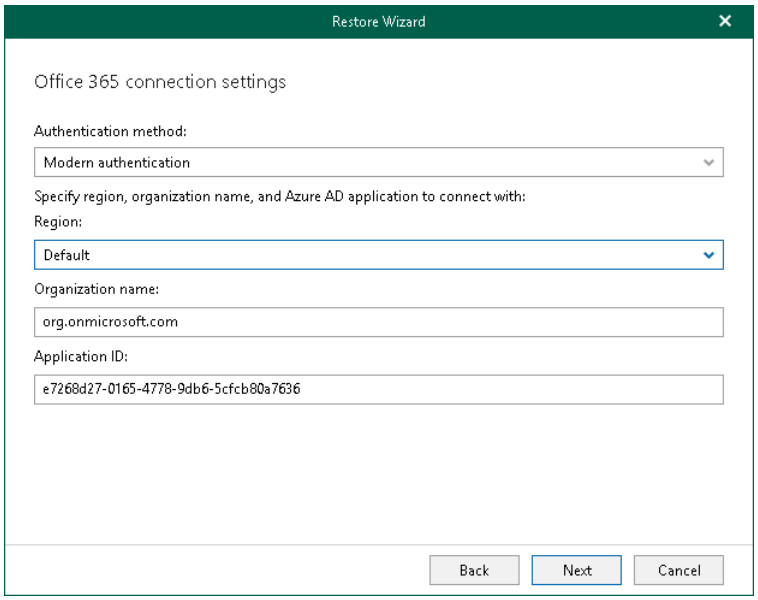
   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.

3. In the **Organization name** field, enter a name of your target SharePoint Online organization.

4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

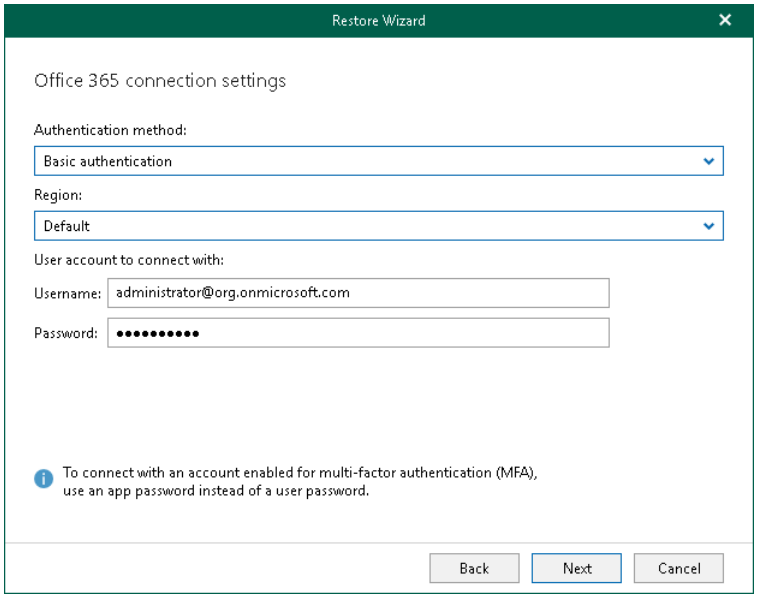
   By default, Veeam Explorer for Microsoft SharePoint populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.
3. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 4. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

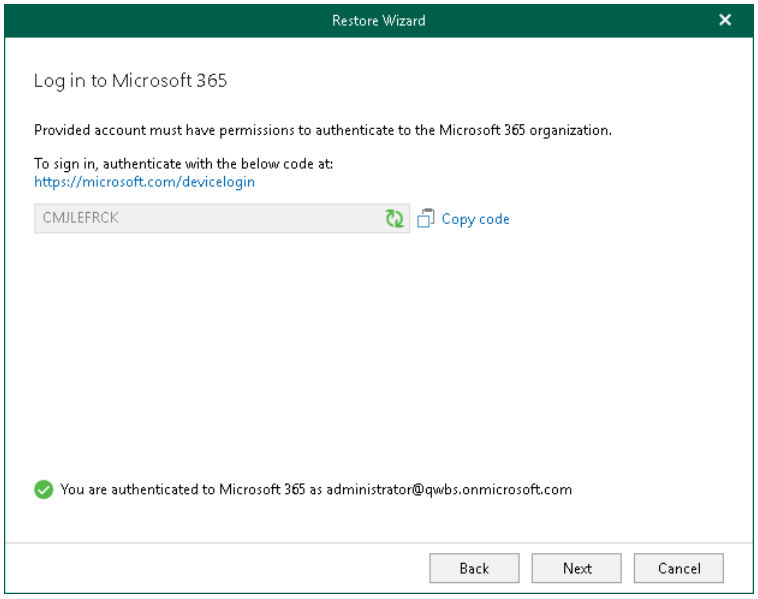
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



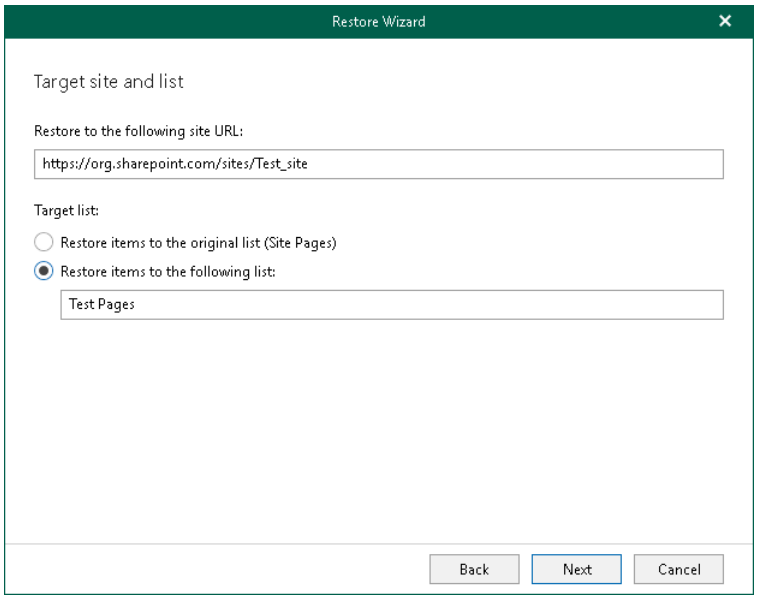
Step 5. Specify Target Site and List

At this step of the wizard, specify web address of a target SharePoint site and select whether you want to restore backed-up data to the original list or specify a custom list.

To specify web address of a target site and a list to restore backed-up data, do the following:

1. In the **Restore to the following site URL** field, specify web address of a target site.
2. In the **Target list** section, select one of the following options:
   - **Restore items to the original list**. To restore the document library or list back to the original list.
   - **Restore items to the following list**. To restore the document library or list to the specified list.

     If the specified list does not exist, Veeam Explorer for Microsoft SharePoint will create it automatically.



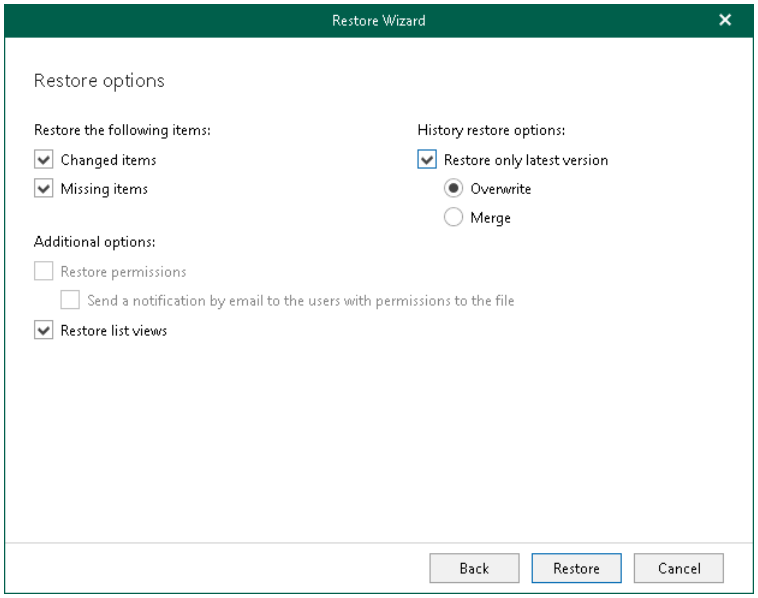
Step 6. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore list views.** Allows you to restore your list views.



Restore to On-Premises Microsoft Servers

You can restore backed-up data to on-premises Microsoft SharePoint servers. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.

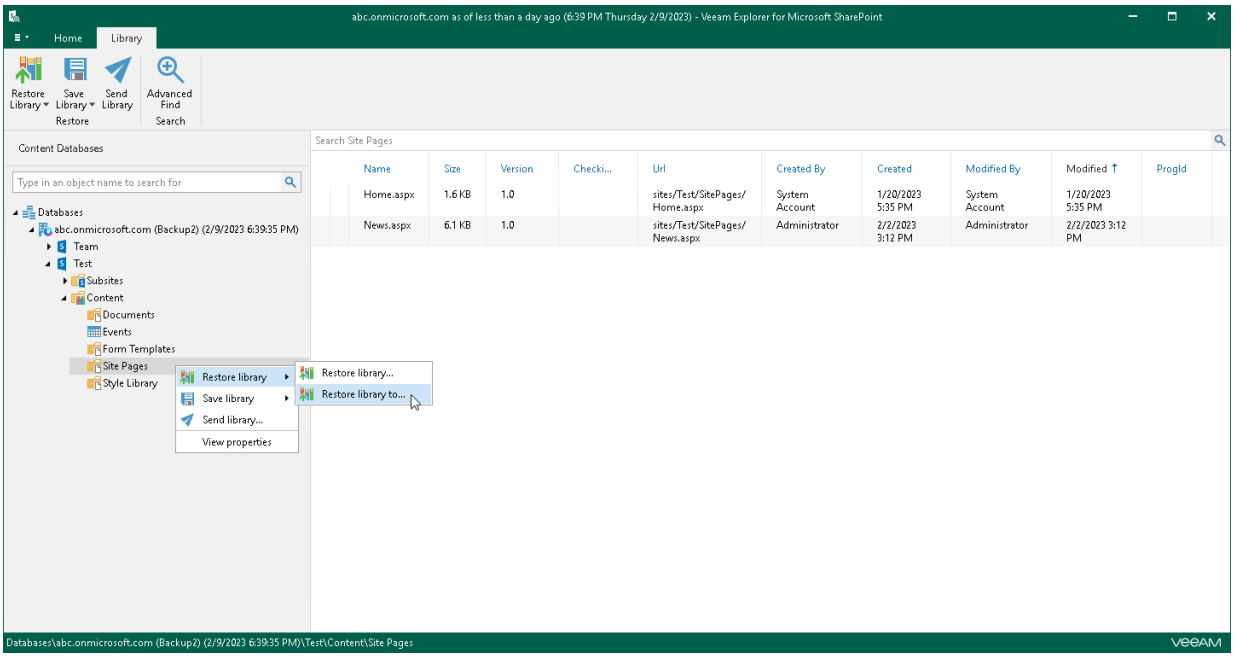
To restore Microsoft SharePoint document libraries and lists to an on-premises Microsoft SharePoint server, do the following:

1. Launch the Restore wizard.
2. Select a target site location.
3. Specify a target site web address and credentials.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

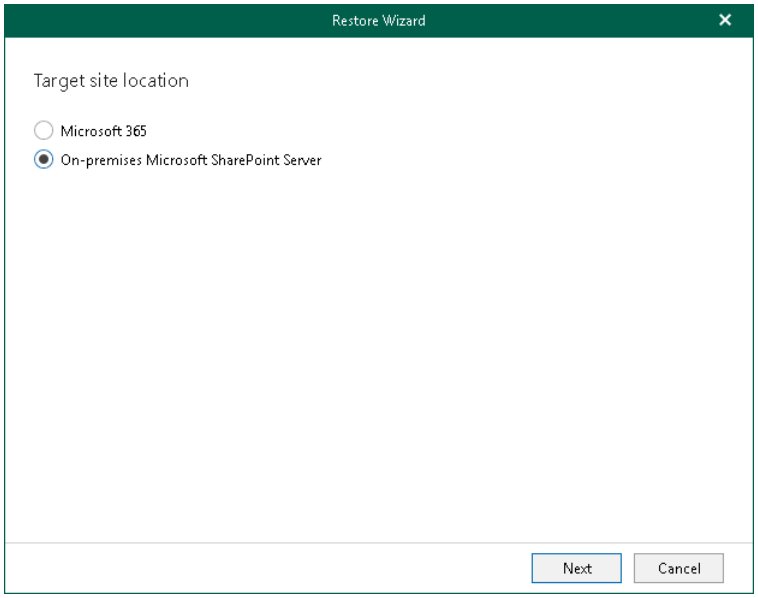
To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a document library or a list that you want to restore.
2. Do one of the following:
   - On the **Library** tab, click **Restore Library** > **Restore library to** on the ribbon.
   - Right-click a library and select **Restore library** > **Restore library to**.
   - On the **List** tab, click **Restore List** > **Restore list to** on the ribbon.
   - Right-click a list and select **Restore list** > **Restore list to**.



Step 2. Select Target Site Location

At this step of the wizard, select **On-premises Microsoft SharePoint Server** to restore the document library or list to an on-premises Microsoft SharePoint organization. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.



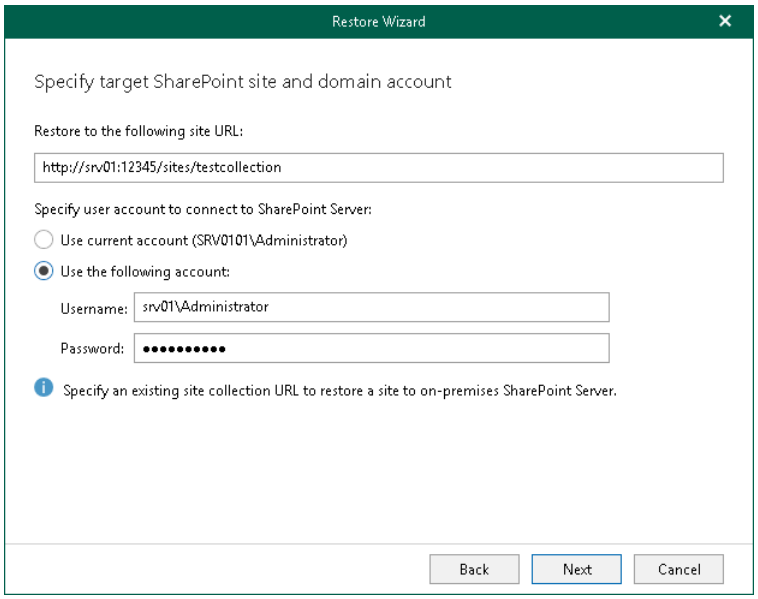
Step 3. Specify Target Site Web Address and Credentials

At this step of the wizard, specify web address of a target SharePoint site and provide credentials to connect to the Microsoft SharePoint server.

> **NOTE**
>
> Make sure that you restore to site collection that exists in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.

To specify web address of a target site and credentials to connect to SharePoint server, do the following:

1. In the **Restore to the following site URL** field, specify web address of a target site.
2. In the **Specify user account to connect to SharePoint Server** section, use an account that you are currently logged in to or provide a user name and password to connect to the on-premises Microsoft SharePoint server.



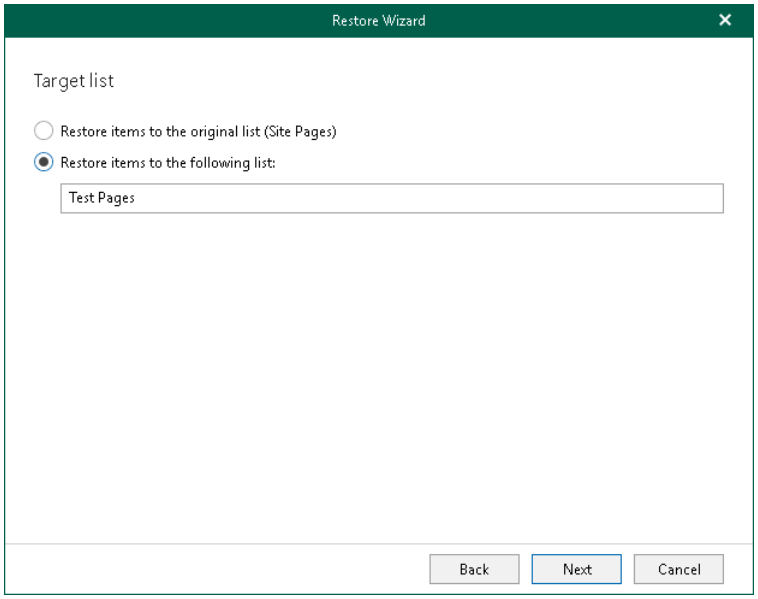
Step 4. Specify Target List

At this step of the wizard, select whether you want to restore backed-up data to the original list or specify a custom list.

You can select one of the following options:

- **Restore items to the original list**. To restore the document library or list back to the original list.
- **Restore items to the following list**. To restore the document library or list to the specified list.

  If the specified list does not exist, Veeam Explorer for Microsoft SharePoint will create it automatically.



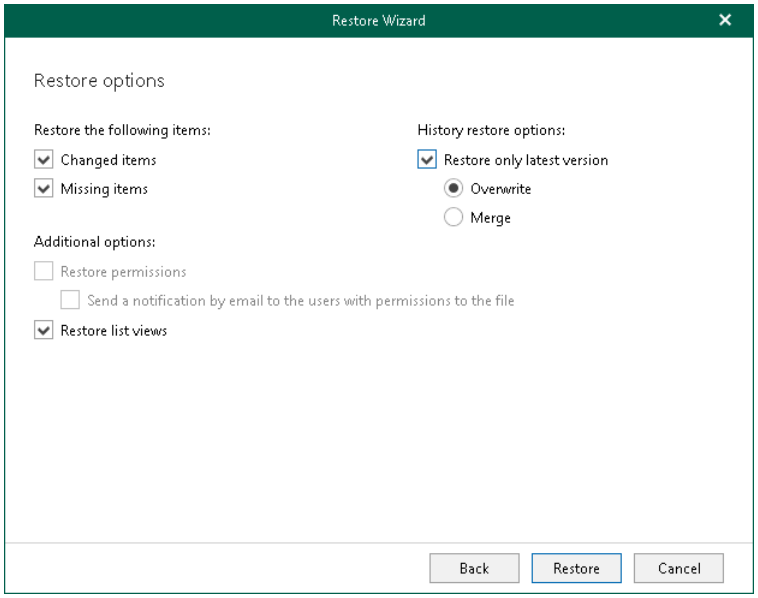
Step 5. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore list views.** Allows you to restore your list views.



Restoring Documents and List Items

Veeam Explorer for Microsoft SharePoint allows you to restore Microsoft SharePoint documents and list items to the original location or other Microsoft 365 organizations and on-premises Microsoft organizations.

Restoring Documents and List Items to Original Location

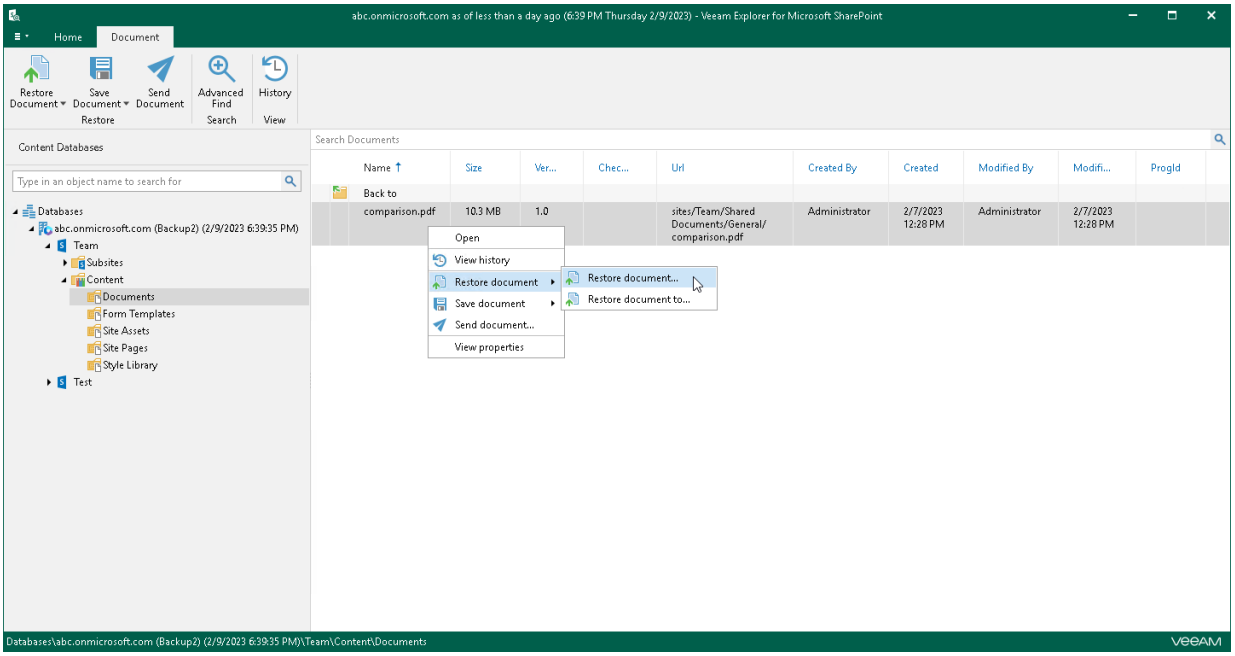
To restore Microsoft SharePoint documents and list items to the original location, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

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

1. In the preview pane, select a document or a list item that you want to restore.
2. Do one of the following:
   - On the **Document** tab, click **Restore Document** > **Restore document to <library_name>** on the ribbon.
   - Right-click a document and select **Restore document** > **Restore document**.
   - On the **Item** tab, click **Restore Item** > **Restore item to <list_name>** on the ribbon.
   - Right-click a list item and select **Restore item** > **Restore item**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server, and specify authentication settings.

Modern Authentication

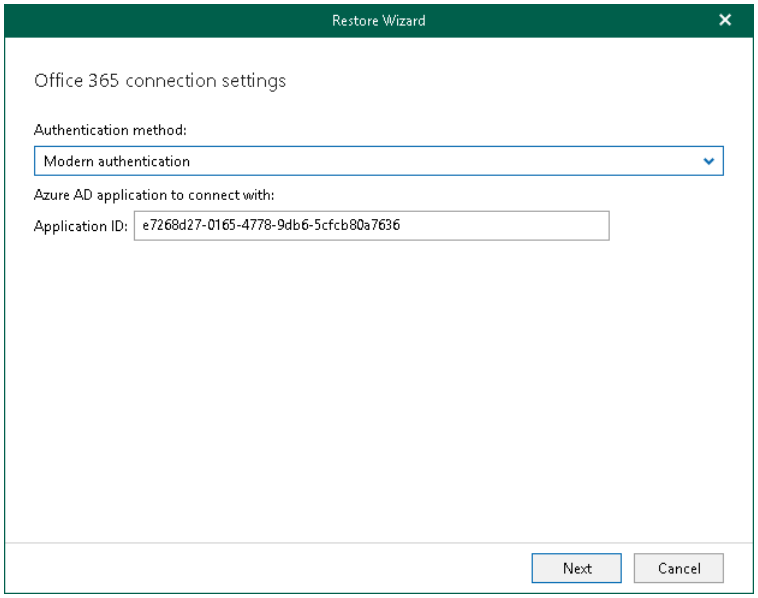
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

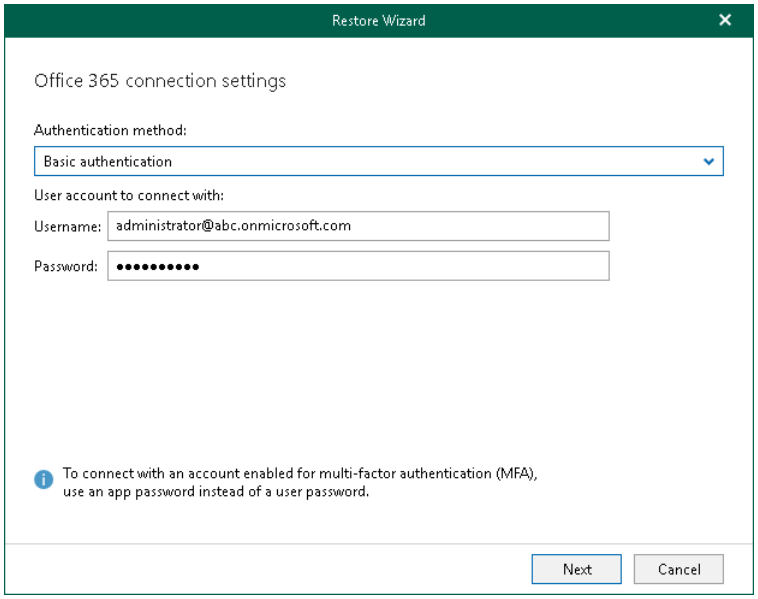
   By default, Veeam Explorer for Microsoft SharePoint populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

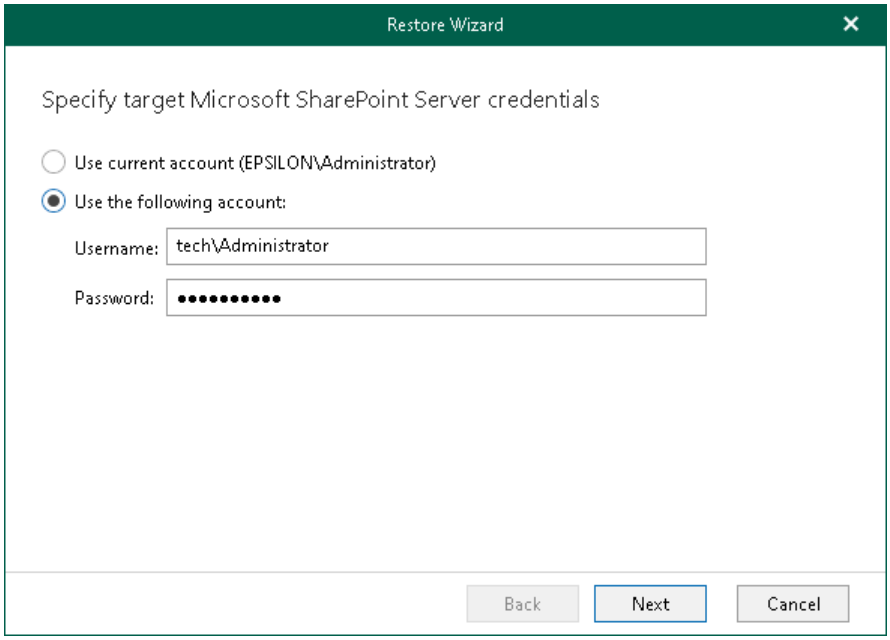
To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, use an account that you are currently logged in to or provide a user name and password.

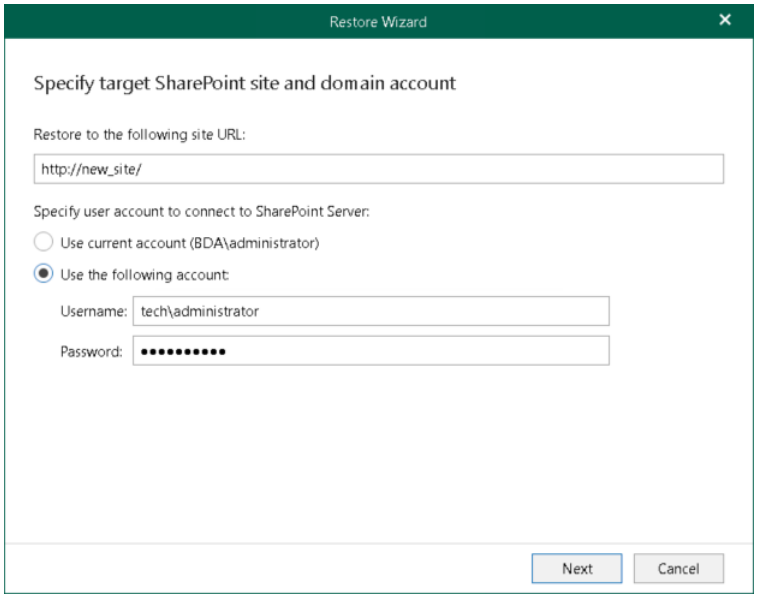


Restoring from Microsoft SQL Database

When restoring from a Microsoft SQL database, provide the following:

- The site URL to which you want to restore your site.
- Authentication credentials.

> **NOTE**
>
> When restoring Microsoft SharePoint documents and list items from a Microsoft SQL database, you will proceed directly to the Specify Restore Options step of the wizard.



Step 3. Log In to Microsoft 365

This step is only available for data restore from backups created by Veeam Backup for Microsoft 365 and if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

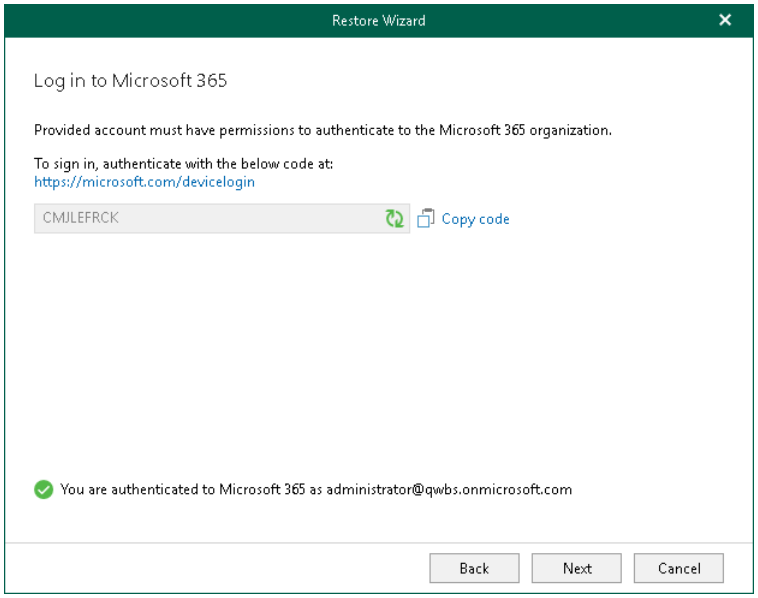
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



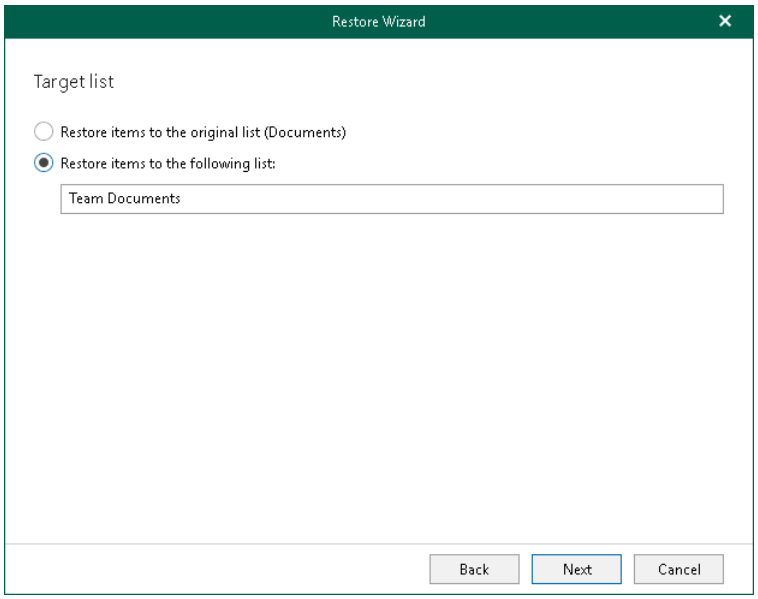
Step 4. Specify Target List

At this step of the wizard, select whether you want to restore backed-up data to the original list or specify a custom list.

You can select one of the following options:

- **Restore items to the original list**. To restore the document or list item back to the original list.
- **Restore items to the following list**. To restore the document or list item to the specified list.

  Make sure to specify a list that exists in the original SharePoint site.



Step 5. Specify Restore Options

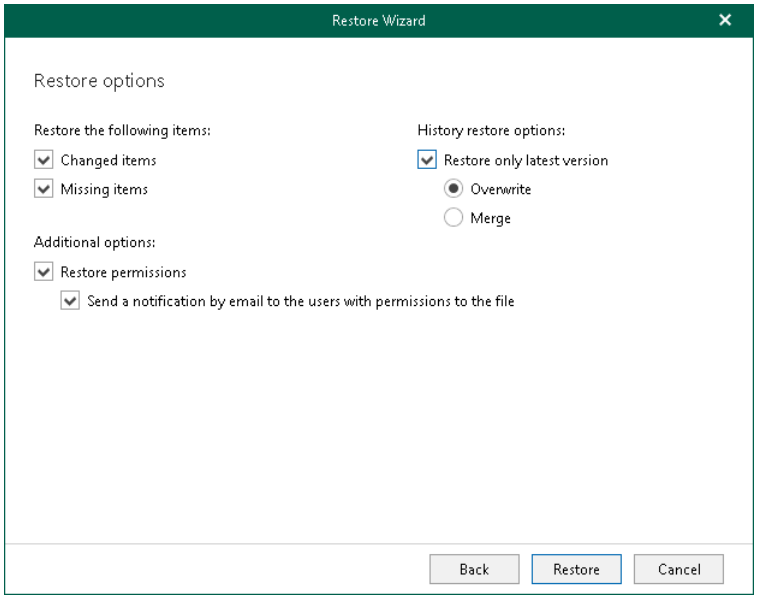
At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items. If this check box is selected, you can select one of the following options:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore permissions**. Allows you to restore permissions. If not selected, the permissions for the restored document library or list will be set in the following way:
  - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
  - If the library (or list) already exists on target, permissions will be preserved.
- **Send a notification by email to the users with permissions to the file**. Select this check box if you want to notify users about items restore. Veeam Explorer for Microsoft SharePoint will notify users with whom items have been shared. You can select this check box only if the **Restore permissions** check box is selected.

  > **NOTE**
  >
  > The **Send a notification by email to the users with permissions to the file** check box is only available when restoring data from backups created by Veeam Backup for Microsoft 365 for Microsoft 365 organizations.



Restoring Documents and List Items to Another Location

You can restore Microsoft SharePoint documents and list items to other Microsoft 365 organizations and on-premises Microsoft organizations.

