Quest® NetVault® Plug-in *for Microsoft 365* 14.1.1

User's Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest Software, Quest, the Quest logo, QoreStor, and NetVault are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

NetVault Plug-in *for Microsoft 365* User's Guide
Updated - May 2026
Software Version - 14.1.1

Contents

Introducing NetVault Plug-in *for Microsoft 365* **3**
NetVault Plug-in *for Microsoft 365*: at a glance 3
Key benefits 3
Feature summary 4
Target audience 5
Recommended additional reading 5

Installing and removing the plug-in **6**
Installation prerequisites 6
Azure AD and SharePoint Online limitations 7
Installing or upgrading the plug-in 7
Removing the plug-in 8
Supporting licensing models 8

Configuring the plug-in **9**
Auto config of Azure application 9
Preparing SharePoint Online for backup and restore 11
Manual Configuration method using Tenant Credentials Authentication method 11
Manual Configuration method using Certificate Authentication method 14
Entering the configuration details in the plug-in 17
Multi-tenant support 18
Adding a tenant 19
Editing a tenant 19
Removing a tenant 20
Improving backup and restore performance by using multiple applications for multiple endpoints 20
Improving backup and restore performance by modifying parameters in the configuration file 20

Backing up data **24**
Defining a backup-and-recovery strategy 24
Adding patterns to use for exclusion and inclusion 25
Performing backups 26
Selecting data for a backup 26
Setting backup options 28
Finalizing and submitting the backup job 29
. 29
Continuous data protection backups 29
Prerequisite 29
Performing continuous backups 29

Selecting data for a continuous backup 29
Setting continuous backup options 31
Finalizing and submitting the continuous backup job 31
To select Target Storage options, click and complete the following steps . . . . . : 32

Restoring data 33
Selecting data for a restore 33
Setting restore options for Outlook 34
Setting restore options for Azure AD 34
Finalizing and submitting the restore job 35
Relocating mailboxes and OneDrive accounts during the restore process 35
Relocating a mailbox and a OneDrive account to a user from another tenant 36
Searching for granular items 36

Troubleshooting 37
Technical support resources 38

1

Introducing NetVault Plug-in *for Microsoft 365*

- NetVault Plug-in for Microsoft 365: at a glance
- Key benefits
- Feature summary
- Target audience
- Recommended additional reading

NetVault Plug-in *for Microsoft 365*: at a glance

Quest® NetVault® Plug-in *for Microsoft 365* (Plug-in *for Microsoft 365*) increases confidence in the recoverability of data that you produce using Microsoft 365, a cloud-based service that provides software as a service (SaaS). The plug-in lets you create flexible backup policies that can account for multiple recovery scenarios. Through a web-based user interface (WebUI) and automated workflow process, the plug-in offers a centralized way to set up, configure, and define backup and restore policies for Microsoft 365. Through integration with a range of backup devices, your data is protected and stored offsite to meet your disaster-recovery and business-continuity goals.

The plug-in enables Full and Incremental Backups and Restores of your Microsoft Outlook, OneDrive, SharePoint Online, Teams, and Azure AD accounts in Microsoft 365. Using the plug-in ensures that you have backups stored in an accessible location as part of your regular backup process. To manage the size of backups and accommodate network bandwidth, your backups can include or exclude the various items as part of the backup process.

NOTE: Plug-in *for Microsoft 365* supports SharePoint Online. It does not support backups or restores for SharePoint Server.

Key benefits

- **Increases confidence and reduces risk while subscribing to Microsoft 365:** The plug-in lets you create backup policies that are flexible enough to account for various recovery scenarios.

  Backup features include:

  - Protection for individual, shared, and resource mailboxes
  - Protection for calendars, calendar groups, and events
  - Protection for SharePoint Online sites and subsites
  - Protection for Teams
  - Full and Incremental Backups while data is online and accessible

> **NOTE:** For Teams, Full Backups include all standard items. Incremental Backups include files, folders, and chat messages.

  - Protection for files and folders located on OneDrive
  - Full and incremental backups of users, groups, and service principals
  - Support for multi-tenant application authentication and authorization models

  By relying on the plug-in to implement backup policies, you can focus on more critical tasks without risking your ability to recover what is needed if a failure occurs. In addition, the IT manager's confidence is increased by knowing that email is protected, no matter what.

- **Speeds up restores to reduce downtime**: With the plug-in, you select what must be restored and the backup set to restore from, and the plug-in automatically performs the restore.

  Additional restore features include:

  - Full and Incremental Restores
  - Restores of individual, shared, and resource mailboxes
  - Restores of calendars, calendar groups, and events
  - Restores of sites and subsites
  - Restores of Teams and supported Microsoft applications
  - Restores of individual email messages
  - Restores of individual files and folders
  - Restores of users, groups, and service principals
  - Restores of individual files, folders, apps, and chats for Teams
  - Restores of document library, page library (Site Pages), events, and lists for SharePoint Online

- **Ensure business continuity**: With offsite backups being an important part of the data-protection for business-critical applications, the plug-in takes advantage of NetVault's integration with a range of backup devices. NetVault lets you select which backup device to store the backup on.

  To address the lack of native backup and flexible recovery abilities for user data, such as the 30-limitation of deleted email, you can use the plug-in to implement a more robust backup and recovery implementation. The plug-in also ensures that your data is protected if a user's mailbox or OneDrive becomes corrupted.

- **Eliminate backup windows and reduce storage**: The plug-in gives you the confidence that your email environment is protected and stored offsite for disaster-recovery purposes. At the same time, it frees administrators from having to be available 24x7 because less-experienced personnel can initiate restores, thus reducing downtime and improving business continuity.

Feature summary

- Full and Incremental Restores
- Protection for individual, shared, and resource mailboxes
- Protection for calendars, calendar groups, and events
- Protection for files and folders located on OneDrive
- Protection for Teams Full and Incremental Backups while data is online and accessible
- Certificate-based authentication
- Multi-tenant support
- Restores of individual, shared, and resource mailboxes

- Restores of calendars, calendar groups, and events
- Restores of Teams and supported Microsoft applications
- Restores of individual email messages
- Restores of individual files and folders
- Restores of documents and form templates
- Restores of style libraries
- Restores of site and subsite pages
- Restore of Azure AD users, groups, and service principals
- Relocation of OneDrive and Outlook data during restore, including across tenants

Target audience

This guide is intended for users who are responsible for the backup and recovery of Microsoft 365. Familiarity with Microsoft 365 administration is assumed. Advanced knowledge of Microsoft 365 is useful for defining an efficient backup-and-recovery strategy.

Recommended additional reading

Quest recommends that you have the following **Microsoft 365 documentation** available for reference when setting up and using this plug-in: https://docs.microsoft.com/en-us/Office365/ and https://technet.microsoft.com/en-us/library/dn127064(v=office.14).aspx

The following documentation is also available:

- *Quest NetVault Installation Guide*: This guide provides details on installing the NetVault Server and Client software.
- *Quest NetVault Administrator's Guide*: This guide explains how to use NetVault and describes the functionality common to all plug-ins.
- *Quest NetVault CLI Reference Guide*: This guide provides a description of the command-line utilities.

You can download these guides from https://support.quest.com/technical-documents.

2

Installing and removing the plug-in

- Installation prerequisites
- Installing or upgrading the plug-in
- Removing the plug-in

Installation prerequisites

You can install the plug-in on any pure 64-bit Windows Server-based NetVault Server or Client that supports the Microsoft .NET Framework, version 4.7.2 or later.

- **Verify that Microsoft .NET Framework is installed:** The server that you use must support version 4.7.2 or later of the .NET Framework.
- **Install NetVault Server or Client software:** At a minimum, the NetVault Client software must be installed on the server. For instructions on installing the NetVault Server or Client software, see the *Quest NetVault Installation Guide*.
- **Ensure that the server or client has access to a high level of internet bandwidth:** Because the data that is backed up resides on a cloud-based server and is downloaded to local storage media, Quest recommends that you install the plug-in on a client or server that has high internet bandwidth.
- **Update TLS versions:** Microsoft deprecated TLS 1.0 and 1.1, which can cause OneDrive, Teams, and SharePoint Online backups to fail. To maintain compatibility between the plug-in and these Microsoft products, before you install Plug-in *for Microsoft 365*, make the following changes to the Windows registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

Azure AD and SharePoint Online limitations

The following limitations should be considered when installing Plug-in *for Microsoft 365* for the purpose of backing up and restoring Azure AD and SharePoint Online content.

