Arcserve® Cloud Backup for Office 365

User Guide

Version 1.2

arcserve

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve product.

Contents

Chapter 1: Understanding Arcserve Cloud Backup for Office 365

This document provides information about setting up, accessing, and using your Cloud Backup instance.

This section contains the following topics:

Introduction

Arcserve Cloud Backup for Office 365 is a cloud computing service that empowers your organization to complete your data protection needs using a seamless integrated Cloud backup and Disaster Recovery (DR). Arcserve Cloud Backup for Office 365 is a business continuity solution that ensures offsite availability and point in time backup copy of your Office 365 data.

Offered as a cloud to cloud backup solution, Cloud Backup for Office 365 leverages global deduplication, encryption, compression, and WAN-optimized replication for complete security and efficiency of your data protection.

Features

With Arcserve Cloud Backup for Office 365, you can do the following:

- **Backing up Office 365 OneDrive to Arcserve Cloud Backup for Office 365:** OneDrive is a file store hosted on Microsoft Cloud. The OneDrive plan consists of a backup task that lets you specify the following such as OneDrive nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication or deduplication data store where you can store your backup data.

  For more information, see How to Create a Microsoft Office 365 OneDrive Node Backup Plan.

- **Backing up Office 365 Exchange Online to the Cloud Backup instance:** Exchange Online is an email application hosted on Microsoft Cloud. Create a plan to protect Exchange Online mail items such as mails, calendar items, contacts, and others using Microsoft Cloud. The Exchange Online plan consists of a backup task that lets you specify the following such as Exchange Online nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication or deduplication data store where you can store your backup data.

  For more information, see How to Create an Exchange Online Plan.

- **Backing up Office 365 SharePoint Online to the Cloud Backup instance:** SharePoint Online is a portal management application hosted on Microsoft Cloud. Create a SharePoint Online plan to protect SharePoint Online list items such as document library, list library, and others using Microsoft Cloud. The SharePoint Online plan consists of a backup task that lets you specify the following such as SharePoint Online nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication data store or deduplication data store where you can store your backup data.

  For more information, see How to Create a SharePoint Online Backup Plan.

- **Backing up Office 365 Teams to the Cloud Backup instance:** Microsoft Teams is a business communication chat based platform. Backup and restore of Microsoft Teams data is enabled using Exchange Online and SharePoint Online. Arcserve UDP provides the backup of messages (chats) and files shared across the private, public, and group channels. Whenever you create a private, public, and group channel in Microsoft Teams, a SharePoint Online site gets created for it automatically. This SharePoint Online site has a default

document library folder, in which all the files shared across all the conversations get saved automatically. You can also customize the permissions and security options for sensitive information.

For more information, see Managing Microsoft Teams Backup and Restore.

What Arcserve Cloud Backup for Office 365 Provides?

Arcserve Cloud Backup for Office 365 provides the following:

- Arcserve UDP Console or RPS server.
- URL to access the Arcserve UDP Console.
- User name and password for the Arcserve UDP Console account available in the Cloud Backup instance.

  Important! The deduplication datastore in Cloud Backup Office 365 has a randomly generated encryption password by default. You must modify the encryption password in the first Cloud Backup login as Arcserve cannot restore the default password. We recommend to keep the newly created password safe as you need the password later to perform tasks such as importing the datastore and running a consistency check on the deduplication datastore. You can modify the newly created password later from datastore setting if the datastore is not deleted from the Cloud instance.

Prerequisites to Access Arcserve Cloud Backup for Office 365

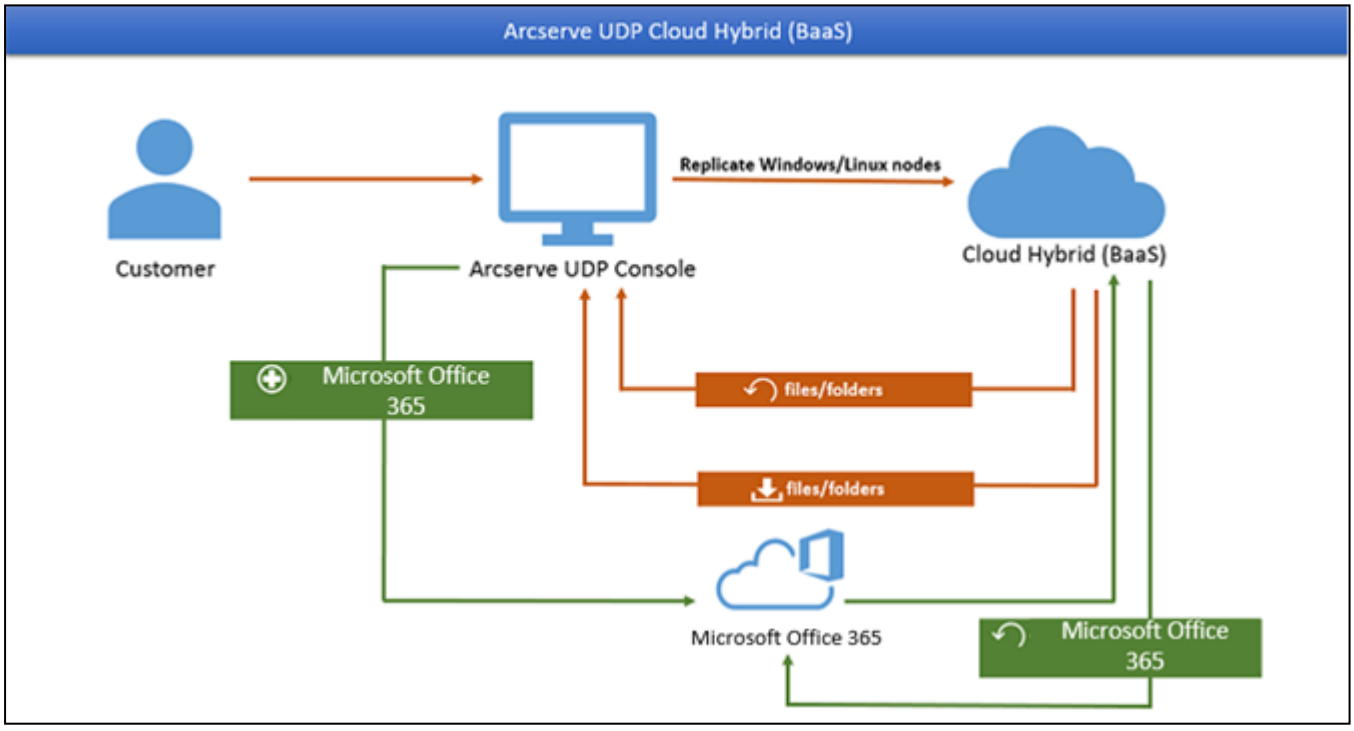
Before accessing the Cloud backup instance, verify the following prerequisites:

- An email from Arcserve Support, which contains the following details:
  - URL to the Arcserve UDP Console
  - Host name (Node name)
  - User name and Password for Cloud backup

Chapter 2: Using Arcserve Cloud instance for Backups

Arcserve Cloud Backup for Office 365 lets you perform the following functions:

- Create a Plan to protect Microsoft Office 365 Exchange Online, SharePoint Online, OneDrive, or Microsoft Teams data to the Cloud backup instance. For more information, see How to Protect Microsoft Office 365 Data.
- Restore Office 365 Exchange Online, SharePoint Online data from the Cloud backup instance to Office 365 Server. For more information, see How to Restore Microsoft Office 365 Data.
- Backup and restore Microsoft Teams data using Exchange Online and SharePoint Online. For more information, see Managing Microsoft Teams Backup and Restore.
- Export Microsoft Office 365 OneDrive data from the Cloud backup instance to local disk. For more information, see Define the Restore Options.



This section contains the following topics:

Create a Plan to protect Microsoft Office 365 data to Arcserve Cloud

Exchange Online

The Microsoft Office 365 Exchange Protection is used to backup and restore Microsoft Exchange Online mail folders and items. To protect your Exchange online content, you need to create a Plan.

For more information about creating plans using the Arcserve UDP 8.0, see How to Create an Exchange Online Plan.

SharePoint Online

The Microsoft Office 365 SharePoint Protection is used to backup and restore Microsoft SharePoint Online site and list item. The SharePoint Online is one of the major products in Microsoft Office 365. To protect your SharePoint content, you need to create a Plan.

For more information about creating plans using the Arcserve UDP 8.0, see How to Create a SharePoint Online Backup Plan.

OneDrive

The Microsoft Office 365 OneDrive Protection is used to backup and restore Microsoft OneDrive file and folder items. The OneDrive is one of the major products in Microsoft Office 365. To protect your OneDrive content, you need to create a Plan.

For more information about creating plans using the Arcserve UDP 8.0, see How to Create a Microsoft Office 365 OneDrive Node Backup Plan.

Note: To view the build number, log into **Arcserve UDP Console**, and then click **Help > About**.

Microsoft Teams

Data backup and restore support is enabled for MS Teams, which is a business communication chat based platform. For more information on using Arcserve UDP 8.0 to protect Microsoft Teams Data, see Managing Microsoft Teams Backup and Restore.

How to Create an Exchange Online Backup Plan

Exchange Online is an email application hosted on Microsoft cloud. To protect your Exchange Online mail items (Mails, Calendar items, Contacts, and so on) from Microsoft cloud, you need to create a plan. The plan for Exchange Online consists of a backup task. This backup task lets you specify the Exchange Online nodes you want to protect, the backup destination, and the backup schedule.

What To Do Next?

1. Review the Prerequisites and Considerations
2. Create an Exchange Online Backup Plan
3. (Optional) Perform a Manual Backup
4. Configuration for Multi-Factor Authentication

Review the Prerequisites and Considerations

Prerequisites:

For Backup account:

- Use a backup service account with Global admin permissions.
- Add impersonation permission for backup user to the Exchange Online backup account to connect the Exchange Online organization, perform backups and restore.

  Note: If you do not add the backup account to the Discovery Management role group and do not assign the Application Impersonation permission, backup fails.

- Associate the Backup user account with one exchange online mailbox.
- If Modern Authentication is set on the Office 365 tenant, the version of Arcserve UDP must be 7.0.4455 Update 2 Build 675 or higher. If the version needs an upgrade to the required build, contact the Arcserve support.

Considerations:

- If modern authentication is set on O365 tenant and Arcserve UDP is recently upgraded to support it, the existing Exchange online jobs needs to be reconfigured with modern authentication related settings, which is described in the Modern Authentication section.

Add Impersonation Permission for Backup User

Add the backup account to the Discovery Management role group and assign Application Impersonation permission to it.

Follow these steps:

1. Add the required role and group using any one of the following ways:

   Using Office 365 portal

a. Log on Office 365 portal as an Administrator or with an account that has Global Admin permissions.

   The **ExchangeAdmin center** page opens.

b. Go to **permissions** and double-click **Discovery Management** from the **Add** drop-down.

   The **Discovery Management** dialog opens.

   Note: Member of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

c. Under **Roles**, click **+** to add the ApplicationImpersonation role.

   The **Discovery Management** dialog opens.

d. Select **ApplicationImpersonation** from the **Display Name** drop-down.

   Note: The ApplicationImpersonation role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.

e. Under **Members**, click **+** to add the backup account as a member.

   A dialog appears.

f. Select the backup account from the **Name** drop-down and click **OK**.

   The selected backup account is displayed under **Members** on the **Discovery Management** dialog.

g. Click **Save**.

The ApplicationImpersonation role and Members group are added to the Exchange Online backup account.

Modern Authentication

This section provides the following information about Modern Authentication for Office 365 backups.

Prerequisites

After UDP is upgraded to support Modern Authentication, make sure to do the following:

- Assign the following roles to the account you are using to run this patch
  - Global Admin
  - Compliance Administrator
  - Company Administrator

  1. To assign roles, log into the Azure portal.
  2. Navigate to **Azure Active Directory** > **Roles and Administrators** > **Your Role**.
  3. Click **Add Assignments** to add roles and role assignments such as Global Admin, Compliance Administrator (role), and Company Administrator (role assignments).
- Add users to Exchange Online Discovery Management and assign **ApplicationImpersonation** role.

  1. Go to https://outlook.office365.com/ecp, and then navigate to **Permissions** > **Admin Roles** > **Discovery Management**.
  2. Add the **ApplicationImpersonation** role.
  3. Add the user to the **Discovery Management** role group.

Troubleshooting

When creating an application in Azure, if the Backup configuration failed error message appears, do the following:

- Verify and assign the Compliance Administrator role. For more information, see Prerequisites.
- Verify and assign the Company administrator role. For more information, see Prerequisites.

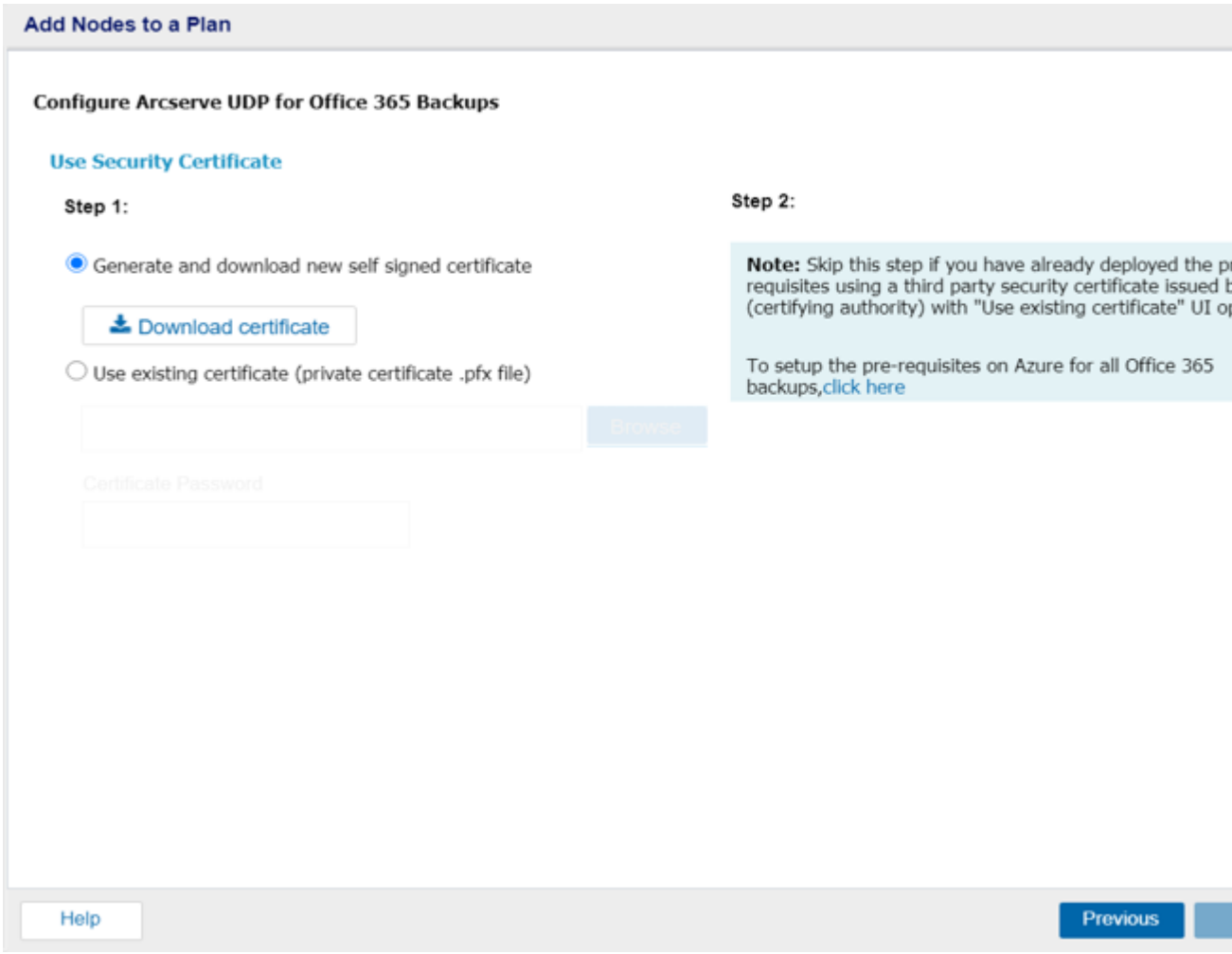
How to Use Security Certificates

You can use the security certificate in one of the following ways:

Method 1: Generate and download new self-signed certificate

To authenticate using a new self-signed certificate, follow these steps:

1. Under Step 1, to allow UDP to generate a new self-signed certificate, select **Generate and download new self-signed certificate**. To save the certificate on your local computer, click the **Download certificate button**.



2. Under Step 2, to upload and set up the application in the Azure portal, follow the steps in the click here link.

Method 2:Use existing certificate

To authenticate using an existing certificate, follow the steps in the click here link:

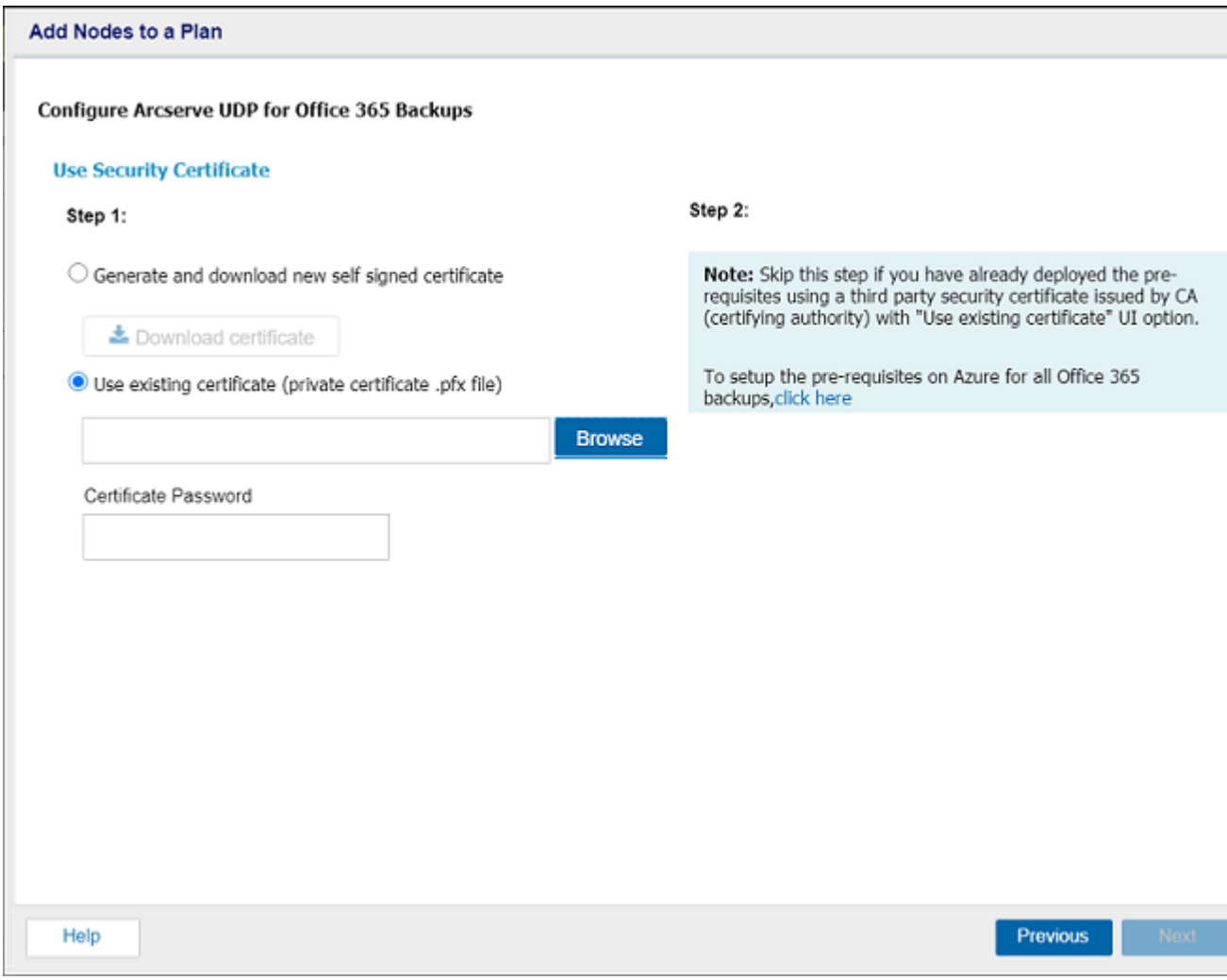
Notes:

- When this option is selected, you are expected to have your own Self signed Certificate (.cer file) and Private key certificate files (.PFX file with password), or certificates provided by CA.
- To setup the prerequisites on Azure for all Office 365 backups, see Review the Prerequisites and Considerations. Skip this step if you have already deployed the prerequisites.

After performing the steps in the click here link, follow these steps from the UDP Console:

1. Browse for the Private Key certificate [.PFX file] and enter the password.
2. Click **Next** to proceed for Node registration.

   Note: If the same certificate is used for multiple plan creations, it is enough to upload the certificate only once in the Azure portal.



How to Upload Certificates in Azure and Assign Global Permissions

Follow these steps:

1. To upload certificate in Azure, sign into the Azure portal
2. Search for **App registrations**.
3. Create an application with a name such as *UDP365*.
4. Copy and save the **Application (client) ID** attribute for future use.
5. Navigate to **Certificates & secrets**.
6. Browse for new or existing certificate [.cer file] and then click **Upload Certificate**.
7. Sign out and close the Azure portal.
8. Download the following PowerShell script:

   https://s3.amazonaws.com/cloud_config/AssignGlobalAdminRoleToADApplication.ps1
9. Run the script to grant application permissions to Arcserve UDP.

   Use the following syntax for the PowerShell script:

   ./AssignGlobalAdminRoleToADApplication.ps1 <AzureAD_applicationID>

   Note: To run the script from PowerShell, use PowerShell version 5.1 or greater.

Create an Exchange Online Backup Plan

A backup plan includes a backup task that performs a backup of Exchange Online mail data items (Mails, Calendar items, Contacts, so on) and stores data either at a non-deduplication data store or deduplication data store. Each task consists of parameters that define the source, destination, schedule, and other backup details.

Follow these steps:

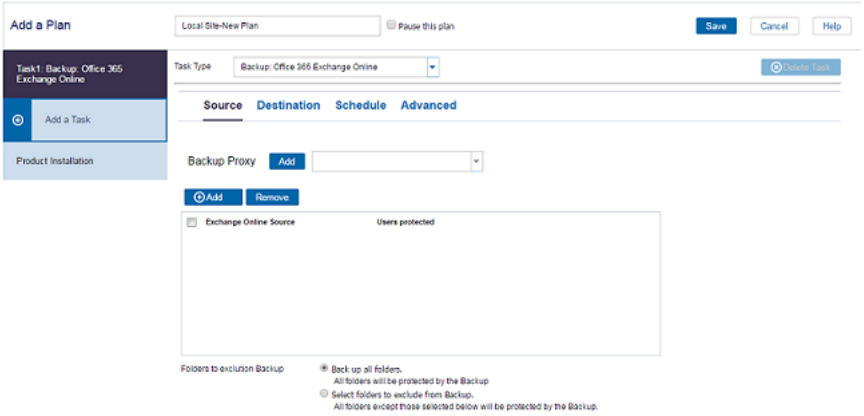
1. Click the **resources** tab on the Console.
2. From the left pane, navigate to **Plans**, and click **All Plans**.

   If you have created plans earlier, those plans are displayed on the center pane.
3. On the center pane, click **Add a Plan**.

   The **Add a Plan** dialog opens.
4. Enter a plan name.
5. (Optional) Select the **Pause this plan** check box.

   The plan does not run until you clear the check box to resume the plan.

   Note: If a plan is paused, then any in-progress job is not paused but all corresponding scheduled jobs associated with that plan are paused. However, you can manually run a job. For example, you can manually run backup job and replication job for a node even if the respective plan is paused. In such case, the following task to the on-demand (manual) job does not run. For example, there is a replication task after an on-demand backup job, the replication job does not run for the on-demand backup job. You need to manually run the replication job. When you resume the plan, the pending jobs do not resume immediately. After you resume the plan, the pending jobs run from the next scheduled time.
6. From the **Task Type** drop-down list, select **Backup: Office 365 Exchange Online**.



Now specify the Source, Destination, Schedule, and Advanced details.

Specify the Source

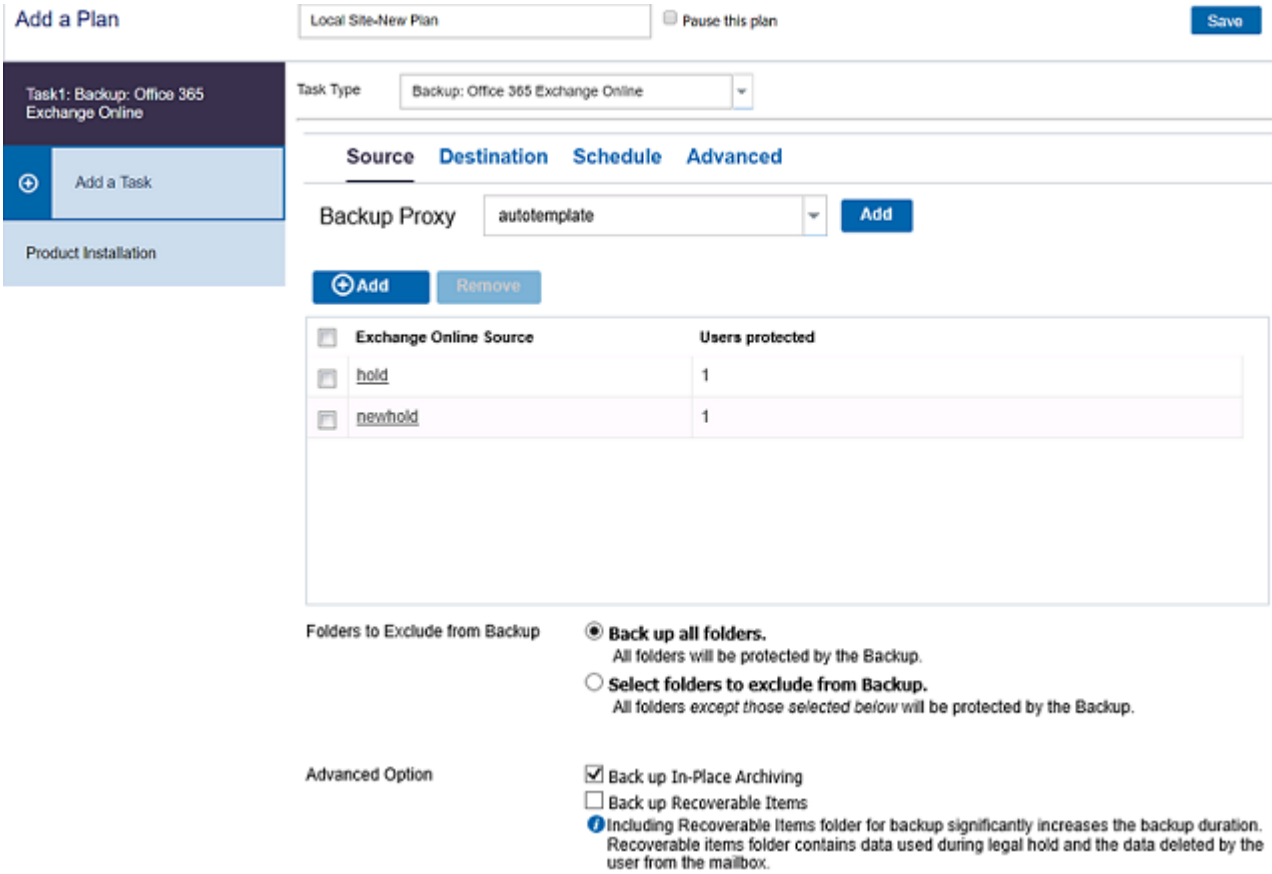
The Source page lets you specify the Exchange Online source nodes that you want to protect. You can select more than one Exchange Online source nodes in a plan. If you have not added any nodes to the Console, you can add Exchange Online source nodes from the Source page.

Note: You can save a plan without adding any source nodes but the plan is not deployed unless you add any nodes.

You can also manage Exchange Online nodes using Public folder Mailbox Support for Exchange Online Protection.

Follow these steps:

1. Click the **Source** tab.



2. From the drop-down list, select the Backup Proxy.
3. Add Exchange Online node using one of the following options:
   - Click Add and then click Select Source to Protect in Arcserve UDP.

     The Add Nodes to Plan dialog is displayed.

a. Select a node and click Connect.

Note: You can also search for the Exchange Online nodes that you want to protect in Search.

b. Select the **Protect all of the office 365 Exchange Sources** check box to protect all the Exchange Online accounts across all the pages.

Note: To add all the Exchange Online accounts to the protected list, you may click the right (>) arrow.

The Exchange Online accounts that you selected are added.

- Click Add and then click Add Exchange online Source in Arcserve UDP.

Note: Unlike other nodes, you cannot add the Exchange Online node from All Nodes page. You can add an Exchange Online node only in a plan or when you modify a plan.

Multiple Exchange online nodes can use the same user account (service account) of Exchange Online.

After you click Add Nodes, you can select Basic Authentication or Modern Authentication to add the Exchange node by plan.