Restore to Microsoft 365 Organizations

You can restore backed-up data to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

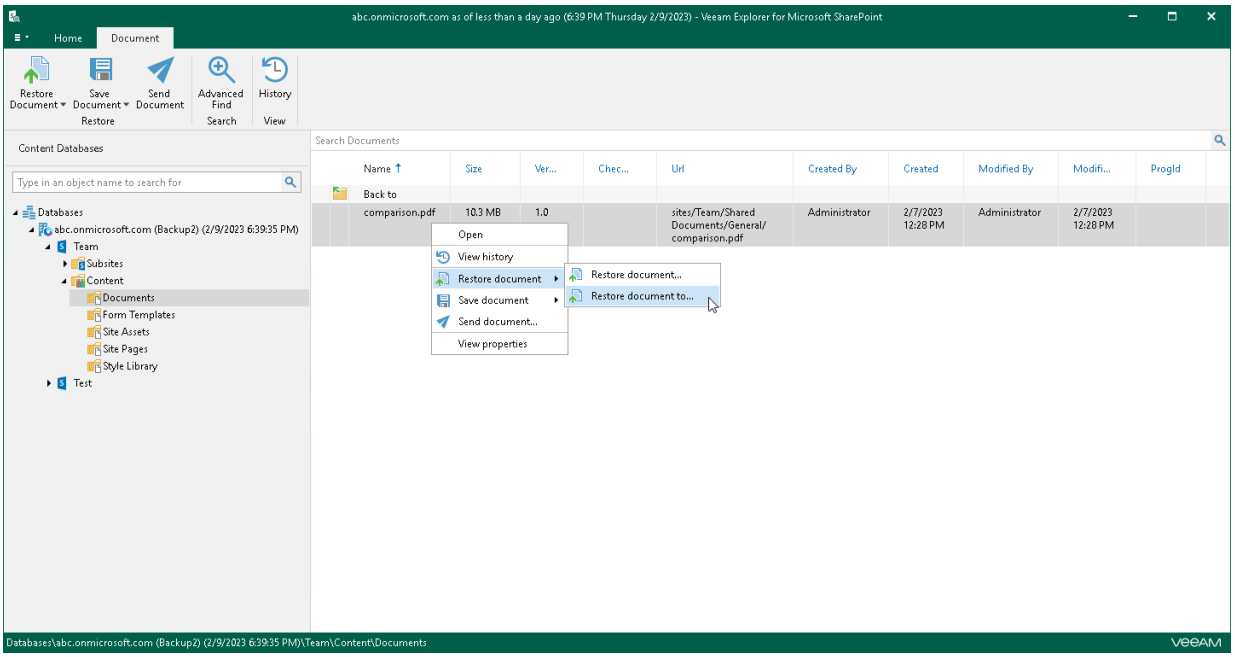
To restore Microsoft SharePoint documents and list items to another Microsoft 365 organization, do the following:

1. Launch the Restore wizard.
2. Select a target site location.
3. Select an authentication method.
4. Log in to Microsoft 365.
5. Specify a target site web address and a target list.
6. Specify restore options.

Step 1. Launch Restore Wizard

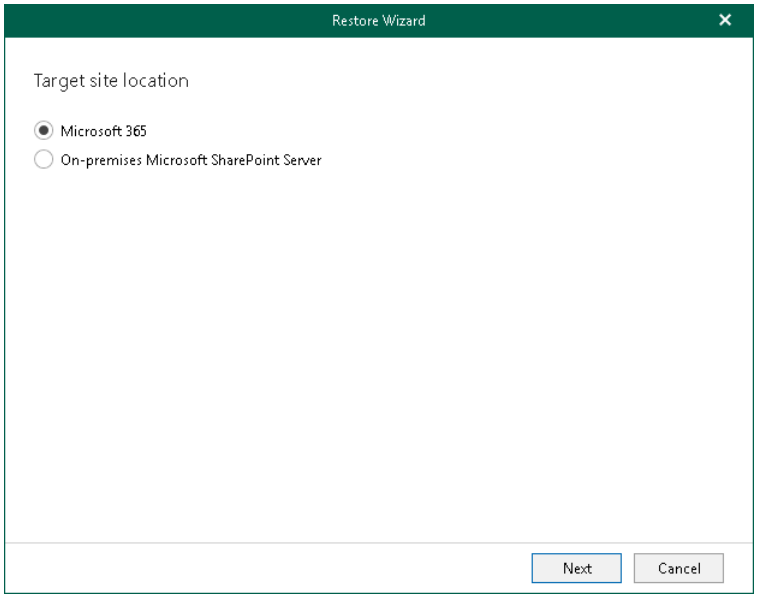
To launch the **Restore** wizard, do the following:

1. In the preview pane, select a document or a list item that you want to restore.
2. Do one of the following:
   - On the **Document** tab, click **Restore Document** > **Restore document to** on the ribbon.
   - Right-click a document and select **Restore document** > **Restore document to**.
   - On the **Item** tab, click **Restore Item** > **Restore item to** on the ribbon.
   - Right-click a list item and select **Restore item** > **Restore item to**.



Step 2. Select Target Site Location

At this step of the wizard, select **Microsoft 365** to restore the document or list item to a SharePoint Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.



Step 3. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

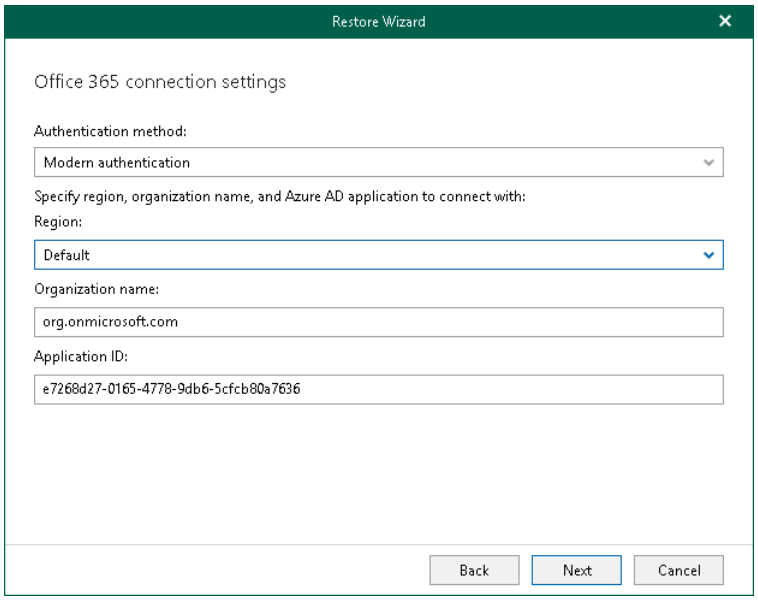
   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.

3. In the **Organization name** field, enter a name of your target SharePoint Online organization.

4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

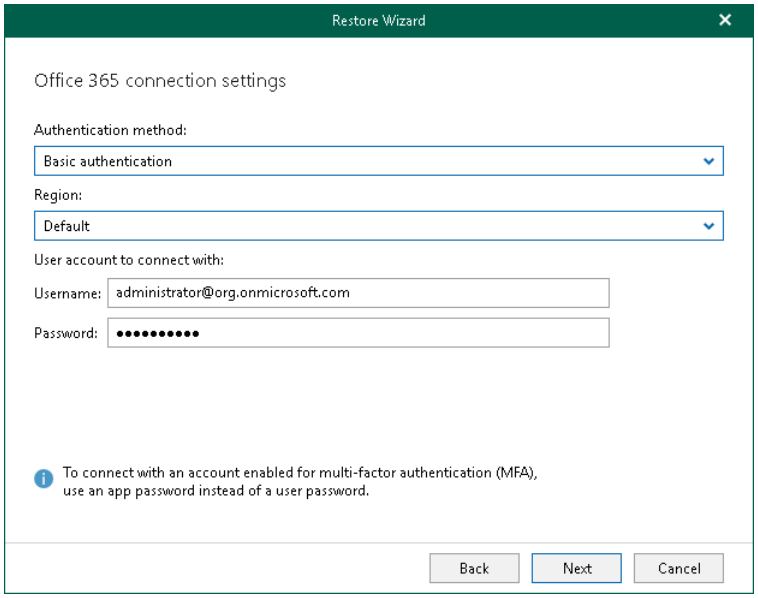
   By default, Veeam Explorer for Microsoft SharePoint populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. From the **Region** drop-down list, select a region to which your target SharePoint Online organization belongs.
3. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 4. Log In to Microsoft 365

This step is only available if you have selected the *Modern Authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

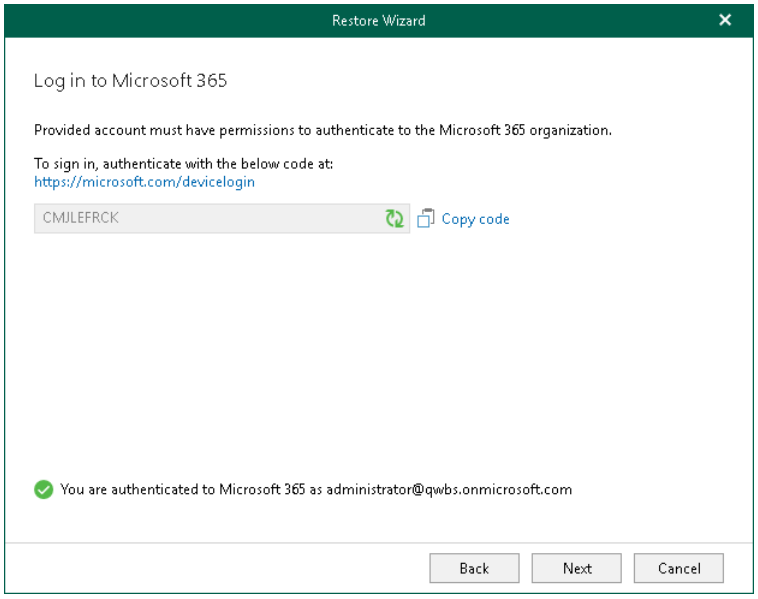
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



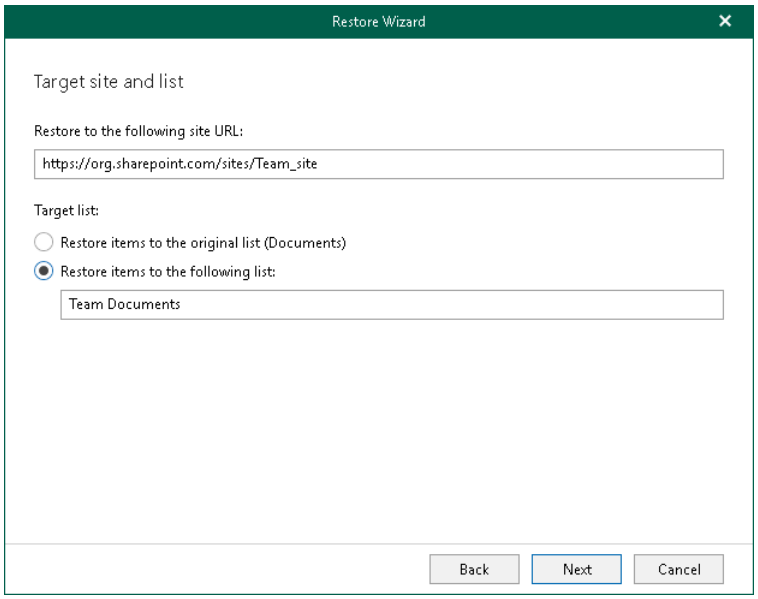
Step 5. Specify Target Site and List

At this step of the wizard, specify web address of a target SharePoint site and select whether you want to restore backed-up data to the original list or specify a custom list.

To specify web address of a target site and a list to restore backed-up data, do the following:

1. In the **Restore to the following site URL** field, specify web address of a target site.
2. In the **Target list** section, select one of the following options:
   - **Restore items to the original list**. To restore the document or list item back to the original list.
   - **Restore items to the following list**. To restore the document or list item to the specified list.

     Keep in mind that if you restore documents and the specified list does not exist, Veeam Explorer for Microsoft SharePoint will create it automatically. If you restore list items, make sure to specify a list that exists in the original SharePoint site.



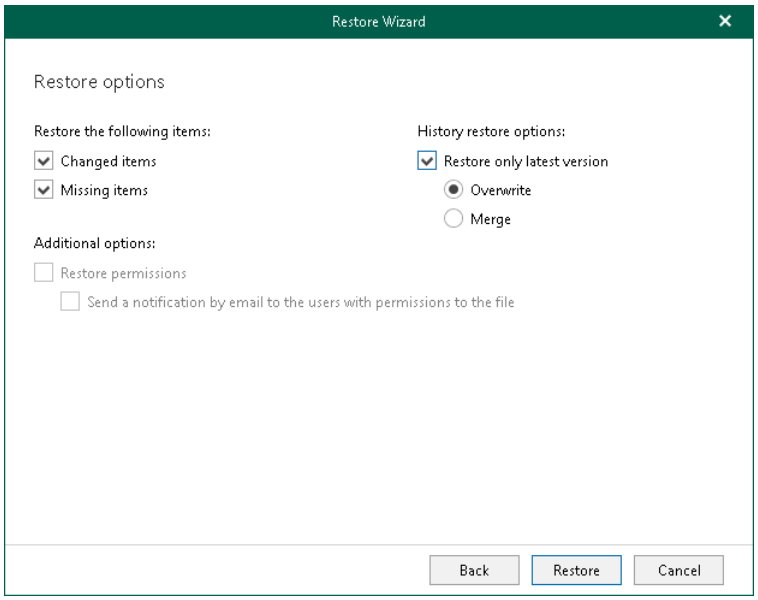
Step 6. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.



Restore to On-Premises Microsoft Servers

You can restore backed-up data to on-premises Microsoft SharePoint servers. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.

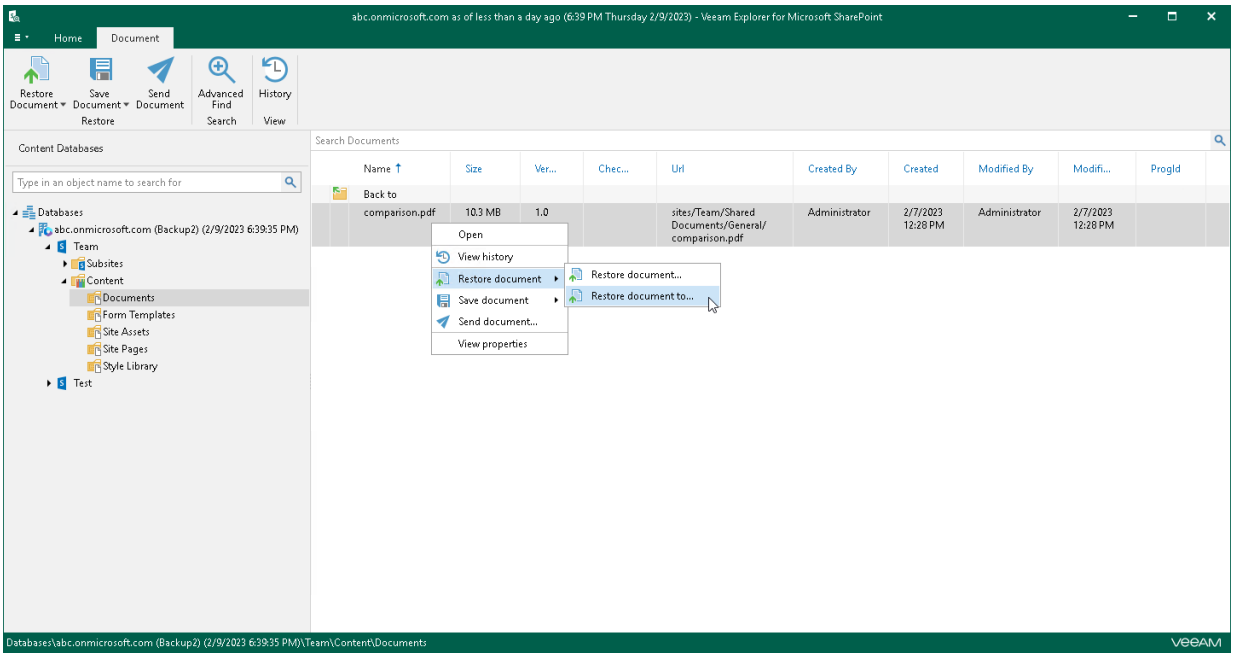
To restore Microsoft SharePoint documents and list items to an on-premises Microsoft SharePoint server, do the following:

1. Launch the Restore wizard.
2. Select a target site location.
3. Specify a target site web address and credentials.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

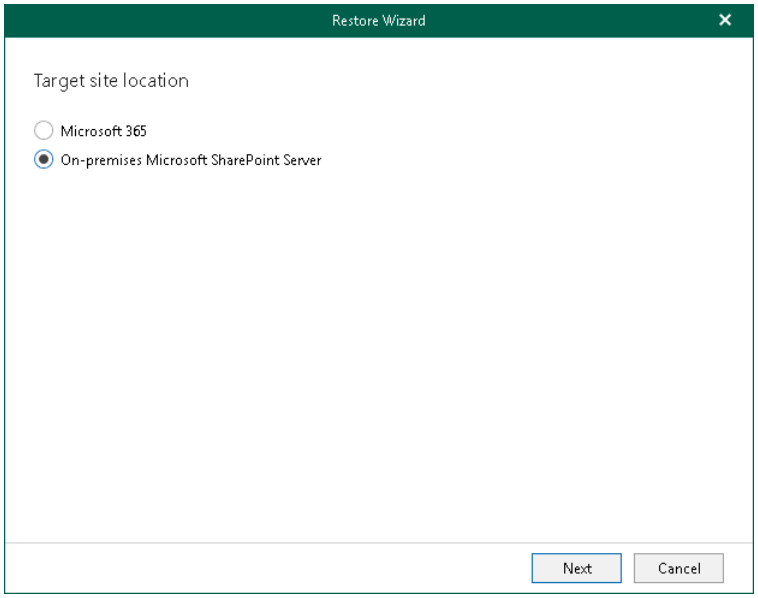
To launch the **Restore** wizard, do the following:

1. In the preview pane, select a document or a list item that you want to restore.
2. Do one of the following:
   - On the **Document** tab, click **Restore Document** > **Restore document to** on the ribbon.
   - Right-click a document and select **Restore document** > **Restore document to**.
   - On the **Item** tab, click **Restore Item** > **Restore item to** on the ribbon.
   - Right-click a list item and select **Restore item** > **Restore item to**.



Step 2. Select Target Site Location

At this step of the wizard, select **On-premises Microsoft SharePoint Server** to restore the document or list item to an on-premises Microsoft SharePoint organization. For more information, see the On-Premises Microsoft Organizations section of the Veeam Backup for Microsoft 365 User Guide.



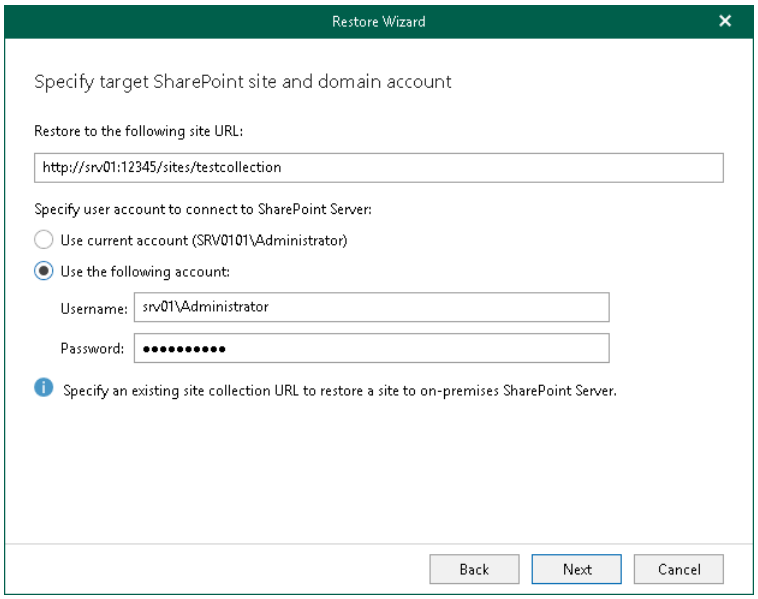
Step 3. Specify Target Site Web Address and Credentials

At this step of the wizard, specify web address of a target SharePoint site and provide credentials to connect to the Microsoft SharePoint server.

> **NOTE**
>
> Make sure that you restore to site collection that exists in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.

To specify web address of a target site and credentials to connect to SharePoint server, do the following:

1. In the **Restore to the following site URL** field, specify web address of a target site.
2. In the **Specify user account to connect to SharePoint Server** section, use an account that you are currently logged in to or provide a user name and password to connect to the on-premises Microsoft SharePoint server.



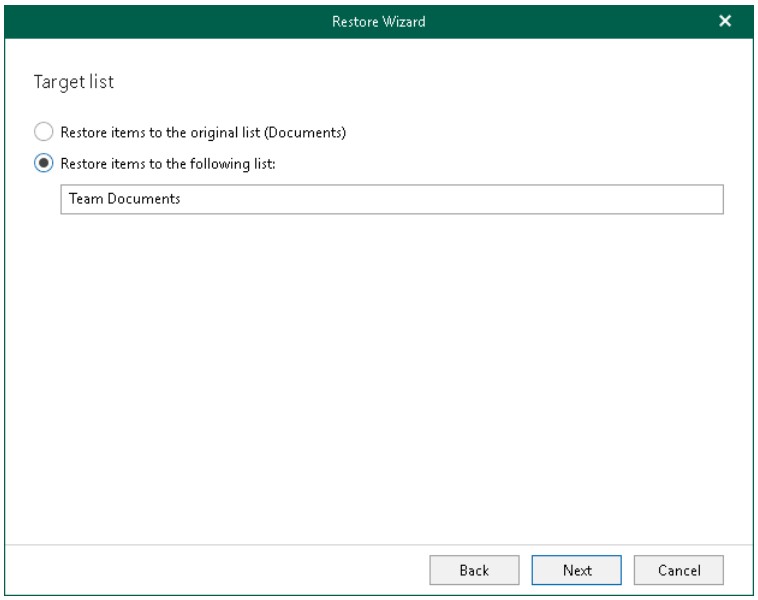
Step 4. Specify Target List

At this step of the wizard, select whether you want to restore backed-up data to the original list or specify a custom list.

You can select one of the following options:

- **Restore items to the original list**. To restore the document or list item back to the original list.
- **Restore items to the following list**. To restore the document or list item to the specified list.

  Keep in mind that if you restore documents and the specified list does not exist, Veeam Explorer for Microsoft SharePoint will create it automatically. If you restore list items, make sure to specify a list that exists in the original SharePoint site.



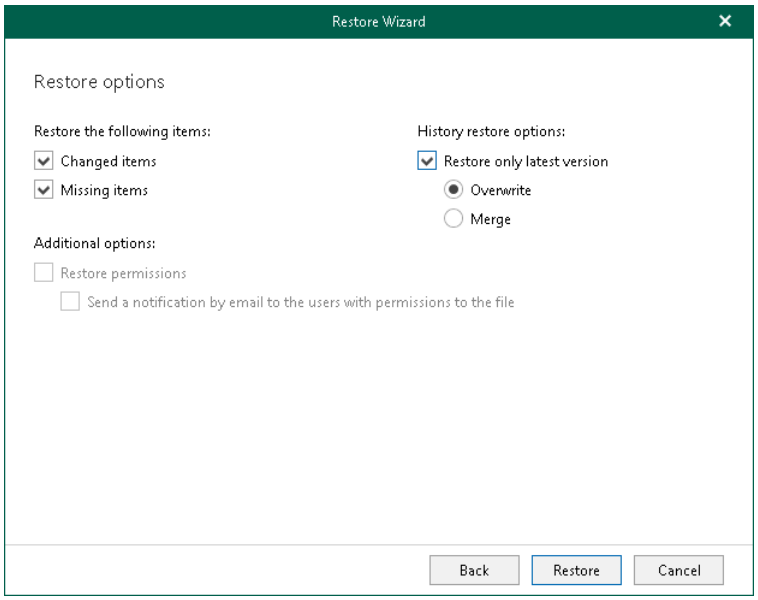
Step 5. Specify Restore Options

At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.



Data Export

You can use Veeam Explorer for Microsoft SharePoint to export and import Microsoft SharePoint data.

Before exporting data, read the Considerations and Limitations section.

Exporting Microsoft SharePoint Data

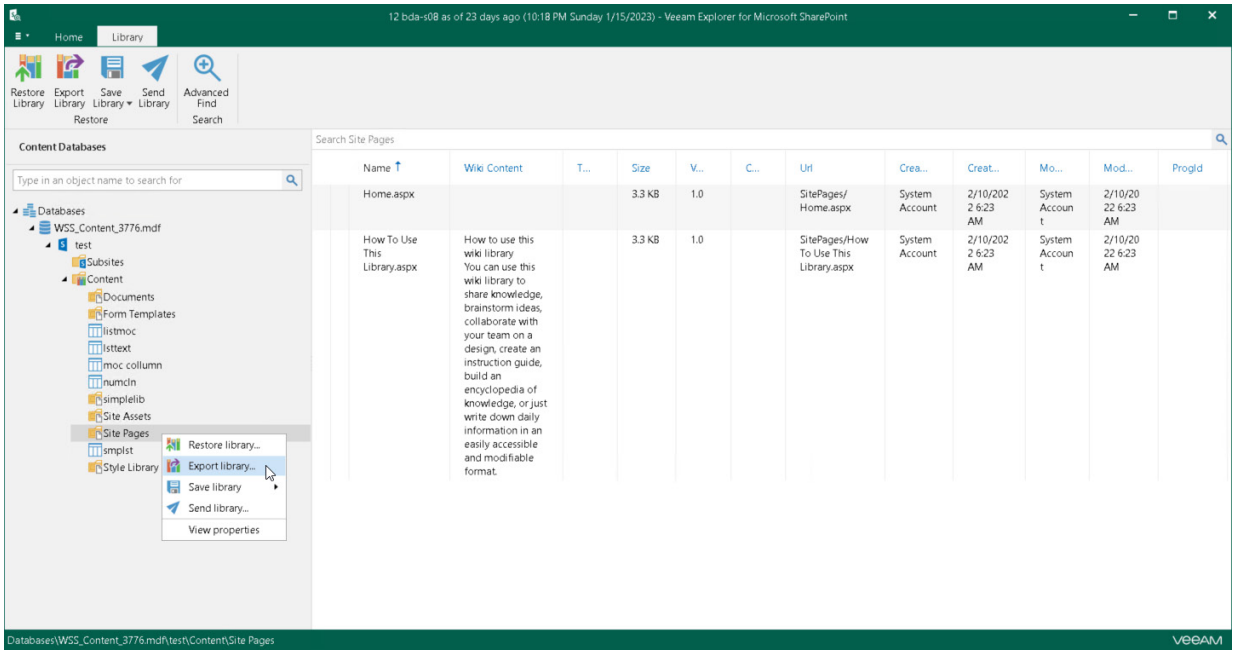
Veeam Explorer for Microsoft SharePoint allows you to export SharePoint document libraries and lists from backups created by Veeam Backup & Replication.

The exported content will be saved as a set of XML files and can be imported to another SharePoint database using PowerShell cmdlets. For more information, see Importing Microsoft SharePoint Data.

To export SharePoint data, do the following:

1. In the navigation pane, select a library or a list that you want to export.
2. Do one of the following:
   - On the **Library** tab, click **Export Library** on the ribbon.
   - Right-click a library and select **Export library**.
   - On the **List** tab, click **Export List** on the ribbon.
   - Right-click a list and select **Export list**.
3. Specify the output directory and click **OK**.

> **NOTE**
>
> You cannot export an empty folder, an empty list and an individual list item.



Importing Microsoft SharePoint Data

To import document library or list, use one of the following PowerShell cmdlets:

- For PowerShell snap-in, use the following command:

```
Add-PsSnapin Microsoft.SharePoint.PowerShell
Import-SPWeb -Identity "http://<web_server_name>/sites/<destination_site>"
-Path "C:\<export_folder>" -NoFileCompression –IncludeUserSecurity
```

- For SharePoint Management Shell, use the following command:

```
Import-SPWeb -Identity "http://<web_server_name>/sites/<destination_site>"
-Path "C:\<export_folder>" -NoFileCompression –IncludeUserSecurity
```

where:

- `<web_server_name>` — destination web server.
- `<destination_site>` — destination website.
- `<export_folder>` — source folder containing exported library/list content.

To get extended help on the `Import-SPWeb` command, use the following command:

```
Get-Help Import-SPWeb -full
```

Saving Microsoft SharePoint Documents and Libraries

Veeam Explorer for Microsoft SharePoint allows you to save your libraries and library documents to a specified location.

To save a Microsoft SharePoint library, do the following:

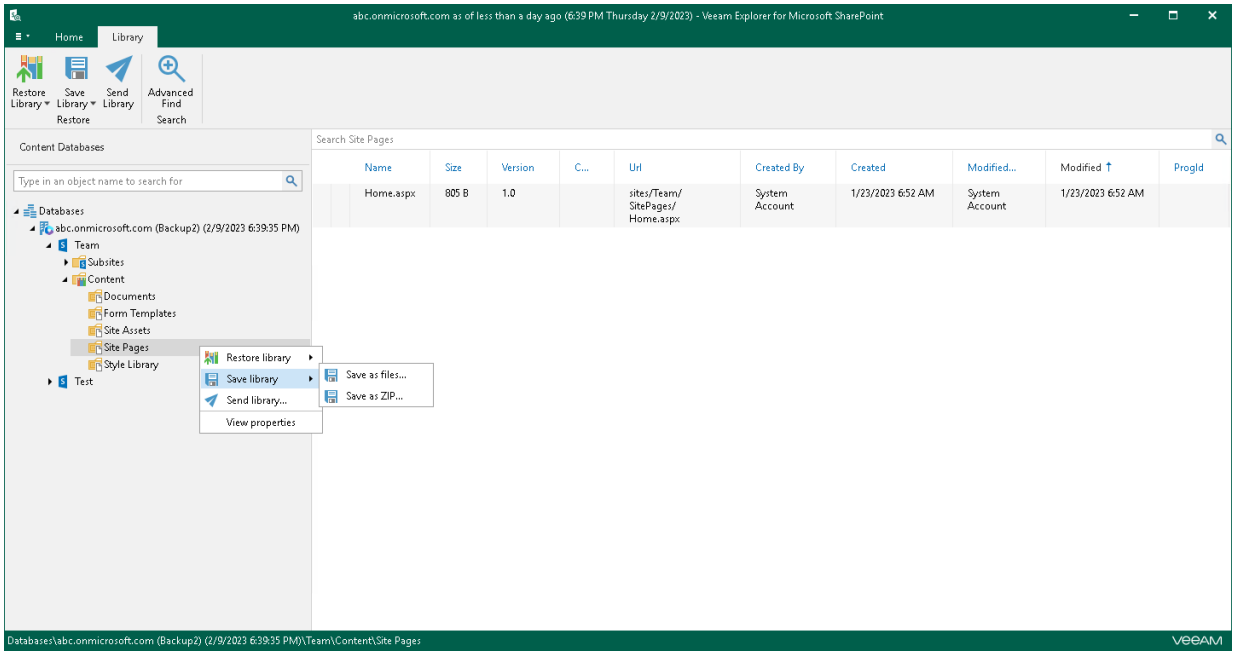
1. In the navigation pane, select a library that you want to save.
2. Do one of the following:
   - On the **Library** tab, click **Save Library** > **Save as files** or **Save Library** > **Save as ZIP** on the ribbon.
   - Right-click a library and select **Save library** > **Save as files** or **Save library** > **Save as ZIP**.
3. In the displayed window, browse to the necessary folder and click **Select Folder** or **Save**.

   Keep in mind that if you select the **Save as ZIP** option, Veeam Explorer for Microsoft SharePoint will save a library to an archive with the *archive.zip* name.

To save a library document, do the following:

1. In the preview pane, select a document that you want to save.
2. Do one of the following:
   - On the **Document** tab, click **Save Document** > **Save as files** or **Save Document** > **Save as ZIP** on the ribbon.
   - Right-click a document and select **Save document** > **Save as files** or **Save document** > **Save as ZIP**.
3. In the displayed window, browse to the necessary folder and click **Select Folder** or **Save**.

   Keep in mind that if you select the **Save as ZIP** option, Veeam Explorer for Microsoft SharePoint will save a library to an archive with the *archive.zip* name.



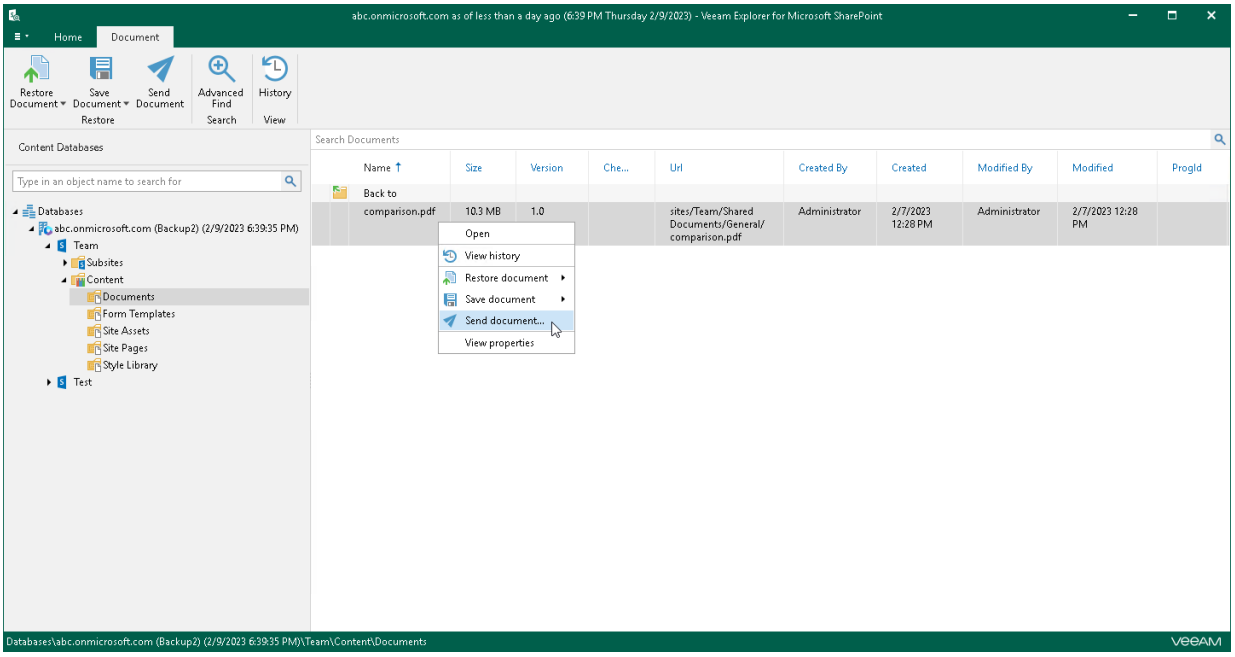
Sending Microsoft SharePoint Documents and Libraries

Veeam Explorer for Microsoft SharePoint allows you to send libraries or library documents to the specified recipients through email.

> **TIP**
>
> Before sending documents, make sure to configure SMTP settings. The amount of data you can send at a time depends on your SMTP server configuration. For more information about configuring SMTP settings, see SMTP Settings.