For Azure AD:

- The plug-in does not support the restore of mail-enabled security and distribution groups.
- The plug-in cannot restore client secret keys for service principals.
- Licenses inherited at the time of the backup are restored as directly assigned licenses.

For SharePoint Online:

- The plug-in does not support the backup and restore of the following types of SharePoint Online site lists:
  - Process diagrams
  - Promoted links
  - Related actions
  - Report library
  - Web part page with status
- For classic team sites only, the plug-in does not back up and restore asset library type lists.

Installing or upgrading the plug-in

The following topic describes the process for installing the plug-in on a single client or upgrading an existing one. If you have multiple clients of the same type, you can use the NetVault Configuration Wizard to install the plug-in on multiple clients at the same time. For more information on using push installation to update multiple clients at the same time, see the *Quest NetVault Administrator's Guide.*

To install or upgrade the plug-in

1. In the Navigation pane, click **Manage Clients**.
2. On the **Manage Clients** page, select the applicable client in the table, and click **Manage**.
3. On the **View Client** page, click ✚.
4. Navigate to the location of the **".npk"** installation file for the plug-in, for example, on the installation CD or the directory to which the file was downloaded from the website.

   Based on the OS in use, the path for this software may vary on the installation CD.
5. Select the file entitled **"not-x-x-x-x-x.npk,"** where **xxxxx** represents the version number and platform, and click **Open**.

   After the plug-in is successfully installed, a message is displayed.

NOTE: After upgrading the Plug-in *for Microsoft 365* from version 13.4.1 to 14.0, the next execution of existing CDP and non-CDP incremental jobs will be treated as a full backup.

NOTE: When upgrading the Plug-in *for Microsoft 365* to version 14.0, ensure to maintain at least one client with the 13.x plug-in to restore backups of the 13.x plug-in. It is mandatory to install the version 14.0 plug-in on a new client if there is only one proxy plug-in. It is recommended to maintain the machine's availability until the backup using the 13.x plug-in has expired.

Removing the plug-in

To remove the plug-in

1. In the Navigation pane, click **Manage Clients**.
2. On the **Manage Clients** page, select the applicable client, and click **Manage**.
3. In the **Installed Software** table on the **View Client** page, select the applicable plug-in, and click —.
4. In the **Confirm** dialog box, click **Remove**.

Supporting licensing models

Currently, we support the following Microsoft 365 licensing models with their plans:

- Office 365 Enterprise plans: E1, E3, and E5
- Microsoft 365 Enterprise plans: E3 and E5
- Office 365 Education plans: A1, A3, and A5
- Microsoft 365 E5 developer subscription

3

Configuring the plug-in

You must create an application in the Azure portal, before configuring the data in the M365 plug-in, as the Azure portal grants you the required permissions, provides secure access that's needed for the M365 plug-in to read and backup M365 data.

Configuration of the Azure application and Plug-in for NetVault M365 can be done in two ways:

1 Auto Config of Azure application

2 Manual Configuration of Azure application

   Manual Configuration method using Tenant Credentials Authentication method

   Manual Configuration method using Certificate Authentication method

Auto Config of Azure application

Plug-in for *Microsoft 365* supports the auto-configuration of the application on the Azure portal. This feature automatically adds API permission, provide grant admin consent, and enable public client flow to the generated application without human intervention.

To auto configure the application

1 In the Navigation Pane, click **Create Backup Job**, and click + next to the **Selections** list.

2 In the selection tree, open the applicable client node.

3 Click **Plug-in *for Microsoft 365***, and select **Add Tenant** from the context menu.

4 On the Add Tenant page, select **Auto Config Application** from the **Configuration Method**.

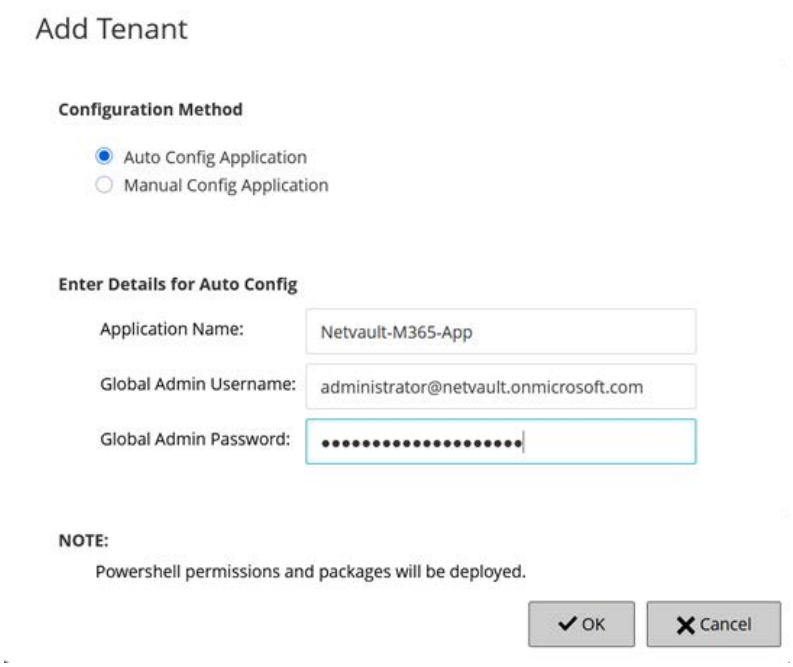
5 Enter the following details for Auto Config:

   - **Application Name**
   - **Global Admin Username**
   - **Global Admin Password**

6 Click **OK** to automatically configure the application.

7 Provide the below details in the NetVault M365 Add Tenant page.

Figure 1. Auto Configuration Method



NOTE: Auto Config application feature works with AzureAD version 2.0.2.140. If you have a higher version of AzureAD (2.0.2.180) already installed on your system, the feature will fail to grant the admin consent to delegated permissions.

NOTE: To perform SharePoint Online backup and restore using an application created with the auto-config requires assigning permission to SharePoint Online CSOM API.
Refer procedure mentioned in the section .

Preparing SharePoint Online for backup and restore

NOTE: These steps are not required for recently created Tenants.

NOTE: To back up and restore Azure AD service principals, the registered application used for the configuration of the plug-in must be the Global Administrator and the Application Administrator.

NOTE: Lack of 'Team' permission results in inaccessible and partial backup of Microsoft Teams application.

Before you can protect your SharePoint Online data with Plug-in *for Microsoft 365*, you must assign permission for the SharePoint Online CSOM API.

NOTE: These steps are required for both Auto Configuration and Manual configuration of Azure Applications.

To prepare SharePoint Online for backup and restore

1 Open the SharePoint Online Tenant site with the Tenant Administrator account. For example: https://<tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx.

2 In the **App Id** text box, enter the Client ID generated from Azure Active Directory.

3 Click **Lookup**.

4 Under **App Domain**, enter **www.localhost.com**.

5 Under **Redirect URL**, enter **https://www.locahost.com**.

6 Under **Permission Request XML**, enter the following XML script:

```
<AppPermissionRequests AllowAppOnlyPolicy="true"> <AppPermissionRequest
Scope="http://sharepoint/content/tenant" Right="FullControl" />
</AppPermissionRequests>
```

7 Click **Create**.

8 In the dialog, click Trust It.

Manual Configuration method using Tenant Credentials Authentication method

You can configure the Azure application from the Microsoft 365 admin portal and use this information in the Add Tenant page for Manual configuration section.

To use the Microsoft 365 admin portal obtain configuration details

1 Go to admin.microsoft.com.

2 In the navigation pane on the left, click **Show All** and then select **Azure Active Directory** from the list.

3 In the **Azure Active Directory admin center**, under **All services**, click **Azure Active Directory**.

4 In the **MANAGE** section, click **App registrations**, and click **New registration**.

5 Complete the following fields:

- **Name:** Enter a name for the NetVault plug-in, such as **PluginMicrosoft365**.
- **Supported account types:** To specify who can use this application or access this API, select **Account in any organizational directory (Any Azure AD directory - Multitenant)**.
- **Redirect URI:** Enter the URI that you use for interacting with NetVault, such as `https://<machineName>:8443`.