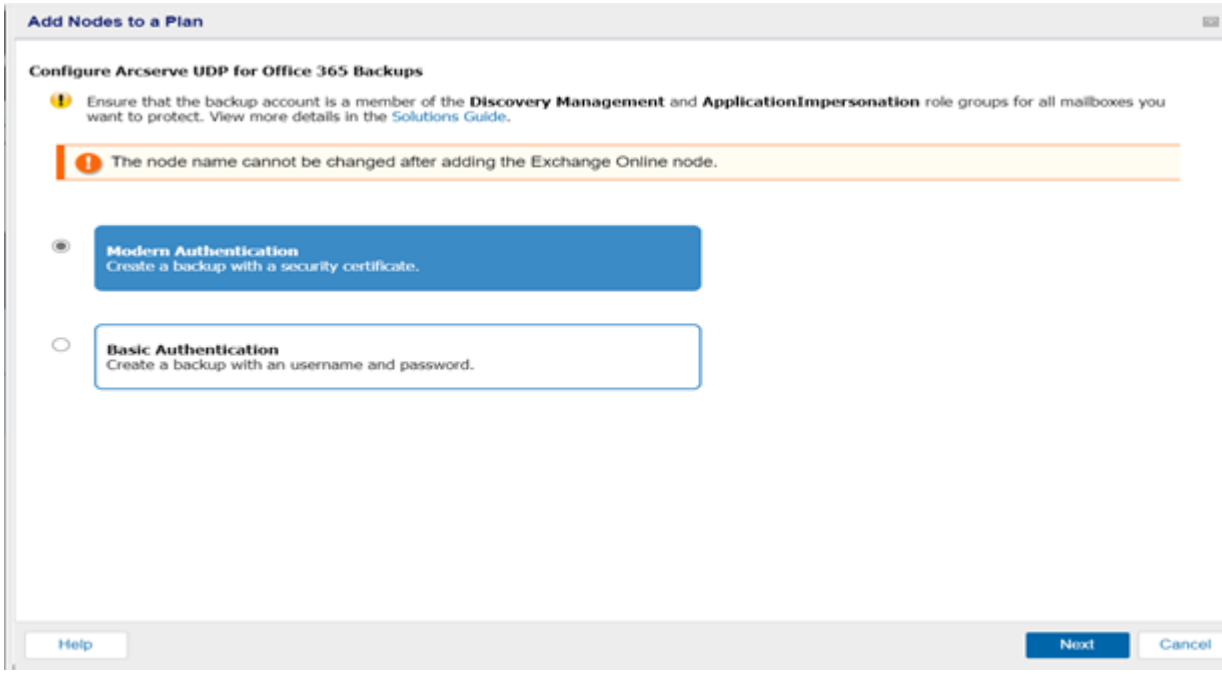
For Basic Authentication, provide the following information:

- Node name
- User name
- Password

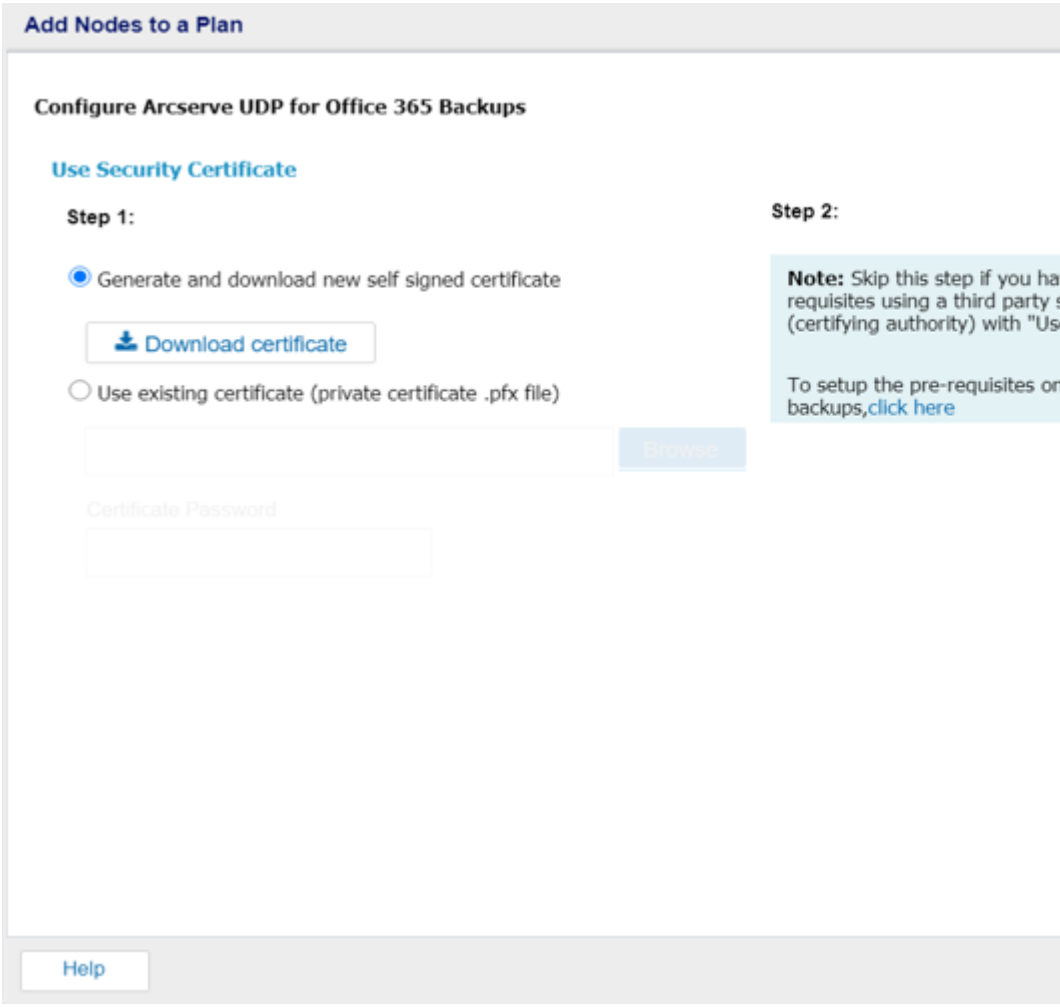
For Modern Authentication, provide the following information:

- Node name
- Application ID
- User name

Note: Exchange online node names cannot change after creating the node.

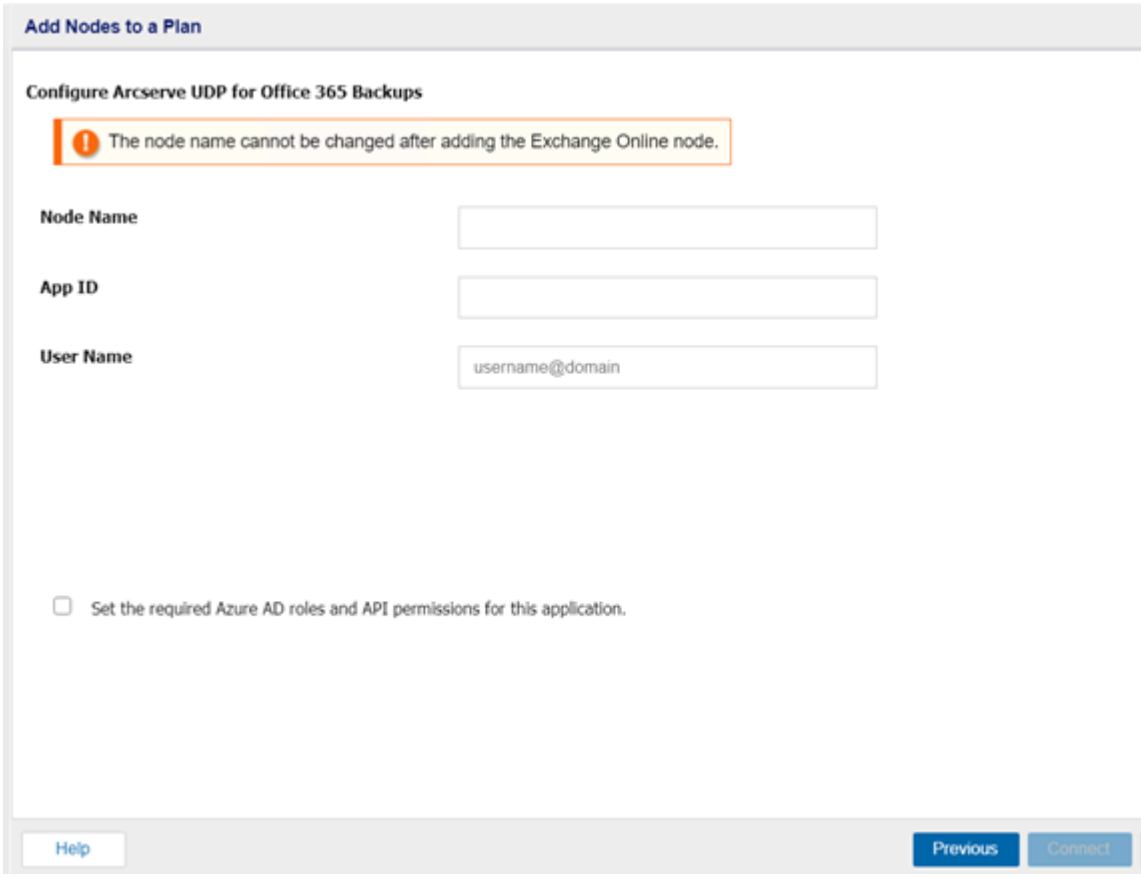


a. To authenticate the UDP application with security certificates, see How to Use Security Certificates.



b. After you upload the certificate to the Azure portal, in the UDP console provide Node Name, Application ID, and Username. To accept the AzureAD Admin consent, select the checkbox, and then click **Connect** to register the node.

   Note: Enter the user name of Exchange Online backup account that meet the prerequisites in Admin Username.



Updating or changing the user accounts may change the number of protected mailboxes. You need to verify that the new or updated service accounts have impersonation rights for the mail-boxes to be protected.

c. Select the Exchange Online accounts that you want to protect and click the right arrow (>) to move them to the protected list.

Note: Select the **Protect all of the Office365 Exchange Source** check box to protect all the Exchange Online accounts across all the pages. To add all the exchange online accounts listed on the page to the protected list, click the right (>) arrow.

d. Click **Save**.

The Exchange Online accounts that you selected are added.

4. On the Source tab, go to **Folders to Exclude from Backup**, and then select the desired check box.
5. From the Advanced option, select the desired check box.
   - To allow Exchange Online Protection support Archiving Mailbox, select the **Backup up In-Place Archiving** check-box.

Note: For more information about Archiving Mailbox, refer to the link.

- Select the **Backup up Recoverable items** check box to enable to protect the mailbox that enables the In-Place Hold or Litigation Hold feature.

  Note: For Archiving In-Place Hold and Litigation Hold for Exchange Online, refer to the link.

Note: To enable both the features in the mailbox at the same time to back up the recoverable items in Archiving mailbox, select both the options **Backup up In-Place Archiving** and **Backup up Recoverable items**.

Specify the Destination

The destination is a location where you store the backup data. You must at least specify the destination to save the plan.

Follow these steps:

1. Click the **Destination** tab.
2. Select the **Arcserve UDP Recovery Point Server** option. **Arcserve UDP Recovery Point Server** specifies that the backup destination is a recovery point server. If you select this option, the data is stored as recovery points. You cannot store data as recovery sets.
3. Provide the following details:
    a. Select a recovery point server.
    b. Select a non-deduplication or deduplication data store. The list displays all the data stores created on the specified recovery point server.
    c. Provide a session password. The session password is optional when the backup destination is an unencrypted RPS data store.
    d. Confirm the session password.

The destination is specified.

Specify the Schedule

The Schedule page lets you define a schedule for Backup, Merge, and Throttle functions to repeat at specific intervals. After you define a schedule, the jobs run automatically per the schedule. You can add multiple schedules and can provide retention settings.

A Backup Schedule refers to regular schedule that is repeated multiple times a day based on the number of hours or minutes you select. Besides the regular schedule, a backup schedule also provides options to add daily, weekly, and monthly schedules.

Note: For more information on scheduling and retention settings, see Understanding Advanced Scheduling and Retention.

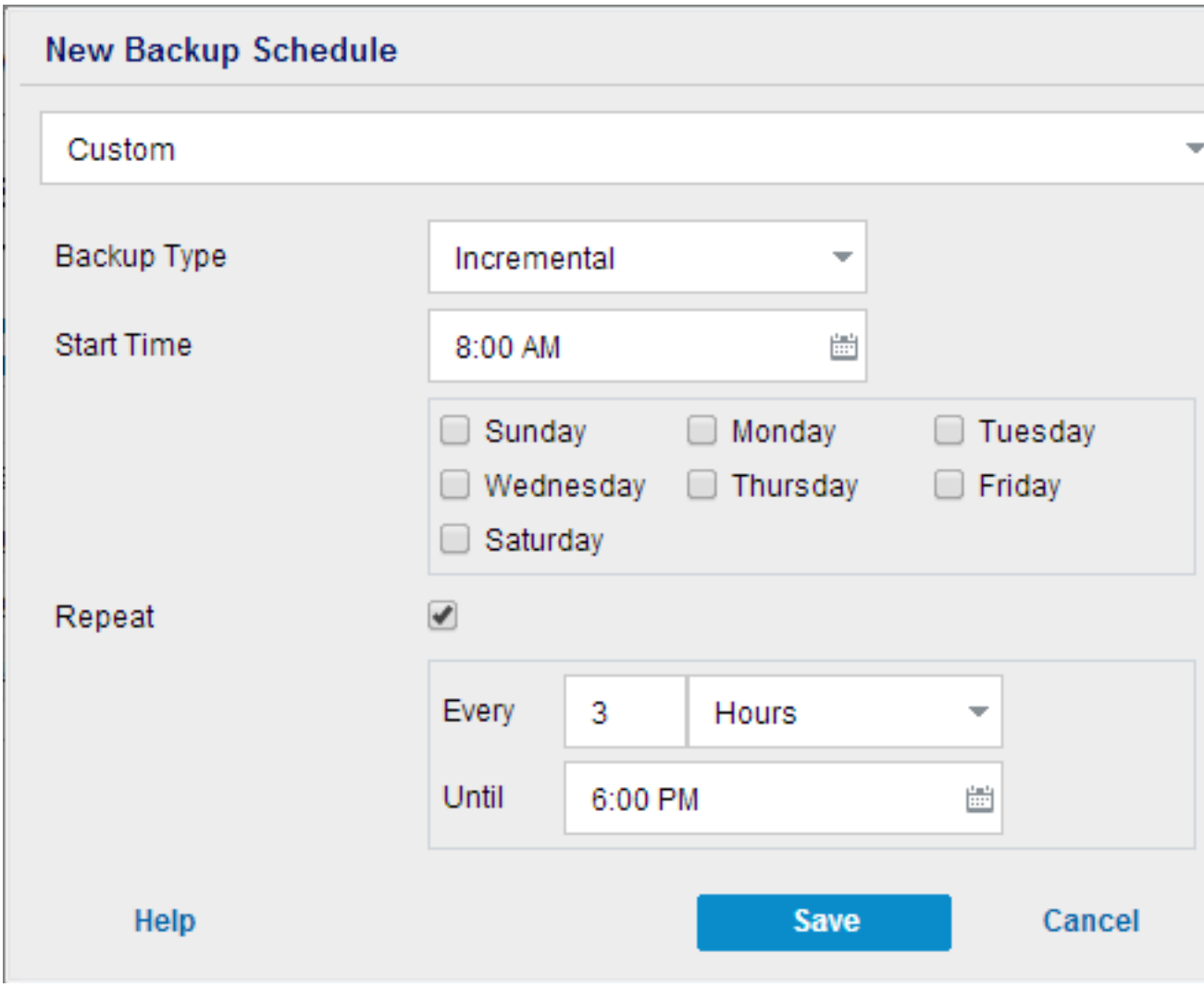
Follow these steps:

1. Add backup, merge, and throttle schedules.

   Add Backup Schedule

   a. Click **Add** and select **Add Backup Schedule**.

      The **New Backup Schedule** dialog opens.



b. Select one of the following options:

Custom

Specifies the backup schedule that repeats multiple times a day.

Daily

Specifies the backup schedule that occurs once a day. By default, all the days of the week are selected for Daily backup. If you do not want to run the backup job on a specific day, clear the check box for that day of the week.

Weekly

Specifies the backup schedule that occurs once a week.

Monthly

Specifies the backup schedule that occurs once a month.

c. Select the backup type.

Full

Determines the backup schedule for Full Backups. As scheduled, Arcserve UDP performs a full backup of all used blocks from the source machine. A full backup typically consumes time depending on the backup size.

Incremental

Determines the backup schedule for Incremental Backups.

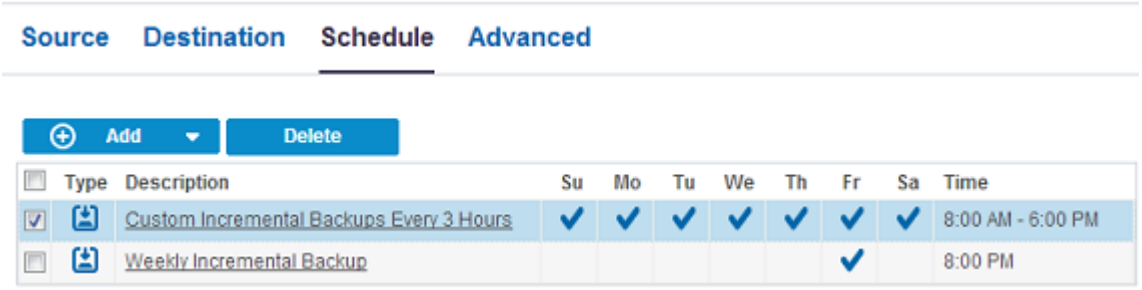
As scheduled, Arcserve UDP incrementally backs up only those blocks that have changed after the last successful backup. The advantages of Incremental Backups are that the backup is a fast backup and it produces a small backup image. This is the most optimal way to perform a backup.

d. Specify the backup start time.

e. (Optional) Select the **Repeat** check box and specify the repeat schedule.

f. Click **Save**.

The Backup Schedule is specified and appears on the **Schedule** page.



Add Merge Schedule

a. Click **Add** and select **Add Merge Schedule**.

The **Add New Merge Schedule** dialog opens.

b. Specify the start time to start the merge job.

c. Specify **Until** to specify an end time for the merge job.

d. Click **Save**.

The Merge Schedule is specified and appears on the **Schedule** page.

Add Throttle Schedule

a. Click **Add** and select **Add Throttle Schedule**.

The **Add New Throttle Schedule** dialog opens.

b. Specify the throughput limit in MB per minutes unit.

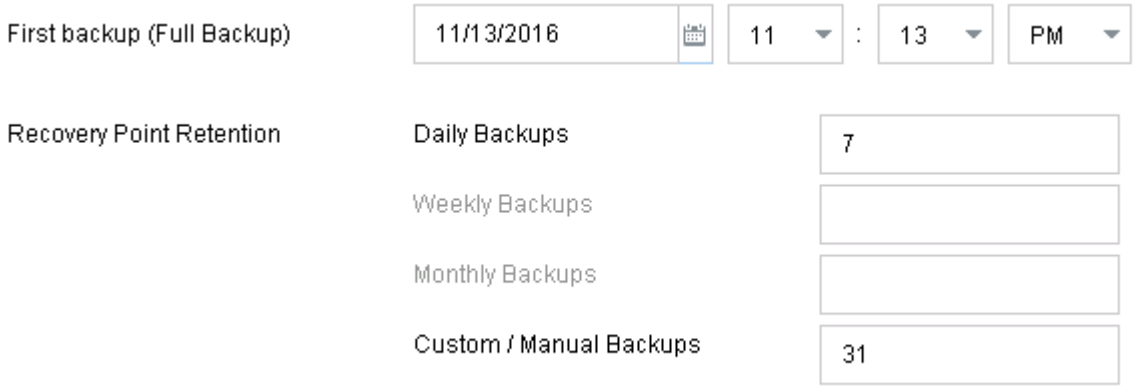
c. Specify the start time to start the backup throughput job.

d. Specify **Until** to specify an end time for the throughput job.

e. Click **Save**.

The Throttle Schedule is specified and displayed on the **Schedule** page.

2. Specify the start time for the scheduled backup.



3. Specify the recovery points retention settings for Custom, Daily, Weekly, and Monthly schedule.

   These options are enabled if you have added the corresponding backup schedule. If you modify the retention settings on this page, the changes are reflected on the **Backup Schedule** dialog.

   The schedule is specified.

Understanding Advanced Scheduling and Retention

The scheduling option lets you specify a Custom schedule or a Daily / Weekly / Monthly schedule, or both the schedules. In the Custom schedule, you can configure the backup schedule for each day of the week and you can add up to four backup schedules each day. You can select a specific day of a week and create a time window to define when to run backup and at what frequency.

Schedule	Supported Job	Comments
Backup	Backup job	Define time windows to run backup jobs.
Backup throttling	Backup job	Define time windows to control the backup speed.
Merge	Merge job	Define when to run merge jobs.
Daily schedule	Backup job	Define when to run daily backup jobs.
Weekly schedule	Backup job	Define when to run weekly backup jobs.
Monthly schedule	Backup job	Define when to run monthly backup jobs.

You can also specify the retention settings for the recovery points.

Note: Set the retention settings within each plan to control how data for the nodes assigned to that plan are retained at the target data store.

Schedules for Daily / Weekly / Monthly backups are independent to the Custom schedule, and each other. You can configure only to run Daily backup, Weekly backup or Monthly backup, without configuring the Custom schedule.

Backup Job Schedule

You can add four time windows per day in your backup schedule. A valid time window is from 12:00 AM until 11:59 PM. You cannot specify a time window such as 6:00 PM to 6:00 AM. In such cases, you have to manually specify two different time windows.

For each time window, the start time is inclusive, and the end time is exclusive. For example, you have configured to run Incremental Backup every one hour between 6:00 AM and 9:00 AM and the backup will start at 6:00 AM. This means the backup runs at 6:00 AM, 7:00 AM, 8:00 AM, but NOT at 9:00 AM.

Note: If you want to run the backup job repeatedly until the end of day, set the schedule until 12:00 AM. For example, to run backup job every 15 minutes for the entire day, set the schedule from 12:00 AM to 12:00 AM, every 15 minutes.

Backup Throttle Schedule

Backup throttle schedule lets you control the backup throughput speed that in turn controls the resource usage (disk I/O, CPU, network bandwidth) of the server being backed up. This is useful if you do not want to affect the server performance during business hours. You can add four time windows per day in your backup throttle schedule. For each time window, you can specify a value, in MB per minute. This value is used to control the backup throughput. Valid values are from 1 MB/minutes to 99999 MB/minutes.

If a backup job extends its specified time, then the throttle limit adjusts according to the specified time window. For example, you have defined the backup throttle limit as 500 MB/minute from 8:00 AM to 8:00 PM, and 2500 MB/minute from 8:00 PM to 10:00 PM. If a backup job starts at 7:00 PM and it runs for three hours, then, from 7:00 PM to 8:00 PM the throttle limit is 500 MB/minute and from 8:00 PM to 10:00 PM the throttle limit is 2500 MB/minute.

If you do not define any backup schedule and backup throughput schedule, the backup runs as fast as it can.

Merge Schedule

Lets you merge recovery points based on the provided schedule.

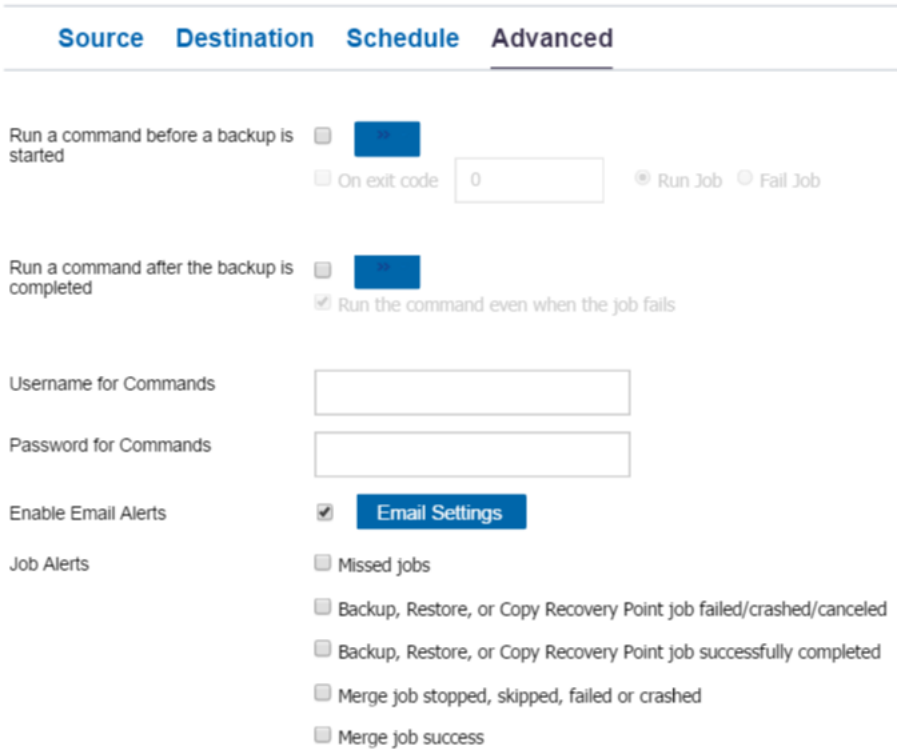
Consider the following points for the merge job:

- At any given time only one merge job can run for a node.
- If a merge job starts, it has to complete before the next merge job can start. This means, if one or more sets of recovery points are merged, new recovery point cannot be added to this merge process, until the merge process of the current set of recovery point completes.
- If a merge job is processing more than one set of recovery points (for example set [1~4], set [5~11], and set [12~14]; they are three sets), recovery point server processes these sets one by one.
- If a merge job is resumed after a pause, the job detects at which point it is paused and resumes the merge from the break-point.

Specify the Advanced Settings

The **Advanced** tab lets you specify some advanced settings for the backup job. The advanced settings include providing the location of any scripts, and email settings.

The following image displays the **Advanced** tab:



Follow these steps:

1. Specify the following details.

   Run a command before a backup is started

   Lets you run a script before the backup job starts. Specify the path where the script is stored inside the proxy node. Click **On exit code** and specify the exit code for **Run Job** or **Fail Job**. **Run Job** indicates that the backup job continues when the script returns the exit code. **Fail Job** indicates that the backup job stops when the script returns the exit code.

   Run a command after a backup is completed

   Lets you run a script after the backup job is completed. Specify the complete path where the script is stored.

   Run a command even when the job fails

If this check box is selected, the script specified in **Run a command after a backup is completed** is executed even when the backup job fails. Otherwise, that script is executed only when backup job completes successfully.

Username for Commands

Lets you specify the username to run the commands.

Password for Commands

Lets you specify the password to run the commands.

Enable Email Alerts

Lets you enable email alerts. You can configure email settings and specify the types of alerts that you want to receive in an email. When you select this option, the following options are enabled for your selection.

Email Settings

Lets you configure the email settings. Click **Email Settings** and configure the email server and proxy server details. For more information about how to configure Email Settings, refer to Email and Alert Configuration.

Job Alerts

Lets you select the types of job alert emails that you want to receive.

2. Click **Save**.

Note: When you select a node as a backup source or backup proxy, Arcserve UDP checks whether the agent is installed on proxy node and if it is the latest version. Arcserve UDP then displays a verification dialog that lists all the nodes that either have an outdated version of the agent or does not have the agent installed. To install/upgrade the agent on these nodes, select the installation method and click **Save**.

The changes are saved and a green checkmark appears next to the task name. The plan page closes.

Note: If you have to add another task, you must select the plan from the **resources** tab and modify the plan. To modify the plan, click the plan from the center pane. The plan opens and you can modify it. You may add the **Copy Recovery Point**, **Copy to Tape**, **Replicate**, and **Replicate from a remote RPS** tasks as follow up tasks.

The plan is automatically deployed to the proxy server node.

The exchange online backup plan for the proxy server is created. The backup runs per the schedule that you have configured on the **Schedule** tab. You can also perform a manual backup at any time.

(Optional) Perform a Manual Backup

Typically, backups are performed automatically and are controlled by the schedule settings. In addition to the scheduled backup, a manual backup provides you the option to back up your nodes on a need basis. For example, if you have a repeat schedule for Full, Incremental, and Verify backups and you want to make major changes to your machine, you should perform an immediate manual backup without waiting for the next scheduled backup to occur.

Follow these steps: to perform a manual backup of Exchange Online nodes

1. From the Console, click the **resources** tab.
2. From the left pane, navigate to **Nodes**, and click **All Nodes**.

   The Exchange Online nodes are displayed in the center pane.
3. Select the Exchange Online nodes (for example, Mail-box@<organizationname.com>) that you want to backup and that has a plan assigned to it. The node name is the account that is used when adding the Exchange Online node and connecting it.
4. On the center pane, click **Actions**, **Backup Now**.

   The **Run a backup now** dialog opens.
5. Select a backup type and optionally provide a name for the backup job.
6. Click **OK**.

   The backup job runs.

Follow these steps: to perform a manual backup of an Exchange Online plan

1. From the Console, click the **resources** tab.
2. From the left pane, navigate to **Plans**, and click **All Plans**.

   The Exchange Online backup plans are displayed in the center pane.
3. Select the plan that you want to backup and that has a plan assigned to it.
4. On the center pane, click **Actions**, **Backup Now**.

   The **Run a backup now** dialog opens.
5. Select a backup type and optionally provide a name for the backup job.
6. Click **OK**.

   The backup job runs.

   The manual backup is successfully performed.

Configuring for Multi-Factor Authentication

When an organization has multi-factor authentication (MFA) with Basic Authentication enabled for the users, the Office 365 backup plan needs to be configured using App Password for the backup service account.

Perform the following steps to configure Arcserve UDP to Support multi-factor authentication:

1. Enable the backup service account to Set app password
2. Create app password for the backup service account

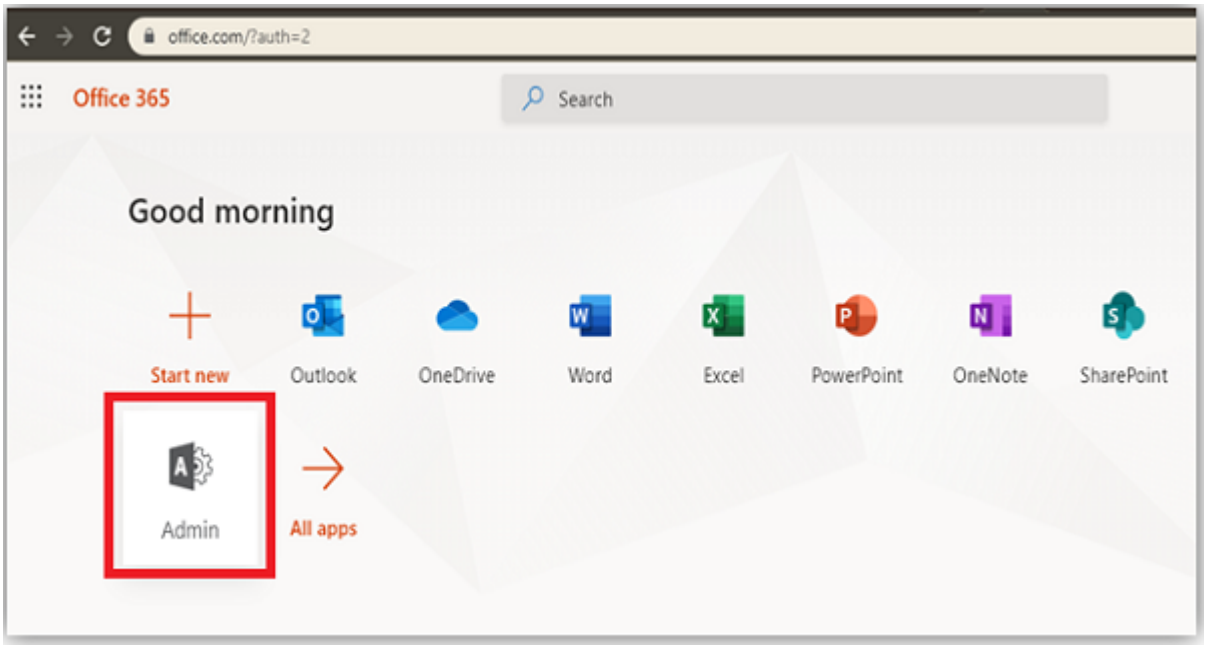
Note: MFA authentication (App password) is currently supported for O365 Exchange Online and SharePoint Online backups only.

