Veeam Backup & Replication

Version 13

User Guide for Microsoft Entra ID

March, 2026

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

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 is designed for IT professionals who plan to use Veeam Backup for Microsoft Entra ID. The guide includes system requirements, licensing information and configuration instructions. It also provides a comprehensive set of features to ensure easy execution of protection and disaster recovery tasks in the Microsoft Entra ID environment.

Overview

Veeam Backup for Microsoft Entra ID is a solution developed for protection and disaster recovery tasks for Microsoft Entra ID. With Veeam Backup for Microsoft Entra ID, you can perform the following operations:

- Create backups of Microsoft Entra ID tenants and store them in PostgreSQL-based Entra ID repositories.
- Create backups of Microsoft Entra ID audit and sign-in logs and store them in backup repositories.
- Restore users, groups, administrative units, roles, applications, service principals, conditional access policies and intune policies from Microsoft Entra ID tenant backups to the Microsoft Entra ID environment.
- Restore properties of users, groups, administrative units, roles, applications, service principals, conditional access policies and intune policies from Microsoft Entra ID tenant backups to the Microsoft Entra ID environment.
- Restore audit and sign-in logs from Microsoft Entra ID log backups to a file server, object storage, or a local machine.

Solution Architecture

The Veeam Backup for Microsoft Entra ID architecture comprises the following set of components:

- Backup server
- General-purpose backup proxy
- Microsoft Entra ID backup repository
- Log backup repositories
- Cache repository

Backup Server

A backup server is a physical or virtual machine on which Veeam Backup & Replication is installed. The backup server is the configuration, administration and management core of the backup infrastructure. It coordinates backup and restore operations, controls job scheduling and manages resource allocation. In addition to its primary functions, backup server also performs the role of a general-purpose backup proxy — an architecture component that processes jobs and transfers data to and from backup repositories.

For more information on the backup server, see the Veeam Backup & Replication User Guide, sections Backup Server and General-Purpose Backup Proxies.

Microsoft Entra ID Backup Repository

A Microsoft Entra ID backup repository is a PostgreSQL instance where Veeam Backup for Microsoft Entra ID stores backups of protected Microsoft Entra ID tenants. By default, Veeam Backup for Microsoft Entra ID uses the local PostgreSQL instance installed on the backup server. To ensure data safety, you can instruct Veeam Backup for Microsoft Entra ID to use a remote instance. For more information on the Microsoft Entra ID backup repository configuration, see Configuring Repositories.

Log Backup Repositories

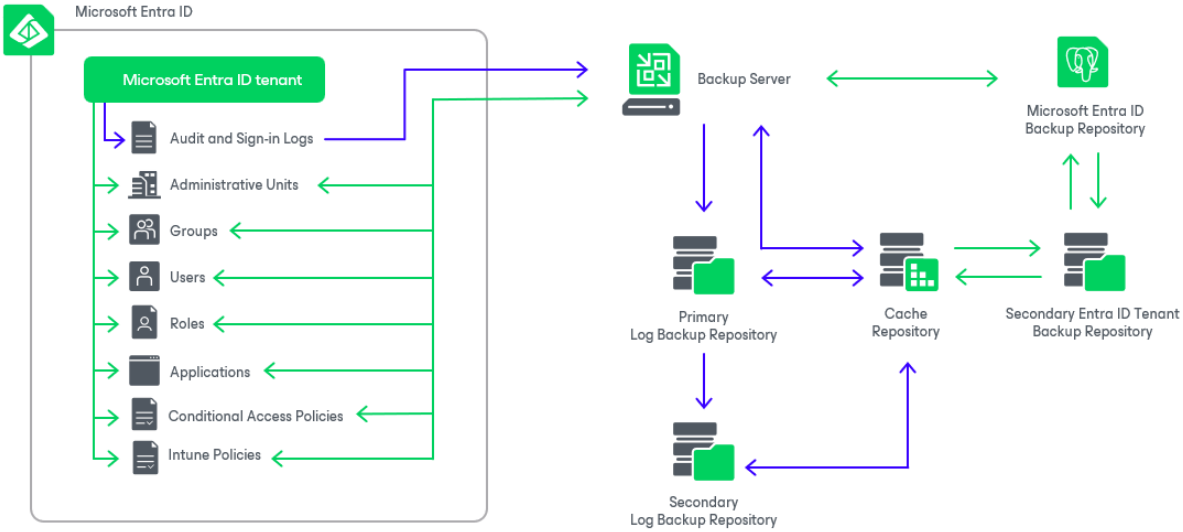
A log backup repository is a storage location where Veeam Backup for Microsoft Entra ID stores backups of audit and sign-in logs of protected Microsoft Entra ID tenants.

To increase log availability and ensure that data can be recovered in case a disaster strikes, you can store backed-up data of audit and sign-in logs in different locations — primary and secondary log backup repositories with their own retention policies and encryption settings.

Cache Repository

A cache repository is a storage location where Veeam Backup for Microsoft Entra ID keeps temporary metadata to reduce the load on the backup server when performing backup operations. The cache repository keeps track of all log records that change between backup sessions.

> **TIP**
>
> To minimize network load during backup operations, it is recommended that you configure the cache repository to be located closer to the backup server in the computer network.


Microsoft Entra ID
Microsoft Entra ID tenant
Audit and Sign-in Logs
Administrative Units
Groups
Users
Roles
Applications
Conditional Access Policies
Intune Policies
Backup Server
Microsoft Entra ID
Backup Repository
Primary
Log Backup Repository
Cache
Repository
Secondary Entra ID Tenant
Backup Repository
Secondary
Log Backup Repository

Protecting Tenant Data

To produce backups of Microsoft Entra ID tenant data, Veeam Backup for Microsoft Entra ID runs backup jobs. A backup job is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

Veeam Backup for Microsoft Entra ID does not install agent software to back up Microsoft Entra ID tenant data — it uses native Microsoft capabilities instead. During every backup session, Veeam Backup for Microsoft Entra ID creates a backup of the Microsoft Entra ID tenant added to a backup job.

How to Protect Microsoft Entra ID Tenant Data

To create a Microsoft Entra ID backup job, complete the following steps:

1. Check limitations and prerequisites.
2. Configure log and cache repositories.
3. Add a Microsoft Entra ID tenant.
4. Connect to a remote Microsoft Entra ID repository, if necessary.
5. Complete the New Microsoft Entra ID Tenant Backup Job wizard.

Tenant Backup

To perform tenant backup, Veeam Backup for Microsoft Entra ID does the following:

1. Creates a Microsoft Entra ID repository on a dedicated PostgreSQL instance.
2. Reads the data from the backup scope of the tenant added to the backup job.
3. Transfers the data to the target repository and stores it as an encrypted database record.

Tenant Restore

Veeam Backup for Microsoft Entra ID offers the following restore operations:

- Item restore — restores Microsoft Entra ID items such as users, groups, roles, administrative units, applications, conditional access policies and intune policies from a backup to the Entra ID environment. You can restore one or more items of the same type at a time.
- Properties restore — restores properties of Microsoft Entra ID items from a backup to the Entra ID environment. You can restore properties of only one item at a time.

You can restore tenant data to the most recent state or to any available restore point.

Protecting Logs

To produce backups of Microsoft Entra ID tenant logs, Veeam Backup for Microsoft Entra ID runs backup jobs. A backup job is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

Veeam Backup for Microsoft Entra ID does not install agent software to back up Microsoft Entra ID tenant logs — it uses native Microsoft capabilities instead. During every backup session, Veeam Backup for Microsoft Entra ID creates a copy of audit and sign-in logs for the Microsoft Entra ID tenant added to a backup job.

How to Protect Microsoft Entra ID Logs

To create a Microsoft Entra ID log backup job, complete the following steps:

1. Check limitations and prerequisites.
2. Configure log and cache repositories.
3. Add a Microsoft Entra ID tenant.
4. Connect to a remote Microsoft Entra ID repository, if necessary.
5. Complete the New Microsoft Entra ID Log Backup Job wizard.

Planning and Preparation

Before you start using Veeam Backup for Microsoft Entra ID, check system requirements, limitations, permissions and network ports used for data transmission.

System Requirements

Specification	Requirement
Veeam Backup & Replication	Veeam Backup & Replication version 13.0.1 must be deployed on the backup server.
Backup server	The backup server must meet the system requirements listed in the Veeam Backup & Replication User Guide, section System Requirements.
Veeam Backup & Replication console	64-bit versions of the following Microsoft Windows operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (versions 22H2, 23H2, 24H2) • Microsoft Windows 10 (versions 1909 to 22H2) • Microsoft Windows 10 LTS (versions 21H2 LTSC, 22H2 GA) Other system requirements for the Veeam Backup & Replication console are listed in the Veeam Backup & Replication User Guide, section Veeam Backup & Replication Console System Requirements.
Backup proxy	The general-purpose backup proxy must meet the system requirements listed in the Veeam Backup & Replication User Guide, section System Requirements.
Microsoft Entra ID backup repository	The Microsoft Entra ID backup repository stores tenant backups. This repository is based on a PostgreSQL instance. The requirements for this instance are the same as for the PostgreSQL instance that stores configuration database on the backup server. For more information, see the Configuration Database row in Backup Server System Requirements section in the Veeam Backup & Replication User Guide. **Note:** It is also recommended that you adjust the settings of the PostgreSQL instance that you plan to use as the Microsoft Entra ID backup repository. For more information, see Veeam Backup & Replication User Guide, section Adjusting PostgreSQL Instance Configuration.
Cache repository	The cache repository stores temporary cache files for log processing. This repository must meet system requirements described in the Cache Repository System Requirements section in the Veeam Backup & Replication User Guide.

Specification	Requirement
Log backup repository	The primary and secondary log backup repositories store audit and sign-in log backups and their copies. These repositories must meet requirements described in the Backup Repository System Requirements section in the Veeam Backup & Replication User Guide. For information on which types of repositories can be used as primary and secondary repositories, see Configuring Repositories.

Permissions

The accounts that Veeam Backup for Microsoft Entra ID uses to deploy and manage backup infrastructure components must be granted the following permissions.

Veeam Backup & Replication User Account Permissions

A user account that you plan to use when installing and working with Veeam Backup & Replication must have permissions described in the Veeam Backup & Replication User Guide, section Installing and Using Veeam Backup & Replication.

Microsoft Entra Roles and Permissions

Veeam Backup for Microsoft Entra ID requires a Microsoft Entra application whose permissions are used to add Microsoft Entra ID tenants to the backup infrastructure and to perform backup and restore operations with Microsoft Entra ID resources.

Adding and Backing Up Tenants

You can specify an existing application or instruct Veeam Backup & Replication to create a new one. The list of permissions granted to the Microsoft Entra application and the list of roles assigned to the Microsoft Entra ID user account that you use to create the application depend on the actions you plan to perform using the application.

Application	Permissions
New	The Microsoft Entra ID user account associated with the tenant where the Microsoft Entra ID application will be created must have the following built-in roles assigned: • Application Administrator • Privileged Role Administrator As an alternative, you can assign the Global Administrator Microsoft Entra built-in role.
Existing	To perform backup, the application must have the following permissions: • Microsoft Graph application permissions: *AuditLog.Read.All*, *Directory.Read.All*, *Group.Read.All*, *MailboxSettings.Read*, *RoleManagement.Read.Directory*, *User.Read.All*, *Policy.Read.All*, *Policy.ReadWrite.ConditionalAccess*, *Agreement.Read.All*, *DeviceManagementConfiguration.Read.All*.

Application	Permissions
	To be able to further perform restore, the application must have the following permissions: • Microsoft Graph delegated permissions: *Directory.ReadWrite.All*, *RoleManagement.ReadWrite.Directory*, *AdministrativeUnit.ReadWrite.All*, *Directory.AccessAsUser.All*, *Application.ReadWrite.All*, *Group.ReadWrite.All*, *Policy.ReadWrite.ConditionalAccess*, *Agreement.Read.All*, *DeviceManagementConfiguration.ReadWrite.All* • API delegated permissions: *user_impersonation* **Note**: Make sure that the Allow public client flows option is enabled for the application. For more information, see Microsoft Docs.

IMPORTANT

By default, Veeam Backup for Microsoft Entra ID does not back up relationships between protected resources and management groups. If you want to add these relationships into the backup scope, you must perform additional configuration steps described in this Veeam KB article.

Restoring Tenant Data

To restore tenant data, Veeam Backup for Microsoft Entra ID uses the Microsoft Entra application that was used to add the tenant. This application has delegated access and acts on behalf of a user that you specify in the restore wizard.

This user must have with the following roles:

- Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Groups Administrator
- Privileged Role Administrator
- Privileged Authentication Administrator
- User Administrator
- Intune Administrator

As an alternative, you can use Global Administrator Microsoft Entra plus Conditional Access Administrator (recommended) or plus Security Administrator roles.

Ports

The main ports required to create backups of Microsoft Entra ID tenants are listed in the following table.

From	To	Protocol	Port	Notes
Veeam Backup & Replication console	Backup server	TCP	9419	—
	Backup server	TCP	443	—
Backup server	[Optional] PostgreSQL server hosting the database for the Microsoft Entra ID backup repository	TCP	5432	This port is required if the database is located on a remote PostgreSQL server. Port number may differ if you configure a custom PostgreSQL server instance as Microsoft Entra ID backup repository.
	[Optional] HTTP proxy server (For Linux-based instances of Veeam Backup & Replication)	TCP	HTTP proxy server port	This port is required if you configure a proxy server as described in Veeam Backup & Replication User Guide, section Configuring HTTP/HTTPS Proxies.
	Microsoft Entra ID Services (Service tag: AzureActiveDirectory)	TCP	443	To access the necessary Azure service, you can use the IP address, DNS name or virtual network service tag of the service. If you want to use an IP address, you can download a .JSON file with the full list of Azure IP ranges and service tags from the Microsoft Download Center.
	Azure Resource Manager (Service tag: AzureResourceManager)	TCP	443	
[Optional] HTTP proxy server (for Linux-based instances of Veeam Backup & Replication)	Microsoft Entra ID Services (Service tag: AzureActiveDirectory)	TCP	443	
	Azure Resource Manager (Service tag: AzureResourceManager)	TCP	443	
[Optional] Cache repository	Gateway server	TCP		Cache repository is required to use the log

From	To	Protocol	Port	Notes
	Primary or secondary backup repository		2500 to 3300	backup and log backup copy features.
[Optional] Backup server	Cache repository	TCP	6160, 6162	
	Old cache repository, new cache repository	TCP	2500 to 3300	

IMPORTANT

- As Veeam Backup for Microsoft Entra ID is installed on the same machine where Veeam Backup & Replication runs, it also uses the same ports. To be able to use the tenant backup copy feature, you must configure the ports listed in the Backup Repositories section of the Veeam Backup & Replication User Guide.
- Veeam Backup for Microsoft Entra ID does not support remote backup proxies — instead, the backup server performs the role of a general-purpose backup proxy.

Considerations and Limitations

When you plan to deploy and configure Veeam Backup for Microsoft Entra ID, keep in mind the following limitations and considerations.

Backup Infrastructure

- It is not recommended that you delete or disable the default general-purpose backup proxy deployed during Veeam Backup & Replication installation. Otherwise, Veeam Backup for Microsoft Entra ID will not be able to perform tenant backup, log backup and backup copy operations.
- Veeam Backup for Microsoft Entra ID does not support creation of more than one Microsoft Entra ID backup repository on the backup server.
- Veeam Backup for Microsoft Entra ID supports storing backed-up tenant data in Microsoft Entra ID backup repositories running PostgreSQL 14 or higher.
- Veeam Backup for Microsoft Entra ID supports only PostgreSQL password authentication to connect to remote Microsoft Entra ID backup repositories. For more information, see Connecting to Remote Microsoft Entra ID Backup Repository.

Tenant Backup and Restore

- Veeam Backup for Microsoft Entra ID does not support the Government and China regions.
- Veeam Backup for Microsoft Entra ID does not support backup and restore of Microsoft Entra External ID tenants and Azure B2C tenants.
- Each restore operation is limited to 1000 items per session.
- For one Microsoft Entra ID tenant, you can create only one tenant backup job. One tenant backup job can protect only one tenant.
- Veeam Backup for Microsoft Entra ID does not support restore of the following item types: built-in role, distribution security group, mail-enabled security group.

By default, Veeam Backup for Microsoft Entra ID does not back up relationships between protected resources and management groups. If you want to add these relationships into the backup scope, you must perform additional configuration steps described in this Veeam KB article.

- During one restore session, you can restore items of one type only. For example, only users or only groups, not users and groups.

[Entire restore of permanently deleted and linked applications and service principles] You can restore a service principle that represents an application only together with this application and within one restore session. If you restore the application in a separate restore session, the restored application gets a new AppID. The service principal will not recognize this new ID, and the restore of the service principal will fail.

- Restore of users synchronized with Microsoft Active Directory (hybrid identities) is possible using Veeam Backup for Microsoft Entra ID. For more information, see Appendix. Restoring Synchronized Users (Hybrid Identity).

- Veeam Backup for Microsoft Entra ID does not support restore of Intune Device Configuration of type `editionUpgradeConfiguration` with application permissions. You can restore this intune policy using delegated permissions only. During restore of Intune Device Configuration of type `editionUpgradeConfiguration`, the properties `License` and `ProductKey` are restored to predefined placeholder values. After restore, these properties must be manually updated in the Intune Admin Center.

Log Backup and Restore

- Veeam Backup for Microsoft Entra ID does not support log backup to multi-bucket repositories. For more information, see Veeam Backup & Replication User Guide.
- You cannot back up sign-in logs with Microsoft Entra ID free license. With this license, you can back up only audit logs.
- To create a log backup, you must have the backup of the tenant whose logs you want to protect. The latest restore point of this backup must be created within 30 days before the log backup.

Supported Entra ID Item Properties

Veeam Backup for Microsoft Entra ID supports protection of the following Microsoft Entra ID items and their properties.

Users

Property	Comments
AccountEnabled	—
AgeGroup	—
AppRoleAssignments	—
AssignedLicenses	—
BusinessPhones	—
City	—
CompanyName	—
ConsentProvidedForMinor	—
Country	—
CreatedDateTime	Read-only property in Entra ID.
Department	—
DirectReports	—
DisplayName	—
EmployeeId	—
EmployeeType	—
FaxNumber	—
GivenName	—
Identities	—
JobTitle	—

Mail	—
MailNickname	—
Manager	—
MemberOf	—
MobilePhone	—
OfficeLocation	—
OnPremisesDistinguishedName	Read-only property in Entra ID.
OnPremisesDomainName	Read-only property in Entra ID.
OnPremisesExtensionAttributes	—
OnPremisesImmutableId	—
OtherMails	—
OwnedObjects	—
PasswordPolicies	—
PostalCode	—
PreferredDataLocation	—
State	—
StreetAddress	—
Surname	—
UsageLocation	—
UserPrincipalName	—

UserType	—

> **NOTE**
>
> Besides the listed properties, Veeam Backup for Microsoft Entra ID also protects role assignments for the users. This role assignment protection is available for Microsoft Entra ID P2 and Governance tenant licenses.

Groups

Property	Comments
AllowExternalSenders	—
AppRoleAssignments	Not available for restore.
AssignedLabels	—
AssignedLicenses	—
Classification	—
CreatedDateTime	Read-only property in Entra ID.
Description	—
DisplayName	—
GroupTypes	—
IsAssignableToRole	Read-only property in Entra ID.
Mail	Read-only property in Entra ID.
MailEnabled	Read-only property in Entra ID.
MailNickname	—
MemberOf	—
Members	—
MembershipRule	—
MembershipRuleProcessingState	—
OnPremisesDomainName	Read-only property in Entra ID.
Owners	—

PreferredDataLocation	–
SecurityEnabled	–
Theme	–
Visibility	–

Administrative Units

Property	Comments
Description	–
Visibility	–
DisplayName	–
Extensions	Not supported for restore.
Members	Can be restored only for non-hidden administrative units.
ScopedRoleMembers	Limited to directory role membership, custom role membership is not supported.

Roles

Property	Comments
Description	—
DisplayName	—
InheritsPermissionsFrom	—
IsBuiltIn	Read-only property in Entra ID.
IsEnabled	—
ResourceScopes	—
RolePermissions	—
TemplateId	—
Version	—

Applications

Property	Comments
AddIns	—
Api	—
AppId	Read-only property in Entra ID.
ApplicationTemplateId	Read-only property in Entra ID.
AppRoles	—
Certification	Read-only property in Entra ID.
CreatedDateTime	Read-only property in Entra ID.
Description	—
DisabledByMicrosoftStatus	Read-only property in Entra ID.
DisplayName	—
ExtensionProperties	—
FederatedIdentityCredentials	—
GroupMembershipClaims	—
IdentifierUris	—
Info	—
IsDeviceOnlyAuthSupported	—
IsFallbackPublicClient	—
Notes	—
Oauth2RequirePostResponse	—

OptionalClaims	—
Owners	—
ParentalControlSettings	—
PublicClient	—
PublisherDomain	Read-only property in Entra ID.
RequestSignatureVerification	—
RequiredResourceAccess	—
SamlMetadataUrl	—
ServiceManagementReference	—
ServicePrincipalLockConfiguration	—
SignInAudience	—
Spa	—
Tags	—
TokenEncryptionKeyId	Read-only property in Entra ID.
VerifiedPublisher	Read-only property in Entra ID.
Web	—

Service Principals

Property	Comments
AccountEnabled	—
AddIns	Read-only property. The property value is inherited from the associated application.
AlternativeNames	—
AppDescription	Read-only property. The property value is inherited from the associated application.
AppDisplayName	Read-only property. The property value is inherited from the associated application.
AppId	Read-only property in Entra ID.
ApplicationTemplateId	Read-only property in Entra ID.
AppManagementPolicies	Read-only property in Entra ID.
AppOwnerOrganizationId	Read-only property in Entra ID.
AppRoleAssignedTo	—
AppRoleAssignmentRequired	—
AppRoleAssignments	—
AppRole	Read-only property. The property value is inherited from the associated application.
Description	—
DisabledByMicrosoftStatus	Read-only property in Entra ID.
DisplayName	Read-only property. The property value is inherited from the associated application.
Endpoints	—
FederatedIdentityCredentials	Read-only property in Entra ID.

Homepage	Read-only property. The property value is inherited from the associated application.
Info	Read-only property. The property value is inherited from the associated application.
LoginUrl	—
LogoutUrl	Read-only property in Entra ID.
MemberOf	—
Notes	—
NotificationEmailAddresses	—
Oauth2PermissionGrants	—
Oauth2PermissionScopes	Read-only property. The property value is inherited from the associated application.
OwnedObjects	Read-only property in Entra ID.
Owners	—
PasswordCredentials	Read-only property in Entra ID.
PreferredSingleSignOnMode	—
ReplyUrls	Read-only property in Entra ID.
ResourceSpecificApplicationPermissions	Read-only property in Entra ID.
SamlSingleSignOnSettings	—
ServicePrincipalNames	Read-only property. The property value is inherited from the associated application.
ServicePrincipalType	Read-only property in Entra ID.
SignInAudience	Read-only property in Entra ID.

Tags	—
TokenEncryptionKeyId	Read-only property in Entra ID.
VerifiedPublisher	Read-only property in Entra ID.

Conditional Access Policies

Property	Comments
Conditions	—
CreatedDateTime	Read-only property in Entra ID.
DisplayName	—
GrantControls	—
ModifiedDateTime	Read-only property in Entra ID.
SessionControls	—
State	—
TemplateId	Read-only property in Entra ID.

Intune Policies A to B

AccountBlockModification	—
AccountManagerPolicy	—
AccountsBlockAddingNonMicrosoftAccountEmail	—
ActivationLockAllowWhenSupervised	—
ActiveHoursEnd	—
ActiveHoursStart	—

AirDropBlocked	–
AirDropForceUnmanagedDropTarget	–
AirPlayForcePairingPasswordForOutgoingRequests	–
AllowLocalStorage	–
AllowPrinting	–
AllowSampleSharing	–
AllowTextSuggestion	–
AllowWindows11Upgrade	–
AllowedAccounts	–
AppLockerApplicationControl	–
AppStoreBlockAutomaticDownloads	–
AppStoreBlockInAppPurchases	–
AppStoreBlockUIAppInstallation	–
AppStoreBlocked	–
AppStoreRequirePassword	–
AppleNewsBlocked	–
AppleWatchBlockPairing	–
AppleWatchForceWristDetection	–
ApplicationGuardAllowPersistence	–
ApplicationGuardAllowPrintToLocalPrinters	–

ApplicationGuardAllowPrintToNetworkPrinters	–
ApplicationGuardAllowPrintToPDF	–
ApplicationGuardAllowPrintToXPS	–
ApplicationGuardBlockClipboardSharing	–
ApplicationGuardBlockFileTransfer	–
ApplicationGuardBlockNonEnterpriseContent	–
ApplicationGuardEnabled	–
ApplicationGuardForceAuditing	–
ApplyOnlyToWindows81	–
ApplyOnlyToWindowsPhone81	–
AppsAllowTrustedAppsSideloading	–
AppsBlockClipboardSharing	–
AppsBlockCopyPaste	–
AppsBlockWindowsStoreOriginatedApps	–
AppsBlockYouTube	–
AppsHideList	–
AppsInstallAllowList	–
AppsLaunchBlockList	–
AppsSingleAppModeList	–
AppsVisibilityList	–

AppsVisibilityListType	–
AssetTagTemplate	–
Assignments	–
AutomaticUpdateMode	–
AutoRestartNotificationDismissal	–
AzureOperationalInsightsBlockTelemetry	–
AzureOperationalInsightsWorkspaceId	–
AzureOperationalInsightsWorkspaceKey	–
BitLockerDisableWarningForOtherDiskEncryption	–
BitLockerEnableStorageCardEncryptionOnMobile	–
BitLockerEnabled	–
BitLockerEncryptDevice	–
BitLockerRemovableDrivePolicy	–
BluetoothAllowedServices	–
BluetoothBlockAdvertising	–
BluetoothBlockDiscoverableMode	–
BluetoothBlockModification	–
BluetoothBlockPrePairing	–
BluetoothBlocked	–
BrowserBlockAutofill	–

BrowserBlockAutomaticDetectionOfIntranetSites	–
BrowserBlockEnterpriseModeAccess	–
BrowserBlockJavaScript	–
BrowserBlockPlugins	–
BrowserBlockPopups	–
BrowserBlockSendingDoNotTrackHeader	–
BrowserBlockSingleWordEntryOnIntranetSites	–
BrowserEnterpriseModeSiteListLocation	–
BrowserInternetSecurityLevel	–
BrowserIntranetSecurityLevel	–
BrowserLoggingReportLocation	–
BrowserRequireFirewall	–
BrowserRequireFraudWarning	
BrowserRequireHighSecurityForRestrictedSites	–
BrowserRequireSmartScreen	–
BrowserTrustedSitesSecurityLevel	–
BusinessReadyUpdatesOnly	–

Intune Policies C to E

Property	Comments
CameraBlocked	—
CellularBlockDataRoaming	—
CellularBlockDataWhenRoaming	—
CellularBlockGlobalBackgroundFetchWhileRoaming	—
CellularBlockMessaging	Read-only property in Entra ID.
CellularBlockPerAppDataModification	—
CellularBlockPersonalHotspot	—
CellularBlockVoiceRoaming	Read-only property in Entra ID.
CellularBlockVpn	—
CellularBlockVpnWhenRoaming	—
CellularBlockWiFiTethering	—
CertificatesBlockManualRootCertificateInstallation	—
CertificatesBlockUntrustedTlsCertificates	—
ClassroomAppBlockRemoteScreenObservation	—
ClassroomAppForceUnpromptedScreenObservation	—
CodeIntegrityEnabled	—
CompliantAppListType	—
CompliantAppsList	—
ConfigurationAccount	—

ConfigurationProfileBlockChanges	–
ConnectAppBlockAutoLaunch	–
ConnectedDevicesServiceBlocked	–
CopyPasteBlocked	–
CortanaBlocked	–
CreatedDateTime	–
DeadlineForFeatureUpdatesInDays	–
DeadlineForQualityUpdatesInDays	–
DeadlineGracePeriodInDays	–
DefinitionLookupBlocked	–
DefenderAdditionalGuardedFolders	–
DefenderAttackSurfaceReductionExcludedPaths	–
DefenderBlockEndUserAccess	–
DefenderCloudBlockLevel	–
DefenderDaysBeforeDeletingQuarantinedMalware	–
DefenderDetectedMalwareActions	–
DefenderExploitProtectionXml	–
DefenderExploitProtectionXmlFileName	–
DefenderFileExtensionsToExclude	–
DefenderFilesAndFoldersToExclude	–

DefenderGuardedFoldersAllowedAppPaths	–
DefenderMonitorFileActivity	–
DefenderProcessesToExclude	–
DefenderPromptForSampleSubmission	–
DefenderRequireBehaviorMonitoring	–
DefenderRequireCloudProtection	–
DefenderRequireNetworkInspectionSystem	–
DefenderRequireRealTimeMonitoring	–
DefenderScanArchiveFiles	–
DefenderScanDownloads	–
DefenderScanIncomingMail	–
DefenderScanMappedNetworkDrivesDuringFullScan	–
DefenderScanMaxCpu	–
DefenderScanNetworkFiles	–
DefenderScanRemovableDrivesDuringFullScan	–
DefenderScanScriptsLoadedInInternetExplorer	–
DefenderScanType	–
DefenderScheduledQuickScanTime	–
DefenderScheduledScanTime	–
DefenderSecurityCenterBlockExploitProtectionOverride	–

DefenderSignatureUpdateIntervalInHours	–
DefenderSystemScanSchedule	–
DeliveryOptimizationMode	–
DeviceBlockEnableRestrictions	–
DeviceBlockEraseContentAndSettings	–
DeviceBlockNameModification	–
DeviceManagementBlockFactoryResetOnMobile	–
DeviceManagementBlockManualUnenroll	–
DeviceSettingStateSummaries	–
DeviceSharingAllowed	–
DeviceStatusOverview	–
DeviceThreatProtectionEnabled	–
DeviceThreatProtectionRequiredSecurityLevel	–
DiagnosticDataBlockSubmission	–
DiagnosticDataBlockSubmissionModification	–
DiagnosticsBlockDataSubmission	–
DiagnosticsDataSubmissionMode	–
DisableAccountManager	–
DisableEduPolicies	–
DisablePowerPolicies	–

DisableSignInOnResume	–
DisplayName	–
DocumentsBlockManagedDocumentsInUnmanagedApps	–
DocumentsBlockUnmanagedDocumentsInManagedApps	–
DriversExcluded	–
EarlyLaunchAntiMalwareDriverEnabled	–
EdgeAllowStartPagesModification	–
EdgeBlockAccessToAboutFlags	–
EdgeBlockAddressBarDropdown	–
EdgeBlockAutofill	–
EdgeBlockCompatibilityList	–
EdgeBlockDeveloperTools	–
EdgeBlockExtensions	–
EdgeBlockInPrivateBrowsing	–
EdgeBlockJavaScript	–
EdgeBlockLiveTileDataCollection	–
EdgeBlockPasswordManager	–
EdgeBlockPopups	–
EdgeBlockSearchSuggestions	–
EdgeBlockSendingDoNotTrackHeader	–

EdgeBlockSendingIntranetTrafficToInternetExplorer	–
EdgeClearBrowsingDataOnExit	–
EdgeCookiePolicy	–
EdgeDisableFirstRunPage	–
EdgeEnterpriseModeSiteListLocation	–
EdgeFirstRunUrl	–
EdgeHomepageUrls	–
EdgeRequireSmartScreen	–
EdgeSearchEngine	–
EdgeSendIntranetTrafficToInternetExplorer	–
EdgeSyncFavoritesWithInternetExplorer	–
EmailBlockAddingAccounts	–
EmailInDomainSuffixes	–
EnableExpeditedTelemetryReporting	–
Enabled	–
EngagedRestartDeadlineInDays	–
EngagedRestartSnoozeScheduleInDays	–
EngagedRestartTransitionScheduleInDays	–
EnterpriseAppBlockTrust	–
EnterpriseAppBlockTrustModification	–

EnterpriseCloudPrintDiscoveryEndPoint	—
EnterpriseCloudPrintDiscoveryMaxLimit	—
EnterpriseCloudPrintMopriaDiscoveryResourceIdentifier	—
EnterpriseCloudPrintOAuthAuthority	—
EnterpriseCloudPrintOAuthClientIdentifier	—
EnterpriseCloudPrintResourceIdentifier	—
ExperienceBlockDeviceDiscovery	—
ExperienceBlockDeviceDiscovery	—
ExperienceBlockErrorDialogWhenNoSIM	—
ExperienceBlockTaskSwitcher	—

Intune Policies F to L

Property	Comments
FaceTimeBlocked	–
FeatureUpdatesDeferralPeriodInDays	Read-only property in Entra ID.
FeatureUpdatesPaused	–
FeatureUpdatesPauseExpiryDateTime	–
FeatureUpdatesPauseStartDate	Read-only property in Entra ID.
FeatureUpdatesRollbackStartDateTime	–
FeatureUpdatesRollbackWindowInDays	–
FeatureUpdatesWillBeRolledBack	Read-only property in Entra ID.
FindMyFriendsBlocked	–
FirewallBlockAllIncoming	–
FirewallBlockStatefulFTP	–
FirewallCertificateRevocationListCheckMethod	–
FirewallEnabled	–
FirewallEnableStealthMode	–
FirewallIdleTimeoutForSecurityAssociationInSeconds	–
FirewallIPSecExemptionsAllowDHCP	–
FirewallIPSecExemptionsAllowICMP	–
FirewallIPSecExemptionsAllowNeighborDiscovery	–
FirewallIPSecExemptionsAllowRouterDiscovery	–

FirewallMergeKeyingModuleSettings	–
FirewallPacketQueueingMethod	–
FirewallPreSharedKeyEncodingMethod	–
FirewallProfileDomain	–
FirewallProfilePrivate	–
FirewallProfilePublic	–
GameCenterBlocked	–
GameDvrBlocked	–
GamingBlockGameCenterFriends	–
GamingBlockMultiplayer	–
GoogleAccountBlockAutoSync	–
GooglePlayStoreBlocked	–
HomeScreenDockIcons	–
HomeScreenPages	–
HostPairingBlocked	–
IBooksStoreBlocked	–
IBooksStoreBlockErotica	–
ICloudBlockActivityContinuation	–
ICloudBlockBackup	–
ICloudBlockDocumentSync	–

ICloudBlockManagedAppsSync	–
ICloudBlockPhotoLibrary	–
ICloudBlockPhotoStreamSync	–
ICloudBlockSharedPhotoStream	–
ICloudRequireEncryptedBackup	–
ITunesBlockExplicitContent	–
ITunesBlockMusicService	–
ITunesBlockRadio	–
IdleTimeBeforeSleepInSeconds	–
InstallationSchedule	–
InternetSharingBlocked	–
KioskAppDisplayName	–
KioskAppUserModelId	–
KioskModeAllowAssistiveSpeak	–
KioskModeAllowAssistiveTouchSettings	–
KioskModeAllowAutoLock	–
KioskModeAllowColorInversionSettings	–
KioskModeAllowRingerSwitch	–
KioskModeAllowScreenRotation	–
KioskModeAllowSleepButton	–

KioskModeAllowTouchscreen	–
KioskModeAllowVoiceOverSettings	–
KioskModeAllowVolumeButtons	–
KioskModeAllowZoomSettings	–
KioskModeAppStoreUrl	–
KioskModeApps	–
KioskModeBlockSleepButton	–
KioskModeBlockVolumeButtons	–
KioskModeBuiltInAppId	–
KioskModeManagedAppId	–
KioskModeRequireAssistiveTouch	–
KioskModeRequireColorInversion	–
KioskModeRequireMonoAudio	–
KioskModeRequireVoiceOver	–
KioskModeRequireZoom	–
LaunchUri	–
LastModifiedDateTime	–
License	–
LicenseType	–
LocationServicesBlocked	–

LockScreenAllowTimeoutConfiguration	–
LockScreenBlockActionCenterNotifications	–
LockScreenBlockControlCenter	–
LockScreenBlockCortana	–
LockScreenBlockNotificationView	–
LockScreenBlockPassbook	–
LockScreenBlockTodayView	–
LockScreenFootnote	–
LockScreenTimeoutInSeconds	–
LogonBlockFastUserSwitching	–

Intune Policies M to P

Property	Comments
MaintenanceStartTime	–
MaintenanceWindowBlocked	–
MaintenanceWindowDurationInHours	–
MaintenanceWindowStartTime	–
ManagedEmailProfileRequired	–
MediaContentRatingApps	–
MediaContentRatingAustralia	–
MediaContentRatingCanada	–
MediaContentRatingFrance	–
MediaContentRatingGermany	–
MediaContentRatingIreland	–
MediaContentRatingJapan	–
MediaContentRatingNewZealand	–
MediaContentRatingUnitedKingdom	–
MediaContentRatingUnitedStates	–
MessagesBlocked	–
MicrosoftAccountBlocked	–
MicrosoftAccountBlockSettingsSync	–
MicrosoftUpdateServiceAllowed	–

MinAndroidSecurityPatchLevel	–
MiracastBlocked	–
MiracastChannel	–
MiracastRequirePin	–
MobileOsMaximumVersion	–
MobileOsMinimumVersion	–
NetworkProxyApplySettingsDeviceWide	–
NetworkProxyAutomaticConfigurationUrl	–
NetworkProxyDisableAutoDetect	–
NetworkProxyServer	–
NetworkUsageRules	–
NfcBlocked	–
NotificationSettings	–
NotificationsBlockSettingsModification	–
OneDriveDisableFileSync	–
OsMaximumVersion	–
OsMinimumVersion	–
PasscodeBlockFingerprintModification	–
PasscodeBlockFingerprintUnlock	–
PasscodeBlockModification	–

PasscodeBlockSimple	–
PasscodeExpirationDays	–
PasscodeMinimumCharacterSetCount	–
PasscodeMinimumLength	–
PasscodeMinutesOfInactivityBeforeLock	–
PasscodeMinutesOfInactivityBeforeScreenTimeout	–
PasscodePreviousPasscodeBlockCount	–
PasscodeRequired	–
PasscodeRequiredType	–
PasscodeSignInFailureCountBeforeWipe	–
PasswordBlockFingerprintUnlock	–
PasswordBlockPicturePasswordAndPin	–
PasswordBlockSimple	–
PasswordBlockTrustAgents	–
PasswordExpirationDays	–
PasswordMinimumCharacterSetCount	–
PasswordMinimumLength	–
PasswordMinutesOfInactivityBeforeLock	–
PasswordMinutesOfInactivityBeforeScreenTimeout	–
PasswordPreviousPasswordBlockCount	–