6 Click **Register**, and note the **Application ID** listed on the page that appears.

Quest strongly recommends that you record this information, for example by copying it to a text file and saving that file.

7 On the **Overview** page, under **Manage**, click **Authentication**.

8 In the **Advanced settings** section, next to **Allow public client flows**, select **Yes**.

9 In the **Manage** section, click **API permissions**.

10 In **API permissions**, click **Add a permission**.

11 Choose one of the following options:

- **Select an API:** To use this method, select **Microsoft Graph** or **SharePoint**, and then click **Select**.
- **Select permissions:** To use this option, complete the following steps:
  a Select **Application Permissions**, and then select the following items:
    - **Calendars.Read**

- **Calendars.ReadWrite**
- **ChannelMember.ReadWrite.All**
- **ChannelMessage.Read.All**
- **Directory.ReadWrite.All**
- **Files.Read.All**
- **Files.ReadWrite.All**
- **Group.Read.All**
- **Group.ReadWrite.All**
- **Mail.Read**
- **Mail.ReadWrite**
- **MailboxSettings.Read**
- **MailboxSettings.ReadWrite**
- **Reports.Read.All**
- **Sites.FullControl.All**
- **Sites.Manage.All**
- **Sites.Read.All**
- **Sites.ReadWrite.All**
- **Team.ReadBasic.All**
- **TeamMember.ReadWrite.All**
- **TeamSettings.Read.All**
- **TeamSettings.ReadWrite.All**
- **User.Read.All**
- **User.ReadWrite.All**

b Select **Delegated Permissions**, and then select the following items:

- **ChannelMessage.Read.All**
- **Group.ReadWrite.All**
- **User.Read (this permission is added by default for the registered App)**

c Click **Add permissions**.

d To assign permissions to the Plug-in *for Microsoft 365* after the plug-in is configured, click **Grant permissions** on the **Required permissions** tab, and click **Yes** when the confirmation message appears.

NOTE: To back up and restore Azure AD service principals, the registered application used for the configuration of the plug-in must be the Global Administrator and the Application Administrator.

NOTE: Lack of 'Team' permission results in inaccessible and partial backup of Microsoft Teams application.

12 On the **Manage** tab, in the **Certificates & secrets** section, click **New client secret** to create passwords for the plug-in to use.

13 Enter a description and select a time period option.

Optionally, you can determine a specific time for when the password is active by selecting a start date and an end date.

14 Click **Add** and note the information in the **VALUE** box.

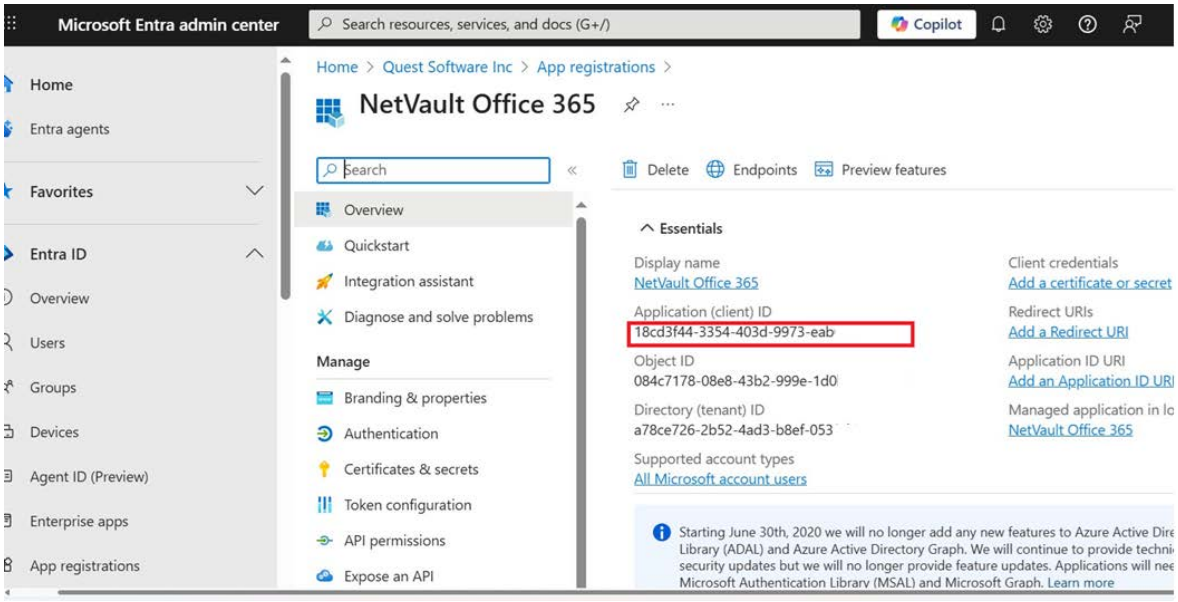
Quest strongly recommends that you record this information, for example by copying it to the same text file that you created and saved earlier.

> **IMPORTANT:** You cannot retrieve this key at a later time. If you do not record it for reference when you configure the plug-in, you have to generate a new key.

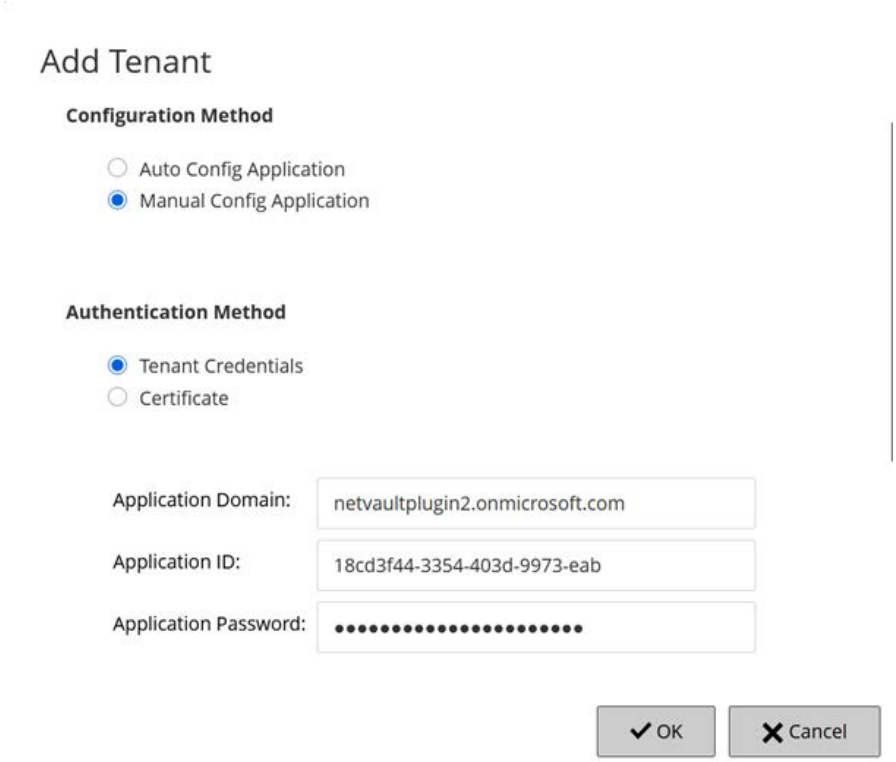
15 To identify the domain name used for Microsoft 365, click **Azure Active Directory** again in the navigation pane on the left.

16 Click Overview, and note the domain name.

> **NOTE:** Quest recommends that you record this information, for example by copying it to a text file and saving that file.



17 Enter Application Domain, Application ID and Application password in M365 plug-in Add Tenant page.



18 To prepare SharePoint Online for backup and restore for Manual configuration using Tenant Credentials Authentication method, refer to Preparing SharePoint Online for backup and restore

Manual Configuration method using Certificate Authentication method

Plug-in *for Microsoft 365* supports certificate-based authentication. NetVault uses certificate thumbprint to fetch the private key from the Windows Certificate Manager.