Enable the backup service account to Set app password

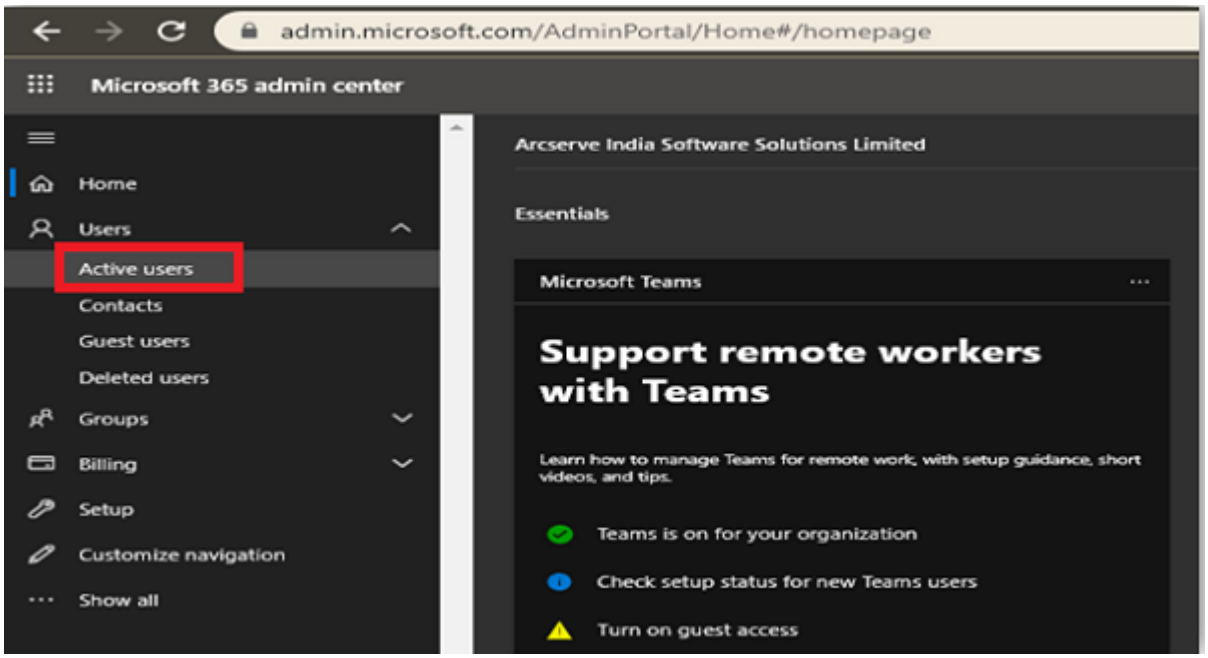
To configure, the first step is to enable the backup service account to Set app password.

Follow these steps:

1. Sign into Microsoft Office 365 using credentials of an administrator account and click the **Admin** icon.

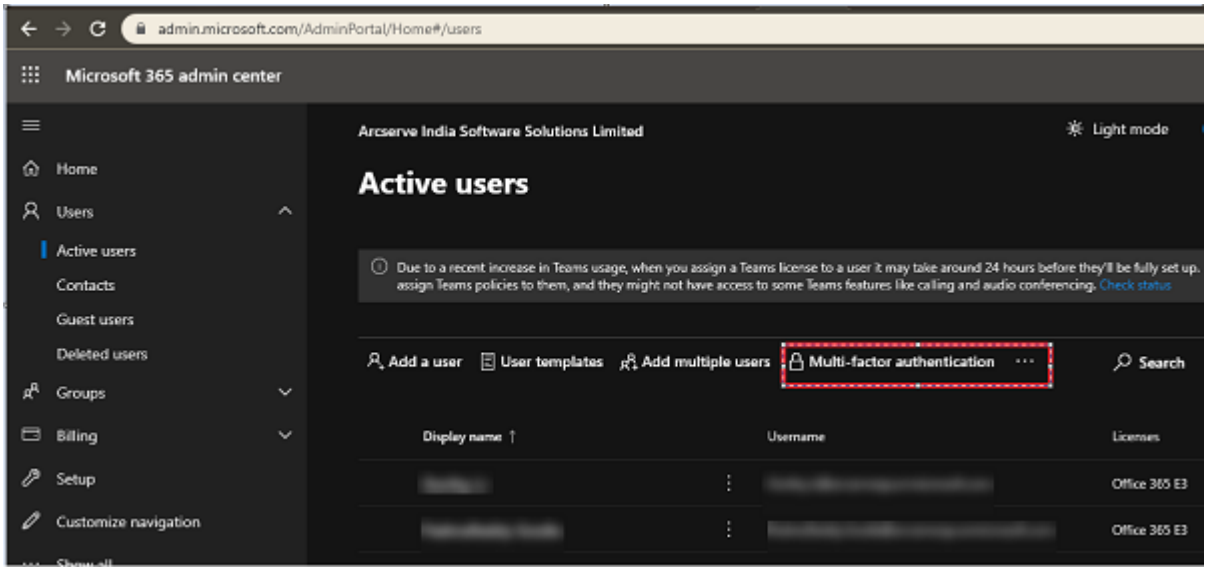


2. From the Microsoft 365 admin center screen, navigate to **Users** > **Active users**.



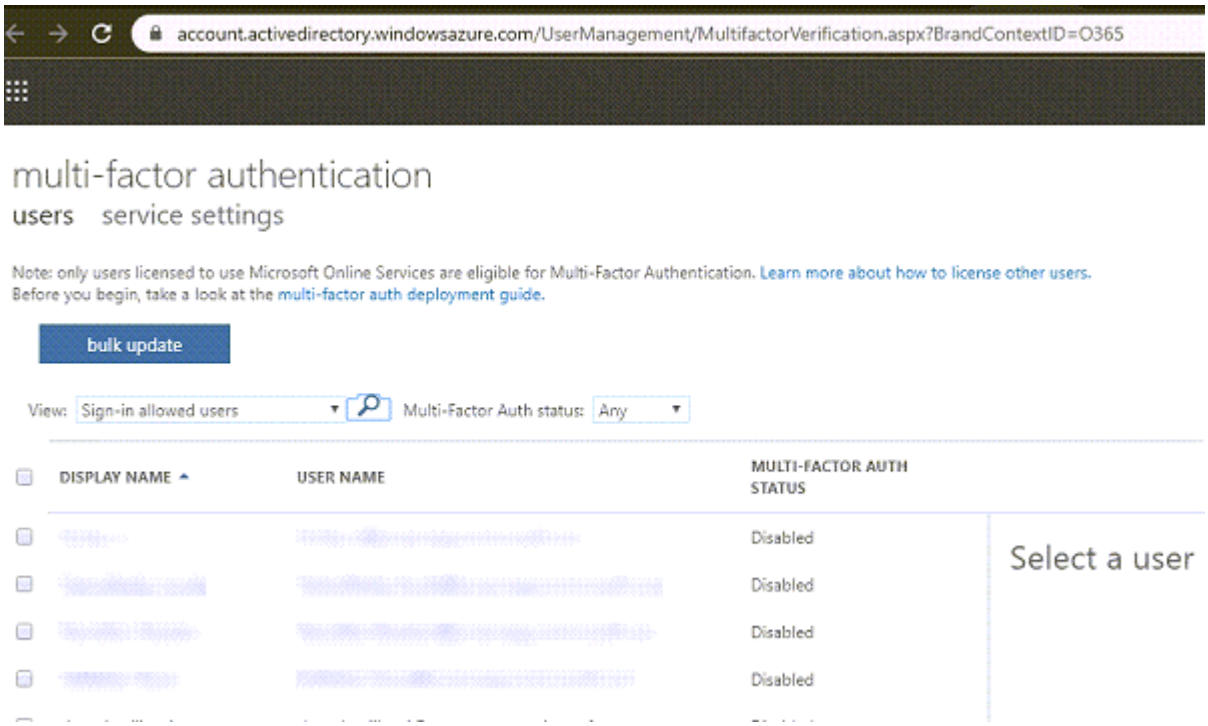
3. From the Active users screen, click the **Multi-factor authentication** option.

   Important! If you do not see the **(...)** option, then you are not a global admin for your subscription.

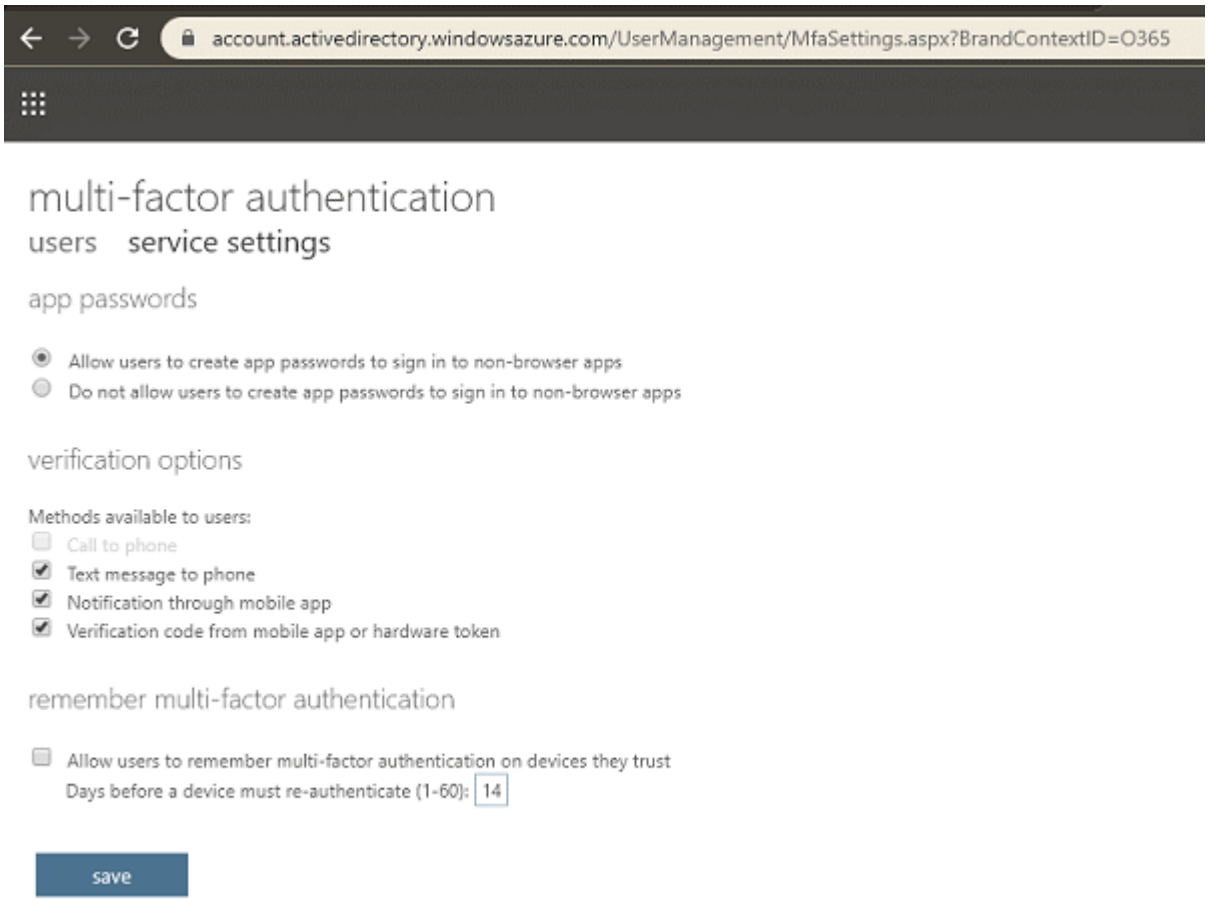


   You are led to the Setup Azure multi-factor authentication.

   Steps 4 and 5 only need to be set once. Then, skip to step 6



4. From the multi-factor authentication screen, click **service settings**.
5. From app passwords, select the checkbox of **Allow users to create app passwords to sign in to non-browser apps**.



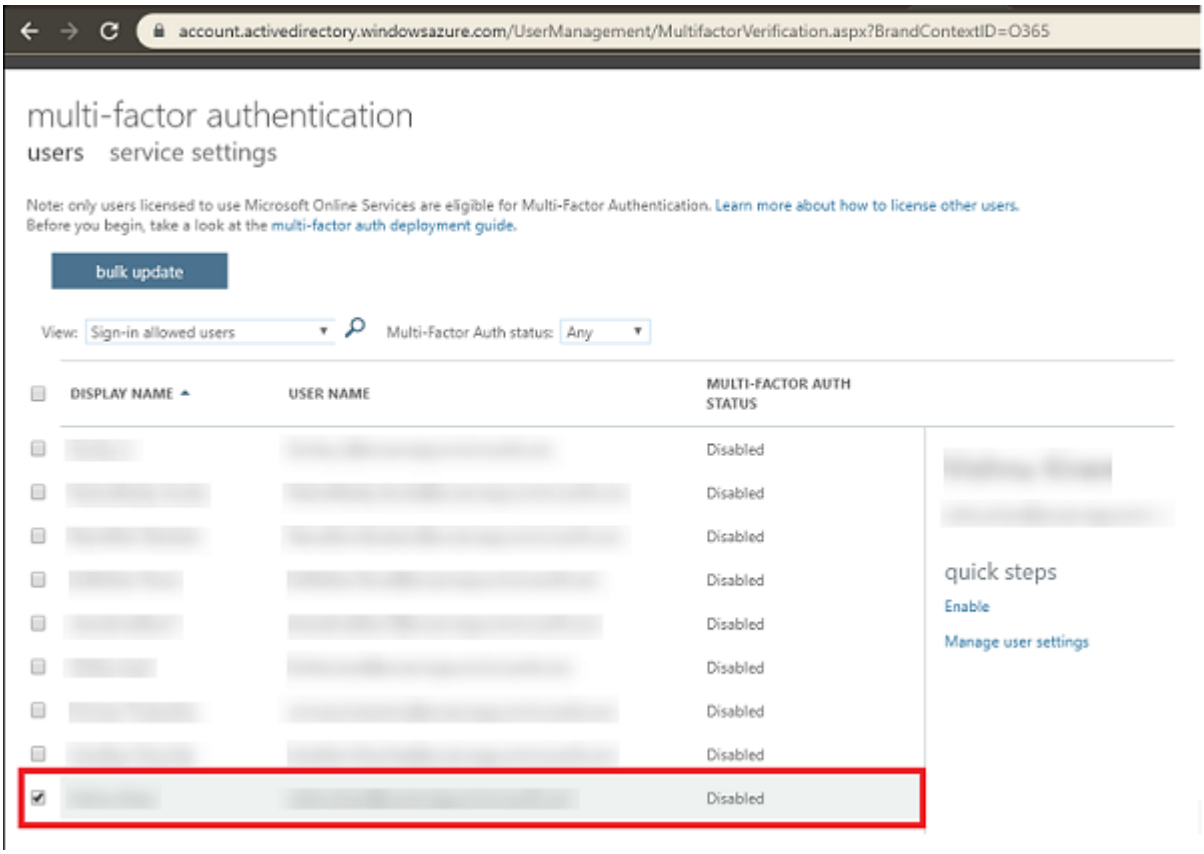
You can then use client Office apps after you create a new password.

6. Click **save** and close the window.

   You return to the users screen.

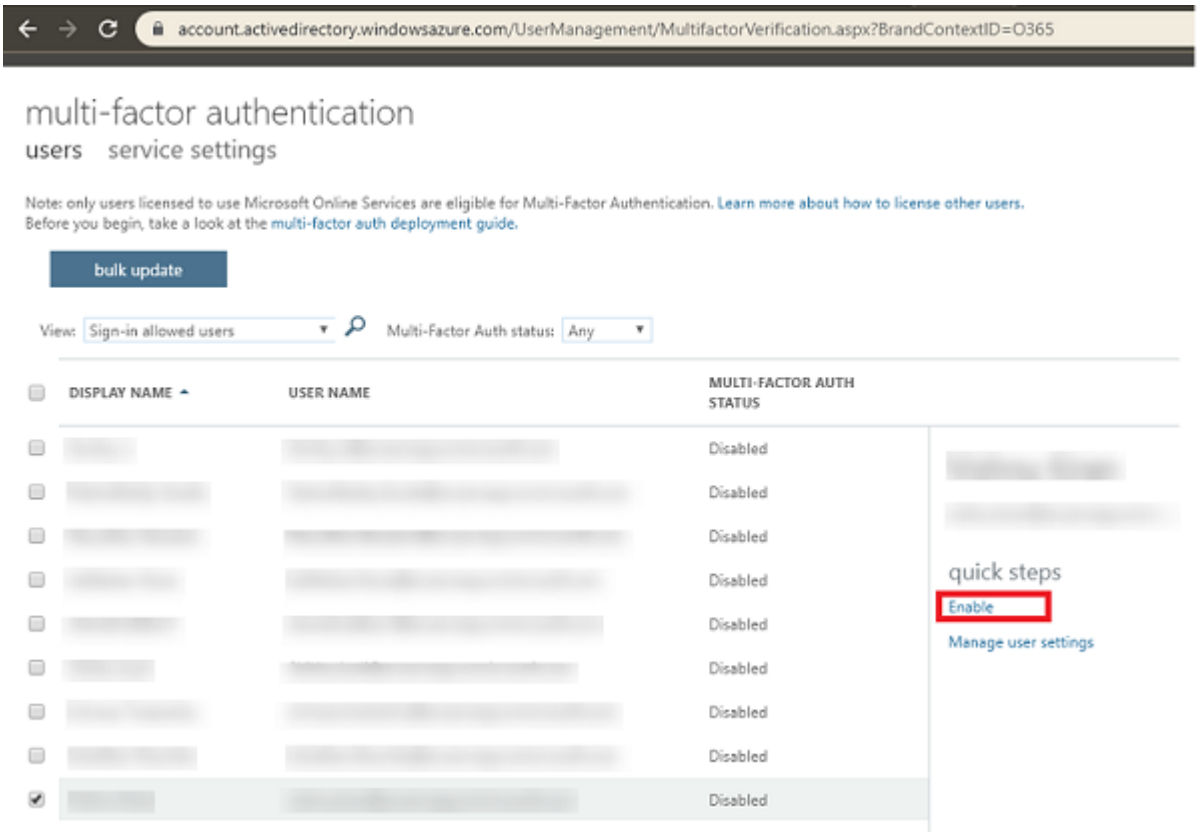
7. From the users screen, perform the following steps:

a. Select the check box for the users to enable MFA.



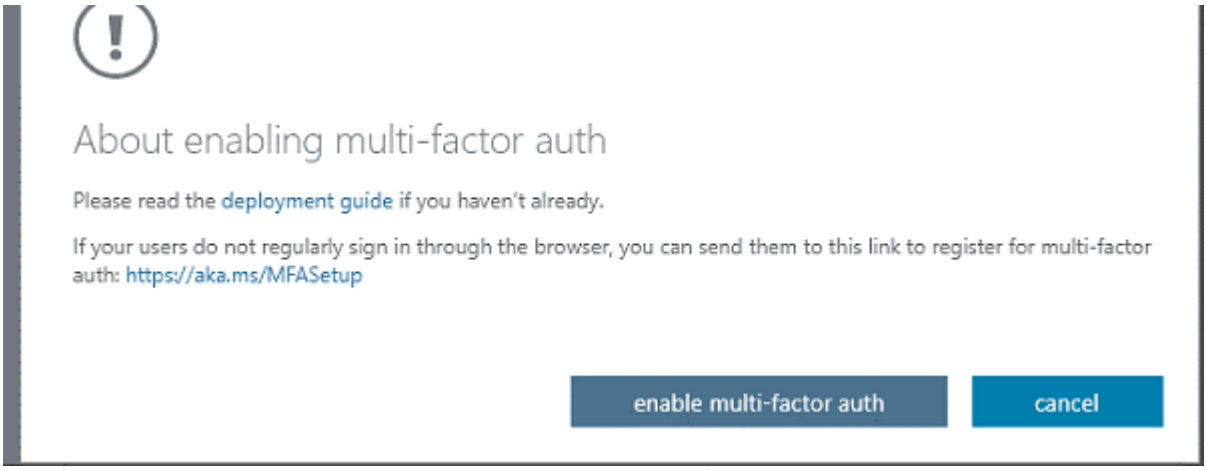
The right pane displays name of the user and under quick steps, you can view Enable and Manage user settings.

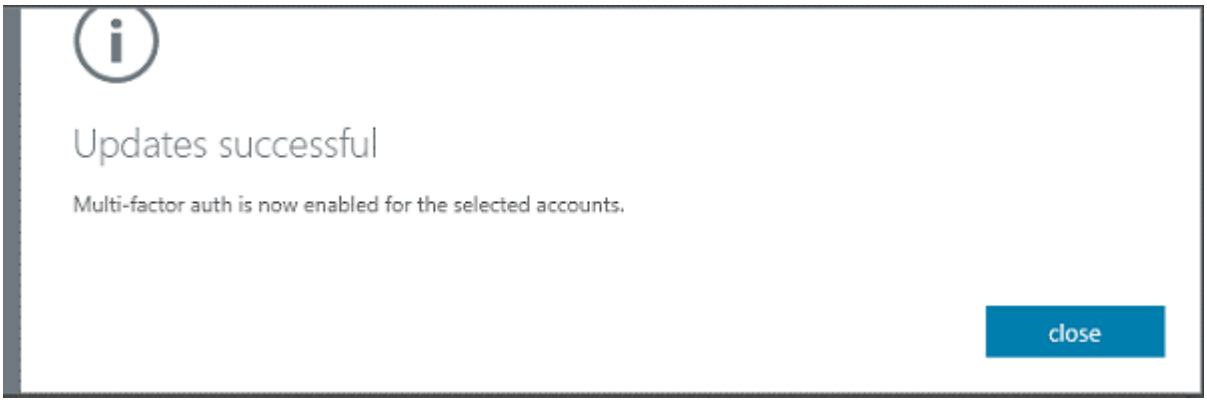
b. Click **Enable**.



A dialog box appears.

c. From the dialog box, click **enable multi-factor auth.**





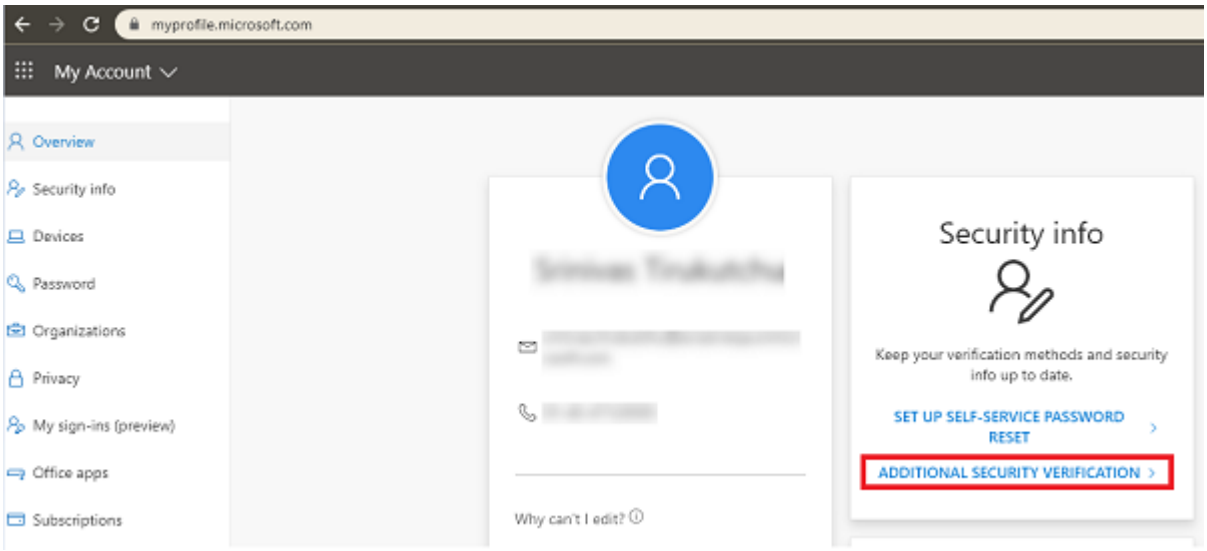
The backup service account to Set app password is enabled.

Creating app password for the backup service account

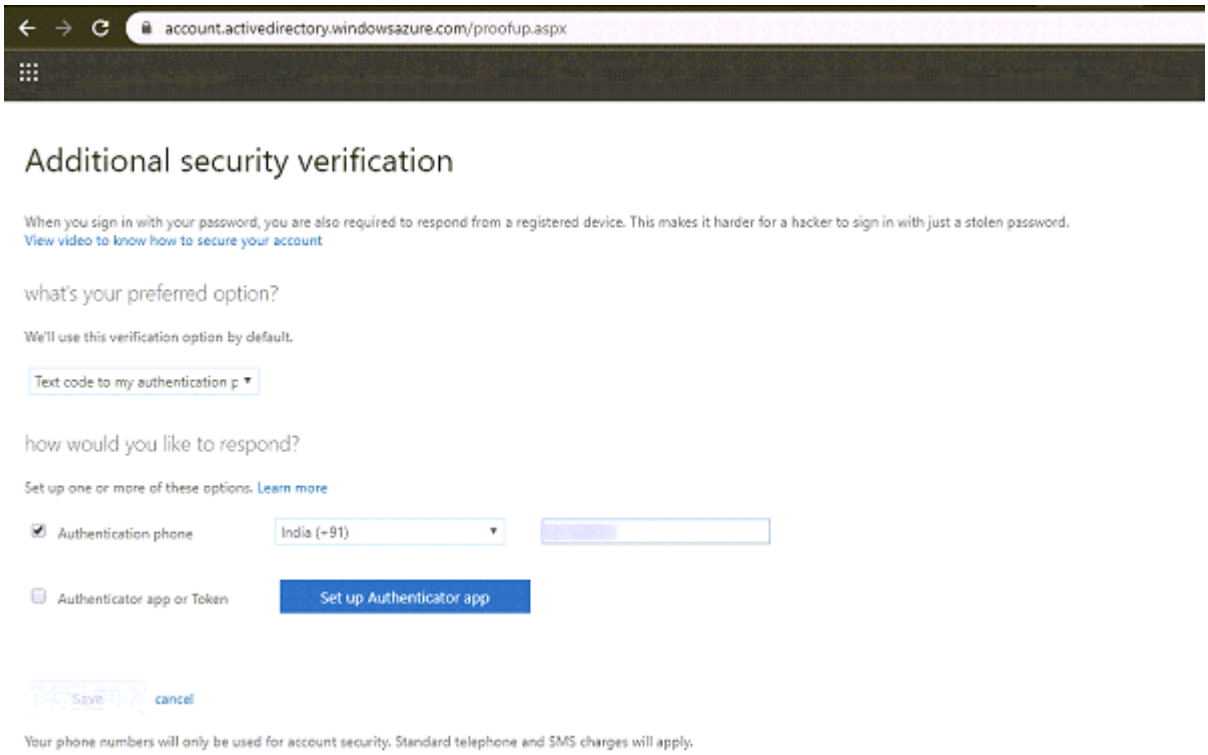
After enabling the backup service account to Set app password, the backup plan needs to use App Password for the backup service account. You need to create app password for the backup service account.

Follow these steps:

1. Sign into Office 365 (https://myprofile.microsoft.com/) with your work or school account and password.
2. Click **Additional Security Verification.**



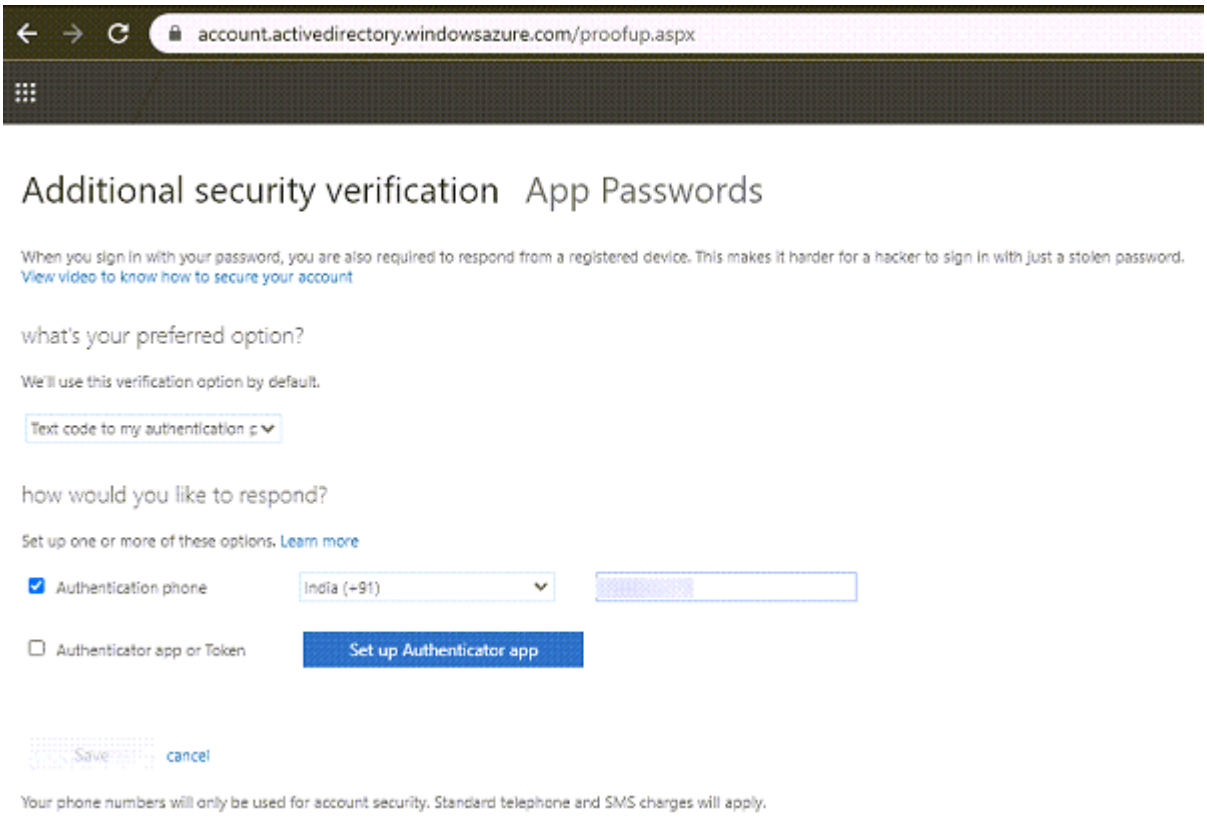
The Additional security verification screen appears.