PasswordRequired	–
PasswordRequiredToUnlockFromIdle	–
PasswordRequiredType	–
PasswordRequireToUnlockFromIdle	–
PasswordRequireWhenResumeFromIdleState	–
PasswordSignInFailureCountBeforeFactoryReset	–
Payload	–
PayloadFileName	–
PayloadName	–
PersonalizationDesktopImageUrl	–
PersonalizationLockScreenImageUrl	–
PodcastsBlocked	–
PostponeRebootUntilAfterDeadline	–
PowerOffBlocked	–
PrereleaseFeatures	–
PrivacyAdvertisingId	–
PrivacyAutoAcceptPairingAndConsentPrompts	–
PrivacyBlockInputPersonalization	–
ProductKey	–

Intune Policies Q to S

Property	Comments
QualityUpdatesDeferralPeriodInDays	–
QualityUpdatesPaused	–
QualityUpdatesPauseExpiryDateTime	–
QualityUpdatesPauseStartDate	–
QualityUpdatesRollbackStartDateTime	–
QualityUpdatesWillBeRolledBack	–
RequireHealthyDeviceReport	–
ResetProtectionModeBlocked	–
SafariBlockAutofill	–
SafariBlocked	–
SafariBlockJavaScript	–
SafariBlockPopups	–
SafariCookieSettings	–
SafariManagedDomains	–
SafariPasswordAutoFillDomains	–
SafariRequireFraudWarning	–
SafeSearchFilter	–
ScheduleImminentRestartWarningInMinutes	–
ScheduleRestartWarningInHours	–

ScheduledActionsForRule	–
ScheduledInstallDays	–
ScreenCaptureBlocked	–
SearchBlockDiacritics	–
SearchDisableAutoLanguageDetection	–
SearchDisableIndexerBackoff	–
SearchDisableIndexingEncryptedItems	–
SearchDisableIndexingRemovableDrive	–
SearchEnableAutomaticIndexSizeManangement	–
SearchEnableRemoteQueries	–
SecureBootEnabled	–
SecurityBlockJailbrokenDevices	–
SecurityDisableUsbDebugging	–
SecurityPreventInstallAppsFromUnknownSources	–
SecurityRequireCompanyPortalAppIntegrity	–
SecurityRequireGooglePlayServices	–
SecurityRequireSafetyNetAttestationBasicIntegrity	–
SecurityRequireSafetyNetAttestationCertifiedDevice	–
SecurityRequireUpToDateSecurityProviders	–
SecurityRequireVerifyApps	–

SettingsBlockAccountsPage	–
SettingsBlockAddProvisioningPackage	–
SettingsBlockAppsPage	–
SettingsBlockChangeLanguage	–
SettingsBlockChangePowerSleep	–
SettingsBlockChangeRegion	–
SettingsBlockChangeSystemTime	–
SettingsBlockDevicesPage	–
SettingsBlockEaseOfAccessPage	–
SettingsBlockEditDeviceName	–
SettingsBlockGamingPage	–
SettingsBlockMyMeetingsAndFiles	–
SettingsBlockNetworkInternetPage	–
SettingsBlockPersonalizationPage	–
SettingsBlockPrivacyPage	–
SettingsBlockRemoveProvisioningPackage	–
SettingsBlockSessionResume	–
SettingsBlockSettingsApp	–
SettingsBlockSigninSuggestions	–
SettingsBlockSystemPage	–

SettingsBlockTimeLanguagePage	–
SettingsBlockUpdateSecurityPage	–
SettingsDefaultVolume	–
SettingsScreenTimeoutInMinutes	–
SettingsSessionTimeoutInMinutes	–
SettingsSleepTimeoutInMinutes	–
SharedUserAppDataAllowed	–
SkipChecksBeforeRestart	–
SiriBlocked	–
SiriBlockedWhenLocked	–
SiriBlockUserGeneratedContent	–
SiriRequireProfanityFilter	–
SmartScreenBlockOverrideForFiles	–
SmartScreenBlockPromptOverride	–
SmartScreenBlockPromptOverrideForFiles	–
SmartScreenEnableAppInstallControl	–
SmartScreenEnableInShell	–
SpotlightBlockInternetResults	–
StartBlockUnpinningAppsFromTaskbar	–
StartMenuAppListVisibility	–

StartMenuHideChangeAccountSettings	–
StartMenuHideFrequentlyUsedApps	–
StartMenuHideHibernate	–
StartMenuHideLock	–
StartMenuHidePowerButton	–
StartMenuHideRecentJumpLists	–
StartMenuHideRecentlyAddedApps	–
StartMenuHideRestartOptions	–
StartMenuHideShutDown	–
StartMenuHideSignOut	–
StartMenuHideSleep	–
StartMenuHideSwitchAccount	–
StartMenuHideUserTile	–
StartMenuLayoutEdgeAssetsXml	–
StartMenuLayoutXml	–
StartMenuMode	–
StartMenuPinnedFolderDocuments	–
StartMenuPinnedFolderDownloads	–
StartMenuPinnedFolderFileExplorer	–
StartMenuPinnedFolderHomeGroup	–

StartMenuPinnedFolderMusic	–
StartMenuPinnedFolderNetwork	–
StartMenuPinnedFolderPersonalFolder	–
StartMenuPinnedFolderPictures	–
StartMenuPinnedFolderSettings	–
StartMenuPinnedFolderVideos	–
StorageBlockGoogleBackup	–
StorageBlockRemovableStorage	–
StorageRequireDeviceEncryption	–
StorageRequireEncryption	–
StorageRequireMobileDeviceEncryption	–
StorageRequireRemovableStorageEncryption	–
StorageRestrictAppDataToSystemVolume	–
StorageRestrictAppInstallToSystemVolume	–
SystemIntegrityProtectionEnabled	–

Intune Policies T to W

Property	Comments
TargetEdition	Required property
TenantLockdownRequireNetworkDuringOutOfBoxExperience	—
UninstallBuiltInApps	—
UpdateNotificationLevel	Read-only property in Entra ID.
UpdateWeeks	—
UpdatesRequireAutomaticUpdates	—
UserAccountControlSettings	—
UserPauseAccess	—
UserStatusOverview	—
UserStatuses	—
UserWindowsUpdateScanAccess	—
UtcTimeOffsetInMinutes	—
Version	—
VoiceAssistantBlocked	—
VoiceDialingBlocked	—
VoiceRecordingBlocked	—
WebBrowserBlockAutofill	—
WebBrowserBlockJavaScript	—
WebBrowserBlockPopups	—

WebBrowserBlocked	–
WebBrowserCookieSettings	–
WebRtcBlockLocalhostIpAddress	–
WelcomeScreenBackgroundImageUrl	–
WelcomeScreenBlockAutomaticWakeUp	–
WelcomeScreenMeetingInformation	–
WiFiBlockAutomaticConnectHotspots	–
WiFiBlocked	–
WiFiBlockManualConfiguration	–
WiFiConnectOnlyToConfiguredNetworks	–
WiFiScanInterval	–
WifiBlockHotspotReporting	–
WindowsSpotlightBlockConsumerSpecificFeatures	–
WindowsSpotlightBlockOnActionCenter	–
WindowsSpotlightBlockTailoredExperiences	–
WindowsSpotlightBlockThirdPartyNotifications	–
WindowsSpotlightBlockWelcomeExperience	–
WindowsSpotlightBlockWindowsTips	–
WindowsSpotlightBlocked	–
WindowsSpotlightConfigureOnLockScreen	–

WindowsStoreBlockAutoUpdate	–
WindowsStoreBlocked	–
WindowsStoreEnablePrivateStoreOnly	–
WirelessDisplayBlockProjectionToThisDevice	–
WirelessDisplayBlockUserInputFromReceiver	–
WirelessDisplayRequirePinForPairing	–
WorkFoldersUrl	–
WorkProfileBlockAddingAccounts	–
WorkProfileBlockCamera	–
WorkProfileBlockCrossProfileCallerId	–
WorkProfileBlockCrossProfileContactsSearch	–
WorkProfileBlockCrossProfileCopyPaste	–
WorkProfileBlockNotificationsWhileDeviceLocked	–
WorkProfileBlockScreenCapture	–
WorkProfileBluetoothEnableContactSharing	–
WorkProfileDataSharingType	–
WorkProfileDefaultAppPermissionPolicy	–
WorkProfilePasswordBlockFingerprintUnlock	–
WorkProfilePasswordBlockTrustAgents	–
WorkProfilePasswordExpirationDays	–

WorkProfilePasswordMinLetterCharacters	–
WorkProfilePasswordMinLowerCaseCharacters	–
WorkProfilePasswordMinNonLetterCharacters	–
WorkProfilePasswordMinNumericCharacters	–
WorkProfilePasswordMinSymbolCharacters	–
WorkProfilePasswordMinUpperCaseCharacters	–
WorkProfilePasswordMinimumLength	–
WorkProfilePasswordMinutesOfInactivityBeforeScreenTimeout	–
WorkProfilePasswordPreviousPasswordBlockCount	–
WorkProfilePasswordRequiredType	–
WorkProfilePasswordSignInFailureCountBeforeFactoryReset	–
WorkProfileRequirePassword	–

Deployment

The Veeam Backup & Replication solution allows you to add Microsoft Entra ID tenants to the backup infrastructure, and to manage data protection and recovery operations for Microsoft Entra ID tenants from a single console.

To access the Veeam Backup for Microsoft Entra ID functionality, you can either deploy a new backup server as described in the Veeam Backup & Replication User Guide or use a backup server that already exists in your backup infrastructure if it meets the Veeam Backup for Microsoft Entra ID system requirements.

Licensing

Veeam Backup for Microsoft Entra ID is licensed by the number of protected Microsoft Entra ID users. Each 10 protected users consume one Veeam Universal License instance from the license scope. All Enabled Member users in the organization must be licensed, partial user coverage is not allowed by Microsoft Entra ID.

For the license consumption, Veeam Backup for Microsoft Entra ID counts only enabled member users. The tenant to whom these users belong must have a restore point created during the past 31 days. Note that disabled users, guest users and logs do not consume license instances, but Veeam Backup for Microsoft Entra ID still protects them.

By default, Veeam Backup for Microsoft Entra ID automatically revokes a license instance from protected users if no new restore points have been created during the past 31 days. However, you can manually revoke license instances from protected users as described in the Veeam Backup & Replication User Guide, section Revoking License.

> **NOTE**
>
> The type of the user account is specified by the value of the *userType* attribute (*Member* or *Guest*). Microsoft Entra ID users who were created before the introduction of the *userType* attribute on August 31, 2014, have *null* value for this attribute instead. Veeam Backup & Replication licenses and processes these user accounts the same way it licenses and processes Entra ID member users.

Obtaining New License

Tenant Backup

Backing up of Microsoft Entra ID tenants is available for all types of licenses:

- **No license (Community Edition, free)** is when you do not have the license key. With the Community Edition, you get 10 instances that allow protection of 100 enabled member users.

  For more information, see Veeam Backup & Replication Community Edition.

- **Evaluation license (free)** is a license that can be used for product evaluation. The license is valid for 30 days from the moment of the product download.

  To obtain this license, request a trial key on the Veeam downloads page as described in in the Veeam Backup & Replication User Guide, section Obtaining and Renewing License.

- **NFR license (free)** is a license used for product demonstration, training and education. The person to whom the license is provided agrees that the license is not for resell or commercial use.

- **Subscription license (paid)** is a license with a limited subscription term. The expiration date of the Subscription license is set to the end of the subscription term. The Subscription license term is normally 1-3 years from the license issue date.

  To obtain this license, choose the required subscription term on the Veeam Backup & Replication Pricing page and contact the Veeam Sales Team.

- **Perpetual license (paid)** is a license without an expiration date. The Perpetual license typically includes one year period of basic support and maintenance that can be extended.

  To obtain this license, contact a reseller in your region.

- **Rental license (paid)** is a license with the license expiration date set according to the chosen rental program (normally 1-12 months from the date of license issue). The Rental license can be automatically updated upon expiration.

  Rental licenses are provided to Veeam Cloud & Service Providers (VCSPs) only. For more information, see the Rental License section in the Veeam Cloud Connect Guide.

> **NOTE**
>
> Protection of Conditional Access policies is included in the Veeam Data Platform Advanced or Premium. For more details about all Veeam Data Platform packages, see Veeam Data Platform Feature Comparison.

After you obtain a license, install it on the backup server as described in the Veeam Backup & Replication User Guide, section Installing License.

Log Backup

The feature is included in the Veeam Data Platform Advanced or Premium. For more details about all Veeam Data Platform packages, see Veeam Data Platform Feature Comparison.

Using Existing License

If you already use Veeam Backup & Replication and you have spare Veeam Universal License instances on your backup server, they can be used to protect Microsoft Entra ID tenants. You can check the number of available license instances in the Veeam Backup & Replication console as described in the Viewing License Information section in the Veeam Backup & Replication User Guide.

If you have a legacy perpetual per-socket license, you must obtain Veeam Universal License instances and merge them with the existing perpetual socket license as described in the Veeam Backup & Replication User Guide, section Merging Licenses section.

Configuring

To start working with Veeam Backup for Microsoft Entra ID, perform the following steps for its configuration:

1. Configure a cache repository.
2. Add to the backup infrastructure the Microsoft Entra ID tenant that you want to protect.
3. [Optional] Configure remote Microsoft Entra ID backup repository where Veeam Backup for Microsoft Entra ID will store backups of Microsoft Entra ID tenants.
4. [Optional] Configure the primary log backup repository where Veeam Backup for Microsoft Entra ID will store backups of audit logs and sign-in logs.
5. [Optional] Configure the secondary log backup repositories where Veeam Backup for Microsoft Entra ID will store backups of audit logs and sign-in logs.
6. [Optional] Configure global email notification options to get notifications with results on jobs performed on the backup server. For more information, see the Veeam Backup & Replication User Guide, section Configuring Global Email Notification Settings.

Configuring Log and Cache Repositories

To protect Microsoft Entra ID tenant data and logs, you require the following repositories:

- Cache repository that stores temporary cache files for log processing.
- Primary log backup repository.
- [Optional] Secondary backup repository that stores copies of backups.

By default, the backup server can perform the roles of cache and primary log backup repositories.

You can also configure other types of repositories to keep data in another location. The following types of repositories are supported for all repositories (the cache, primary and secondary repositories):

- **Direct attached storage**: Microsoft Windows or Linux virtual or physical machines. For the cache repository only 64-bit versions are supported.
- **Network attached storage**: SMB (CIFS) shares or NFS shares.

The following types of repositories are supported only for the primary and secondary log backup repositories:

- **Direct attached storage**: Hardened repositories
- Deduplicating storage appliances: ExaGrid, Quantum DXi, Dell Data Domain or other
- Backup repositories with rotated drives
- Object storage repositories: Amazon S3, S3 compatible, Google Cloud or other
- Scale-out backup repositories (SOBR)

> **NOTE**
>
> Veeam Backup for Microsoft Entra ID does not support using Veeam Cloud Connect repositories or multi-bucket repositories to store log backups. For more information, see the Veeam Cloud Connect Guide, section Cloud Repository and Veeam Backup & Replication User Guide, section Object Storage Repositories.

Managing Microsoft Entra ID Tenants

To be able to perform data protection and disaster recovery tasks for Microsoft Entra ID resources, you must first add to Veeam Backup for Microsoft Entra ID a tenant that manages access to these resources and choose an application that will be used to interact with this tenant.

Adding Microsoft Entra ID Tenants

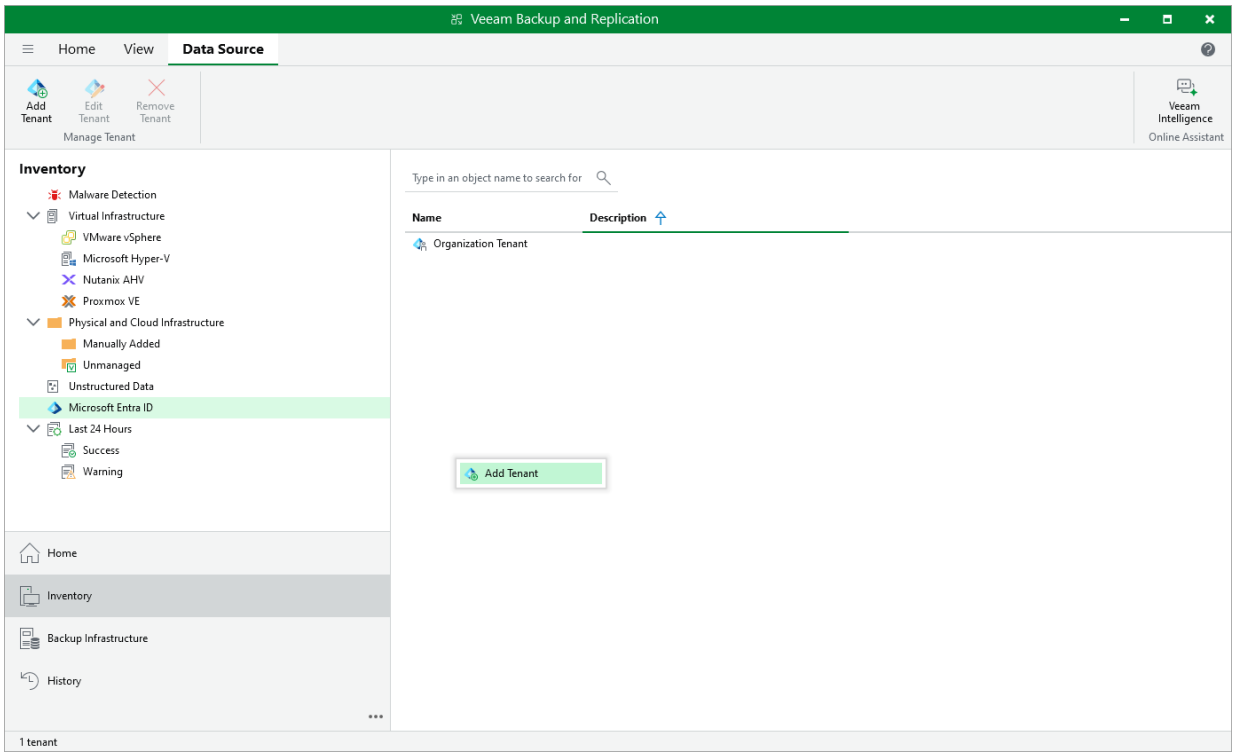
To add a Microsoft Entra ID tenant, do the following:

Step 1. Launch Microsoft Entra ID Tenant Wizard

To launch the **Microsoft Entra ID Tenant** wizard, do the following:

1. Open the **Inventory** view.
2. In the inventory pane, click the **Microsoft Entra ID** node.
3. Right-click the **Microsoft Entra ID** node and select **Add Microsoft Entra ID tenant**.

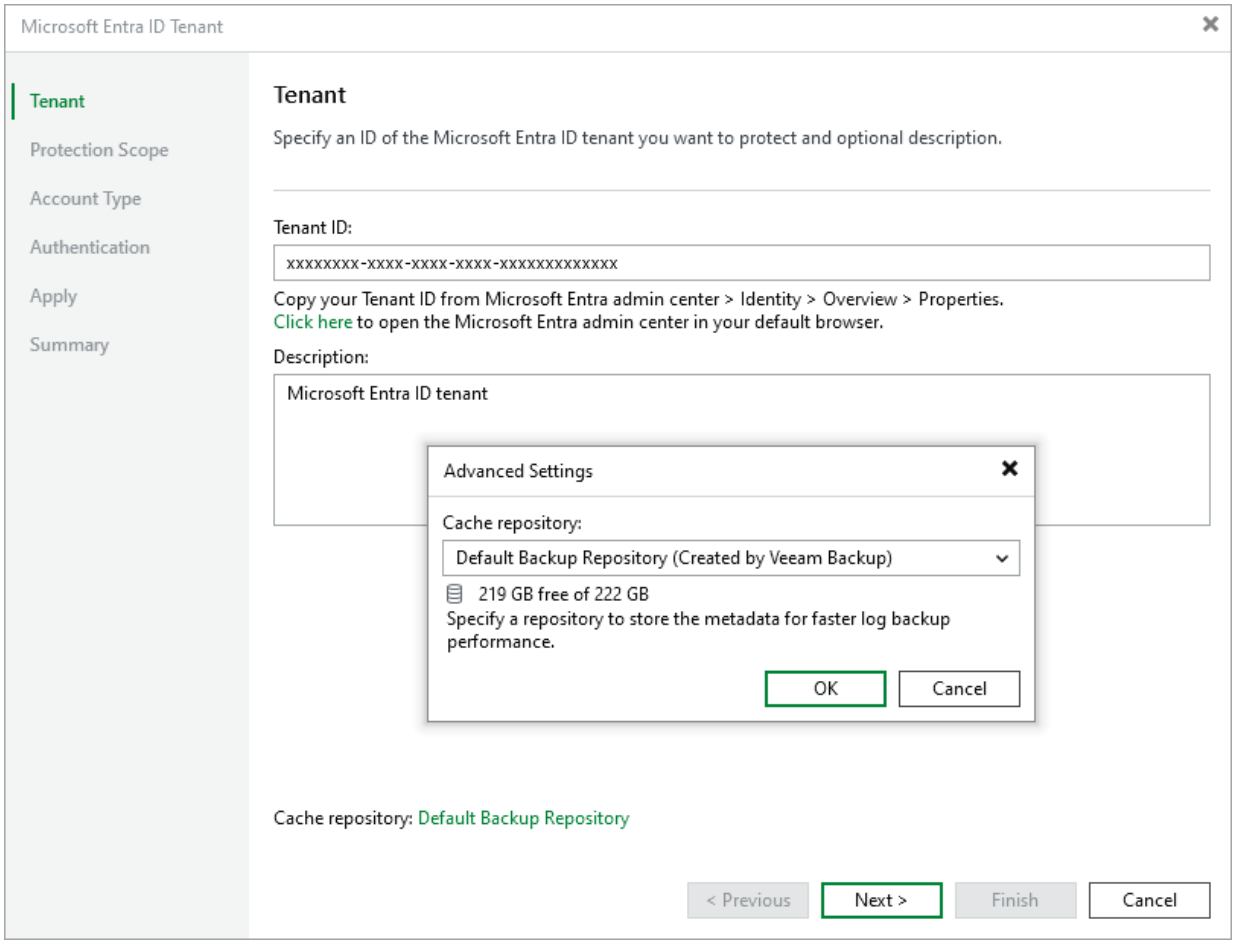
   Alternatively, click **Add Tenant** on the ribbon.



Step 2. Specify Tenant ID and Cache Repository

At the **Tenant** step of the wizard, specify the GUID of a Microsoft Entra ID tenant whose resources you plan to back up and provide a description for future reference.

You can also choose a repository where Veeam Backup & Replication will store temporary cache files while performing data protection and disaster recovery operations. By default, these files are stored on the PostgreSQL instance running the configuration database; however, you can specify another repository to distribute backup traffic — to do that, click **Cache** and select the necessary repository in the **Advanced Settings** window. For a repository to be displayed in the **Cache repository** list, it must be added to the backup infrastructure as described in in the Veeam Backup & Replication User Guide, section Backup Repositories.



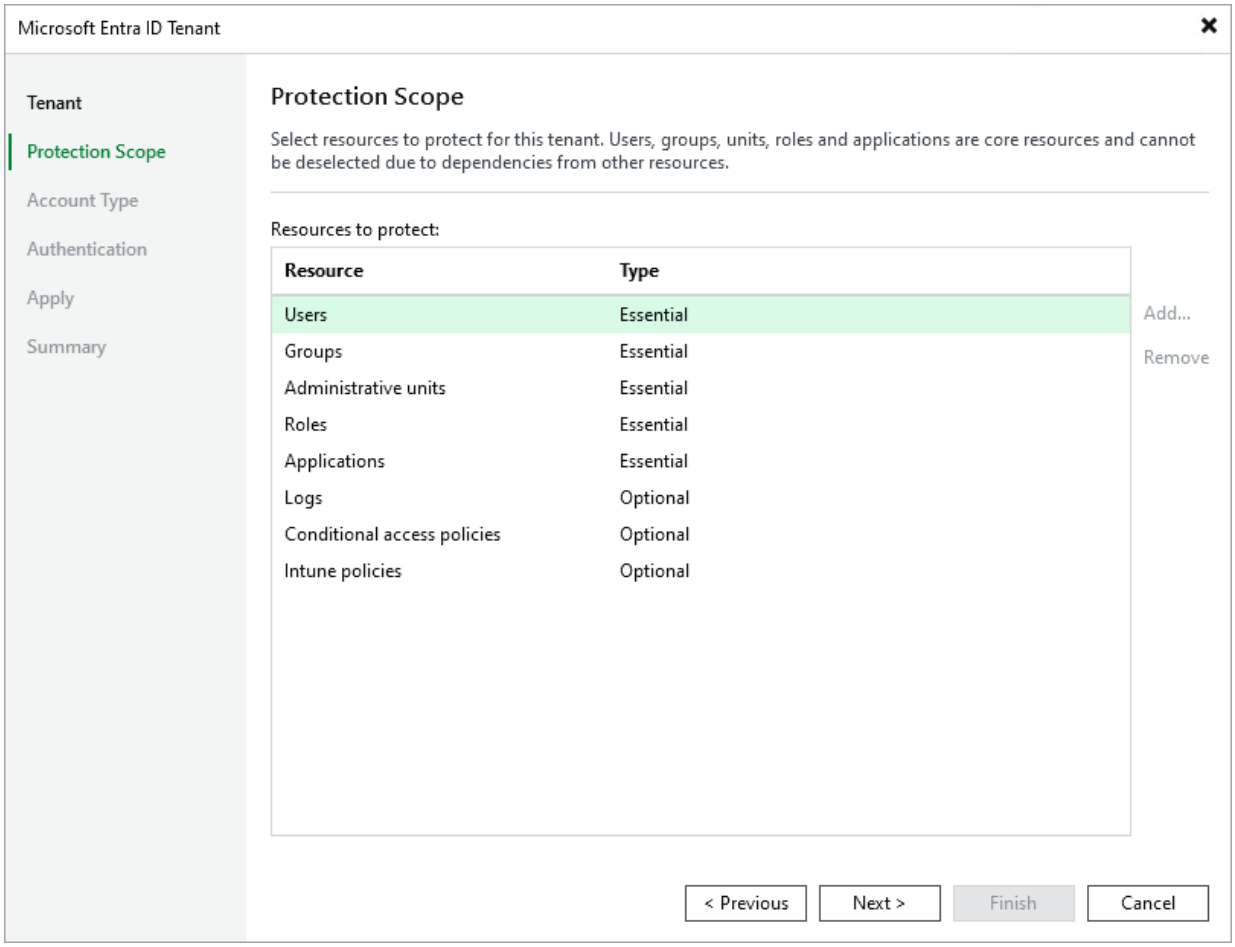
Step 3. Specify Protection Scope

When you add a new tenant to Veeam Backup for Microsoft Entra ID, you can specify the scope of resources that the product will be able to protect for this tenant. By default, the protection scope contains users, groups, administrative units, roles, applications, logs, conditional access policies and intune policies.

At the **Protection Scope** step of the wizard, you can exclude resources from the protection scope — to do that, select the necessary resources and click **Remove**.

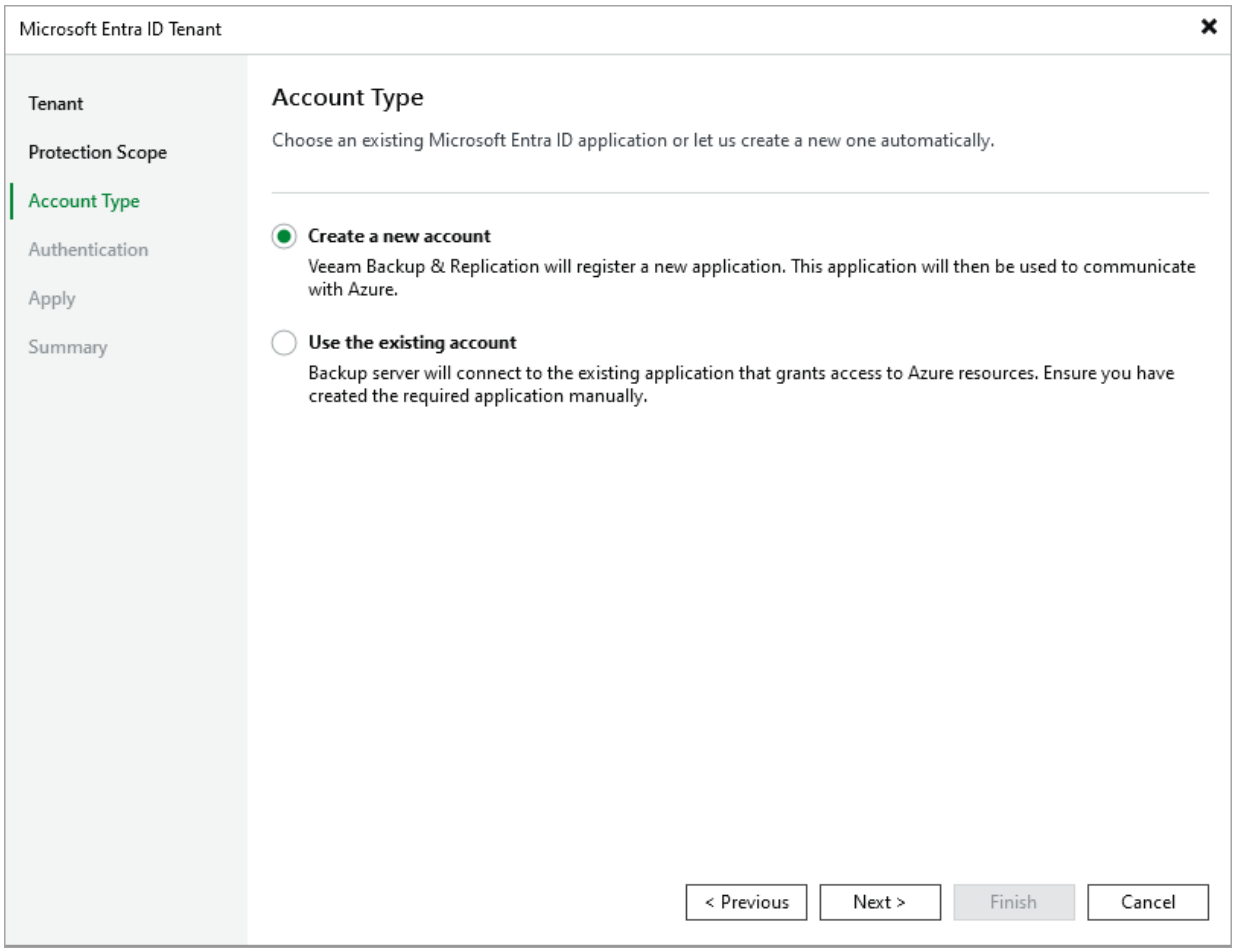
NOTES

- Resources that are marked as *Essential* cannot be excluded from the protection scope.
- You will be able to update the protection scope later, using the Edit Tenant wizard.



Step 4. Choose Connection Method

At the **Account Type** step of the wizard, choose if you want to connect to Microsoft Azure using an existing or a newly created Microsoft Entra ID application. In the latter case, Veeam Backup & Replication will create a new Microsoft Entra ID application automatically.



Creating New Application

This step applies only if you have selected the **Create a new account** option at the Account Type step of the wizard.

If you choose to create a new account, Veeam Backup & Replication registers a new Microsoft Entra ID application for the specified Microsoft Entra ID tenant. Veeam Backup & Replication will use this application to authenticate to Microsoft Azure and will grant this application all the permissions necessary to process the selected protection scope. For more information on Microsoft Entra ID applications, see Microsoft Docs. To create the Microsoft Entra ID application, you must use a single-use verification code that Veeam Backup & Replication provides you.

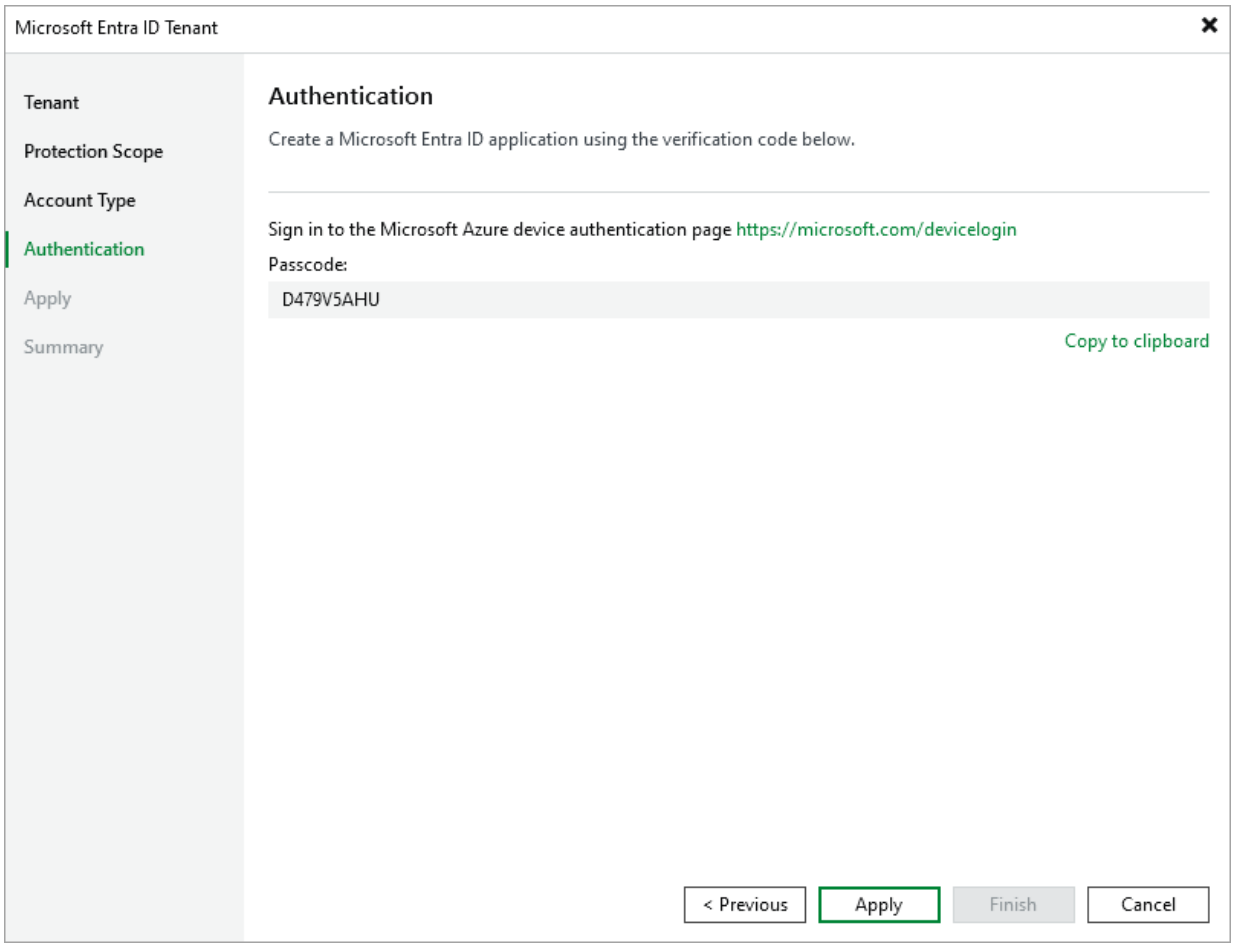
At the **Authentication** step of the wizard, do the following:

1. Click **Copy to clipboard** to copy the verification code.
2. Click the https://microsoft.com/devicelogin link.
3. On the Microsoft Azure device authentication page, do the following:
    a. Paste the code that you have copied and click **Next**. Note that the code will expire in 15 minutes.

b. Specify a Microsoft Azure account that will be used to create an application. Note that the user name must be specified in the user principal name format (username@domain). The account must have permissions described in section Permissions.

4. Go back to the **Entra ID Tenant** wizard.

5. Click **Apply** and check whether any errors occurred during the authentication process.



Specifying Existing Application

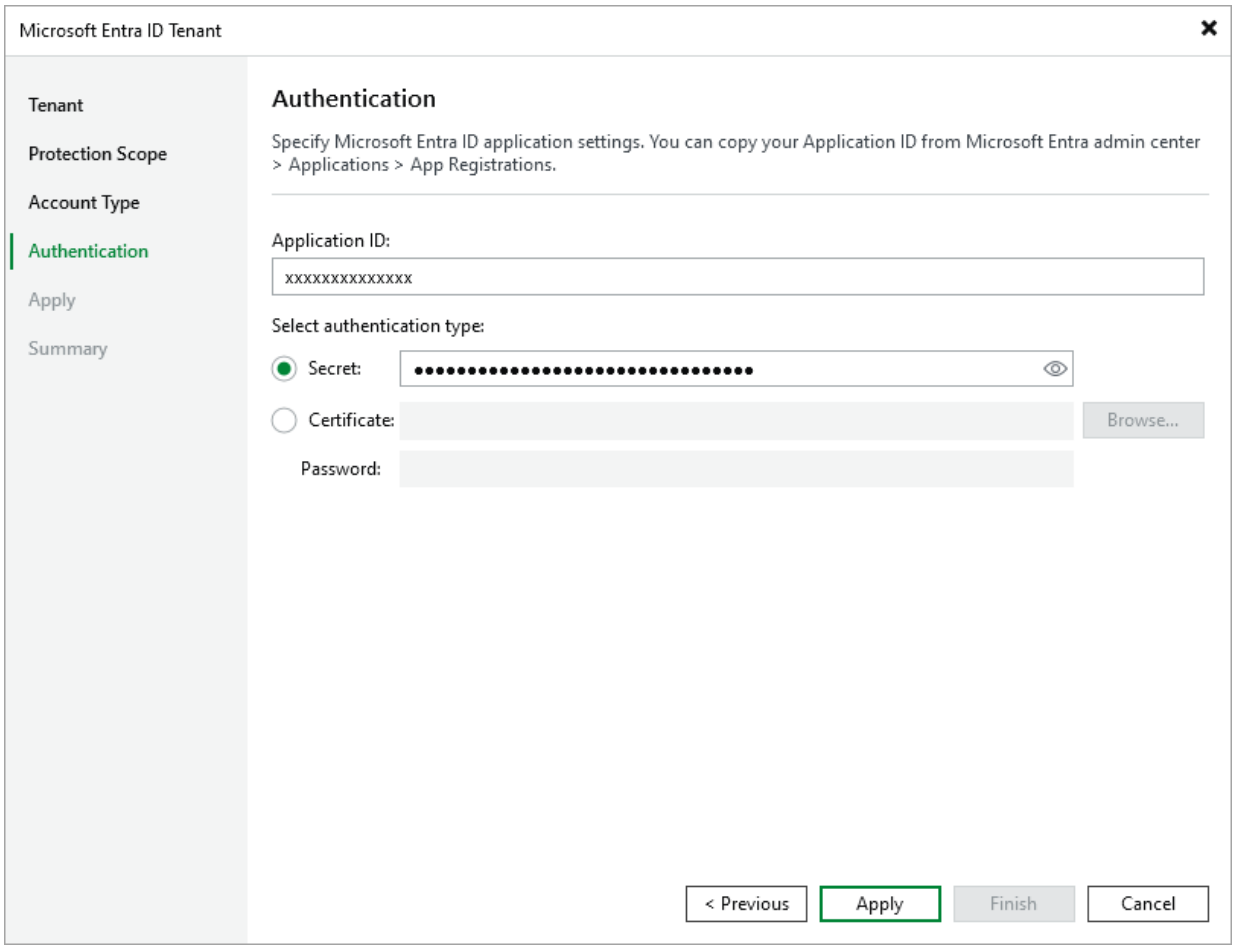
This step applies only if you have selected the **Use the existing account** option at the Account Type step of the wizard.