Microsoft recommends certificate-based authentication over the domain, key, and access key method. Reasons for using a certificate to authenticate includes:

- Credential rotation is prone to human error.
- Certificates last longer than credentials (mostly more than one year).
- Using a certificate shares responsibility with Microsoft Credential Manager (Windows OS), Certificate Authority, and Azure AD.
- It is the highest level of security for Microsoft Graph Client.
- It has reliable credential encryption for compliance

Before you add the certificate to your configuration as a means for authenticating, complete the following processes.

1 Follow steps from 1 to 11 as mentioned in the Manual Configuration method using Tenant Credentials Authentication method. After step 11, follow the below steps to configure Certificate-based Authentication.

2 Creating a self signed certificate using Powershell

Follow the steps to create a self-signed certificate using PowerShell

Run the following script as an administrator:

```
# --- config start

$dnsName = "mytenant.sharepoint.com" # Your DNS name

$password = "Come up with something secure!" # Certificate password

$folderPath = "C:\temp" # Where do you want the files to get saved to? The
folder needs to exist.

$fileName = "mycert" # What do you want to call the cert files? without the
file extension

$yearsValid = 10 # Number of years until you need to renew the certificate

# --- config end


$certStoreLocation = "cert:\LocalMachine\My"

$expirationDate = (Get-Date).AddYears($yearsValid)


$certificate = New-SelfSignedCertificate -DnsName $dnsName -CertStoreLocation
$certStoreLocation -NotAfter $expirationDate -KeyExportPolicy Exportable -
KeySpec Signature


$certificatePath = $certStoreLocation + '\' + $certificate.Thumbprint

$filePath = $folderPath + '\' + $fileName

$securePassword = ConvertTo-SecureString -String $password -Force -AsPlainText


Export-Certificate -Cert $certificatePath -FilePath ($filePath + '.cer')

Export-PfxCertificate -Cert $certificatePath -FilePath ($filePath + '.pfx') -
Password $securePassword
```

NOTE: Change the $dnsName, $password and $folderPath to run the script.

3 Adding a certificate in the Azure AD admin portal

Follow the steps below, to add a certificate in the Azure AD admin portal

- Login to the Azure AD admin portal.
- Go to **Certificates & secrets**.
- Click **Upload certificate**.
- Select the .cer file you generated with the PowerShell script, and click **Add**. Note the thumbprint that appears. You will need it for Entering the configuration details in the plug-in.

4 While using a second proxy, import a self signed certificate to the local machine certificate store.

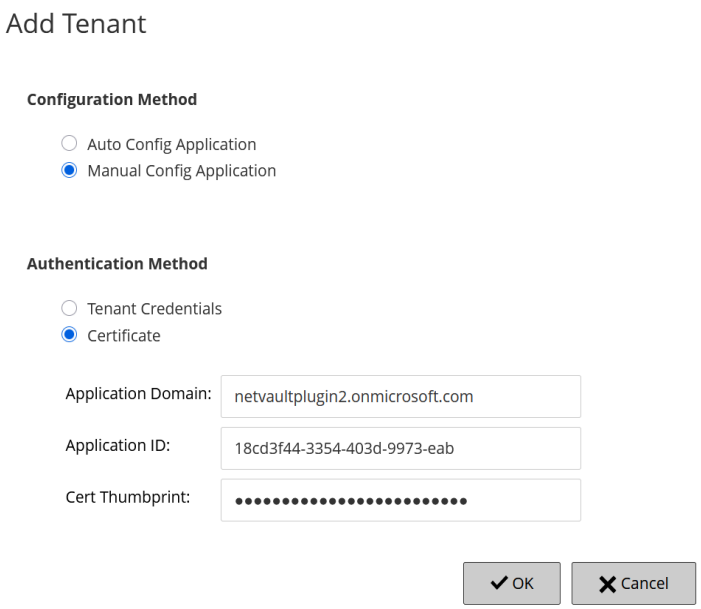
Follow the steps below, to import a self-signed certificate to the local machine certificate store.

- In Windows, run MMC
- Click File
- Click **Add/Remove Snap-in**

- In the Add or Remove Snap-ins window, select **Certificates** and then click **Add.**
- In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
- When prompted, select the computer account and then click **Next**.
- Select **Local computer** (selected by default) and then click **Finish**.
- In the Add or Remove Snap-ins window, click **OK**.
- In the MMC main console, expand the certificate snap-in by clicking the plus (**+**) symbol.
- Navigate to the **Personal | Certificates** pane.
- Open the Certificate Import Wizard by right-clicking within the Certificates panel and clicking **All Tasks | Import**.
- To import the private key alone with a password, follow the Certificate Import Wizard.

NOTE: For SharePoint Online backup and restore, the private key should reside in the Personal folder with certificates managed on the local computer.

5 Provide Application Domain, Application ID and Cert Thumbprint in M365 plugin in Add Tenant page.



6 To prepare SharePoint Online for backup and restore for Manual configuration using Certificate Authentication method refer to Preparing SharePoint Online for backup and restore

Entering the configuration details in the plug-in

After you have identified application ID, password, and domain name, you must enter the information in the configuration section for the plug-in.

NOTE: Plug-in *for Microsoft 365* requires Global administrator access for the following sites:

- Team Site with Group (Primary)
- Business Intelligence Center (Classic)
- Visio Process Repository (Classic)
- Product Catalog (Classic)

NOTE: The user configured for the plug-in must be a member of the Teams platform to generate backup and restore jobs for Teams.

To enter the configuration details in the plug-in:

1. In the Navigation Pane, click **Create Backup Job**, and click + next to the **Selections** list.
2. In the selection tree, open the applicable client node.
3. Click **Plug-in *for Microsoft 365***, and select **Configure** from the context menu.
4. On the Add Tenant page, select one of the following options as the tenant authentication method, and then enter the details for your selection:

   NOTE: Use the information that you recorded during the process, Entering the configuration details in the plug-in.

   - **Tenant Credentials**
     - **Application Domain**
     - **Application ID**
     - **Application Password**
   - **Certificate**
     - **Application Domain**
     - **Application ID**
     - **Cert Thumbprint**

     NOTE: NetVault uses certificate thumbprint to fetch the private key from the Windows Certificate Manager.

CAUTION: Do not use the Change Settings option in the WebUI to enter or update these settings.

5. To save the settings, click **OK**.

   With the account properly configured, you can click the **Plug-in *for Microsoft 365*** node to display the available mailboxes and the OneDrive users and groups.

NOTE: Plugin for Microsoft 365 does not support connecting to graph server through proxy.

Multi-tenant support

Plug-in *for Microsoft 365* features multi-tenant support, which lets you backup and restore data for multiple tenants. Multi-tenant support also provides the following advantages:

- **Cost savings** for managed service providers (MSPs) due to a single plug-in deployment for managing multiple tenants.
- **Instant recovery** with a new domain in the case of a ransomware attack on your existing domain.
- **Cross-tenant restores,** which you can use in cases of mergers and acquisitions. For more information about cross-tenant relocation, see The mailbox is restored with its new name to the original location as a subset of the original mailbox..

To view all tenants, use the **Open** action in the click menu of the plug-in under NetVault Selections.

This section includes the following processes:

- Adding a tenant
- Editing a tenant
- Removing a tenant

Adding a tenant

To add a tenant

1. Under NetVault Selections, click **Plug-in *for Microsoft 365***.
2. In the menu, click **Add Tenant**.
3. On the Add Tenant page, select one of the following options as the tenant authentication method, and then enter the details for your selection:

   NOTE: Use the information that you recorded during the process, Entering the configuration details in the plug-in.

   - **Tenant Credentials**
     - **Application Domain**
     - **Application ID**
     - **Application Password**
   - **Certificate**
     - **Application Domain**
     - **Application ID**
     - **Cert Thumbprint**

     NOTE: NetVault uses certificate thumbprint to fetch the private key from the Windows Certificate Manager.
4. Optionally, under Global Administrator Details, select **Enter Global Administrator Credentials**, and then enter the administrator user name and password.
5. Click **OK**.