3. Perform the following steps on the Additional security verification screen:

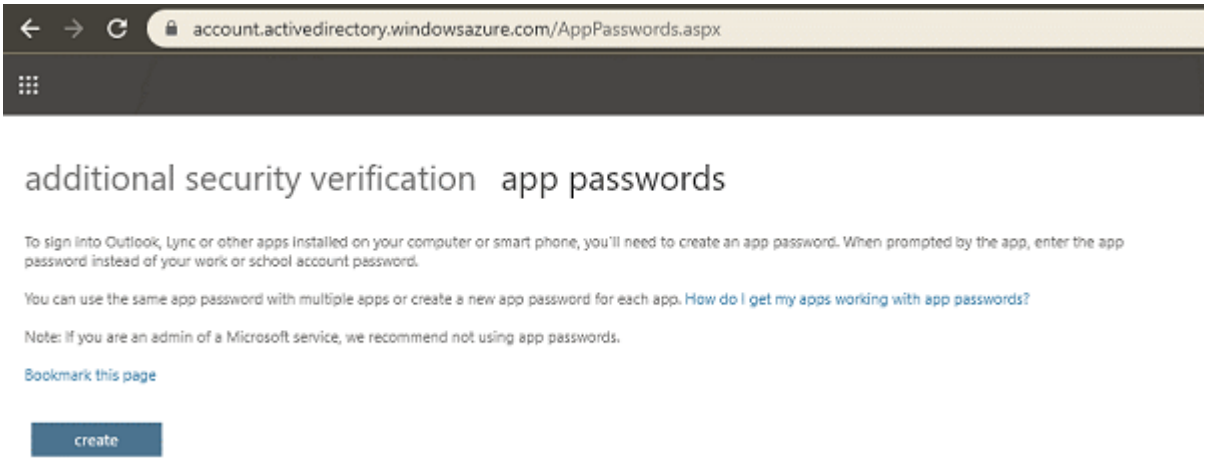
    a. Select your authentication method, and then follow the prompts on the page.

    For example, if you select the authentication phone, you should select your country and enter the phone number. You can also select a method to get the verification code.



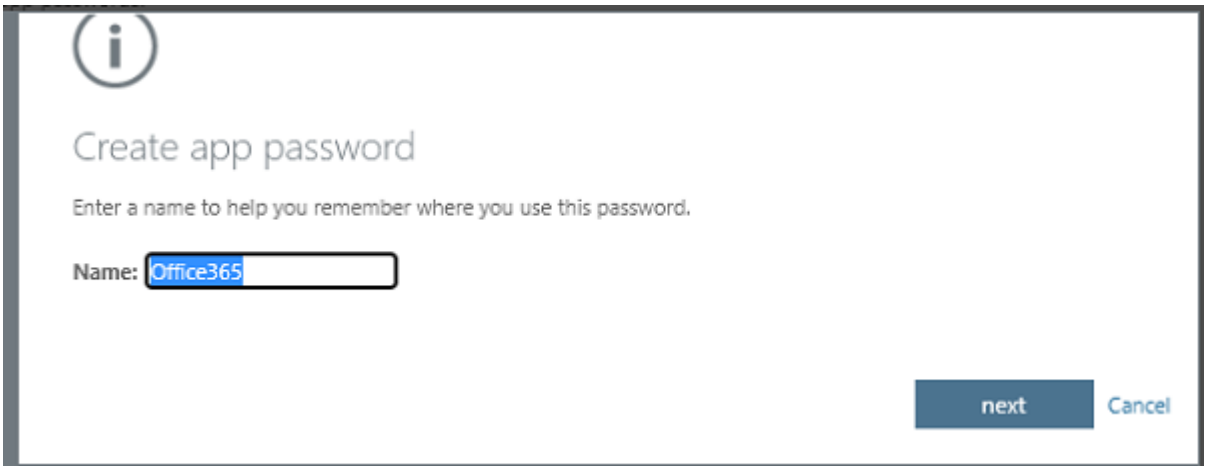
b. Click **App Passwords**.

The app passwords screen appears.



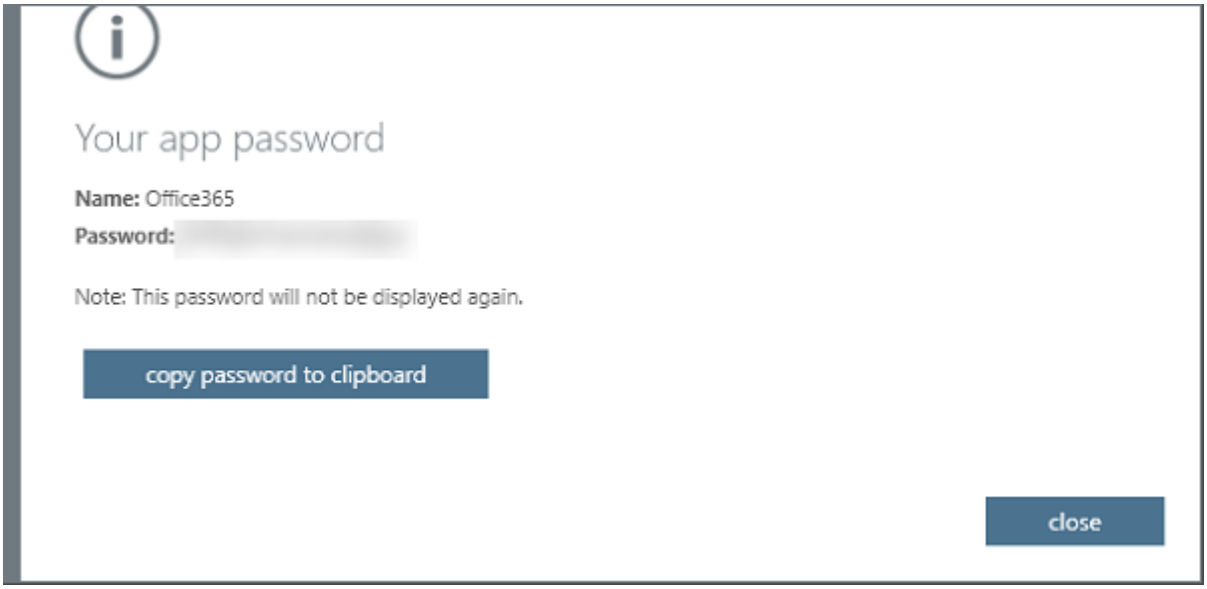
c. Click **create**.

The Create app password screen appears.

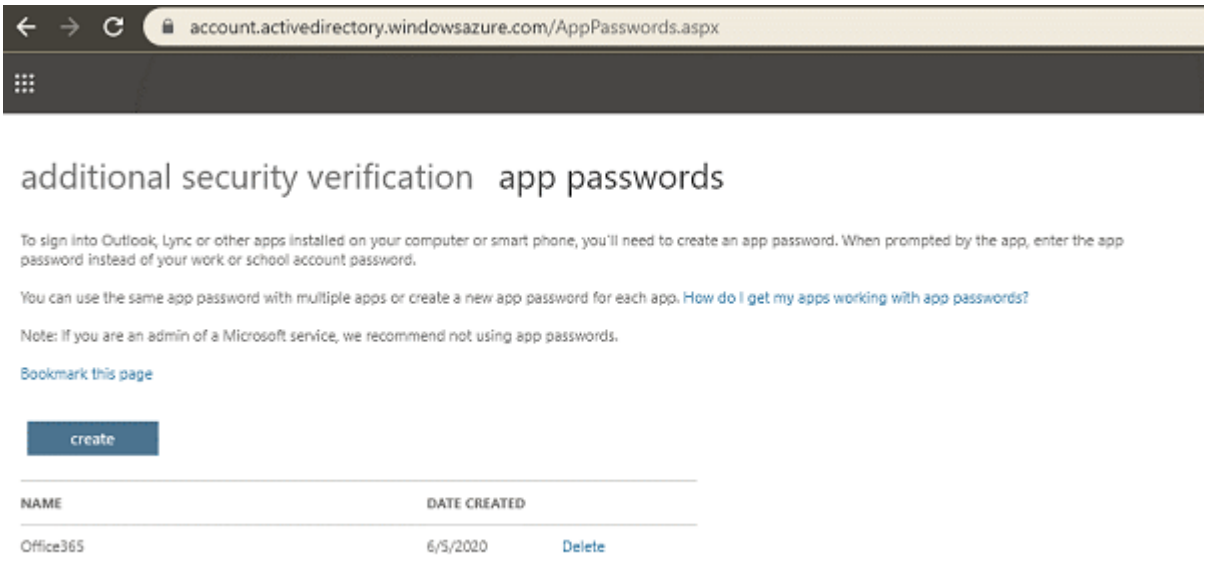


d. From the Create app password screen, enter a name, and then click **next**.

You will receive an app password that you can use with Outlook, Apple Mail, and other Email options.



e. Select the **copy password to clipboard** option and the password is copied to your clipboard.



App password for the backup service account is created.

How to Create a SharePoint Online Backup Plan

The SharePoint Protection is used to backup and restore Microsoft SharePoint Online site and list item. The SharePoint Online is one of the major products in Microsoft Office 365. To protect your SharePoint content, you need to create a Plan.

What To Do Next?

1. Review the Prerequisites and Considerations
2. Create a SharePoint Online Backup Plan
3. Verify the Backup Plan
4. Configuration for Multi-Factor Authentication

Review the Prerequisites

Verify the following prerequisites before performing a backup and restore:

- You have the SharePoint Site Collection URL to backup.
- The backup account is a member of Site Collection Administrators groups or assigned with *SharePoint admin* Role.

  To add an account to Site Collection Administrators group, refer to the link.
- If modern authentication is set on O365 tenant and Arcserve UDP is recently upgraded to support it, the existing Exchange online jobs needs to be reconfigured with modern authentication related settings, which is described in the Modern Authentication section.
- If Modern Authentication is set on the Office 365 tenant, the version of Arcserve UDP must be 7.0.4455 Update 2 Build 675 or higher. If the version needs an upgrade to the required build, contact the Arcserve support.

Create a SharePoint Online Backup Plan

A backup plan includes a **Backup: Office 365 SharePoint Online** task that performs a backup of SharePoint Online node and stores data to a deduplication Data store or non-deduplication Data store. Each task consists of parameters that define the source, destination, schedule, and other backup details.

Watch video and view how to create the SharePoint Online Backup plan.

Follow these steps:

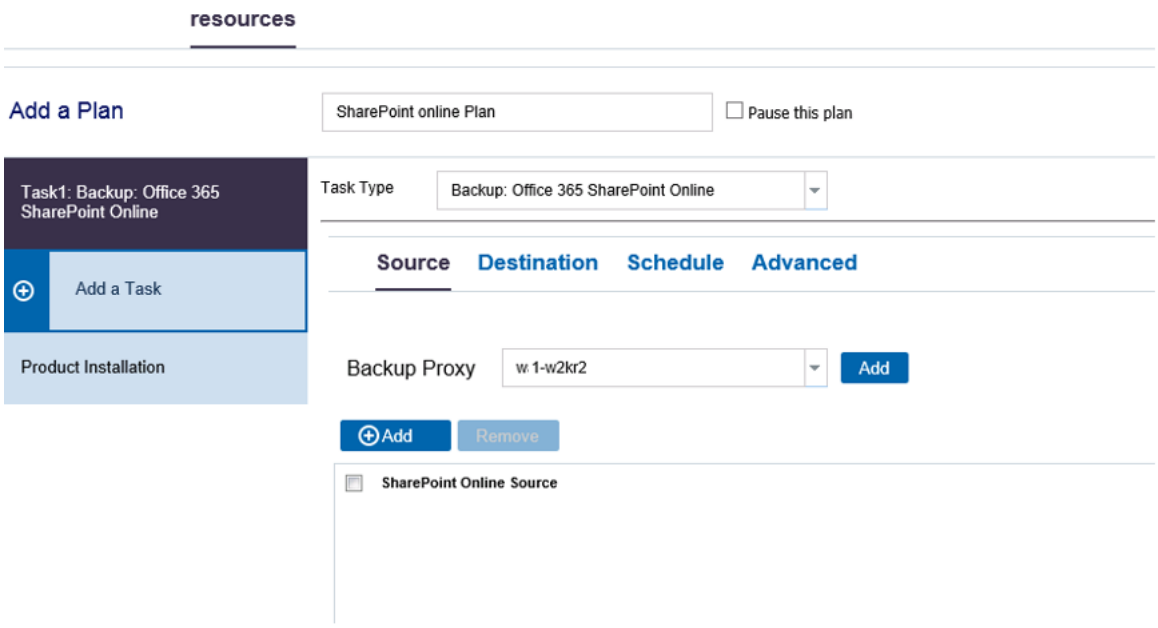
1. Click the **resources** tab on the Console.
2. From the left pane, navigate to **Plans**, and click **All Plans**.

   If you have created plans earlier, those plans are displayed on the center pane.
3. On the center pane, click **Add a Plan**.

   The **Add a Plan** dialog opens.
4. Enter a plan name.
5. (Optional) Select the **Pause this plan** check box.

   The plan does not run until you clear the check box to resume the plan.

   Note: If a plan is paused, then any in-progress job is not paused but all corresponding scheduled jobs associated with that plan are paused. However, you can manually run a job. For example, you can manually run backup job and replication job for a node even if the respective plan is paused. In such case, the following task to the on-demand (manual) job does not run. For example, there is a replication task after an on-demand backup job, the replication job does not run for the on-demand backup job. You need to manually run the replication job. When you resume the plan, the pending jobs do not resume immediately. After you resume the plan, the pending jobs run from the next scheduled time.
6. From the **Task Type** drop-down list, select **Backup: Office 365 SharePoint Online**.



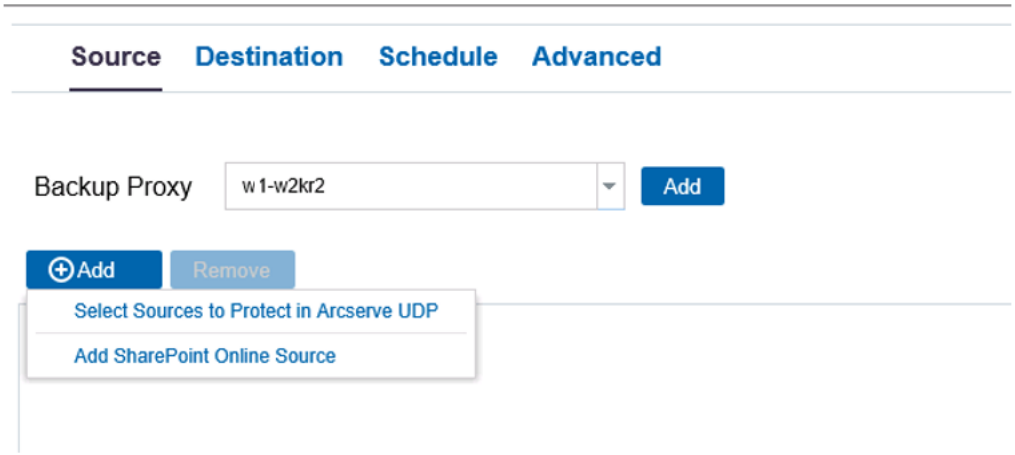
Now specify the Source, Destination, Schedule, and Advanced details.

Specify the Source

The Source page lets you specify the SharePoint Online source nodes that you want to protect. You can select more than one SharePoint Online source nodes in a plan.

Follow these steps:

1. Click the **Source** tab.



2. Select the **Backup Proxy** from the drop-down list.
3. Add SharePoint Online node using one of the following methods:
   - **Method 1:** You can save a plan without adding any source nodes. But, the plan is not deployed unless you add a node.
     a. Click **Add**, and then click **Select Source to Protect** in Arcserve UDP.

        The Add Nodes to Plan dialog is displayed.

        Note: Use this option only if you have already added SharePoint node.

     b. Select a node, and then click **Connect**.
   - **Method 2:** To find the SharePoint Online nodes that you want to protect, use **Search**. Click **Add**, and then click **Add SharePoint Online Source**.

     Note: Unlike other nodes, you cannot add the SharePoint Online node from the All Nodes page. You can add a SharePoint Online node only in a plan while creating or modifying a plan.
4. After you click Add Nodes, you can select Basic Authentication or Modern Authentication to add the Exchange node by plan.

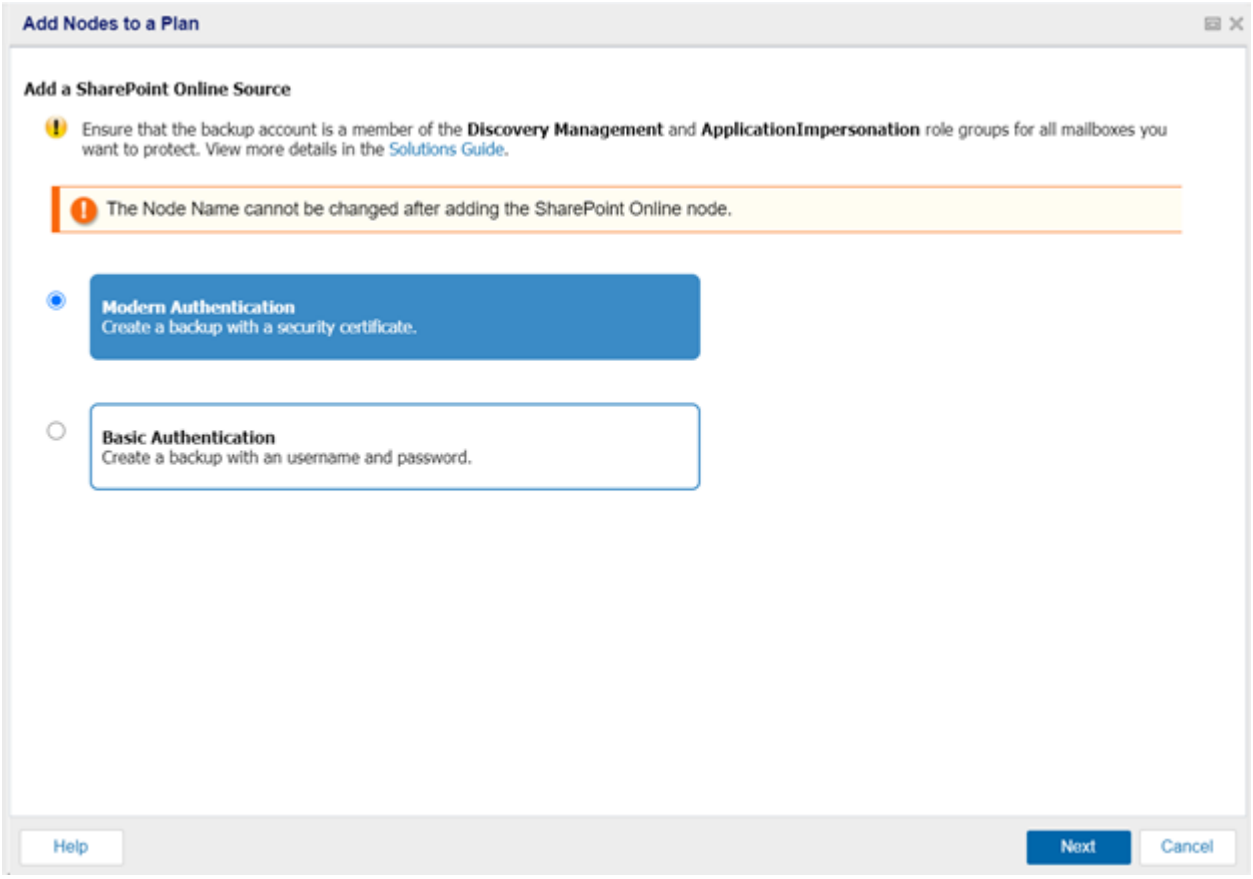
   For Basic Authentication, provide the following information:
   - Node name
   - Site Collection URL

- User Name
- Password

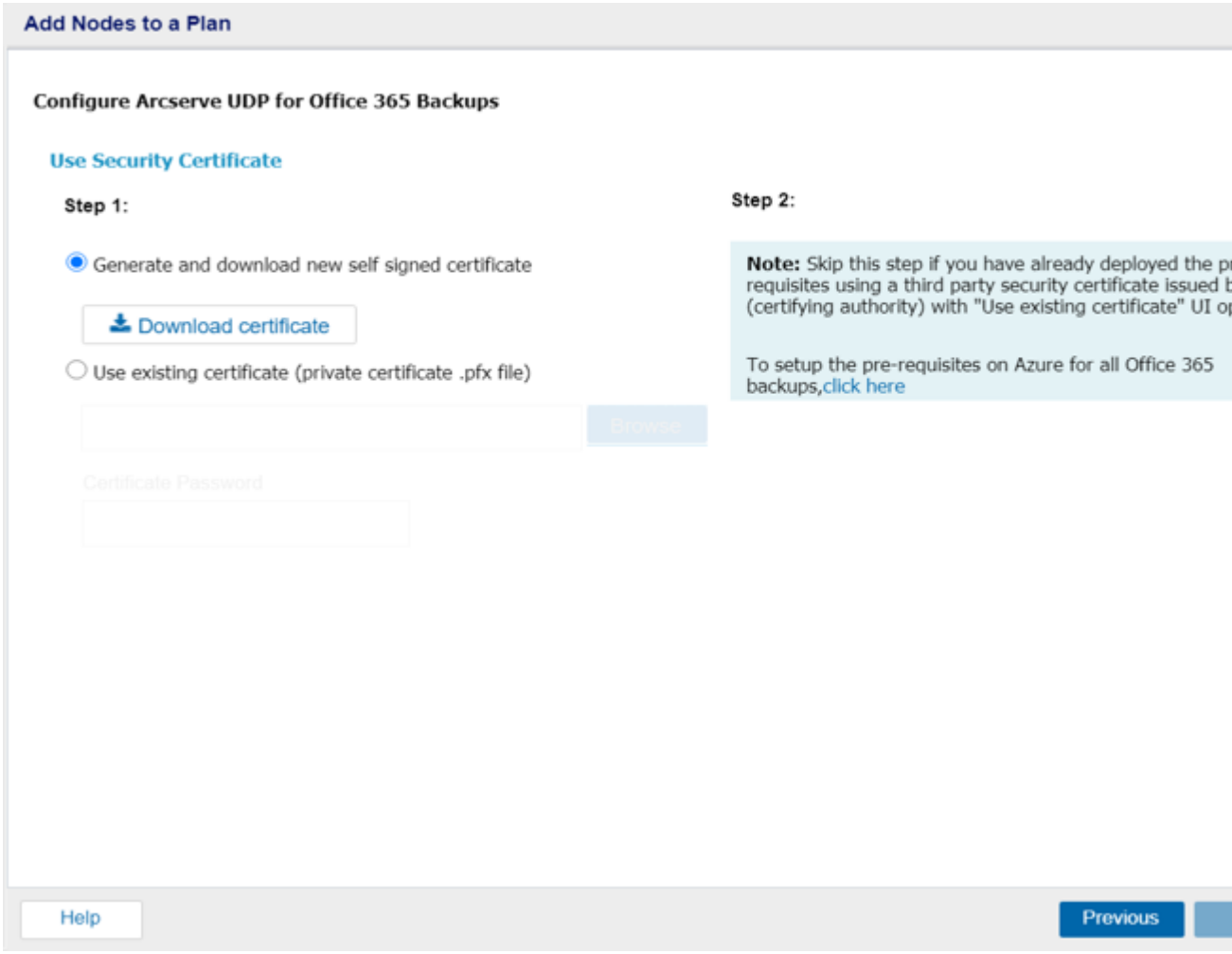
For Modern Authentication, provide the following information:

- Node name
- Site Collection URL
- Application ID
- User name

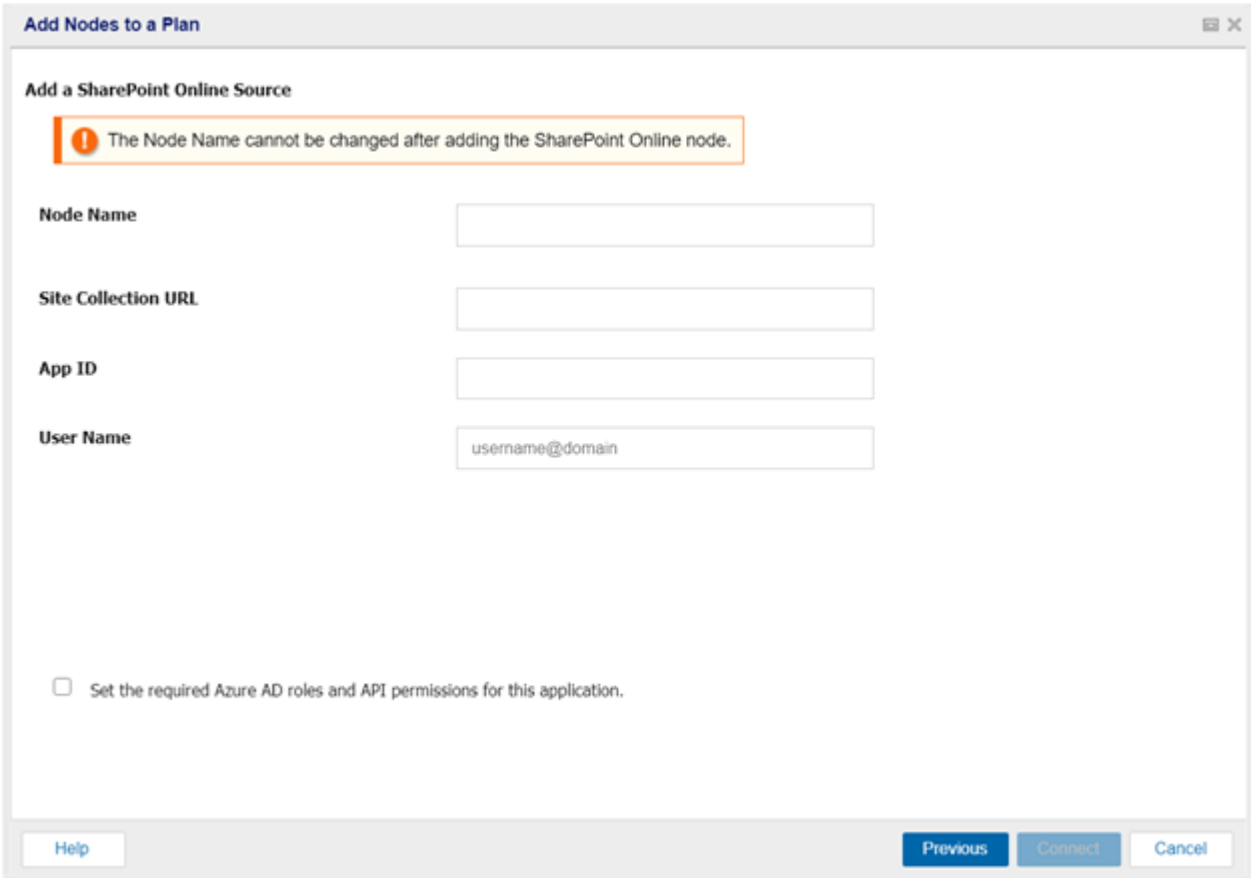
Note: Exchange online node names cannot change after creating the node.



To authenticate the UDP application with security certificates, see How to Use Security Certificates.



5. After you upload the certificate to the Azure portal, in the UDP console provide Node Name, Application ID, and Username. To accept the AzureAD Admin consent, select the checkbox, and then click **Connect** to register the node.



Notes:

- You can use a single account to protect multiple SharePoint Online nodes.
- Fill in the app password if Multi-Factor Authentication is enabled and the tenant is set to use Basic Authentication.

6. Select the SharePoint list/Library, documents, or other list items that you want to protect.

   Note: Arcserve UDP 7.0 protects only SharePoint Online lists, Libraries, and Documents.

7. Click **Save**.

   The SharePoint Online sources that you want to protect are added to the plan.

Specify the Destination

The destination is a location where you store the backup data. You must at least specify the destination to save the plan.

Follow these steps:

1. Click the **Destination** tab.

   The **Arcserve UDP Recovery Point Server** option. **Arcserve UDP Recovery Point Server** specifies that the backup destination is a recovery point server.

   You cannot store data as recovery sets.

2. Perform the following steps:

   a. Select a recovery point server.

   b. Select a non-deduplication or deduplication data store.

      The list displays all the data stores created on the specified recovery point server.

   c. Provide a session password.

      The session password is optional when the backup destination is an unencrypted RPS data store.

   d. Confirm the session password.

   The destination is specified.

Specify the Schedule

The Schedule page lets you define a schedule for Backup, Merge, and Throttle functions to repeat at specific intervals. After you define a schedule, the jobs run automatically per the schedule. You can add multiple schedules and provide retention settings.

A Backup Schedule refers to regular schedule that is repeated multiple times a day based on the number of hours or minutes you select. Besides the regular schedule, a backup schedule also provides options to add daily, weekly, and monthly schedules.