To use an existing Microsoft Entra ID application:

1. In the **Application ID** field, specify the ID of the necessary application. The Microsoft Entra ID application must have permissions listed in Permissions.

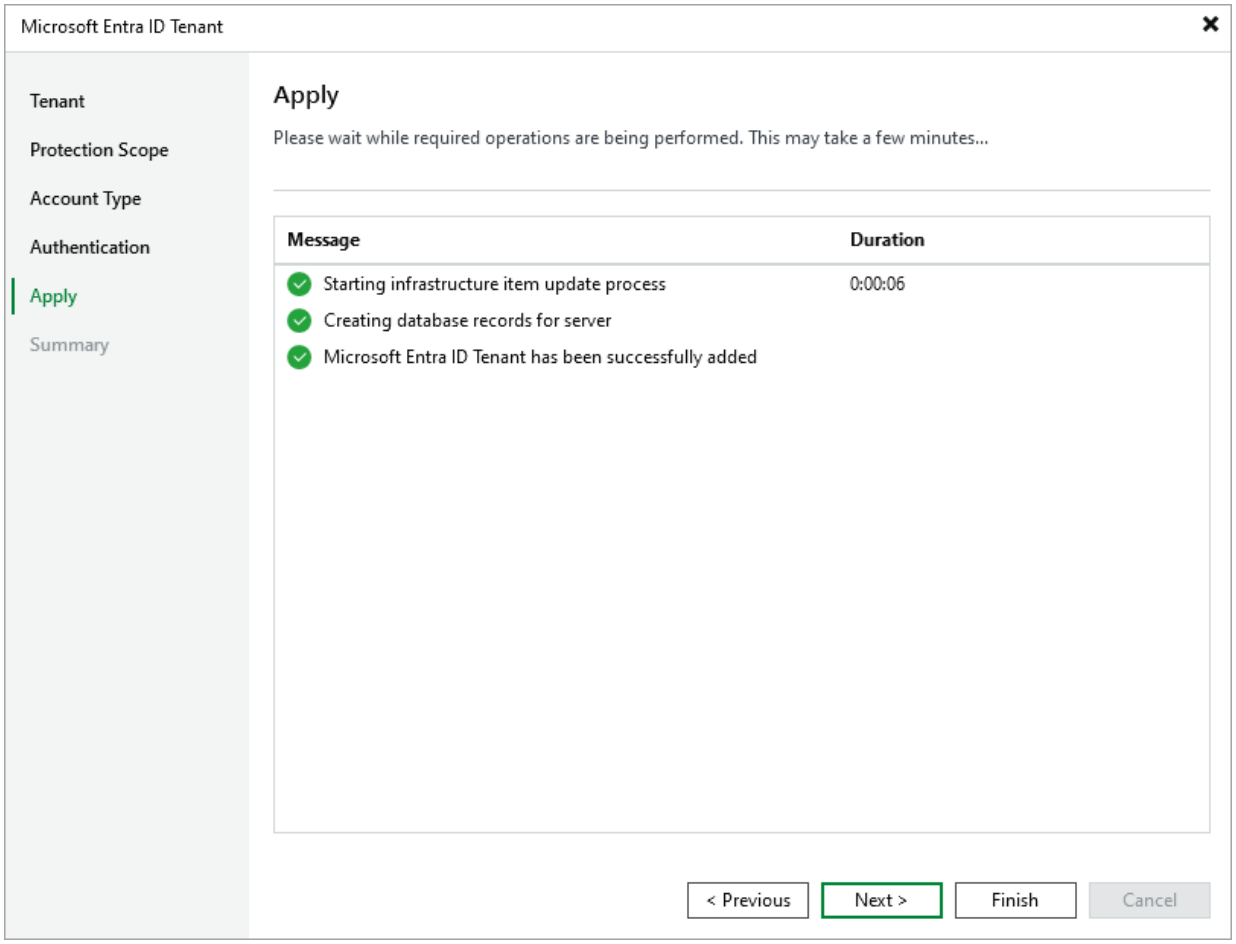
2. In the **Select authentication type** area, choose if you want to use password-based authentication (application secret) or certificate-based authentication. Then provide the necessary information.

For more information on how to get tenant and application IDs, a secret and a certificate, see Microsoft Docs.



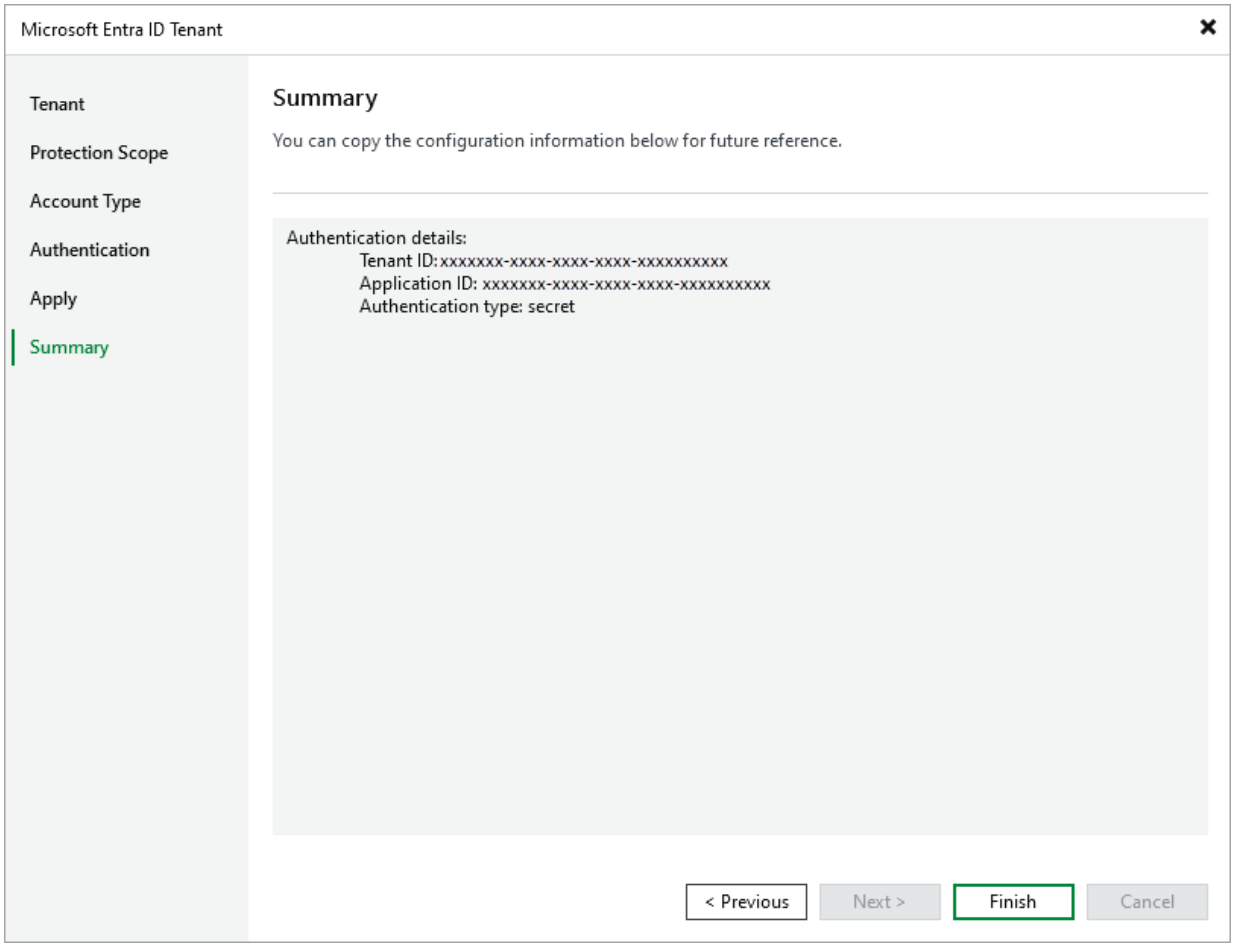
Step 5. Track Progress

At the **Apply** step of the wizard, wait until the Microsoft Entra ID tenant is added to the backup infrastructure and then click **Next**.



Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review details of configured settings and click **Finish** to close the wizard.

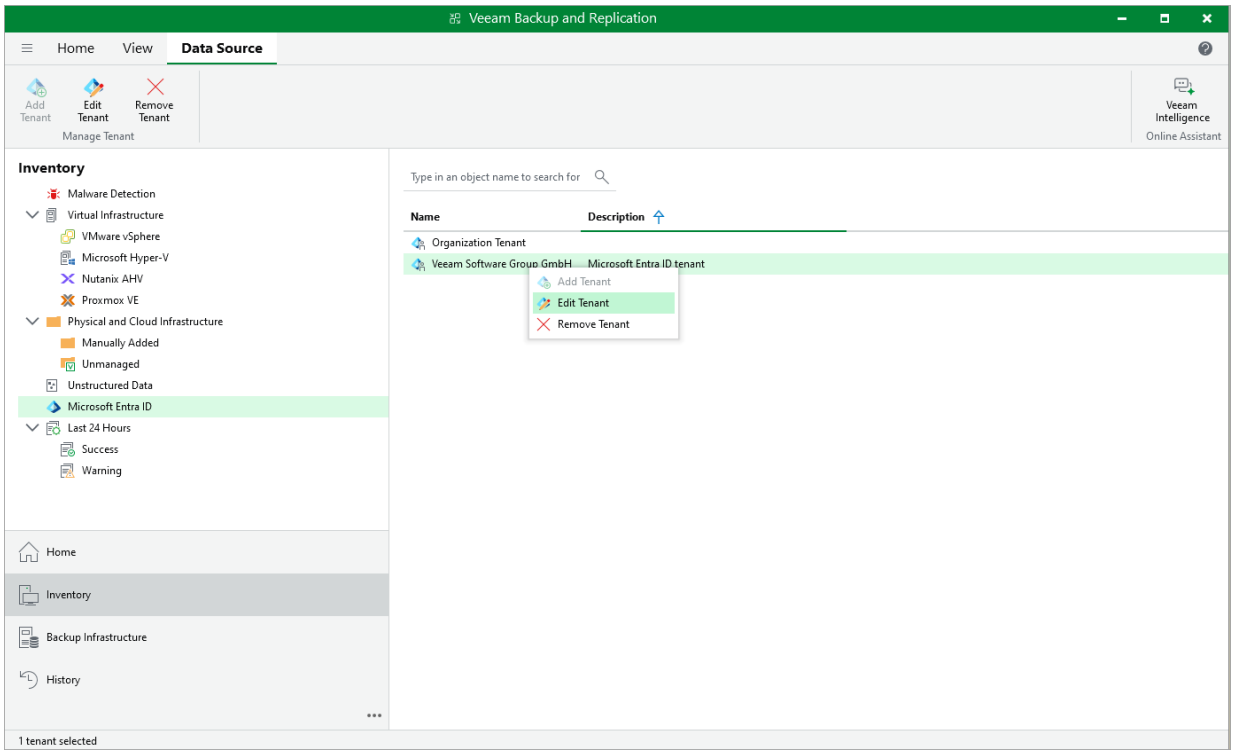


Editing Microsoft Entra ID Tenants

You can edit properties of the Microsoft Entra ID tenant added to the backup infrastructure. These properties include the tenant description in Veeam Backup & Replication, cache repository, application used to perform operations and authentication method used to access the application.

To edit tenant properties:

1. Open the **Inventory** view.
2. In the inventory pane, click **Microsoft Entra ID**.
3. Select the tenant that you want to edit.
4. Right-click the tenant and select **Edit**. Alternatively, click **Edit Tenant** on the ribbon.



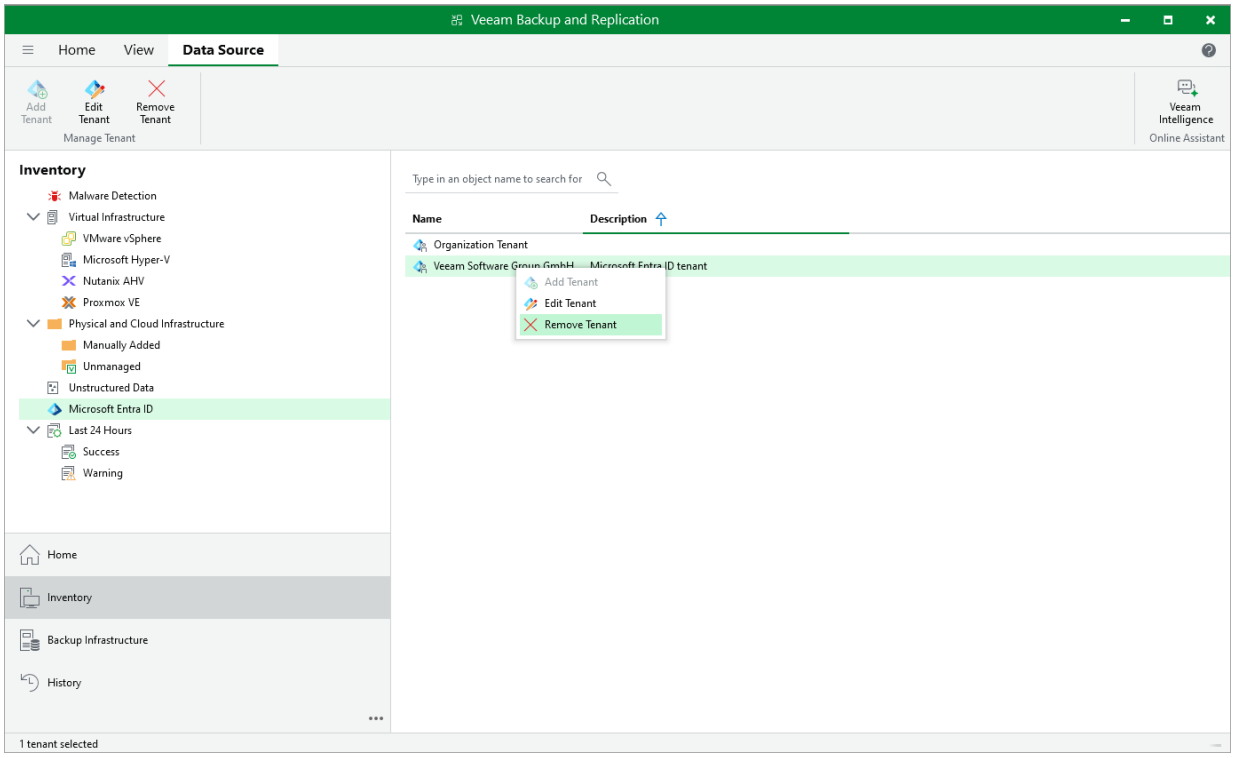
Removing Microsoft Entra ID Tenants

If you do not want to protect the added Microsoft Entra ID tenant anymore, you can remove it from the backup infrastructure. Note that the tenant will be removed only from the backup infrastructure, not Entra ID.

> **NOTE**
>
> You cannot remove a Microsoft Entra ID tenant protected by any job. To remove such a tenant, you first need to delete the backup jobs associated with this tenant.

To remove a tenant:

1. Open the **Inventory** view.
2. In the inventory pane, click **Microsoft Entra ID**.
3. Select the tenant that you want to delete.
4. Right-click the tenant and select **Remove**. Alternatively, click **Remove Tenant** on the ribbon.



Connecting to a Remote Microsoft Entra ID Repository

A Microsoft Entra ID backup repository is a PostgreSQL instance where Veeam Backup for Microsoft Entra ID stores backups of protected Microsoft Entra ID tenants. By default, Veeam Backup & Replication saves all backed-up data to the local PostgreSQL instance installed on the backup server. To change this behavior, you can connect to a remote PostgreSQL instance and use it as the target backup repository in your Windows or Linux deployment of Veeam Backup & Replication. Consider that Veeam Backup for Microsoft Entra ID supports only PostgreSQL password authentication to connect to remote Microsoft Entra ID backup repositories.

> **IMPORTANT**
>
> Due to technical limitations, Veeam Backup for Microsoft Entra ID supports connection only to one repository at a time, which means that as soon as you connect to a new repository, the connection to the previous one will be lost, and VBR will not be able to use the backups stored in the previous repository. Consider copying your existing backups from the previous PostgreSQL instance to a new one.

Connecting to Remote Microsoft Entra ID Backup Repository

To use for the Microsoft Entra ID backup repository a remote PostgreSQL instance instead of the local one, use the Veeam Configuration Database Connection Utility.

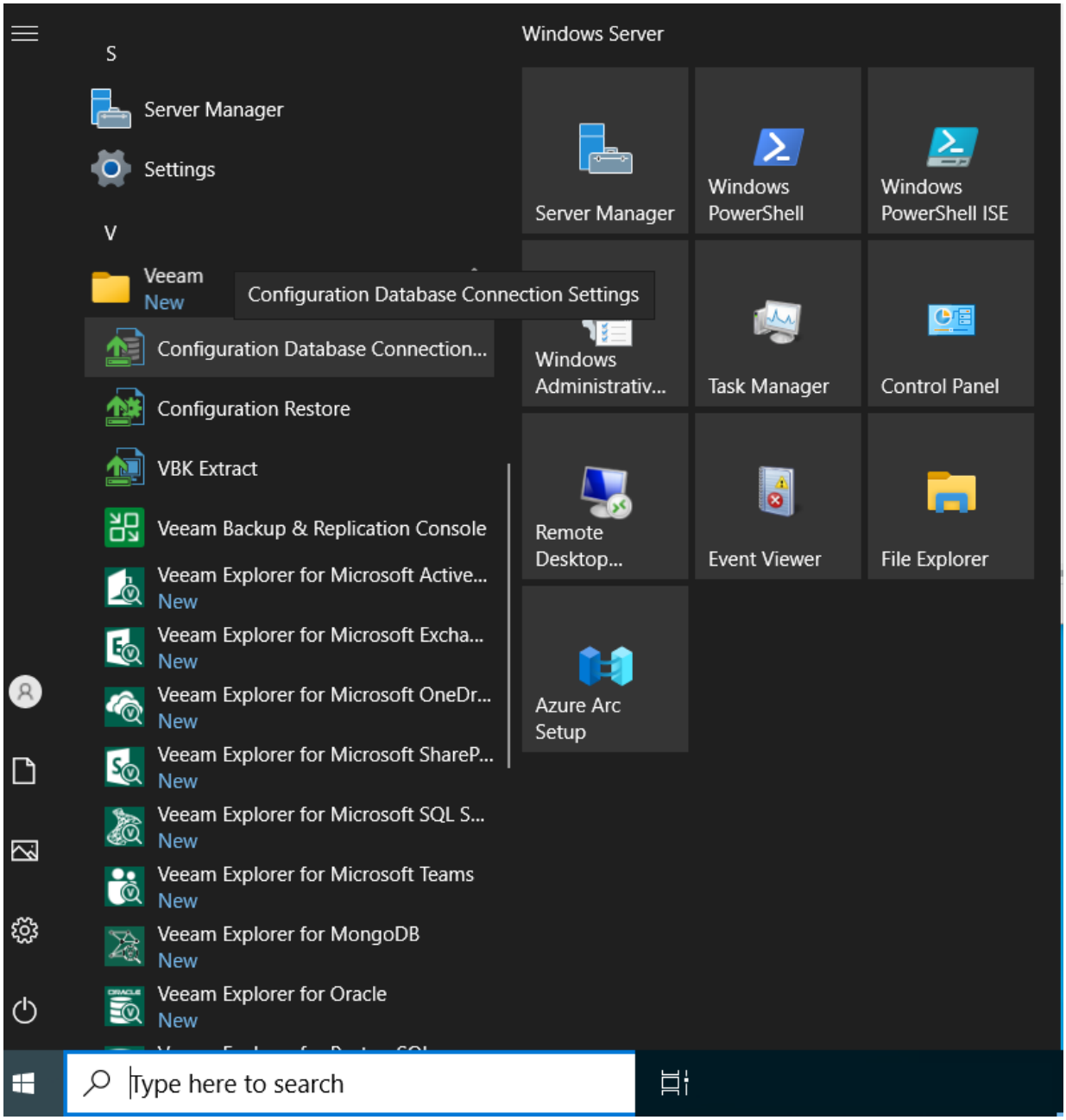
1. Launch the Veeam Configuration Database Connection Utility
2. Select a product
3. Configure the connection
4. Finish working with the wizard

Step 1. Launch Utility

You can launch the configuration database connection utility using one of the following ways:

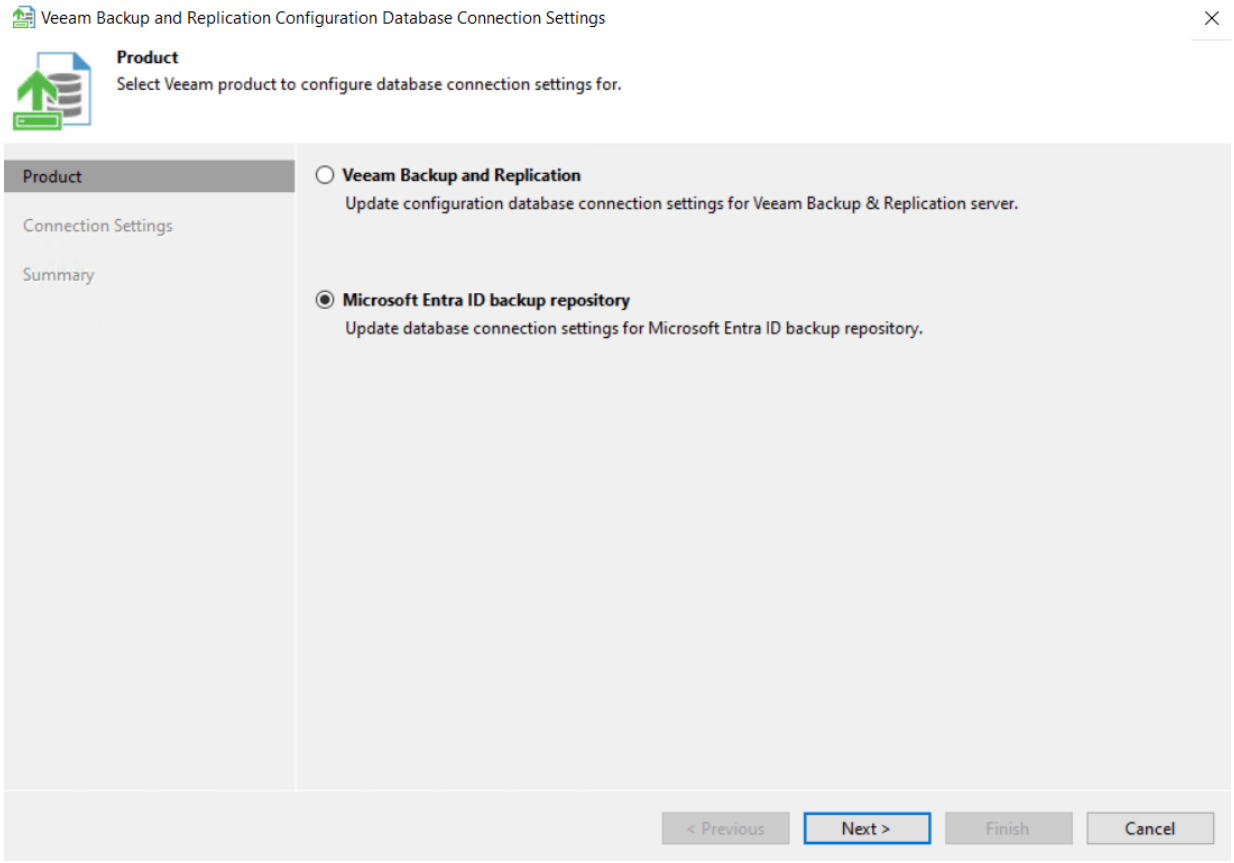
- From the **Start** menu, click **Configuration Database Connection Settings**.
- Use the `Veeam.Backup.DBConfig.exe` file located in the installation folder. The default path to the folder is the following: `%PROGRAMFILES%\Common Files\Veeam\Backup and Replication\DBConfig`.
- Use the `Veeam.Backup.DBConfig.exe` file located in the ISO file. The path to the file is the following: `%ISO%:\Tools\DBConfig`.

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



Step 2. Select Product

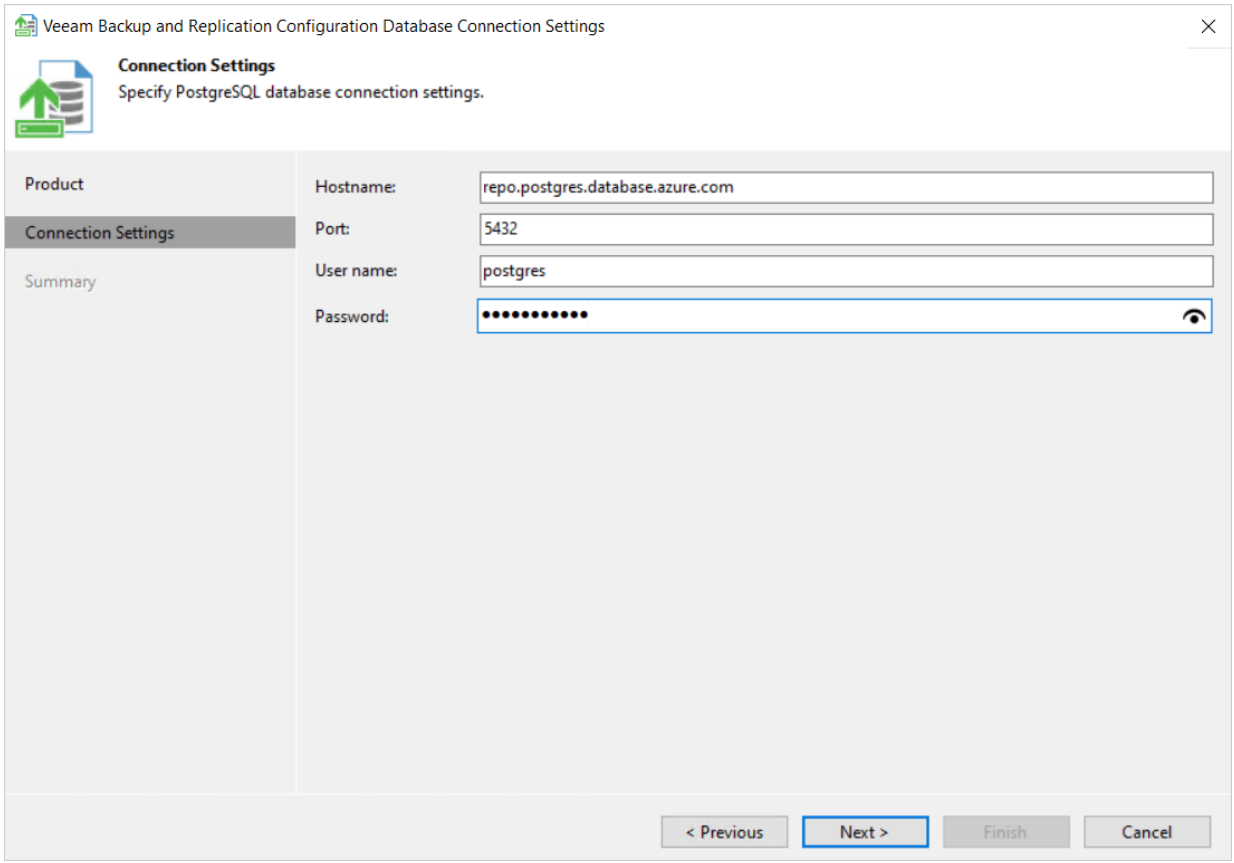
At the **Product** step of the wizard, select **Microsoft Entra ID backup repository**.



Step 3. Configure Connection

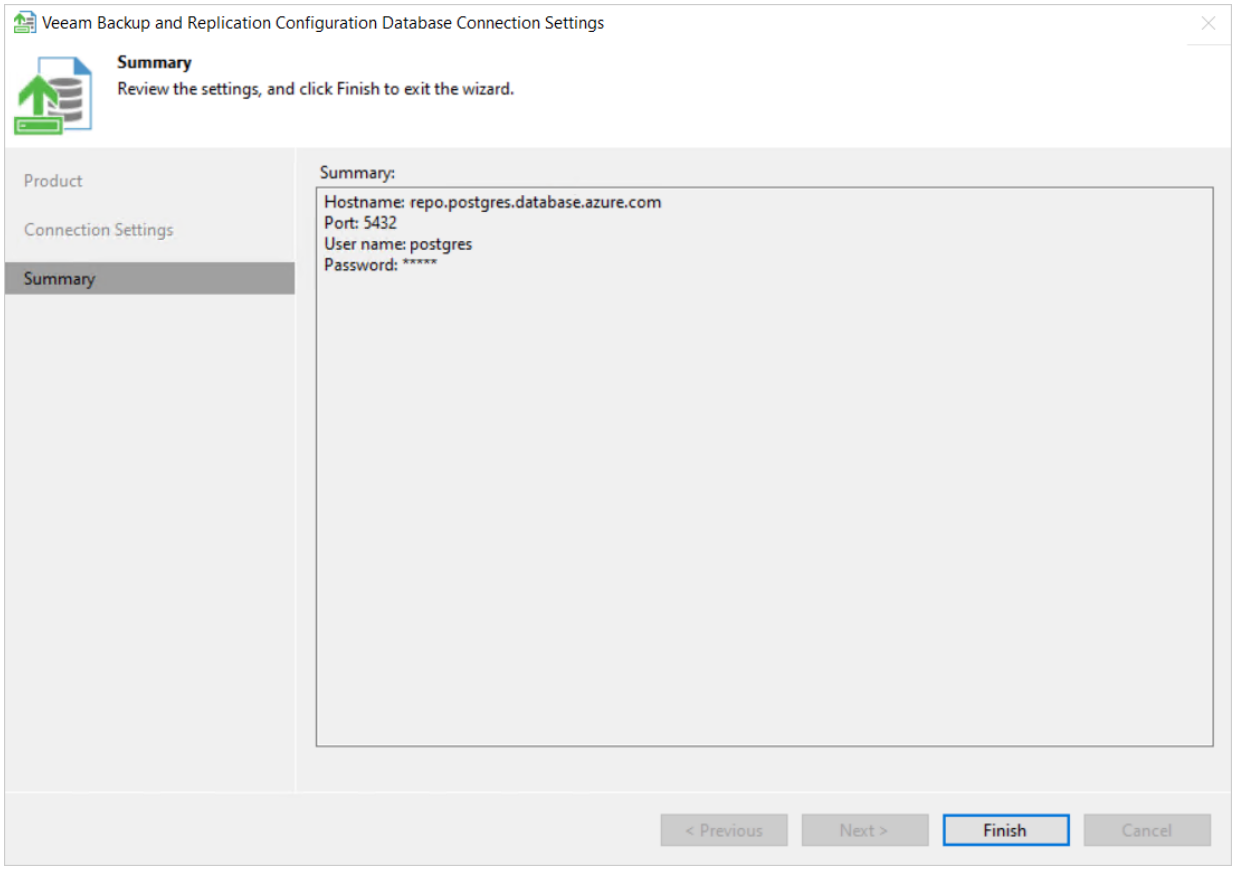
At the **Connection Settings** step of the wizard, provide the connection settings for the PostgreSQL database server that will be used as a remote Microsoft Entra ID backup repository. Specify the host where the database instance is located, the port that will be used to connect to the database instance, and the credentials of the database account.

> **IMPORTANT**
>
> You can connect to a PostgreSQL database using PostgreSQL password authentication only.



Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review the configured settings.



Connecting to Microsoft Entra ID Repositories (Linux Deployments)

In case if your version of Veeam Backup & Replication does not have a pre-packed configuration database connection utility that allows you to connect to Entra ID repositories automatically, you need to establish the connection manually — to do that, obtain root access and run the following command on the backup server:

```
VEEAM_SETUP_ENTRA_ID_PGSQL_PASSWORD=<password> dotnet /opt/veeam/vbr/Veeam.Backup.Setup.Linux.dll entraiddbconfigurator /EntraIdSqlServerName:<servername> /EntraIdSqlServerPort:<portnumber> /EntraIdSqlServerLogin:<serverlogin>
```

Make sure to run the command as a single line and specify the password, DNS name or IP address, port and login required to connect to the necessary instance.

Every time a new backup job starts, Veeam Backup & Replication will check whether a dedicated database for the protected tenant already exists on the remote PostgreSQL instance; if there is no such database, Veeam Backup & Replication creates it. If Veeam Backup & Replication encounters any connectivity issues when running the job, you will be prompted to run a repository rescan.

Rescanning Microsoft Entra ID Repository

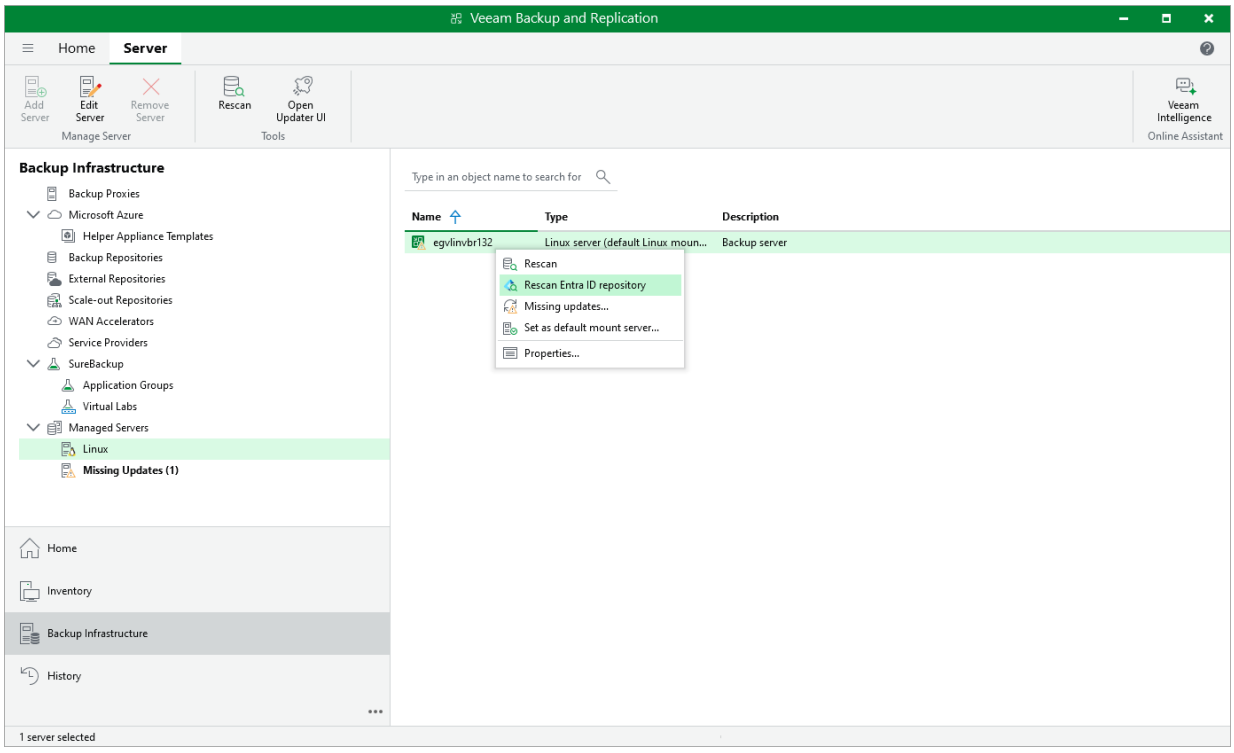
Backup repository rescan can be required in the following cases:

- You have moved information from one PostgreSQL instance on which the repository is based to another instance.
- You have restored the Veeam Backup & Replication configuration database.
- After a job failed and it requested backup repository rescan.
- Other cases.

> **NOTE**
>
> We recommend you to stop or disable all jobs before performing the rescan.Veeam Backup & Replication skips from scanning backups created by active jobs.

To rescan the Microsoft Entra ID backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Managed Servers** > **Microsoft Windows** or **Linux** node.
3. In the working area, select the backup server.
4. Press and hold the [Ctrl] key, right-click the backup server and select **Rescan Entra ID repository**.



Performing Backup

To produce backups, Veeam Backup for Microsoft Entra ID runs backup jobs. A backup job is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

Veeam Backup for Microsoft Entra ID supports two types of backup jobs:

- Tenant backup jobs that protect tenant data, such as users, groups, administrative units, roles, applications and conditional access policies.
- Log jobs that protect tenant audit and sign-in logs.

One backup job can protect data or logs of only one tenant. You can instruct Veeam Backup for Microsoft Entra ID to run jobs automatically according to a specified schedule or start them manually.

Creating Tenant Backup Jobs

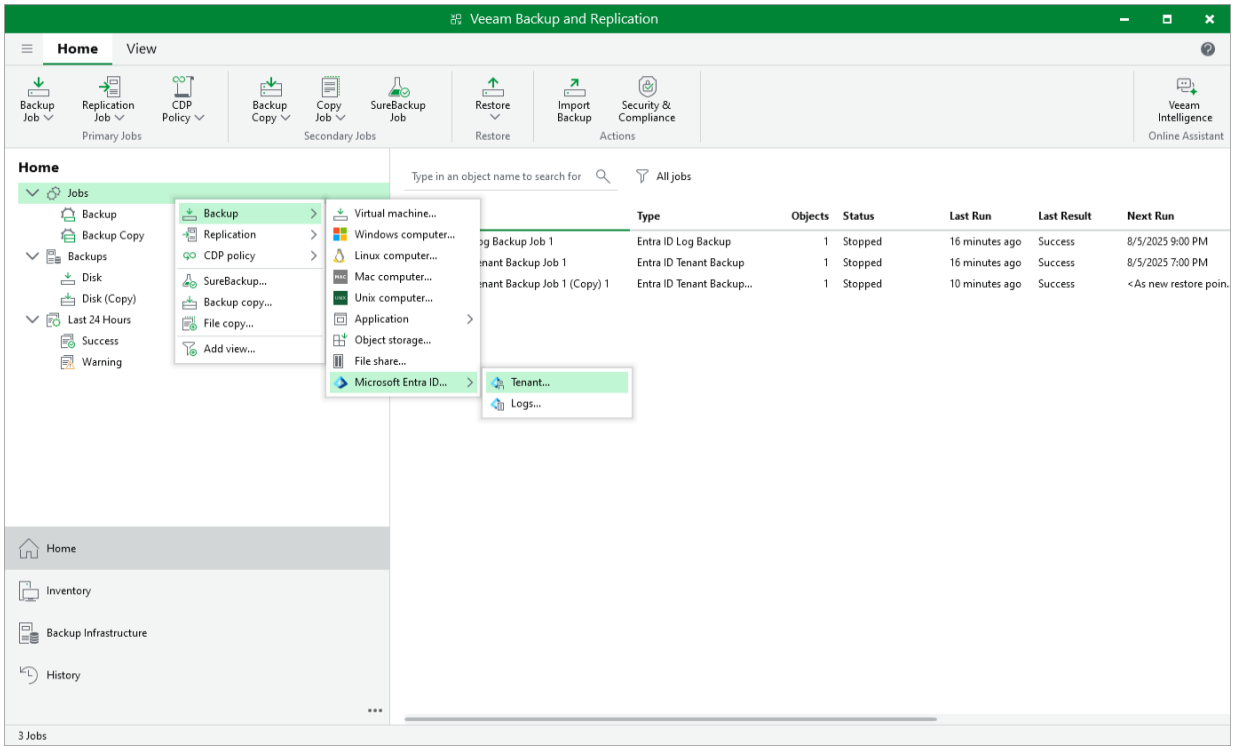
To create a Microsoft Entra ID tenant backup job, do the following:

1. Launch the New Microsoft Entra ID Tenant Backup Job wizard.
2. Specify a job name and description.
3. Specify a tenant and retention settings.
4. Specify backup copy settings.
5. Define a job schedule.
6. Finish working with the wizard.