Editing a tenant

To edit a tenant

1. Under NetVault Selections, expand **Plug-in *for Microsoft 365***, and then click the domain.
2. In the menu, click **Edit**.
3. On the Add Tenant page, select one of the following options as the tenant authentication method, and then enter the details for your selection:

   NOTE: Use the information that you recorded during the process, Entering the configuration details in the plug-in.

   - **Tenant Credentials**
     - **Application Domain**
     - **Application ID**
     - **Application Password**
   - **Certificate**
     - **Application Domain**
     - **Application ID**
     - **Cert Thumbprint**

     NOTE: NetVault uses certificate thumbprint to fetch the private key from the Windows Certificate Manager.
4. Optionally, under Global Administrator Details, select **Enter Global Administrator Credentials**, and then enter the administrator user name and password.
5. Click **OK**.

Removing a tenant

To remove a tenant

1. Under NetVault Selections, expand **Plug-in *for Microsoft 365***, and then click the domain.
2. In the menu, click **Remove**.
3. To confirm your selection, click **OK**.

Improving backup and restore performance by using multiple applications for multiple endpoints

To reduce graph API throttling at large scale enterprise, register endpoint specific application in AzureAD.

For Ex: Azure-App-Outlook for Outlook endpoint, Azure-App-OneDrive for OneDrive endpoint, etc.

Improving backup and restore performance by modifying parameters in the configuration file

If you want to manage the performance of backup and restore jobs for Microsoft Outlook, SharePoint Online, Teams, and OneDrive accounts, you can modify the following parameters in the **"nvoffice.cfg"** file. The default location of this file is **C:\Program Files\Quest\NetVault\config**.

The values that you use depend on the value that you select for the **Enable multi-streaming** options for backup and restore jobs, as well as the bandwidth supported by your network.

The following tables list the parameters, their default settings, and a description of their impact.

Table 1. Parameters supported for network resilience

Parameter	Default	Description
Resiliency:Retry Count	10	Indicates the number of times that the plug-in runs GRAPH API after a failure occurs.
Resiliency:Retry Delay	5 (in seconds)	Indicates how long the plug-in should wait before running GRAPH API again after a failure occurs.

Table 2. Parameters supported for Outlook

Parameter	Default	Description
MsOutlook:Mails Without Attachment	1000	Indicates the number of email messages that one GRAPH API call can fetch of emails that do not have attachments. The 1000 value is the maximum allowed.
MsOutlook:Mails With Attachment	10	Indicates the number of email messages that one GRAPH API call can fetch of emails that have attachments. You can increase this value to increase the data-transfer rate, depending on the size of the attachments and network bandwidth.
MsOneDrive:Restore Chunk Size	5 (in MB)	Indicates the Chunk Size that can be used to restore—upload—mail attachments and attachments of type Event in chunks over OneDrive. The Chunk Size *must* be a multiple of 320 KiB (327,680 bytes). Using a Chunk Size that does not divide evenly by 320 KiB results in errors when committing some the files. You can increase this value to increase the data-transfer rate, depending on the network bandwidth. If you exceed a supported rate, the GRAPH API might generate a TIMEOUT exception.

Table 3. Parameters supported for OneDrive

Parameter	Default	Description
MsOneDrive:Backup Chunk Size	5 (in MB)	Indicates the Chunk Size that can be used to back up—download—files. The Chunk Size *must* be a multiple of 320 KiB (327,680 bytes). Using a Chunk Size that does not divide evenly by 320 KiB results in errors when committing some the files. You can increase this value to increase the data-transfer rate, depending on the network bandwidth. If you exceed a supported rate, the GRAPH API might generate a TIMEOUT exception.
MsOneDrive:Parallel Files Metadata per folder	1000	Indicates the number of files with metadata that one GRAPH API call can fetch. The 1000 value is the maximum allowed.

Table 3. Parameters supported for OneDrive

Parameter	Default	Description
MsOneDrive:Restore Chunk Size	5 (in MB)	Indicates the Chunk Size that can be used to restore—upload—files. The Chunk Size *must* be a multiple of 320 KiB (327,680 bytes). Using a Chunk Size that does not divide evenly by 320 KiB results in errors when committing some the files. You can increase this value to increase the data-transfer rate, depending on the network bandwidth. If you exceed a supported rate, the GRAPH API might generate a TIMEOUT exception.
MsOneDrive:Enable Parallel Download per User	TRUE	Enables parallel downloads of OneDrive files for each OneDrive user. Otherwise, files download sequentially.
MsOneDrive:Maximum Parallel Download Sessions per User	20	Controls the number of parallel file downloads. By default, 20 download sessions occur at any time and at most, 20 files download in parallel.
MsOneDrive:File Size Limit in Parallel Download Sessions	2048 (in KB)	Filters out the files to be downloaded in parallel. Only files whose size is less than or equal to the value of this parameter download in parallel.

Table 4. Parameters supported for SharePoint Online

Parameter	Default	Description
MsSharePoint:Backup Chunk Size	5 (in MB)	Indicates the Chunk Size that can be used to back up—download—files. The Chunk Size *must* be a multiple of 320 KiB (327,680 bytes). Using a Chunk Size that does not divide evenly by 320 KiB results in errors when committing some the files. You can increase this value to increase the data-transfer rate, depending on the network bandwidth. If you exceed a supported rate, the GRAPH API might generate a TIMEOUT exception.
MsSharePoint:Enable Parallel Download per Site	TRUE	Enables parallel downloads of SharePoint files for each SharePoint site. Otherwise, files download sequentially.
MsSharePoint:Maximum Parallel Download Sessions per Site	20	Controls the number of parallel file downloads. By default, 20 download sessions occur at any time and at most, 20 files download in parallel.
MsSharePoint:File Size Limit in Parallel Download Sessions	2048 (in KB)	Filters out the files to be downloaded in parallel. Only files whose size is less than or equal to the value of this parameter download in parallel.
MsSharePoint:Parallel Files Metadata per Folder	1000	Fetches the metadata for a number of files in a single Graph API call. This is the maximum value possible. This parameter is only applicable when the value of the parameter [MsSharePoint:Enable Parallel Download per Site] is set to FALSE.

Table 5. Parameters supported for Teams

Parameter	Default	Description
MsTeams:Backup Chunk Size	5 (in MB)	Indicates the Chunk Size that can be used to back up—download—files. The Chunk Size *must* be a multiple of 320 KiB (327,680 bytes). Using a Chunk Size that does not divide evenly by 320 KiB results in errors when committing some the files. You can increase this value to increase the data-transfer rate, depending on the network bandwidth. If you exceed a supported rate, the GRAPH API might generate a TIMEOUT exception.
MsTeams:Enable Parallel Download per Team	TRUE	Enables parallel downloads of Teams files for each Teams channel. Otherwise, files download sequentially.
MsTeams:Maximum Parallel Download Sessions per Team	20	Controls the number of parallel file downloads. By default, 20 download sessions occur at any time and at most, 20 files download in parallel.
MsTeams:File Size Limit in Parallel Download Sessions	2048 (in KB)	Filters out the files to be downloaded in parallel. Only files whose size is less than or equal to the value of this parameter download in parallel.

Table 6. Parameters supported for CDP

Parameter	Default	Description
Custom: Synthetic FullRetryCount	2	Controls the number of Synthetic Full Backup job retries after the Synthetic Full Backup job failure. **Note:** The parameter "Custom: Synthetic FullRetryCount" is supported only with NetVault version 13.3

4

Backing up data

- Defining a backup-and-recovery strategy
- Adding patterns to use for exclusion and inclusion
- Performing backups

Defining a backup-and-recovery strategy

The purpose of creating Microsoft 365 backups is to recover a mailbox or site contents that are damaged from media failure or data corruption. Reliable use of backup for recovery requires a strategy that maximizes data availability and minimizes data loss, while accounting for defined business requirements.

A strategy is divided into two pieces: a backup piece and a restore piece.

- The backup piece defines the type and frequency of backups that are required to meet the goals for availability of the database and for minimizing data loss.
- The restore piece defines who is responsible for performing restores, and how restores should be performed to recover from the particular type of damage or failure.