Note: For more information on scheduling and retention settings, see Understanding Advanced Scheduling and Retention.

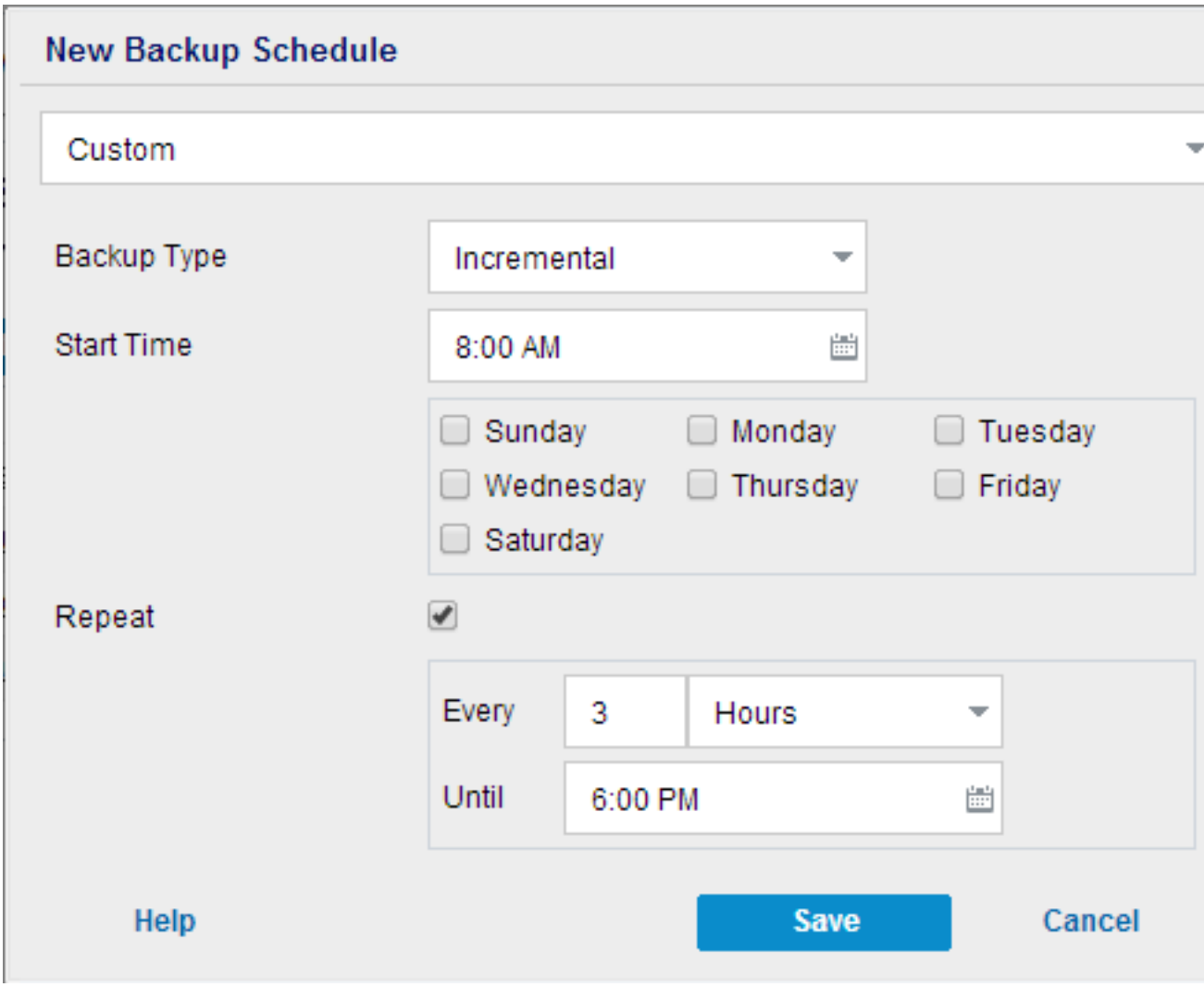
Follow these steps:

1. Add backup, merge, and throttle schedules.

   Add Backup Schedule

   a. Click **Add** and select **Add Backup Schedule**.

      The **New Backup Schedule** dialog opens.



b. Select one of the following options:

Custom

Specifies the backup schedule that repeats multiple times a day.

Daily

Specifies the backup schedule that occurs once a day. By default, all the days of the week are selected for Daily backup. If you do not want to run the backup job on a specific day, clear the check box for that day of the week.

Weekly

Specifies the backup schedule that occurs once a week.

Monthly

Specifies the backup schedule that occurs once a month.

c. Select the backup type.

Full

Determines the backup schedule for Full Backups. As scheduled, Arcserve UDP performs a full backup of all used blocks from the source machine. A full backup typically consumes time depending on the backup size.

Incremental

Determines the backup schedule for Incremental Backups.

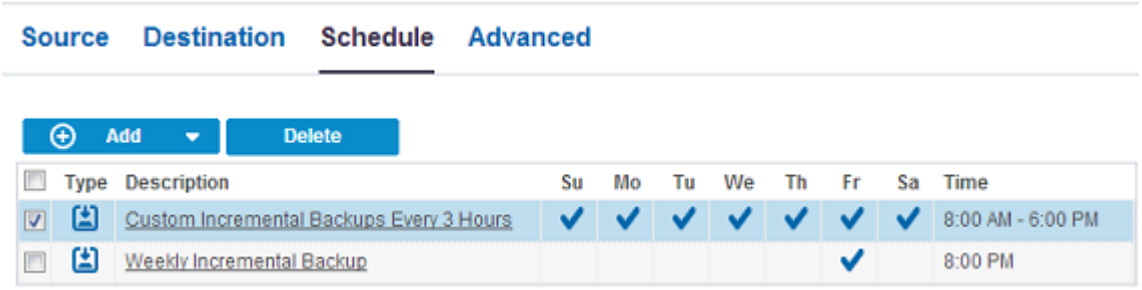
As scheduled, Arcserve UDP incrementally backs up only those blocks that have changed after the last successful backup. The advantages of Incremental Backups are that the backup is a fast backup and it produces a small backup image. This is the most optimal way to perform a backup.

d. Specify the backup start time.

e. (Optional) Select the **Repeat** check box and specify the repeat schedule.

f. Click **Save**.

The Backup Schedule is specified and appears on the **Schedule** page.



Add Merge Schedule

a. Click **Add** and select **Add Merge Schedule**.

The **Add New Merge Schedule** dialog opens.

b. Specify the start time for the merge job.

c. Specify **Until** to provide an end time for the merge job.

d. Click **Save**.

The Merge Schedule is specified and appears on the **Schedule** page.

Add Throttle Schedule

a. Click **Add** and select **Add Throttle Schedule**.

The **Add New Throttle Schedule** dialog opens.

b. Specify the throughput limit in MB per minutes unit.

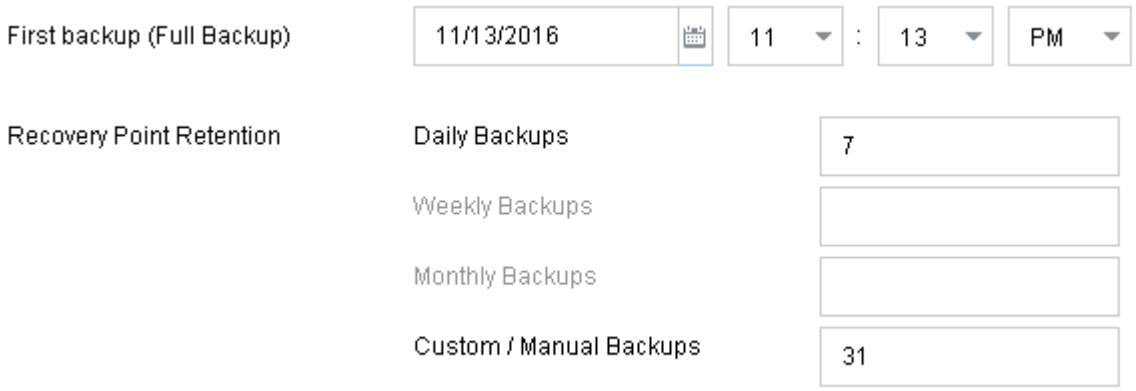
c. Specify the start time for the backup throughput job.

d. Specify **Until** to provide an end time for the throughput job.

e. Click **Save**.

The Throttle Schedule is specified and displayed on the **Schedule** page.

2. Specify the start time for the scheduled backup.



3. Specify the recovery points retention settings for Custom, Daily, Weekly, and Monthly schedule.

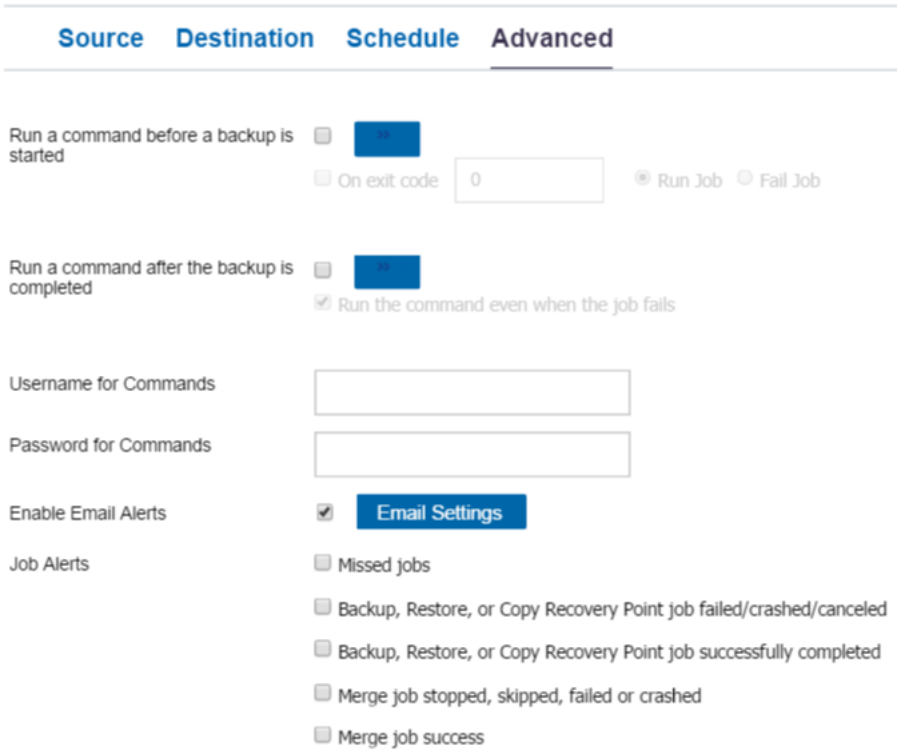
   The options are enabled if you have added the corresponding backup schedule. If you modify the retention settings on this page, the changes are reflected on the **Backup Schedule** dialog.

   The schedule is specified.

Specify the Advanced Settings

The **Advanced** tab lets you specify some advanced settings for the backup job. The advanced settings include providing the location of any scripts, and email settings.

The following image displays the **Advanced** tab:



Follow these steps:

1. Specify the following details.

   Run a command before a backup is started

   Lets you run a script before the backup job starts. Specify the path where the script is stored inside the proxy node. Click **On exit code** and specify the exit code for **Run Job** or **Fail Job**. **Run Job** indicates that the backup job continues when the script returns the exit code. **Fail Job** indicates that the backup job stops when the script returns the exit code.

   Run a command after a backup is completed

   Lets you run a script after the backup job is completed. Specify the complete path where the script is stored.

   Run a command even when the job fails

If this check box is selected, the script specified in **Run a command after a backup is completed** is executed even when the backup job fails. Otherwise, that script is executed only when backup job completes successfully.

Username for Commands

Lets you specify the username to run the commands.

Password for Commands

Lets you specify the password to run the commands.

Enable Email Alerts

Lets you enable email alerts. You can configure email settings and specify the types of alerts that you want to receive in an email. When you select this option, the following options are enabled for your selection.

Email Settings

Lets you configure the email settings. Click **Email Settings** and configure the email server and proxy server details. For more information about how to configure Email Settings, refer to Email and Alert Configuration.

Job Alerts

Lets you select the types of job alert emails that you want to receive.

2. Click **Save**.

Note: When you select a node as a backup source or backup proxy, Arcserve UDP checks whether the agent is installed on proxy node and if it is the latest version. Arcserve UDP then displays a verification dialog that lists all the nodes that either have an outdated version of the agent or does not have the agent installed. To install/upgrade the agent on these nodes, select the installation method and click **Save**.

The changes are saved and a green checkmark appears next to the task name. The plan page closes.

Note: If you have to add another task, you must select the plan from the **resources** tab and modify the plan. To modify the plan, click the plan from the center pane. The plan opens and you can modify it. You may add the **Copy Recovery Point**, **Copy to Tape**, **Replicate**, and **Replicate from a remote RPS** tasks as follow up tasks.

The plan is automatically deployed to the proxy server node.

The SharePoint Online backup plan for the proxy server is created. The backup runs per the schedule that you have configured on the **Schedule** tab. You can also perform a manual backup at any time.

Verify the Backup

To verify your backup, confirm that you have successfully created the backup plan. After you verify that the plan is created successfully, confirm whether the backup job is running as scheduled. You can verify the status of backup jobs from the **Jobs** tab.

Follow these steps to verify plans:

1. Click the **resources** tab.
2. From the left pane, navigate to **Nodes**, and click **All Nodes**.

   A list of all nodes is displayed on the center pane.
3. Verify that plans are mapped with nodes.

Follow these steps to verify backup jobs:

1. Click the **jobs** tab.
2. From the left pane, click **All Jobs**.

   The status of each job is listed on the center pane.
3. Verify that the backup job is successful.

   The backup job is verified.

Configuring for Multi-Factor Authentication

When an organization has multi-factor authentication (MFA) enabled for the users, the office 365 backup plan needs to be configured using the App Password for the backup service account.

Perform the following steps to configure Arcserve UDP to Support multi-factor authentication:

1. Enable the backup service account to Set app password
2. Create app password for the backup service account

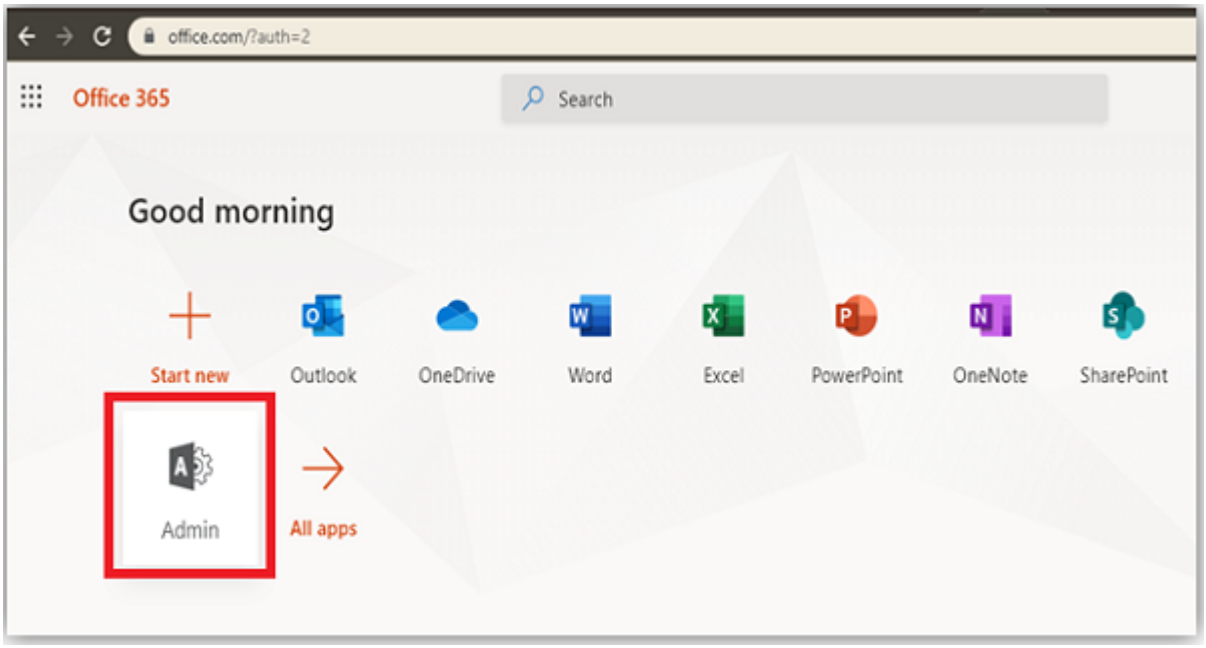
Note: MFA authentication (App password) is currently supported for O365 Exchange Online and SharePoint Online backups only.

Enable the backup service account to Set app password

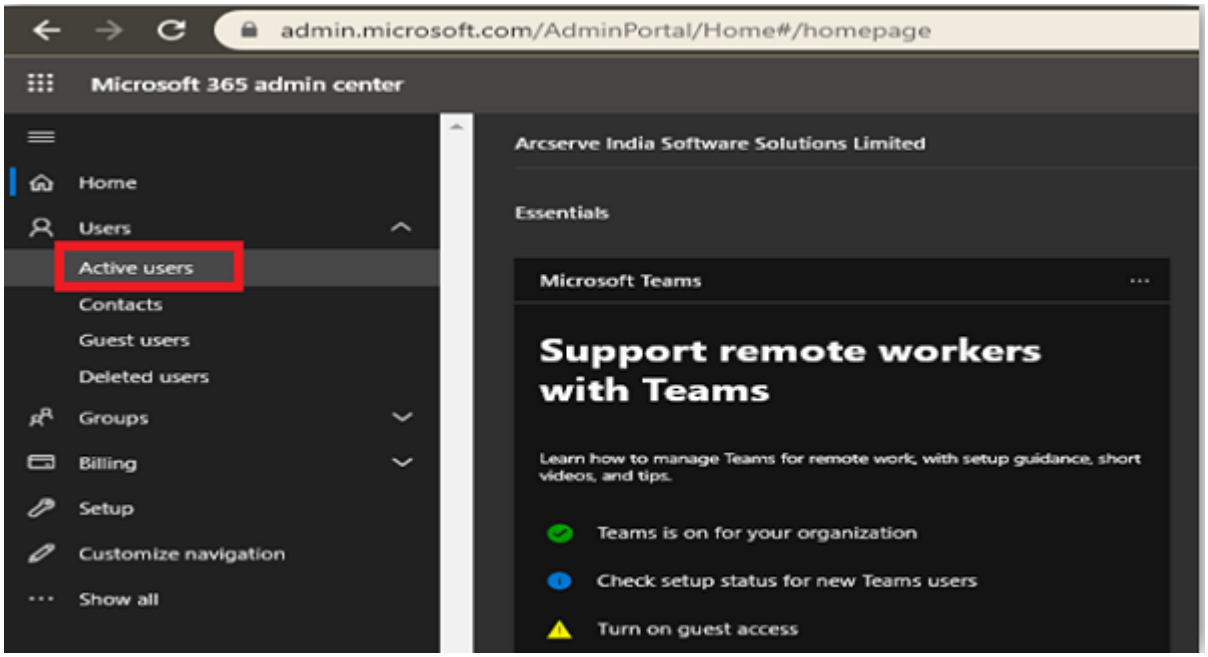
To configure, the first step is to enable the backup service account to Set app password.

Follow these steps:

1. Sign into Microsoft Office 365 using credentials of an administrator account and click the **Admin** icon.

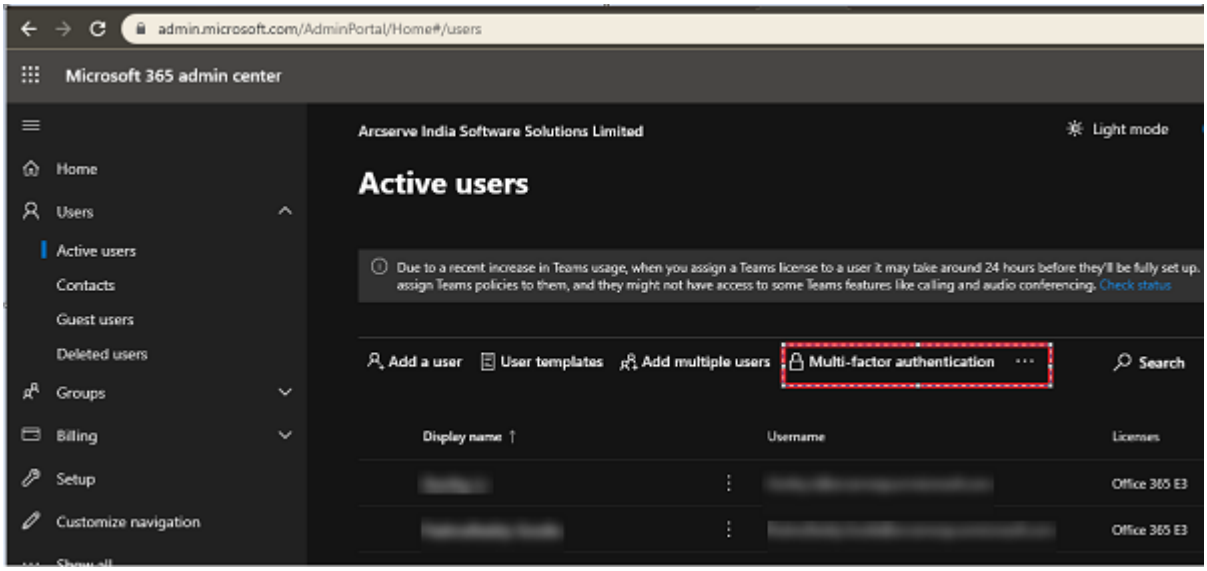


2. From the Microsoft 365 admin center screen, navigate to **Users** > **Active users**.



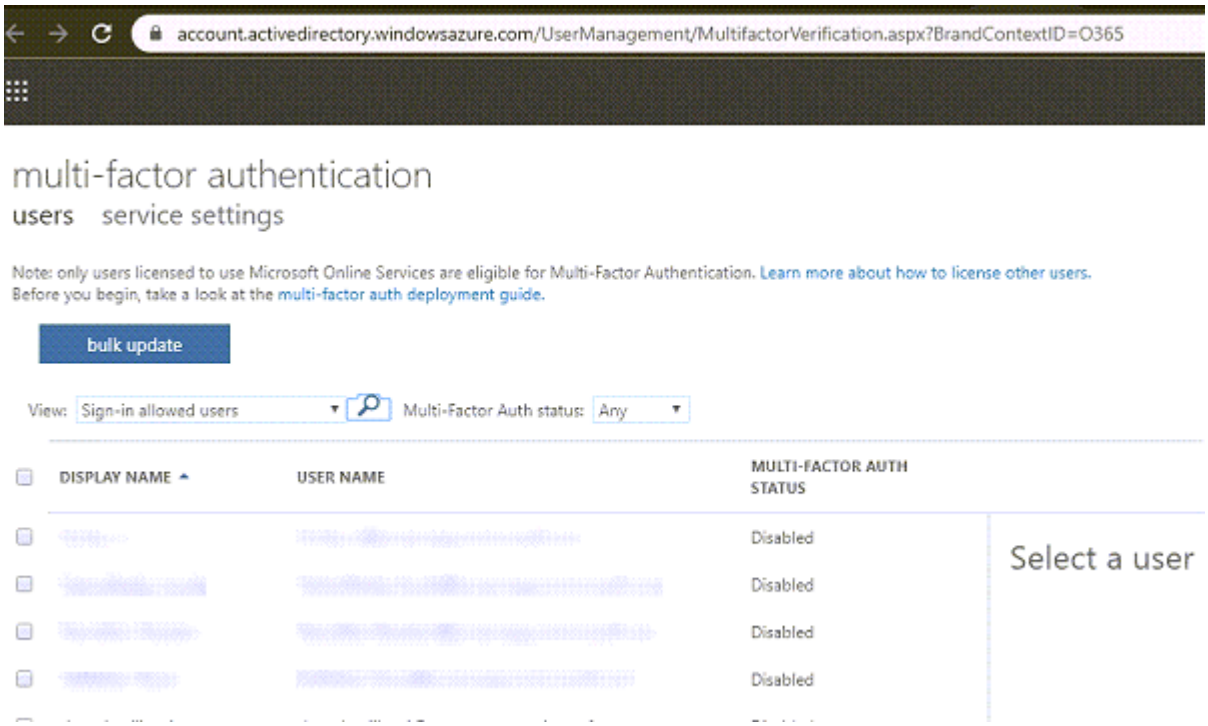
3. From the Active users screen, click the **Multi-factor authentication** option.

   Important! If you do not see the **(...)** option, then you are not a global admin for your subscription.

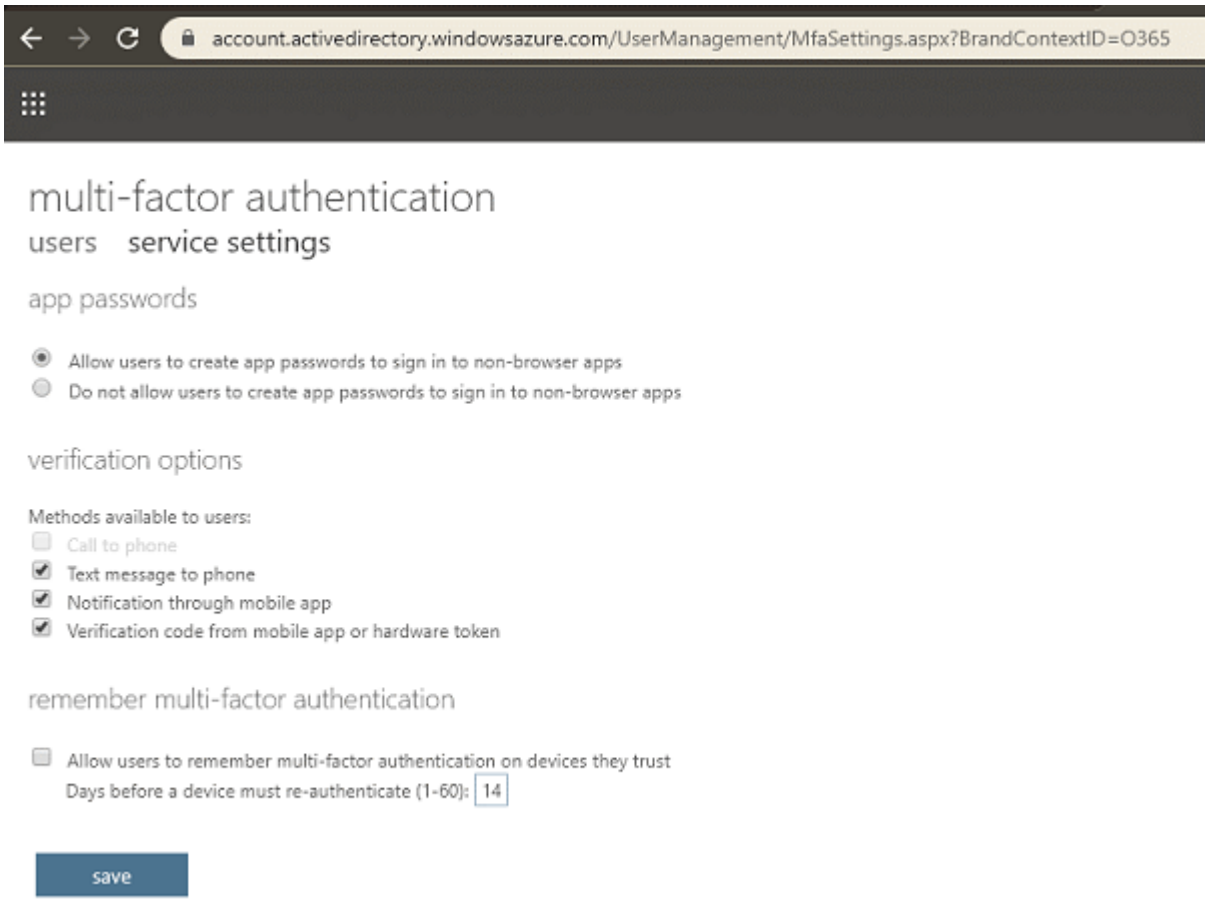


   You are led to the Setup Azure multi-factor authentication.

   Steps 4 and 5 only need to be set once. Then, skip to step 6



4. From the multi-factor authentication screen, click **service settings**.
5. From app passwords, select the checkbox of **Allow users to create app passwords to sign in to non-browser apps**.



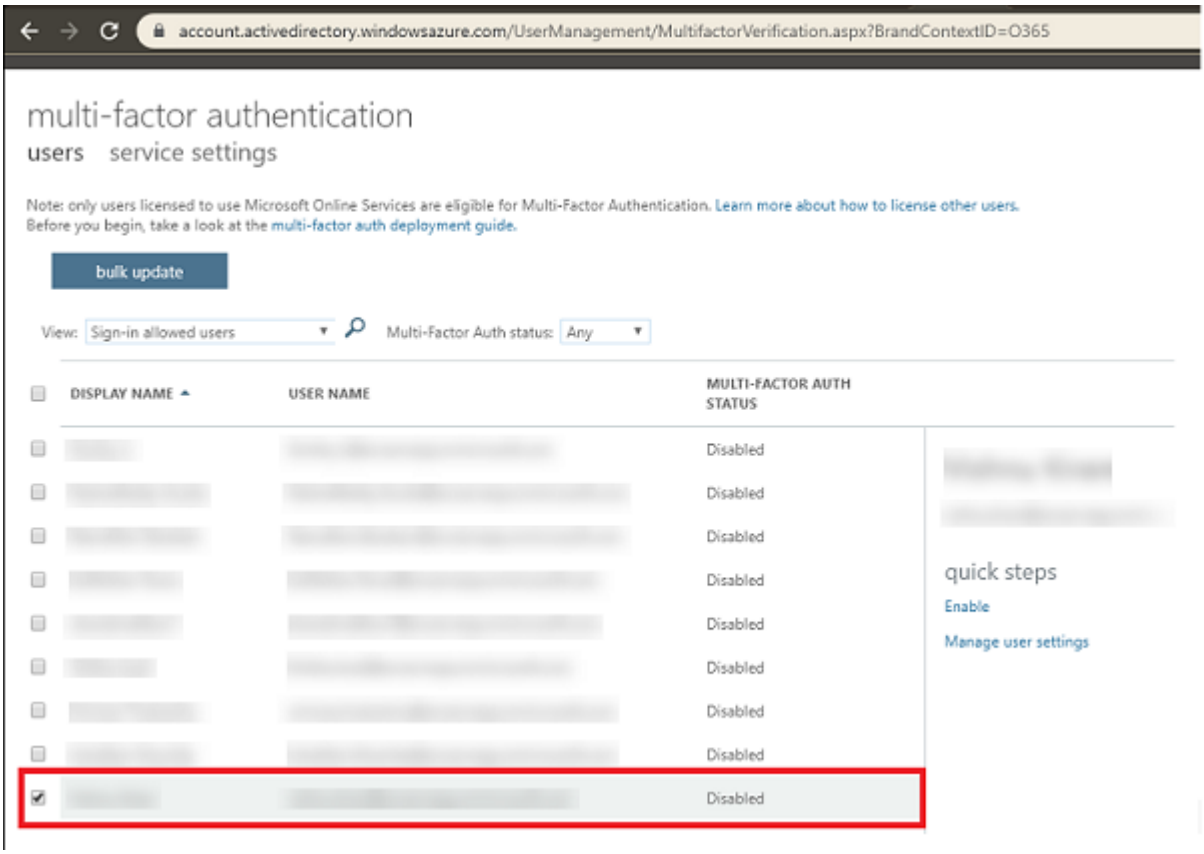
You can then use client Office apps after you create a new password.