To send libraries or library documents through email, do the following:

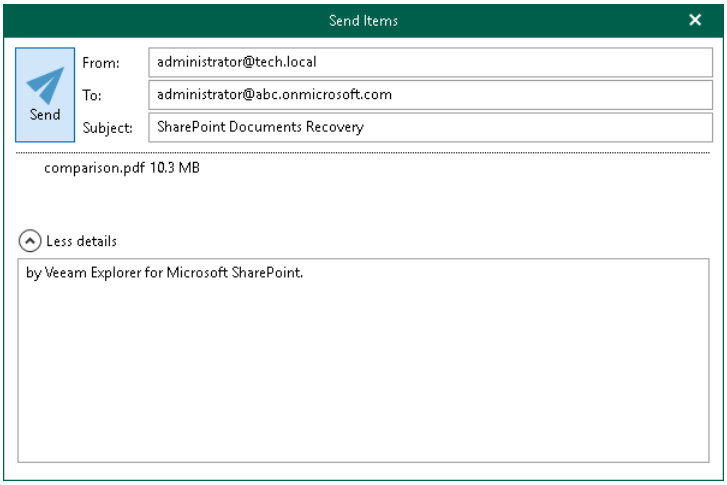
1. Select an object that you want to send through email:
   - To send a Microsoft SharePoint library, select the necessary library in the navigation pane.
   - To send a library document, select a library that contains the document in the navigation pane and then select the document in the preview pane.
2. Do one of the following:
   - On the **Library/Document** tab, click **Send Library/Send Document** on the ribbon.
   - Right-click an object that you want to send and select **Send library/Send document**.



3. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

You can also edit the message subject and body. To edit the message body, click **More details**.



Veeam Explorer for Microsoft OneDrive for Business

Veeam Explorer for Microsoft OneDrive for Business allows you to restore Microsoft OneDrive data from backups created by Veeam Backup for Microsoft 365.

Planning and Preparation

Veeam Explorer for Microsoft OneDrive for Business comes as part of the Veeam Explorer for Microsoft SharePoint installation package and has the same system requirements.

Consider that when Veeam Explorer for Microsoft SharePoint is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft 365 are installed, the notification settings will be inherited from the Veeam Backup & Replication Global Notification settings.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft OneDrive for Business and load backups, you can use any of the following methods:

- The **Explore** option to load backups created by Veeam Backup for Microsoft 365. For more information, see the Data Restore section of the Veeam Backup for Microsoft 365 User Guide.

  When loading backups located in object storage, Veeam Explorer for Microsoft OneDrive for Business will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To disable these notifications, clear the **Show pop-up notifications on startup** check box. For more information, see Advanced Settings.

- Go to **Start**, click **Veeam Explorer for Microsoft OneDrive for Business** and manually open Microsoft OneDrive databases. For more information, see Standalone Databases.

  When you open Veeam Explorer for Microsoft OneDrive for Business from the **Start** menu, all backed-up databases will be loaded automatically.

If you open Veeam Explorer for Microsoft OneDrive for Business from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

- The domain name or IP address of a server to which you want to connect.
- The port number.
- User account credentials.

  Consider the following:

  - To perform restore operations, Veeam Explorer for Microsoft OneDrive for Business must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorer for Microsoft OneDrive for Business is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft OneDrive for Business is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.

Getting to Know User Interface

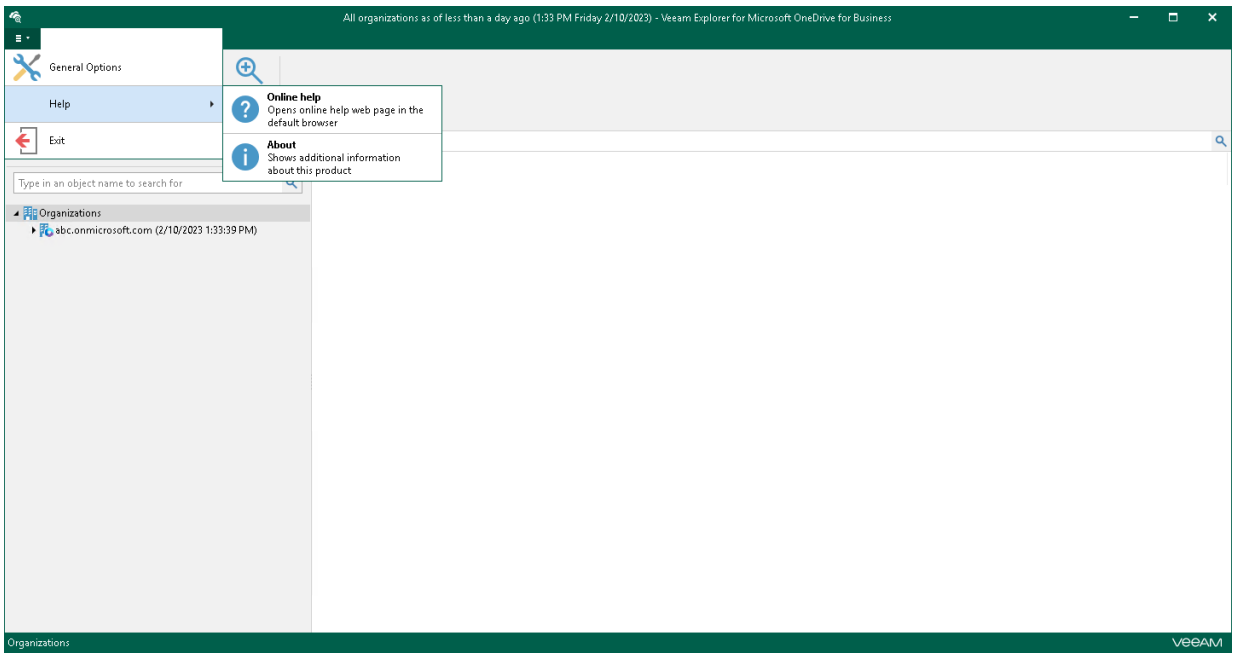
The user interface of Veeam Explorer for Microsoft OneDrive for Business is designed to let you quickly find commands that you need to restore Microsoft OneDrive data from backups created by Veeam Backup for Microsoft 365.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings. For more information, see General Application Settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft OneDrive for Business window.

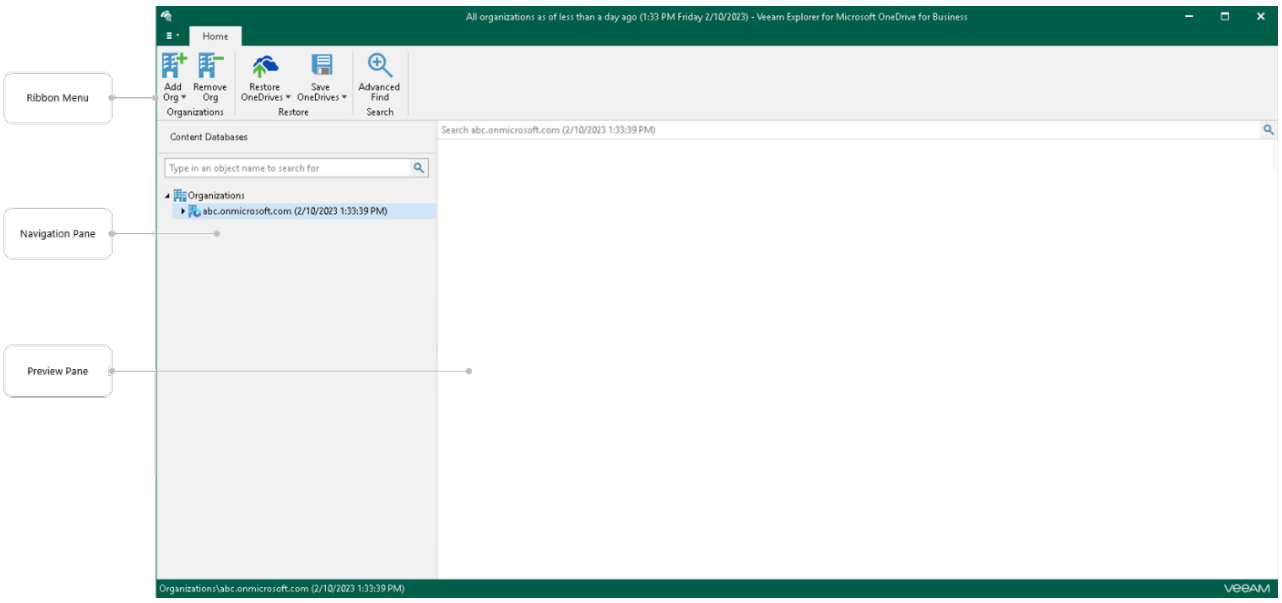
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft OneDrive for Business wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.
- The navigation pane that allows you to browse through the hierarchy of folders with backed-up data. Also, it allows you to search for OneDrives using keywords.
- The preview pane that provides search capabilities and allows you to view details about items that are contained in a folder you have selected in the navigation pane.



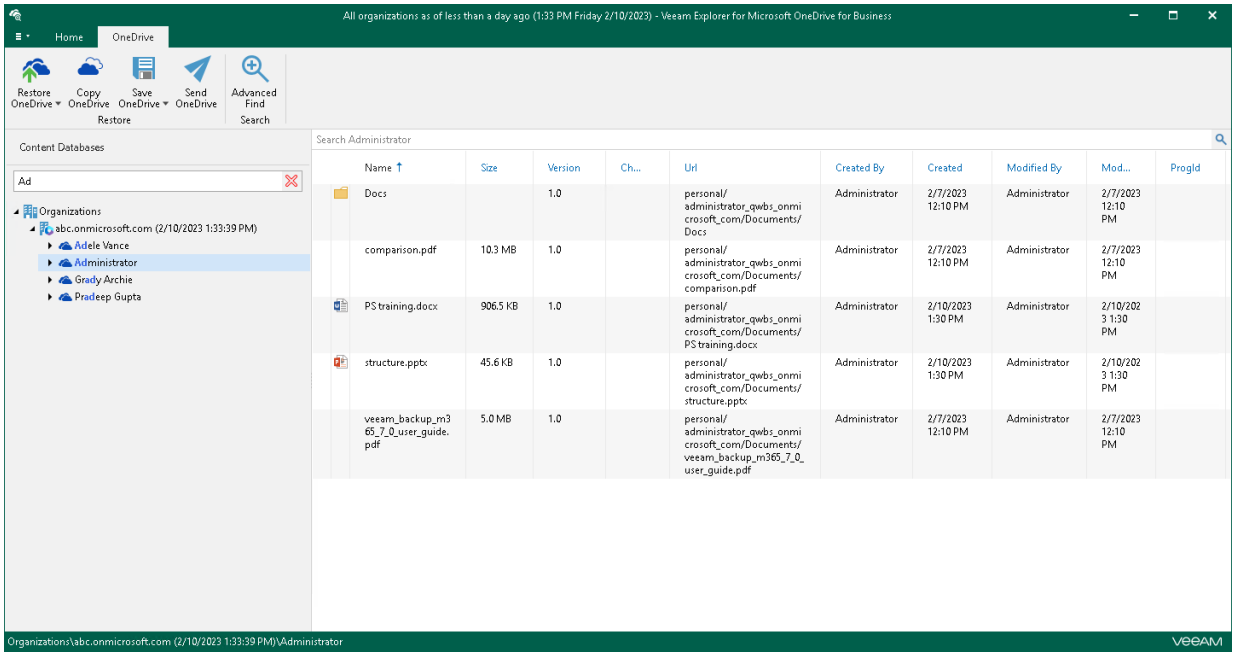
Browsing, Searching and Viewing Items

You can use Veeam Explorer for Microsoft OneDrive for Business to view the contents of a backup file, view object properties, open files, search for OneDrives and for items in a backup file as well as customize criteria of your search.

Searching for OneDrives

You can use keywords to search for OneDrives in the database structure containing your OneDrive objects. To do this, enter a search query in the search field at the top of the navigation pane.

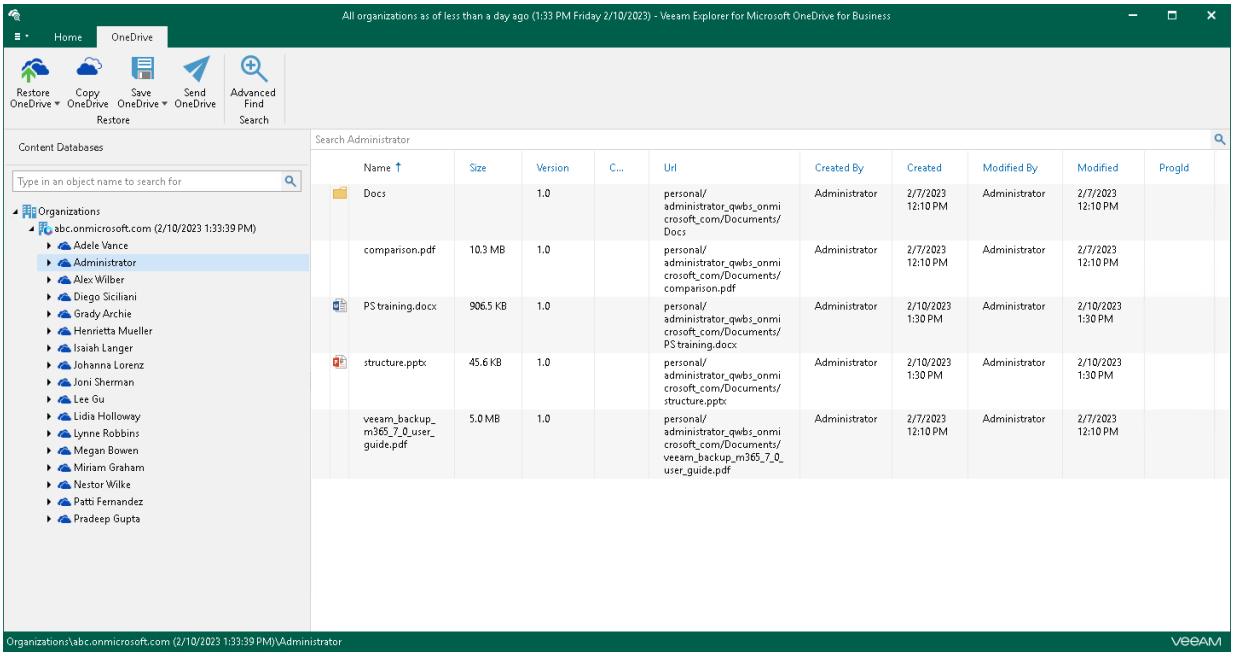
To remove a keyword, click the cross mark.



Browsing Backup Content

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your OneDrive objects.

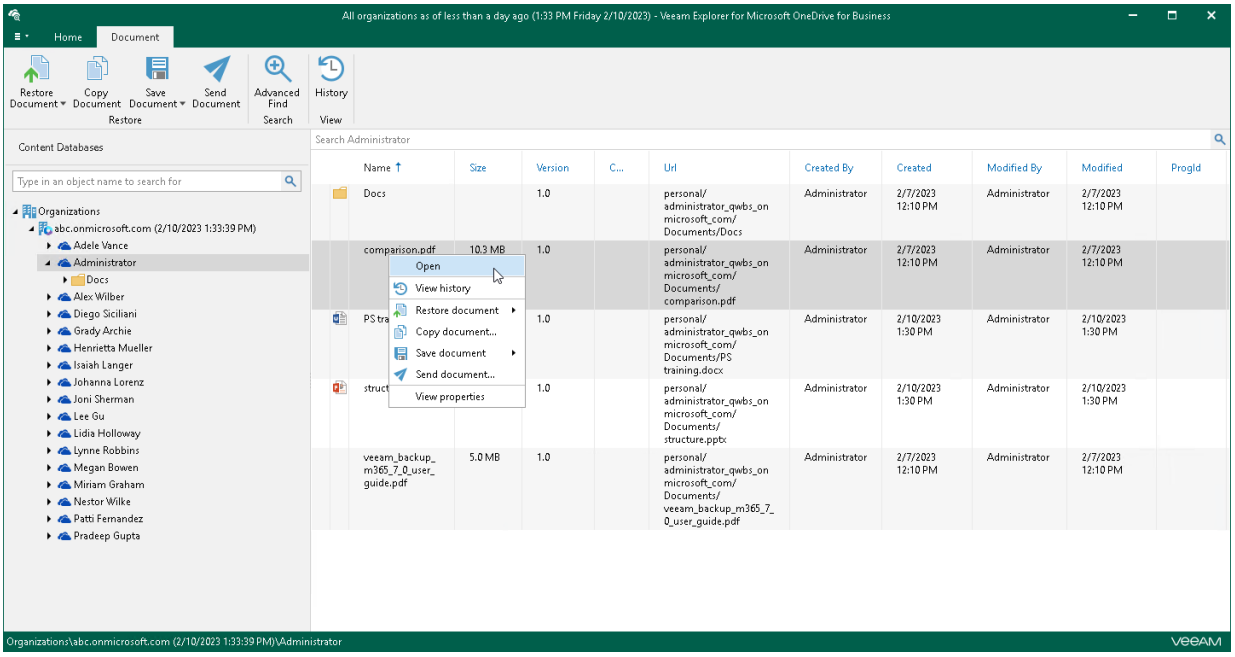
After you select an object in the navigation pane, you can see its content in the preview pane.



Viewing Objects Properties and Opening Files

To view object properties, right-click an object in the preview pane and select **View properties**.

To open a document using an associated application, right-click a document in the preview pane and select **Open**.



Searching for Objects in Backup File

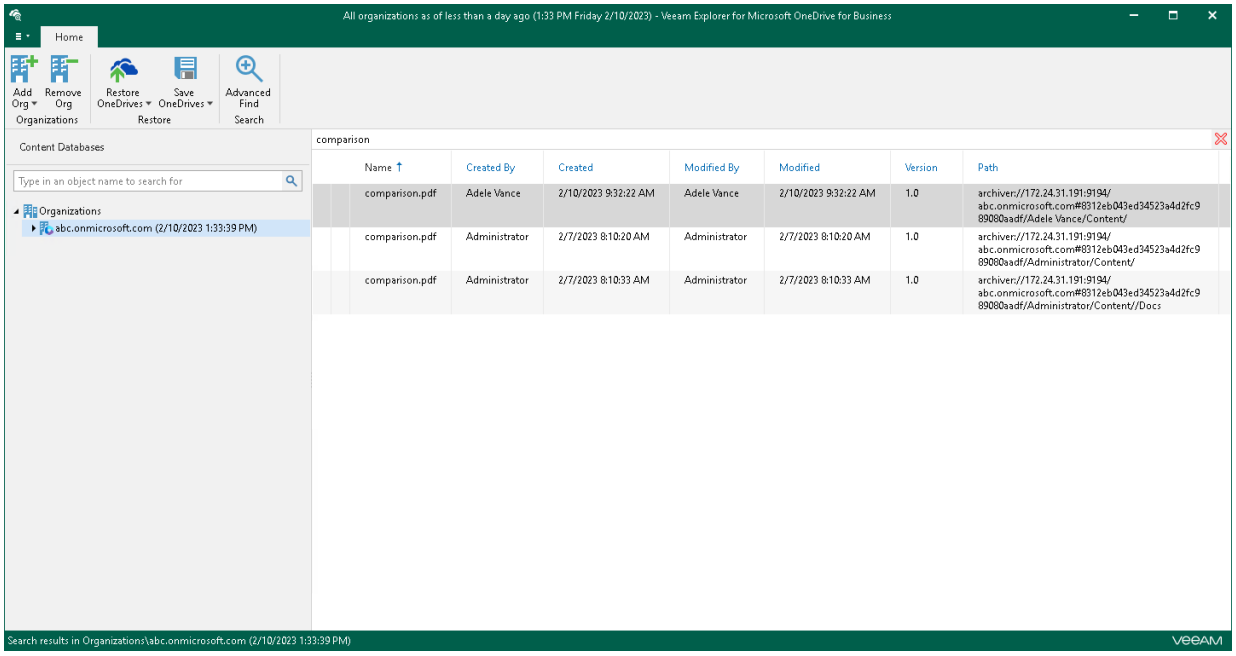
The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find your data.
2. Enter a search query in the search field at the top of the preview pane.

> **NOTE**
>
> To find the exact phrase, use double quotes. For example, "*Attachments*".

You can narrow your search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



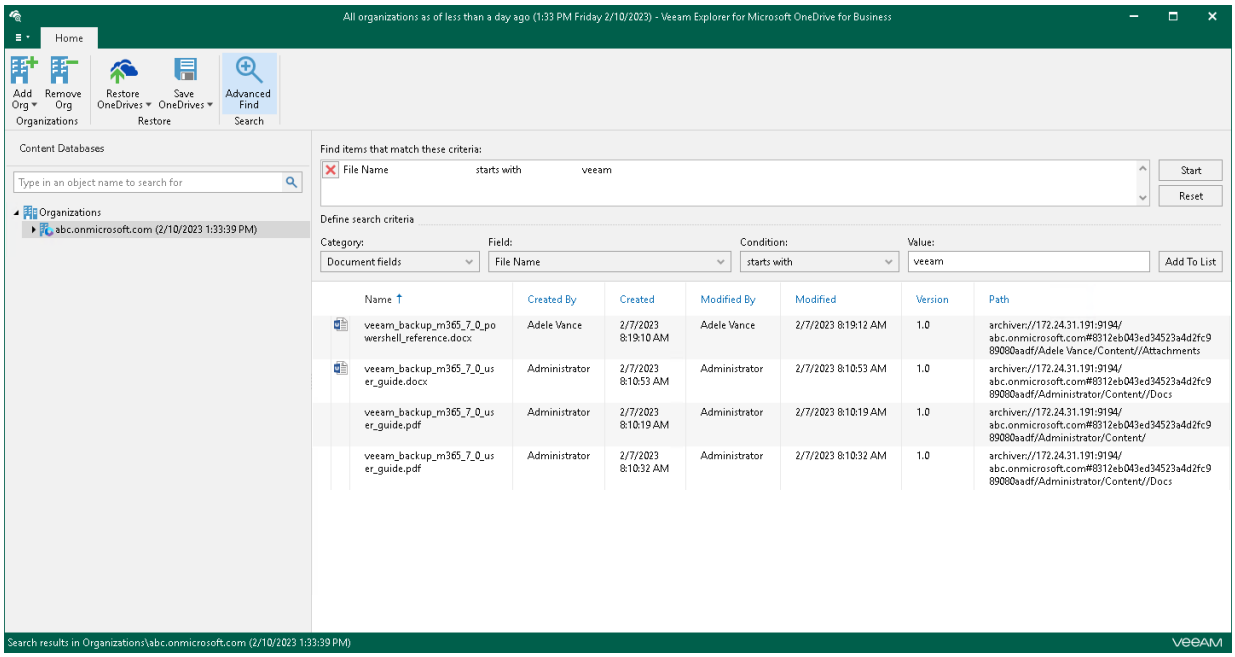
Using Advanced Find

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find an object that starts with the word *Document*, do the following:

1. In the preview pane, select a node and click **Advanced Find** on the ribbon.
2. In the **Define search criteria** section, select **Category** > **Document fields**.
3. In the **Field** list, select **File Name**.
4. In the **Condition** list, select **starts with**.
5. In the **Value** field, specify a file name.
6. Click **Add to List** and then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



General Application Settings

You can configure general settings for Veeam Explorer for Microsoft OneDrive for Business.

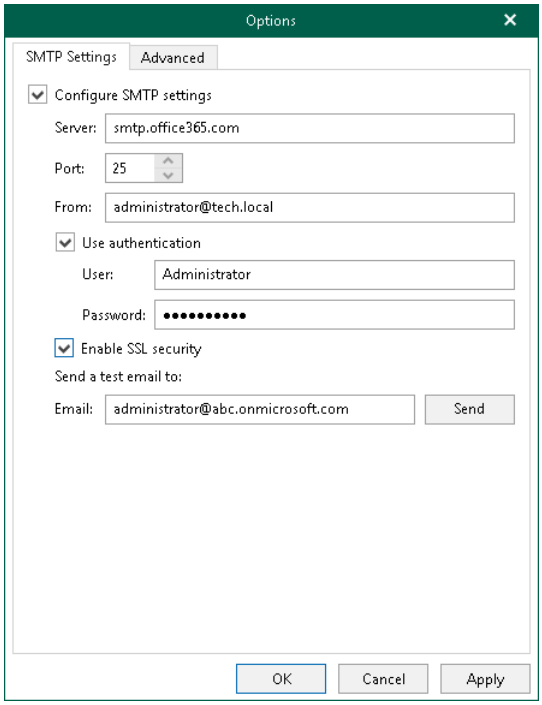
SMTP Settings

To send Microsoft OneDrive items as attachments, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
   a. In the **Server** field, specify a DNS name or IP address of the SMTP server.
   b. In the **Port** field, specify a port number of the specified SMTP server.

      The default port number is *25*. If you want to use SSL data encryption, specify port *587*.
   c. In the **From** field, specify the sender email address. This address will appear in the **From** field when sending OneDrive items. See Sending Microsoft OneDrive Documents.
   d. If the specified SMTP server requires an authentication for outgoing mail, select the **Use authentication** check box and provide valid credentials.
   e. Select the **Enable SSL security** check box to enable SSL data encryption.
4. Click **Send** to send a test email message.
5. Click **OK**.



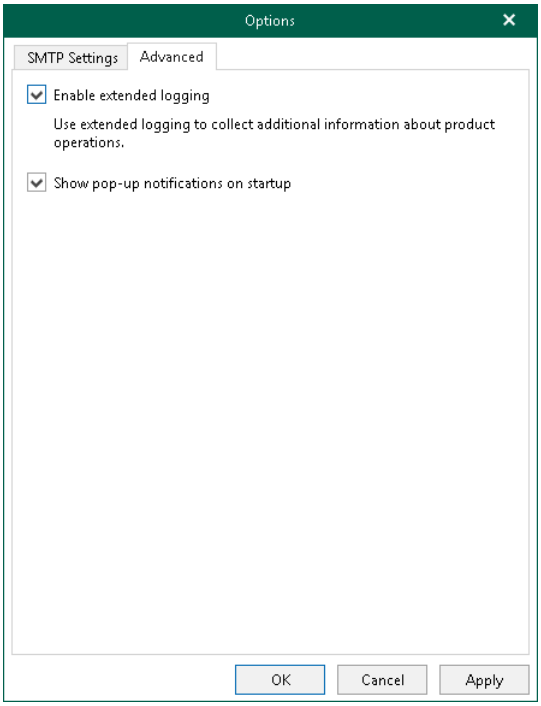
Advanced Settings

Veeam Explorer for Microsoft OneDrive for Business allows you to configure advanced settings such as extended logging mode and pop-up notifications.

To configure advanced settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Advanced** tab.
3. If you want to enable extended logging mode to collect logs that contain additional information on specific operations, select the **Enable extended logging** check box.

   After enabling extended logging mode, you can go back to the application and perform actions for which you want to collect additional information. Then you can collect logs.
4. By default, Veeam Explorer for Microsoft OneDrive for Business displays notifications when loading backups created by Veeam Backup for Microsoft 365 from object storage. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.
5. Click **OK**.



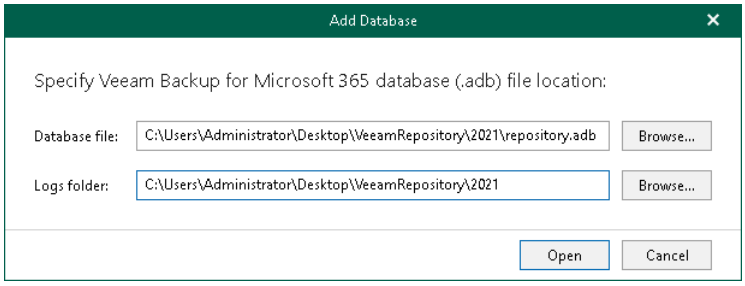
Standalone Databases

You can add standalone databases to the Veeam Explorer for Microsoft OneDrive for Business scope and connect to a Veeam Backup for Microsoft 365 server and service provider server to view backups located on these servers.

Adding Veeam Backup for Microsoft 365 Databases

To manually add databases that store Microsoft 365 organization data, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 database** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 database**.
2. Specify the database file location and log directory.
3. Click **Open**.



NOTE

Make sure you have disabled the *Veeam Backup Proxy for Microsoft 365 Service* when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will not be able to access the database due to database lock.

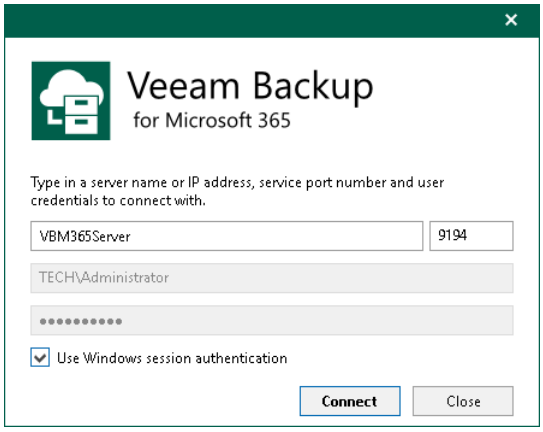
Adding Veeam Backup for Microsoft 365 Server

You can use the built-in Veeam Explorer for Microsoft OneDrive for Business abilities to connect to another Veeam Backup for Microsoft 365 server and add its databases to the Veeam Explorer for Microsoft OneDrive for Business scope.

To connect to another Veeam Backup for Microsoft 365 server remotely, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 server** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 server**.
2. Specify a server name or IP address and enter credentials to access the specified server.

   Select the **Use Windows session authentication** check box to connect with the user account under which you are currently logged in.
3. Click **Connect**.



Adding Veeam Backup for Microsoft 365 Service Provider

In Veeam Explorer for Microsoft OneDrive for Business, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.

> **NOTE**
>
> Make sure that both Veeam Explorer for Microsoft OneDrive for Business and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication. For more information, see the Connecting to Service Providers section of the Veeam Cloud Connect Guide.

To add Veeam Backup for Microsoft 365 service providers, do the following:

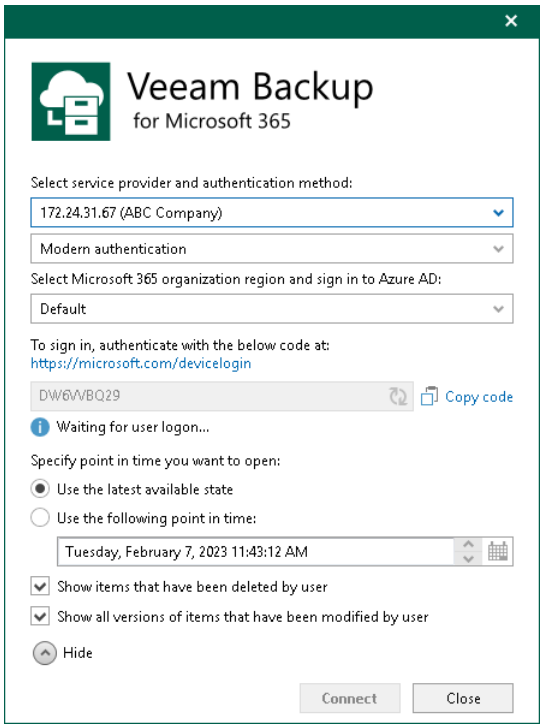
1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 service provider** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 service provider**.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and select an authentication method that can be either *Modern authentication* or *Basic authentication*.
3. [For *Modern authentication*] Select a region to which a Microsoft 365 organization of the selected service provider belongs.
4. [For *Modern authentication*] Copy the device code and use it to sign in to Azure Active Directory.

   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.

   > **NOTE**
   >
   > You cannot use *Basic authentication* to load backups if a Microsoft 365 organization has been added to the service provider infrastructure using *Modern authentication*.
5. Select a point-in-time state as of which you want to load Microsoft 365 backups.

   To select a point in time, use the calendar control.
6. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
7. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.

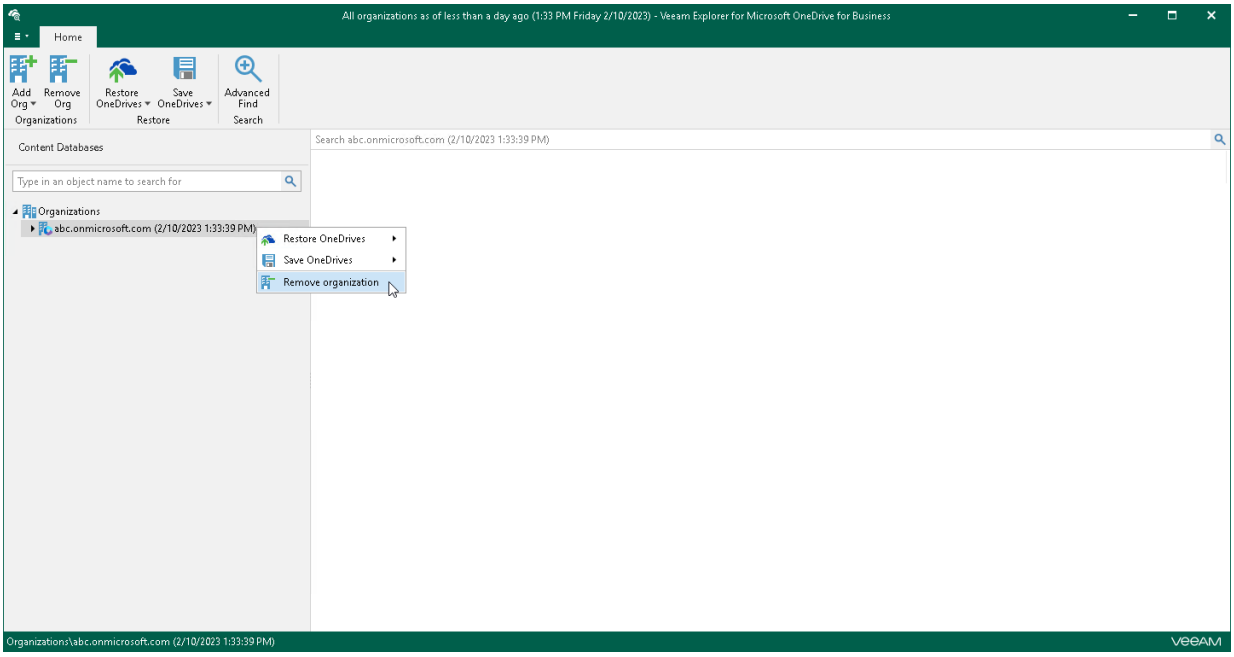
8. Click **Connect**.



Removing Organizations

Veeam Explorer for Microsoft OneDrive for Business allows you to remove an organization from the application scope when you no longer need it.

To remove an organization from the application scope, right-click an organization in the navigation pane and select **Remove organization**.



Data Restore

You can use Veeam Explorer for Microsoft OneDrive for Business to restore data to Microsoft 365 organizations.

> **NOTE**
>
> By default, Veeam Explorer for Microsoft OneDrive for Business restores only the latest version of OneDrive items to their original location. If you want to restore all versions of OneDrive items and specify another location, you can copy your OneDrive data. For more information, see Data Copy.