Step 1. Launch New Microsoft Entra ID Tenant Backup Job Wizard

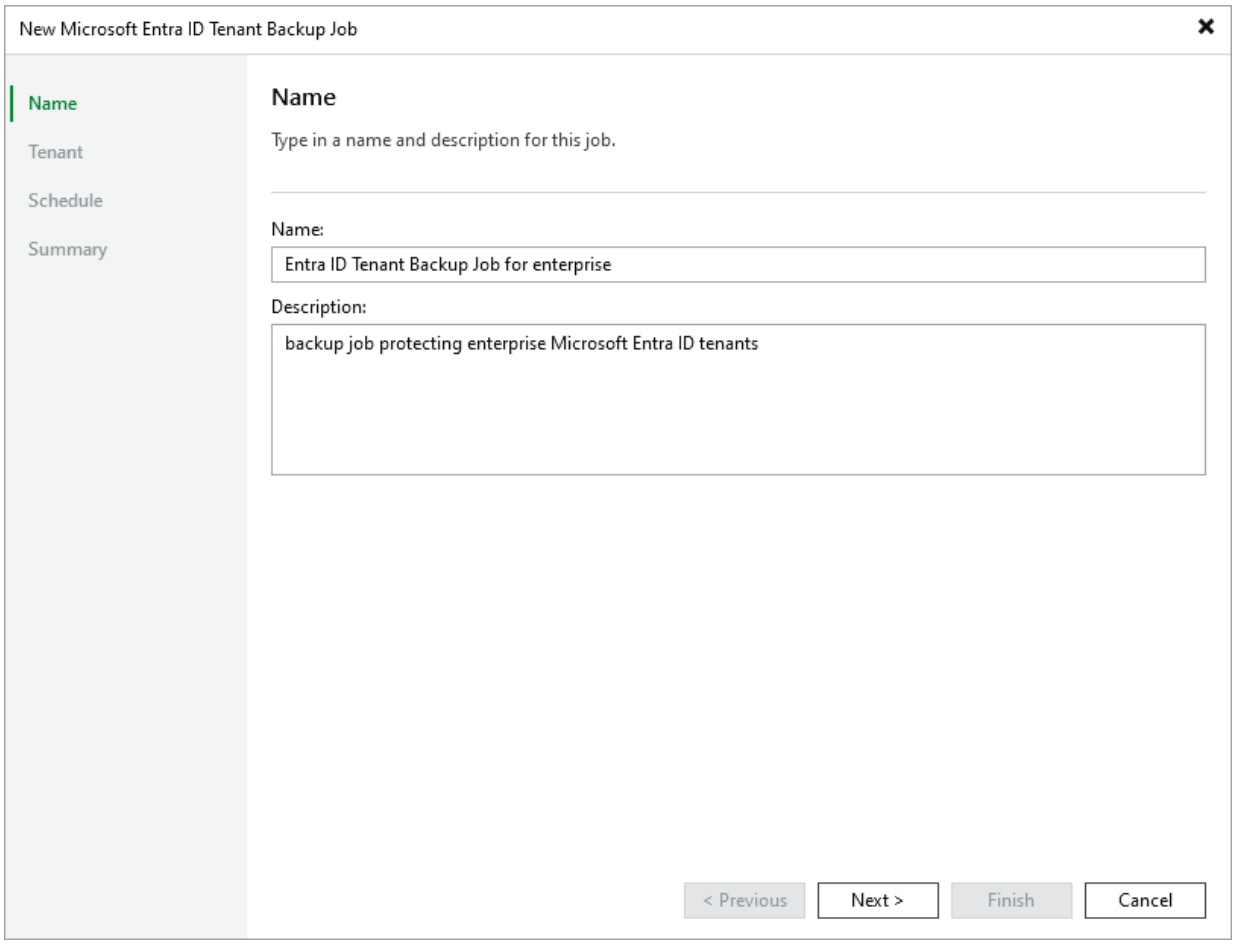
To launch the **Microsoft Entra ID Tenant Backup Job** wizard, do either of the following:

- Open the **Home** view. On the ribbon, click **Backup Job** > **Microsoft Entra ID** > **Tenant**.
- Open the **Home** view. In the inventory pane, right-click **Jobs** and select **Backup** > **Microsoft Entra ID** > **Tenant**.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup job and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $.



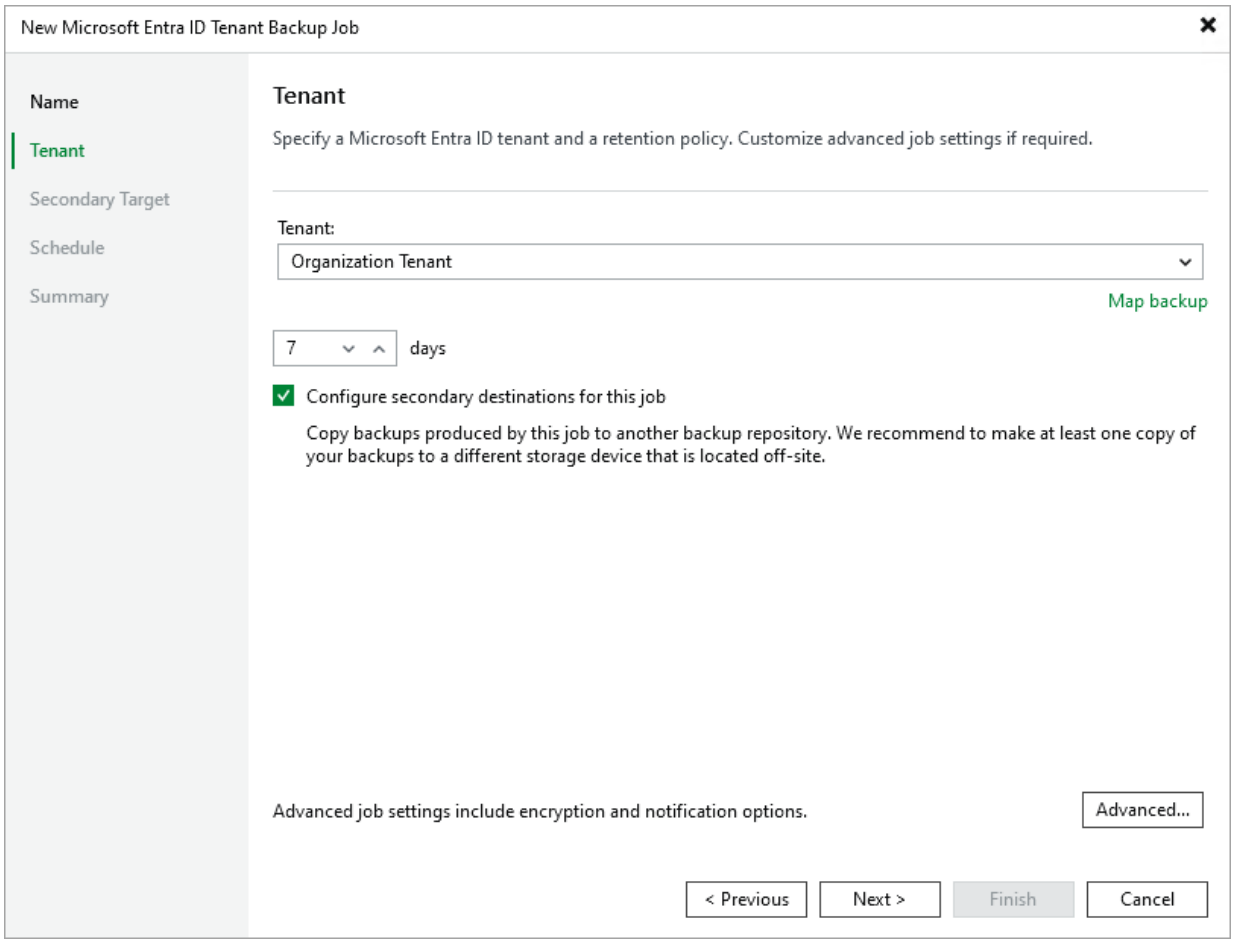
Step 3. Configure Backup Source Settings

At the **Tenant** step of the wizard, select a Microsoft Entra ID tenant whose resources you want to back up, and specify the number of days for which you want to keep restore points in a backup chain. If a restore point is older than the specified time limit, Veeam Backup for Microsoft Entra ID removes the restore point from the chain.

By default, Veeam Backup & Replication saves all backed-up tenant data to the local Microsoft Entra ID backup repository. To increase data availability and ensure that it can be recovered in case a disaster strikes, you can instruct Veeam Backup for Microsoft Entra ID to copy the backed-up tenant data to another location. To do that, select the **Configure secondary destinations for this job** check box and follow the instructions provided at step 4.

When restoring data of the backed-up tenant, Veeam Backup & Replication will offer you to choose a restore point from the list of all restore points available both in the default and secondary backup repositories (if applicable). To allow Veeam Backup & Replication to detect restore points created for this tenant by other backup jobs or stored in other backup repositories, you can map these restore points to this backup job — this way, Veeam Backup & Replication will transfer less data over network, reducing unwanted overhead for the production environment. To do that, click **Map backup** and choose the necessary backup.

> **TIP**
>
> Veeam Backup for Microsoft Entra ID does not encrypt backed-up data and uses the global notification settings configured for the backup server. To use password-based data encryption and specify custom notification settings for the backup job, click **Advanced** and follow the instructions provided in section Advanced Settings.



Advanced Settings

In the **Advanced Settings** window, you can instruct Veeam Backup for Microsoft Entra ID to use password-based data encryption and specify custom notification settings for the backup job.

Encryption Settings

To enable encryption for the backed-up data, switch to the **Encryption** tab and do the following:

1. Select the **Enable backup data encryption** check box.
2. From the **Password** drop-down list, select the password that you want to use for encryption.

   For a password to be displayed in the **Password** list, it must be added to the **Password Manager** as described the Veeam Backup & Replication User Guide, section Password Manager. If you have not added the necessary password to the **Password Manager** beforehand, you can do it without closing the **Advanced Settings** window. To do that, click either the **Manage passwords** link or the **Add** button, and specify the password and hint in the **Password** window.

   You can also use KMS keys for encryption. For more information, see Veeam Backup & Replication User Guide, section Key Management System Keys.

Notification Settings

To instruct Veeam Backup & Replication to send email notifications on the backup job results, switch to the **Notifications** tab and do the following:

1. To enable SNMP notifications for the backup job, select the **Send SNMP notifications for this job** check box.

   By default, Veeam Backup & Replication applies global SNMP settings configured as described in the Veeam Backup & Replication User Guide, section Specifying SNMP Settings.

2. To add specific recipients, select the **Send e-mail notifications to the following recipients** check box and specify the necessary e-mail addresses. Use a semicolon to separate multiple recipient addresses.

3. Choose whether you want to apply global notification settings or configure custom settings.

   Note that if you choose to use the global notification settings, Veeam Backup & Replication will also send email notifications on the backup job results to recipients configured in the global notification settings.

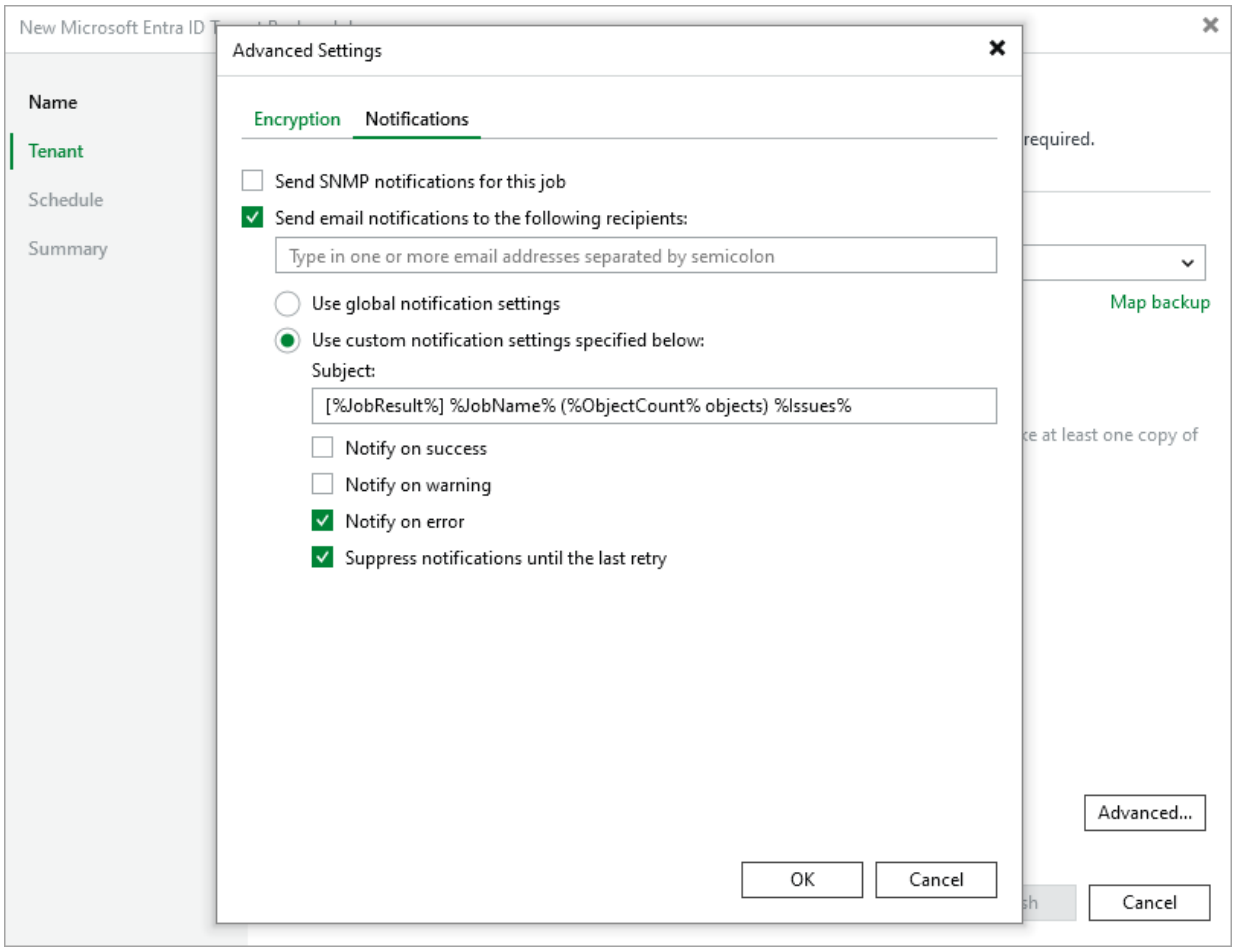
4. [Applies only if you choose to use custom notification settings] You can specify a subject for notifications in the **Subject** field. You can use the following runtime variables:

   - %JobName% — a backup job name.
   - %JobResult% — a backup job result.
   - %ObjectCount% — the number of Entra ID resources in a backup job.
   - %Issues% — the number of Entra ID resources in a backup job that encountered any issues (errors and warnings) while being processed.

   The default subject for email notifications is: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%.

5. [Applies only if you choose to use custom notification settings] You can choose whether you want Veeam Backup & Replication to send email notifications in case the backup job completes successfully, completes with warnings or completes with errors.

   By default, Veeam Backup & Replication retries to run failed backup jobs 3 times and sends notifications after every retry. To instruct Veeam Backup & Replication to send notifications only after the latest retry, select the **Suppress notifications until the last retry** check box.



Step 4. Configure Backup Copy Settings

[This step applies only if you have selected the **Configure secondary destinations for this job** check box at the **Tenant** step of the wizard]

Veeam Backup for Microsoft Entra ID stores tenant backups produced by all backup jobs in the same Microsoft Entra ID backup repository where the Veeam Backup & Replication configuration database resides. At the **Secondary Target** step of the wizard, you can increase data availability by instructing Veeam Backup for Microsoft Entra ID to copy the backed-up tenant data to another location — to do that, click **Add** and choose the necessary repository in the **Select Repository** window. For a backup repository to be displayed in the **Secondary repositories** list, it must be added to the backup infrastructure as described in in the Veeam Backup & Replication User Guide, section Backup Repositories.

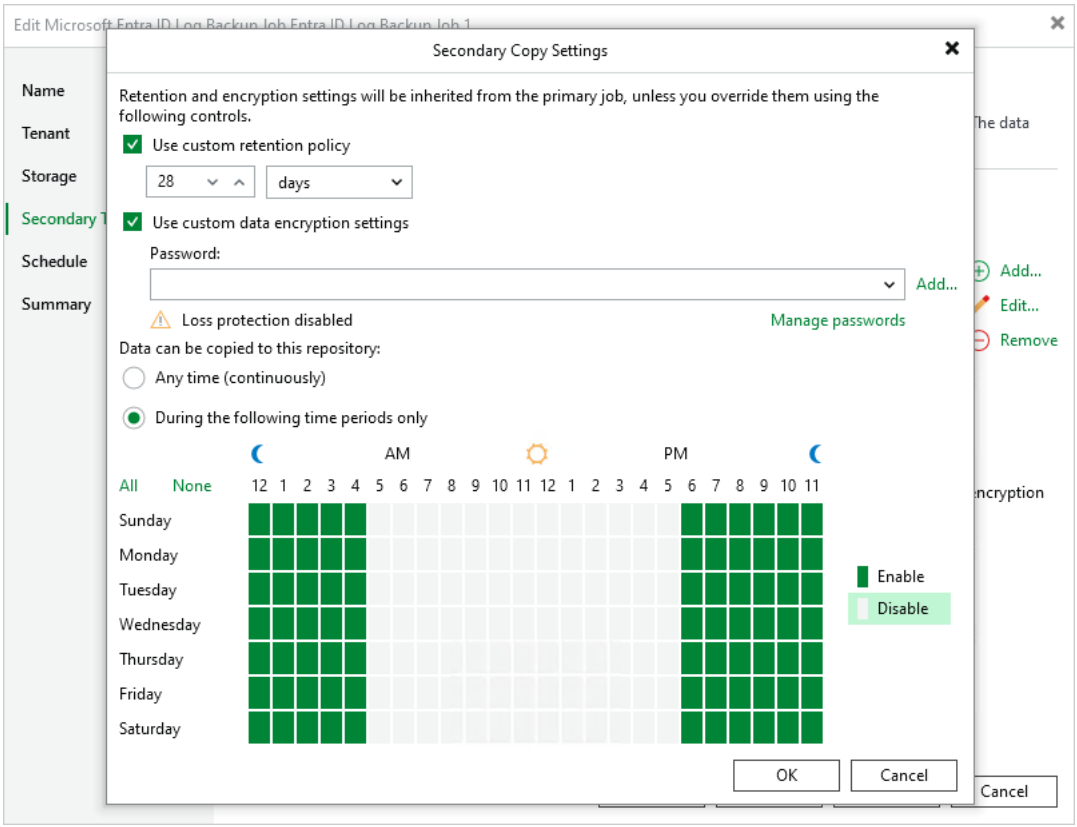
> **NOTE**
>
> To enhance data protection, you can instruct Veeam Backup for Microsoft Entra ID to copy tenant backups to multiple repositories. However, keep in mind that Veeam Cloud Connect repositories are not supported.

By default, Veeam Backup for Microsoft Entra ID will start creating backup copies as soon as the tenant backup job completes successfully, and will apply the same retention and encryption settings that you have configured at step 3. To change this behavior, you can do the following:

- Extend the retention period for the created backup copies — to do that, select the **Use custom retention policy** check box and specify a number of days (or months) for which Veeam Backup for Microsoft Entra ID will retain these copies.
- Increase the security of the created backup copies — to do that, select the **Use custom data encryption settings** check box and provide a specific password that will be used to access these copies.

  For a password to be displayed in the list of available passwords, it must be added to the Password Manager as described in the Veeam Backup & Replication User Guide, section Password Manager. If you have not added the necessary password to the Password Manager beforehand, you can do it without closing the **Secondary Copy Settings** window. To do that, click either the **Manage passwords** link or the **Add** button, and specify the password and hint in the **Password** window.
- Prevent backup copy operations from overlapping with production hours — to do that, select the **During the following time periods only** check box and configure a specific time interval for Veeam Backup for Microsoft Entra ID to create backup copies.

> **IMPORTANT**
>
> If a backup copy operation exceeds the configured time interval, this operation will be terminated automatically.


Edit Microsoft Entra ID Log Backup Job Entra ID Log Backup Job 1
Name
Tenant
Storage
Secondary T
Schedule
Summary
Secondary Copy Settings
Retention and encryption settings will be inherited from the primary job, unless you override them using the following controls.
Use custom retention policy
28
days
Use custom data encryption settings
Password:
Add...
Loss protection disabled
Manage passwords
Data can be copied to this repository:
Any time (continuously)
During the following time periods only
AM
PM
All
None
12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Enable
Disable
OK
Cancel
The data
Add...
Edit...
Remove
ncryption
Cancel

Step 5. Define Job Schedule

At the **Schedule** step of the wizard, you can instruct Veeam Backup for Microsoft Entra ID to run the backup job automatically according to a specific backup schedule — to do that, select the **Run the job automatically** check box. The backup schedule defines how often data of the tenant added to the backup job will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Entra ID allows you to create schedules of the following types:

- **Daily** — the backup job will run at a specific time on specific days.

  To create a daily schedule for the backup job, select the **Daily at this time** option and define the exact hour when the job will create restore points. Then, use the drop-down list to choose whether you want the backup job to run every day, on weekdays (Monday through Friday) or on specific days.

- **Monthly** — the backup job will run once a day on specific days.

  To create a monthly schedule for the backup job, select the **Monthly at this time** option and define the exact hour when the job will create restore points. Then, use the drop-down lists to schedule the specific days and months for the backup job to run.

- **Periodically** — the backup job will run repeatedly throughout a day with a specific time interval.

  To create a periodical schedule for the backup job, select the **Periodically every** option and define the frequency (in hours or minutes) with which the job will create restore points. Alternatively, you can instruct Veeam Backup for Microsoft Entra ID to create backups continuously, one after another.

  To prevent backup operations from overlapping with production hours, it is recommended that you configure a time interval during which Veeam Backup for Microsoft Entra ID is allowed to create restore points; to do that, click **Schedule** and configure the necessary interval. If a backup operation exceeds the configured time interval, this operation will not be terminated unless you specify a backup window.

- **Subsequently** — the backup job will run after another job.

  To create a subsequent schedule for the backup job, select the **After this job** option and use the drop-down list to choose the necessary job.

NOTES

- If you do not select the **Run the job automatically** check box, Veeam Backup for Microsoft Entra ID will only create restore points when you start the backup job manually.
- If you select the **Run the job automatically** check box but do not configure any scheduling settings, Veeam Backup for Microsoft Entra ID will run the job daily at 10:00 PM.

Additionally, you can configure the following settings:

- Instruct Veeam Backup for Microsoft Entra ID to run the backup job again if it fails on the first try.

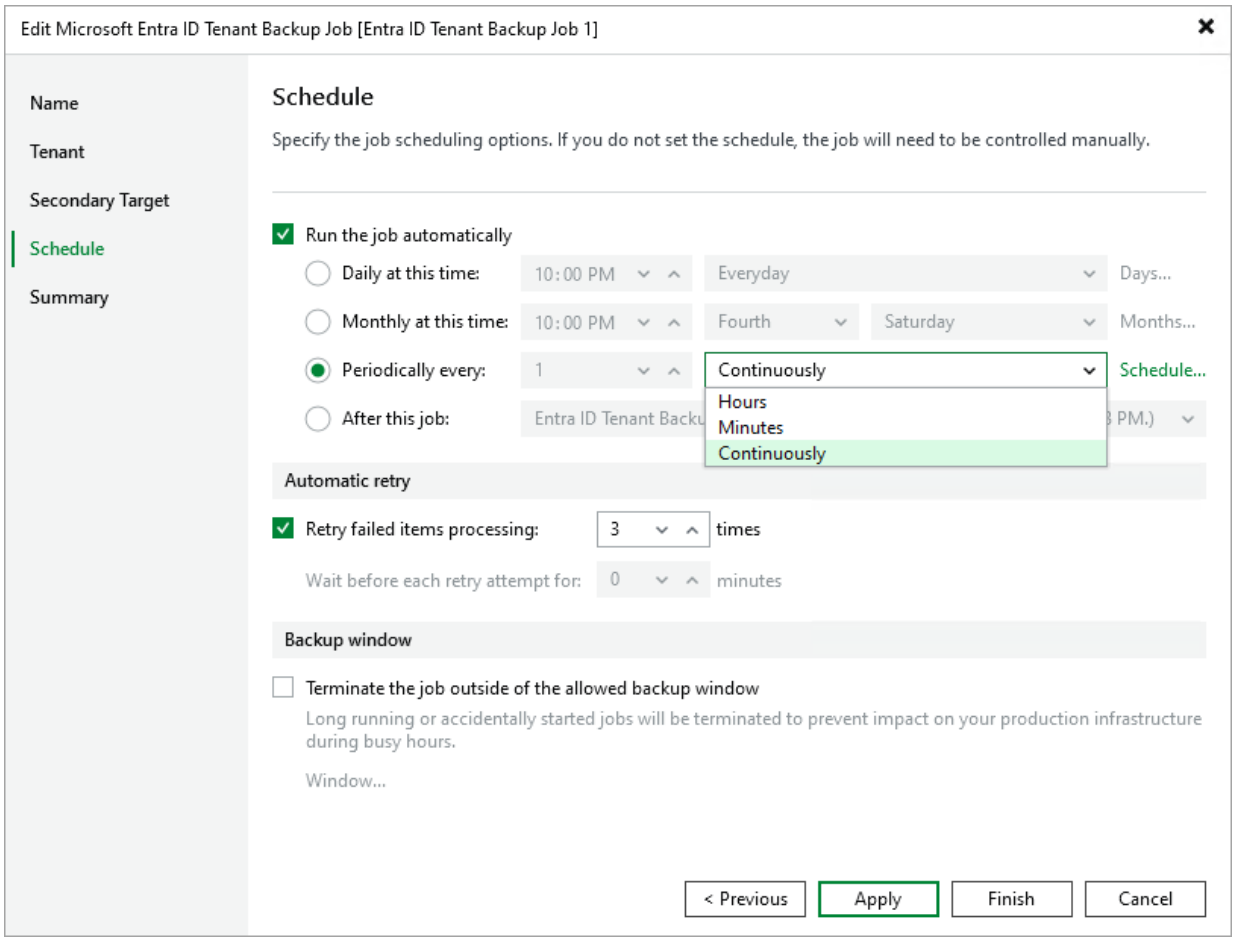
  To do that, select the **Retry failed items processing** check box and specify the maximum number of attempts to run the backup job.

- Instruct Veeam Backup for Microsoft Entra ID to terminate the backup job if it creates unwanted overhead for the production environment.

  To do that, select the **Terminate the job outside of the allowed backup window** check box and click **Window**. Then, define a time interval during which Veeam Backup for Microsoft Entra ID is allowed to run the backup job. If a backup operation exceeds the configured time interval, this operation will be terminated automatically.

NOTES

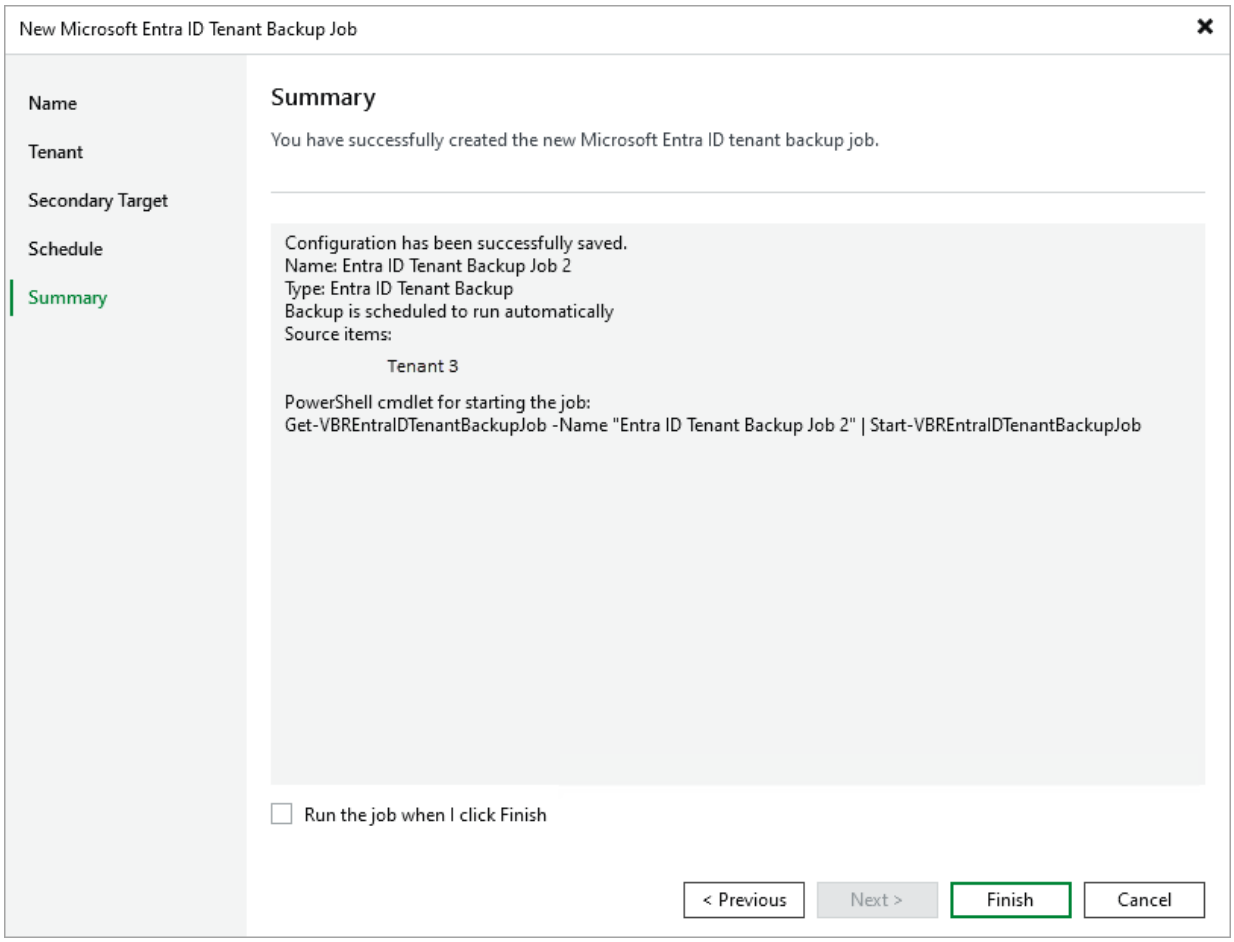
- When retrying backup jobs, Veeam Backup & Replication processes only those items that failed to be backed up during the previous attempt.
- Automatic retry settings apply only to backup jobs that run according to specific schedules — these settings do not apply to jobs started manually.
- The default time interval between retries cannot be modified for backup jobs that create restore points continuously according to a periodical schedule. When running these jobs, Veeam Backup & Replication will make retry attempts one after another, without any interval.



Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

> **TIP**
>
> If you want to run the backup job right after you finish working with the wizard, select the **Run the job when I click Finish** check box. Alternatively, you can run the job manually later as described in section Starting and Stopping Backup Jobs.



Creating Log Backup Jobs

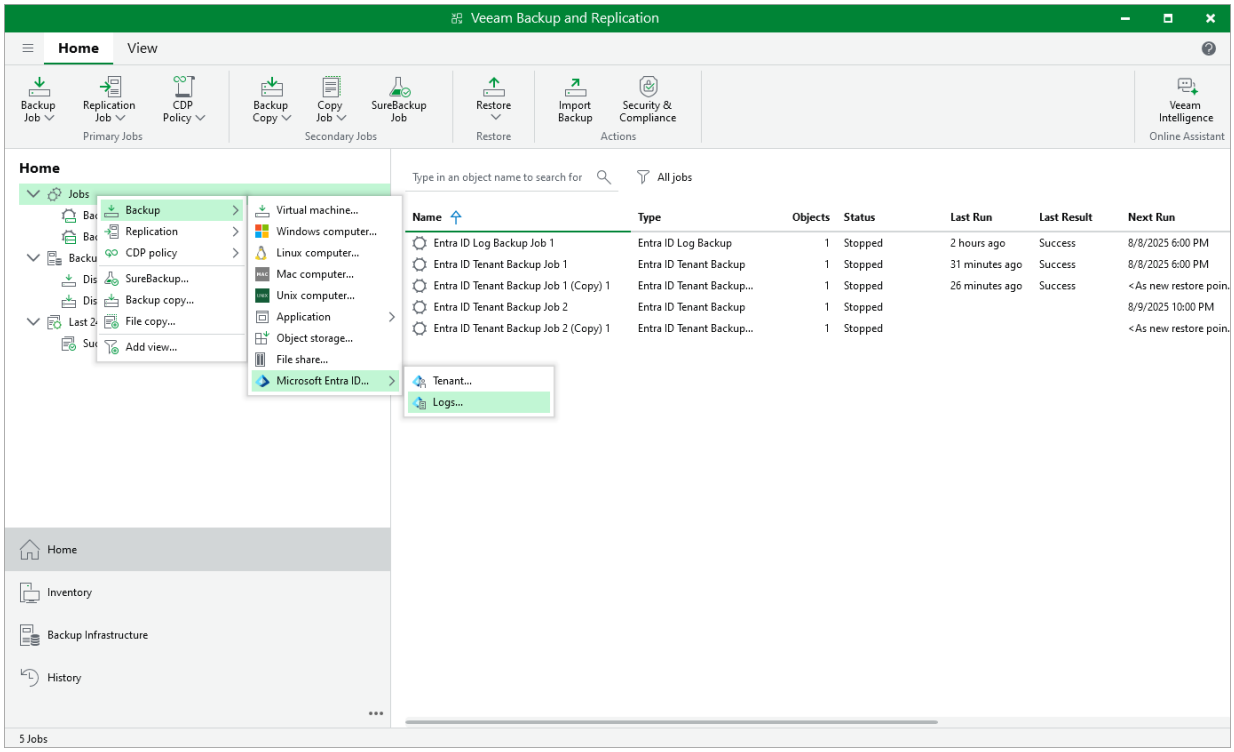
To create a Microsoft Entra ID log backup job, do the following:

1. Launch the New Microsoft Entra ID Log Backup Job wizard.
2. Specify a job name and description.
3. Specify a tenant.
4. Specify backup repository settings.
5. Specify secondary repository settings.
6. Define a job schedule.
7. Finish working with the wizard.

Step 1. Launch New Microsoft Entra ID Log Backup Job Wizard

To launch the **Microsoft Entra ID Log Backup Job** wizard, do either of the following:

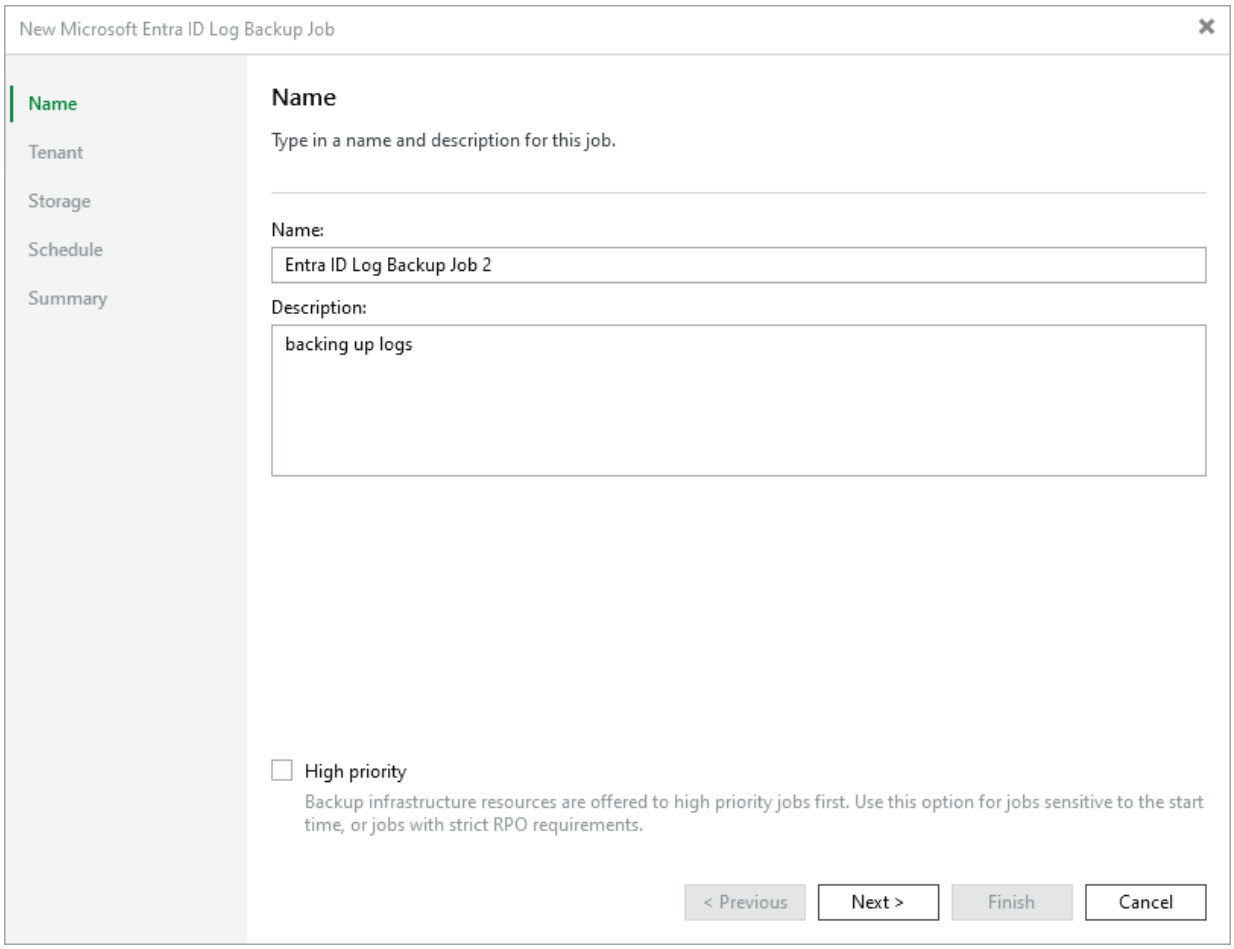
- Open the **Home** view. On the ribbon, click **Backup Job** > **Microsoft Entra ID** > **Logs**.
- Open the **Home** view. In the inventory pane, right-click **Jobs** and select **Backup** > **Microsoft Entra ID** > **Logs**.