Your backup plan should define at what intervals the backups are performed, how backups are stored, how long backups are retained, and how the backup media are reused.

The plug-in provides the following types of backup:

- **Full Backups only:** You can choose to perform only Full Backups if the backup size is small, the backup window is not an issue, or storage media is not a constraint. In such scenarios, you can schedule Full Backups every night or every N hours depending on the frequency of updates.

  If a failure occurs, the plug-in is only required to restore a single saveset.
- **Full and Incremental Backups:** For quicker backups and minimum use of storage media, you can include Full and Incremental Backups in your strategy. For example, you can schedule Full Backups every Sunday and Incremental Backups every day or every N hours depending on the frequency of updates.

  If a failure occurs, the plug-in is required to restore data from the recent Full Backup and each Incremental Backup in the backup sequence. The restore might take longer if several Incremental savesets have to be restored. For example, if the failure occurs on Saturday, the plug-in is required to restore the Full Backup taken on Sunday and Incremental Backups taken from Monday through Friday.
- **Continuous Data Backups:** Continuous data protection (CDP) occurs when NetVault takes an initial full backup of a selection set and then takes a series of incremental backups to capture the changes of the selection set before it combines the backups into a synthetic full backup.

  NOTE: For Teams, Full Backups include all standard items. Incremental Backups include files, folders, and chat messages.

Adding patterns to use for exclusion and inclusion

From the backup selection tree, you can create and store patterns of mailboxes, mailbox folders, users, sites, and teams that you want to include and exclude for all selected user mailboxes that you back up and for each tenant. When you specify patterns to exclude or include, or both, the plug-in stores them with a Backup Selection Set. When you submit a backup job, you can select the set with the stored patterns. The plug-in then populates the backup list with mailboxes whose folder names meet the specified inclusion and exclusion patterns. There is no limit to the number of patterns that you can specify. Be aware that the plug-in gives priority to exclusions.

To add patterns to use for exclusion and inclusion

1. In the Navigation Pane, click **Create Backup Job**, and click + next to the **Selections** list.
2. In the selection tree, open the applicable client node.
3. Click **Plug-in *for Microsoft 365***, and select **View Inclusion/Exclusion** from the context menu.

   The plug-in adds two subnodes, **Include Patterns** and **Exclude Patterns**, to the **Microsoft 365** node.
4. To specify an exclusion pattern, which takes priority over inclusion patterns, complete the following steps:
   a. Click **Exclude Patterns**, and then select one of the following options:
      - **Add Folder Pattern**

      NOTE: The Add Folder Pattern feature supports only mailbox folders; it does not support OneDrive, SharePoint Online, or Teams.

      - **Add User Pattern**

      NOTE: The Add User Pattern supports exclusion and inclusion of selected users, sites, and teams.

   b. In the **Enter exclude pattern** dialog box, type the pattern to exclude, and click **OK**.

      Use a Portable Operating System Interface (POSIX) regular expression (regex) to create an exclusion pattern. For example, if you want to exclude the **Junk E-Mail** folder, type **Junk***.
5. To specify an inclusion pattern, complete the following steps:
   a. Click **Include Patterns**, and then select one of the following options:
      - **Add Folder Pattern**
      - **Add User Pattern**

   b. In the **Enter include pattern** dialog box, type the pattern to include, and click **OK**.

      Use a POSIX regex to create an inclusion pattern. For example, if you want to select all mailboxes that start with A to G or a to g, type **^[a-gA-G]**.

      NOTE: The exclusion and inclusion feature supports all regex patterns.

   The plug-in lists an informational node with the new patterns below the corresponding subnodes. When you set up a backup job, you can select or clear the applicable patterns.
6. When you are finished, click **Save**, enter a name in the **Create New Set** dialog box, and click **Save**.

   The name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

Performing backups

A backup using the plug-in includes the steps outlined in the following topics:

- Selecting data for a backup
- Setting backup options
- Finalizing and submitting the backup job

Selecting data for a backup

You must use sets—Backup Selection Set, Backup Options Set, Schedule Set, Target Set, and Advanced Options Set—to create a backup job.

Backup Selection Sets are essential for Incremental Backups. Create the Backup Selection Set during a Full Backup, and use it for Full and Incremental Backups. The backup job reports an error if you do not use a Selection Set for the Incremental Backup. For more information, see the *Quest NetVault Administrator's Guide*.

1. In the Navigation pane, click **Create Backup Job**.

   You can also start the wizard from the Guided Configuration link. In the Navigation pane, click **Guided Configuration**. On the **NetVault Configuration Wizard** page, click **Create backup jobs**.

2. In **Job Name**, specify a name for the job.

   Assign a descriptive name that lets you easily identify the job when monitoring its progress or restoring data. The job name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction; however, a maximum of 40 characters is recommended.

3. Next to the **Selections** list, click ✚.

4. In the list of plug-ins, open **Plug-in *for Microsoft 365***, open the tenant node, and complete the applicable following actions:

   - If you are creating a backup job for Outlook, OneDrive, SharePoint Online, or Teams, expand the **Microsoft 365 Apps** node and select the applicable items.
   - If you are creating a backup job for Azure AD, select the **AzureAD** node for users, groups, or service principals.

   NOTE: In a single selection set, you can select items from Microsoft 365 applications or items from Azure AD, but not both. You must restore Microsoft 365 items and Azure AD items in separate selection sets. When editing an existing selection set of Azure AD items, if you want to add Microsoft 365 application items, you must clear the Azure AD items; likewise, for an existing selection set of items from Microsoft 365, if you want to add Azure AD items, you must clear the other Microsoft 365 items.

   - If you are creating a selection set for OneDrive and Mailbox users with a dynamic membership rule set for groups, users will be evaluated for matches with the membership rule. When an attribute changes for a user, all dynamic group rules in the organization are processed for membership changes. Users are added or removed if they meet the conditions for a group. With this approach, newly joined members will be added dynamically to the group overcoming the need to manually modify the selection list. Refer to the following articles that explain how to create dynamic membership rules for users and to set up a rule for a dynamic group in the Azure portal.
   - Create or update a dynamic group in Azure Active Directory
   - Dynamic membership rules for groups in Azure Active Directory

NOTE: The backup fails for inactive Microsoft Teams.

NOTE: The backup fails for shared mailboxes larger than 50 GB that have no assigned licenses.

5 Click **Save**, enter a name in the **Create New Set** dialog box, and click **Save**.

The name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

Setting backup options

The next step involves creating the Backup Options Set or selecting an existing one.

Starting from version 13.1, only the granular restore is available for all aspects of Microsoft 365.

TIP: To use an existing set, in the **Plugin Options** list, select the set that you want to use.

1 Next to the **Plugin Options** list, click ✚.

NOTE: To prevent a pop-up from appearing and causing the WebUI to be unresponsive, before creating the new plug-in set, click **Edit** and save the existing default plug-in options, and then click the **+** icon.

2 In the **Backup Type** section, select the applicable option:

- **Full Backup:** To perform a complete backup of the selected mailbox—including its folders, messages, mailbox settings, and rules—or the selected OneDrive or Teams node, select this option.
- **Incremental Backup:** To back up all data changed in the selected mailbox, OneDrive, or Teams node since the last occurrence of a Full or Incremental Backup, select this option.

NOTE: For Teams, Full Backups include all standard items. Incremental Backups include files, folders, and chat messages.

For more information, see Defining a backup-and-recovery strategy.

- In the **Additional Options** section, if you want to use parallel streams to increase the speed of backup jobs, optionally select **Enable multi-streaming** and then indicate the number of streams.

NOTE: Added the process IDs of Master and child processes in the binary log for easier troubleshooting.

The value that you enter depends on your configuration and network bandwidth. The maximum value is 30.

If the number of mailboxes included in a selection set is less than the specified number of streams, the plug-in automatically adjusts the Number of Streams setting.

3 If you are setting up a backup job for Outlook, in the **Outlook Options** section, select the applicable options:

- **Enable Restartable backup:** If you want to be able to pause a backup and have it resume from the point at which it was stopped, select this option.

This option lets you manually interrupt a backup job; it does not restart a backup job that has failed.