6. Click **save** and close the window.

   You return to the users screen.

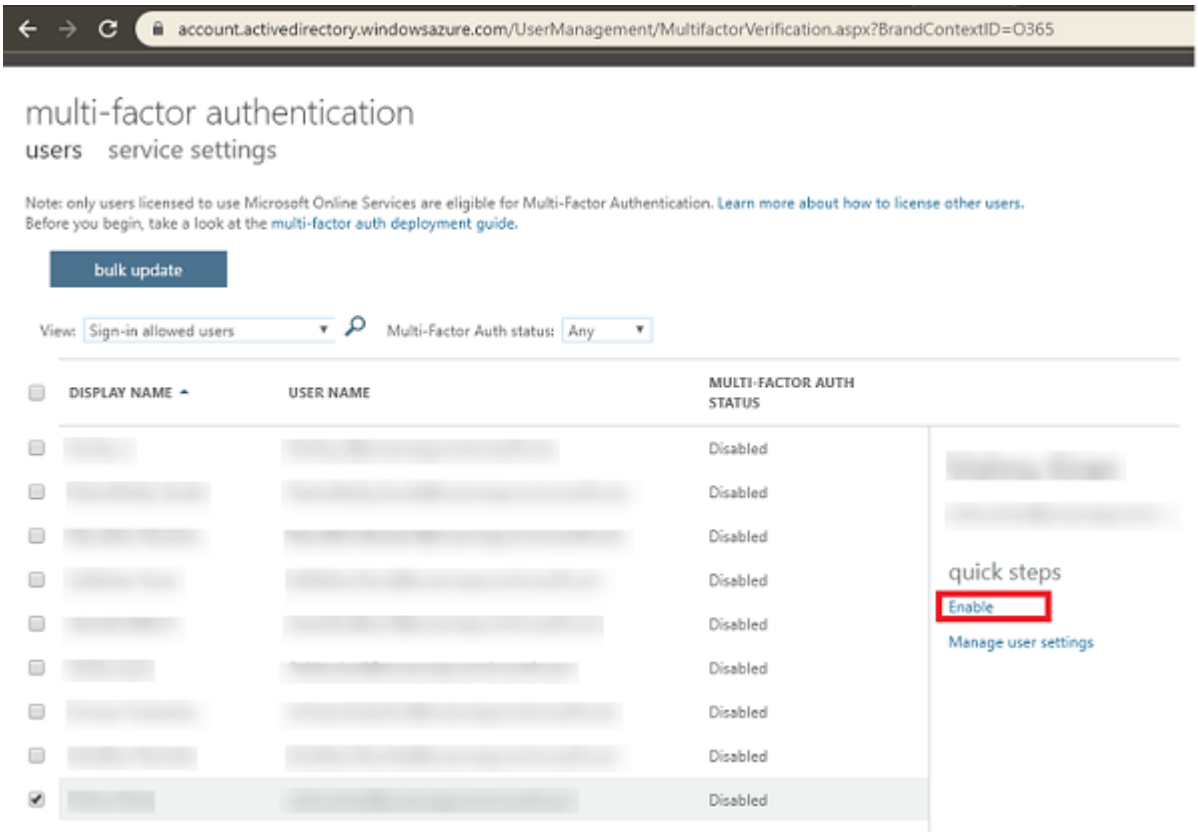
7. From the users screen, perform the following steps:

a. Select the check box for the users to enable MFA.



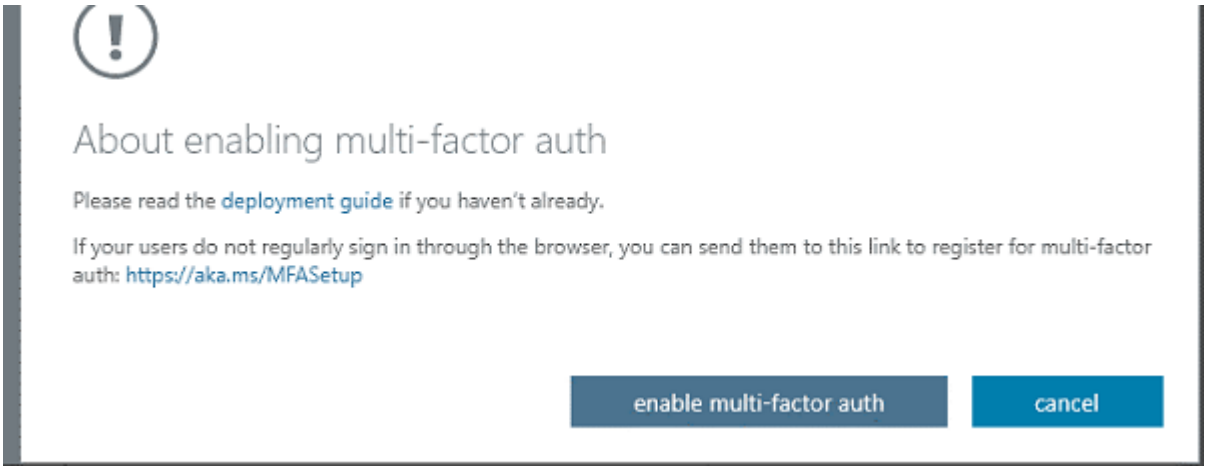
The right pane displays name of the user and under quick steps, you can view Enable and Manage user settings.

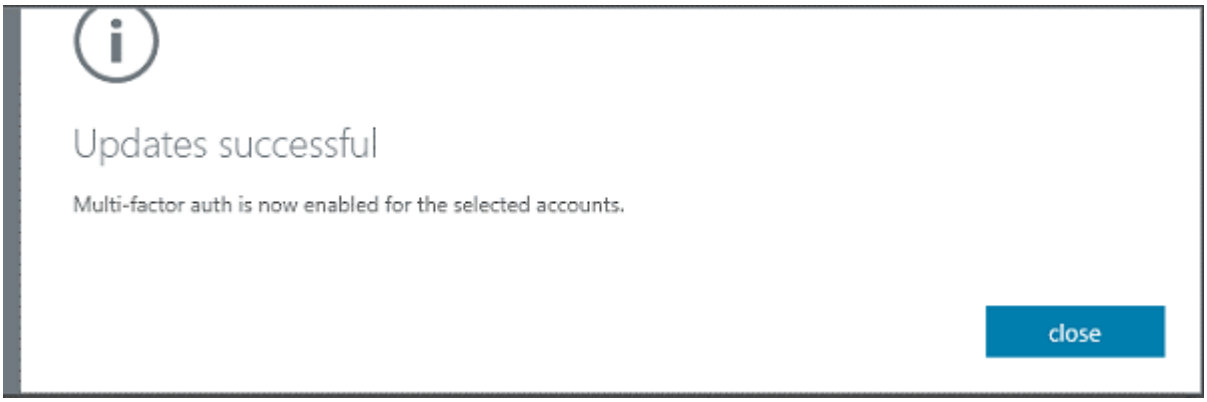
b. Click **Enable**.



A dialog box appears.

c. From the dialog box, click **enable multi-factor auth.**





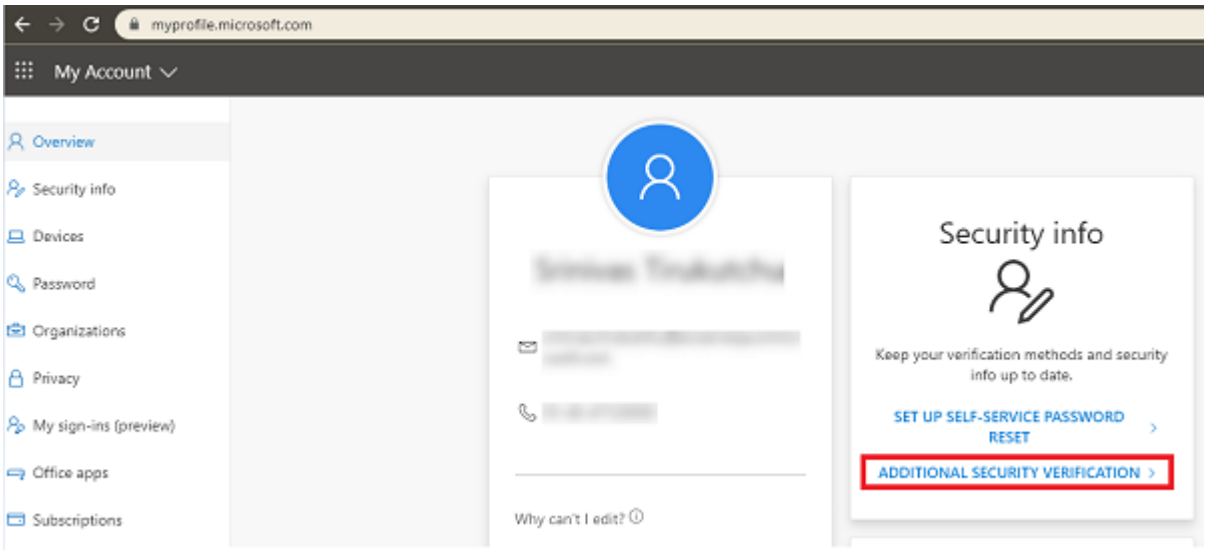
The backup service account to Set app password is enabled.

Creating app password for the backup service account

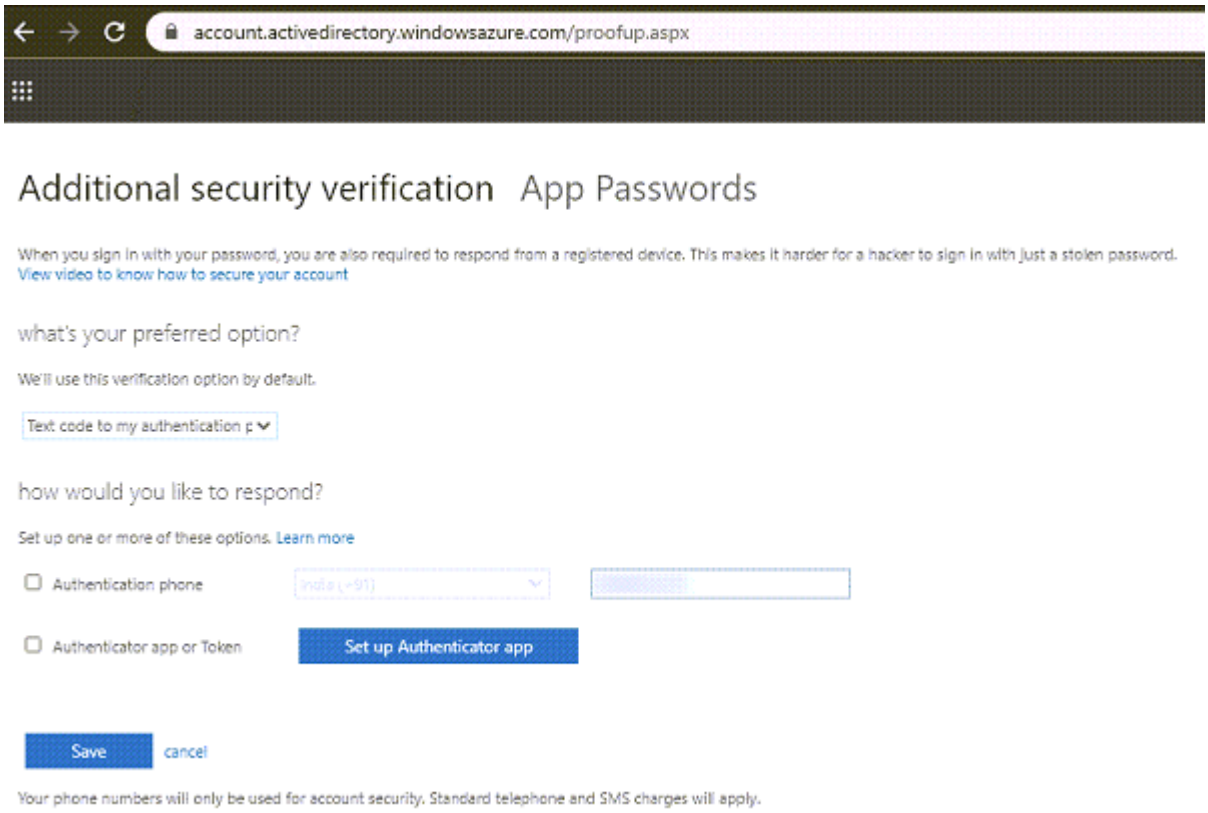
After enabling the backup service account to Set app password, the backup plan needs to use App Password for the backup service account. You need to create app password for the backup service account.

Follow these steps:

1. Sign into Office 365 (https://myprofile.microsoft.com/) with your work or school account and password.
2. Click **Additional Security Verification.**

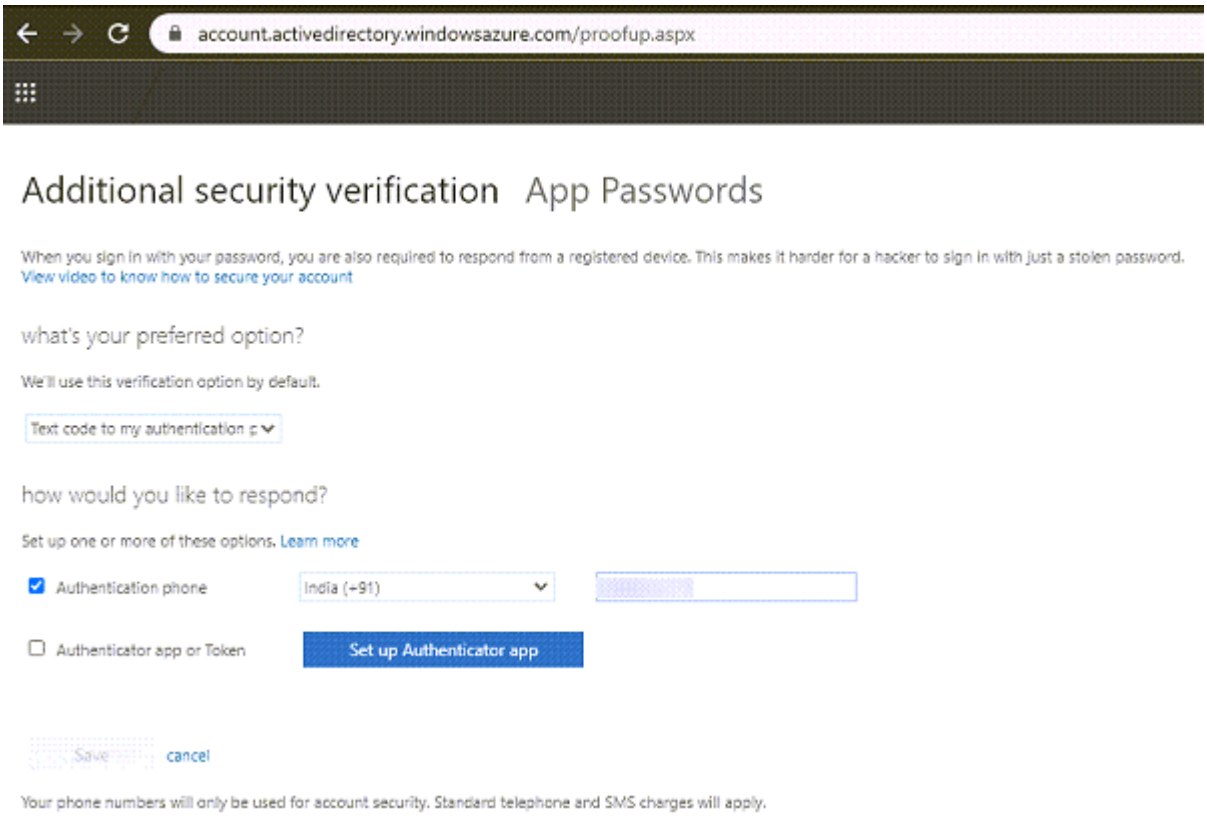


The Additional security verification screen appears.



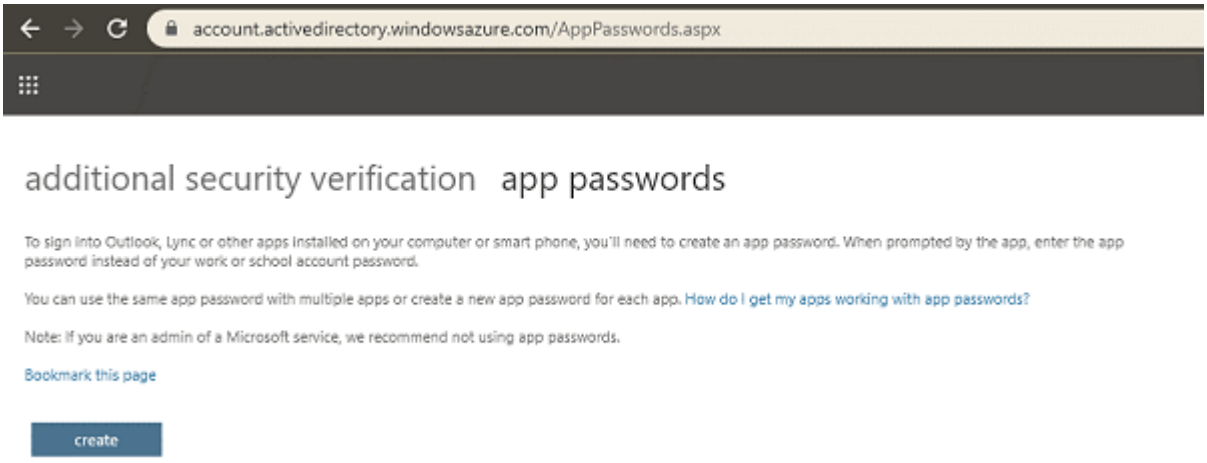
3. Perform the following steps on the Additional security verification screen:
    a. Select your authentication method, and then follow the prompts on the page.

       For example, if you select the authentication phone, you should select your country and enter the phone number. You can also select a method to get the verification code.



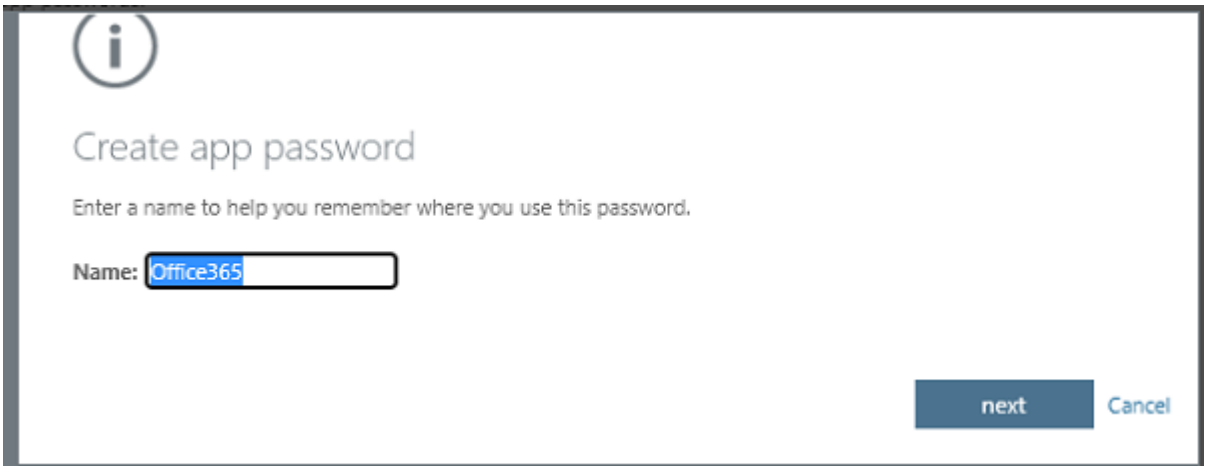
b. Click **App Passwords**.

The app passwords screen appears.



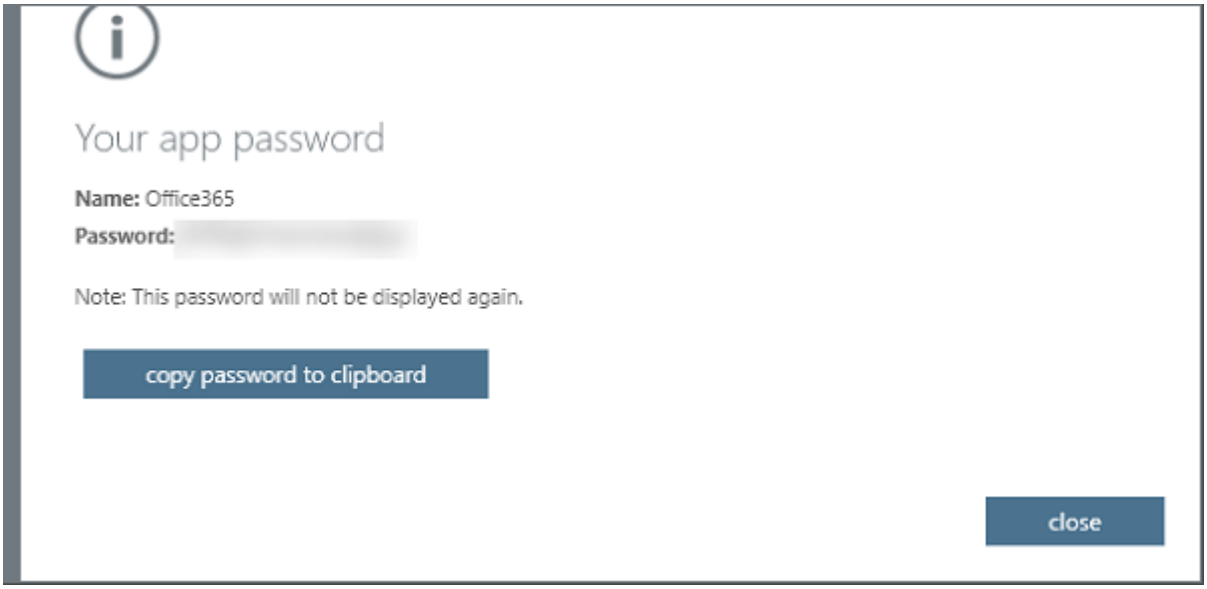
c. Click **create**.

The Create app password screen appears.

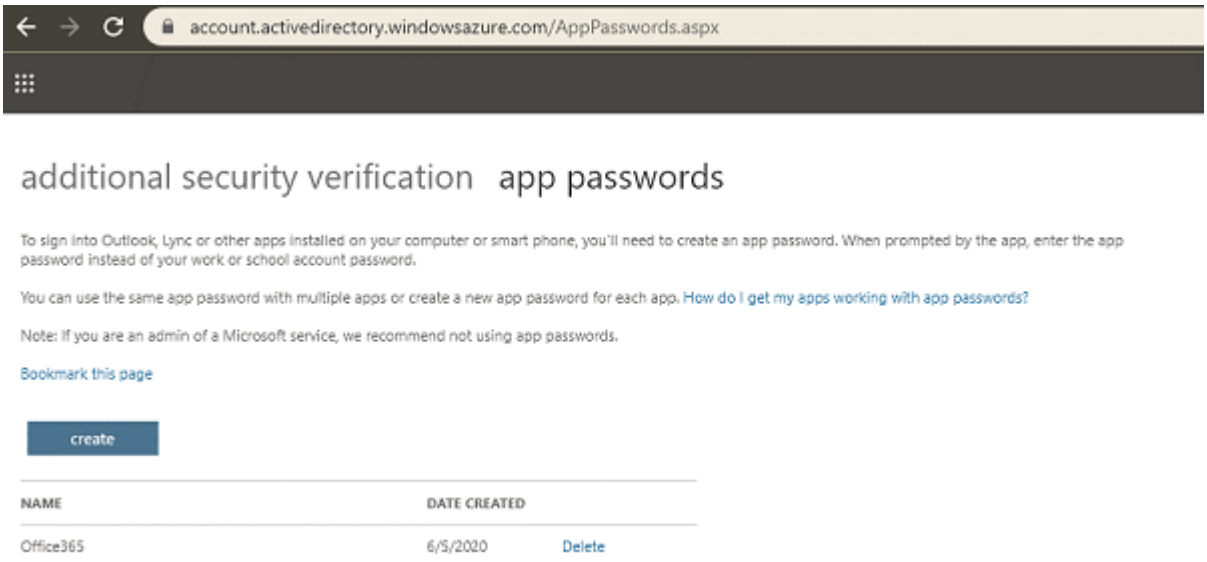


d. From the Create app password screen, enter a name, and then click **next**.

You will receive an app password that you can use with Outlook, Apple Mail, and other Email options.



e. Select the **copy password to clipboard** option and the password is copied to your clipboard.



App password for the backup service account is created.

How to Create a Microsoft Office 365 OneDrive Backup Plan

OneDrive, part of Microsoft Office 365 Cloud service, facilitates cloud storage and sharing of files. To protect your Onedrive items (Files, Folders, and so on) from Microsoft cloud, you need to create a plan. The plan for OneDrive consists of a backup task. This backup task lets you specify the OneDrive nodes that you want to protect, the backup destination, and the backup schedule.

What To Do Next?

1. Review the Prerequisites and Considerations
2. Create a OneDrive Backup Plan
3. (Optional) Perform a Manual Backup
4. Verify the Backup

Review the Prerequisite and Consideration

Prerequisite:

- Console server must connect to Microsoft Azure.
- If modern authentication is set on O365 tenant and Arcserve UDP is recently upgraded to support it, the existing Exchange online jobs needs to be reconfigured with modern authentication related settings, which is described in the Modern Authentication section.

Create a OneDrive Backup Plan

A backup plan includes a backup task that performs a backup of OneDrive data items (Files, Folders, and so on) and stores data either at a non-deduplication data store or deduplication data store. Each task consists of parameters that define the source, destination, schedule, and other backup details.

Follow these steps:

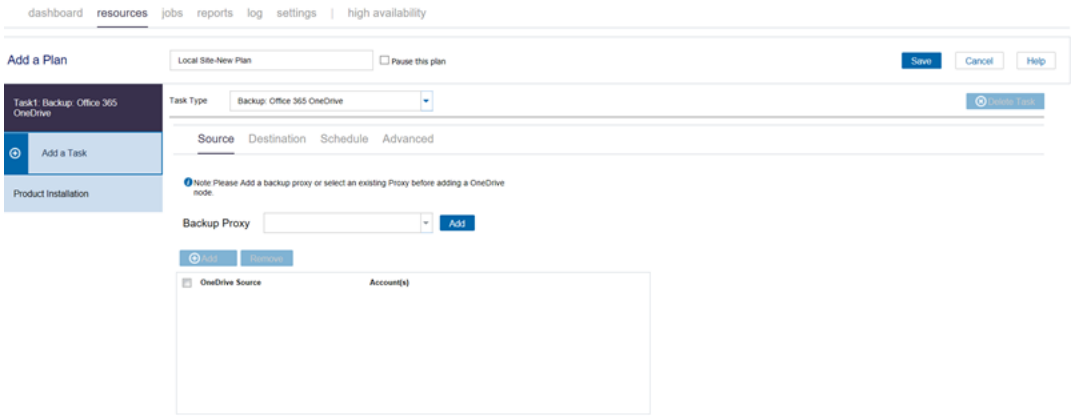
1. Click the **resources** tab on the Console.
2. From the left pane, navigate to **Plans**, and click **All Plans**.

   If you have created plans earlier, those plans are displayed on the center pane.
3. On the center pane, click **Add a Plan**.

   The **Add a Plan** dialog opens.
4. Enter a plan name.
5. (Optional) Select the **Pause this plan** check box.

   The plan does not run until you clear the check box to resume the plan.

   Note: If a plan is paused, then any in-progress job is not paused but all corresponding scheduled jobs associated with that plan are paused. However, you can manually run a job. For example, you can manually run backup job and replication job for a node even if the respective plan is paused. In such case, the following task to the on-demand (manual) job does not run. For example, there is a replication task after an on-demand backup job, the replication job does not run for the on-demand backup job. You need to manually run the replication job. When you resume the plan, the pending jobs do not resume immediately. After you resume the plan, the pending jobs run from the next scheduled time.
6. From the **Task Type** drop-down list, select **Backup: Office 365 OneDrive**.



Now specify the Source, Destination, Schedule, and Advanced details.

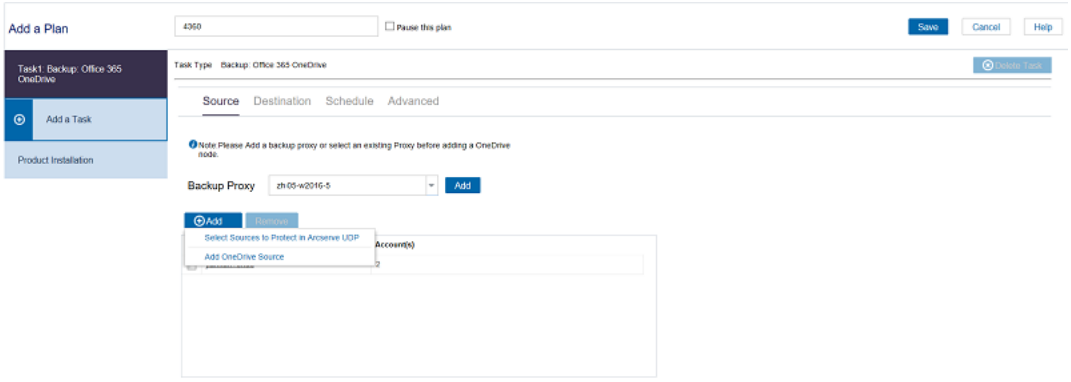
Specify the Source

The Source page lets you specify the OneDrive source nodes that you want to protect. You can select more than one OneDrive source nodes in a plan. If you have not added any nodes to the Console, you can add OneDrive source nodes from the Source page.