Step 2. Specify Job Name and Description

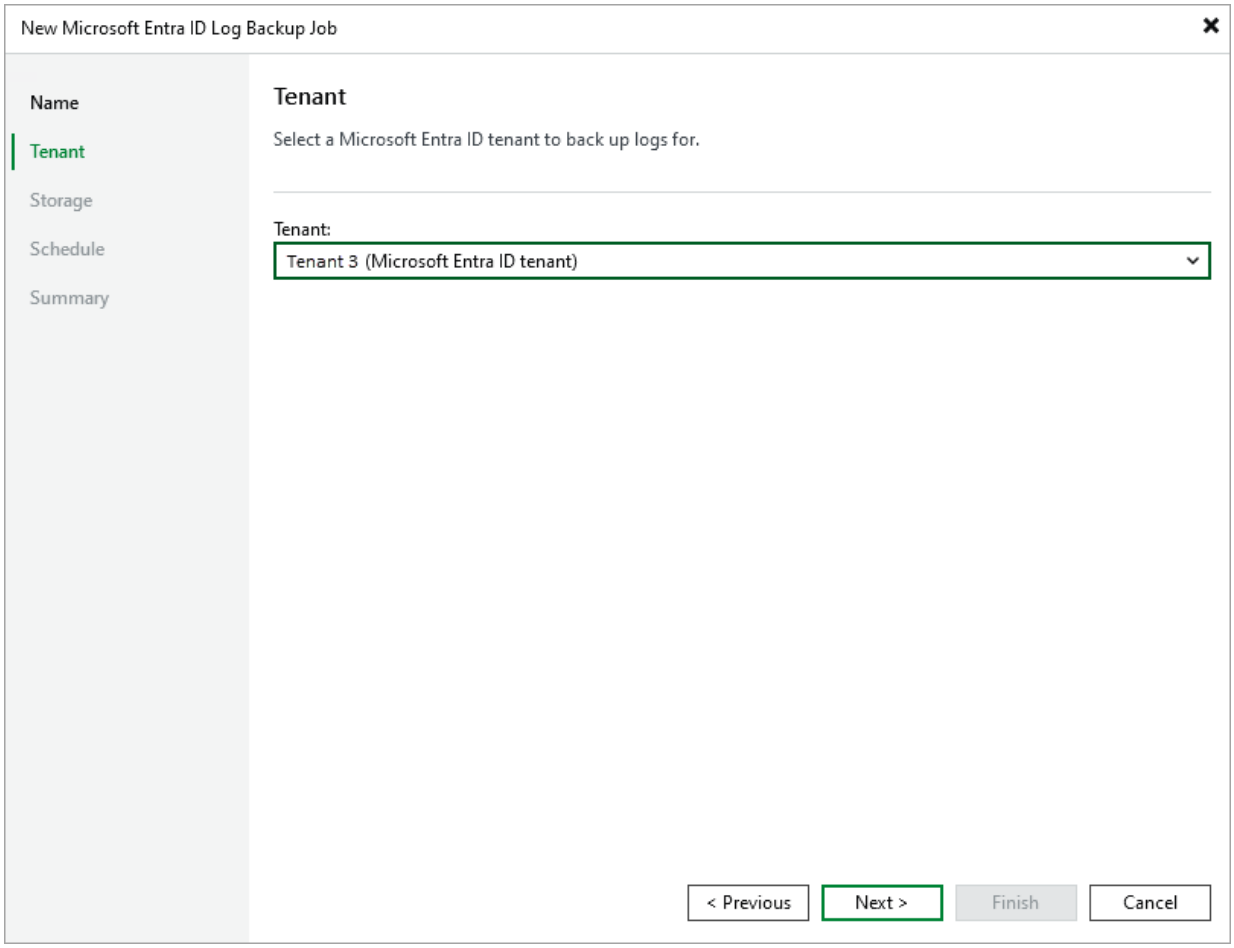
At the **Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup job and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $.

> **TIP**
>
> If you want Veeam Backup & Replication to prioritize the log backup job over other jobs and to allocate backup infrastructure resources to this job first, select the **High priority** check box. For more information on job priorities, see the Veeam Backup & Replication User Guide, section Getting Started.



Step 3. Specify Tenant

At the **Tenant** step of the wizard, select a Microsoft Entra ID tenant whose audit and sign-in logs you want to back up.



Step 4. Specify Backup Repository Settings

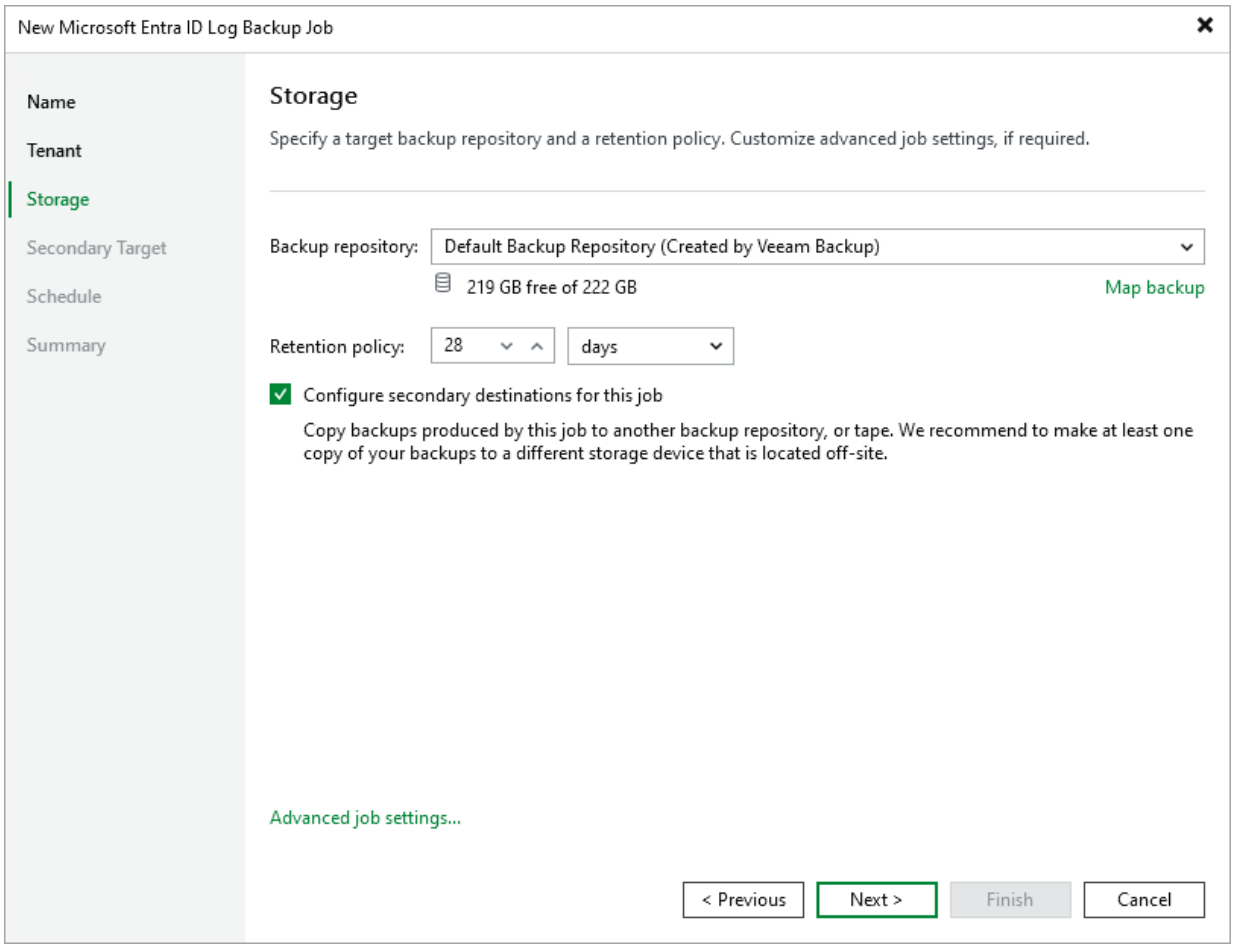
At the **Storage** step of the wizard, you can choose a backup repository where the backed-up log data will be stored. You can also specify the number of days, months or years for which you want to keep restore points in a backup chain — if a restore point is older than the specified time limit, Veeam Backup for Microsoft Entra ID removes the restore point from the chain.

To increase data availability and ensure that it can be recovered in case a disaster strikes, you can instruct Veeam Backup for Microsoft Entra ID to copy the backed-up log data to another backup repository. To do that, select the **Configure secondary destinations for this job** check box and follow the instructions provided at step 4.

> **NOTE**
>
> Veeam Backup for Microsoft Entra ID does not support storing log backups in Veeam Cloud Connect repositories or Amazon S3 repositories with multiple buckets.

When restoring backed-up log data, Veeam Backup & Replication will offer you to choose a restore point from the list of all restore points available both in the primary and secondary backup repositories (if applicable). To allow Veeam Backup & Replication to detect restore points created for this log data by other backup jobs or stored in other backup repositories, you can map these restore points to this backup job — this way, Veeam Backup & Replication will transfer less data over network, reducing unwanted overhead for the production environment. To do that, click **Map backup** and choose the necessary backup.

> **TIP**
>
> To help you implement a comprehensive backup strategy, Veeam Backup & Replication allows you to configure additional backup job settings (for example, you can enable health check, upload custom scripts and customize email notifications). To do that, click **Advanced job settings** and follow the instructions provided in section Advanced Settings.



Advanced Settings

In the **Advanced Settings** window, you can configure additional log backup job settings, such as compression level, password-based data encryption and custom notification settings.

Data Compression and Encryption Settings

By default, Veeam Backup & Replication does not encrypt backup files and uses the *Optimal* compression level to store these files. To change this behavior, switch to the **Storage** tab and do the following:

- To decrease the size of the files, select a compression level from the **Compression level** drop-down list (*None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*). For more information on compression levels, see the Veeam Backup & Replication User Guide, section Data Compression and Deduplication.
- To encrypt the content of the files, select the **Enable backup file encryption** check box and specify a password that will be used to encrypt data.

  For a password to be displayed in the list of available passwords, it must be added to the Password Manager as described in the Veeam Backup & Replication User Guide, section Managing Credentials. If you have not added the necessary password beforehand, you can do it without closing the **Advanced Settings** window. To do that, click either **Manage passwords** or **Add**, and specify the password and a hint in the **Password** window.

NOTES

- For security reasons, Veeam Backup & Replication does not store the password you specify to encrypt data — that is why you will not be able to restore data from encrypted backups in case you lose the password. However, if your backup server is connected to Veeam Backup Enterprise Manager, you can recover the password as described in the Veeam Backup & Replication User Guide, section Password Loss Protection.
- To encrypt backed-up data, you can also use KMS keys as described in the Veeam Backup & Replication User Guide, section Key Management System Keys.

Maintenance Settings

Health checks help you ensure that the restore points created by the backup job are consistent and that you will be able to restore data using these restore points. To instruct Veeam Backup & Replication to periodically perform a health check for the restore points created by the job, switch to the **Maintenance** tab and do the following:

- Select the **Perform backup files health check** check box.
- To configure a custom schedule, click **Configure** and choose whether you want the health check sessions to run monthly, weekly or on specific days.

  By default, Veeam Backup & Replication runs health check sessions every last Saturday of a month.

Script Settings

Scripts allow you to execute customized tasks before or after backup sessions, such as removing temporary files or tracking permission updates in Entra ID environment. To instruct Veeam Backup & Replication to run a custom script, switch to the **Scripts** tab and do the following:

1. Select the **Run the following script before the job** or **Run the following script after the job** check box.
2. Click **Browse** to choose executable files from a local folder on the backup server.
3. Choose whether you want Veeam Backup & Replication to execute the script periodically or on specific days only.

Notification Settings

Notification settings help you automate and customize delivery of the backup job results. To instruct Veeam Backup & Replication to send email notifications on the backup job status to specific addresses, switch to the **Notifications** tab and do the following:

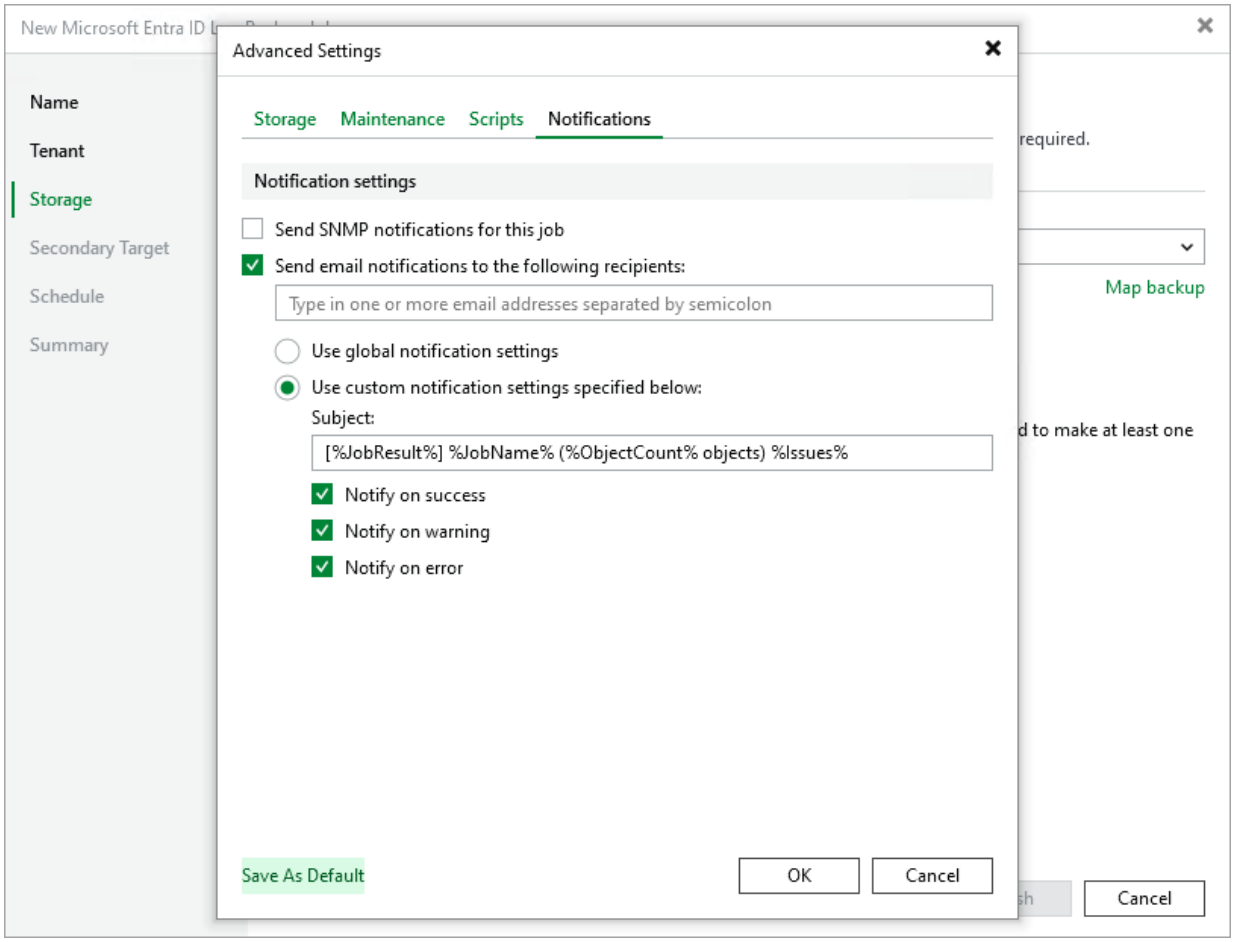
- To receive SNMP notifications on the backup job, select the **Send SNMP notifications for this job** check box.

  For Veeam Backup & Replication to be able to send SNMP notifications, you must configure global SNMP settings as described in the Veeam Backup & Replication User Guide, section Specifying SNMP Settings.
- To receive notifications by email in case of backup failure, success or warning, select the **Send email notifications to the following recipients** check box and specify an email address of a recipient; use a semicolon to separate multiple recipient addresses.

  For Veeam Backup & Replication to be able to send email notifications, you must configure global email notification settings as described in the Veeam Backup & Replication User Guide, section Configuring Global Email Notification Settings.

- To specify custom notification subject, select **Use custom notification settings specified below** check box, and create a notification subject using the runtime variables provided in the **Subject** field.

> **TIP**
>
> To instruct Veeam Backup & Replication to further use any of the updated advanced settings by default, click **Save As Default** in the respective tab.



How Health Check Works

When Veeam Backup & Replication saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup & Replication verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

On the day scheduled for a health check to run, Veeam Backup & Replication starts a new health check session. For each restore point in the standard backup chain, Veeam Backup & Replication calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup & Replication also checks whether data blocks that are required to rebuild the restore point are available.

If Veeam Backup & Replication does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error. Depending on the detected data inconsistency, Veeam Backup & Replication performs the following operations:

- If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup & Replication marks the backup chain as corrupted in the configuration database. During the next backup job session, Veeam Backup & Replication copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.
- If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup & Replication marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup job session, Veeam Backup & Replication copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.

Step 5. Specify Secondary Repository Settings

[This step applies only if you have selected the **Configure secondary destinations for this job** check box at the **Storage** step of the wizard]

Veeam Backup for Microsoft Entra ID stores log backups produced by all backup jobs in the same Microsoft Entra ID backup repository where the Veeam Backup & Replication configuration database resides. At the **Secondary Target** step of the wizard, you can increase data availability by instructing Veeam Backup for Microsoft Entra ID to copy the backed-up tenant data to another location — to do that, click **Add** and choose the necessary repository in the **Select Repository** window. For a backup repository to be displayed in the **Secondary repositories** list, it must be added to the backup infrastructure as described in in the Veeam Backup & Replication User Guide, section Backup Repositories.

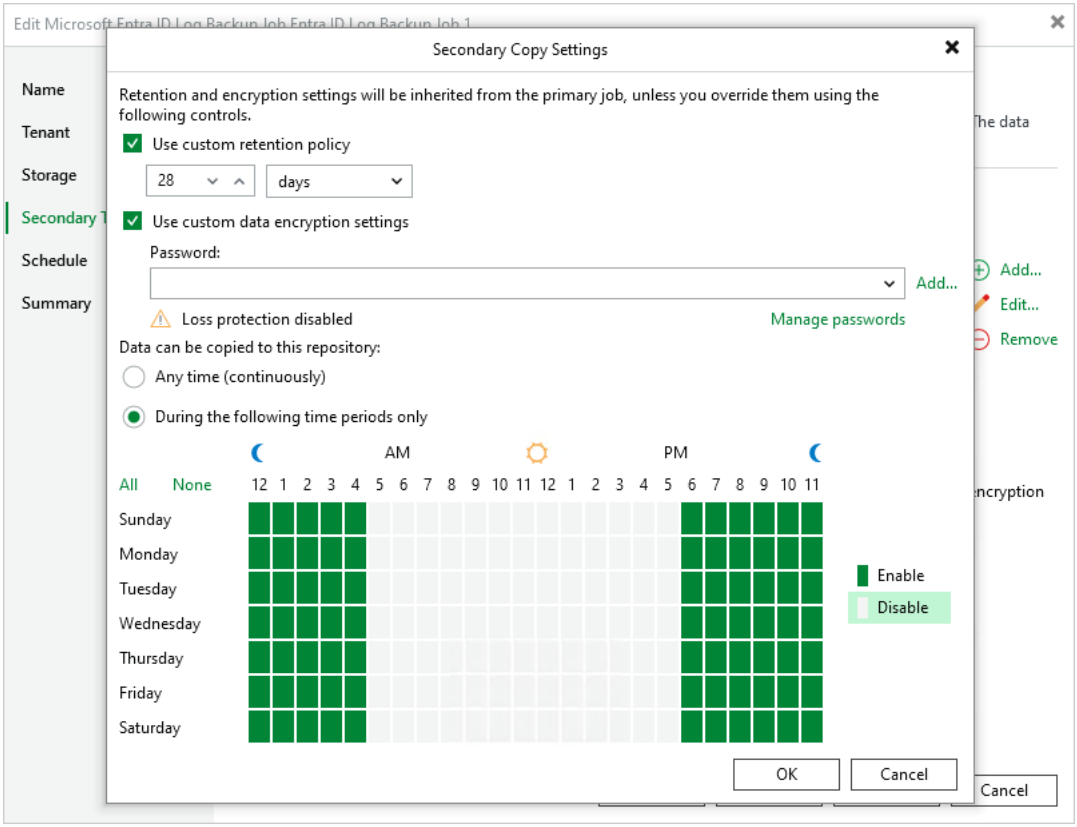
> **NOTE**
>
> To enhance data protection, you can instruct Veeam Backup for Microsoft Entra ID to copy log backups to multiple repositories. However, keep in mind that Veeam Cloud Connect repositories are not supported.

By default, Veeam Backup for Microsoft Entra ID will start creating backup copies as soon as the log back up job completes successfully, and will apply the same retention and encryption settings that you have configured at step 4. To change this behavior, you can do the following:

- Extend the retention period for the created backup copies — to do that, select the **Use custom retention policy** check box and specify a number of days (or months) for which Veeam Backup for Microsoft Entra ID will retain these copies.
- Increase the security of the created backup copies — to do that, select the **Use custom data encryption settings** check box and provide a specific password that will be used to access these copies.

  For a password to be displayed in the list of available passwords, it must be added to the Password Manager as described in the Veeam Backup & Replication User Guide, section Password Manager. If you have not added the necessary password to the Password Manager beforehand, you can do it without closing the **Secondary Copy Settings** window. To do that, click either the **Manage passwords** link or the **Add** button, and specify the password and hint in the **Password** window.
- Prevent backup copy operations from overlapping with production hours — to do that, select the **During the following time periods only** check box and configure a specific time interval for Veeam Backup for Microsoft Entra ID to create backup copies.

> **IMPORTANT**
>
> If a backup copy operation exceeds the configured time interval, this operation will be terminated automatically.


Edit Microsoft Entra ID Log Backup Job Entra ID Log Backup Job 1
Name
Tenant
Storage
Secondary T
Schedule
Summary
Secondary Copy Settings
Retention and encryption settings will be inherited from the primary job, unless you override them using the following controls.
Use custom retention policy
28
days
Use custom data encryption settings
Password:
Add...
Loss protection disabled
Manage passwords
Data can be copied to this repository:
Any time (continuously)
During the following time periods only
AM
PM
All
None
12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Enable
Disable
OK
Cancel
The data
Add...
Edit...
Remove
ncryption
Cancel

Step 6. Define Job Schedule

At the **Schedule** step of the wizard, you can instruct Veeam Backup for Microsoft Entra ID to run the backup job automatically according to a specific backup schedule — to do that, select the **Run the job automatically** check box. The backup schedule defines how often data of the tenant added to the backup job will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Entra ID allows you to create schedules of the following types:

- **Daily** — the backup job will run at a specific time on specific days.

  To create a daily schedule for the backup job, select the **Daily at this time** option and define the exact hour when the job will create restore points. Then, use the drop-down list to choose whether you want the backup job to run every day, on weekdays (Monday through Friday) or on specific days.

- **Monthly** — the backup job will run once a day on specific days.

  To create a monthly schedule for the backup job, select the **Monthly at this time** option and define the exact hour when the job will create restore points. Then, use the drop-down lists to schedule the specific days and months for the backup job to run.

- **Periodically** — the backup job will run repeatedly throughout a day with a specific time interval.

  To create a periodical schedule for the backup job, select the **Periodically every** option and define the frequency (in hours or minutes) with which the job will create restore points. Alternatively, you can instruct Veeam Backup for Microsoft Entra ID to create backups continuously, one after another.

  To prevent backup operations from overlapping with production hours, it is recommended that you configure a time interval during which Veeam Backup for Microsoft Entra ID is allowed to create restore points; to do that, click **Schedule** and configure the necessary interval. If a backup operation exceeds the configured time interval, this operation will not be terminated unless you specify a backup window.

- **Subsequently** — the backup job will run after another job.

  To create a subsequent schedule for the backup job, select the **After this job** option and use the drop-down list to choose the necessary job.

NOTES

- If you do not select the **Run the job automatically** check box, Veeam Backup for Microsoft Entra ID will only create restore points when you start the backup job manually.
- If you select the **Run the job automatically** check box but do not configure any scheduling settings, Veeam Backup for Microsoft Entra ID will run the job daily at 10:00 PM.

Additionally, you can configure the following settings:

- Instruct Veeam Backup for Microsoft Entra ID to run the backup job again if it fails on the first try.

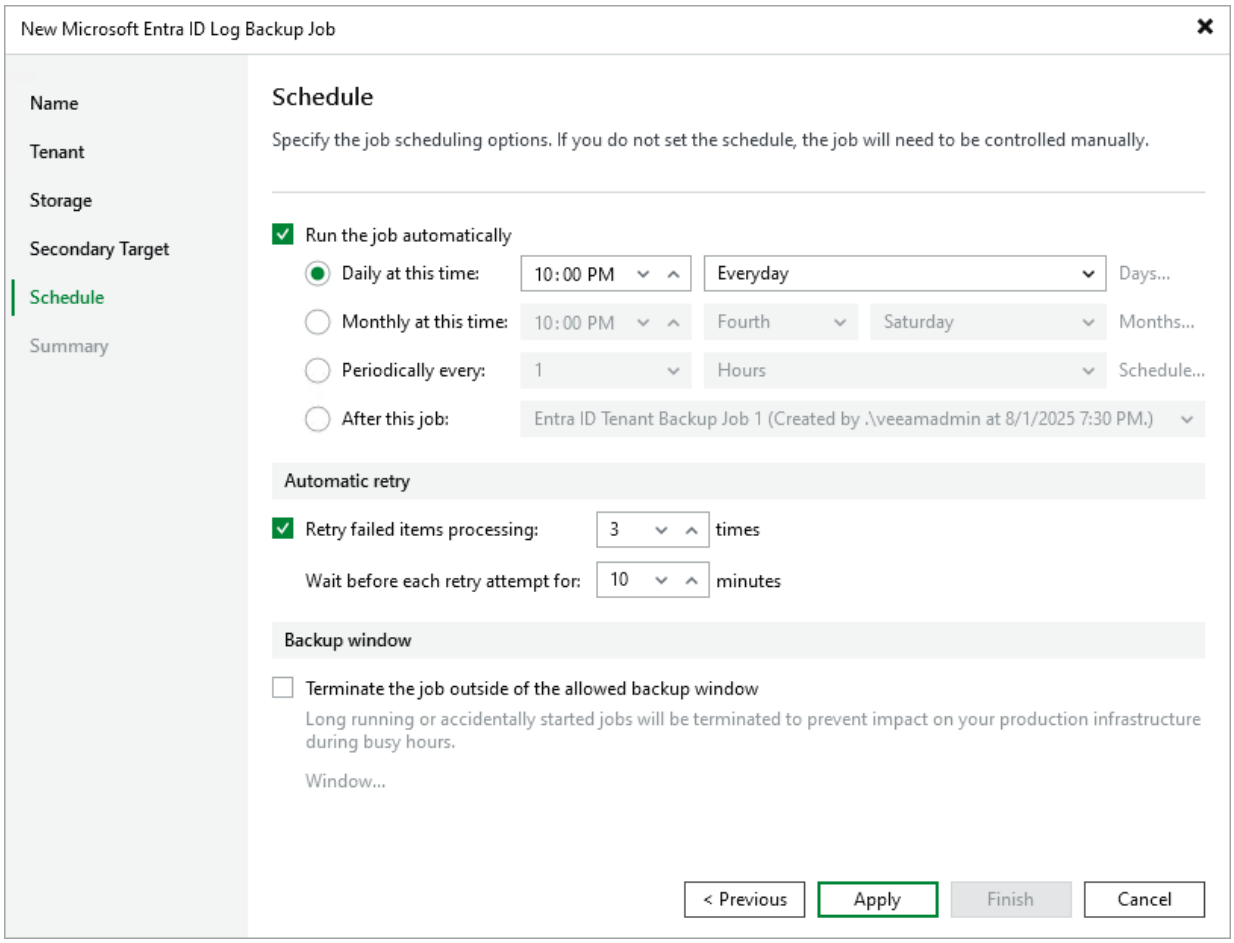
  To do that, select the **Retry failed items processing** check box and specify the maximum number of attempts to run the backup job.

- Instruct Veeam Backup for Microsoft Entra ID to terminate the backup job if it creates unwanted overhead for the production environment.

  To do that, select the **Terminate the job outside of the allowed backup window** check box and click **Window**. Then, define a time interval during which Veeam Backup for Microsoft Entra ID is allowed to run the backup job. If a backup operation exceeds the configured time interval, this operation will be terminated automatically.

NOTES

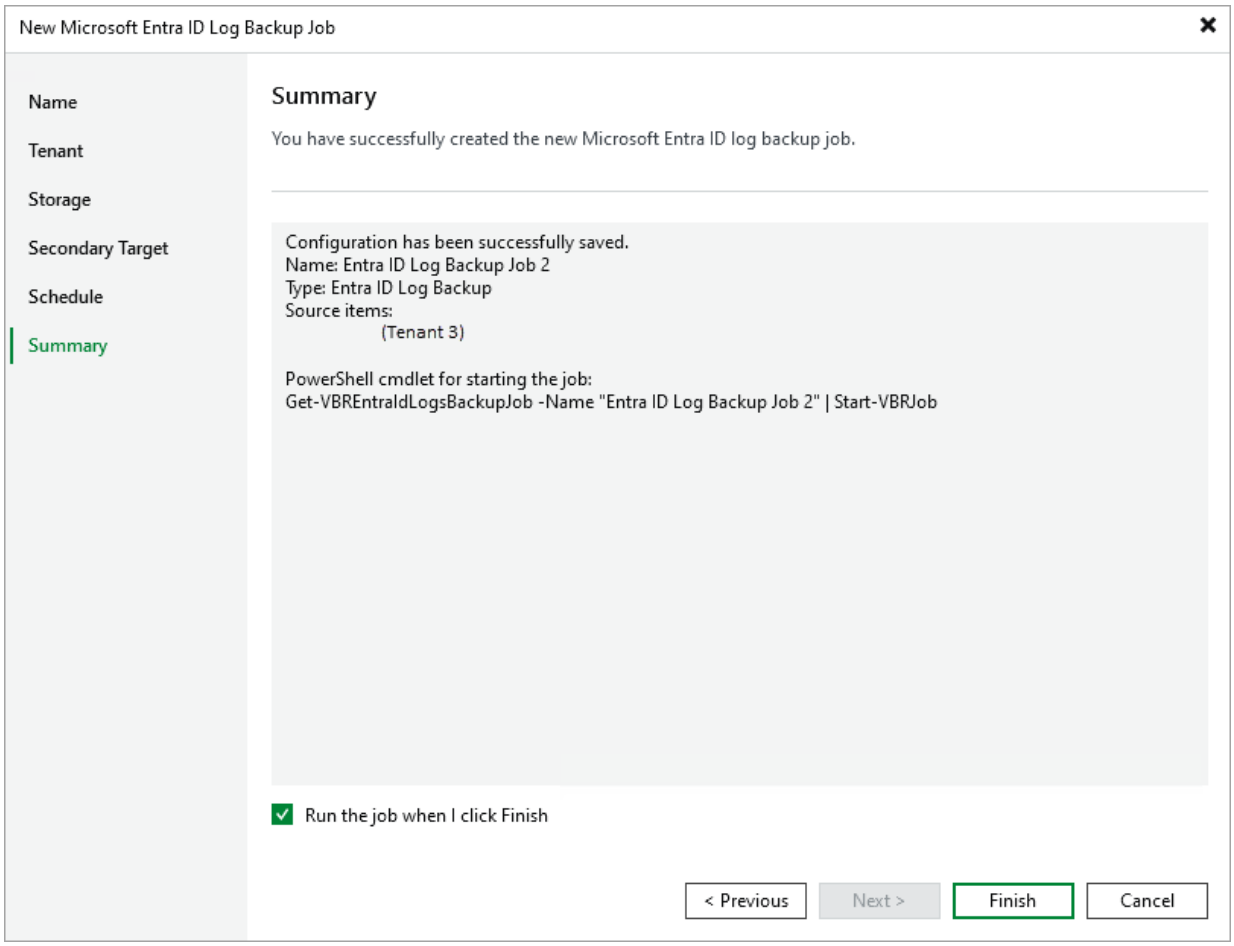
- When retrying backup jobs, Veeam Backup & Replication processes only those items that failed to be backed up during the previous attempt.
- Automatic retry settings apply only to backup jobs that run according to specific schedules — these settings do not apply to jobs started manually.
- The default time interval between retries cannot be modified for backup jobs that create restore points continuously according to a periodical schedule. When running these jobs, Veeam Backup & Replication will make retry attempts one after another, without any interval.



Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**. You will be able to edit the configured backup job settings as described in the Editing Backup Job Settings section.

> **TIP**
>
> If you want to run the job immediately after you finish working with the wizard, select the **Run the job when I click Finish** check box.



Managing Backup Jobs

To view all jobs configured on the backup server, open the **Home** view and select the **Jobs** node in the inventory pane. The list of available jobs is displayed in the working area. You can start and stop jobs, retry failed jobs, edit job properties, clone jobs, view job statistics and delete unnecessary jobs.

Starting and Stopping Backup Jobs

You can start a backup job manually, for example, if you want to create an additional restore point and do not want to modify the configured job schedule.

You can also stop a backup job manually if data processing is about to take too long, and you do not want to impact the production environment during business hours. When you stop a running job, Veeam Backup & Replication creates a new restore point only for those workloads that have already been processed by the time you stop the job.

Considerations

Consider the following:

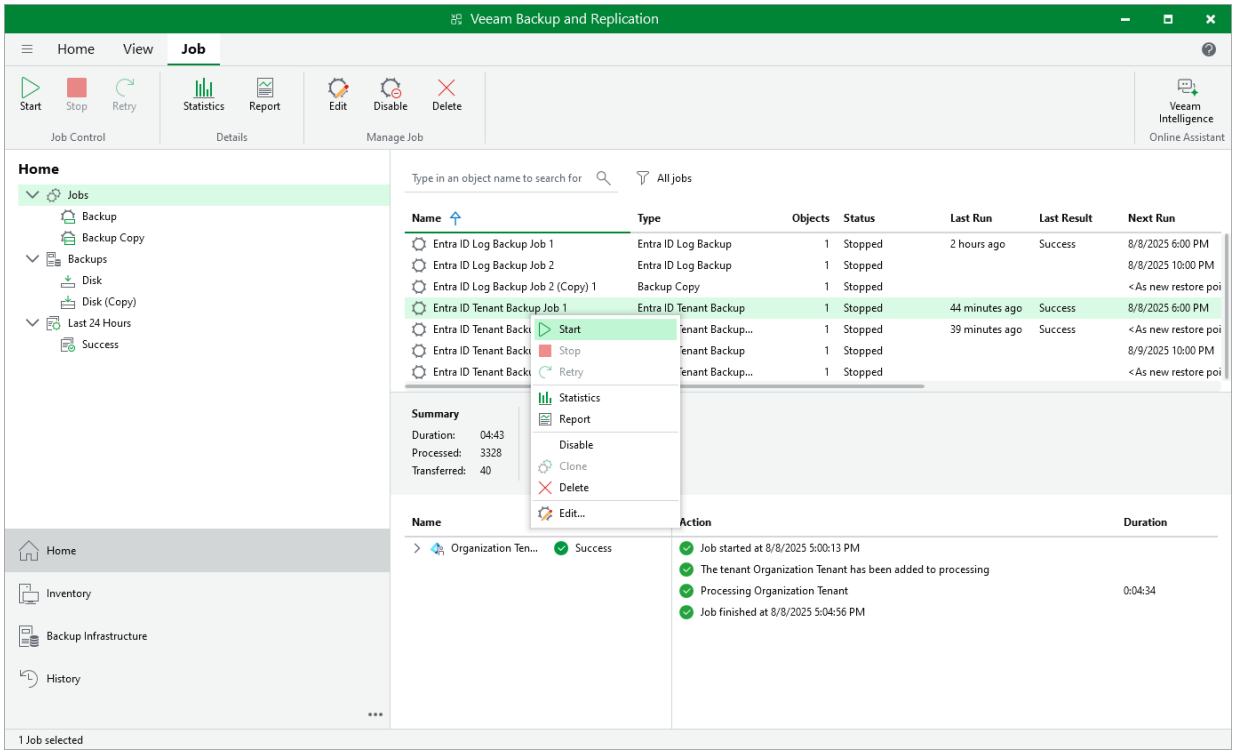
- [For tenant backup job] Veeam Backup & Replication will stop the job immediately and produce a new restore point only for those workloads that have already been processed when you stop the job.
- [For log backup jobs] You can stop the job in two ways:
  - Stop the job immediately. In this case, Veeam Backup & Replication will produce a new restore point only for those workloads that have already been processed when you stop the job.
  - Stop the job after the current file. In this case, Veeam Backup & Replication will produce a new restore point only for those workloads that have already been processed and for objects that are being processed at the moment.

Starting and Stopping Job

To start or stop a backup job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.

3. In the working area, select the necessary job and click **Start** or **Stop** on the ribbon. Alternatively, right-click the job and select **Start** or **Stop**.