NOTE: The M365 plug-in does not support Restartable Backups.

- **Exclude attachments in backup:** If you want to exclude attachments and inline images from messages, select this option.

  By default, the plug-in includes attachments and inline images in backup jobs. Excluding attachments reduces the size of the backup and increases the speed at which it is processed.

- **Exclude Calendar backup:** If you want to exclude calendars, select this option.

NOTE: Even if calendars and events are included in the backup job, the plug-in excludes event attachments of type Item.

NOTE: Shared calendars will not be backed up.

4 In **Set Name**, specify a name for the set, and click **Save**.

The name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction; however, a maximum of 40 characters is recommended.

Finalizing and submitting the backup job

1 Use the **Schedule**, **Target Storage**, and **Advanced Options** lists to configure any additional required options.

2 Click **Save** or **Save & Submit**, whichever is applicable.

> **TIP:** To run a job that you have already created and saved, select **Manage Job Definitions** on the Navigation pane, select the applicable job, and click **Run Now**.

You can monitor progress on the **Job Status** page and view the logs on the **View Logs** page. For more information, see the *Quest NetVault Administrator's Guide*.

> **IMPORTANT:** The **Restart** feature is available for mailbox-related backup jobs; it is not available for OneDrive-related backup jobs.

Continuous data protection backups

Continuous data protection (CDP) occurs when NetVault takes an initial full backup of a selection set and then takes a series of incremental backups to capture the changes of the selection set before it combines the backups into a synthetic full backup. This protection method reduces time on the backup job, lightens load on the bandwidth, and saves space in. Also, with this protection method no need to maintain separate backup jobs for Full and incremental.

Prerequisite

Performing continuous data protection (CDP) requires that your system uses QoreStor version 7.1.2 or later as a primary storage location.

> **NOTE:** CDP is only available with QoreStor version 7.1.2 or later. Only supported devices appear as available target storage. If you do not have a supported devices, then no devices appear as target options.

Performing continuous backups

The following procedure describes how to back up files continuously using the built-in Plug-in *for Microsoft 365*.

- Selecting data for a continuous backup
- Setting continuous backup options
- Finalizing and submitting the continuous backup job

Selecting data for a continuous backup

Follow the procedure to select the data for a backup

1 In the Navigation pane, click **Create Continuous Backup Job** to start the configuration wizard..

2 In **Job Name**, specify a name for the job.

Assign a descriptive name that lets you easily identify the job when monitoring its progress or restoring data. The job name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction; however, a maximum of 40 characters is recommended.

3 Next to the **Selections** list, click ✚.

4 In the list of plug-ins, open **Plug-in *for Microsoft 365***, open the tenant node, and complete the applicable following actions:

- If you are creating a backup job for Outlook, OneDrive, SharePoint Online, or Teams, expand the **Microsoft 365 Apps** node and select the applicable items.

NOTE: Synthetic Backup does not support Azure Active Directory.

5 Click **Save**, enter a name in the **Create New Set** dialog box, and click **Save**.

The name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

NOTE: The ability to make a copy of a Continuous Data Protection (CDP) backup is available with the built-in Plug-in for Data Copy. Only Full or Synthetic Full Backup whichever is the latest is allowed for Data Copy. Make Sure Data Copy Plug-in's schedule allows the next Synthetic Full Backup to be complete.

Setting continuous backup options

The next step involves creating the Backup Options Set or selecting an existing one.

The As of release 13.1, granular restore is available for all aspects of Microsoft 365.

TIP: To use an existing set, in the **Plugin Options** list, select the set that you want to use.

1. Next to the **Plugin Options** list, click ✚.

   NOTE: To prevent a pop-up from appearing and causing the WebUI to be unresponsive, before creating the new plug-in set, click **Edit** and save the existing default plug-in options, and then click the **+** icon.

2. In the **Additional Options** section, if you want to use parallel streams to increase the speed of backup jobs, optionally select **Enable multi-streaming** and then indicate the number of streams.

   The value that you enter depends on your configuration and network bandwidth. The maximum value is 30.

   If the number of mailboxes included in a selection set is less than the specified number of streams, the plug-in automatically adjusts the Number of Streams setting.

3. If you are setting up a backup job for Outlook, in the **Outlook Options** section, select the applicable options:

   - **Enable Restartable backup:** If you want to be able to pause a backup and have it resume from the point at which it was stopped, select this option.
   - This option lets you manually interrupt a backup job; it does not restart a backup job that has failed.**Exclude attachments in backup:** If you want to exclude attachments and inline images from messages, select this option.

     NOTE: The M365 plug-in does not support Restartable Backups.

     By default, the plug-in includes attachments and inline images in backup jobs. Excluding attachments reduces the size of the backup and increases the speed at which it is processed.
   - **Exclude Calendar backup:** If you want to exclude calendars, select this option.

     NOTE: Even if calendars and events are included in the backup job, the plug-in excludes event attachments of type Item.

     NOTE: Shared calendars will not be backed up.

4. In **Set Name**, specify a name for the set, and click **Save**.

   The name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction; however, a maximum of 40 characters is recommended.

Finalizing and submitting the continuous backup job

Use the **Schedule**, **Target Storage**, and **Advanced Options** lists to configure any additional required options.

To select **Schedule** options, click and complete the following steps

1. In the **Schedule** window, enter the Run at and set the number of hours you want to have in between each incremental job. The minimum value is 1 hour.

NOTE: The synthetic incremental backup, which is executed before the synthetic full backup, must be completed within the designated timeframe. Should it fail to be completed within the specified time, the synthetic full backup will not be initiated. Consequently, only synthetic incremental backups will be performed.

2 From the release 14.1.1 and above, synthetic full backup executes once a week. Select one day and one or more weeks to run a synthetic full backup.

To select **Target Storage** options, click and complete the following steps.

NOTE: CDP is only available with QoreStor version 7.1.2 or later. Only supported devices appear as available target storage. If you do not have a supported devices, then no devices appear as target options.

1 In the Backup Target window, select an available QoreStor device.

2 Click **Save**.

To select the **Advanced Options**, click and complete the following steps.

1 In the Backup life: Continuous, enter the number of synthetic full backups keep before deleting them from the storage device.

2 Optionally, select **Make Backup immutable**.

NOTE: The Discard after a full synthetic backup count selected in Advanced Options also determines the length of time for which a backup is immutable.

3 Click **Save**.

4 On the **Create Continuous Backup Job** page, to submit the job for scheduling, click **Save & Submit.**

5 To save the job definition without scheduling it, click **Save**.

You can view, edit, or run this job from the **Manage Job Definitions** page. This job is not displayed on the **Job Status** page until you submit it.

You can monitor progress on the **Job Status** page and view the logs on the **View Logs** page. For more information, see the *Quest NetVault Administrator's Guide*.

5

Restoring data

- Selecting data for a restore
- Finalizing and submitting the restore job
- Relocating mailboxes and OneDrive accounts during the restore process
- Searching for granular items

Selecting data for a restore

NOTE: Plug-in *for Microsoft 365* does not support restoring Client Secret Keys for service principals.

NOTE: The restore is not supported for guest users in the Teams channel.

1 On the Navigation pane, click **Create Restore Job**.

2 To filter the items displayed in the saveset table, click **Filter** .

The table displays the saveset name (job title and saveset ID), creation date and time, size, and catalog status. By default, the list is sorted by creation date.

3 In the saveset table, select the applicable saveset.

When you select a saveset, the following details are displayed in the **Saveset Information** area: Job ID, job title, server name, client name, plug-in name, saveset date and time, retirement setting, Incremental Backup or not, Archive or not, saveset size, and snapshot-based backup or not.

4 Select one of the following options:

- **Restore All Using Defaults:** To restore using the prepopulated defaults, click this button, and proceed to Step 6.
- **Restore:** To use the **Create Selection Set** page to select the items that you want to restore, click this button and proceed to the next step.

5 On the **Create Selection Set** page, select the data that you want to restore.

NOTE: While relocation is generally supported for Outlook and OneDrive, it is not supported for Teams or Azure AD accounts.