Restoring Single OneDrive

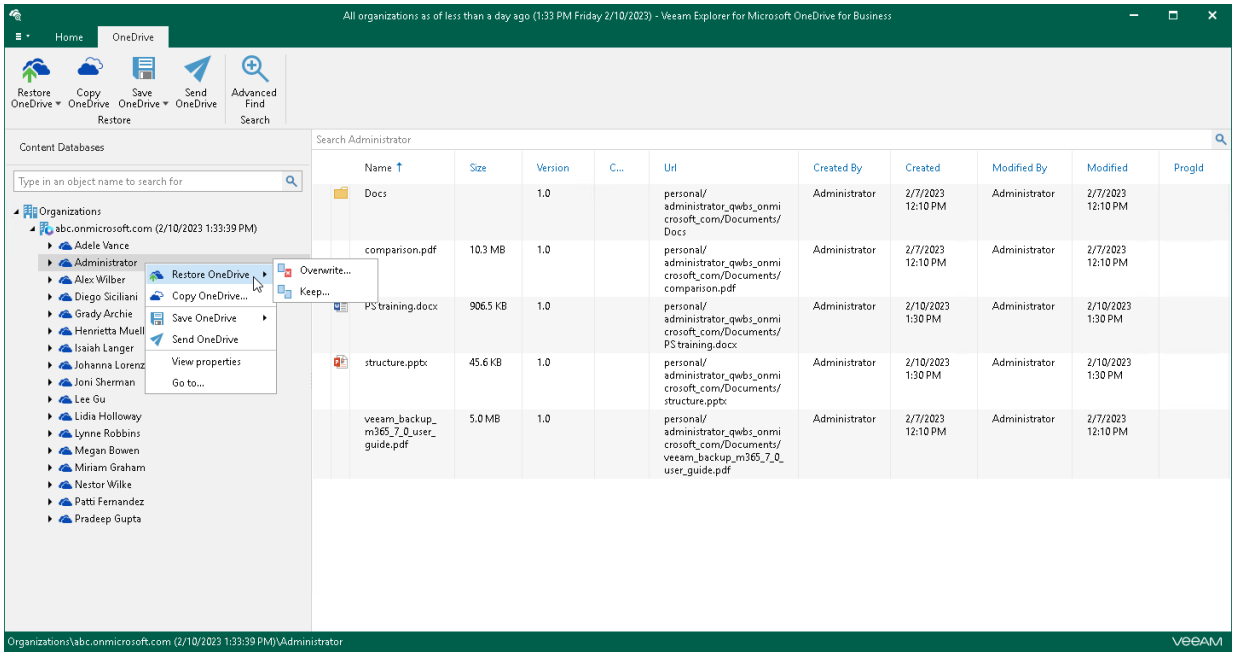
To restore data of a single OneDrive, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.

Step 1. Launch Restore Wizard

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

1. Select an object that you want to restore:
   - To restore OneDrive, select the necessary OneDrive in the navigation pane.
   - To restore a folder, select the necessary folder in the navigation pane.
   - To restore a document, select a folder that contains the document in the navigation pane and then select the document in the preview pane.
2. Do one of the following:
   - On the **OneDrive/Folder/Document** tab, click **Restore OneDrive/Restore Folder/Restore Document** on the ribbon **and select one of the following options:**
     - **Overwrite** — to completely overwrite existing OneDrive data.
     - **Keep** — to preserve existing data and restore items with the `RESTORED` prefix (`RESTORED-<file_name>.ext`).
   - Right-click an object that you want to restore and select **Restore OneDrive/Restore folder/Restore document** > **Overwrite** or **Restore OneDrive/Restore folder/Restore document** > **Keep**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

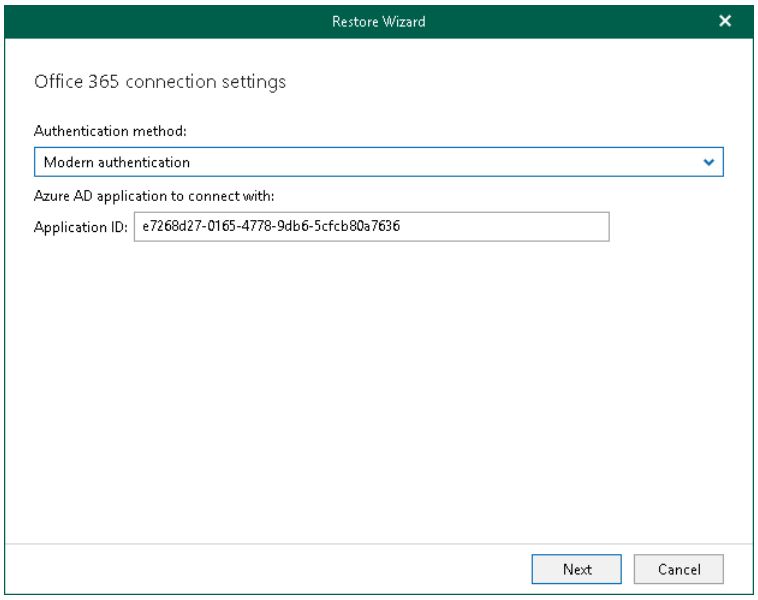
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

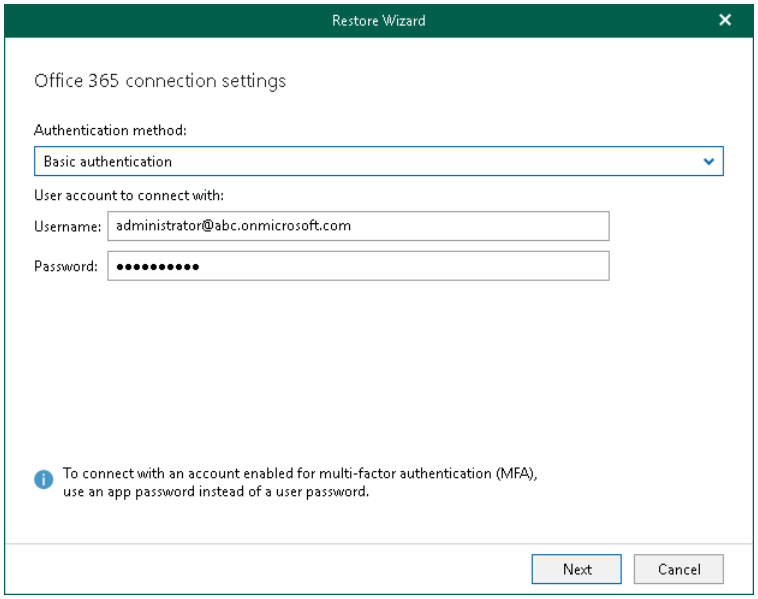
   By default, Veeam Explorer for Microsoft OneDrive for Business populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

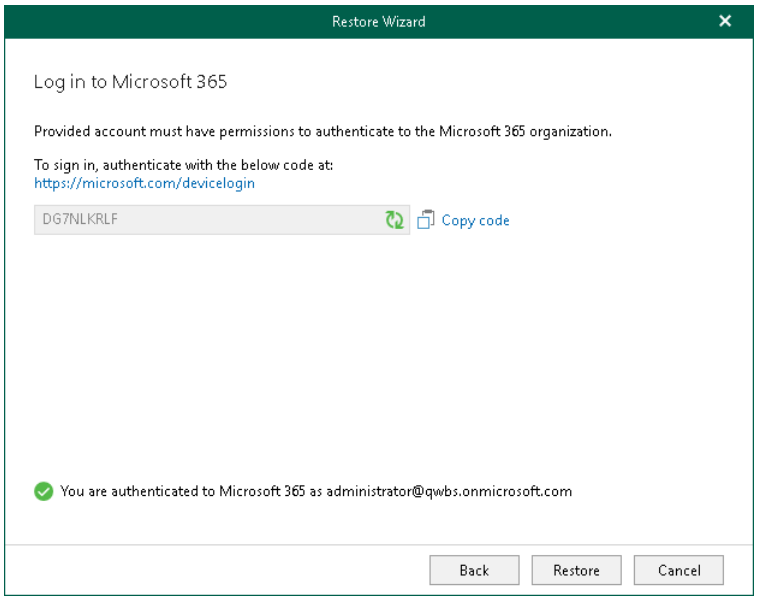
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For Veeam Explorer for Microsoft OneDrive for Business, required permissions are the same as for Veeam Explorer for Microsoft SharePoint. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Restore**.



Restoring Multiple OneDrives

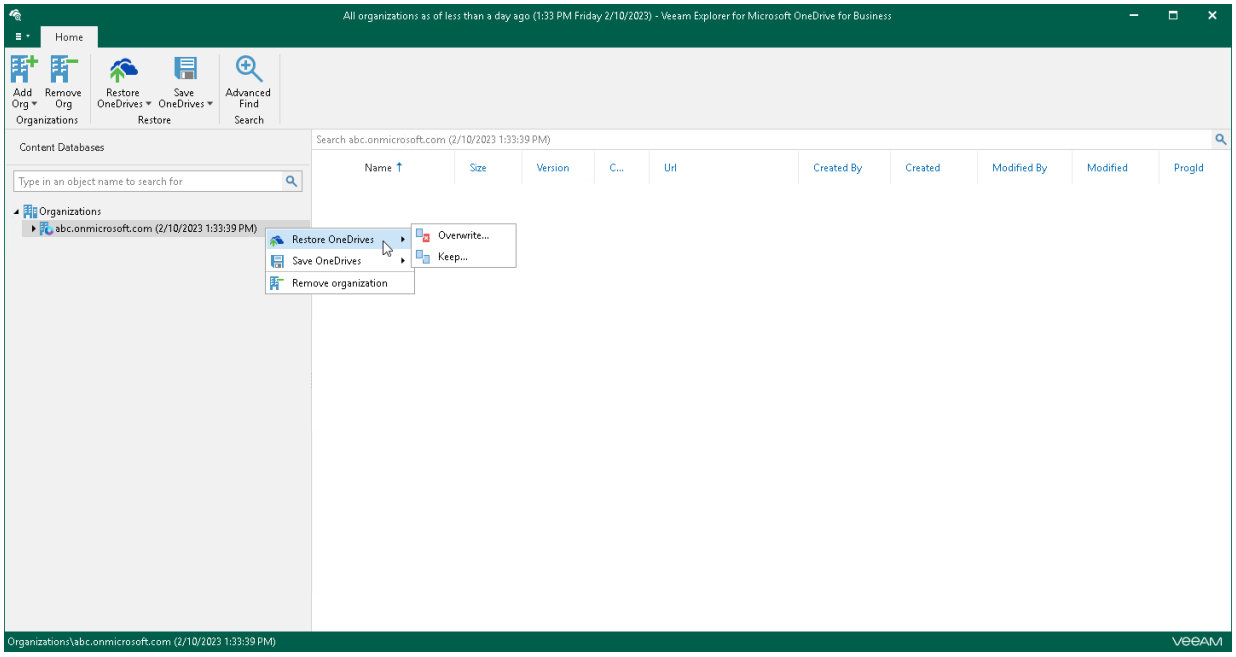
To restore multiple OneDrives, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Select OneDrives.

Step 1. Launch Restore Wizard

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

1. In the navigation pane, select an organization with OneDrives.
2. Do one of the following:
   - On the **Home** tab, click **Restore OneDrives** on the ribbon and select one of the following options:
     - **Overwrite** — to completely overwrite existing OneDrives.
     - **Keep** — to preserve existing data and restore items with the `RESTORED` prefix (`RESTORED-<file_name>.ext`).
   - Right-click an organization with OneDrives and select **Restore OneDrives** > **Overwrite** or **Restore OneDrives** > **Keep**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

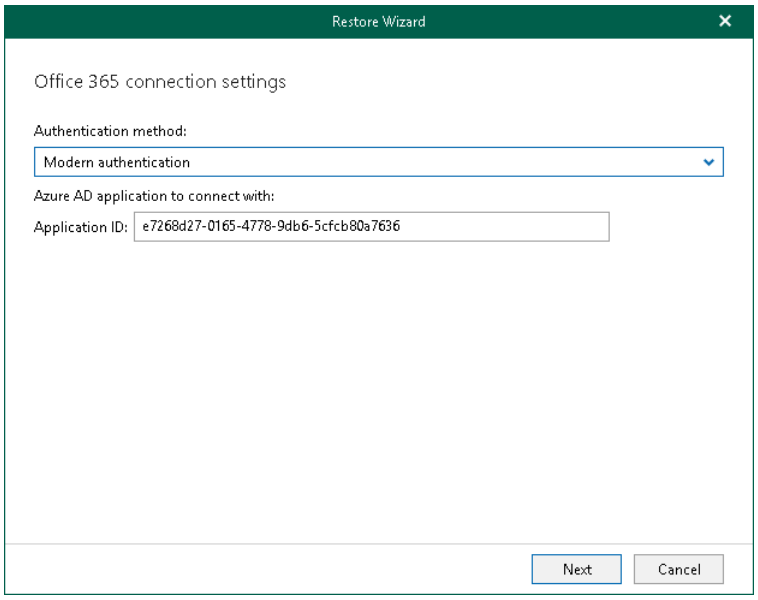
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

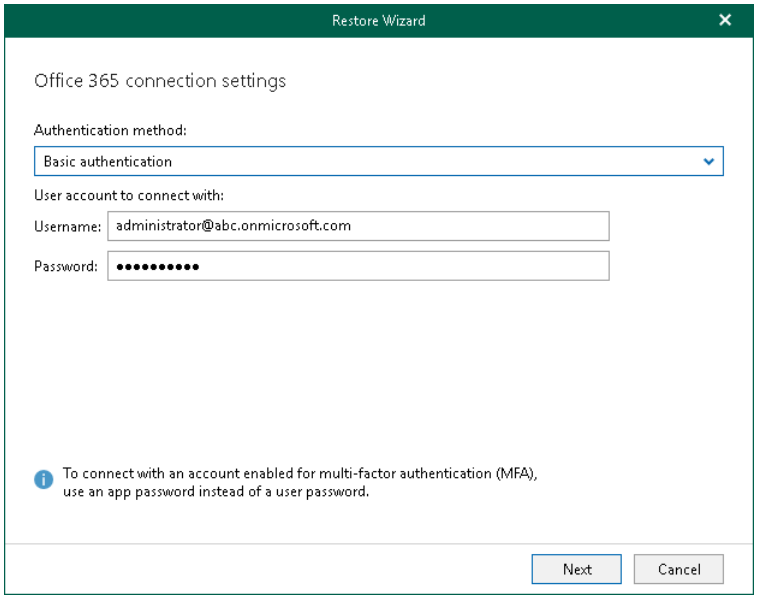
   By default, Veeam Explorer for Microsoft OneDrive for Business populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

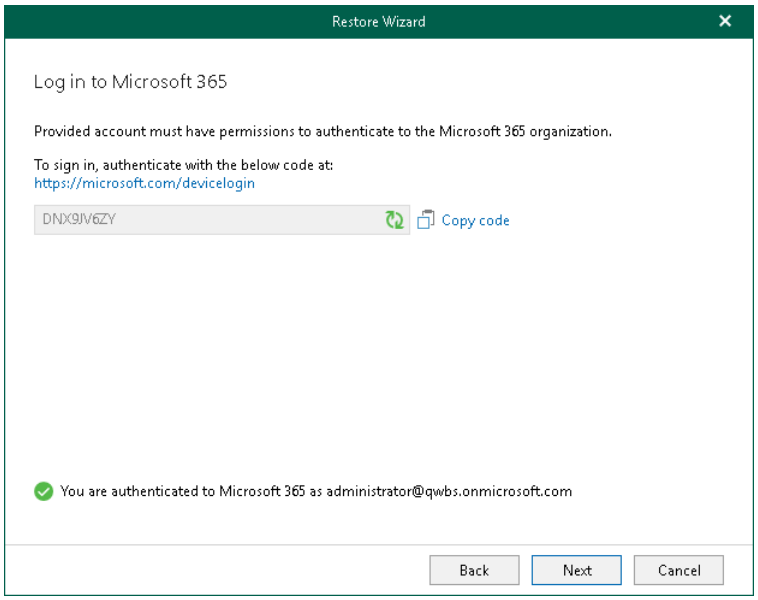
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For Veeam Explorer for Microsoft OneDrive for Business, required permissions are the same as for Veeam Explorer for Microsoft SharePoint. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

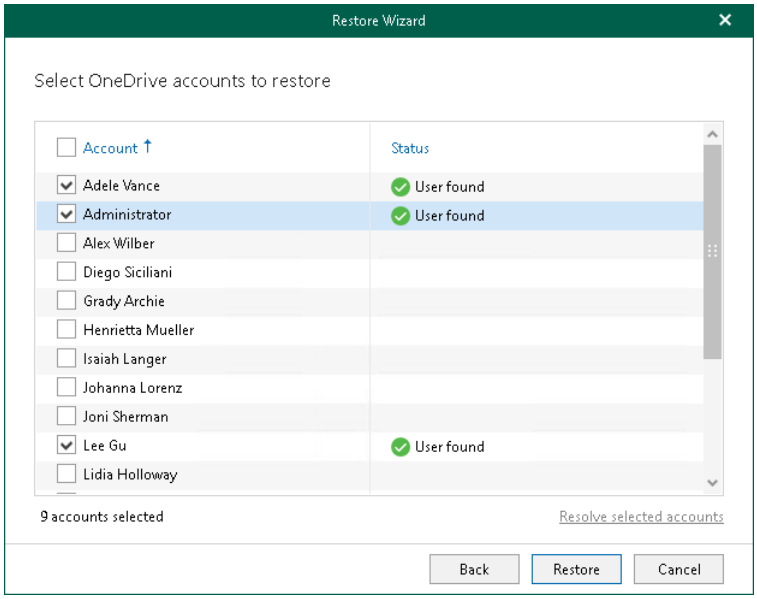
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Select OneDrives

At this step of the wizard, select OneDrives that you want to restore and click **Restore**.

If you want to check whether user accounts whose OneDrives you want to restore exist, click **Resolve selected accounts**.



Data Copy

You can use Veeam Explorer for Microsoft OneDrive for Business to copy OneDrive data to a different location.

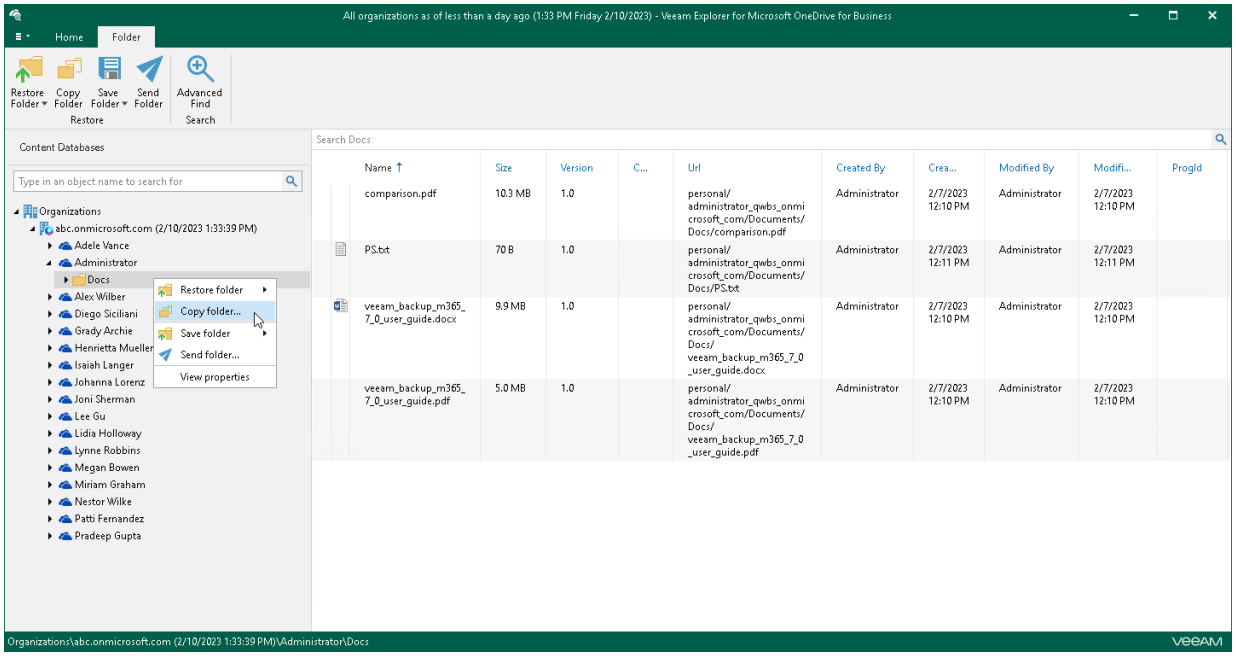
To copy OneDrive data to the same or different user, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify a target user.
5. Specify a target folder.
6. Specify restore options.

Step 1. Launch Restore Wizard

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

1. Select an object that you want to copy:
   - To copy OneDrive, select the necessary OneDrive in the navigation pane.
   - To copy a folder, select the necessary folder in the navigation pane.
   - To copy a document, select a folder that contains the document in the navigation pane and then select the document in the preview pane.
2. Do one of the following:
   - On the **OneDrive/Folder/Document** tab, click **Copy OneDrive/Copy Folder/Copy Document** on the ribbon.
   - Right-click an object that you want to copy and select **Copy OneDrive/Copy folder/Copy document**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

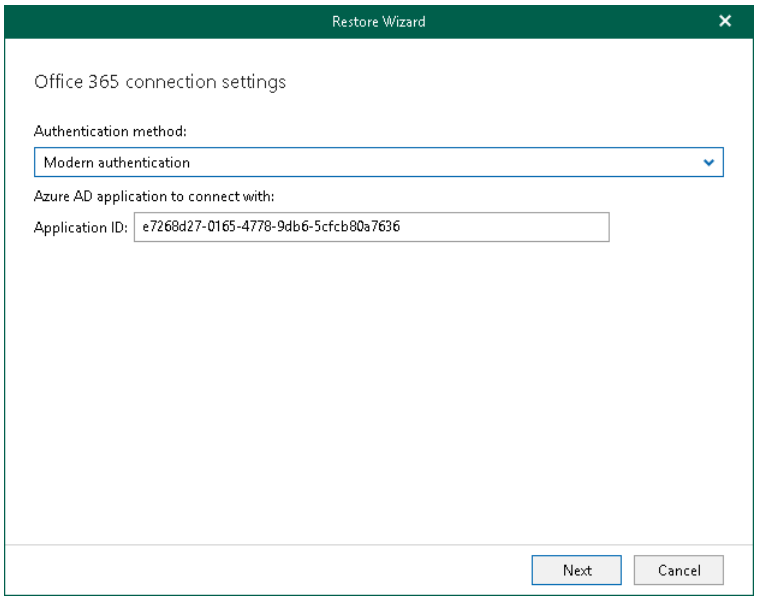
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified object back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

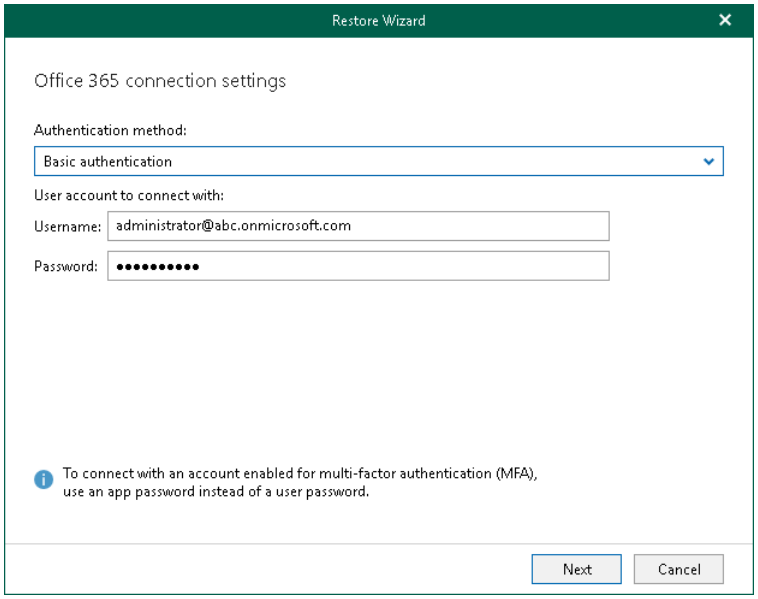
   By default, Veeam Explorer for Microsoft OneDrive for Business populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the SharePoint organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

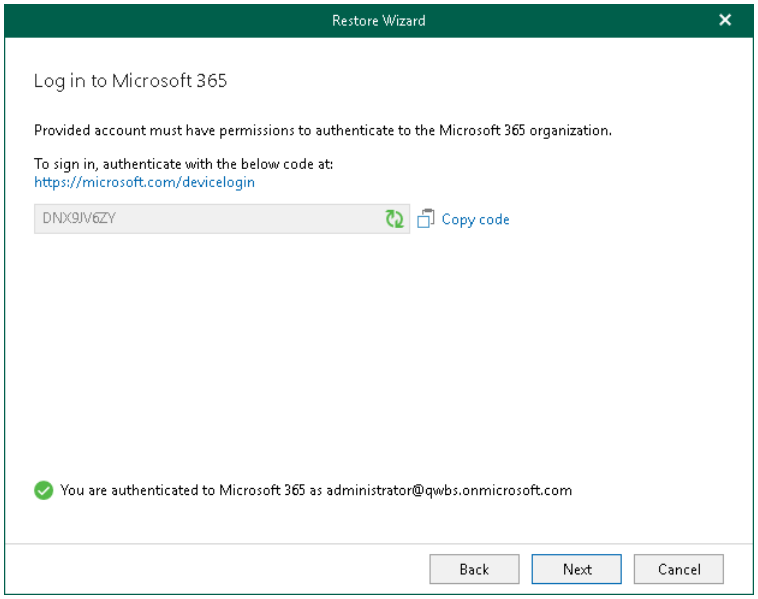
2. Click the Microsoft authentication portal link.

   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has the *SharePoint Administrator* role.

4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Specify Target User

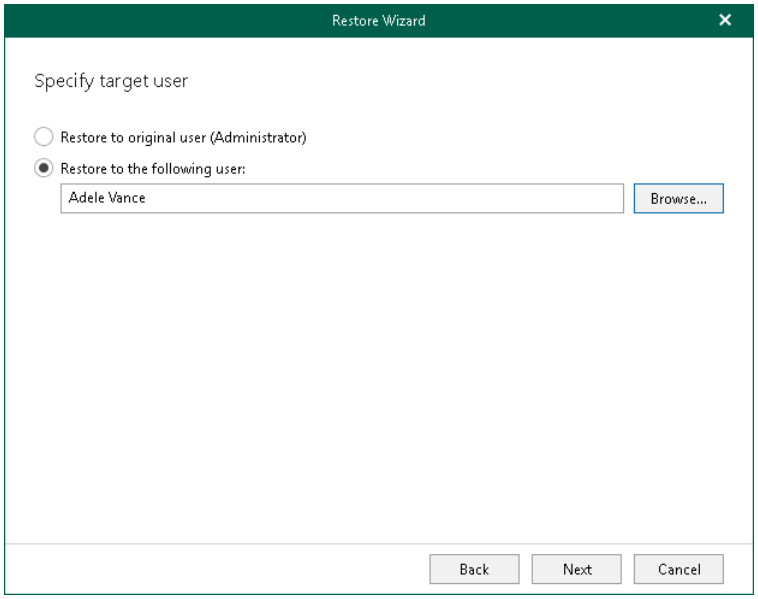
At this step of the wizard, specify a target user where you want to copy data.

You can select one of the following options:

- **Restore to original user**. To copy OneDrive data back to the original user.
- **Restore to the following user**. To copy OneDrive data to the specified user.

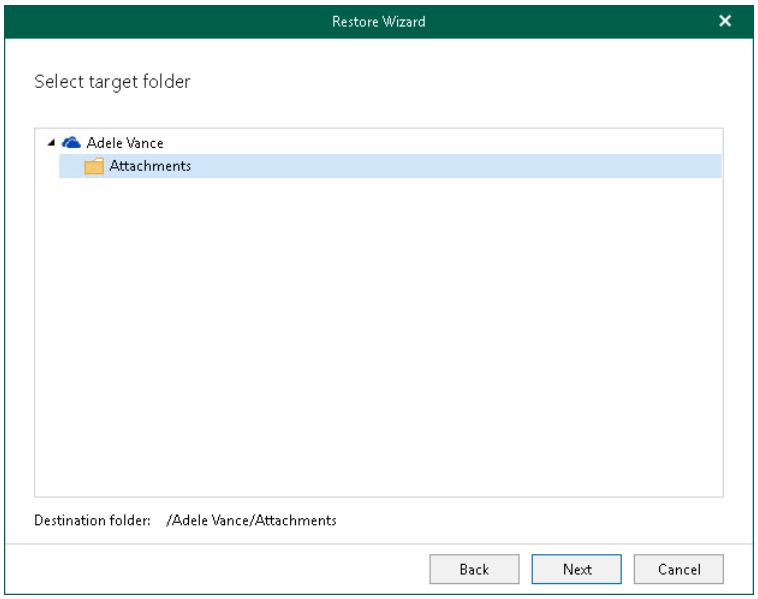
To select a target user, do the following:

1. Click **Browse**.
2. In the **Browse OneDrive Accounts** window, select the necessary account and click **Select**.



Step 5. Specify Target Folder

At this step of the wizard, specify the target folder to which you want to copy data.



Step 6. Specify Restore Options

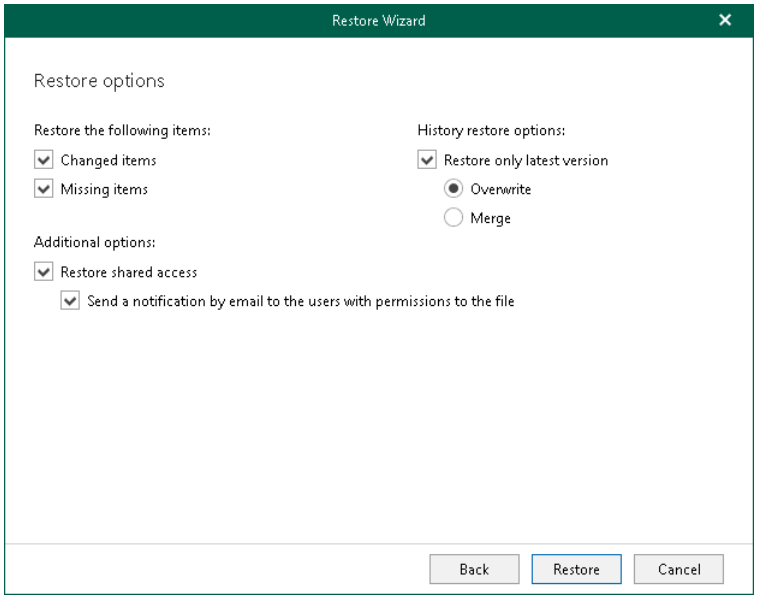
At this step of the wizard, select check boxes next to the restore options that you want to apply and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to restore data that has been modified in your production environment.
- **Missing items**. Allows you to restore missing items.
- **Restore only latest version**. Allows you to restore only the latest version of items. If this check box is selected, you can select one of the following options:
  - **Overwrite**. To overwrite data in the production environment.
  - **Merge**. To merge an existing and a backup version of items.

  If the **Restore only latest version** check box is not selected, all versions of items in the production environment will be replaced with the relevant data from the backup file.
- **Restore shared access**. Allows you to restore shared access.
- **Send a notification by email to the users with permissions to the file**. Select this check box if you want to notify users about items restore. Veeam Explorer for Microsoft OneDrive for Business will notify users with whom items have been shared. You can select this check box only if the **Restore shared access** check box is selected.

> **NOTE**
>
> The **Send a notification by email to the users with permissions to the file** check box is only available when restoring data from backups created by Veeam Backup for Microsoft 365 for Microsoft 365 organizations.



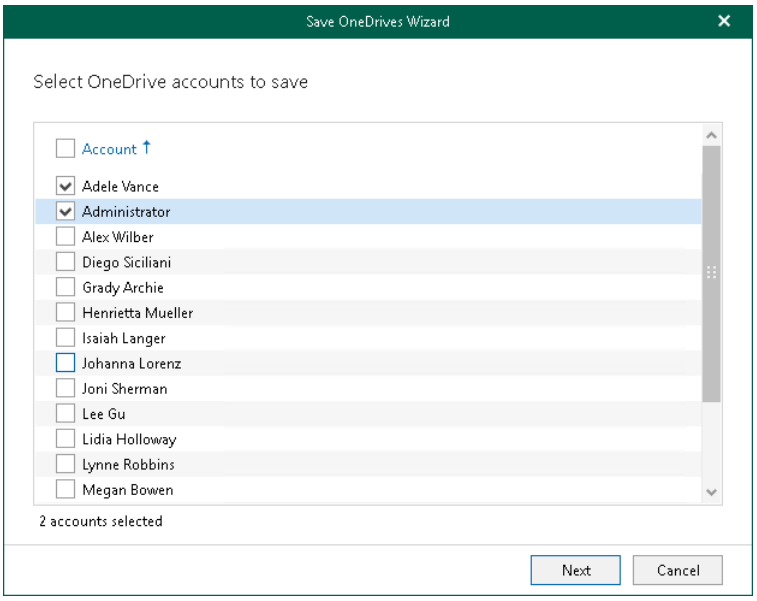
Saving Microsoft OneDrives

Veeam Explorer for Microsoft OneDrive for Business allows you to save OneDrive content to the specified location.

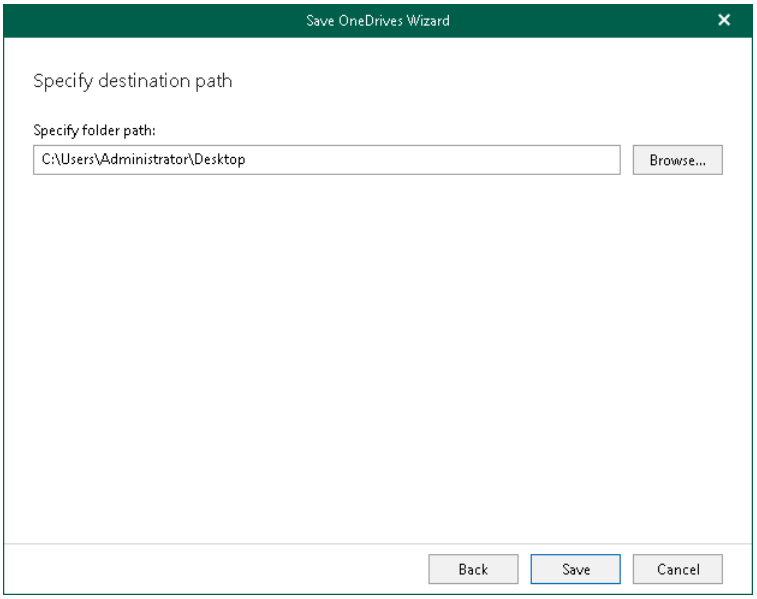
Saving Multiple OneDrives

To save data of multiple OneDrives, do the following:

1. In the navigation pane, select an organization with OneDrives.
2. Do one of the following:
   - On the **Home** tab, click **Save OneDrives** on the ribbon and select how you want to save data:
     - **Save as files**. Select this option if you want to save each file separately to a specified location.
     - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. Veeam Explorer for Microsoft OneDrive for Business will save files to an archive with the *OneDrives_<timestamp>.zip* name.
   - Right-click an organization with OneDrives and select **Save OneDrives** > **Save as files** or **Save OneDrives** > **Save as ZIP**.
3. In the **Save OneDrives Wizard** wizard, select OneDrive accounts to save.