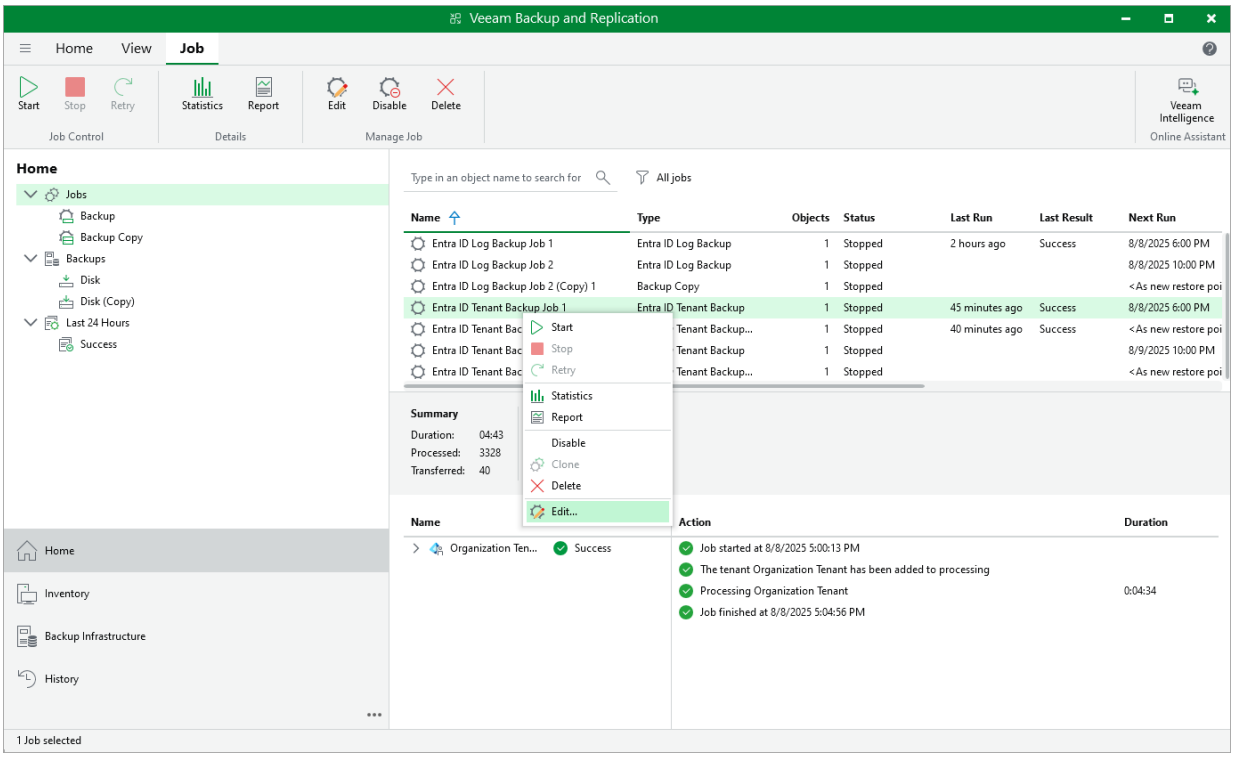
Editing Backup Job Settings

For each backup job, you can modify the settings configured while creating the job:

1. Open the **Home** view and navigate to **Jobs** > **Backup**.
2. In the working area, select the job and click **Edit** on the ribbon.

   Alternatively, you can right-click the job and select **Edit**.
3. Edit the necessary job settings as follows:
   - To provide a new name and description for the job, follow the instructions provided in section Creating Tenant Backup Jobs (step2) or Creating Log Backup Jobs (step 2).
   - To choose another project or folder that manages resources that you want to protect, or change the service account whose permissions are used to perform backup operations, follow the instructions provided in section Performing VM Backup (step 3), Performing SQL Backup (step 3) or Performing Spanner Backup (step 3).
   - To modify the list of regions in which instances that you plan to back up reside, or to add instances to the backup scope, follow the instructions provided in section Performing VM Backup (step 4a or step 4b), Performing SQL Backup (step 4a or step 4b) or Performing Spanner Backup (step 4a or step 4b).
   - To instruct Veeam Backup & Replication to create image-level backups, follow the instructions provided in section Performing VM Backup (step 5), Performing SQL Backup (step 5) or Performing Spanner Backup (step 5).
   - To modify the schedule configured for the policy, follow the instructions provided in section Performing VM Backup (step 6), Performing SQL Backup (step 6) or Performing Spanner Backup (step 6).
   - [Applies only to VM backup policies] To assign labels to cloud-native snapshots, follow the instructions provided in section Performing VM Backup (step 7).
   - [Applies only to SQL backup policies] To choose whether you want to use a staging server to perform backup, follow the instructions provided in section Performing SQL Backup (step 7).
   - To configure automatic retry, health check and notification settings, follow the instructions provided in section Performing VM Backup (step 8), Performing SQL Backup (step 8) or Performing Spanner Backup (step 8).
   - At the Summary step of the wizard, review configuration information and click Finish to confirm the changes.

You will follow the same steps you followed when creating the job and can change job settings as required.



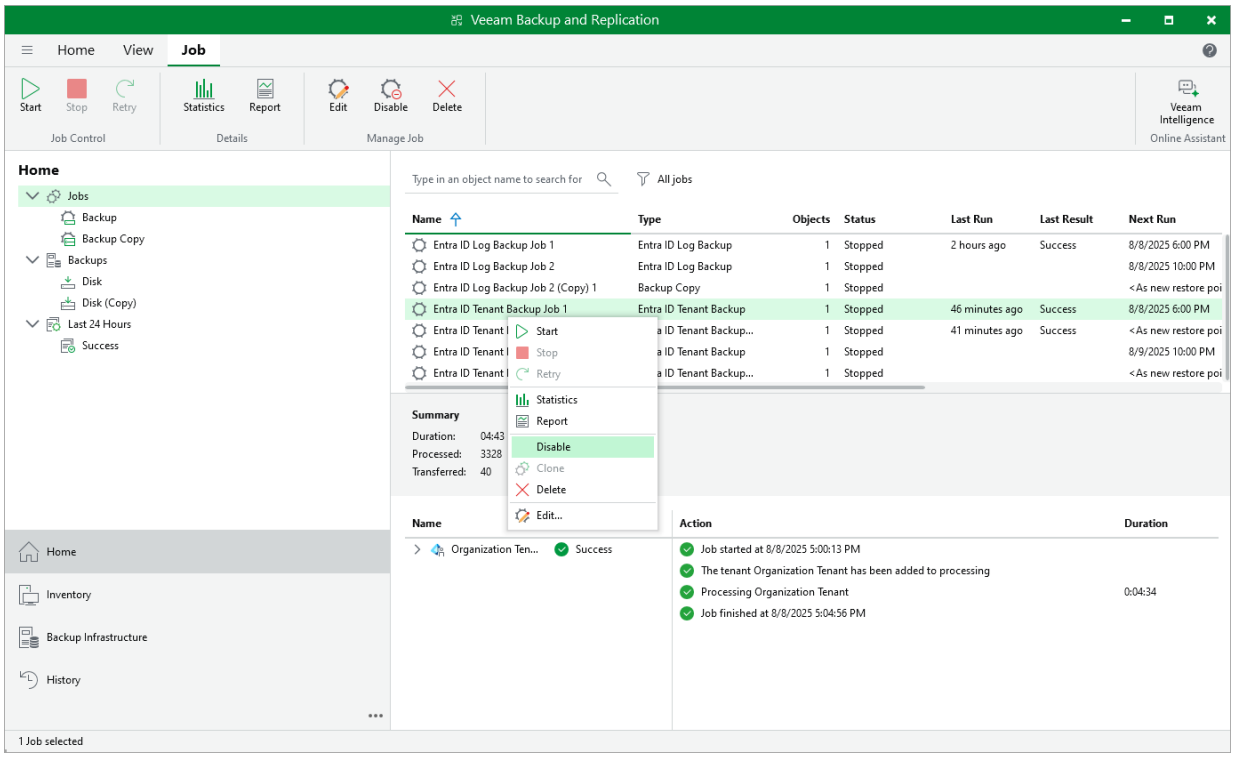
Enabling and Disabling Backup Jobs

You can disable a job with the enabled schedule.

To disable a job:

1. Open the **Home** view.
2. In the inventory pane, navigate to the **Jobs** > **Backup** node.
3. In the working area, select the job and select **Disable** on the ribbon or right-click the job and select **Disable**.

To enable a disabled job, select it in the list and click **Disable** on the ribbon once again.

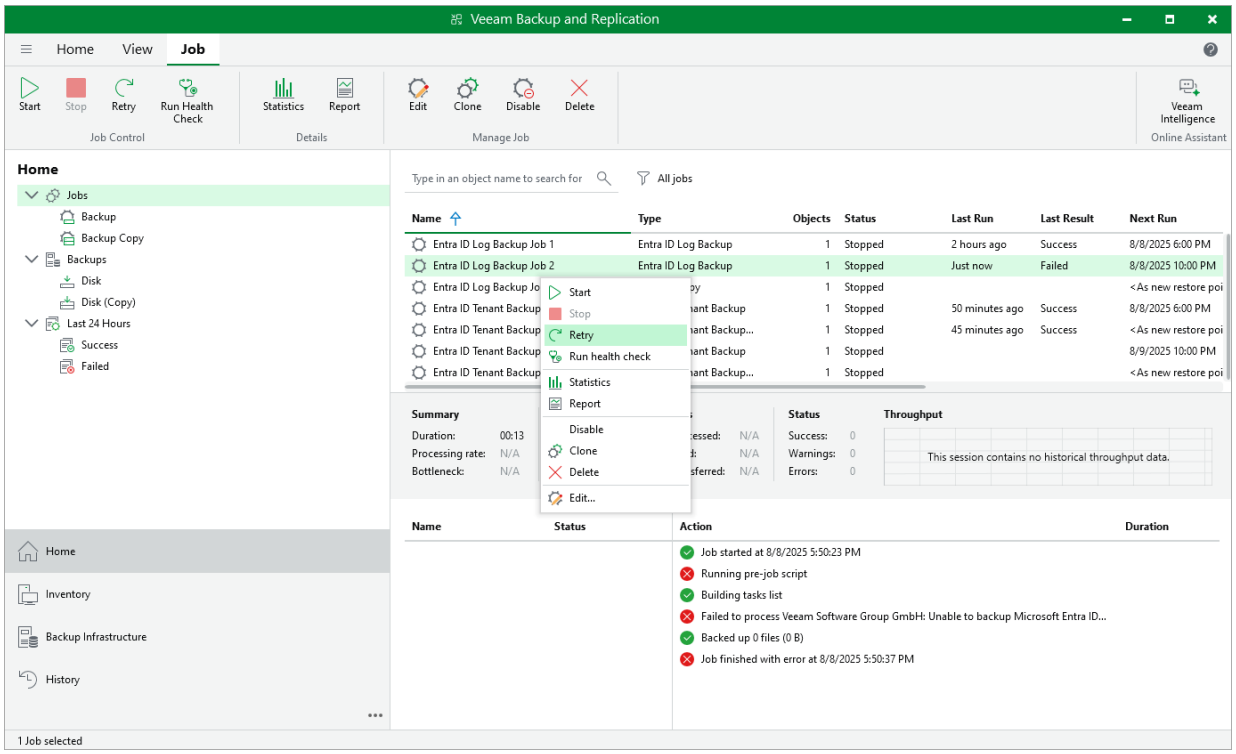


Retrying Jobs

The retry option is necessary if a job fails and you want to retry this operation again. When you perform a retry, Veeam Backup & Replication restarts the operation only for the failed workloads added to the job and does not process workloads that have been processed successfully. As a result, the retry operation takes less time than running the job for all workloads.

To perform retry:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Retry** on the ribbon. Alternatively, you can right-click the job and select **Retry**.



Cloning Log Backup Jobs

This option is available only for log backups.

You can create a new job by cloning an existing one. Job cloning allows you to create an exact copy of any job with the same job settings.

The name of the cloned job is formed by the following rule: *<job_name_clone1>*, where *job_name* is the name of the original job and *clone1* is a suffix added to the original job name. If you clone the same job again, the number in the name will be incremented, for example, *job_name_clone2*, *job_name_clone3*, and so on. To change the name of a cloned job, edit the job as described in Editing Backup Job Settings.

Considerations

When cloning a job, Veeam Backup & Replication can change some job settings so that cloned jobs do not hinder original jobs.

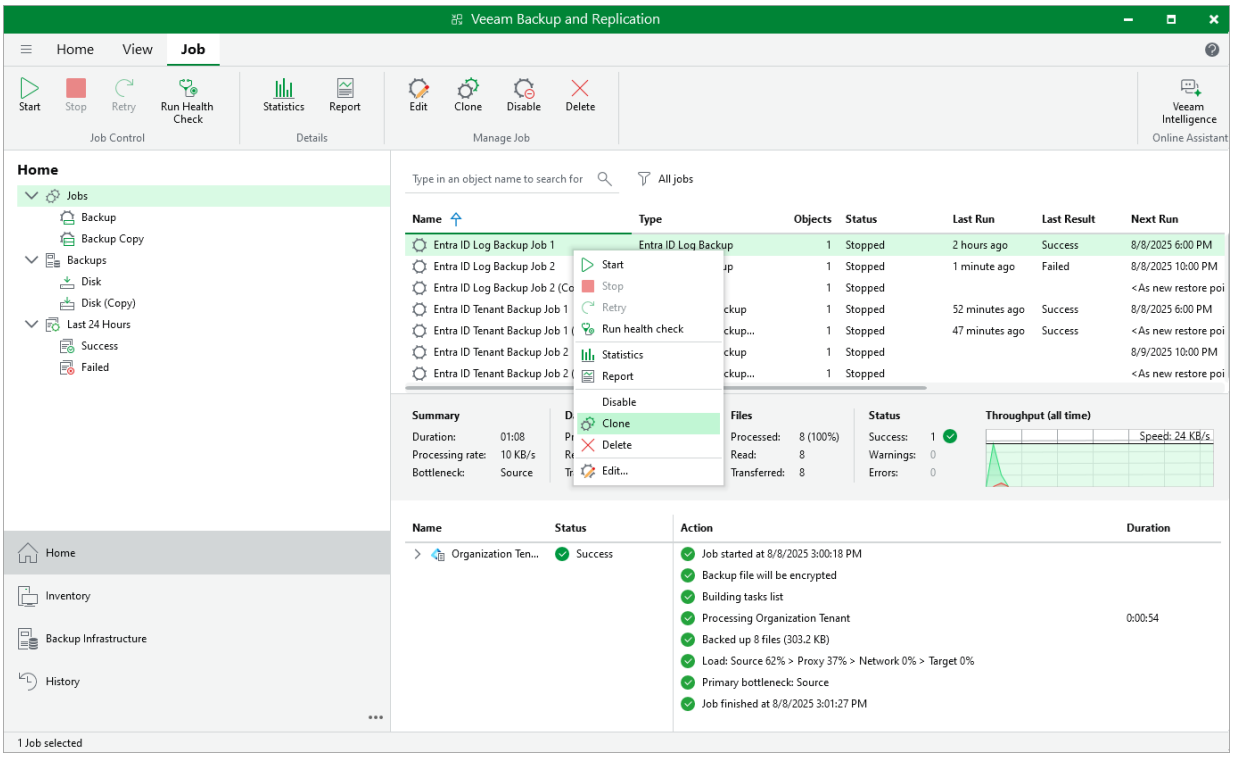
- If the original job is scheduled to run automatically, Veeam Backup & Replication disables the cloned job. To enable the cloned job, select it in the job list and click **Disable** on the ribbon or right-click the job and select **Disable**.
- If the original job is configured to use a secondary target, Veeam Backup & Replication also clones the copy job.

Cloning Job

To clone a log backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Clone** on the ribbon. Alternatively, right-click the job and select **Clone**.

After a job is cloned, you can edit all its settings, including the job name.

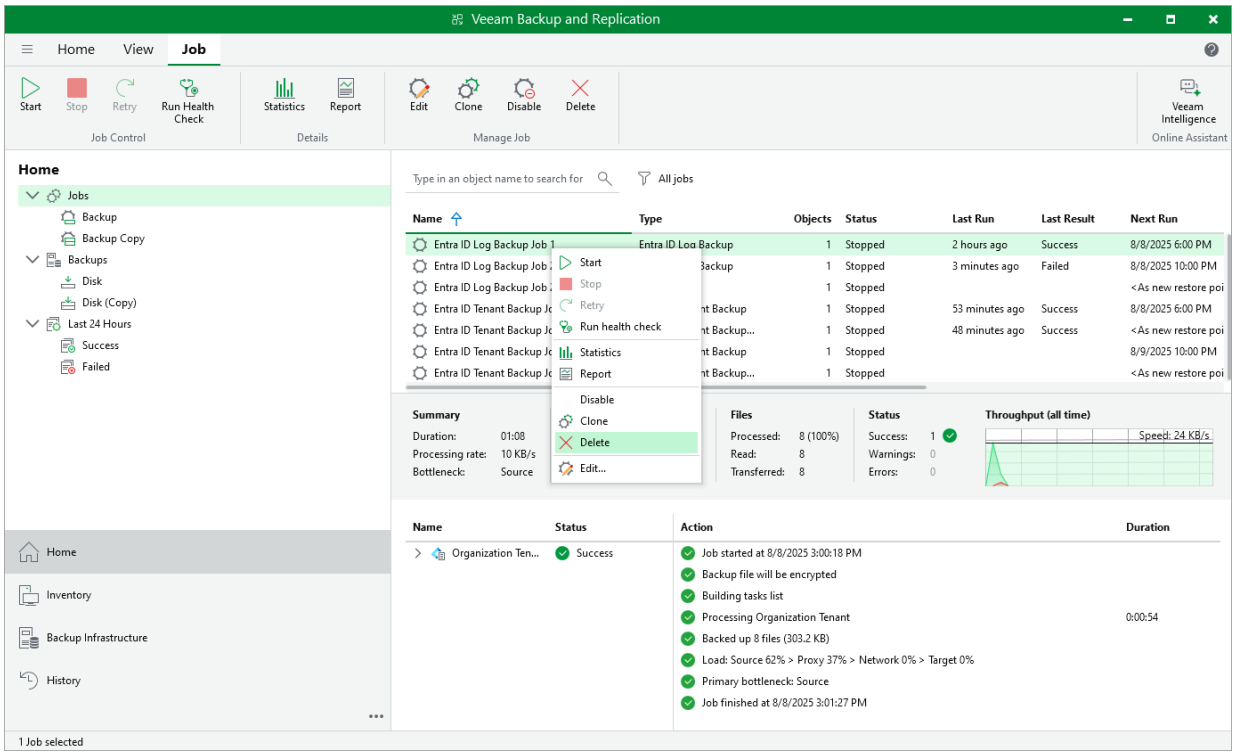


Deleting Backup Jobs

To delete a job:

1. Open the **Home** view.
2. In the inventory pane, navigate to the **Jobs** > **Backup** node.
3. In the working area, select the job and click **Delete** on the ribbon or right-click the job and select **Delete**.

After the job is deleted, the backups created by this job are displayed under the **Backups** > **Disk (Orphaned)** node.



Managing Backed-Up Data

The following operations are available for backups:

- Viewing backup properties
- Performing health check for log backups
- Copying log backups
- Removing tenant and log backups
- Retrieving tenant data from backup copies

Viewing Log Backup Properties

This section applies to log backups only.

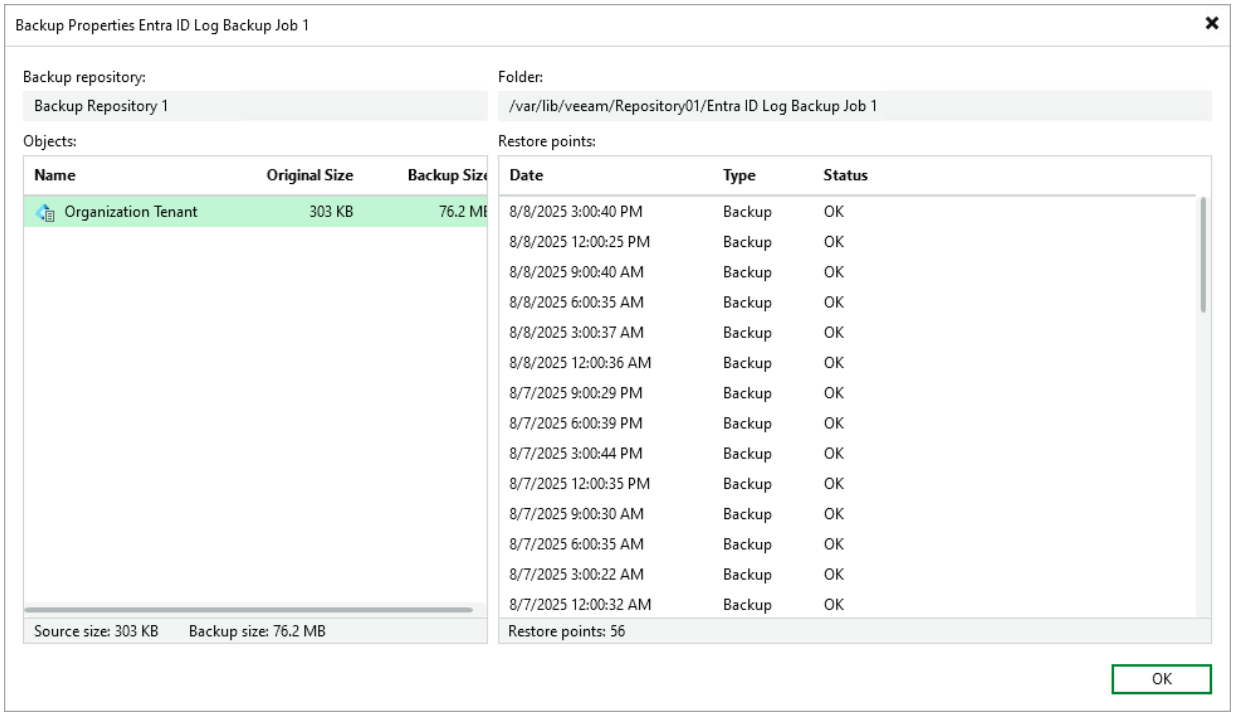
You can view summary information about the log backup. The summary information provides the following data:

- Name and path to the backup repository that stores backup files.
- Size of the backup source and the backup.
- Available restore points: date of their creation, their type and status.

  You can restore the logs from any of these points. To learn how to restore the log data, see Entra ID Log Restore.

To view summary information for backups:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the log backup and select **Properties**.
4. To see the list of available restore points, select the required tenant from the **Objects** list.



Performing Health Check for Log Backups

This section applies to log backups only.

In this section, you will learn how to perform health check and repair log backups.

Health Check for Log Backup Files

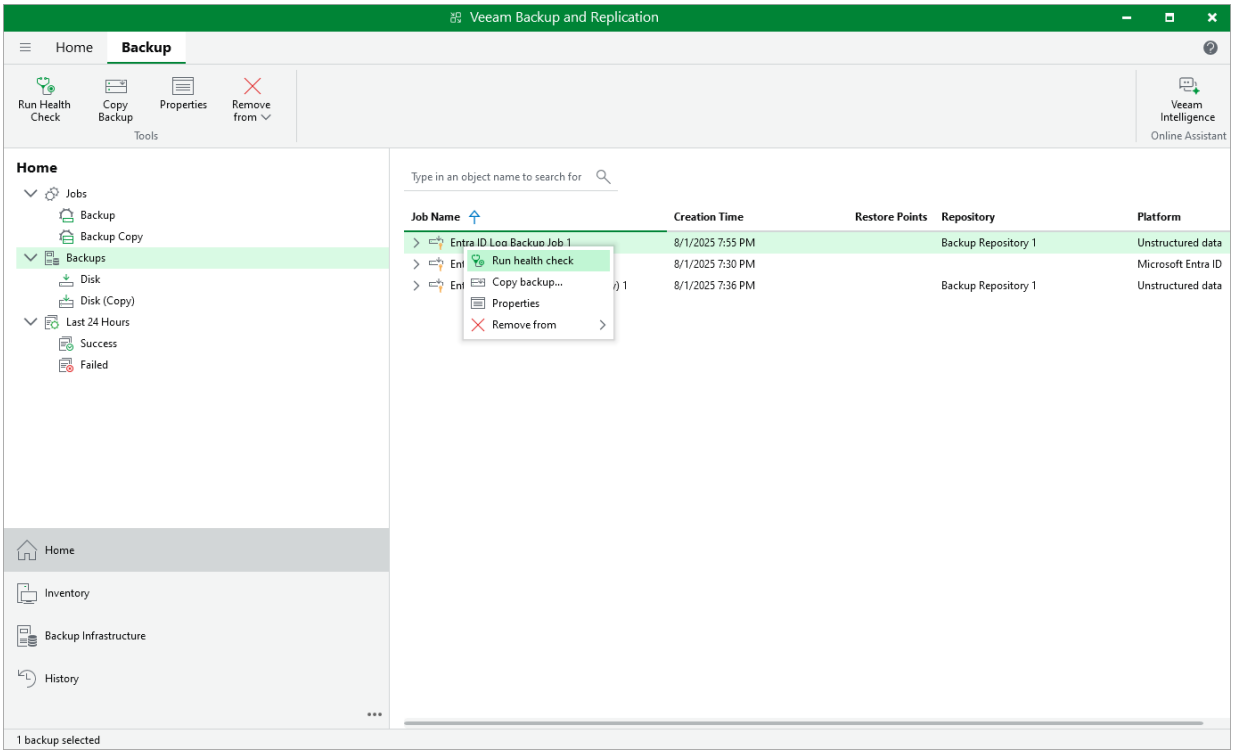
You can manually perform a health check for the backup chain. During the health check, Veeam Backup & Replication performs a cyclic redundancy check (CRC) for metadata and a hash check for data blocks in backup files to verify their integrity. The health check helps make sure that the restore point is consistent, and you will be able to restore data from this restore point.

To run the health check:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the required log backup and click **Run Health Check** on the ribbon. Alternatively, you can right-click the backup and select **Run health check**.

To run the health check periodically, you must enable the **Perform backup files health check** option in the backup job settings and define the health check schedule. By default, the health check is performed on the last Friday of every month. You can change the schedule and run the health check weekly or monthly on specific days. To learn how to configure periodic health check, see Maintenance Settings.

> **IMPORTANT**
>
> If you store your backups on public cloud object storage repositories, running the health check operations may result in constantly downloading and uploading data to and from the storage, which may lead to higher costs. To avoid this, use helper appliances configured for the repositories within the public clouds. For more information, see the Unstructured Data Backups in Object Storage Repositories section in the Veeam Backup & Replication User Guide.



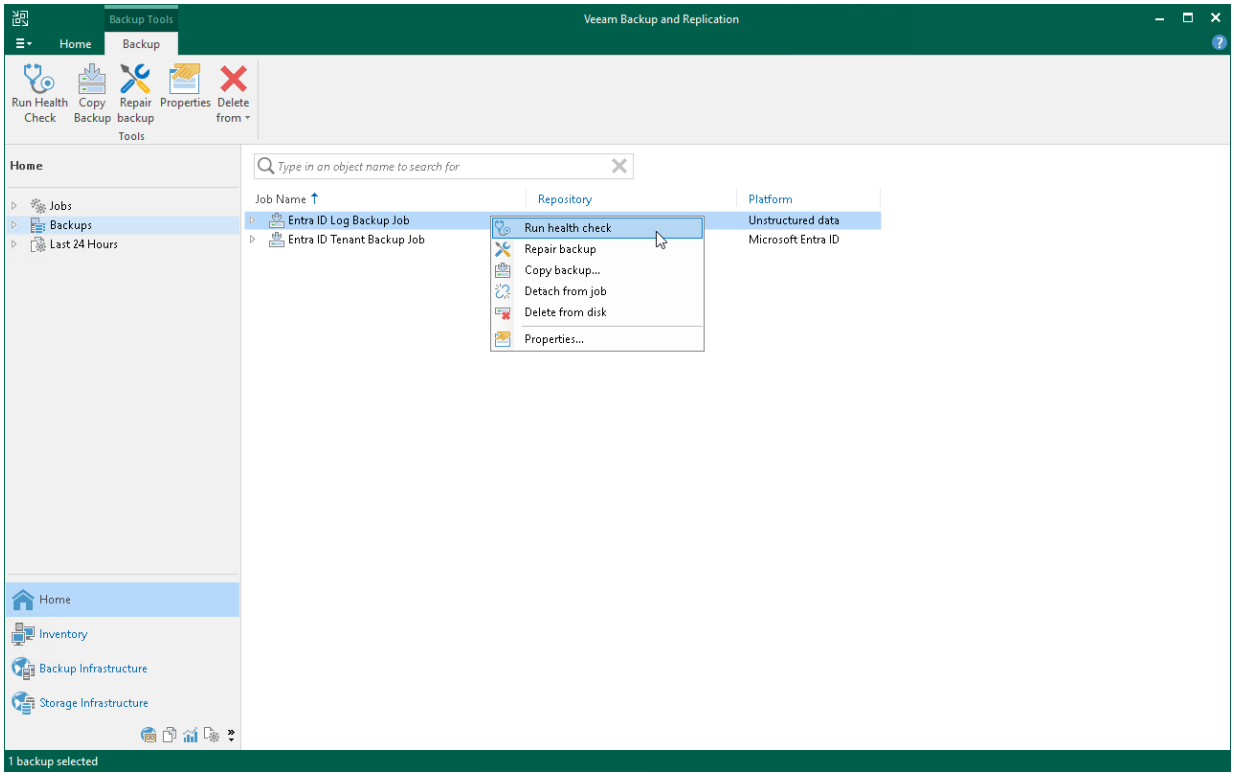
Repair of Log Backup Files

If Veeam Backup & Replication detects some inconsistency in the log backup files during the health check, you can run the backup repair procedure to fix the issues.

To run the backup repair:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.

3. In the working area, select the required log backup, click **Repair backup** on the ribbon. Alternatively, you can right-click the backup and select **Repair backup**.



Copying Log Backups

This section applies to log backups only.

Copying backups can be helpful if you want to copy audit and sign-in log backups to a repository, or local or shared folder. Veeam Backup & Replication copies the whole backup chain.

When Veeam Backup & Replication performs the copy operation, it disables the job, copies files to the target location and then enables the job. After the copy operation finishes, the copied backups are shown in a node with the **(Exported)** postfix in the inventory pane.

> **NOTE**
>
> This section is about one-time copy operation. If you want to copy backups on a schedule, configure the secondary destination on the job settings.

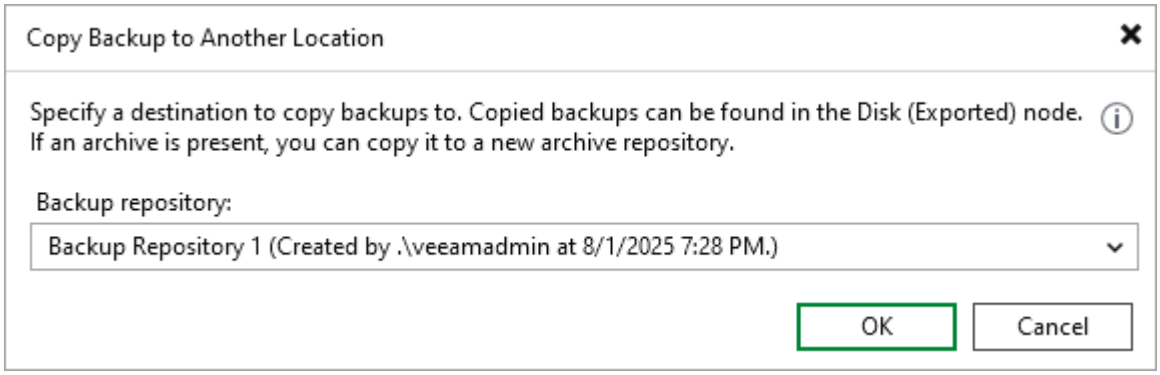
Copying Backups

To copy log backups, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** node.
3. In the working area, select the necessary job.
4. Right-click the job and select **Copy backup**. Alternatively, click **Copy Backup** on the ribbon.
5. In the **Copy Backup to Another Location** window, choose a repository to which you want to copy backups.
6. Click **OK**.

After the copy process finishes, the copied backups are shown in the **Disk (Exported)** node in the inventory pane.

> **NOTE**
>
> Consider the following:
>
> - If you copy backups from a scale-out backup repository and some backups are stored on extents in the Maintenance mode, such backups are not copied.
> - Veeam Backup & Replication copies backups only from the performance tier of the scale-out backup repository. If you want to copy data from the capacity tier, you first need to download it to the performance tier. For more information, see the Downloading Data from Capacity Tier section in the Veeam Backup & Replication User Guide.



Removing Tenant and Log Backups

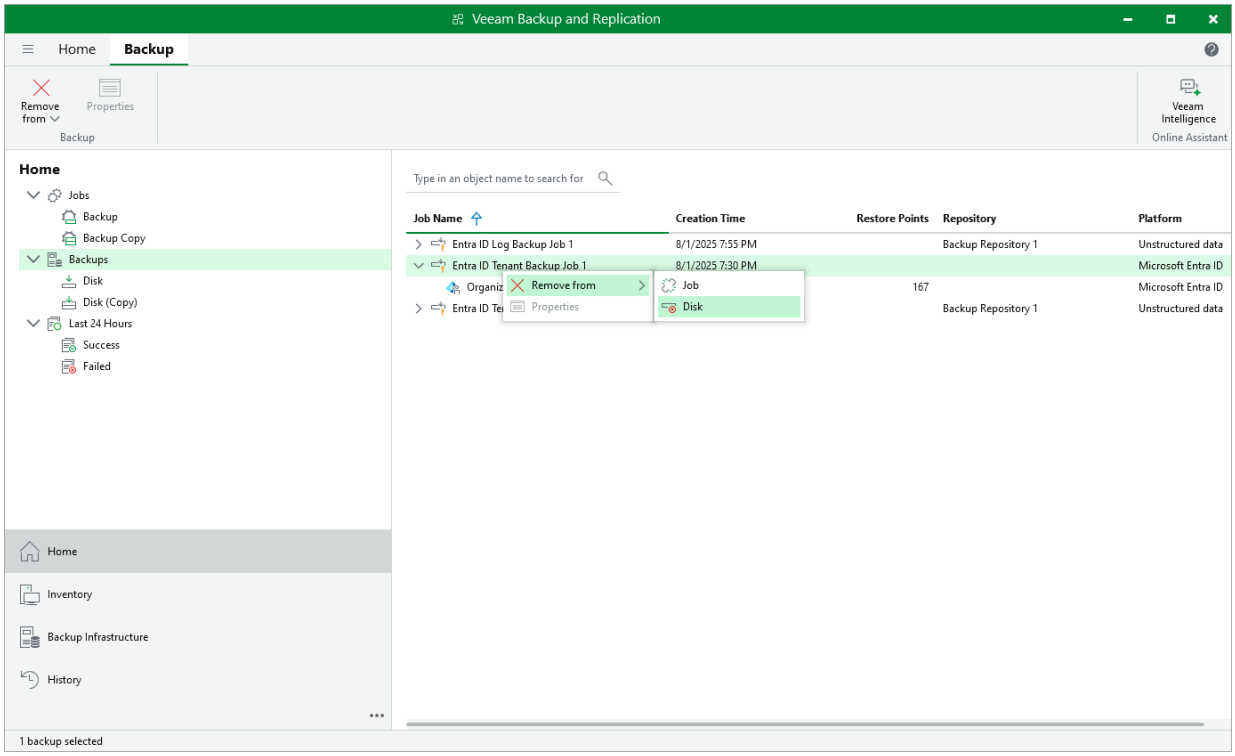
Veeam Backup for Microsoft Entra ID applies the configured retention policy settings to automatically remove backups and backup copies from backup repositories (both primary and secondary). If necessary, you can also remove the backed-up data manually.

Alternatively, you can detach backups from a backup or backup copy job — this may be helpful, for example, if you plan to reconfigure the job. In this case, backup files will remain in the target backup repository but will be treated by Veeam Backup & Replication as orphaned entities, which will be retained according to their own background retention settings. For more information, see the Veeam Backup & Replication User Guide, section Background Retention.

Removing Backups

To remove backed-up data manually, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup and click **Remove from** > **Disk** on the ribbon. Alternatively, you can right-click the backup and select **Remove from disk**.

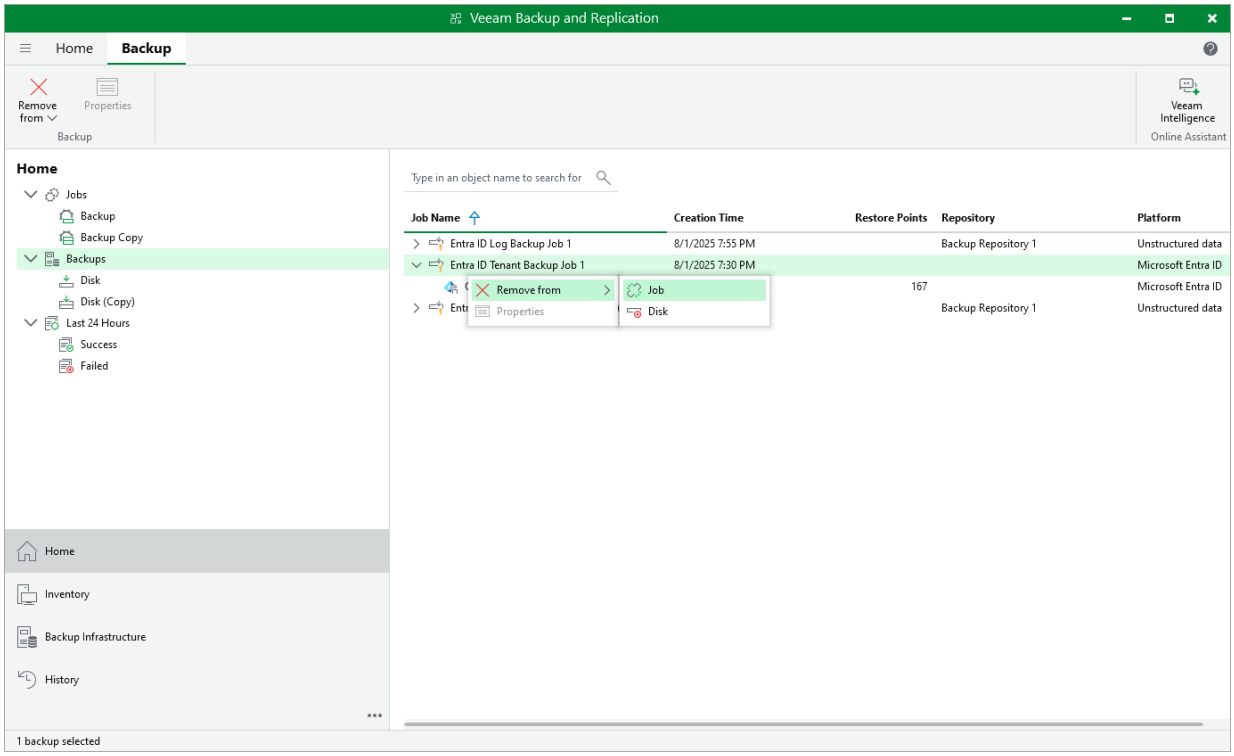


Detaching Backups

To detach backups from a backup or backup copy job:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** node.

3. In the working area, select the necessary backup and select **Remove from** > **Job** on the ribbon. Alternatively, you can right-click the backup and select **Remove from** > **Job**



IMPORTANT

Before you detach any backup or backup copy, make sure that all related jobs are disabled.