Note: You can save a plan without adding any source nodes but the plan is not deployed unless you add any nodes.

Follow these steps:

1. Click the **Source** tab.



2. Select the **Backup Proxy** from the drop-down list.
3. Add OneDrive node using one of the following methods:

   Method 1

   a. Click **Add**, and then click **Select Source to Protect** in Arcserve UDP.

      The Add Nodes to Plan dialog is displayed.

   b. Select a node and click Connect.

      Note: You can also search for the OneDrive nodes that you want to protect in Search.

   c. Select the **Protect all the OneDrive Accounts** check box to protect all the OneDrive accounts across all pages. To select few accounts, click the arrow placed on the right side of check box, and then specify the accounts.

      The OneDrive accounts that you selected are added.

   Method 2

   a. Click **Add**, and then click **Add OneDrive Source** in Arcserve UDP.

      Note: Unlike other nodes, you cannot add the OneDrive node from All Nodes page. You can add a OneDrive node only in a plan or when you modify a plan.

b. To add OneDrive node by plan, specify the node name, user name, and password. You cannot change the nodename after creating the OneDrive node. Multiple OneDrive nodes can use the same user account (service account) of OneDrive.

   Note: We recommend selecting user accounts of Azure Active Directory Administrators.

4. After you click Add Nodes, you can select Basic Authentication or Modern Authentication to add the Exchange node by plan.

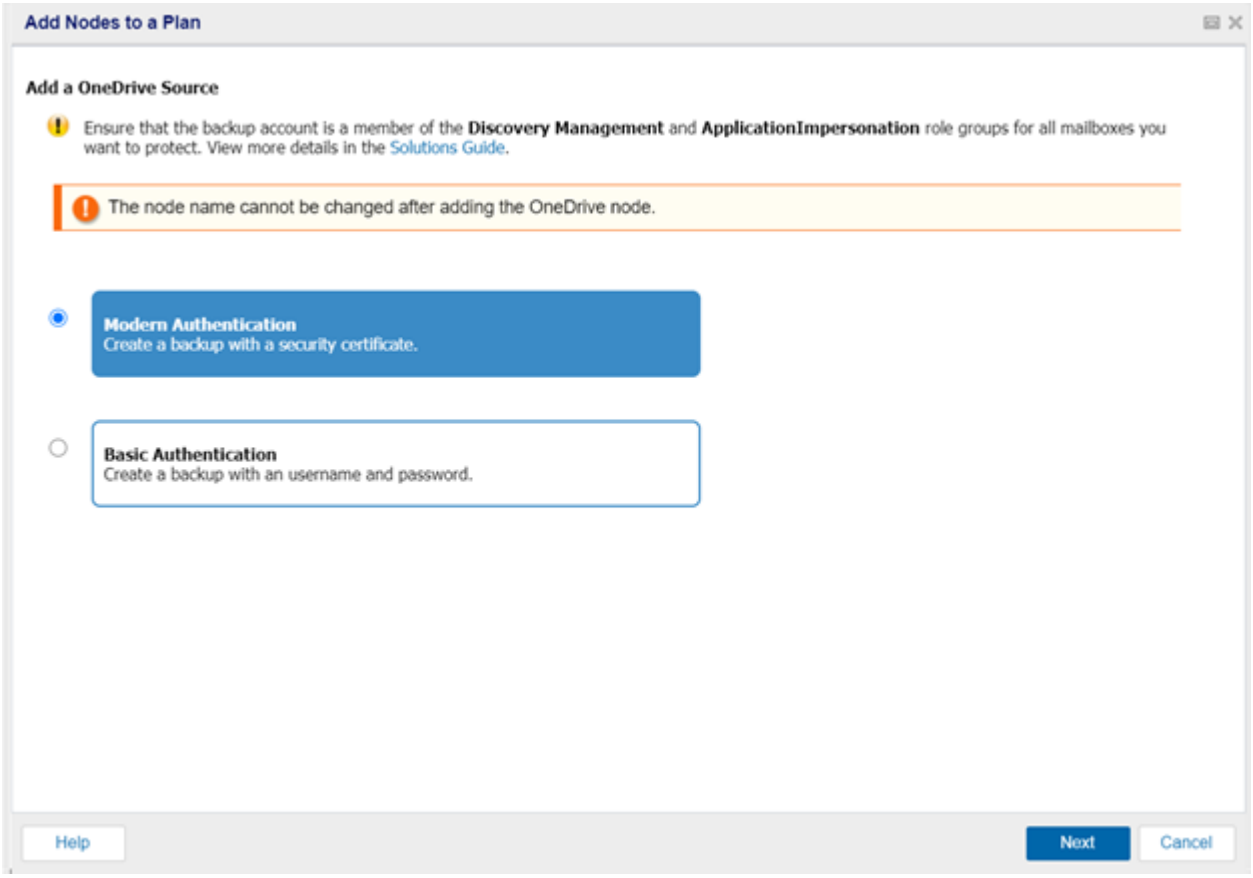
   For Basic Authentication, provide the following information:

   - Node name
   - Site Collection URL
   - User Name
   - Password

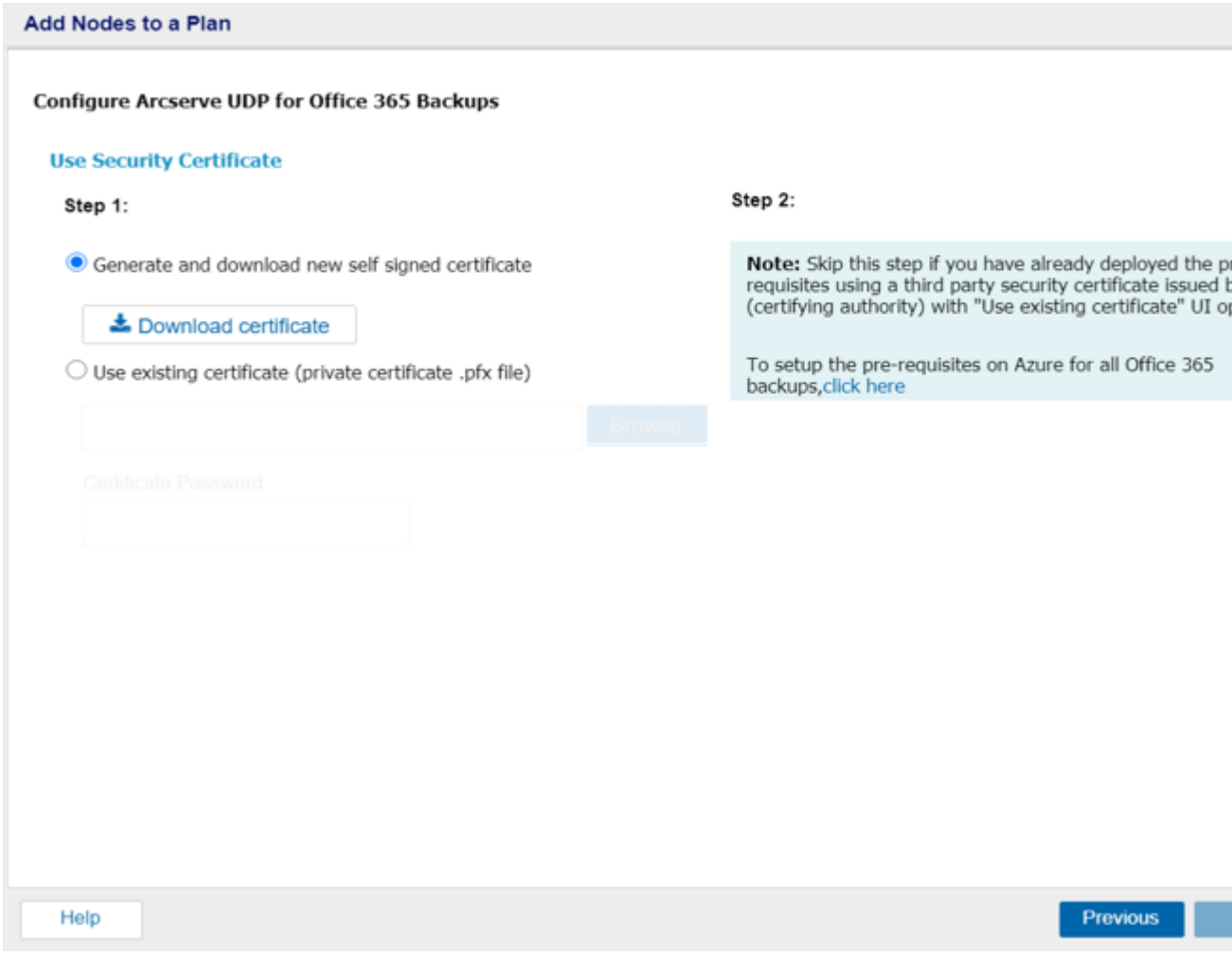
   For Modern Authentication, provide the following information:

   - Node name
   - Site Collection URL
   - Application ID
   - User name

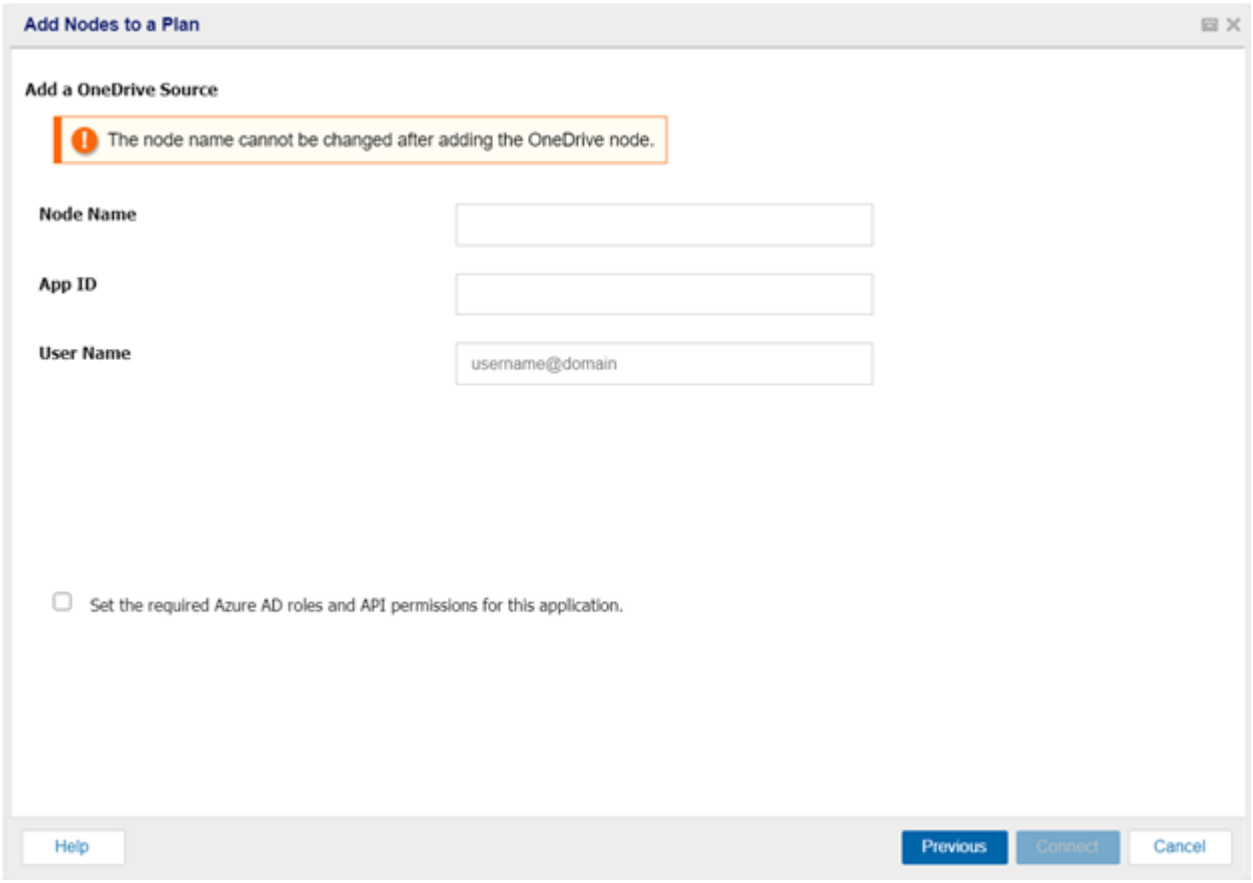
   Note: Exchange online node names cannot change after creating the node.



a. To authenticate the UDP application with security certificates, see How to Use Security Certificates.



5. After you upload the certificate to the Azure portal, in the UDP console provide Node Name, Application ID, and Username. To accept the AzureAD Admin consent, select the checkbox, and then click **Connect** to register the node.



If basic authentication is set on Office 365 tenant, do the following:

a. Select the Basic Authentication option, and then type Node name, Username and Password.

   The Arcserve UDP URL opens in a browser and requests permission for all Arcserve UDP read-write data from the OneDrive portal.

b. In the browser, use the Microsoft Azure administrator credentials to sign in.

   The Azure portal opens.

c. From the Microsoft Azure portal, perform the following steps to configure the UDP App:

   i. Click **API permissions**.
   ii. On the right pane, click the **Grant permissions for** button.
   iii. Click **Yes** to agree to Grant permissions.
   iv. After granting permission, in Arcserve UDP, navigate to **Add a Plan > Add Nodes to a Plan**, and then click the **Next** button.

   Note: If you close the grant permission URL and want to reopen it, click the **Here** button in the UDP Add Node to Plan screen.

Arcserve UDP lists all the account under current tenant.

6. Select the OneDrive accounts that you want to protect and click the right arrow (>) to move them to the protected list.

   Note: Select the **Protect all the OneDrive Accounts** check box to protect all the OneDrive accounts across all the pages.

7. Click **Save**.

   The selected OneDrive accounts are added.

Specify the Destination

The destination is a location where you store the backup data. You must at least specify the destination to save the plan.

Follow these steps:

1. Click the **Destination** tab.

   The **Arcserve UDP Recovery Point Server** option is automatically selected. **Arcserve UDP Recovery Point Server** specifies that the backup destination is a recovery point server. If you select this option, the data is stored as recovery points. You cannot store data as recovery sets.

2. Provide the following details:

   a. Select a recovery point server.

   b. Select a non-deduplication or deduplication data store. The list displays all the data stores created on the specified recovery point server.

   c. Provide a session password. The session password is optional when the backup destination is an unencrypted RPS data store.

   d. Confirm the session password.

The destination is specified. Now, specify the Schedule and Advanced details.

Specify the Schedule

The Schedule page lets you define a schedule for Backup, Merge, and Throttle functions to repeat at specific intervals. After you define a schedule, the jobs run automatically per the schedule. You can add multiple schedules and can provide retention settings.

A Backup Schedule refers to regular schedule that is repeated multiple times a day based on the number of hours or minutes you select. Besides the regular schedule, a backup schedule also provides options to add daily, weekly, and monthly schedules.

Note: For more information on scheduling and retention settings, see Understanding Advanced Scheduling and Retention.

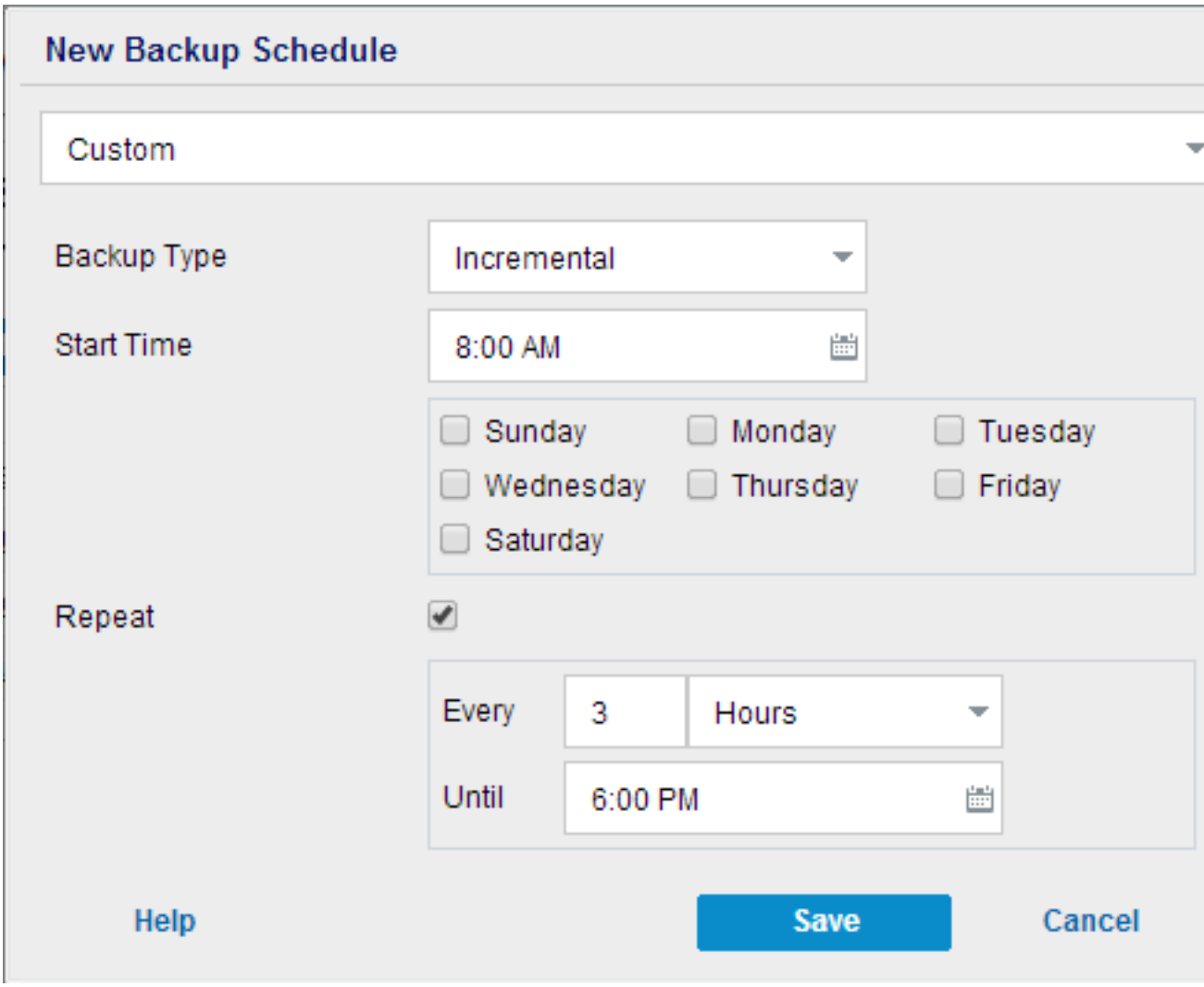
Follow these steps:

1. Add backup, merge, and throttle schedules.

   Add Backup Schedule

   a. Click **Add** and select **Add Backup Schedule**.

      The **New Backup Schedule** dialog opens.



b. Select one of the following options:

Custom

Specifies the backup schedule that repeats multiple times a day.

Daily

Specifies the backup schedule that occurs once a day. By default, all the days of the week are selected for Daily backup. If you do not want to run the backup job on a specific day, clear the check box for that day of the week.

Weekly

Specifies the backup schedule that occurs once a week.

Monthly

Specifies the backup schedule that occurs once a month.

c. Select the backup type.

Full

Determines the backup schedule for Full Backups. As scheduled, Arcserve UDP performs a full backup of all used blocks from the source machine. A full backup typically consumes time depending on the backup size.

Incremental

Determines the backup schedule for Incremental Backups.

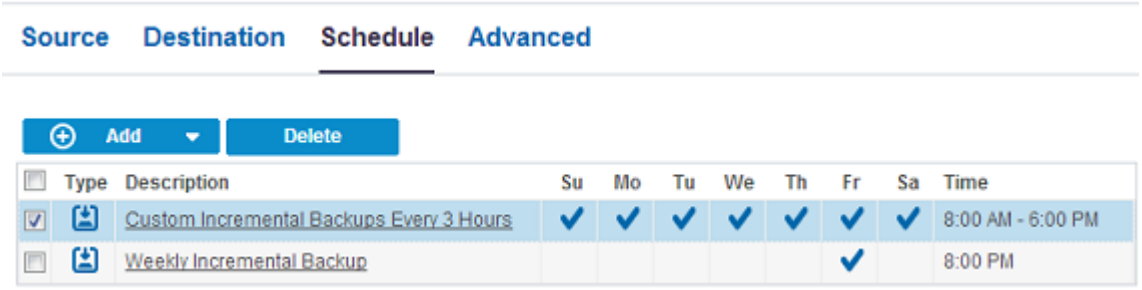
As scheduled, Arcserve UDP incrementally backs up only those blocks that have changed after the last successful backup. The advantages of Incremental Backups are that the backup is a fast backup and it produces a small backup image. This option is the most optimal way to perform a backup.

d. Specify the backup start time.

e. (Optional) Select the **Repeat** check box and specify the repeat schedule.

f. Click **Save**.

The Backup Schedule is specified and appears on the **Schedule** page.



Add Merge Schedule

a. Click **Add** and select **Add Merge Schedule**.

The **Add New Merge Schedule** dialog opens.

b. Specify the start time to start the merge job.

c. Specify **Until** to specify an end time for the merge job.

d. Click **Save**.

The Merge Schedule is specified and appears on the **Schedule** page.

Add Throttle Schedule

a. Click **Add** and select **Add Throttle Schedule**.

The **Add New Throttle Schedule** dialog opens.

b. Specify the throughput limit in MB per minutes unit.

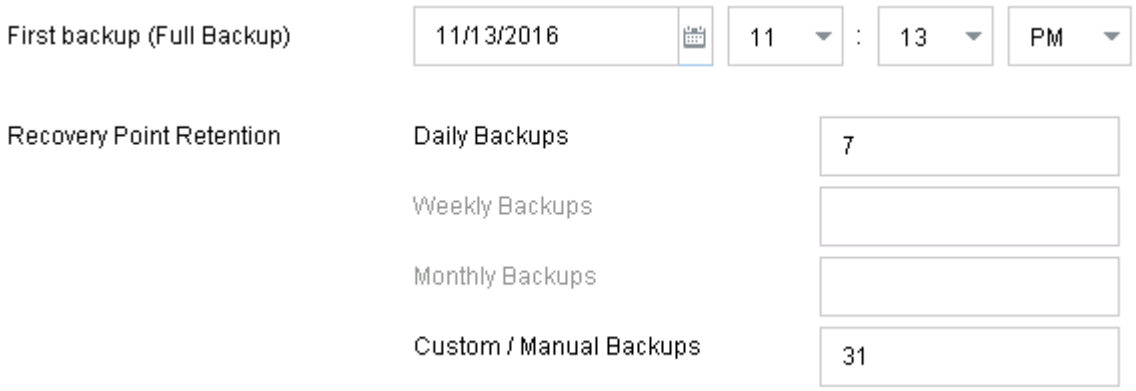
c. Specify the start time to start the backup throughput job.

d. Specify **Until** to specify an end time for the throughput job.

e. Click **Save**.

The Throttle Schedule is specified and displayed on the **Schedule** page.

2. Specify the start time for the scheduled backup.



3. Specify the recovery points retention settings for Custom, Daily, Weekly, and Monthly schedule.

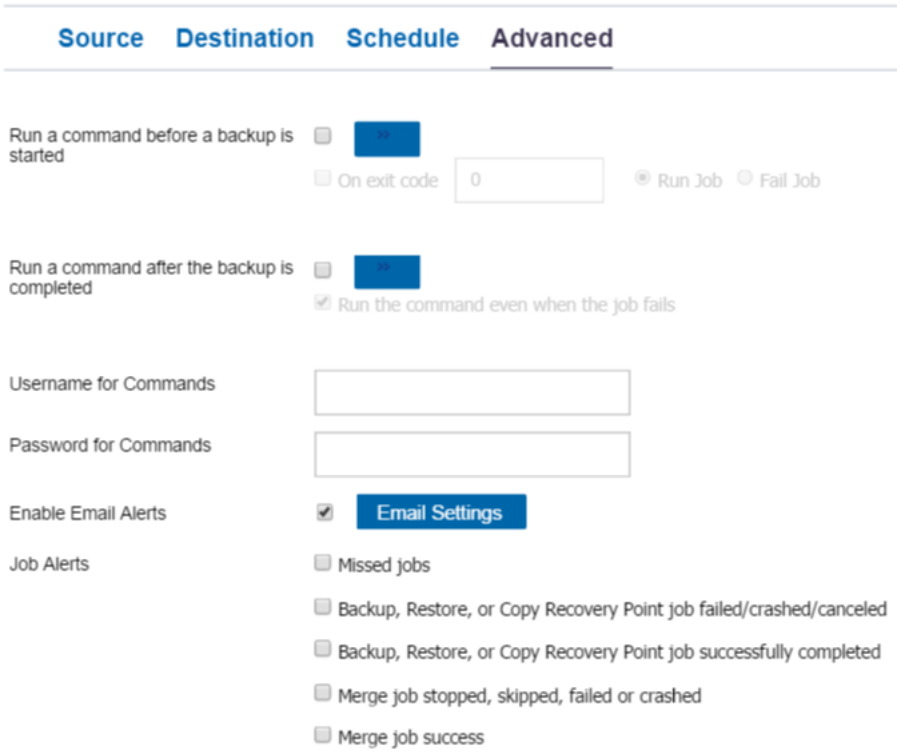
   These options are enabled if you have added the corresponding backup schedule. If you modify the retention settings on this page, the changes are reflected on the **Backup Schedule** dialog.

   The schedule is specified. Now specify Advanced details.

Specify the Advanced Settings

The **Advanced** tab lets you specify some advanced settings for the backup job. The advanced settings include providing the location of any scripts, and email settings.

The following image displays the **Advanced** tab:



Follow these steps:

1. Specify the following details.

   Run a command before a backup is started

   Lets you run a script before the backup job starts. Specify the path where the script is stored inside the proxy node. Click **On exit code** and specify the exit code for **Run Job** or **Fail Job**. **Run Job** indicates that the backup job continues when the script returns the exit code. **Fail Job** indicates that the backup job stops when the script returns the exit code.

   Run a command after a backup is completed

   Lets you run a script after the backup job is completed. Specify the complete path where the script is stored.

   Run a command even when the job fails

If this check box is selected, the script specified in **Run a command after a backup is completed** is executed even when the backup job fails. Otherwise, that script is executed only when backup job completes successfully.

Username for Commands

Lets you specify the username to run the commands.

Password for Commands

Lets you specify the password to run the commands.

Enable Email Alerts

Lets you enable email alerts. You can configure email settings and specify the types of alerts that you want to receive in an email. When you select this option, the following options are enabled for your selection.

Email Settings

Lets you configure the email settings. Click **Email Settings** and configure the email server and proxy server details. For more information about how to configure Email Settings, refer to Email and Alert Configuration.

Job Alerts

Lets you select the types of job alert emails that you want to receive.

2. Click **Save**.

Note: When you select a node as a backup source or backup proxy, Arcserve UDP checks whether the agent is installed on proxy node and if it is the latest version. Arcserve UDP then displays a verification dialog that lists all the nodes that either have an outdated version of the agent or does not have the agent installed. To install/upgrade the agent on these nodes, select the installation method and click **Save**.

The changes are saved and a green checkmark appears next to the task name. The plan page closes.

Note: If you have to add another task, you must select the plan from the **resources** tab and modify the plan. To modify the plan, click the plan from the center pane. The plan opens and you can modify it. You may add the **Copy Recovery Point**, **Copy to Tape**, **Replicate**, and **Replicate from a remote RPS** tasks as follow up tasks.

The plan is automatically deployed to the proxy server node.

The exchange online backup plan for the proxy server is created. The backup runs per the schedule that you have configured on the **Schedule** tab. You can also perform a manual backup at any time.

(Optional) Perform a Manual Backup

Typically, backups are performed automatically and are controlled by the schedule settings. In addition to the scheduled backup, a manual backup provides you the option to back up your nodes on a need basis. For example, if you have a repeat schedule for Full and Incremental backups and you want to make major changes to your machine, you should perform an immediate manual backup without waiting for the next scheduled backup to occur. You can submit the backup job from both, Console and proxy user interface. Using the Job Monitor, you view the job status and cancel the ongoing job.

Follow these steps: to perform a manual backup of OneDrive nodes

1. From the Console, click the **resources** tab.
2. From the left pane, navigate to **Nodes**, and click **All Nodes**.

   The OneDrive nodes are displayed in the center pane.
3. Select the OneDrive nodes that you want to backup and that has a plan assigned to it.
4. On the center pane, click **Actions**, **Backup Now**.

   The **Run a backup now** dialog opens.
5. Select a backup type and optionally provide a name for the backup job.
6. Click **OK**.

   The backup job runs.

Follow these steps: to perform a manual backup of a OneDrive plan

1. From the Console, click the **resources** tab.
2. From the left pane, navigate to **Plans**, and click **All Plans**.

   The OneDrive backup plans are displayed in the center pane.
3. Select the plan that you want to backup and that has a plan assigned to it.
4. On the center pane, click **Actions**, **Backup Now**.

   The **Run a backup now** dialog opens.
5. Select a backup type and optionally provide a name for the backup job.
6. Click **OK**.

   The backup job runs.

   The manual backup is successfully performed. Now, you can verify the Backup.

Verify the Backup

To verify your backup, confirm that you have successfully created the backup plan. After you verify that the plan is created successfully, confirm whether the backup job is running as scheduled. You can verify the status of backup jobs from the **Jobs** tab.

Follow these steps to verify plans:

1. Click the **resources** tab.
2. From the left pane, navigate to **Nodes**, and click **All Nodes**.

   A list of all nodes is displayed on the center pane.
3. Verify that plans are mapped with nodes.