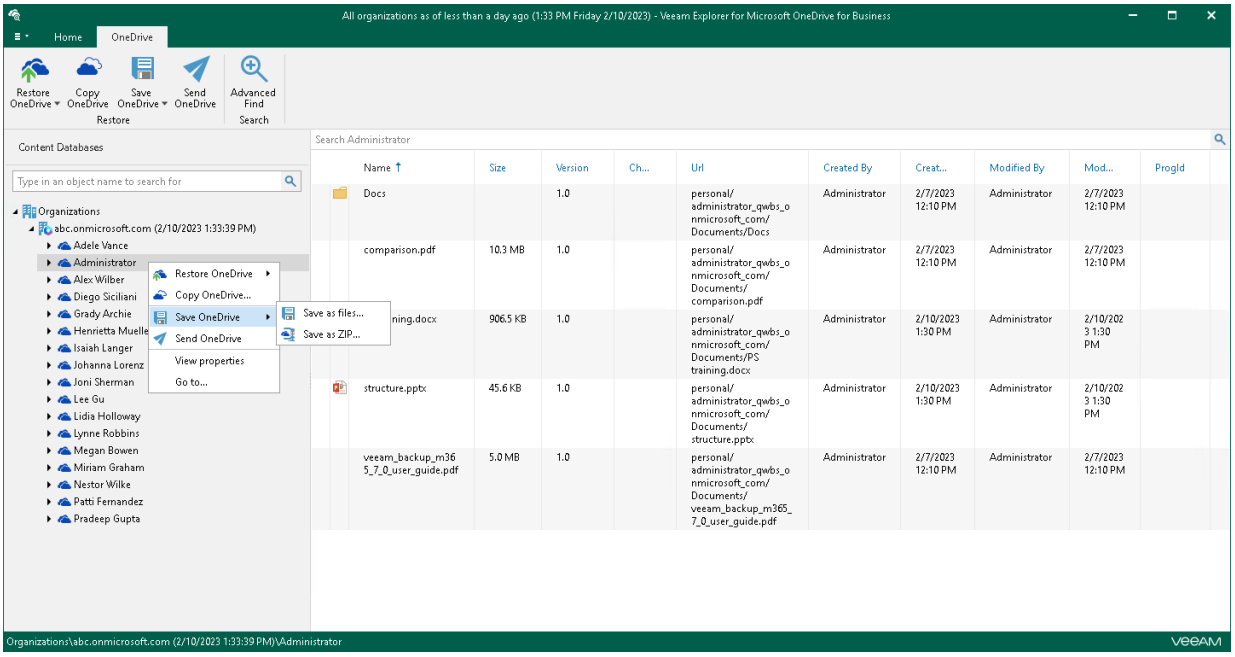
4. Specify a folder where to save OneDrive data and click **Save**.



Saving Individual OneDrives

To save data of a specific OneDrive, do the following:

1. In the navigation pane, select OneDrive.
2. Do one of the following:
   - On the **OneDrive** tab, click **Save OneDrive** on the ribbon and select how you want to save data:
     - **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
     - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Save**. Veeam Explorer for Microsoft OneDrive for Business will save files to an archive with the *<user_name>.zip* name in this folder.
   - Right-click OneDrive and select **Save OneDrive** > **Save as files** or **Save OneDrive** > **Save as ZIP**.



Saving Microsoft OneDrive Documents and Folders

Veeam Explorer for Microsoft OneDrive for Business allows you to save documents and folders located in Microsoft OneDrive to a specified location.

To save a folder, do the following:

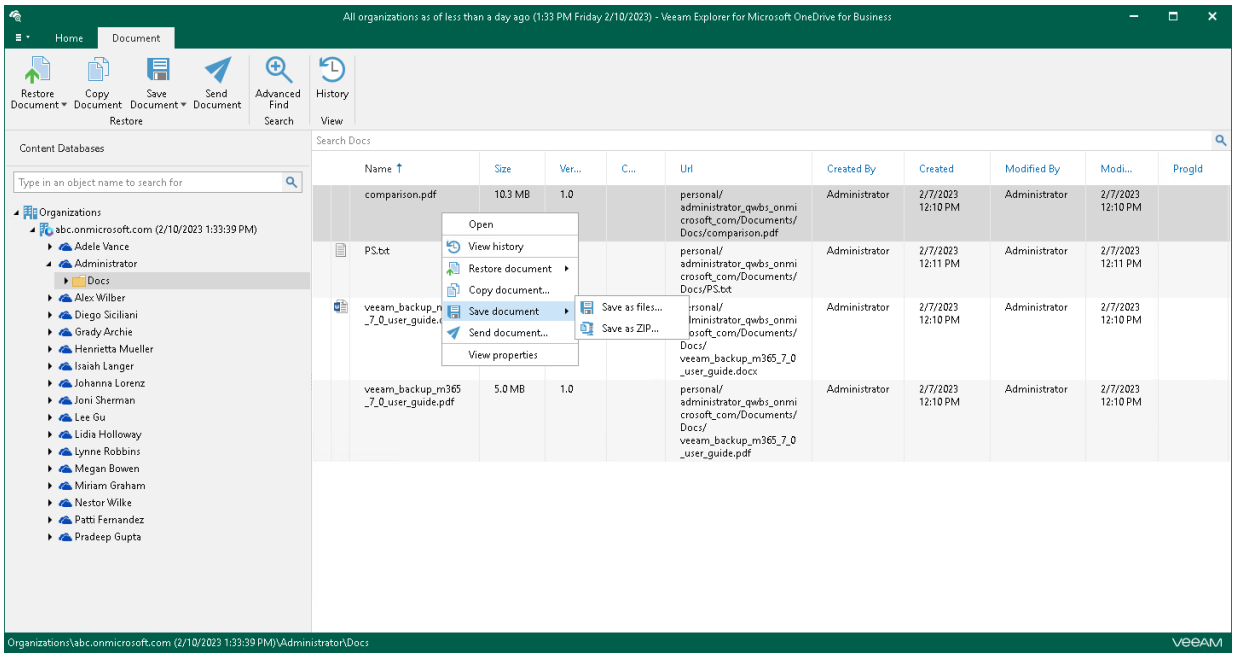
1. In the navigation pane, select a folder that you want to save.
2. Do one of the following:
   - On the **Folder** tab, click **Save Folder** > **Save folder as files** or **Save Folder** > **Save folder as ZIP** on the ribbon.
   - Right-click a folder and select **Save folder** > **Save folder as files** or **Save folder** > **Save folder as ZIP**.
3. In the displayed window, browse to the necessary folder and click **Select Folder** or **Save**.

   Keep in mind that if you select the **Save as ZIP** option, Veeam Explorer for Microsoft OneDrive for Business will save a folder to an archive with the *archive.zip* name.

To save a document, do the following:

1. In the preview pane, select a document that you want to save.
2. Do one of the following:
   - On the **Document** tab, click **Save Document** > **Save as files** or **Save Document** > **Save as ZIP** on the ribbon.
   - Right-click a document and select **Save document** > **Save as files** or **Save document** > **Save as ZIP**.
3. In the displayed window, browse to the necessary folder and click **Select Folder** or **Save**.

   Keep in mind that if you select the **Save as ZIP** option, Veeam Explorer for Microsoft OneDrive for Business will save a document to an archive with the *archive.zip* name.



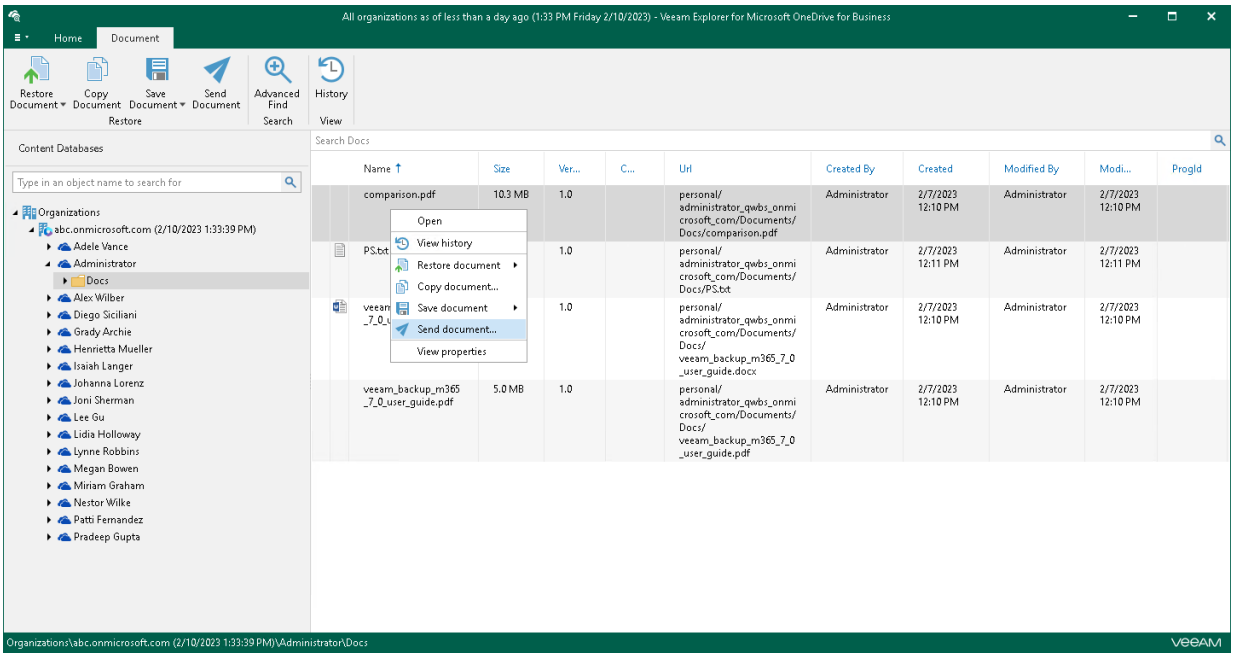
Sending Microsoft OneDrive Data

Veeam Explorer for Microsoft OneDrive for Business allows you to send OneDrive data to specified recipients through email.

> **TIP**
>
> Before sending documents, make sure to configure SMTP settings. The amount of data you can send at a time depends on your SMTP server configuration. For more information about configuring SMTP settings, see SMTP Settings.

To send OneDrive data through email, do the following:

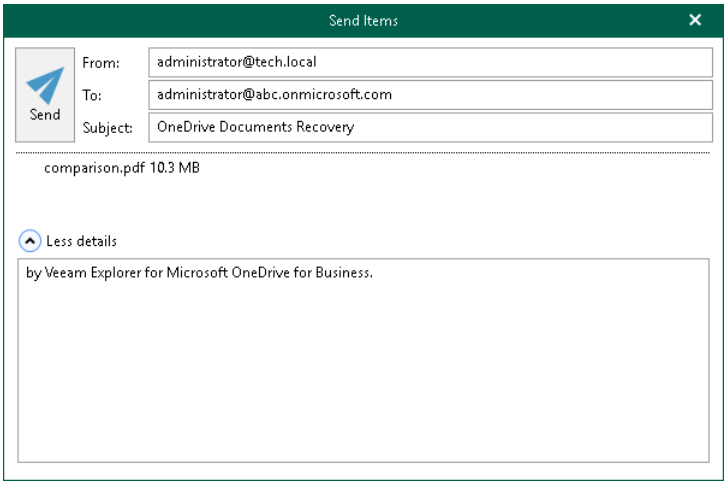
1. Select an object that you want to send through email:
   - To send OneDrive, select the necessary OneDrive in the navigation pane.
   - To send a folder, select the necessary folder in the navigation pane.
   - To send a document, select a folder that contains the document in the navigation pane and then select the document in the preview pane.
2. Do one of the following:
   - On the **OneDrive/Folder/Document** tab, click **Send OneDrive/Send Folder/Send Document** on the ribbon.
   - Right-click an object that you want to send and select **Send OneDrive/Send folder/Send document**.



3. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

You can also edit the message subject and body. To edit the message body, click **More details**.



Veeam Explorer for Microsoft Teams

Veeam Explorer for Microsoft Teams allows you to restore and export Microsoft Teams data from backups created by Veeam Backup for Microsoft 365.

Planning and Preparation

You can configure your environment before you start using Veeam Explorer for Microsoft Teams.

Ports

For restore of Microsoft Teams data, you must open the same ports that are required for restore of Microsoft Exchange and Microsoft SharePoint data. For more information, see Veeam Explorer for Microsoft Exchange: Ports and Veeam Explorer for Microsoft SharePoint: Ports.

Permissions

The following table lists required permissions for data restore.

Operation	Required Roles and Permissions
Restore to Microsoft 365	To restore Microsoft Teams data, you must grant the following roles and permissions to user accounts: **Restore Using Basic Authentication Method** • The user account must have a Microsoft 365 license that permits access to Microsoft Teams API. The minimum sufficient license is Microsoft Teams Exploratory experience. For more information about the Microsoft Teams Exploratory experience, see this Microsoft article. • To restore Microsoft Teams data, the user account must have the *Teams Administrator* role. **Restore Using Modern Authentication Method** • The user account must have a Microsoft 365 license that permits access to Microsoft Teams API. The minimum sufficient license is Microsoft Teams Exploratory experience. • To restore Microsoft Teams data, the user account must have the *Teams Administrator* role. • Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide. • If you restore data with Azure AD applications using a certificate, make sure that your Azure AD application is granted the required permissions. For more information, see the Permissions for Modern App-Only Authentication section of the Veeam Backup for Microsoft 365 User Guide.

Considerations and Limitations

This section lists considerations and limitations of Veeam Explorer for Microsoft Teams.

Data Restore

Consider the following when planning to restore Microsoft Teams data:

- Use of modern authentication with legacy protocols allowed is not supported for data restore with Veeam Explorer for Microsoft Teams.
- You can restore Microsoft Teams data to the original organization only.
- Veeam Explorer for Microsoft Teams does not change roles for team owners during restore. For example, you create a backup of your organization, and then change role for a team member from *Member* to *Owner*. In this case, if you restore this team member from the backup, Veeam Explorer for Microsoft Teams will not set their role to *Member*.
- Restore of OneNote notebooks from backups of Microsoft Teams data for organizations with modern app-only authentication is not supported.
- When restoring a channel tab, Veeam Explorer for Microsoft Teams does not preserve relation between the link to a file published on the tab and the file itself. You will need to link the tab to the file manually after restore. This limitation does not apply to the scenario where you restore an entire team.
- Veeam Explorer for Microsoft Teams does not restore posts to their original location in the team channel. Instead, Veeam Explorer for Microsoft Teams exports posts to a file of the HTML format, creates a separate tab in the original channel and attaches the HTML file to this tab.
- If a user never opened the *Files* tab of a team channel in Microsoft Teams before data backup, files from this tab are not displayed in Veeam Explorer for Microsoft Teams.
- Before restoring posts, make sure that Website App is unblocked both for your organization and the user account that you use to restore Microsoft Teams data.
- When restoring a channel, Veeam Explorer for Microsoft Teams cannot rename this channel.
- Before restoring team data for a tenant organization with modern app-only authentication, make sure that a user account used for authorization has access to the root SharePoint site of this tenant organization.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Teams and load backups, you can use any of the following methods:

- The **Explore** option to load backups created by Veeam Backup for Microsoft 365. For more information, see the Data Restore section of the Veeam Backup for Microsoft 365 User Guide.

  When loading backups located in object storage, Veeam Explorer for Microsoft Teams will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To disable these notifications, clear the **Show pop-up notifications on startup** check box. For more information, see Advanced Settings.

- Go to **Start**, click **Veeam Explorer for Microsoft Teams** and manually open Microsoft Teams databases. For more information, see Standalone Databases.

  When you open Veeam Explorer for Microsoft Teams from the **Start** menu, all backed-up databases will be loaded automatically.

If you open Veeam Explorer for Microsoft Teams from the **Start** menu on a machine that runs the Veeam Backup & Replication console and Veeam Explorers only, specify the following:

- The domain name or IP address of a server to which you want to connect.
- The port number.
- User account credentials.

  Consider the following:

  - To perform restore operations, Veeam Explorer for Microsoft Teams must be run with elevated permissions. The user account must be a member of the local *Administrators* group on the machine where Veeam Explorer for Microsoft Teams is installed.
  - The account must have the Veeam Backup Administrator or Veeam Restore Operator role on the target backup server.

  To use the account under which Veeam Explorer for Microsoft Teams is running, select **Use Windows session authentication**.

To save the connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.

Getting to Know User Interface

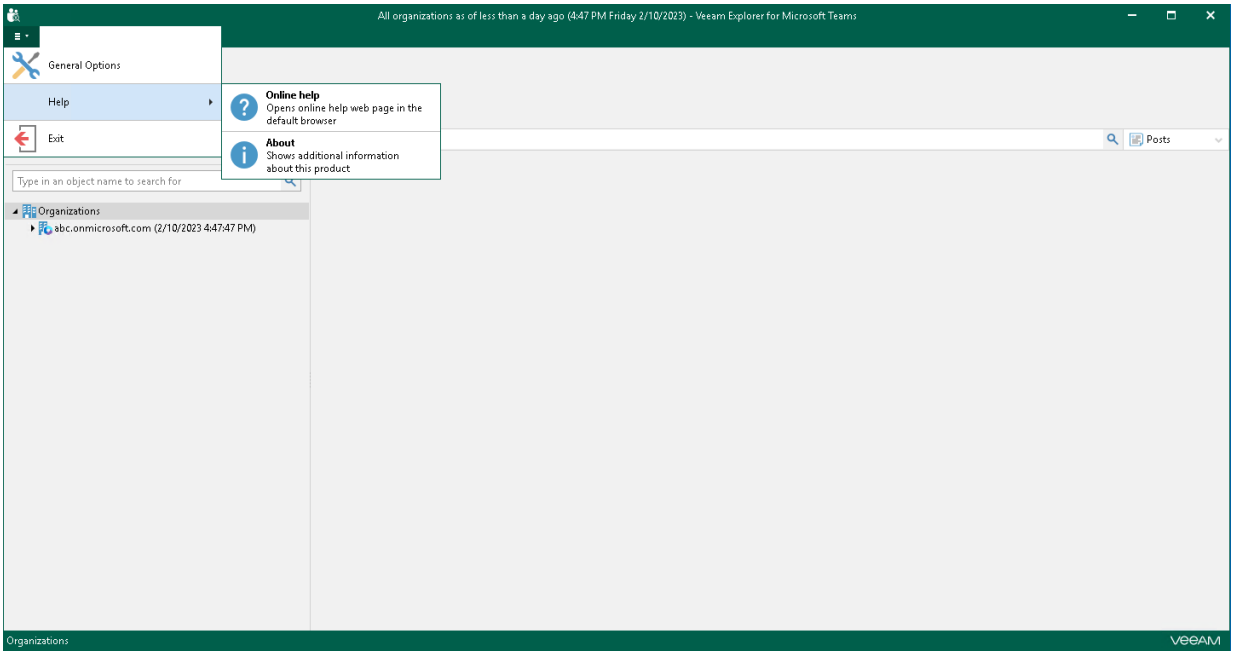
The user interface of Veeam Explorer for Microsoft Teams is designed to let you quickly find commands that you need to restore and export Microsoft Teams data from backups created by Veeam Backup for Microsoft 365.

Main Menu

The main menu comprises the following:

- **General Options**. Allows you to configure general application settings. For more information, see General Application Settings.
- **Help**.
  - **Online help**. Opens the online help page.
  - **About**. Shows the additional information including build number.
- **Exit**. Closes the Veeam Explorer for Microsoft Teams window.

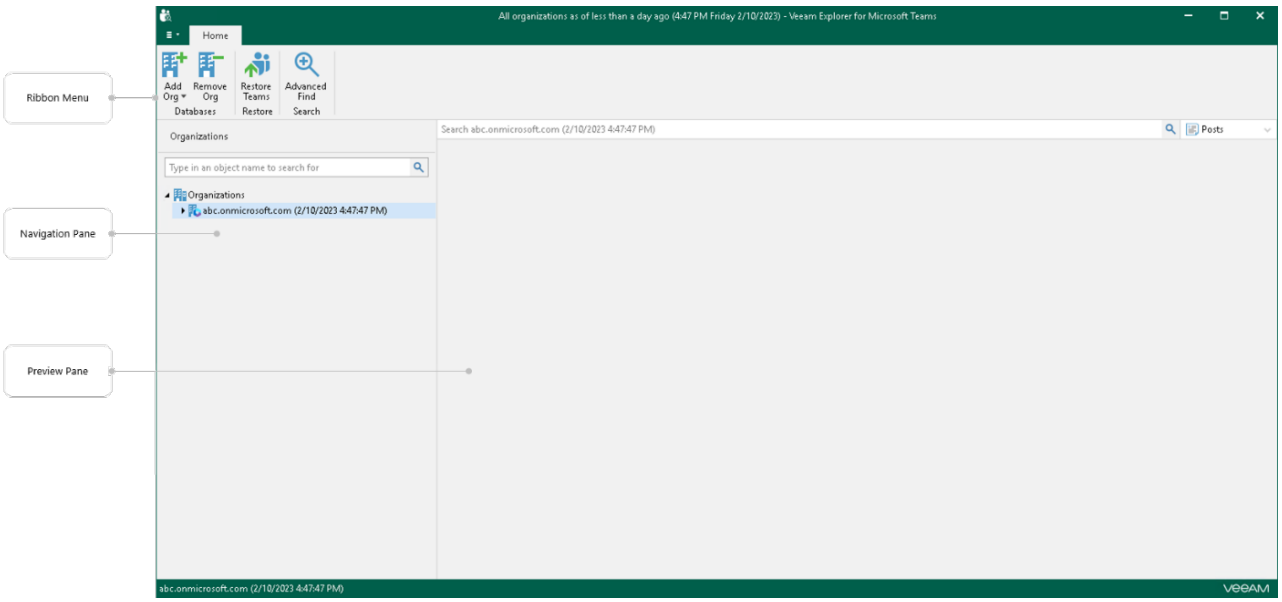
> **TIP**
>
> You can also open online help by pressing [F1] in any Veeam Explorer for Microsoft Teams wizard or window. You will then be redirected to the relevant section of the Veeam Explorers User Guide.



Main Application Window

The main application window can be divided into three categories:

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.
- The navigation pane that allows you to browse through the hierarchy of folders with backed-up data. Also, it allows you to search for teams using keywords.
- The preview pane that provides search capabilities and allows you to view details about items that are contained in a folder you have selected in the navigation pane.



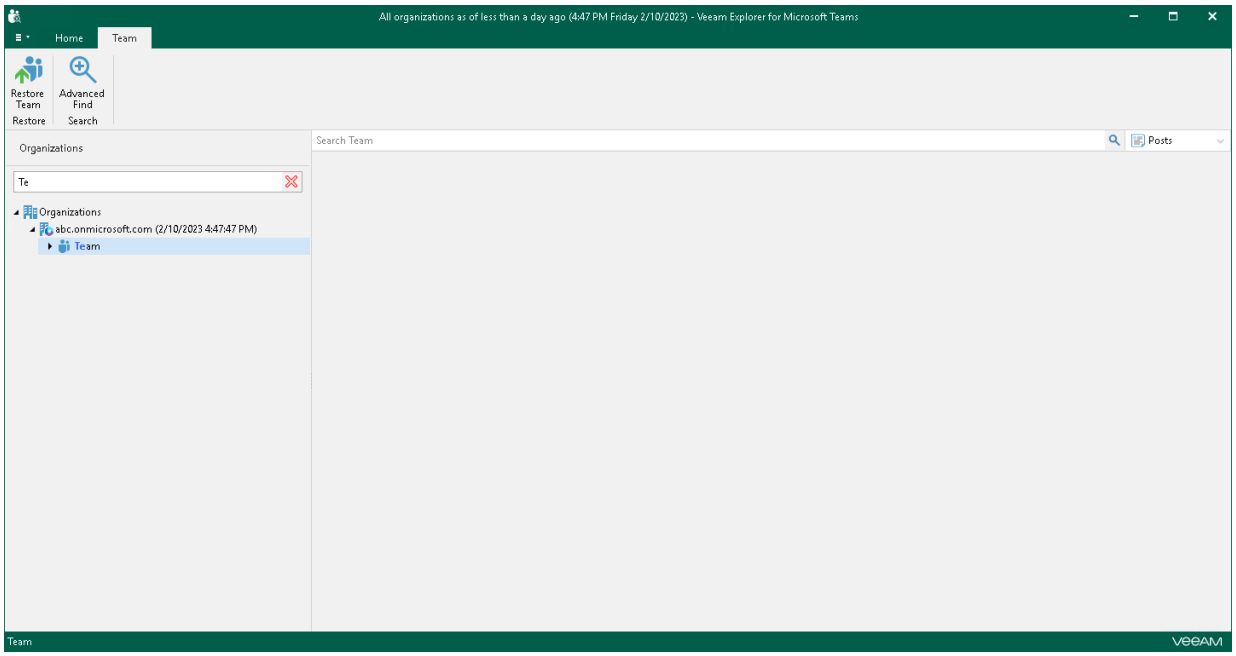
Browsing, Searching and Viewing Items

You can use Veeam Explorer for Microsoft Teams to view the contents of a backup file, view team properties, open posts and files, search for teams and for items in a backup file as well as customize criteria of your search.

Searching for Teams

You can use keywords to search for teams in the database structure containing your Microsoft Teams objects. To do this, enter a search query in the search field at the top of the navigation pane.

To remove a keyword, click the cross mark.

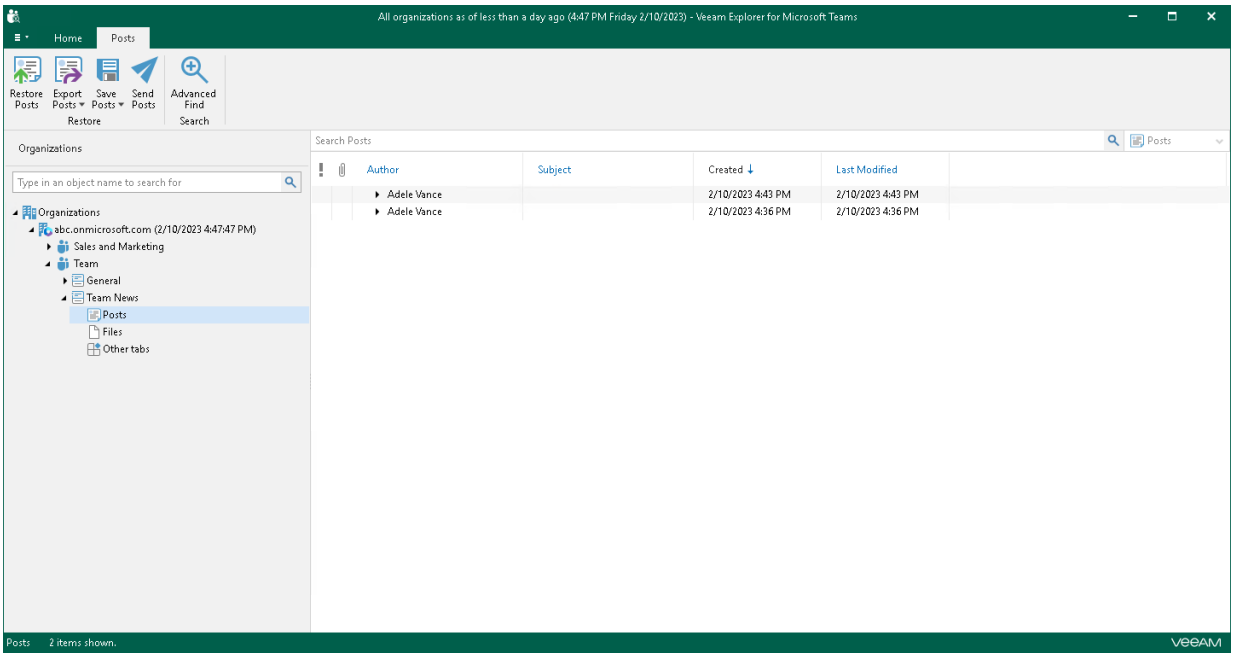


Browsing Backup Content

To view the contents of a backup file, you use the navigation pane which displays the database structure containing your Microsoft Teams objects: teams, channels and channel tabs. Veeam Explorer for Microsoft Teams groups channel tabs in the following nodes of the navigation pane:

- **Posts**. Contains the *Posts* tab of the channel.
- **Files**. Contains the *Files* tab of the channel.
- **Other tabs**. Contains other tabs of the channel that link to sites, documents, applications, and and other objects.

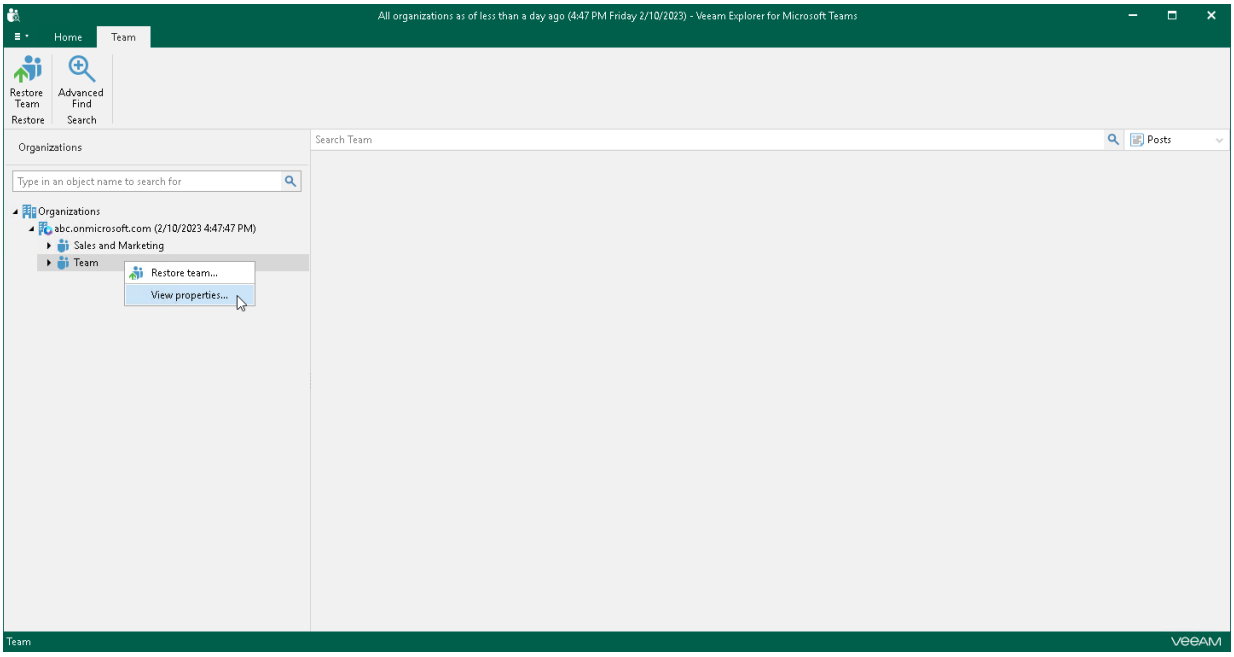
After you select an object in the navigation pane, you can see its content in the preview pane.



Viewing Team Properties

You can view properties of a backed-up team. This may be useful, for example, in case you want to decide whether to restore team properties during restore of a team.

To view team properties, in the navigation pane, right-click a necessary team and select **View properties**.

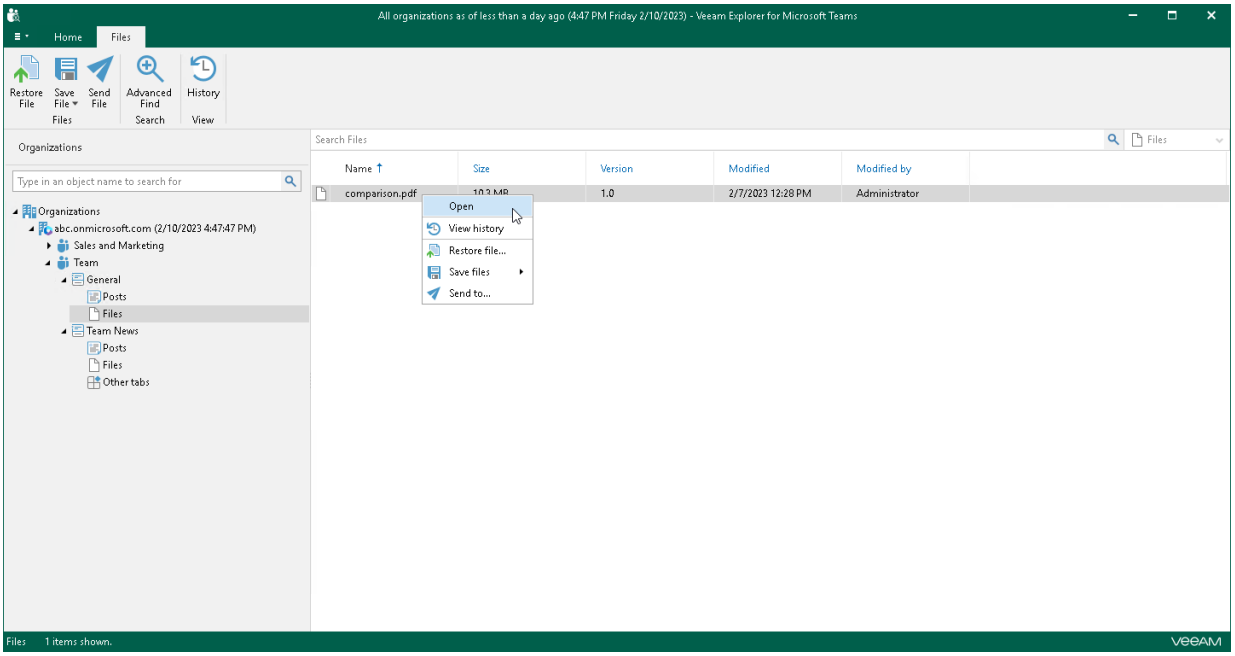


Opening Posts and Files

You can use Veeam Explorer for Microsoft Teams to open backed-up posts and files.

To open a post or file, do the following:

1. In the navigation pane, browse to the channel whose post or file you want to open and click the necessary node: **Posts** or **Files**.
2. In the preview pane, right-click a post or file and select **Open**.



Searching for Objects in Backup File

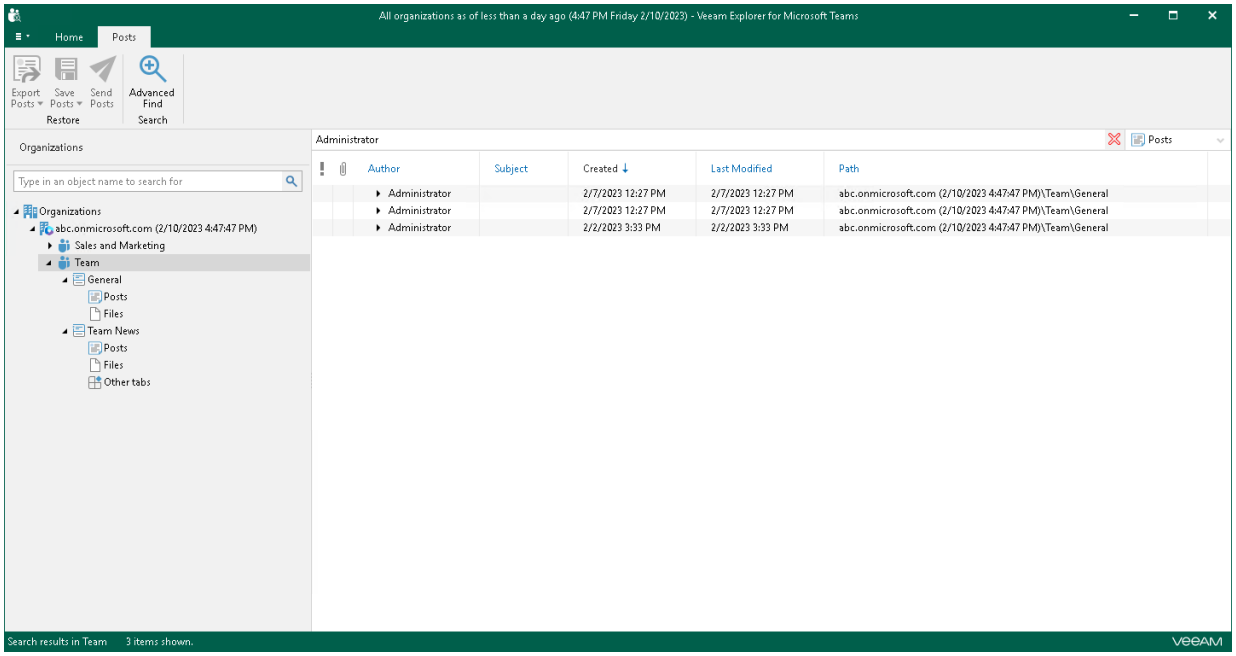
The search mechanism allows you to find items (posts, files and tabs) matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane, do one of the following:
   - Select a node that contains an item you want to find: **Posts**, **Files** or **Other tabs**.
   - Select a team or channel whose items you want to find. Then, from the drop-down list next to the search field, select what type of items you want to find: *Files*, *Posts* or *Other tabs*.
2. Enter a search query in the search field.