Retrieving Tenant Data From Backup Copies

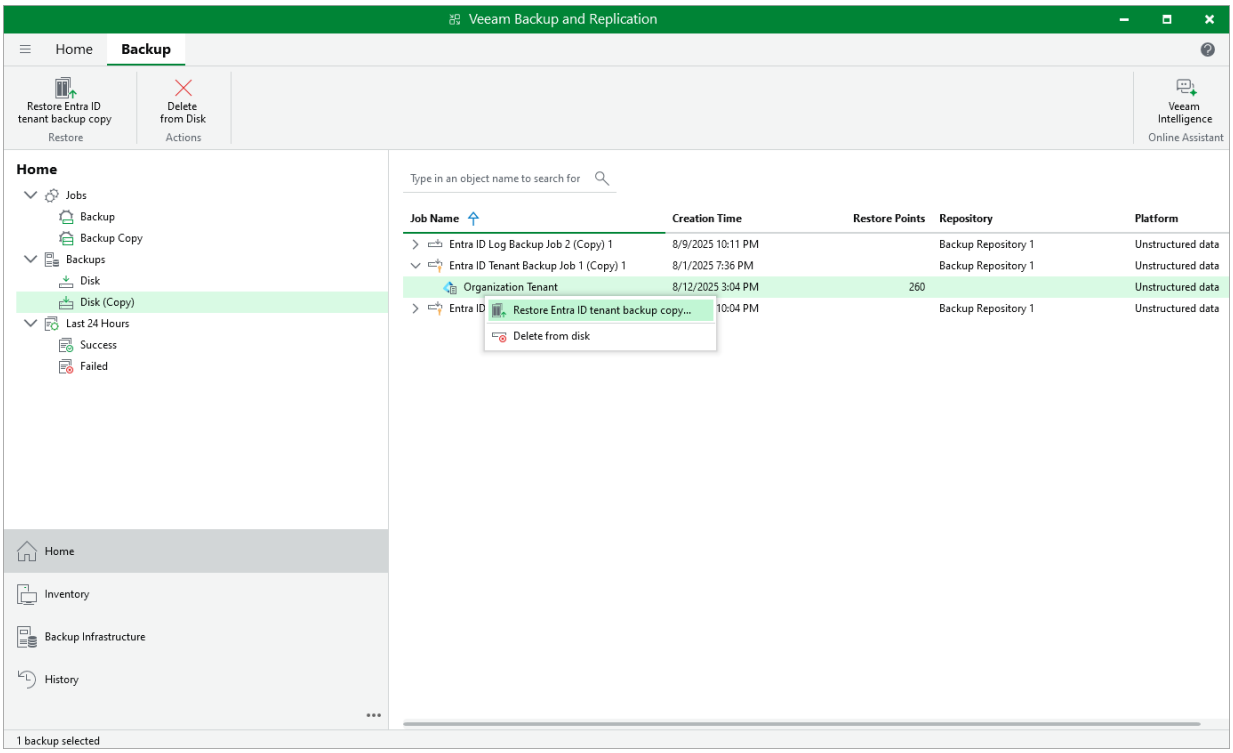
Backup copies stored in backup repositories (both primary and secondary) are not immediately accessible; if you want to restore tenant data from a backup copy, you must retrieve the data first. During the data retrieval process, Veeam Backup & Replication imports the unstructured backup copy data to the PostgreSQL database that stores Entra ID backups. The imported backups are displayed in the **Home** view under the **Disk (Imported)** node.

To retrieve tenant data from a backup copy, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view and navigate to **Backups** > **Disk (Copy)**.
2. In the working area, expand the backup job that protects the Microsoft Entra ID tenant whose backup copy you want to retrieve, select the tenant and click **Restore Entra ID tenant backup copy** on the ribbon.

   Alternatively, you can right-click the tenant and select **Restore Entra ID tenant backup copy**.
3. In the **Entra ID Tenant Backup Copy Restore** window, choose a restore point that will be used to retrieve the data, specify a reason for performing the operation, and wait for the process to complete.

As soon as Veeam Backup & Replication retrieves the tenant data, you will be able to use the imported backup to perform tenant restore.



Performing Restore

Entra ID offers the following restore operations:

- Tenant restore — restore tenant items and their properties.
- Tenant activity log restore — restore audit and sign-in logs.

You can restore tenant data to the most recent state or to any available restore point.

Tenant Restore

In case a disaster strikes, you can use backups created by Veeam Backup for Microsoft Entra ID to restore the following tenant items and their properties: Microsoft Entra users, groups, roles, administrative units, applications, service principals and conditional access policies. Veeam Backup for Microsoft Entra ID allows you to restore tenant data to the original location only.

> **IMPORTANT**
>
> To restore tenant data from a backup copy that is stored in a secondary backup repository, you must retrieve the copied data first.

To restore data of a protected Microsoft Entra tenant, do the following:

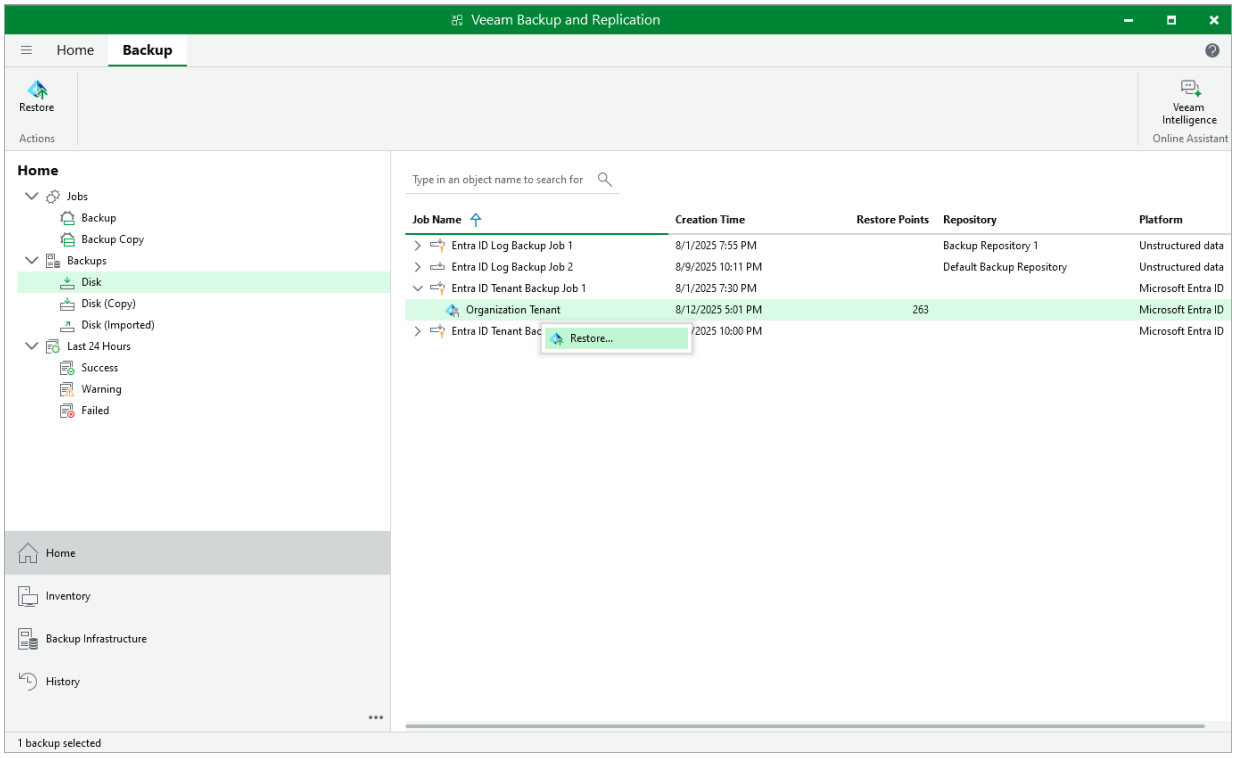
1. Launch the Microsoft Entra ID Tenant Restore wizard.
2. Choose items to restore.
3. Select a restore point.
4. Connect to Microsoft Azure.
5. Specify restore options.
6. Specify a restore reason.
7. Finish working with the wizard.

Step 1. Launch Microsoft Entra ID Tenant Restore Wizard

To launch the **Microsoft Entra ID Tenant Restore** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view and navigate to **Backups**.
2. In the working area, expand the backup job that protects the Microsoft Entra tenant whose data you want to restore, select the tenant and click **Restore** on the ribbon.

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



Step 2. Choose Items to Restore

In the **Microsoft Entra ID Tenant Restore** wizard, switch to the necessary tab and then do either of the following:

- If you want to restore an item, select this item and click **Restore** > **Full restore**. Alternatively, right-click the item and select **Restore** > **Full restore**.

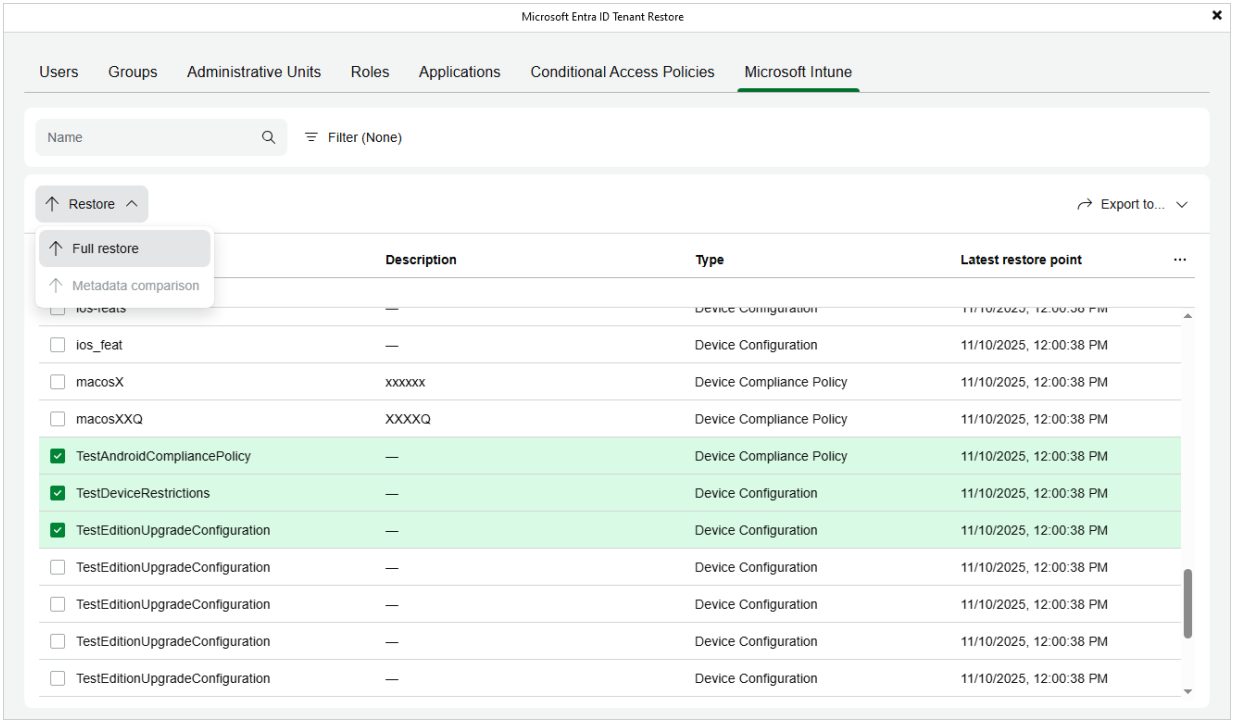
  Veeam Backup for Microsoft Entra ID allows you to restore multiple items at a time. However, keep in mind that your selection is discarded when you switch between tabs since restoring different item types simultaneously is not supported.

- If you want to restore properties of an item, select this item and click **Restore** > **Metadata comparison**.

  Veeam Backup for Microsoft Entra ID allows you to restore multiple properties at a time. However, keep in mind that restoring properties of different items simultaneously is not supported.

TIPS

- You can narrow down the list of items available on the selected tab by applying a number of filters. To do that, either use the search field or click **Filter** (if available). You can use SQL wildcard characters *%* and _ for item names search.
- You can export the list of filtered items to further use it for any internal purposes or if you decide to add items to the restore scope at step 3. To do that, click **Export to** and select the necessary format. Veeam Backup & Replication will save the file with the exported data to the default download directory on the local machine.



Step 3. Select Restore Points

At the first step of the wizard, choose a restore point that will be used to restore the selected items or properties. The actions that you can perform with restore points depend on whether you have selected the **Full restore** or **Metadata comparison** option when proceeding with the wizard.

Restoring Items

[This step applies only if you have selected the **Full restore** option when proceeding with the wizard]

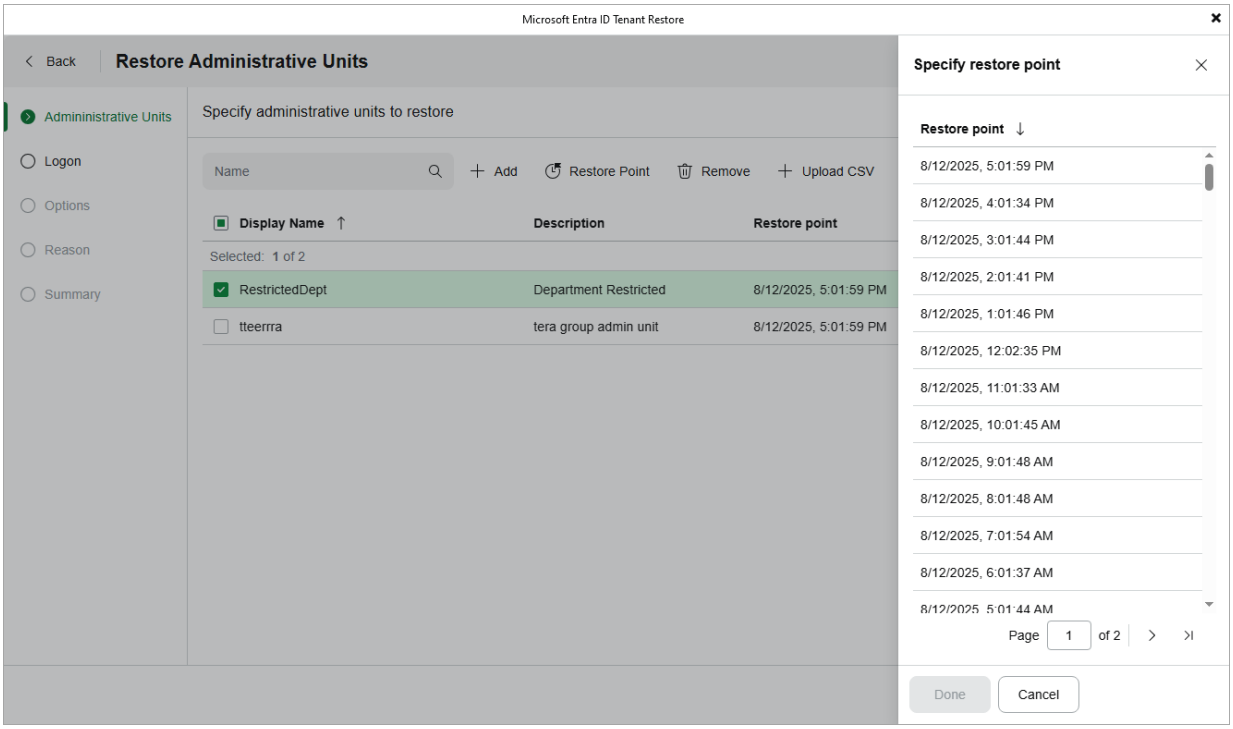
By default, Veeam Backup & Replication uses the most recent valid restore point when restoring an item. However, you can restore the backed-up data to an earlier state. To do that:

1. Select the item and click **Restore Point**.
2. In the **Specify restore point** window, choose the necessary restore point and click **Done**.

   Veeam Backup & Replication allows you to choose one restore point for multiple items. However, if the chosen restore point does not exist for any of the selected items, Veeam Backup for Microsoft Entra ID will display a warning notifying that the requested value was not found and will use the closest available restore point for these items instead.

TIP

If you want to adjust the restore scope, you can click **Upload CSV** to import the list if items that you have previously exported at step 2. Keep in mind that you will have to manually modify the .CSV file to remove all columns except *Id* (or *Id* and *DisplayName* for users) before uploading the file — otherwise, Veeam Backup & Replication will not be able to process the file properly.



Restoring Item Properties

[This step applies only if you have selected the **Metadata comparison** option when proceeding with the wizard]

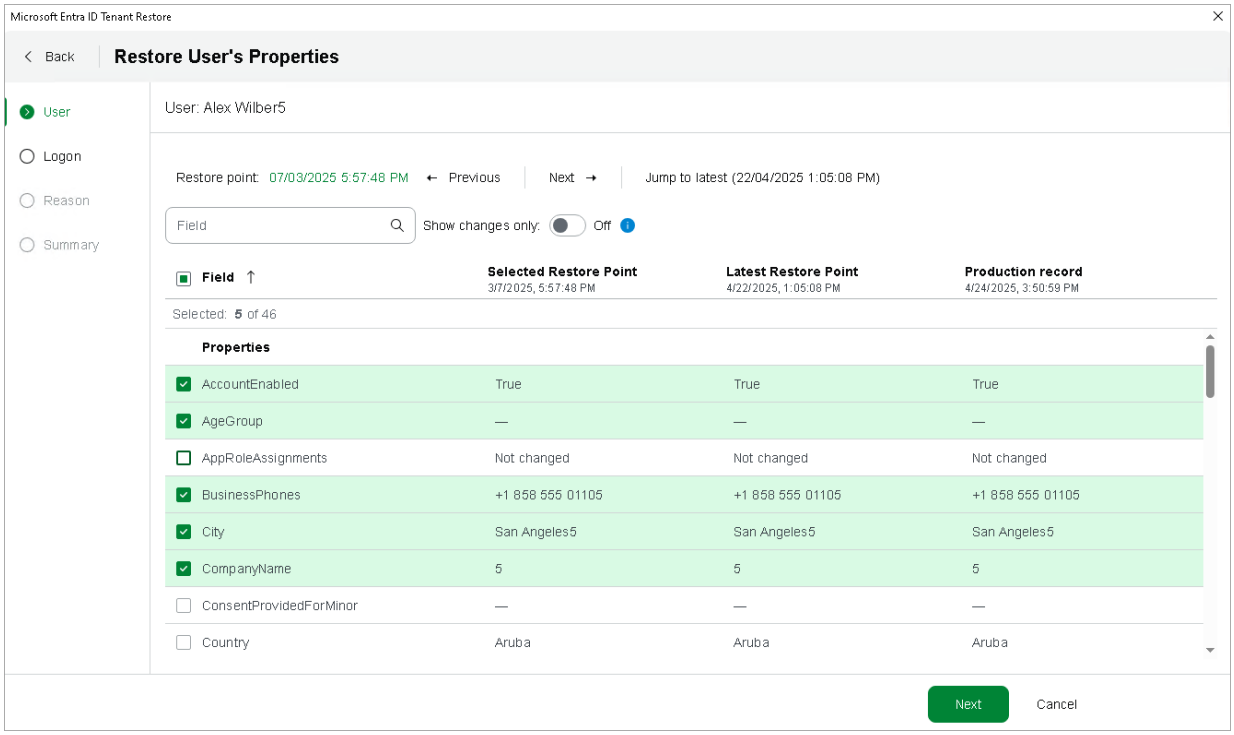
By default, Veeam Backup & Replication uses the second most recent restore point when restoring item properties. However, you can restore the backed-up data to an earlier or a later state. To do that:

1. Click the link in the **Restore point** field.
2. Choose the necessary restore point in the calendar.

   To help you choose a restore point, Veeam Backup for Microsoft Entra ID provides a comparison between property values contained in the selected restore point, in the most recent restore point and in the current Microsoft Entra ID production environment.

TIPS

- By default, the comparison list includes only those properties whose values changed since any of the restore points was created. To view the full list of properties, set the **Show changes only** toggle to *Off*.
- If you decide to choose the most recent restore point, you can click **Jump to latest**. Alternatively, you can click **Previous** and **Next** to switch between restore points.

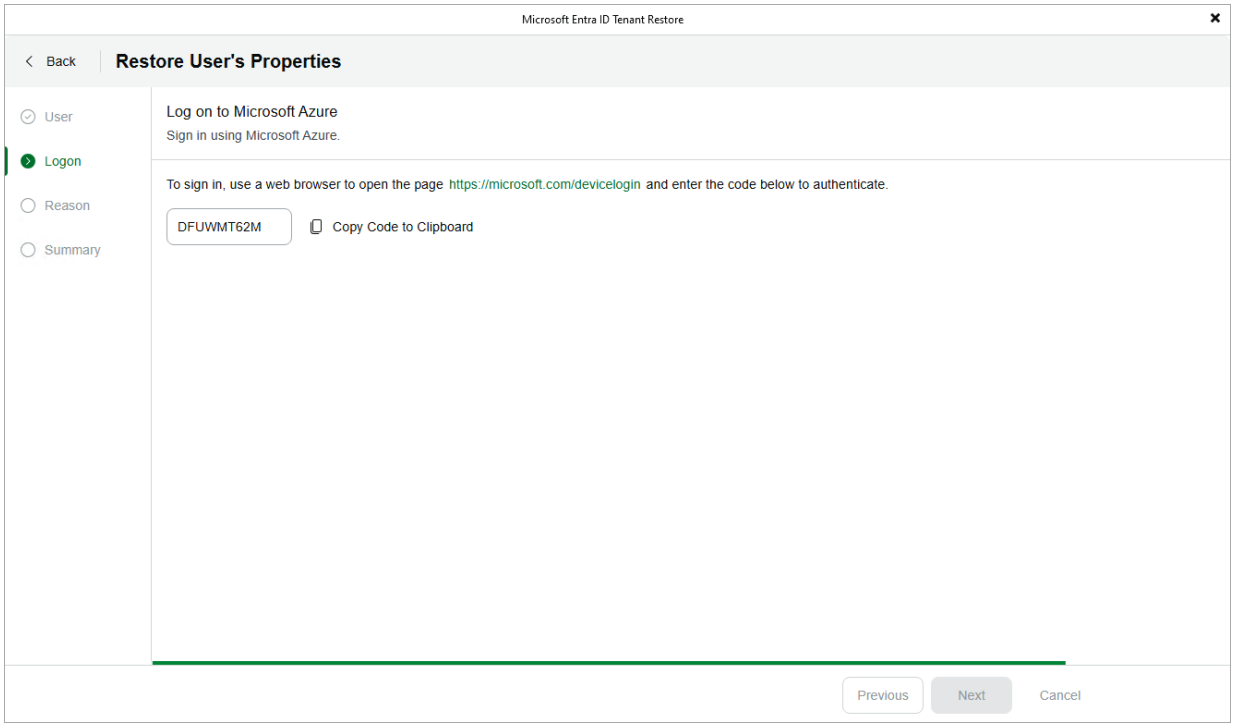


Step 4. Connect to Microsoft Azure

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

2. Copy the authentication code to the clipboard.
4. Open the **https://microsoft.com/devicelogin** link.
5. On the Microsoft Azure device authentication page, do the following:
   a. Paste the code that you have copied and click **Next**.
   b. Specify the name of a Microsoft Entra ID user account associated with the tenant whose data you want to restore. The name of the account must be specified in the *username@domain* format.

      Keep in mind that the account must have all the permissions required to perform operations with the selected items. For more information on the required permissions, see Permissions.
   c. Wait for the authentication process to complete, check whether any errors occurred, and then close the Microsoft Azure device authentication page.
5. Back to the **Microsoft Entra ID Tenant Restore** wizard, click **Next**.



Step 5. Specify Restore Options

[This step applies only if you have selected the **Full restore** option when proceeding with the wizard]

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

- Choose a restore mode
- Provide passwords for users
- Configure advanced options

Choosing Restore Mode

When processing an item added to the restore scope, Veeam Backup for Microsoft Entra ID checks whether the item still exists in the production environment:

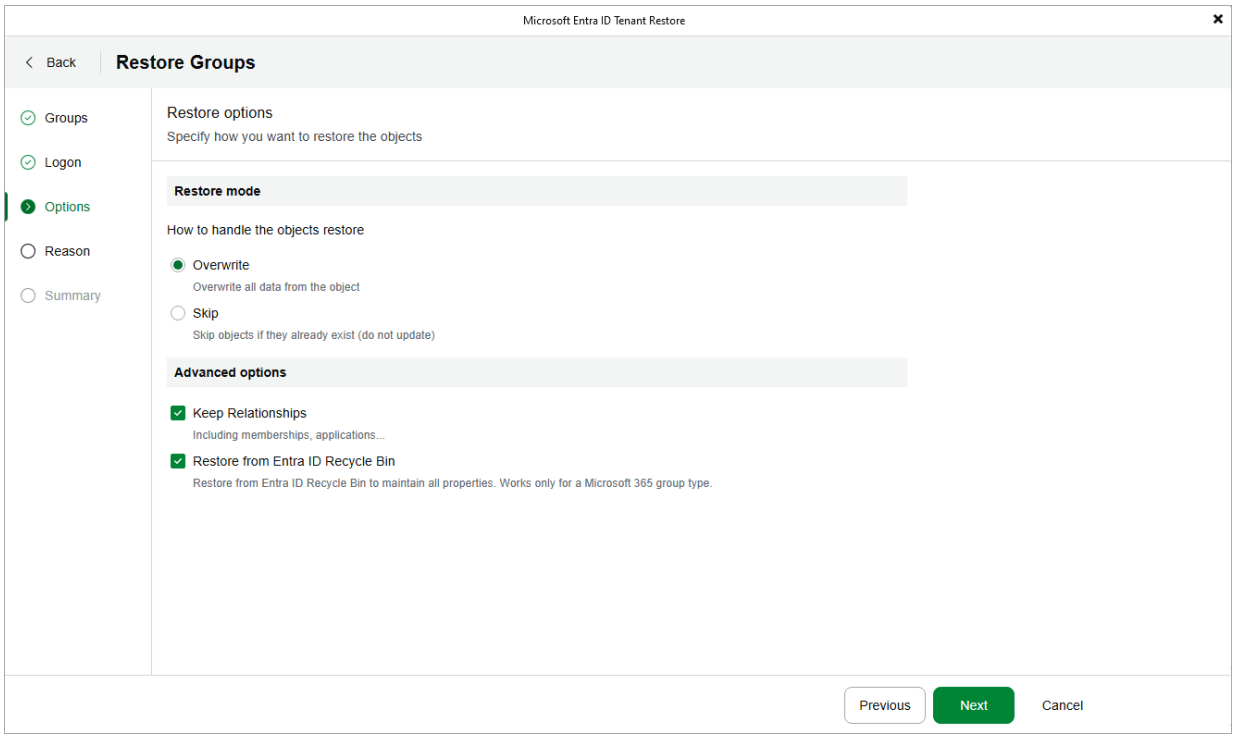
- If the item still exists in the environment, Veeam Backup for Microsoft Entra ID also checks whether the unique identifier (object ID) of this item matches the identifier of the backed-up item. If it does, the product overwrites the original item data (excluding metadata, such as item creation date).

  To change this behavior, select the **Skip** option in the **Restore mode** section of the **Options** step of the wizard. In this case, the product will exclude this item from the restore process and then proceed to another item.

- [This option is applicable only for the following item types: users, groups and applications] If the item exists in the environment but it is in the Entra ID Recycle Bin, the product restores this item from the Recycle Bin.

  To change this behavior, clear the **Restore from Entra ID Recycle Bin** check box in the **Advanced options** section of the **Options** step of the wizard. In this case, the product will restore this item using the backed-up data. For more information, see Configuring Advanced Options.

- If the item does not exist in the environment, Veeam Backup for Microsoft Entra ID restores this item using the backed-up data.



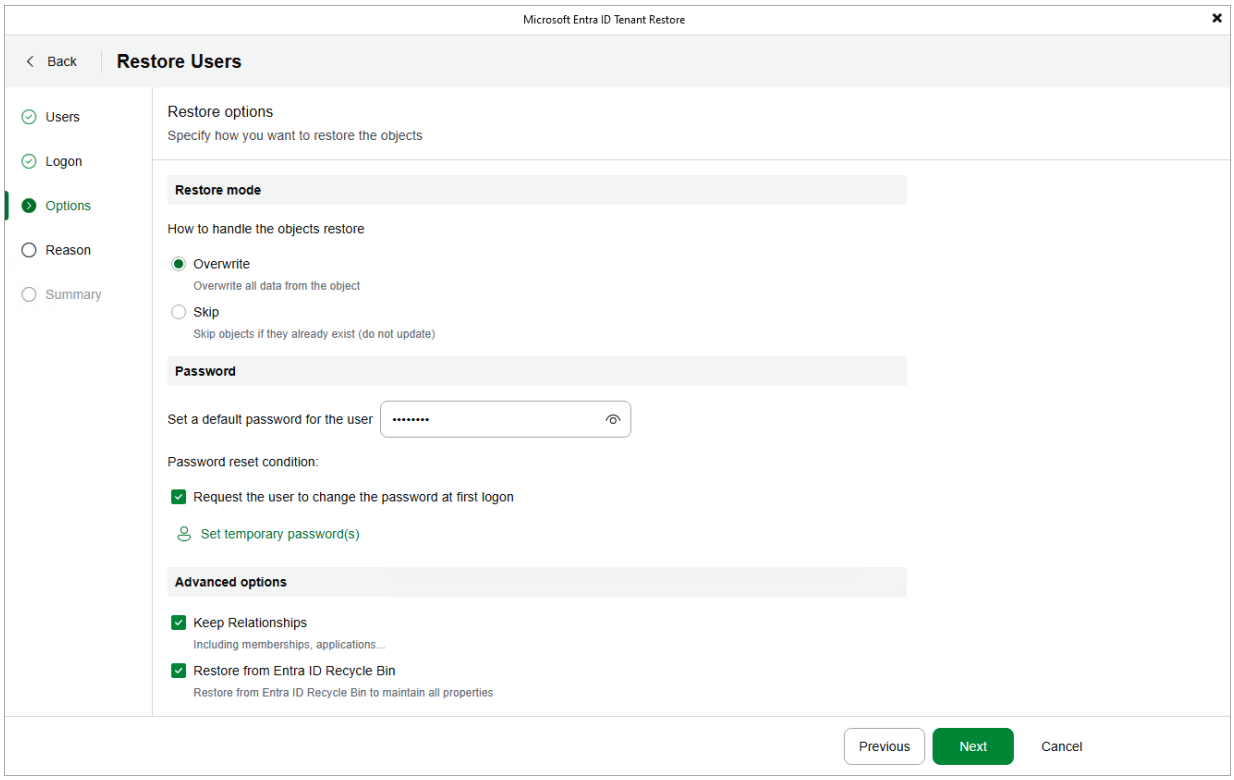
Setting User Passwords

[This step applies only if you have chosen to restore users when proceeding with the wizard]

When processing a user added to the restore scope, Veeam Backup for Microsoft Entra ID resets their password. For the restored user to be able to authenticate in the Microsoft Entra ID portal, a new password must be created for this user — to do that, provide the password in the **Password** section of the **Options** step of the wizard. The password must meet the length restrictions and complexity requirements listed in Microsoft Docs.

By default, Veeam Backup for Microsoft Entra ID will apply the provided password to all users in the restore scope. To change this behavior, click **Set temporary password(s)** and specify a new password for each user — to do that, you can either specify the passwords manually or click **Autogenerate password(s)** to create them automatically. You can then click **Export** to save the new passwords as a single .CSV file to the default download directory on the local machine.

> **TIP**
>
> For security reasons, all new passwords are considered as temporary and the restored users are prompted to reset these passwords as soon as they log in to the Microsoft Entra ID portal for the first time. To change this behavior, clear the **Request the user to change the password at first logon** check box.



Configuring Advanced Options

In the **Advanced options** section, choose whether you want to restore not only the processed items themselves but also their relationships. Additionally, you can instruct Veeam Backup for Microsoft Entra ID to use data temporarily stored in the Entra ID Recycle Bin to perform the restore operation.

Restoring Item Relationships

When processing an item added to the restore scope, Veeam Backup for Microsoft Entra ID restores the list of relationships that the original item had when the selected restore point was created. To change this behavior, clear the **Keep Relationships** check box — in this case, the product will restore this item without preserving its relationships.

Keep in mind that Veeam Backup for Microsoft Entra ID restores only those relationships associated with items that still exist in the production environment. Also, the list of relationships that Veeam Backup for Microsoft Entra ID can restore depends on the restore scope:

Items	Relationships
Users	• Role assignments • Group memberships • Group ownerships • Administrative unit memberships • Application ownerships • Assignments to managers • Assignments to direct reports
Groups	• Role assignments • Group memberships • Administrative unit memberships • User memberships • User ownerships
Administrative units	• Role assignments • Group memberships • User memberships
Roles	• Assignments to groups • Assignments to users
Applications	• Ownerships
Service principals	• Ownerships • User memberships • Group memberships • Application representations

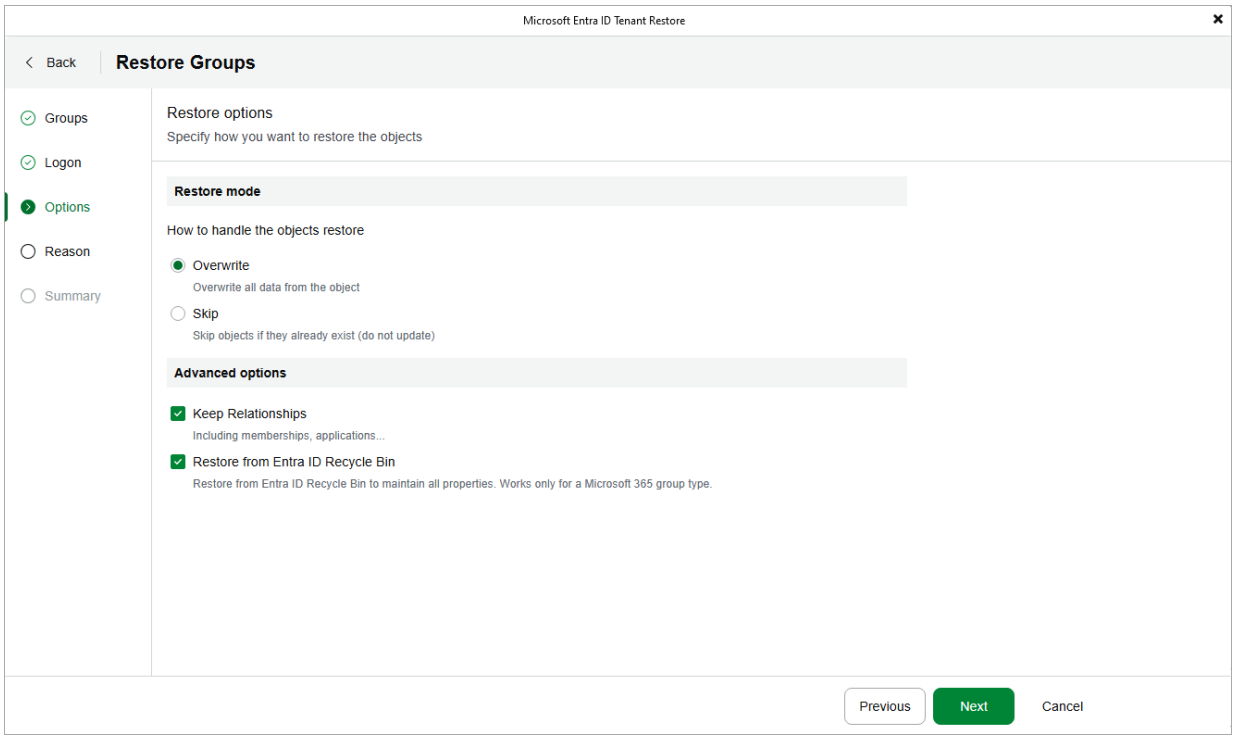
NOTE

Restoring item relationships is not supported for Conditional Access policies.

Restoring from Entra ID Recycle Bin

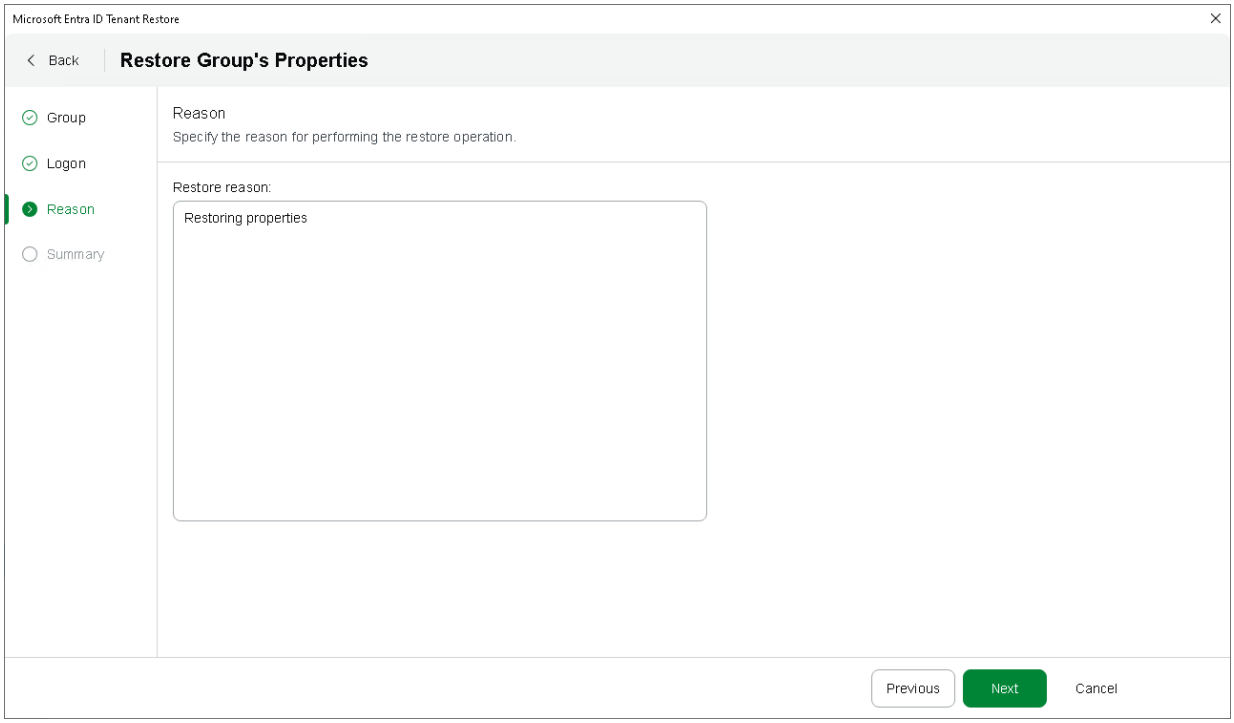
When restoring an item that still exists in the production environment, Veeam Backup for Microsoft Entra ID checks whether this item is stored in the Entra ID Recycle Bin. If the item is detected both in the Recycle Bin and in the backup, the product restores the item from the Recycle Bin and preserves its object ID by default. To change this behavior, clear the **Restore from Entra ID Recycle Bin** check box — in this case, the product will restore the item using the backed-up data and will assign a new object ID to it.