NOTE: If you want to relocate the backup of the publishing portal template of a SharePoint Online site rather than restore it to its original location, create a site for this template and provide the new site's name to the restore job in the **Relocate** option.

NOTE: The plug-in does not support the restore of calendars or events created by a different user.

NOTE: The plug-in does not support the restore of calendar events while relocating a mailbox from one user to the mailbox of another user.

NOTE: Parent level selection requires exclusive selection of supported endpoints; SPO and Teams mixed restore selection should be avoided.

NOTE: After the restoration, the Manage Channel page for the shared channel does not display the Teams it was previously associated with.

6 If you want to increase the speed of the restore job, complete the following steps:

   a On the **Create Selection Set** page, click , and select the **General** tab of the **Microsoft 365 Restore Options** dialog box.

   b Select **Enable multi-streaming**, enter the number of streams, and click **OK**. The value that you enter depends on your configuration and network bandwidth. The maximum value is 10. If the number of items included in a selection set is less than the specified number of streams, the plug-in automatically adjusts the number of streams setting.

7 Proceed to the steps in the applicable topic:

   - If you are creating a restore job for Outlook, complete the next section, Setting restore options for Outlook.
   - If you are creating a restore job for Azure AD, complete the section Setting restore options for Azure AD.
   - If you are creating a restore job for OneDrive, SharePoint Online, or Teams, skip to Finalizing and submitting the restore job.

     NOTE: Plug-in *for Microsoft 365* does not support the restore of on-premises synced users and groups while the sync is enabled.

     When you delete on-premises synced Windows Server Active Directory (AD) users from Azure AD after disabling the AD sync, the users restore as Azure AD users. The administrator then receives an email of duplicate attributes for users that changed to Azure AD users on every sync. If the administrator wants to sync them again as Windows Server AD users, you must delete the users from Azure AD and sync again.

Setting restore options for Outlook

On the **Create Selection Set** page, click , and configure the following parameters on the **Outlook** tab of the **Microsoft 365 Restore Options** dialog box:

- **Restore mailbox to particular folder:** If you want to specify a specific location to restore the selected mailbox folder to, select this option and enter the name of the folder.
- **Restore Mailbox Settings:** To include the settings and rules associated with the selected mailboxes, select this option.
- **Exclude Calendar:** If you want to exclude calendars, select this option.
- **Exclude attachments:** If attachments and inline images were included in the backup, select this option if you want to exclude the attachments and images from the restore.

  IMPORTANT: If attachments are included, you must have a SharePoint Online license to perform a restore to a OneDrive account.

Setting restore options for Azure AD

On the **Create Selection Set** page, click , and configure the following parameters on the **Azure Active Directory** tab of the **Microsoft 365 Restore Options** dialog box:

- **Set password for user(s):** The plug-in assigns the default password `nvbu123*#$`from the **"config"** file to the user. As the administrator, you can use this option to assign the user a different password during restore to match domain policies. This password is set for all users that are restored after being deleted from the Azure AD.
- **Skip assigned license(s):** By default, all licenses that are backed up for the Azure AD user are assigned by a restore operation. If you do not want to assign those licenses, select this option.

- **Delete existing application(s):** By default, the previous application associated with a service principal is not deleted from Azure AD on restoring a service principal. If you want to delete the existing application from Azure AD after restoring the service principal, select this option.

Finalizing and submitting the restore job

The final steps include setting additional options on the Schedule, Source Options, and Advanced Options pages, submitting the job, and monitoring the progress through the Job Status and View Logs pages. These pages and options are common to all NetVault Plug-ins. For more information, see the *Quest NetVault Administrator's Guide*.

1. To save the settings, click **OK**, and then click **Next**.
2. In **Job Name**, specify a name for the job if you do not want to use the default setting.

   Assign a descriptive name that lets you easily identify the job when monitoring its progress. The job name can contain alphanumeric and nonalphanumeric characters, but it cannot contain non-Latin characters. On Windows, there is no length restriction; however, a maximum of 40 characters is recommended.
3. Use the **Schedule**, **Source Options**, and **Advanced Options** lists to configure any additional required options.
4. Click **Save** or **Save & Submit**, whichever is applicable.

   You can monitor progress on the **Job Status** page and view the logs on the **View Logs** page. For more information, see the *Quest NetVault Administrator's Guide*.

Relocating mailboxes and OneDrive accounts during the restore process

Plug-in *for Microsoft 365* supports relocation at the Outlook mailbox and OneDrive user levels. You can relocate data to any plug-in user, including a user from a different tenant.

To relocate mailboxes and OneDrive accounts during the restore process

1. After the prerequisites have been met, click **Create Restore Job**.
2. To filter the items displayed in the saveset table, click **Filter** .
3. In the backup saveset, select the applicable saveset.
4. To use the **Create Selection Set** page to select the mailbox or OneDrive user account that you want to restore, click **Restore**.
5. On the **Create Selection Set** page, select the mailbox or OneDrive user account that you want to relocate, and select **Rename** from the context menu.

IMPORTANT: Even if you entered an email ID earlier, the plug-in does not select the check box for the applicable mailbox or OneDrive user account; you must manually select the mailbox or OneDrive user account.

6. In the **Rename/Relocate** dialog box, enter the new location for the mailbox or OneDrive user account in the **Relocate** box, and click **OK**.
7. Continue with the restore procedure as explained in Setting restore options for Outlook and Finalizing and submitting the restore job.

   The mailbox is restored with its new name to the original location as a subset of the original mailbox.

Relocating a mailbox and a OneDrive account to a user from another tenant

Plug-in *for Microsoft 365* supports cross-tenant relocation for Outlook and OneDrive data. To restore a mailbox or OneDrive data from a user from one tenant to a user from another tenant, see Relocating mailboxes and OneDrive accounts during the restore process.

Searching for granular items

The **Search** option on the **Create Restore Job — Choose Saveset** page lets you find specific files or data items without opening any savesets or browsing through their contents. You can use filenames, regular expressions, or Team names to find the data items that you want to restore, as well as subject, sender, recipient, and received date and time to find email messages. You can also search in Azure AD backup for Azure AD users, groups, or service principals; and search for SharePoint Online savesets by site name using the Name criterion.

To configure or enable the catalog search, select **Catalog Search** from the Navigation pane. The catalog search supports the regular expression syntax used by Elasticsearch. For more information on Elasticsearch, see https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html. For more information on catalog search, see the *Quest NetVault Administrator's Guide*.

To search for items in savesets:

1 On the **Create Restore Job — Choose Saveset** page, click **Search**.

2 In the **Search for files in savesets** dialog box, configure the following options:

- **Search String:** Type the search string.
- **Regular expression search:** To use POSIX regular expressions in the **Search String** box, select this check box.
- **Use legacy search method**: If both cataloged and non-cataloged savesets are included in the search, the plug-in displays this check box.

  If only non-cataloged savesets are included in the search or if **Use legacy search method** is selected, the legacy search is used.

  If only cataloged savesets are included in the search or if **Use legacy search method** is cleared, the catalog search is used.

NOTE: For an Outlook backup, you can filter your search using Subject, Sender, Recipient, and Received Date and Time.

3 To search in one or more specific savesets, select the applicable savesets, and click **Search**.

If you do not select a saveset, all savesets are included in the search. On the **Search Results** page, you can view the savesets that contain the specified files or data items.

4 Select the items you want to restore.

You can only restore items from one saveset.

5 Click **Restore selected items**.

6 Complete Step 6 in Selecting data for a restore.

A

Troubleshooting

This topic describes some common errors and their solutions.

Table 7. Troubleshooting

Issue	Explanation
• Failed to add backup record • Failed to write index of backup to the database These messages indicate that the selected data was backed up, but the job's index information was not properly added by NetVault to its database. Without this index information, the data cannot be properly restored.	**Method 1:** Open the **Manage Devices** page, select the backup media, and click **Scan**. NetVault stores index information for backup jobs in two locations: in the NetVault Database and on the media targeted by the backup. When you scan the backup media, the index information is added to the NetVault Database. To verify that the information was added, open the **Manage Job Definitions** page, and locate the specific job. If you can run the job now, the scan process has corrected the problem. **Method 2:** If the scan has failed, run the backup job again.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.