> **NOTE**
>
> To find the exact phrase, use double quotes. For example, "*Document*".

You can narrow your search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



Using Advanced Find

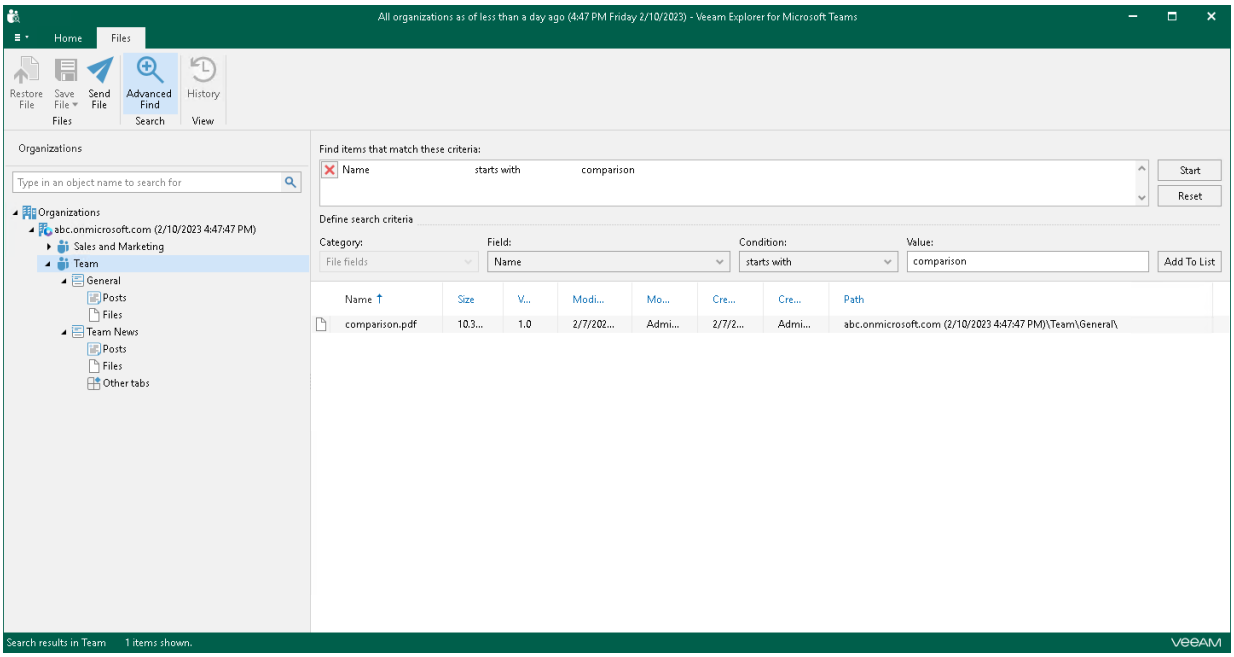
The **Advanced Find** mechanism allows you to define your search criteria more precisely.

> **NOTE**
>
> The **Advanced Find** mechanism is supported for posts and files only. The mechanism is not supported for tabs.

For example, to find a file whose name starts with *"word"*, do the following:

1. In the preview pane, select a node and click **Advanced Find** on the ribbon.
2. In the **Define search criteria** section, select **Category** > **File fields**.
3. In the **Field** list, select **Name**.
4. In the **Condition** list, select **starts with**.
5. In the **Value** field, specify a file name.
6. Click **Add to List** and then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



General Application Settings

You can configure general settings for Veeam Explorer for Microsoft Teams.

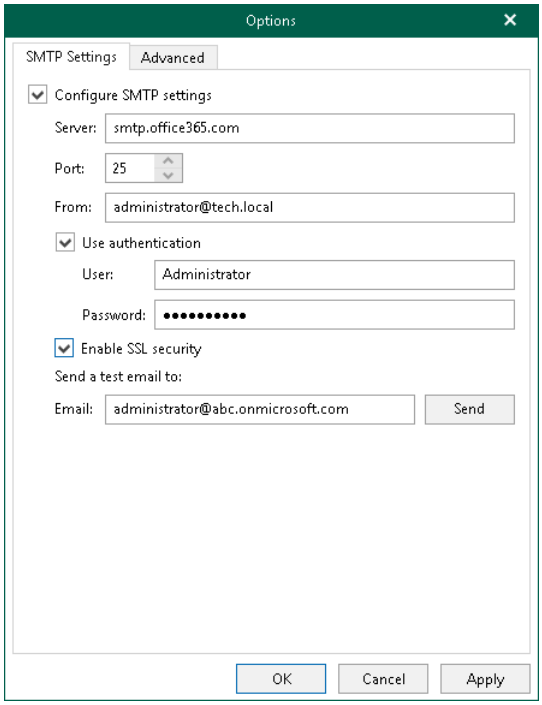
SMTP Settings

To send Microsoft Teams items as attachments, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
   a. In the **Server** field, specify a DNS name or IP address of the SMTP server.
   b. In the **Port** field, specify a port number of the specified SMTP server.

      The default port number is *25*. If you want to use SSL data encryption, specify port *587*.
   c. In the **From** field, specify the sender email address. This address will appear in the **From** field when sending Microsoft Teams posts or files. For more information, see Sending Posts and Files.
   d. If the specified SMTP server requires an authentication for outgoing mail, select the **Use authentication** check box and provide valid credentials.
   e. Select the **Enable SSL security** check box to enable SSL data encryption.
4. Click **Send** to send a test email message.
5. Click **OK**.



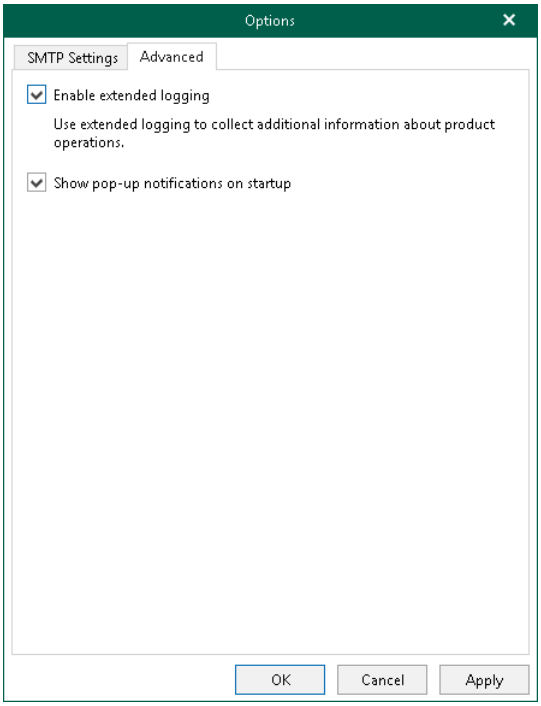
Advanced Settings

Veeam Explorer for Microsoft Teams allows you to configure advanced settings such as extended logging mode and pop-up notifications.

To configure advanced settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Advanced** tab.
3. If you want to enable extended logging mode to collect logs that contain additional information on specific operations, select the **Enable extended logging** check box.

   After enabling extended logging mode, you can go back to the application and perform actions for which you want to collect additional information. Then you can collect logs.
4. By default, Veeam Explorer for Microsoft Teams displays notifications when loading backups created by Veeam Backup for Microsoft 365 from object storage. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.
5. Click **OK**.



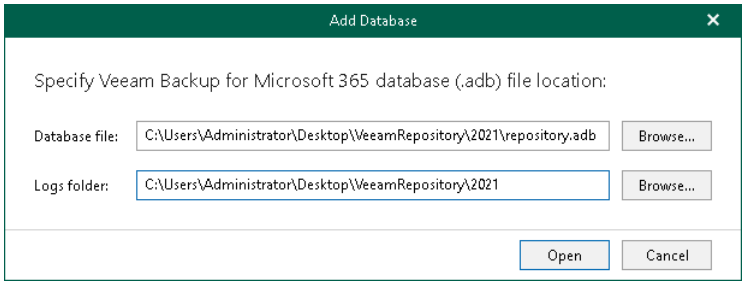
Standalone Databases

You can add standalone databases to the Veeam Explorer for Microsoft Teams scope and connect to a Veeam Backup for Microsoft 365 server and service provider server to view backups located on these servers.

Adding Veeam Backup for Microsoft 365 Databases

To manually add databases that store Microsoft 365 organization data, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 database** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 database**.
2. Specify the database file location and log directory.
3. Click **Open**.



NOTE

Make sure you have disabled the *Veeam Backup Proxy for Microsoft 365 Service* when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will not be able to access the database due to database lock.

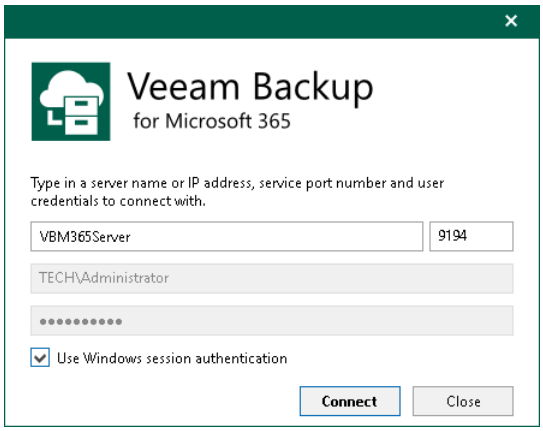
Adding Veeam Backup for Microsoft 365 Server

You can use Veeam Explorer for Microsoft Teams to connect to another Veeam Backup for Microsoft 365 server and add its databases to the Veeam Explorer for Microsoft Teams scope.

To connect to another Veeam Backup for Microsoft 365 server remotely, do the following:

1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 server** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 server**.
2. Specify a server name or IP address and enter credentials to access the specified server.

   Select the **Use Windows session authentication** check box to connect with the user account under which you are currently logged in.
3. Click **Connect**.



Adding Veeam Backup for Microsoft 365 Service Provider

In Veeam Explorer for Microsoft Teams, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.

> **NOTE**
>
> Make sure that both Veeam Explorer for Microsoft Teams and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication. For more information, see the Connecting to Service Providers section of the Veeam Cloud Connect Guide.

To add Veeam Backup for Microsoft 365 service providers, do the following:

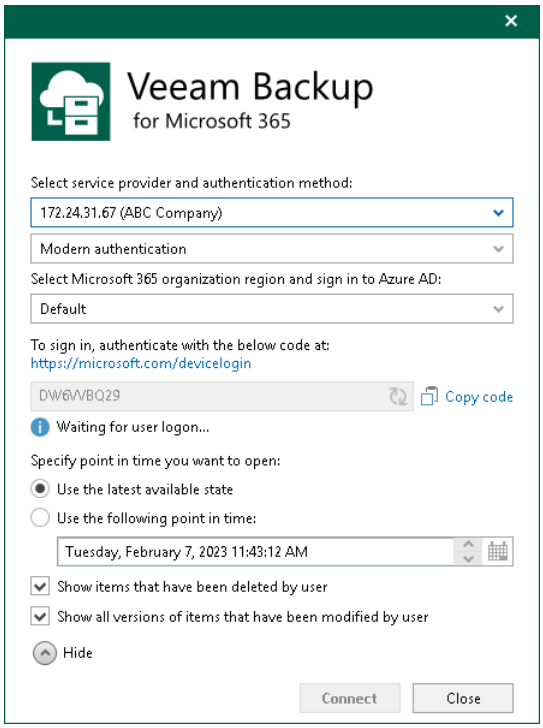
1. Do one of the following:
   - On the **Home** tab, click **Add Org** > **Veeam Backup for Microsoft 365 service provider** on the ribbon.
   - Right-click the **Organizations** node and select **Veeam Backup for Microsoft 365 service provider**.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and select an authentication method that can be either *Modern authentication* or *Basic authentication*.
3. [For *Modern authentication*] Select a region to which a Microsoft 365 organization of the selected service provider belongs.
4. [For *Modern authentication*] Copy the device code and use it to sign in to Azure Active Directory.

   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.

   > **NOTE**
   >
   > You cannot use *Basic authentication* to load backups if a Microsoft 365 organization has been added to the service provider infrastructure using *Modern authentication*.
5. Select a point-in-time state as of which you want to load Microsoft 365 backups.

   To select a point in time, use the calendar control.
6. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
7. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.

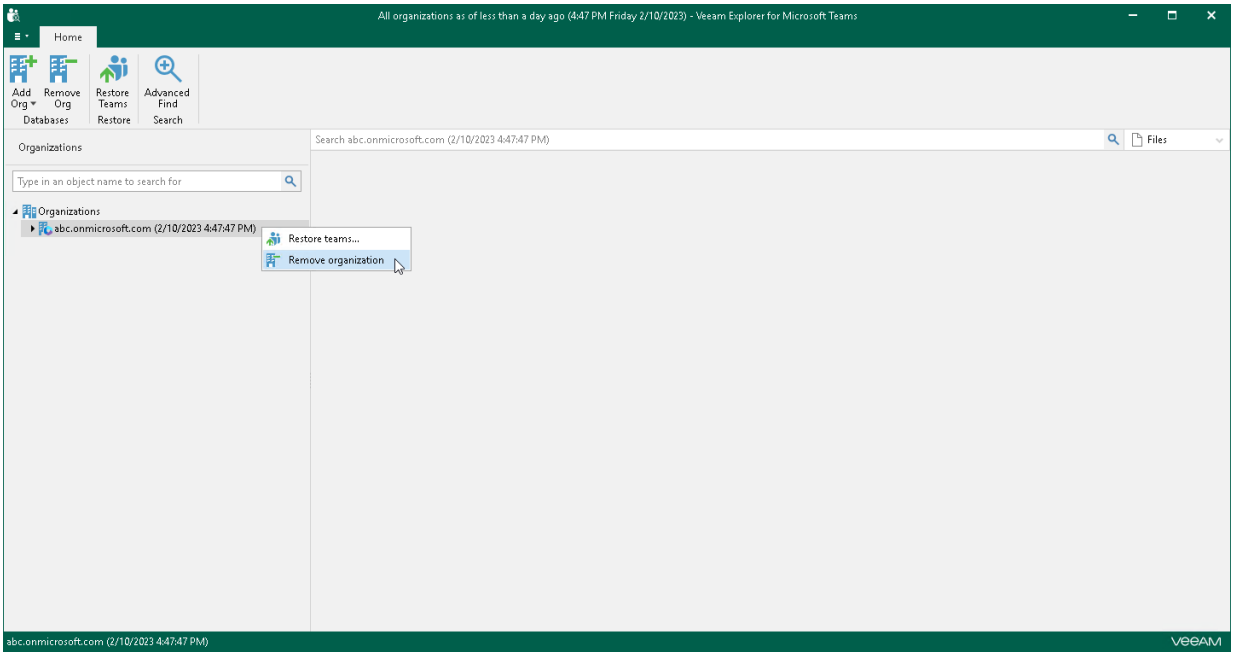
8. Click **Connect**.



Removing Organizations

Veeam Explorer for Microsoft Teams allows you to remove an organization from the application scope when you no longer need it.

To remove an organization from the application scope, right-click an organization in the navigation pane and select **Remove organization**.



Data Restore

You can use Veeam Explorer for Microsoft Teams to restore Microsoft Teams data to Microsoft 365 organizations.

Restoring Teams

You can use Veeam Explorer for Microsoft Teams to restore all teams of a Microsoft 365 organization or a specific team of an organization.

Before restoring data, read the Considerations and Limitations section.

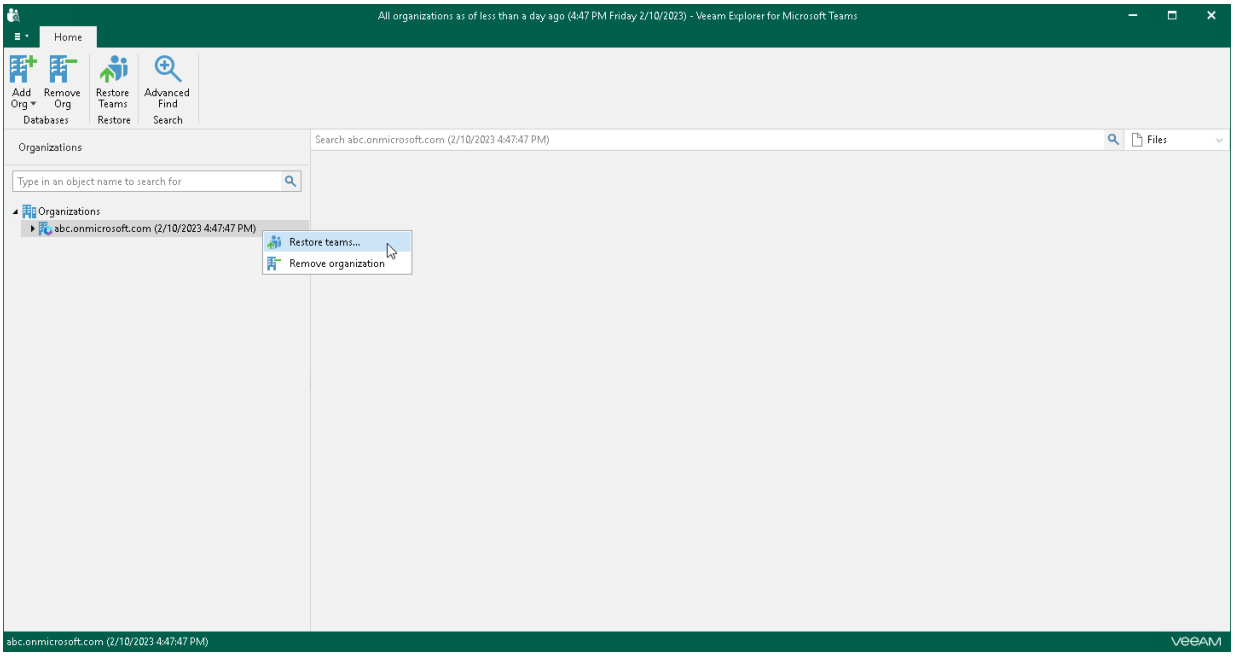
To restore teams, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Select teams to restore.
5. Specify restore options.
6. Select team members to restore.

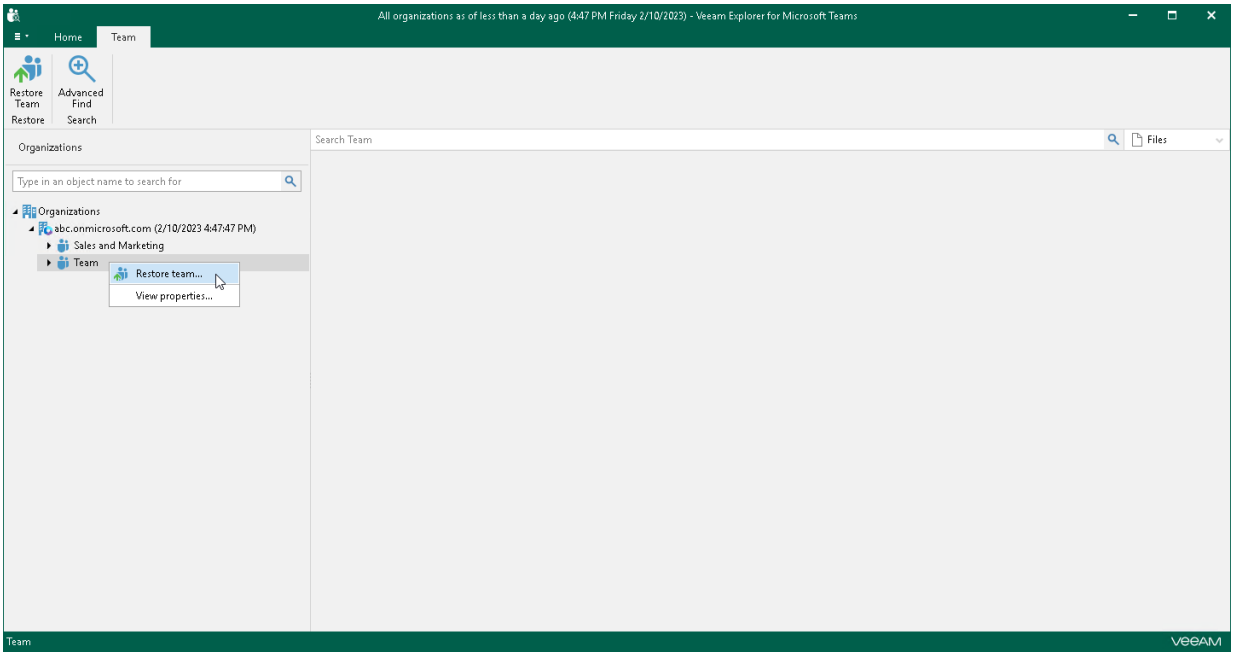
Step 1. Launch Restore Wizard

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

- If you want to restore multiple teams of a Microsoft 365 organization, in the navigation pane, do one of the following:
  - Select an organization whose teams you want to restore and on the **Home** tab, click **Restore Teams** on the ribbon.
  - Right-click an organization whose teams you want to restore and select **Restore teams**.



- If you want to restore a specific team, in the navigation pane, do one of the following:
  - Select a team that you want to restore and on the **Team** tab, click **Restore Team** on the ribbon.
  - Right-click a team that you want to restore and select **Restore team**.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

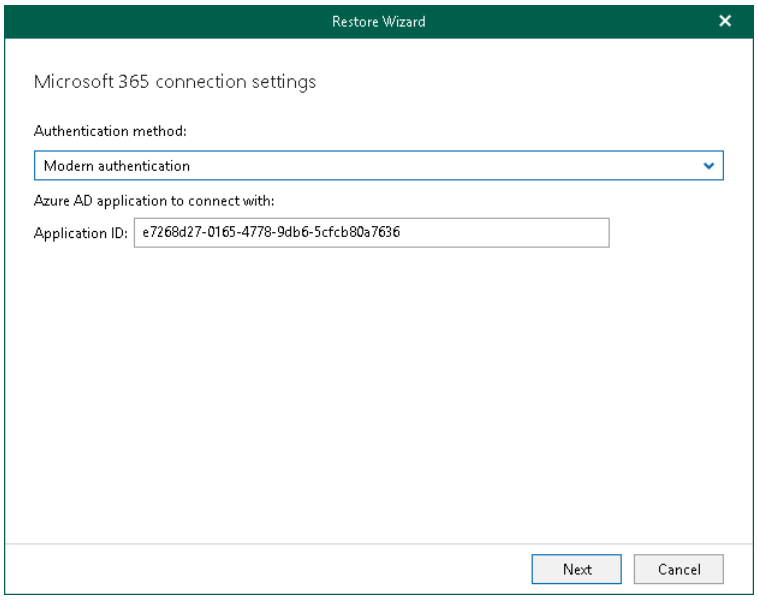
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

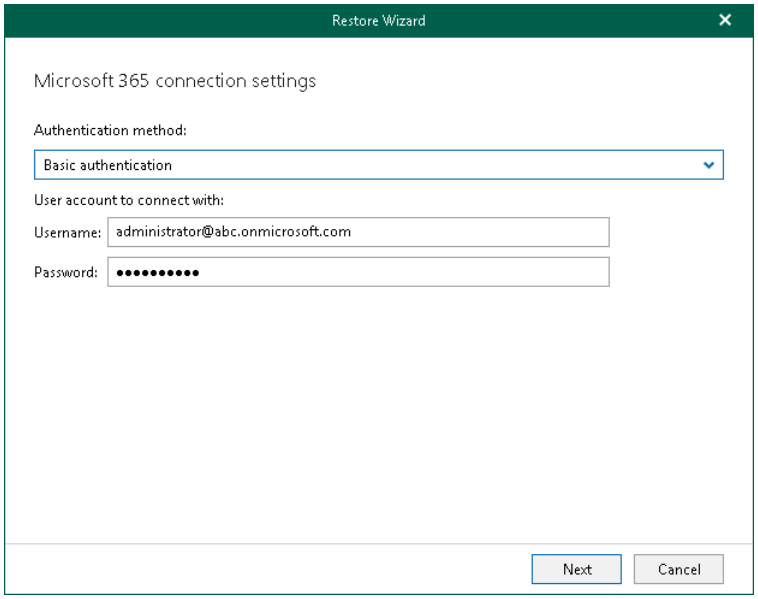
   By default, Veeam Explorer for Microsoft Teams populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft 365 organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

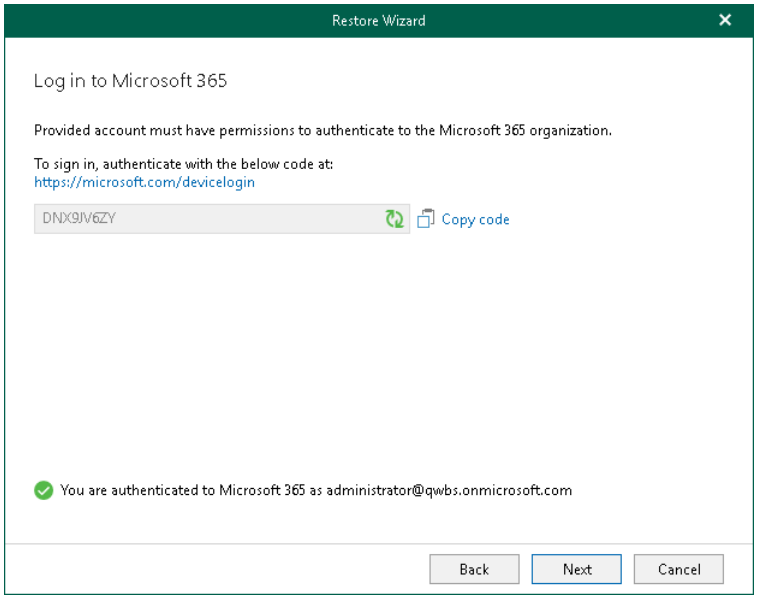
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

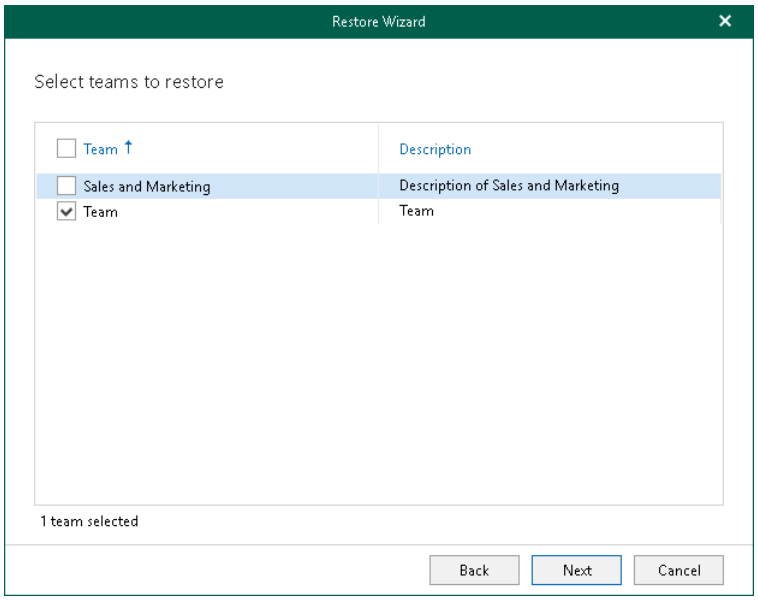
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Select Teams

This step is only available if you launched the **Restore** wizard to restore multiple teams.

At this step of the wizard, select check boxes next to the teams that you want to restore.



Step 5. Specify Restore Options

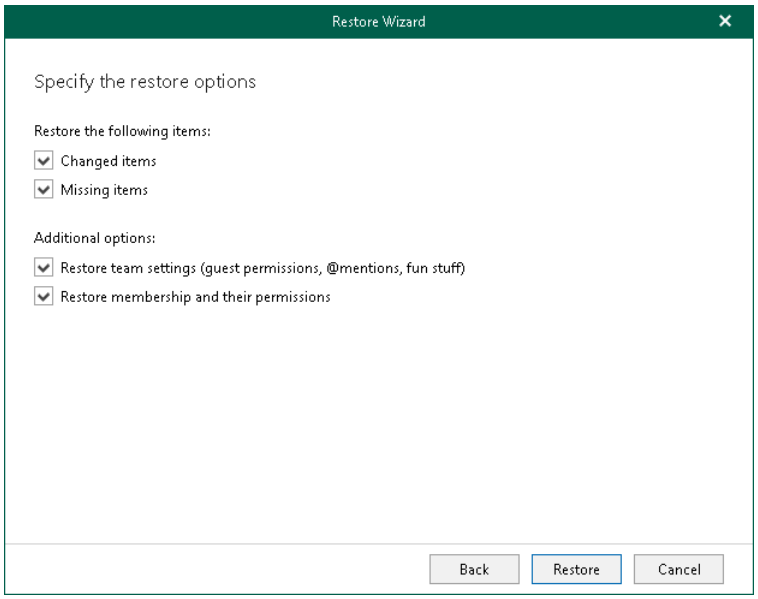
At this step of the wizard, specify data restore options:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created. When you select this option, Veeam Explorer for Microsoft Teams overwrites existing items in the original team.
2. Select the **Missing items** check box if you want to restore items that are missing in the original team. For example, some of the items were removed and you want to restore them from the backup.
3. Select the **Restore team settings** check box if you want to replace the current team settings with team settings from the backup. For information on how to view team settings in the backup, see Viewing Team Properties.

   Keep in mind that you cannot select this check box if both the **Changed items** and **Missing items** check boxes are cleared.
4. If you want to restore information about team members and their roles from the backup, make sure that the **Restore membership and their permissions** check box is selected.
   - If you launched the **Restore** wizard to restore a specific team, you will be able to review team members at the next step of the wizard. Click **Next**.
   - If you launched the **Restore** wizard to restore multiple teams, you cannot review team members. Click **Restore** to start the restore operation.

   You cannot proceed to the next step or start the restore operation, if you clear both the **Changed items** and **Missing items** check boxes.

> **TIP**
>
> If you clear the **Restore membership and their permissions** check box, you can start the restore operation immediately. To do this, click **Restore**.



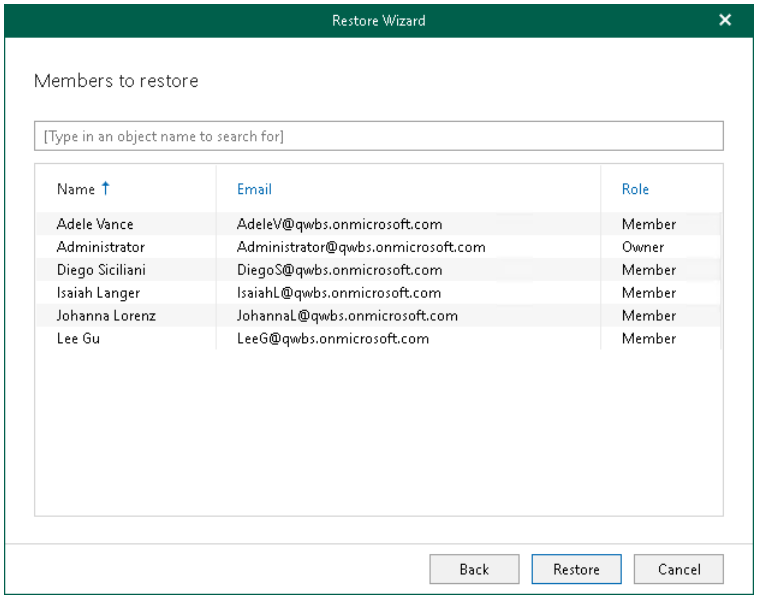
Step 6. Review Team Members

This step is only available if you launched the **Restore** wizard to restore a specific team and selected the **Restore membership and their permissions** check box at the previous step of the wizard.

At this step of the wizard, review the list of users whose membership and roles in the team will be restored and click **Restore**.

To quickly find the necessary team members, use the search field at the top of the wizard window.

> **NOTE**
>
> Veeam Explorer for Microsoft Teams does not change roles for team owners during restore. For example, you create a backup of your organization, and then change role for a team member from *Member* to *Owner*. In this case, if you choose to restore this team member from the backup, Veeam Explorer for Microsoft Teams will not set their role to *Member*.
>
> In the opposite case, if a team member role was changed from *Owner* to *Member* after the backup was created, and you choose to restore team membership from the backup, Veeam Explorer for Microsoft Teams will elevate the role to *Owner* during restore.



Restoring Channels and Tabs

You can use Veeam Explorer for Microsoft Teams to restore individual channels of a team. You can restore an entire channel or specific tabs of a channel.

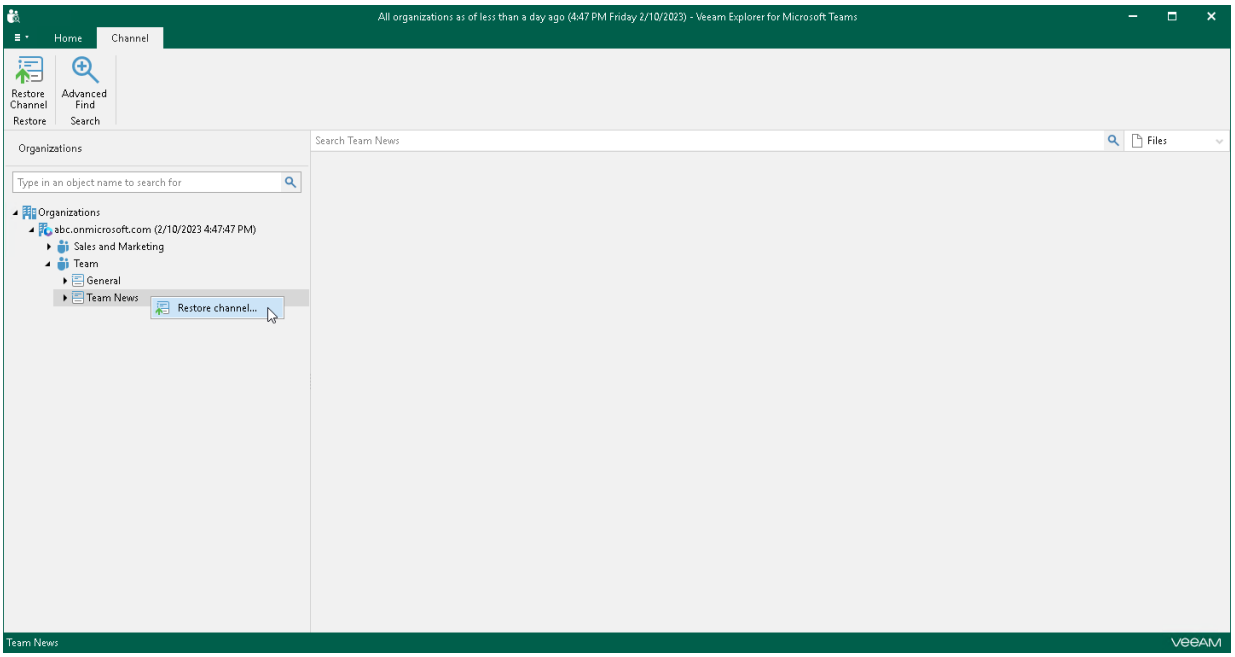
To restore channels and tabs, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify restore options.