To learn how Microsoft Entra ID retains data in the Recycle Bin, see Microsoft Docs.



Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring tenant data. This information will be saved to the session history, and you will be able to reference it later.

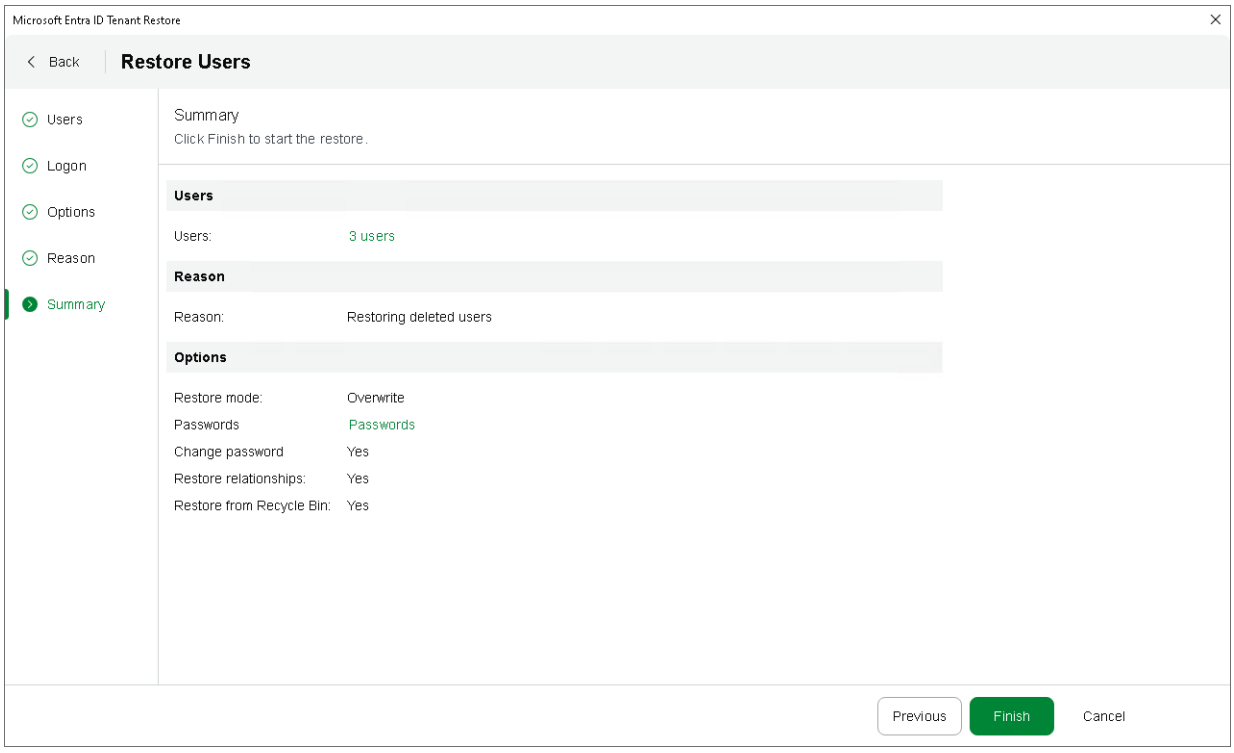


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review the summary information and click **Finish**.

If you have chosen to restore users at step 2, you can export all the passwords created for these users at step 5 as a single .CSV file. To do that, click **Passwords** — Veeam Backup & Replication will save the file with the exported data to the default download directory on the local machine.

> **IMPORTANT**
>
> As soon as you click **Finish**, Veeam Backup for Microsoft Entra ID will check whether the provided passwords meet the Microsoft Entra ID requirements. If a password does not comply with the length restrictions or complexity requirements, Veeam Backup for Microsoft Entra ID will check whether the user with the same object ID still exists in the Microsoft Entra ID production environment and will do either of the following:
>
> - If the user still exists in the environment, the product will overwrite the new password. In this case, the user will be able to authenticate in the Microsoft Entra ID portal using the password from the backed-up password profile.
> - If the user exists in the environment but it is in the Entra ID Recycle Bin, the product will ignore the new password. In this case, the user will be able to authenticate in the Microsoft Entra ID portal using their current password.
> - If the user does not exist in the environment, the product will terminate the restore operation.



Log Restore

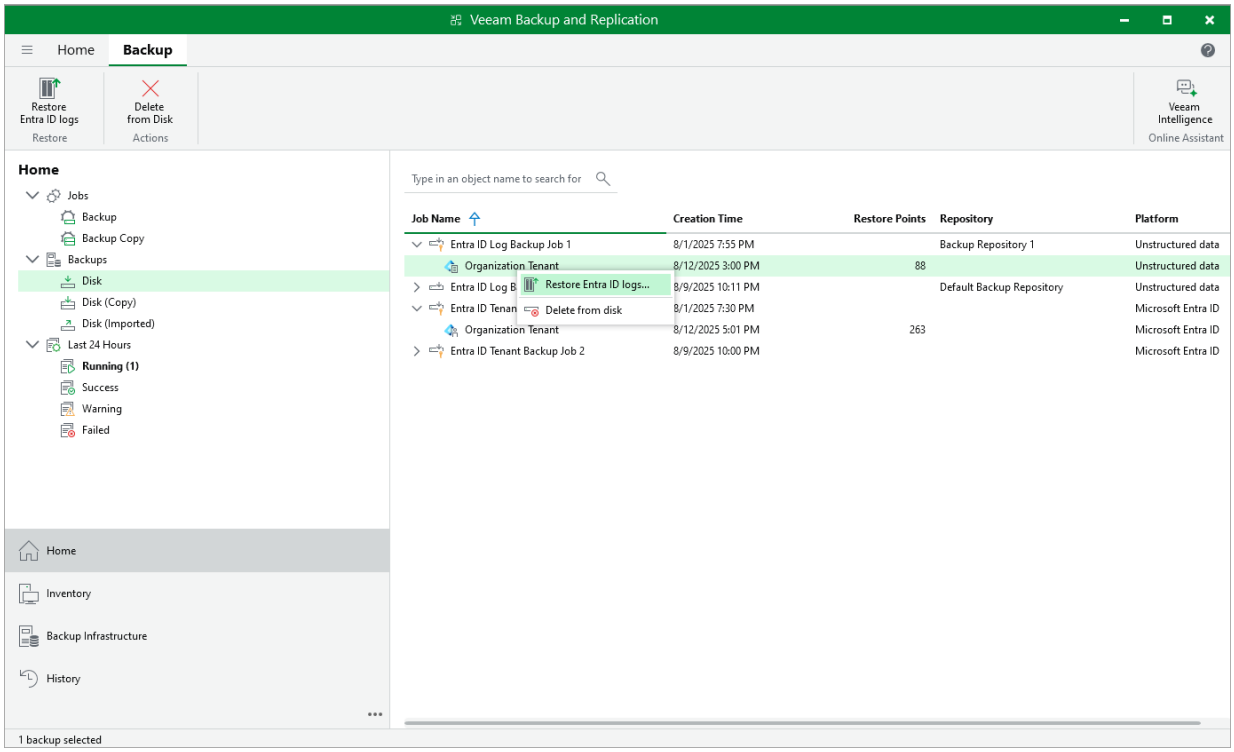
Entra ID log restore allows restoring folders containing log files or individual log files.

To restore folders with audit and sign-in logs or individual log files, use the **Microsoft Entra ID Audit Restore** wizard.

Step 1. Launch Microsoft Entra ID Audit Restore Wizard

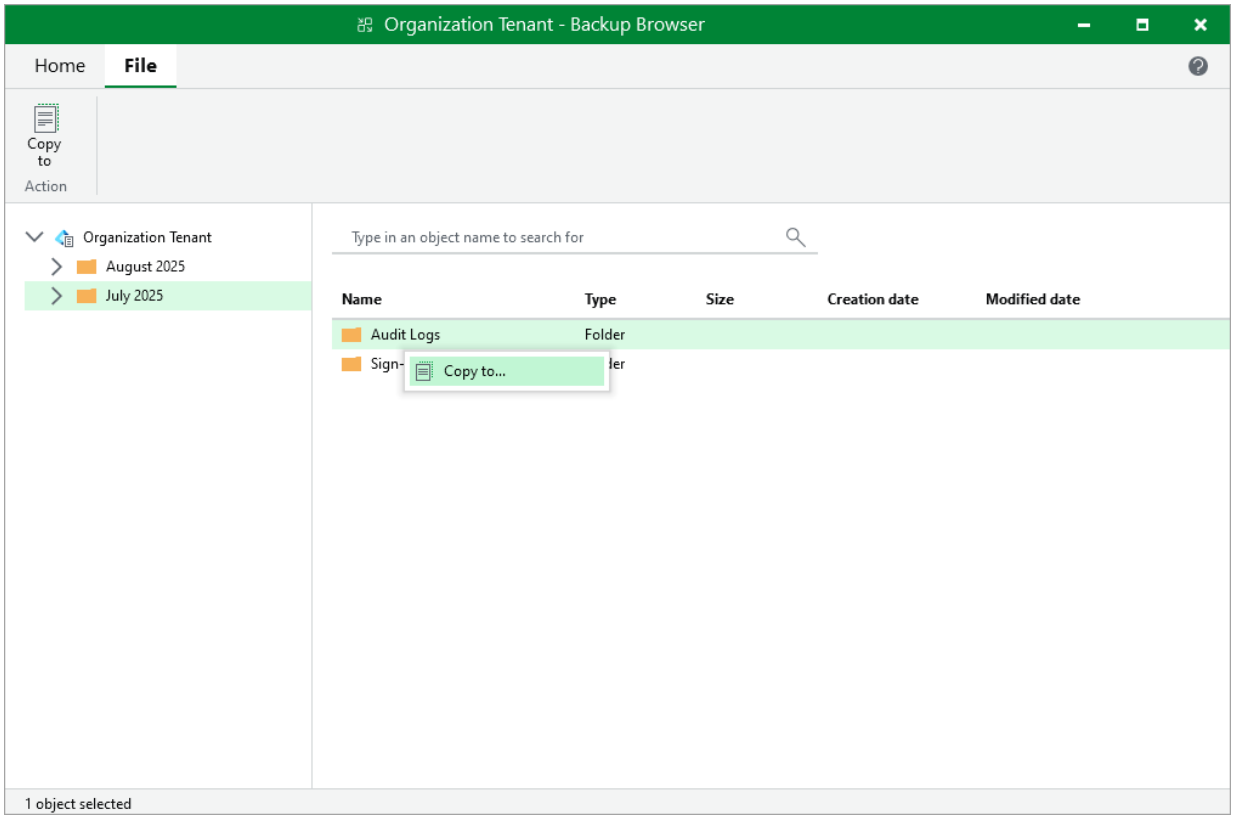
To launch the restore wizard, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** > **Disk** node.
3. In the working area, expand the backup job that protects the logs that you want to restore.
4. Select the tenant whose logs are protected and click **Restore Entra ID Logs Restore** on the ribbon. Alternatively, you can right-click the tenant and select **Restore Entra ID logs**.



Step 2. Select Files and Folders to Restore

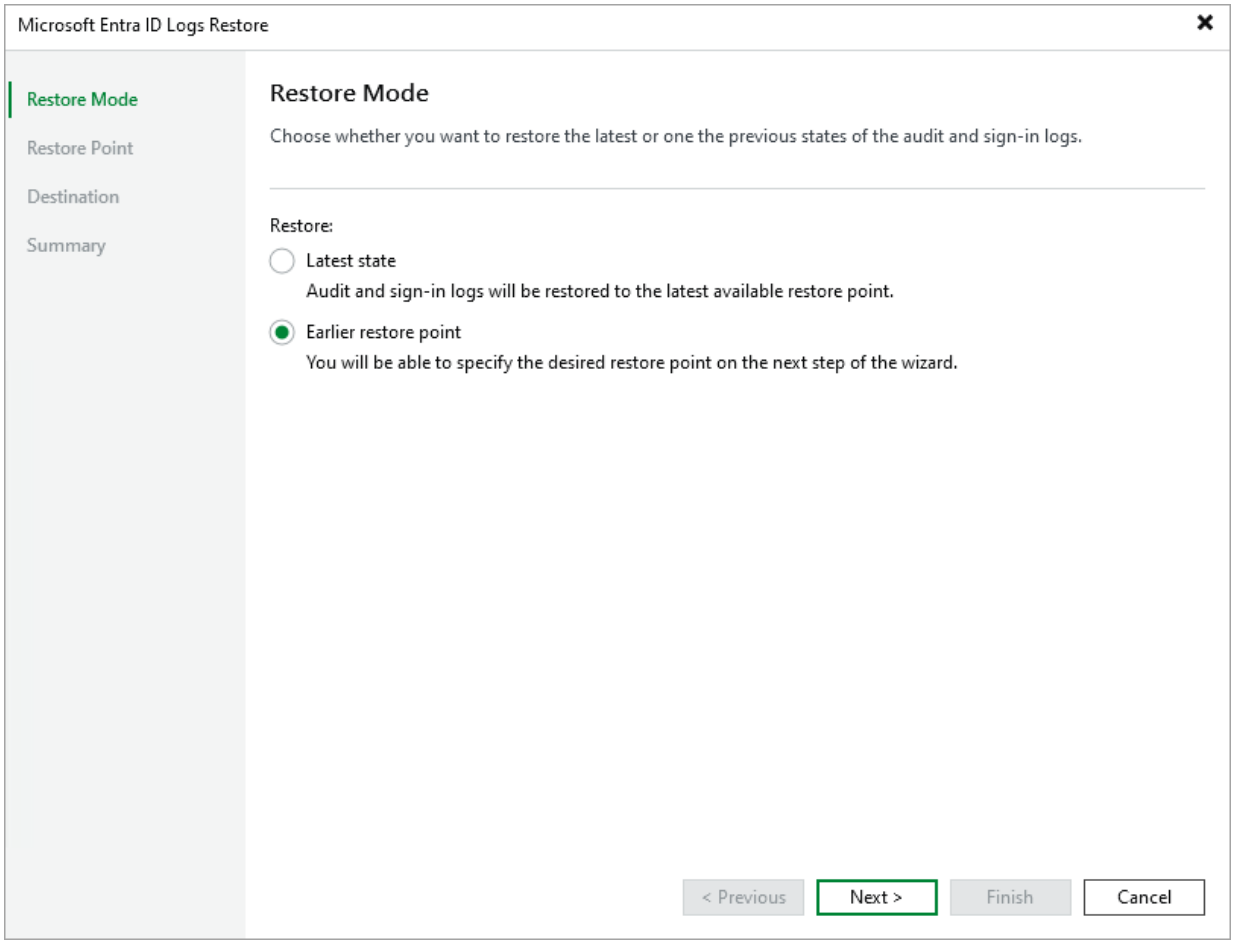
In the **Backup Browser** window, select files or folders that you want to restore, right-click one of them and select **Copy to**. Alternatively, you can use **Copy to** on the ribbon.



Step 3. Select Restore Mode

This step is available if you restore one or multiple folders. A log file itself plays the role of a restore point as it contains data for a certain period of time.

In the **Microsoft Entra ID Audit Restore** wizard, select if you want to restore folders to the latest state or to an earlier restore point. If you select the **Earlier restore point** option, the wizard will include the Restore Point step.



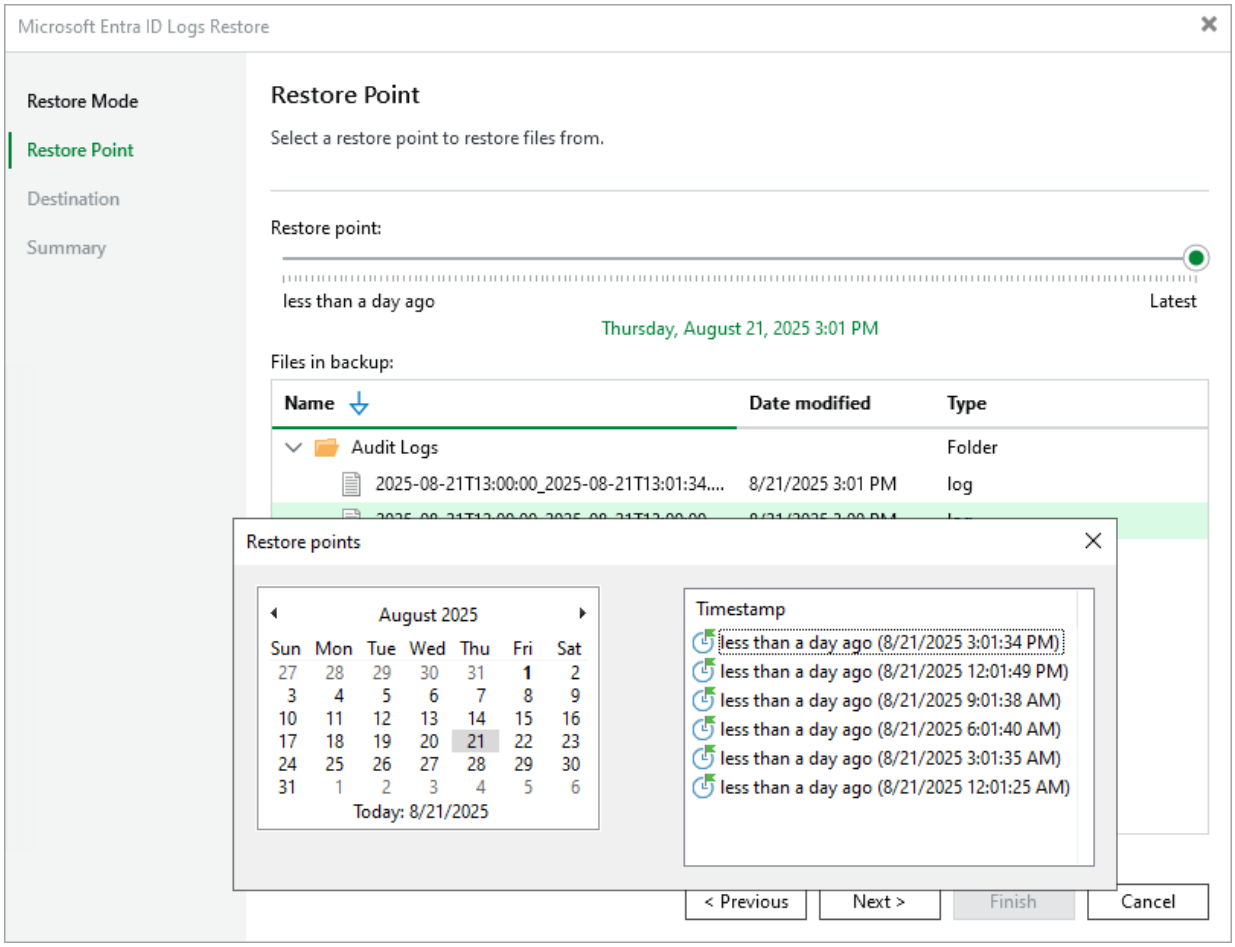
Step 4. Select Restore Point

This step is available if you restore folders and you have selected **Earlier restore point** at the Restore Mode step of the wizard.

At the **Restore Point** step of the wizard, select the point in time to restore folders and files to. To select the required restore point, do one of the following:

- Use the **Restore point** slider.
- Click the date link under the **Restore point** slider. In the calendar in the left pane of the **Restore points** window, select the date when the required restore point was created. The list of restore points in the right pane displays restore points created on the selected date. Select the point to which you want to restore the files and folders.

In the **Files in backup** tree, you can see what folders and files are covered by the selected restore point and the date when files and folders were modified.



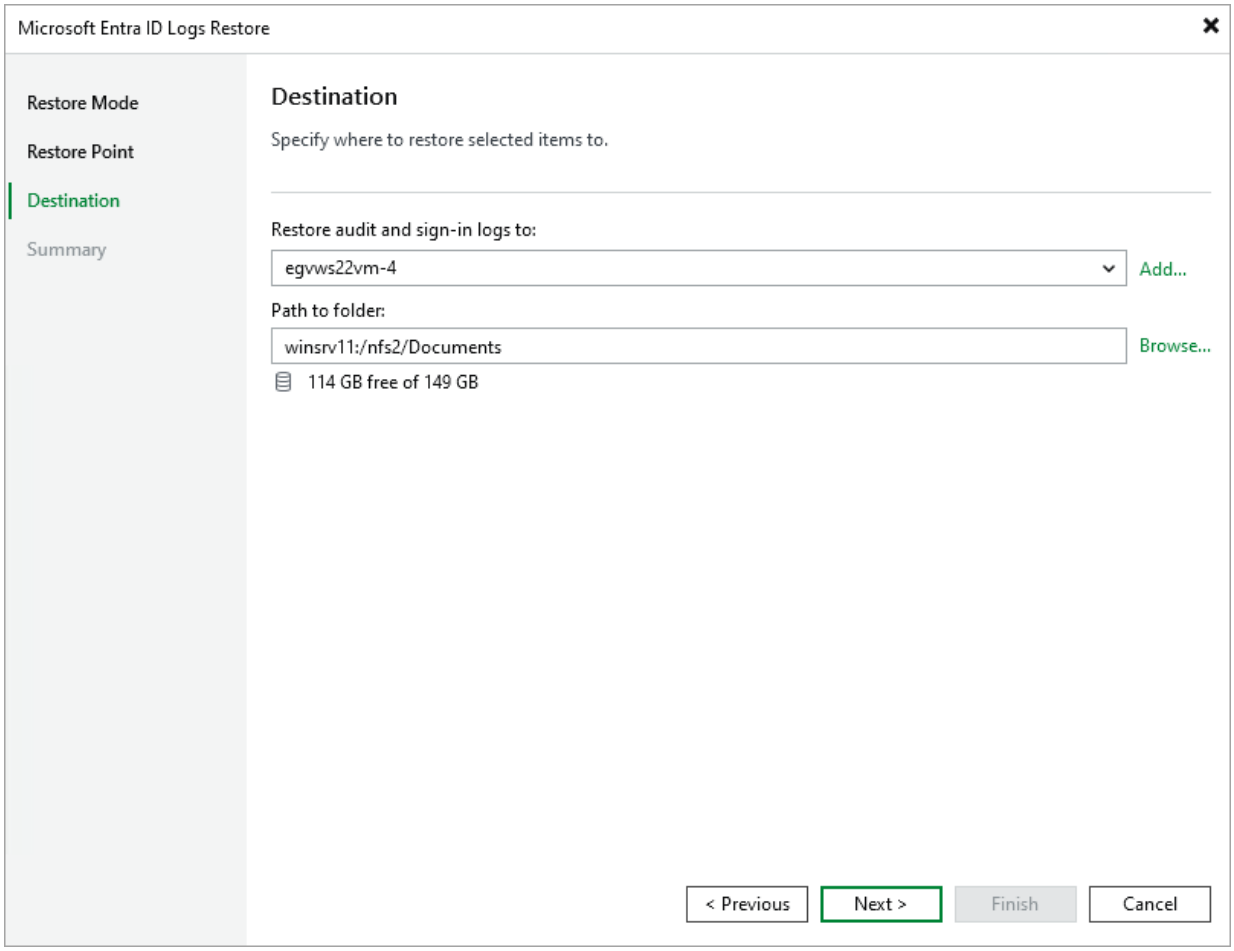
Step 5. Specify Destination for File Restore

At the **Destination** step, specify the destination where the restored files and folders must be stored:

1. In the **Restore files and folders to** field, select a file share to which the files must be restored.

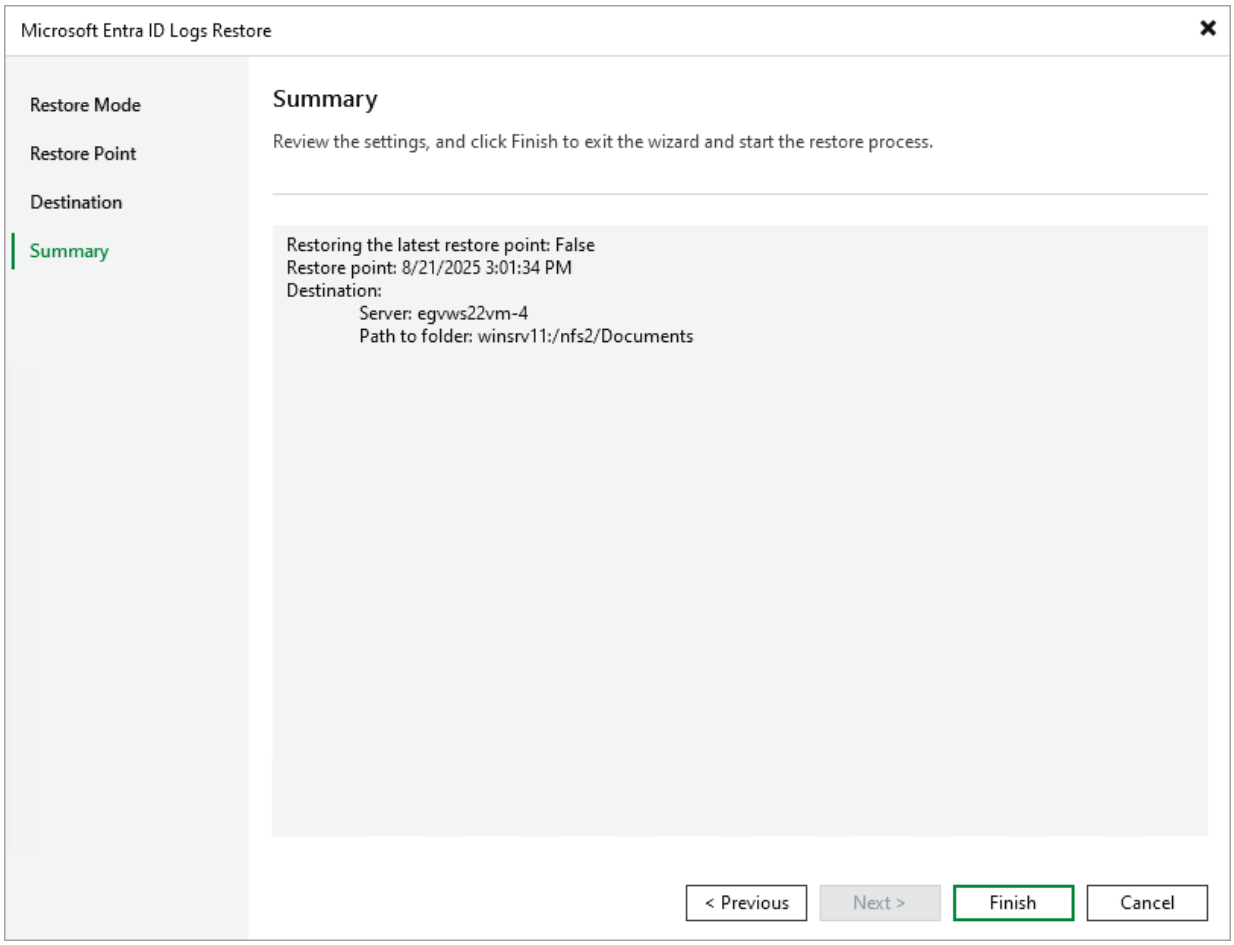
   All file shares added to the inventory of Veeam Backup & Replication are available in the drop-down list. If the required file share is missing, click **Add** and add a new file share to Veeam Backup & Replication. For more information on how to add a new file share, see the Adding Unstructured Data Source section in the Veeam Backup & Replication User Guide.

2. In the **Path to folder** field, specify a path to the folder on the selected file share where files must be restored. You can enter the path or specify it using **Browse**.



Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review the summary information and click **Finish**.



Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for Microsoft Entra ID starts a new session and stores its records in the configuration database.

Viewing Session Statistics Using Console

You can track real-time statistics of all running and completed operations on the **Jobs**, **Last 24 hours** and **Running** nodes. For more information, see the Veeam Backup & Replication User Guide, sections Viewing Real-Time Statistics and Viewing Job Session Results.

Veeam Backup & Replication also allows you track statistics of most data recovery operations initiated from Veeam Backup for Microsoft Entra ID. To do that, do either of the following:

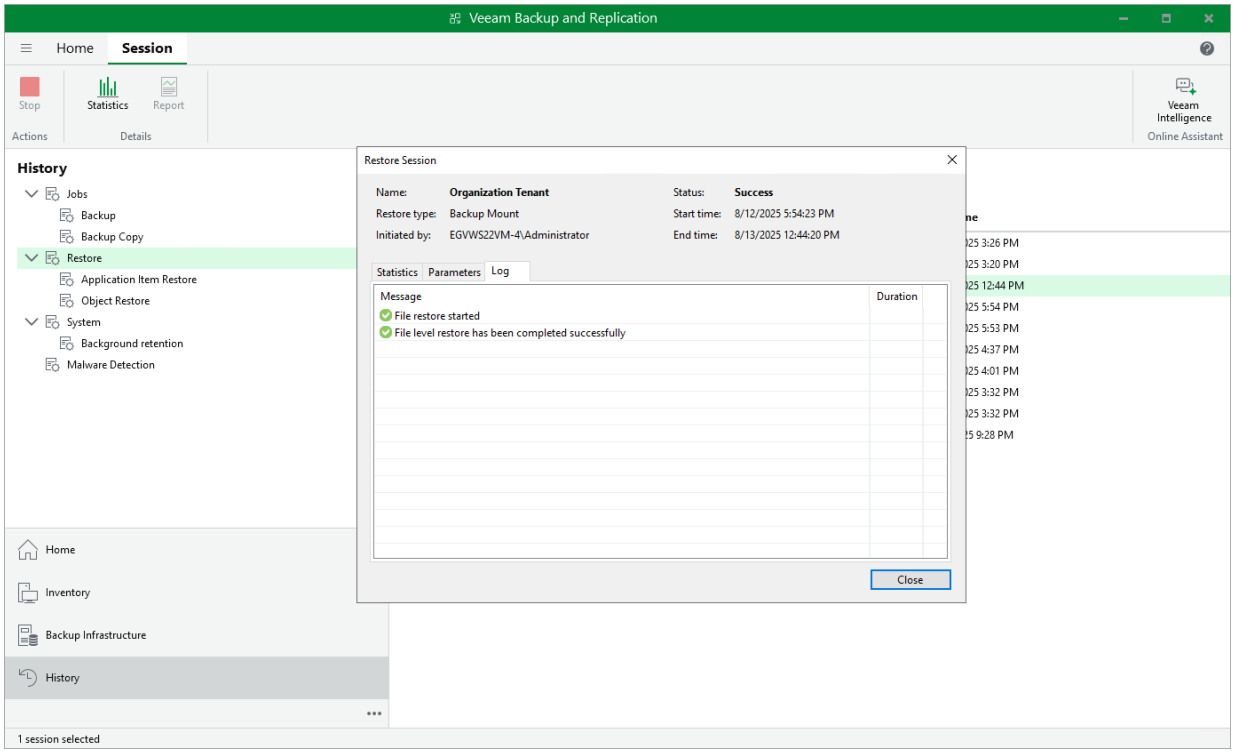
- In the Veeam Backup & Replication console, open the **Home** view and navigate to **Last 24 hours**. In the working area, double-click the necessary session.

  Alternatively, select the session and click **Statistics** on the ribbon.

- In the Veeam Backup & Replication console, open the **History** view and navigate to **Jobs** or **Restore**. In the working area, double-click the necessary session.

  Alternatively, select the session and click **Statistics** on the ribbon.

The opened window will display restore session details such as the name of the Microsoft Entra tenant whose data is being processed, the session status and duration, information on the restore point selected for the operation, and the list of tasks performed during the session.



Getting Technical Support

If you have any questions or issues with Veeam Backup for Microsoft Entra ID, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

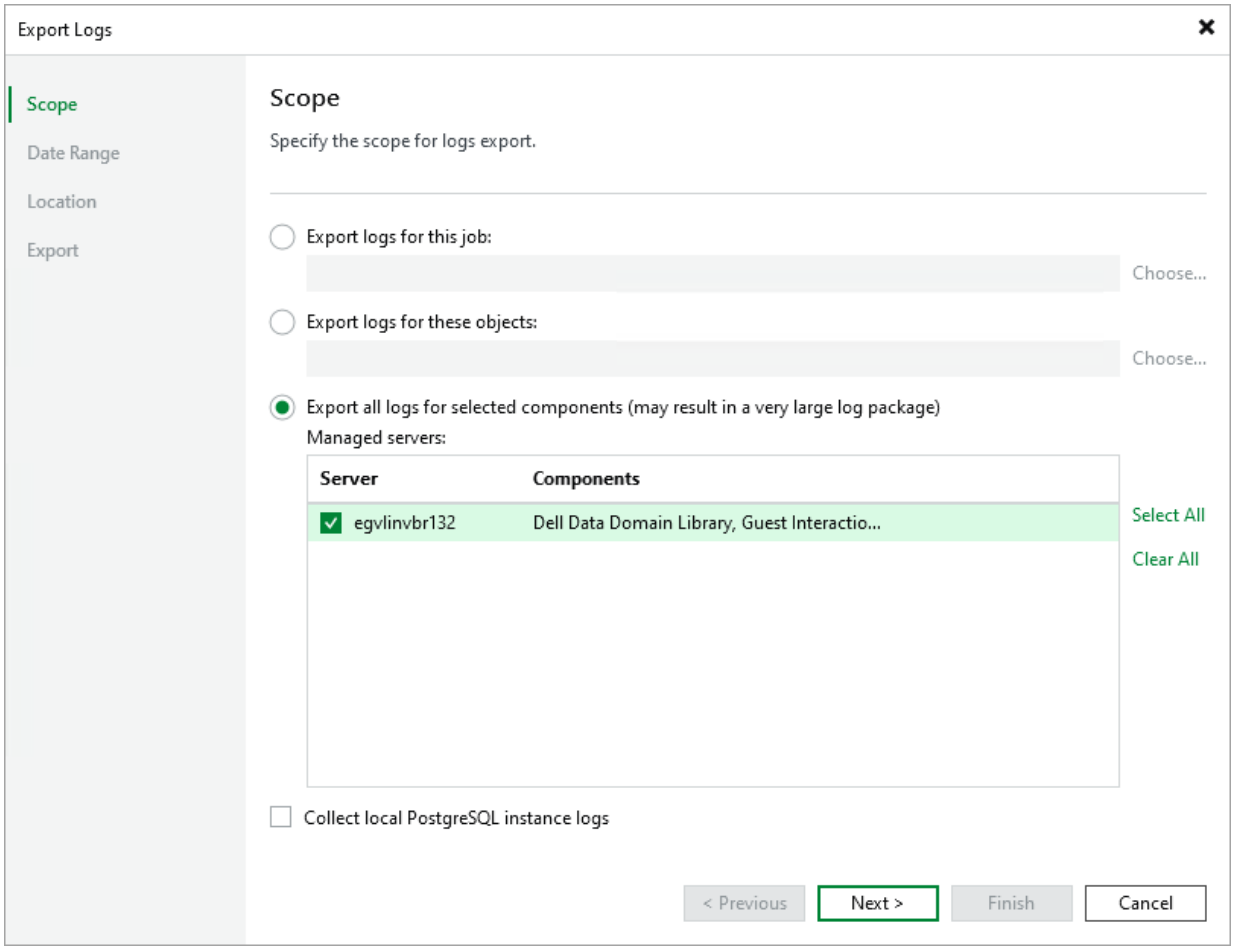
- Version information for the product and its infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

Downloading Logs

To export the product logs, do the following:

1. In the Veeam Backup & Replication console, open the main menu and navigate to **Help** > **Support Information**.
2. In the **Export Logs** wizard, do the following:
   a. At the **Scope** step, do the following:
      i. Select the **Export all logs for selected components** option.
      ii. In the **Managed servers** list, select the backup server.
      iii. If you use installed Veeam Backup & Replication with the PostgreSQL database and the same database is used to store tenant backups, select **Collect local PostgreSQL instance logs**.
   b. At the **Date Range** step, specify the time interval for which logs must be collected.
   c. At the **Location** step, specify the destination folder to which the logs will be exported.

d. Wait for the export process to complete, review the results and click the **Open folder** link to browse to exported log files and log package.



Appendix. Restoring Synchronized Users (Hybrid Identity)

Veeam Backup for Microsoft Entra ID allows you to restore users synchronized with Microsoft Active Directory (hybrid identities). Unlike the synchronization software (for example, Microsoft Entra Connect), restore with Veeam Backup for Microsoft Entra ID preserves relations stored in the Entra ID: group memberships, assigned roles, used licenses and other relations.

Veeam Backup for Microsoft Entra ID restores properties and relations listed in Supported Entra ID Item Properties. To restore other properties, you still need synchronization software and, in some cases, local Active Directory restore. This section describes possible scenarios and steps for restore.

User Removed from Entra ID Without Synchronization After

If a synchronized user was removed only from Entra ID, and there was no synchronization process after the removal, do the following:

1. Use Veeam Backup for Microsoft Entra ID to restore an entire user to Entra ID. In the wizard, make sure that restore of relations is enabled.

Veeam Backup for Microsoft Entra ID will restore a user with a new object ID.

2. Wait or launch synchronization with Active Directory, for example, using Microsoft Entra Connect.

   After the synchronization, the relations restored using Veeam Backup for Microsoft Entra ID will be preserved, the properties will be overwritten, and lacking properties will be restored. The user will become the hybrid identity.

User Removed from Entra ID with Synchronization After

If a synchronized user was removed only from Entra ID, but the synchronization process has already restored this user, Veeam Backup for Microsoft Entra ID will not be able to map this user and restore the relationships. In this case, do the following:

1. Remove from Entra ID the user created after the synchronization.
2. Use Veeam Backup for Microsoft Entra ID to restore an entire user to Entra ID. In the wizard, make sure that restore of relations is enabled.

   Veeam Backup for Microsoft Entra ID will restore a user with a new object ID.
3. Wait or launch synchronization with Active Directory, for example, using Microsoft Entra Connect.

   After the synchronization, the relations restored using Veeam Backup for Microsoft Entra ID will be preserved, the properties will be overwritten, and lacking properties will be restored. The user will become the hybrid identity.

User Removed from Entra ID and Active Directory

If a synchronized user was removed from Entra ID and Active Directory, do the following:

1. Use Veeam Backup for Microsoft Entra ID to restore an entire user to Entra ID. In the wizard, make sure that restore of relations is enabled.

   Veeam Backup for Microsoft Entra ID will restore a user with a new object ID.

2. Use application item restore or Veeam Explorer for Microsoft Active Directory to restore the user locally in Active Directory.

3. Wait or launch synchronization with Active Directory, for example, using Microsoft Entra Connect.

   After the synchronization, the relations restored using Veeam Backup for Microsoft Entra ID will be preserved, the properties will be overwritten, and lacking properties will be restored. The user will become the hybrid identity.