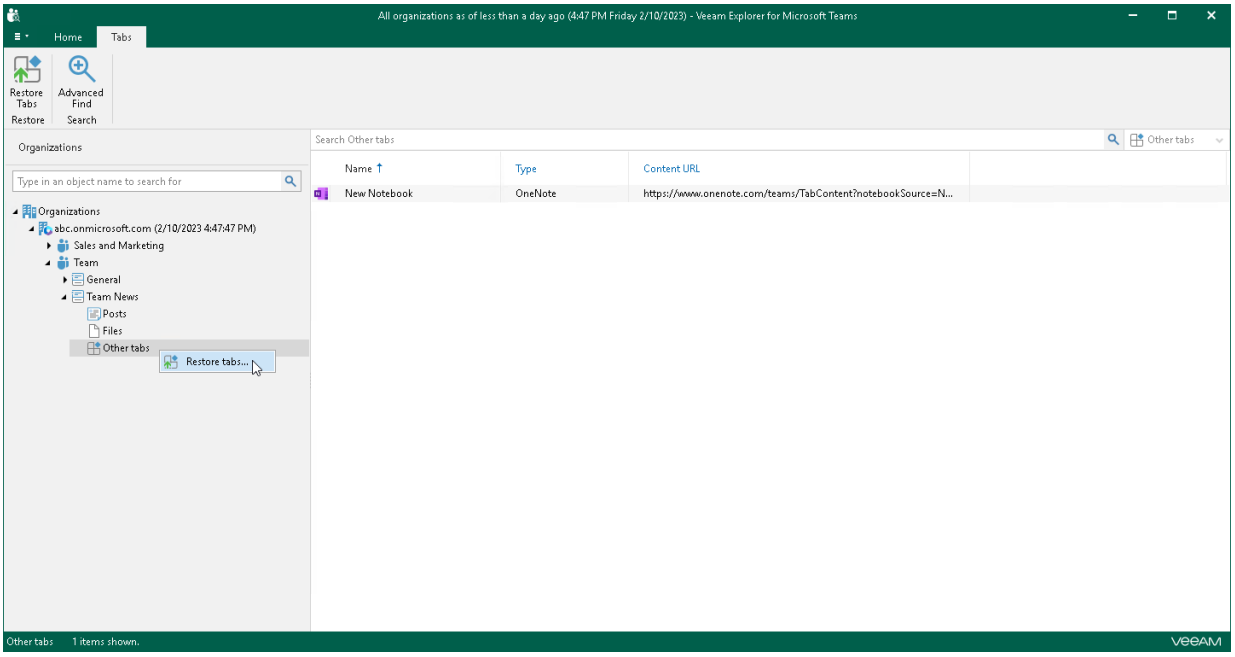
Step 1. Launch Restore Wizard

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

- If you want to restore a channel, in the navigation pane, do one of the following:
  - Select a channel that you want to restore and on the **Channel** tab, click **Restore Channel** on the ribbon.
  - Right-click a channel that you want to restore and select **Restore channel**.

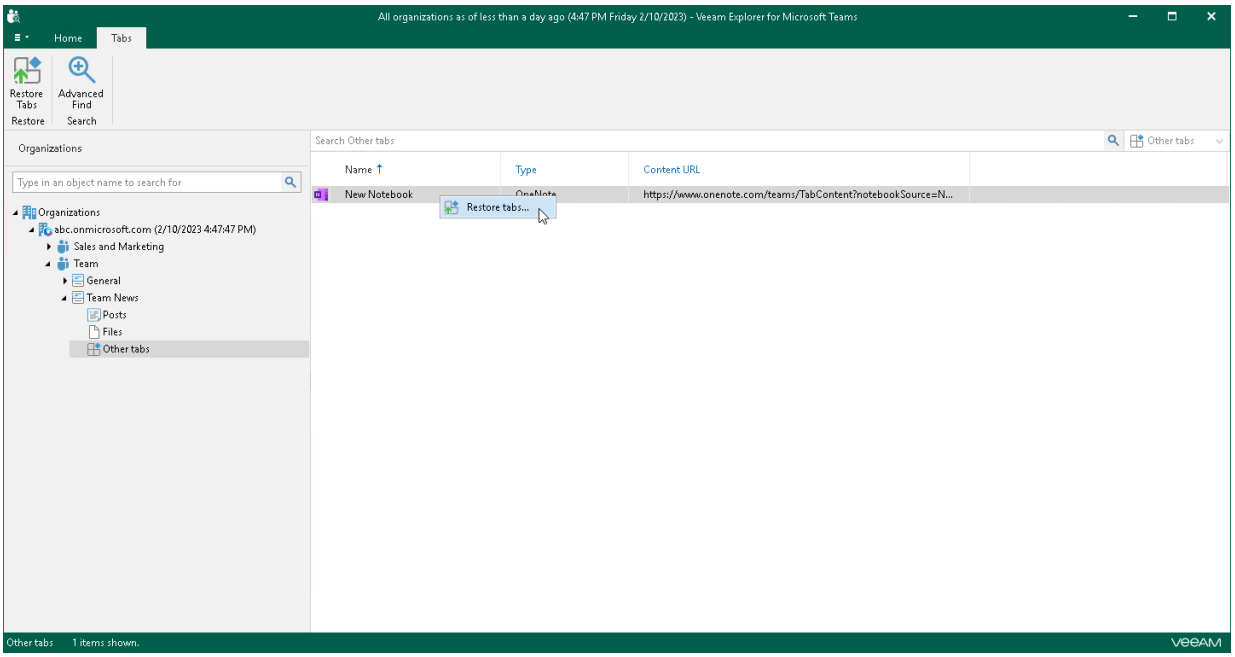


- If you want to restore all tabs of a channel, in the navigation pane, do one of the following:
  - Expand a channel whose tabs you want to restore, select **Other tabs** and on the **Tabs** tab, click **Restore Tabs** on the ribbon.
  - Expand a channel whose tabs you want to restore, right-click **Other tabs** and select **Restore tabs**.



- If you want to restore individual tabs of a channel, do the following:
  a. In the navigation pane, expand a channel whose tabs you want to restore and select **Other tabs**.
  b. In the preview pane, select a necessary tab and click **Restore Tabs** on the ribbon or right-click a tab and select **Restore tabs**.

> **TIP**
>
> To select more than one tab in the preview pane, press and hold the **[CTRL]** key and select the necessary tabs.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

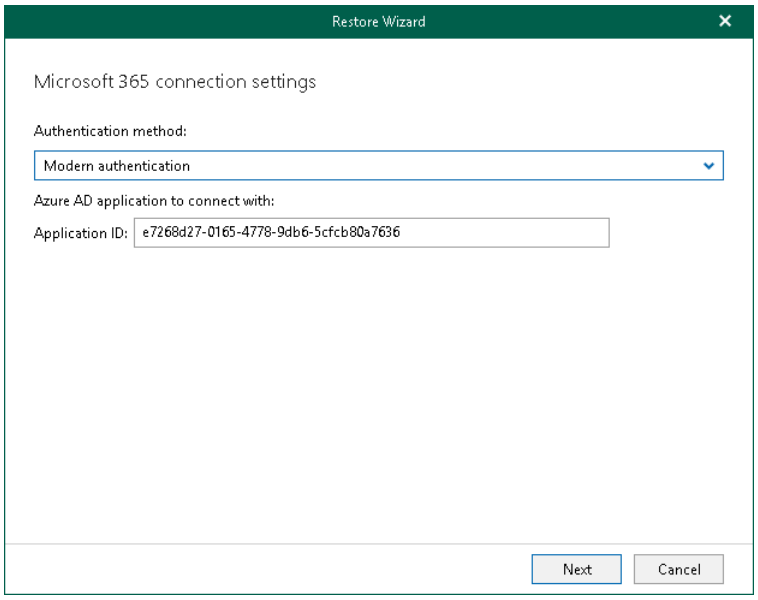
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

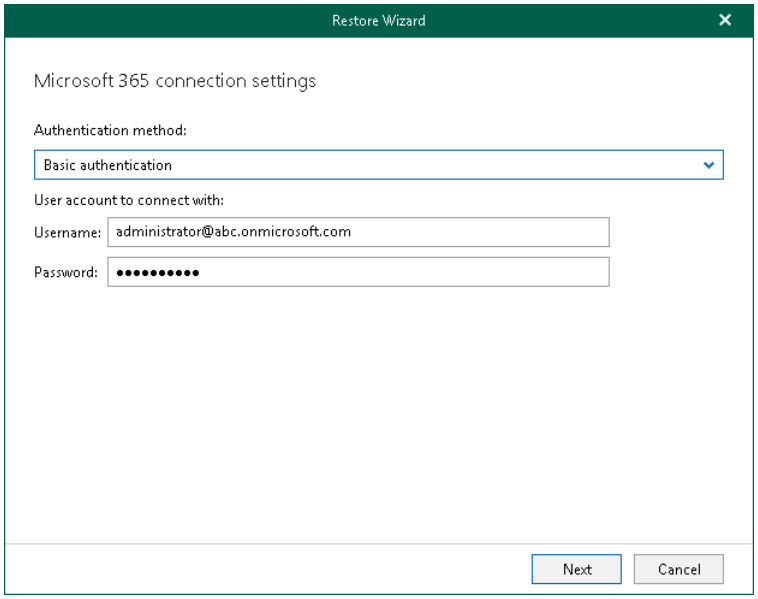
   By default, Veeam Explorer for Microsoft Teams populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft 365 organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

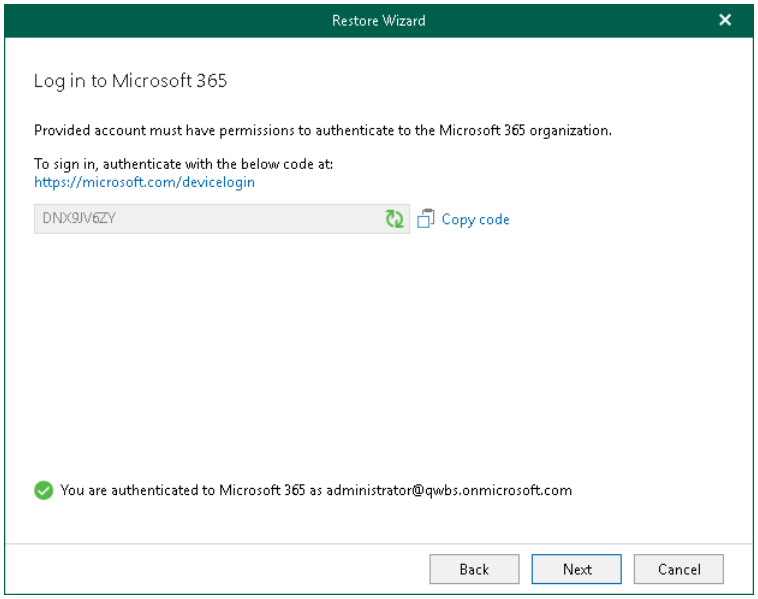
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.

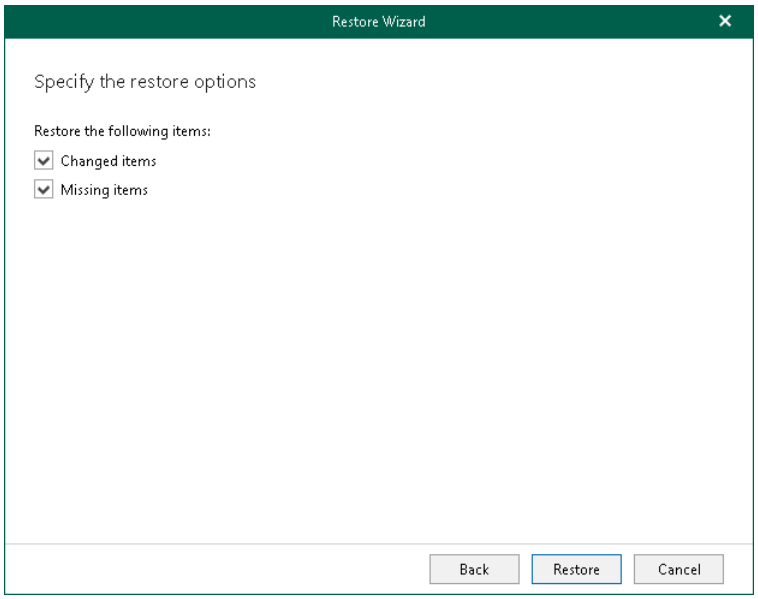


Step 4. Specify Restore Options

At this step of the wizard, specify data restore options and start the restore operation:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created. When you select this option, Veeam Explorer for Microsoft Teams overwrites existing items in your target location.
2. Select the **Missing items** check box if you want to restore items that are missing in the target location. For example, some of the items were removed and you want to restore them from the backup.
3. Click **Restore**.

> **NOTE**
>
> During restore of a tab, Veeam Explorer for Microsoft Teams restores the name of the tab and a link to an object published on the tab. The object itself, for example, a SharePoint site or document, is not restored from the backup in this scenario. To restore such objects along with tabs, consider restoring an entire team. For more information, see Restoring Teams.



Restoring Posts

You can use Veeam Explorer for Microsoft Teams to restore posts of a team channel. When you restore posts, you can choose to restore all posts of a channel or restore posts published within a specified time period.

> **NOTE**
>
> Veeam Backup for Microsoft 365 does not restore posts to their original location in the team channel. Instead, Veeam Backup for Microsoft 365 creates a new tab in the original channel and restores posts to this tab. If you want to restore posts to another channel, use the export operation. For more information, see Data Export.

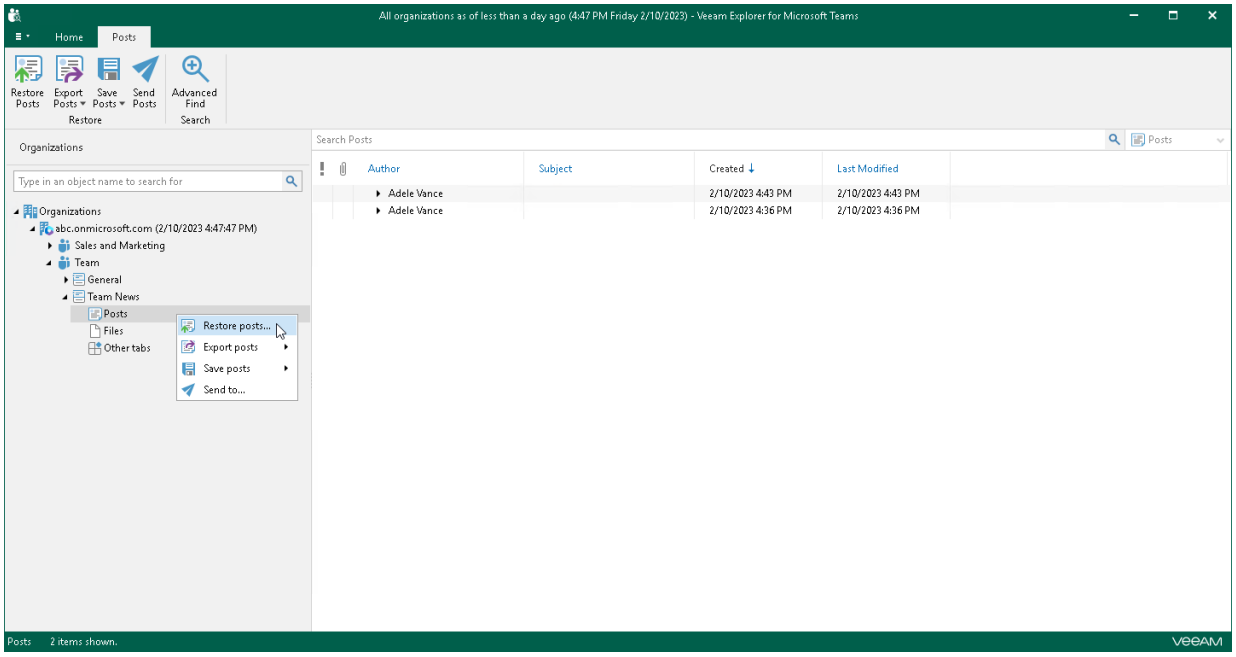
To restore posts, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, in the navigation pane, do one of the following:

- Expand a channel whose posts you want to restore, select **Posts** and on the **Posts** tab, click **Restore Posts** on the ribbon.
- Expand a channel whose posts you want to restore, right-click **Posts** and select **Restore posts.**



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

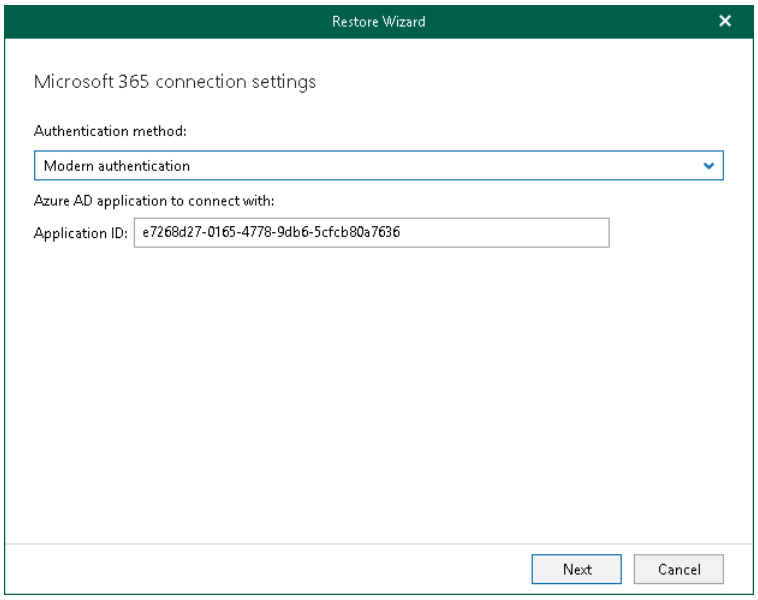
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

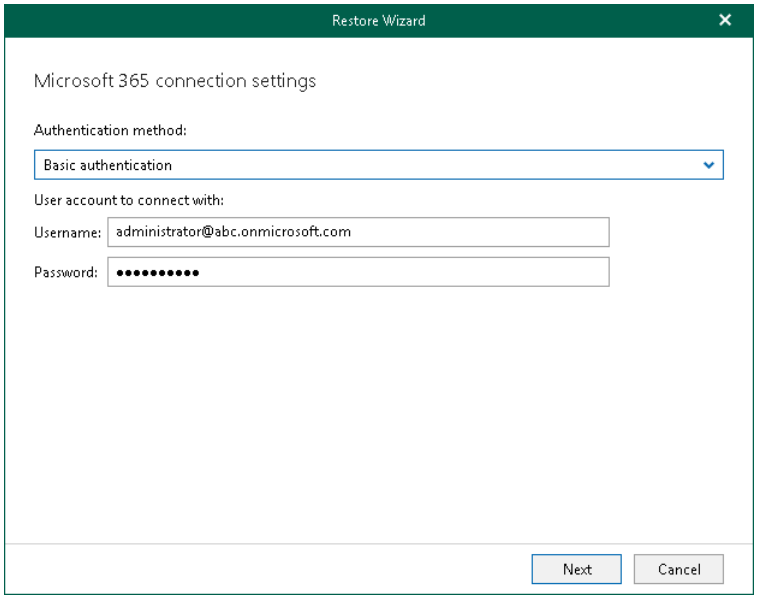
   By default, Veeam Explorer for Microsoft Teams populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft 365 organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

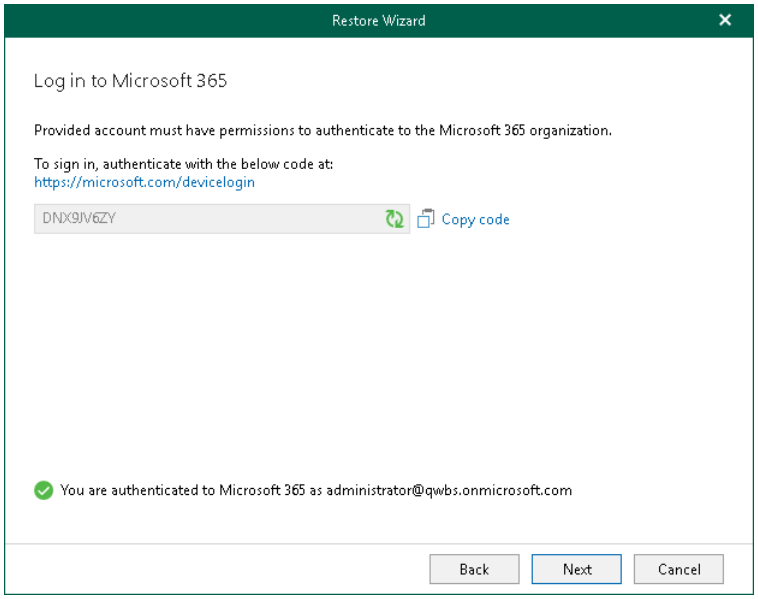
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select one of the following options:

- **Restore all posts**

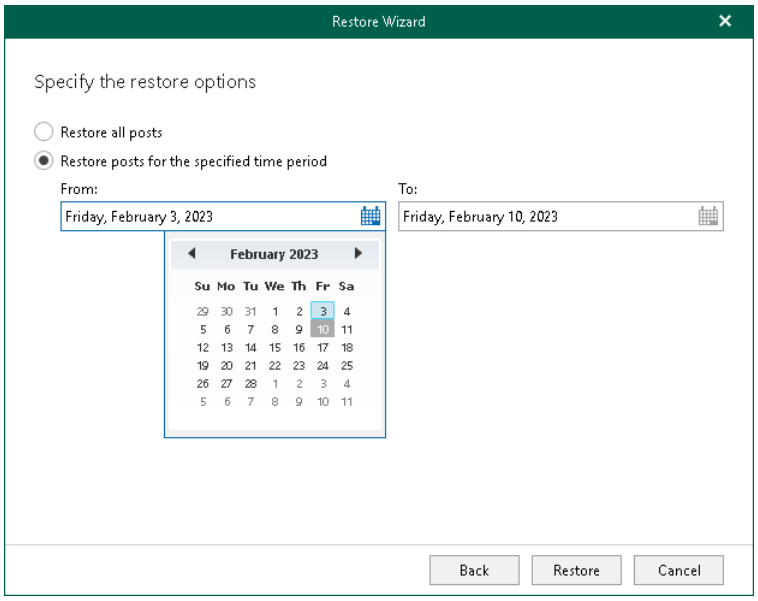
  Select this option if you want to restore all posts published in the channel.

- **Restore posts for the specified time period**

  Select this option if you want to restore posts published in the channel during the specified time period.

  If you select this option, in the **From** and **To** fields, specify the dates that define the start and end of the desired time period. Veeam Explorer for Microsoft Teams will restore posts whose last modification date belongs to the specified period.

When you restore posts, Veeam Backup for Microsoft 365 will create a separate tab in the original team channel and restore posts to this tab.



Restoring Files

You can use Veeam Explorer for Microsoft Teams to restore files of a team channel.

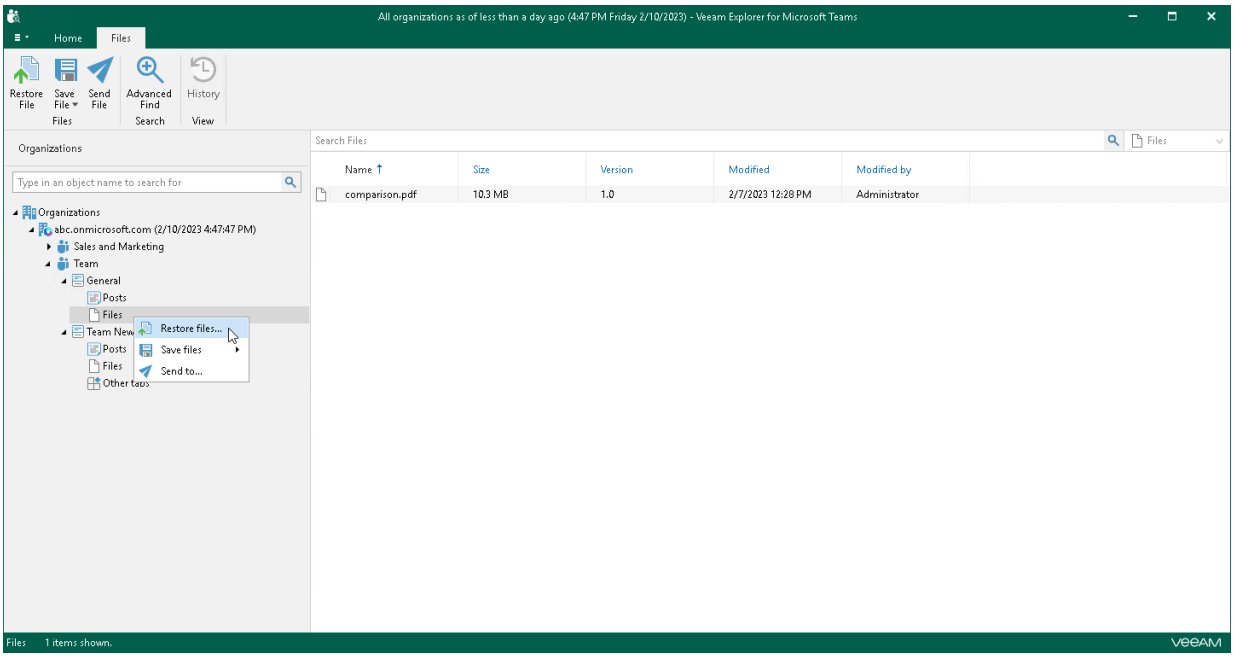
To restore files, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Microsoft 365.
4. Specify restore options.

Step 1. Launch Restore Wizard

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

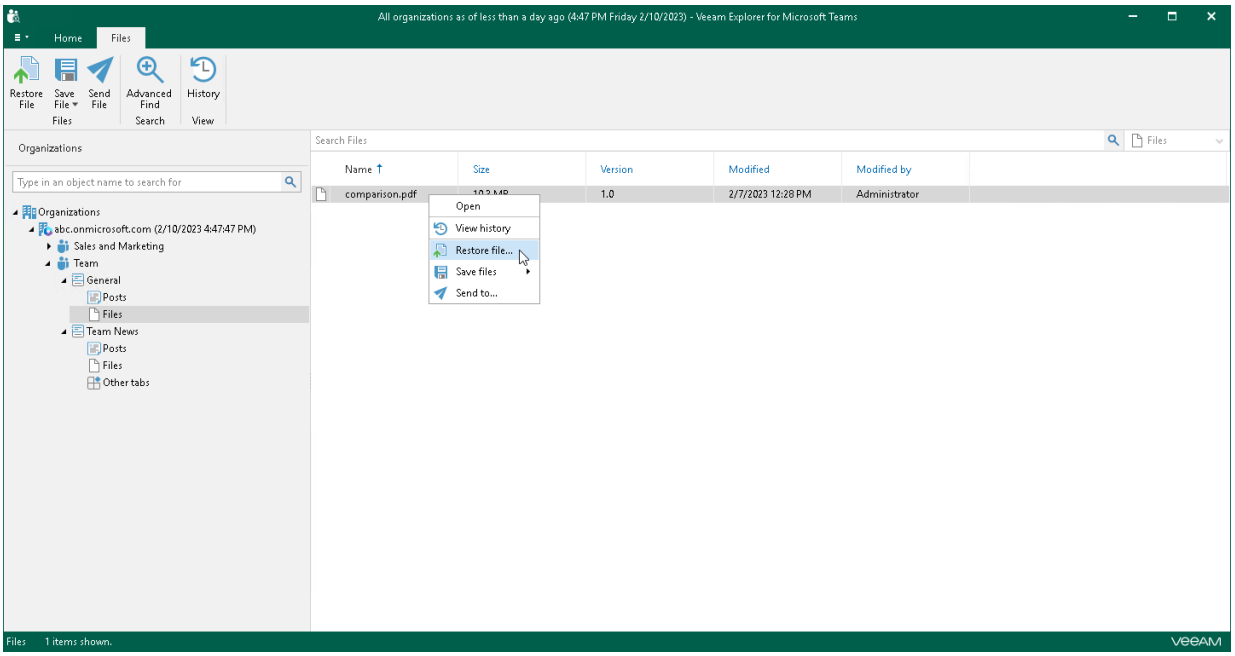
- If you want to restore all files of a channel, in the navigation pane, do one of the following:
  - Expand a channel whose files you want to restore, select **Files** and on the **Files** tab, click **Restore File** on the ribbon.
  - Right-click a channel whose files you want to restore, right-click **Files** and select **Restore files**.



- If you want to restore individual files, do the following:
  a. In the navigation pane, expand a channel whose files you want to restore and select **Files**.
  b. In the preview pane, select a necessary file and click **Restore File** on the ribbon or right-click a file and select **Restore file**.

TIP

To select more than one file in the preview pane, press and hold the **[CTRL]** key and select the necessary files.



Step 2. Select Authentication Method

At this step of the wizard, select either modern or basic authentication and specify authentication settings.

Modern Authentication

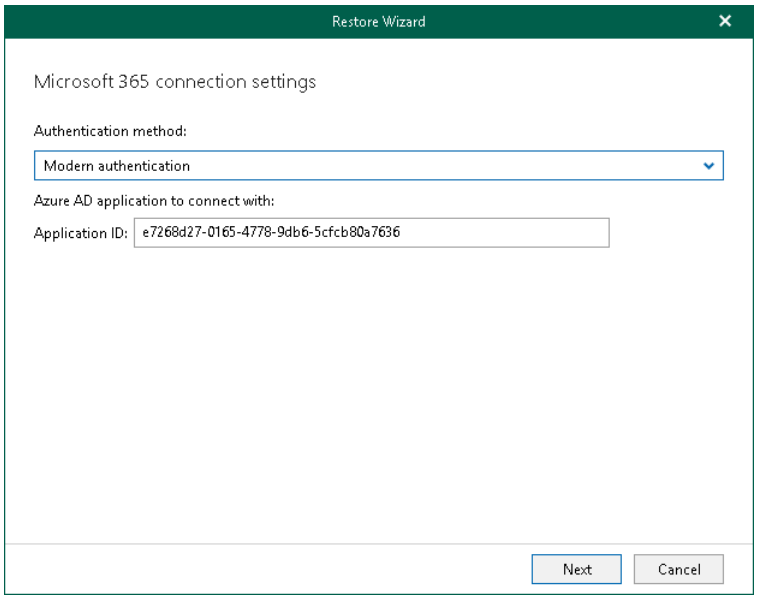
To use modern authentication, do the following:

1. From the **Authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team back to Microsoft 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see the Microsoft 365 Organizations section of the Veeam Backup for Microsoft 365 User Guide.

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for data restore.

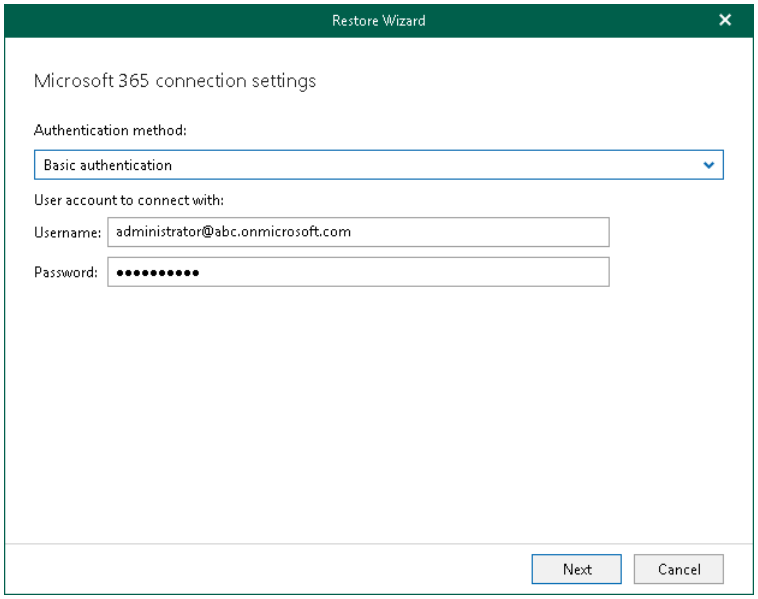
   By default, Veeam Explorer for Microsoft Teams populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see the Azure AD Application Permissions section of the Veeam Backup for Microsoft 365 User Guide.



Basic Authentication

To use basic authentication, do the following:

1. From the **Authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft 365 organization.



Step 3. Log In to Microsoft 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

   Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.

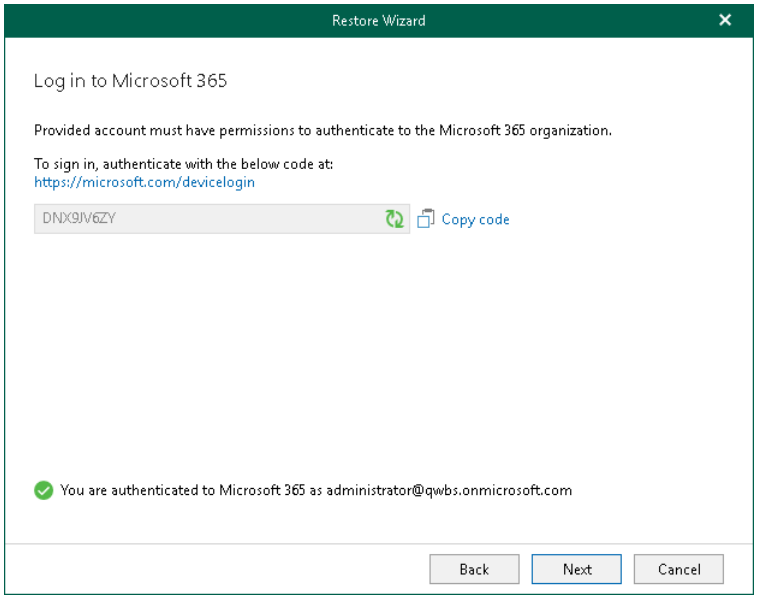
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

   Make sure to log in with the user account that has required permissions assigned. For more information, see Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see the Configuring Azure AD Application Settings section of the Veeam Backup for Microsoft 365 User Guide.

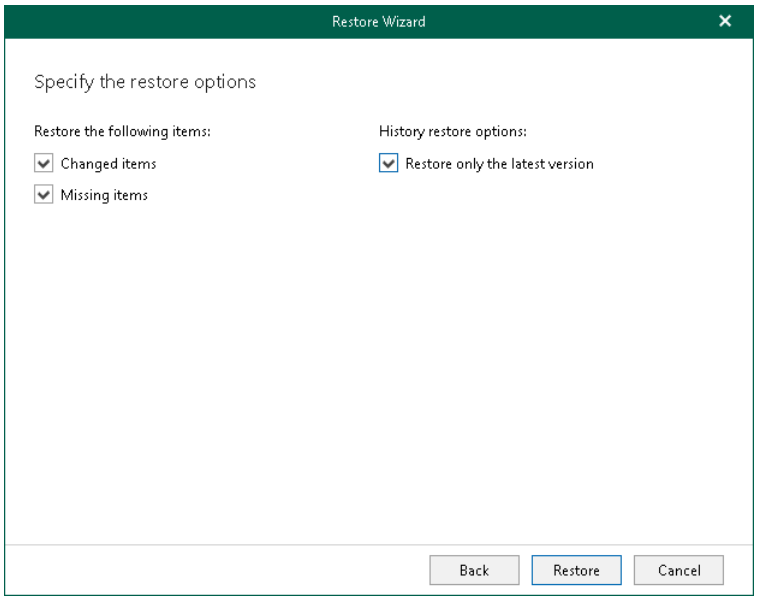
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Specify Restore Options

At this step of the wizard, specify data restore options and start the restore operation:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created.
2. Select the **Missing items** check box if you want to restore items that are missing in the target location. For example, some of the items were removed and you want to restore them from the backup.
3. By default, Veeam Explorer for Microsoft Teams restores all versions of backed-up files from the backup. If you want to restore only the latest version of a file, select the **Restore only the latest version** check box. If you select this option, Veeam Explorer for Microsoft Teams will merge original files in the production environment with the latest version of the files in the backup.
4. Click **Restore**.



Data Export

You can use Veeam Explorer for Microsoft Teams to export posts published in a team channel to a file of the HTML format. You can export all posts of a channel, export posts created during a specified time period or export individual posts.

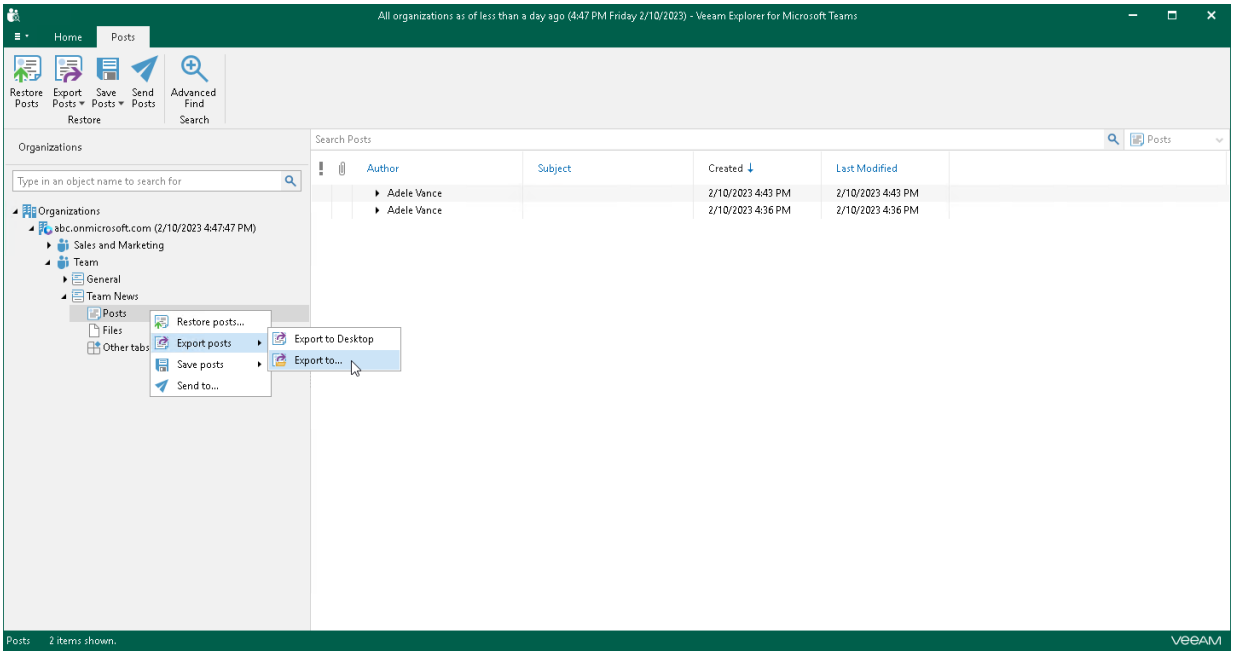
The export operation can be useful, for example, if you want to restore posts of a team channel to another channel. To do this, you can export posts to an HTML file, publish this file in Microsoft SharePoint and publish a link to this file in a custom tab of the necessary channel.

Before exporting data, read the Considerations and Limitations section.

Exporting Multiple Posts

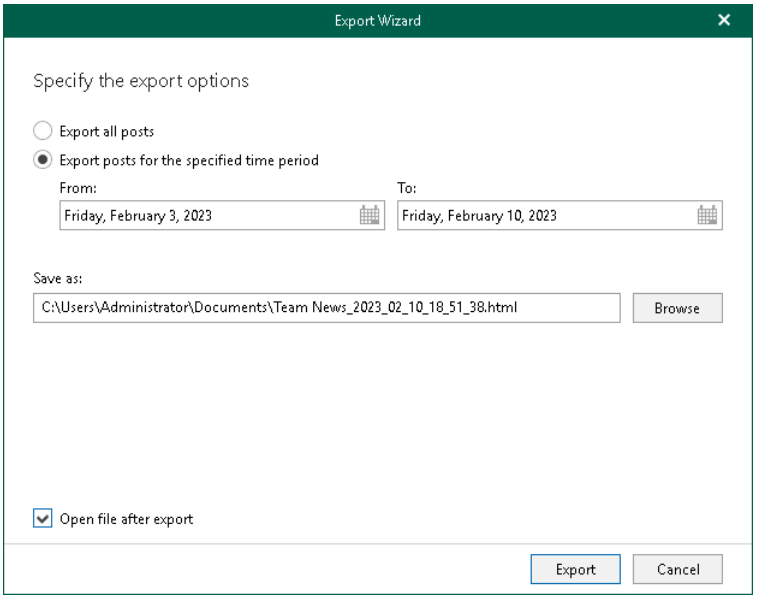
To export posts of a channel, do the following:

1. In the navigation pane, expand a channel whose posts you want to export and select **Posts**.
2. Do one of the following:
   - On the **Posts** tab, click **Export Posts** on the ribbon and select how you want to export posts:
     - **Export to Desktop**. Select this option if you want to perform the *1-Click Export* operation. Veeam Explorer for Microsoft Teams will immediately export all posts of the channel to the *Desktop* folder.
     - **Export to**. Select this option if you want to specify what posts to export and where to export posts.
   - Right-click **Posts** and select **Export posts** > **Export to Desktop** or **Export posts** > **Export to**.



3. If you selected the **Export to** option at the step 2, in the **Export** wizard, do the following:
   a. Specify what posts you want to export. You can select from the following options:
      - **Export all posts**. If you select this option, Veeam Explorer for Microsoft Teams will export all posts published in the channel to an HTML file.
      - **Export posts for the specified time period**. If you select this option, you can define a time period when posts that you want to export were created. To do this, specify the start date and end date of the period in the **From** and **To** fields. Veeam Explorer for Microsoft Teams will export posts whose last modification date belongs to the specified period.
   b. In the **Save as** field, click **Browse** and browse to a folder where you want to save an HTML file with exported posts. By default, Veeam Explorer for Microsoft Teams exports posts to a file with the following name: *<Channel_name>_<date_and_time>.html*. For example: *Team News_2023_02_10_18_51_38.html*.
   c. Select the **Open file after export** check box if you want to open the resulting HTML file right after the export operation is completed.

d. Click **Export**.

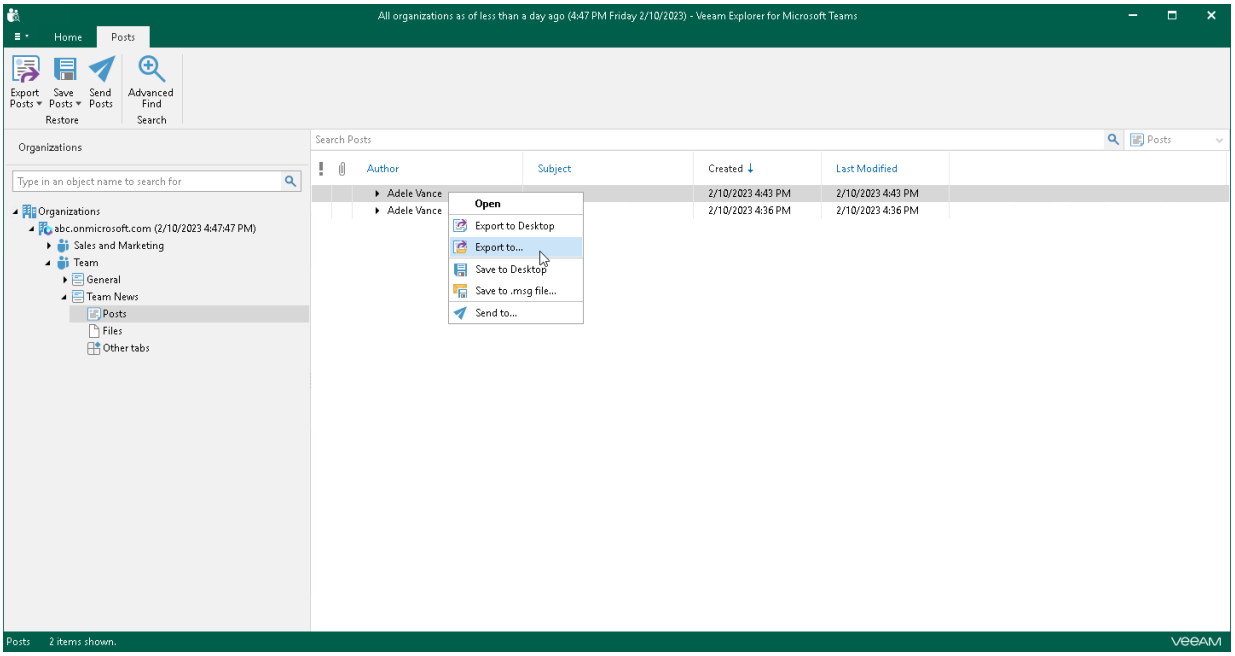


Exporting Individual Posts

To export a specific post of a channel, do the following:

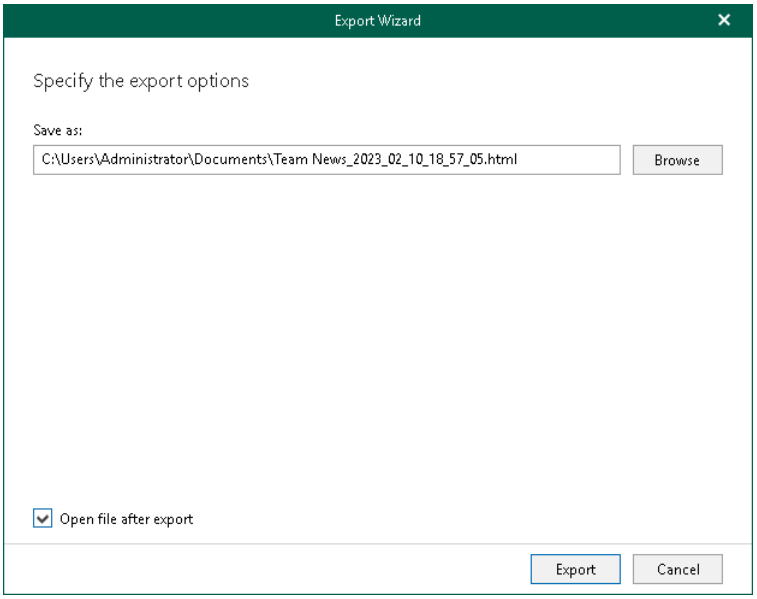
1. In the navigation pane, expand a channel whose post you want to export and select **Posts**.
2. In the preview pane, do one of the following:
   - Select a necessary post and on the **Posts** tab, click **Export Posts** on the ribbon and select how you want to export the post:
     - **Export to Desktop**. Select this option if you want to perform the *1-Click Export* operation. Veeam Explorer for Microsoft Teams will immediately export the post to the *Desktop* folder.
     - **Export to**. Select this option if you want to export the post to a custom location.
   - Right-click a necessary post and select **Export to Desktop** or **Export to**.

> **TIP**
>
> To select more than one post in the preview pane, press and hold the **[CTRL]** key and select the necessary posts.



3. If you selected the **Export to** option at the step 2, in the **Export** wizard, do the following:
   a. In the **Save as** field, click **Browse** and browse to a folder where you want to save an HTML file with exported posts. By default, Veeam Explorer for Microsoft Teams exports posts to a file with the following name: *<Channel_name>_<date_and_time>.html*. For example: *Team News_2023_02_10_18_57_05.html*.
   b. Select the **Open file after export** check box if you want to open the resulting HTML file right after the export operation is completed.

c. Click **Export**.



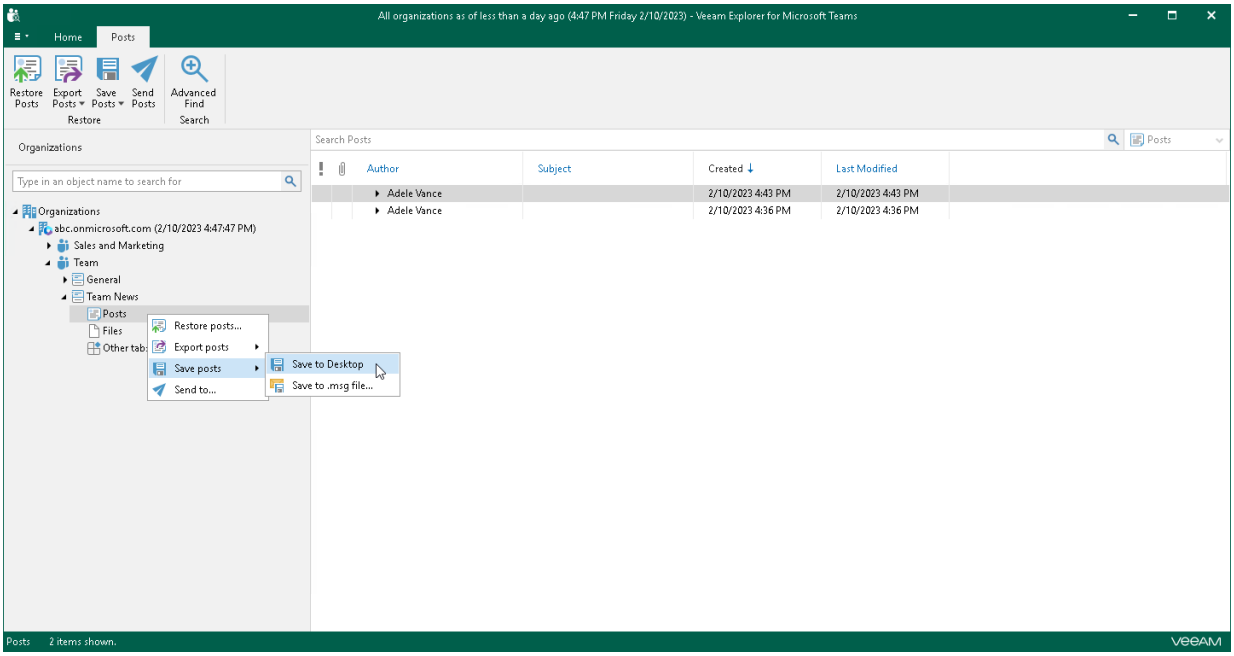
Saving Posts

You can use Veeam Explorer for Microsoft Teams to save posts published in a team channel as *Microsoft Exchange Mail Document* (*.msg*) files. You can save all posts of a channel or specific posts. Veeam Explorer for Microsoft Teams saves each post to a separate *.msg* file in the specified location.

Saving All Posts of Channel

To save posts published in a team channel, do the following:

1. In the navigation pane, expand a channel whose posts you want to save and select **Posts**.
2. Do one of the following:
   - On the **Posts** tab, click **Save Posts** on the ribbon and select where you want to save posts:
     - **Save to <folder_name>**. Select this option if you want to perform the *1-Click Save* operation. Veeam Explorer for Microsoft Teams will save posts to the latest location that was used when saving posts. If you have not saved posts yet, Veeam Explorer for Microsoft Teams save posts to the *Desktop* folder.
     - **Save to .msg file**. Select this option if you want to save posts to a custom location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
   - Right-click **Posts** and select **Save posts** > **Save to <folder_name>** or **Save posts** > **Save to .msg file**.



Saving Individual Posts

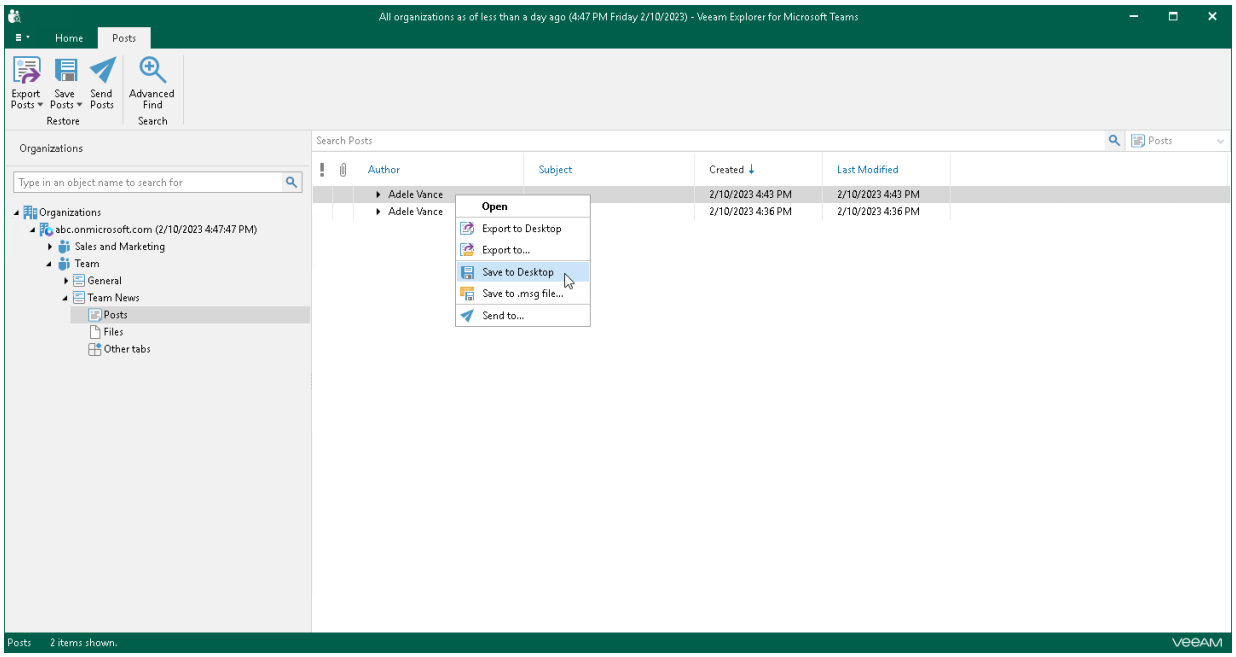
To save a specific post published in a team channel, do the following:

1. In the navigation pane, expand a channel whose post you want to save and select **Posts**.
2. In the preview pane, do one of the following:
   - Select a necessary post and on the **Posts** tab, click **Save Posts** on the ribbon and select where you want to save posts:

- **Save to <folder_name>**. Select this option if you want to perform the *1-Click Save* operation. Veeam Explorer for Microsoft Teams will save posts to the latest location that was used when saving posts. If you have not saved posts yet, Veeam Explorer for Microsoft Teams save posts to the *Desktop* folder.
- **Save to .msg file**. Select this option if you want to save posts to a custom location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.

o Right-click a necessary post and select **Save to <folder_name>** or **Save to .msg file**.

> **TIP**
>
> To select more than one post in the preview pane, press and hold the **[CTRL]** key and select the necessary posts.



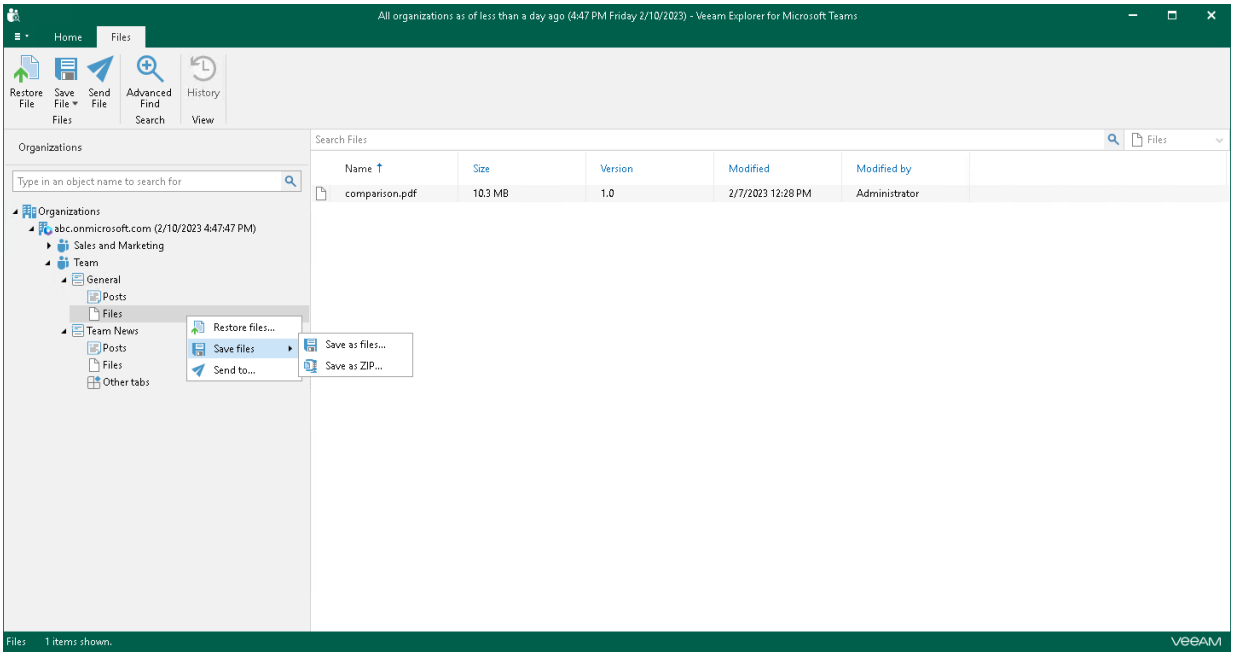
Saving Files

You can use Veeam Explorer for Microsoft Teams to save files published in a team channel to a specified location. You can save all files of a channel or specific posts.

Saving All Files of Channel

To save files published in a team channel, do the following:

1. In the navigation pane, expand a channel whose files you want to save and select **Files**.
2. Do one of the following:
   - On the **Files** tab, click **Save File** on the ribbon and select how you want to save files:
     - **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
     - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Save**. Veeam Explorer for Microsoft Teams will save files to an archive with the *<channel_name>.zip* name.
   - Right-click **Files** and select **Save files** > **Save as files** or **Save files** > **Save as ZIP**.



Saving Individual Files

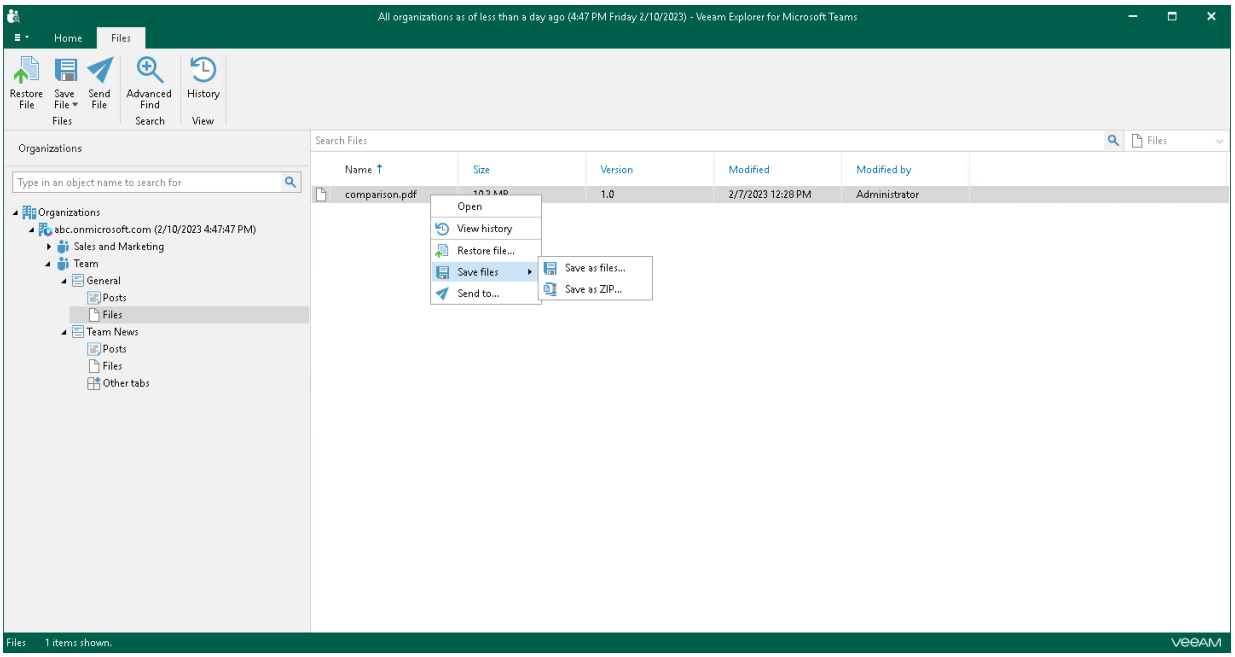
To save a specific file published in a team channel, do the following:

1. In the navigation pane, expand a channel whose files you want to save and select **Files**.
2. In the preview pane, do one of the following:
   - Select a necessary file and on the **Files** tab, click **Save File** on the ribbon and select how you want to save files:

- **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
- **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Save**. Veeam Explorer for Microsoft Teams will save files to an archive with the *archive.zip* name.

o Right-click a necessary file and select **Save file** > **Save as files** or **Save file** > **Save as ZIP**.

> **TIP**
>
> To select more than one file in the preview pane, press and hold the **[CTRL]** key and select the necessary files.



Sending Posts and Files

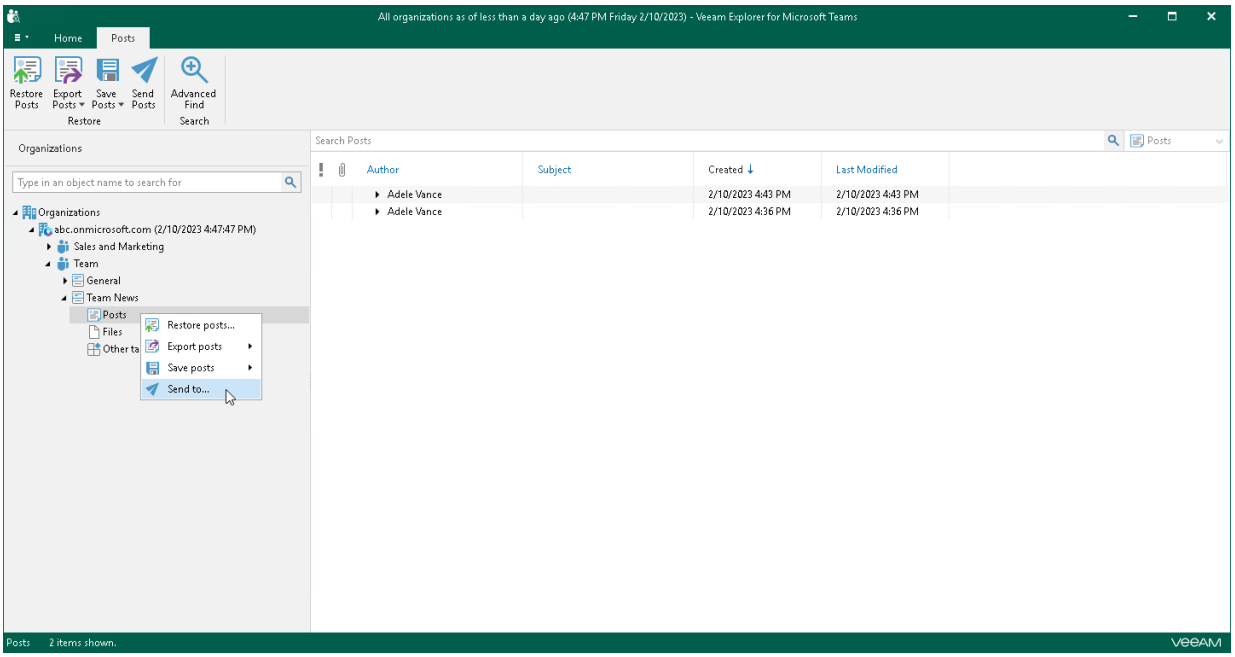
You can use Veeam Explorer for Microsoft Teams to send posts and files published in a team channel to specified recipients through email. You can send all posts or files of a channel or send individual posts or files.

> **TIP**
>
> Before sending documents, make sure to configure SMTP settings. The amount of data you can send at a time depends on your SMTP server configuration. For more information about configuring SMTP settings, see SMTP Settings.

Sending All Posts or Files of Channel

To send all posts or files of a team channel through email, do the following:

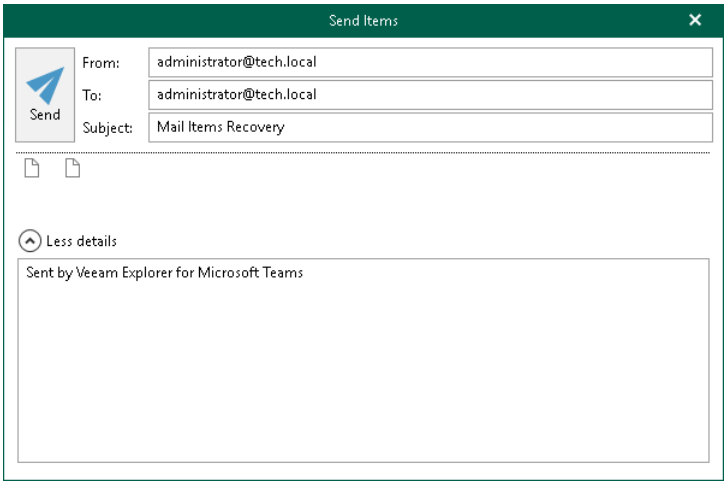
1. In the navigation pane, expand a channel whose posts or files you want to send and select **Posts** or **Files**.
2. Do one of the following:
   - On the **Posts/Files** tab, click **Send Posts/Send File** on the ribbon.
   - Right-click **Posts** or **Files** and select **Send to**.



3. In case the size of the message with files exceeds the size allowed by your SMTP server configuration, Veeam Explorer for Microsoft Teams will prompt whether you want to send files. In the notification window, click **Yes**.
4. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

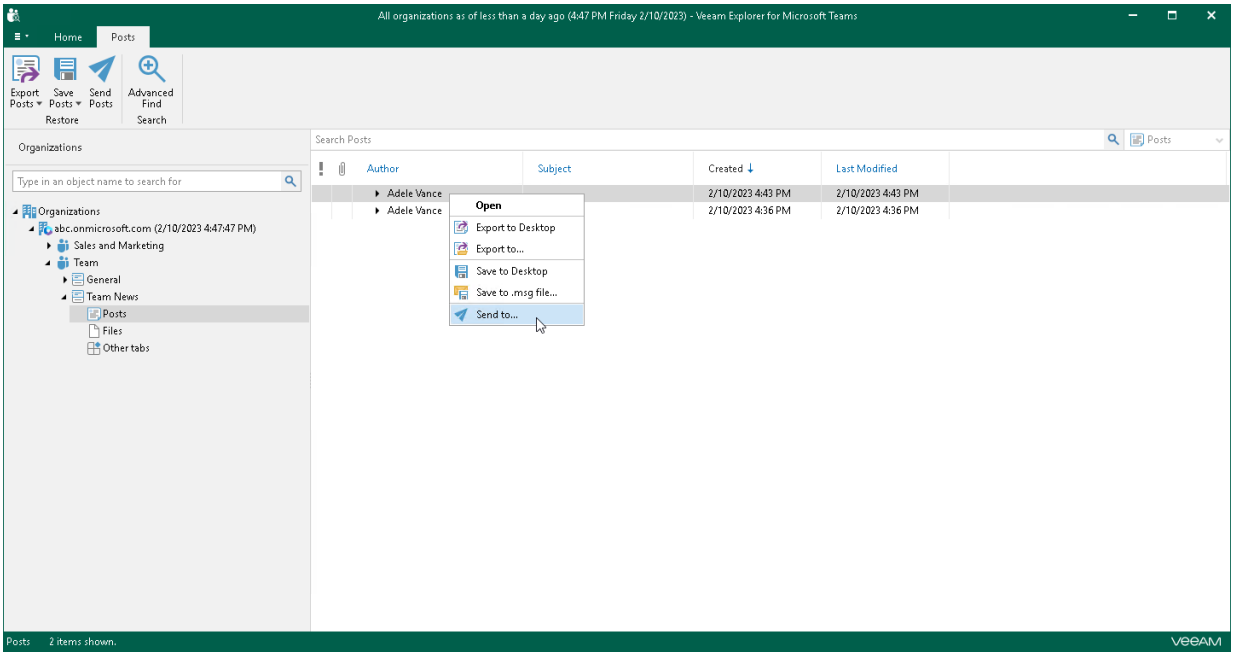
You can also edit the message subject and body. To edit the message body, click **More details**.



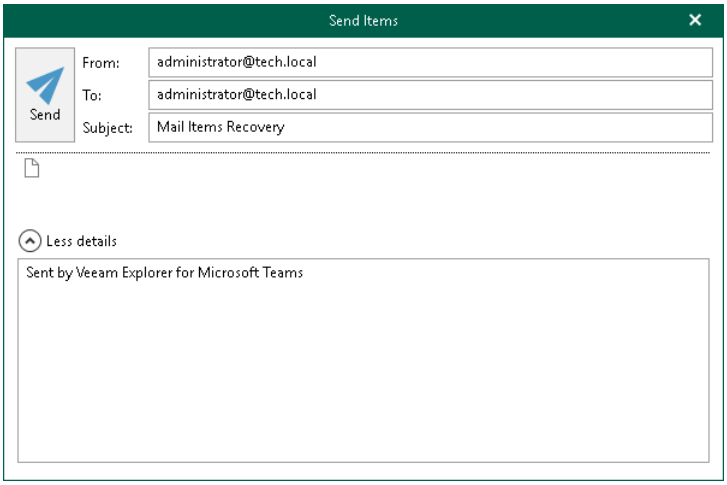
Sending Individual Posts or Files

To send a specific post or file of a team channel through email, do the following:

1. In the navigation pane, expand a channel whose post or file you want to send and select **Posts** or **Files**.
2. In the preview pane, do one of the following:
   - Select a necessary post or file and on the **Posts/Files** tab, click **Send Posts/Send File** on the ribbon.
   - Right-click a necessary post or file and select **Send to**.



3. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

You can also edit the message subject and body. To edit the message body, click **More details**.