Follow these steps to verify backup jobs:

1. Click the **jobs** tab.
2. From the left pane, click **All Jobs**.

   The status of each job is listed on the center pane.
3. Verify that the backup job is successful.

   The backup job is verified.

Restoring Protected Data

This section contains the following topics:

How to Restore Exchange Online Mailbox Data

You can restore Exchange Online mailbox data (emails, calendars, contacts, notes, tasks, and so on) from Microsoft cloud using any computer. You can restore data from recovery point to the original or an alternate location.

Perform the following tasks to restore Exchange Online mailbox data:

1. Select the Exchange Online Mailbox Items to Restore
2. Define the Restore Options
3. Restore the Recoverable Items
4. Restore the Recovery Point Content
5. Verify that Content is Restored

Select the Exchange Online Mail Items to Restore

You can restore Exchange Online mail data from a recovery point. When you select a recovery date, and then specify the time, all the associated recovery points for that duration are displayed. You can then browse and select the backup content (including applications) to restore.

Follow these steps:

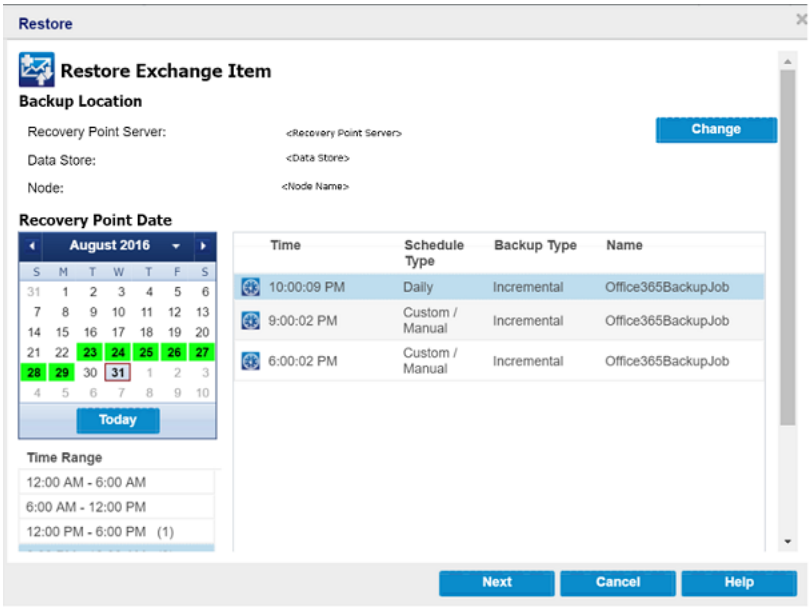
1. Log in to Arcserve UDP.
2. Click the **resources** tab.
3. Select **All Nodes** in the left pane.

   All the added nodes are displayed in the center pane.
4. In the center pane, select the Exchange Online node and click **Actions**.
5. Click **Restore** from the **Actions** drop-down menu.

   The **Restore Exchange Item** dialog opens.

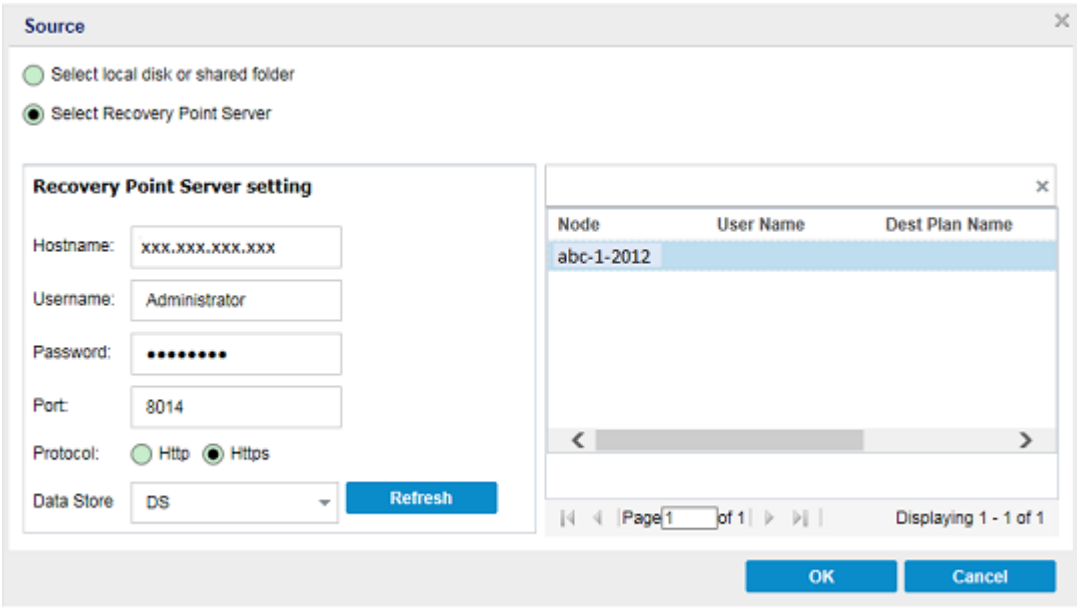
   Note: You are automatically logged in to the agent node and the **Restore Exchange Item** dialog opens.

   You can see the **Recovery Point Server** details in the **Backup Location**.



6. (Optional) Click **Change**, if you want to modify change the backup location.

   The **Source** dialog opens. You can select the backup location in this dialog.



7. To specify Source, select one of the following options, and click **OK**:

   Select local disk or shared folder

   Note: In Arcserve UDP, we do not recommend to select the **Select local disk or shared folder** option.

   Select Recovery Point Server

   a. Specify the Recovery Point Server setting details and click **Refresh**.

      All the agents are listed in the Data Protection Agent column in the **Source** dialog.

   b. Select the agent from the displayed list and click **OK**.

      The recovery points are listed in the **Restore Exchange Item** dialog.

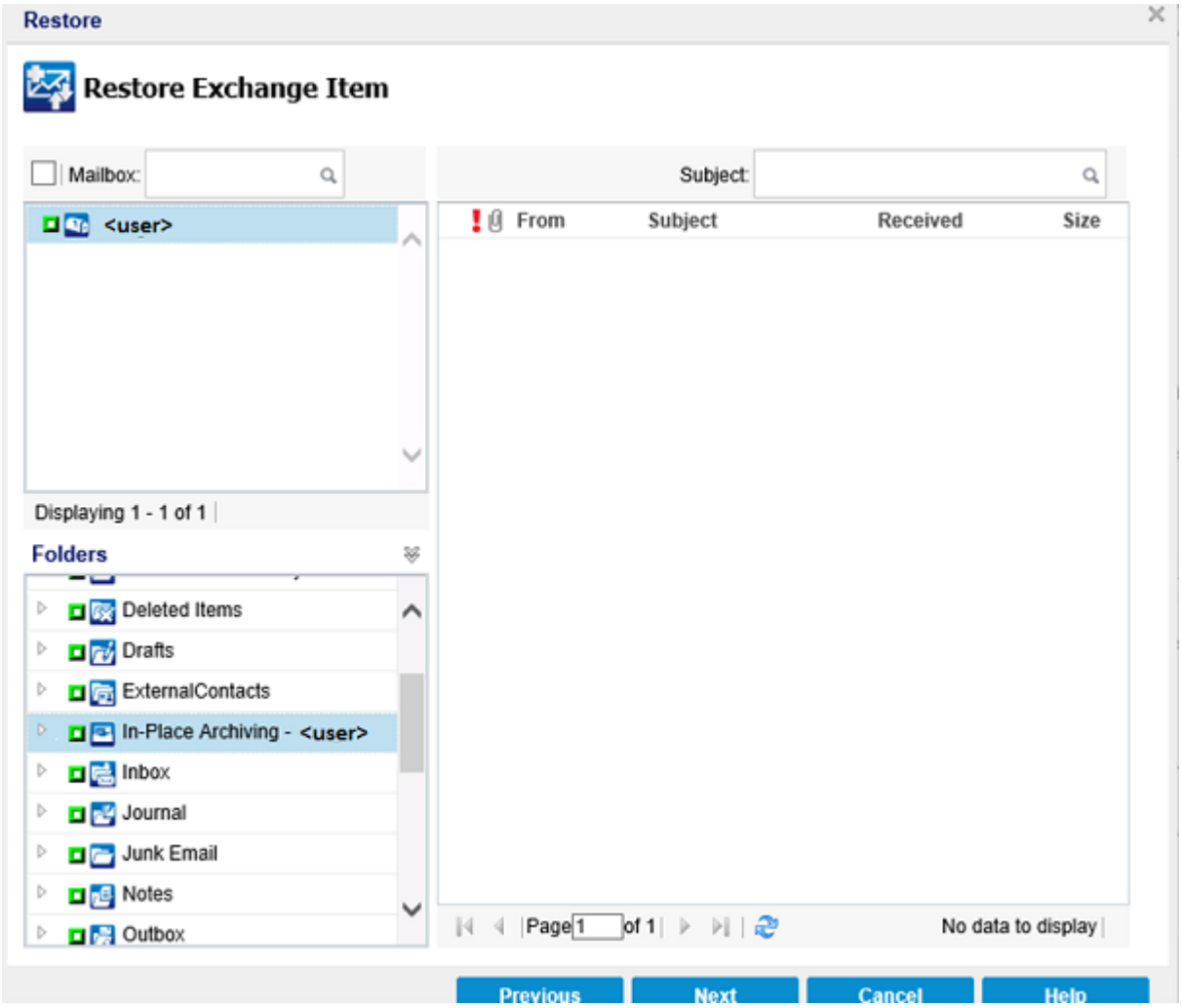
      Note: From the recovery point **Folder**, you may see many folders with the same name along with the exchange online nodes. This happens because the node GUID changes and a new recovery point folder is created when you delete a node and add again in the test plan.

8. Select the calendar date for the backup image to restore and click **Next**.

   All the dates containing recovery points for the specified backup source are high-lighted in green.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed (Full, Incremental, or Verify), and the name of the backup.

9. From the **Mailbox** pane, click the mailbox that you want to restore. For example, Archiving.



All mail items related to the mailbox are displayed in the **Folders** pane.

10. Select the related mail items or folders (including the entire mailbox, emails, calendars, contacts, notes, tasks, and so on) that you want to restore from **Folders**, and click **Next**.

Notes:

- You can select the entire content or partial content of the Exchange object to restore. To select partial content, expand the object, and click the check box of that content.
- You can select multiple Exchange objects to restore.

The **Restore Options** dialog opens.

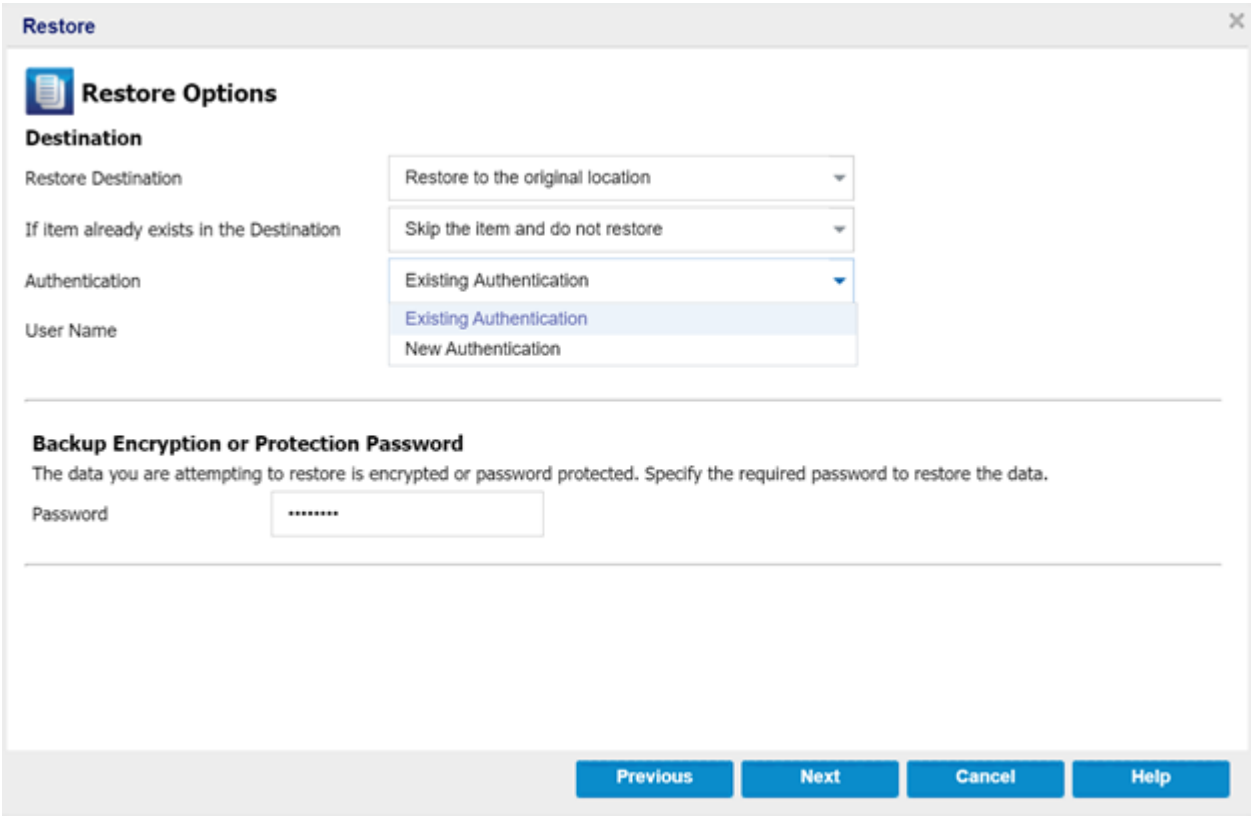
The Exchange Online mail items to restore are selected. Now, you can define the restore options.

Define the Restore Options

After you specify the Exchange Online information to restore, define the restore options for the selected content.

Follow these steps:

1. On the **Restore Options** dialog, select the restore destination.



The available destination options are:

Restore to original location

Restores the mail data to the same location from where you took a back up.

Notes:

- If you restore a mail item to original location using the overwrite option twice, then after restoring second time, the first restore mail item is not over-written. As a result, two similar mail items appear in original location.
- If you restore a mail item to original location using the skip option, and in the original folder an item similar to the restored item already exists, then the backup job displays incomplete result.

Restore to an alternate location

Restores the mail data to another mailbox or another folder in the original mailbox. When you select this option, you can browse and select the destination.

2. Specify one of the following options from the **If Item already exists in the Destination** drop-down:

   Skip the item and do not restore

   Skips over the items and does not restore.

   Default: The Skip the item and do not restore.

   Overwrite the item in the destination

   Overwrites the item in the destination.

   Note: The **If Item already exists in the Destination** drop-down list is available if you select the **Restore to original location** option from the **Restore Destination** drop-down list.

   Authentication

   Validates and identifies the user account. Select one of the following options:

   - **Existing Authentication**

     When you select Existing Authentication, the authentication type that was selected during Node creation is used.

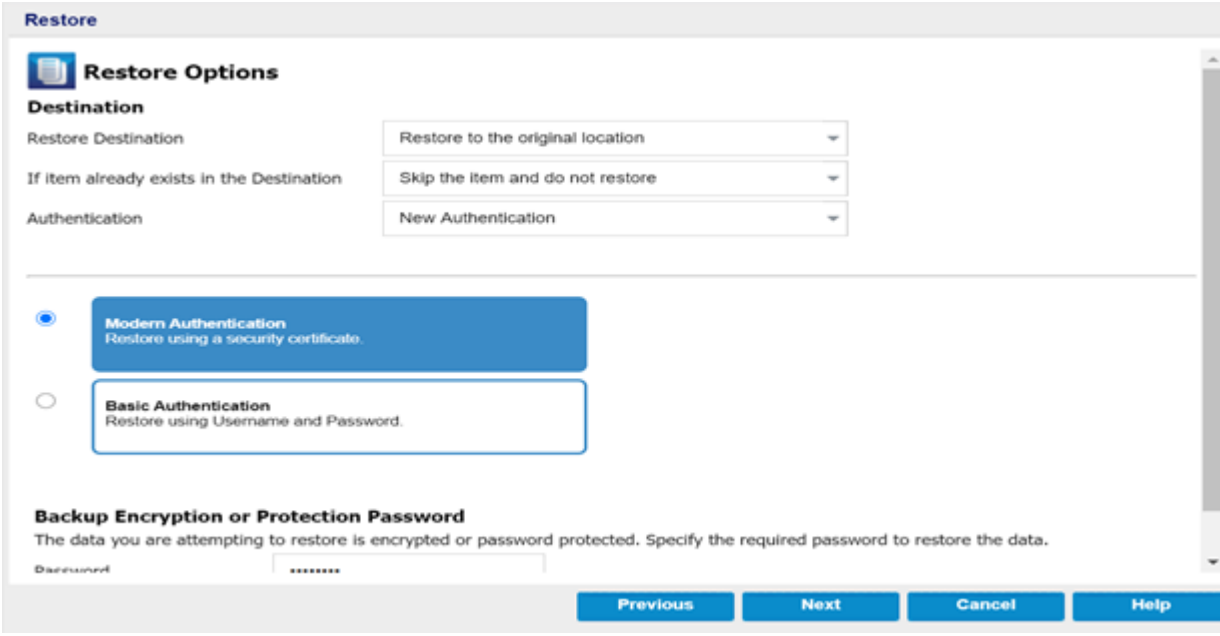
     - If the Node Authentication is basic, parameters such as Username, Password and Backup Encryption or Protection Password [If Encrypted] are loaded automatically to proceed with the restore.
     - If the Node Authentication is modern, parameters such as Username and Backup Encryption or Protection Password [If Encrypted] are loaded automatically to proceed with the restore.

   - **New Authentication**

     During restore, you can select one of the following to change the authentication type:

     - Modern Authentication

- Basic Authentication

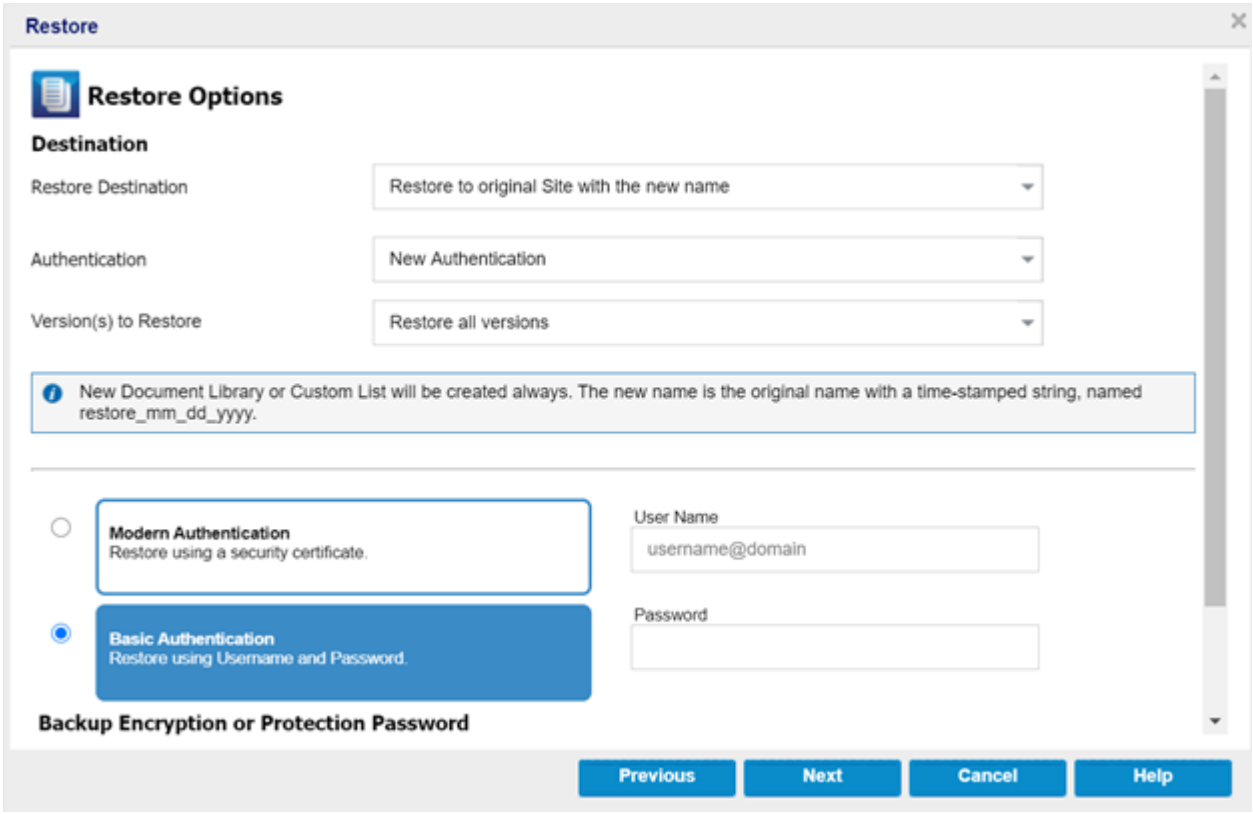


3. To apply authentication, do one of the following:
   - Modern Authentication

     For more information, see How to Use Security Certificates.
   - Basic Authentication

     For Basic Authentication, to proceed with the restore, enter UserName and Password.

     Note: This option fails if you have Modern Authentication enabled on the Tenant or Account.



Specify the **Username** and **Password**, as needed.

4. Click **Next**.

   The **Restore Summary** dialog opens.

   The restore options are defined to restore the Exchange Online information.

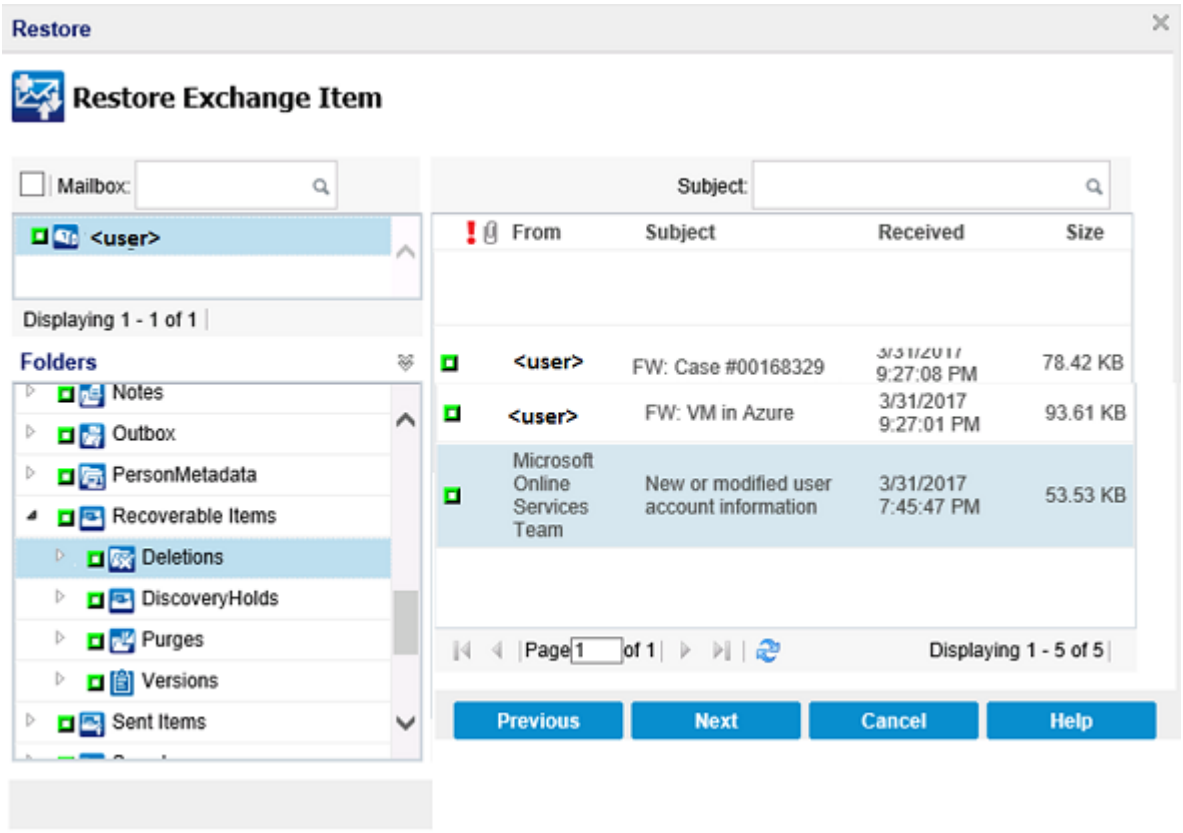
Restore the Recoverable Items

You can restore the recoverable items from the mailbox that enables the In-Place Hold or Litigation Hold feature , from Exchange online node UI to browse backup session. To enable this feature, see Specify the Source.

After you enable the feature, using the Restore wizard you can restore the recoverable items.

Follow these steps:

1. On the **Restore Exchange Item** dialog, select required folders under **Recoverable Items** and click **Next**.



The Restore Option screen is displayed.

2. From the Restore Option screen, perform the following details and click **Next**:
   - Select Restore Destination.
   - Skip or overwrite if the item already exists in the destination.

     You can perform either Original or Alternate restore.

     Original restore

The items under Recoverable Items are restored at the *UDP_RecoverableItems_yyyyMMdd_HHmmssfff* folder that is created on the target mailbox. Skip and Overwrite options for restore are not applicable to these items.

Alternate restore

As with user mailbox, restores the selected items to the destination path in a unique time stamped folder, such as *titled /restore_yyyyMMdd-mmssff*.

- Provide user id and password of the destination where you want to restore.

The selected recoverable items are restored.

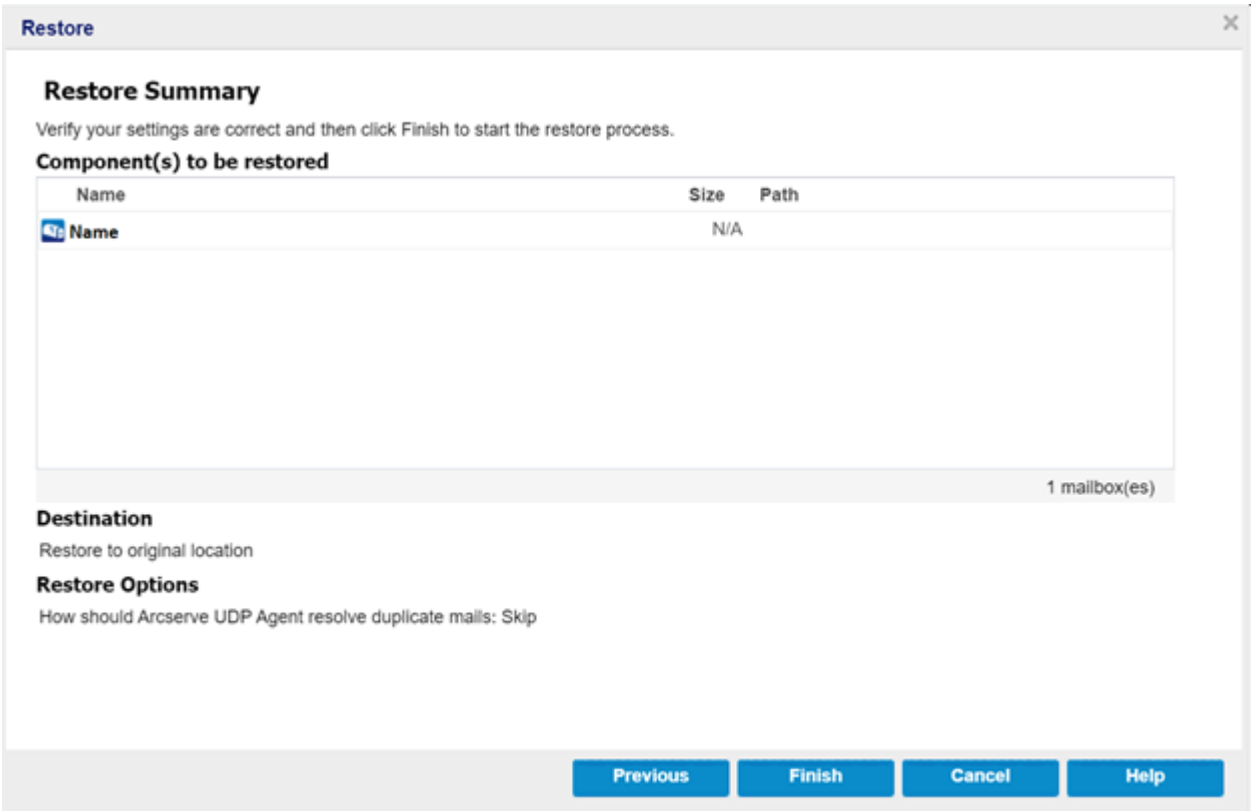
The recovery point content is stored.

Restore the Recovery Point Content

After you define the restore options, verify that your settings are correct and confirm the restore process. **Restore Summary** helps you to review all the restore options that you defined and modify them if necessary.

Follow these steps:

1. On the **Restore Summary** dialog, review the displayed information to verify that all the restore options and settings are correct.



- If the summary information is incorrect, click **Previous** and go back to the applicable dialog to change the incorrect setting.
- If the summary information is correct, click **Finish** to launch the restore job.

The recovery point content is stored.

Verify that Content is Restored

After the completion of the restore process, verify that content was restored to the specified destination.

Follow these steps:

1. Log into the destination mailbox.
2. Check the mailbox item that you restored.
3. Verify the restored content.

   The restored content is successfully verified.

How to Restore SharePoint Online Site Collection Data

You can restore SharePoint Online List/Library or List item in Site. The Site Collection and Site are not supported yet in Arcserve UDP 7.0. You can restore the data to original site with new name, restore the data to original location and export to disk from the recovery points.

Perform the following tasks to restore SharePoint Online List item:

1. Select the SharePoint Online site list Items to Restore
2. Define the Restore Options
3. Verify that Content is Restored

Select the SharePoint Online Site List Items to Restore

You can restore SharePoint Online list items data from a recovery point. When you select a recovery date, and then specify the time, all the associated recovery points for that duration are displayed. You can then browse and select the backup content (including applications) to restore.

Follow these steps:

1. Log into Arcserve UDP.
2. Click the **resources** tab.
3. Select **All Nodes** in the left pane.

   All the added nodes are displayed in the center pane.

   Or

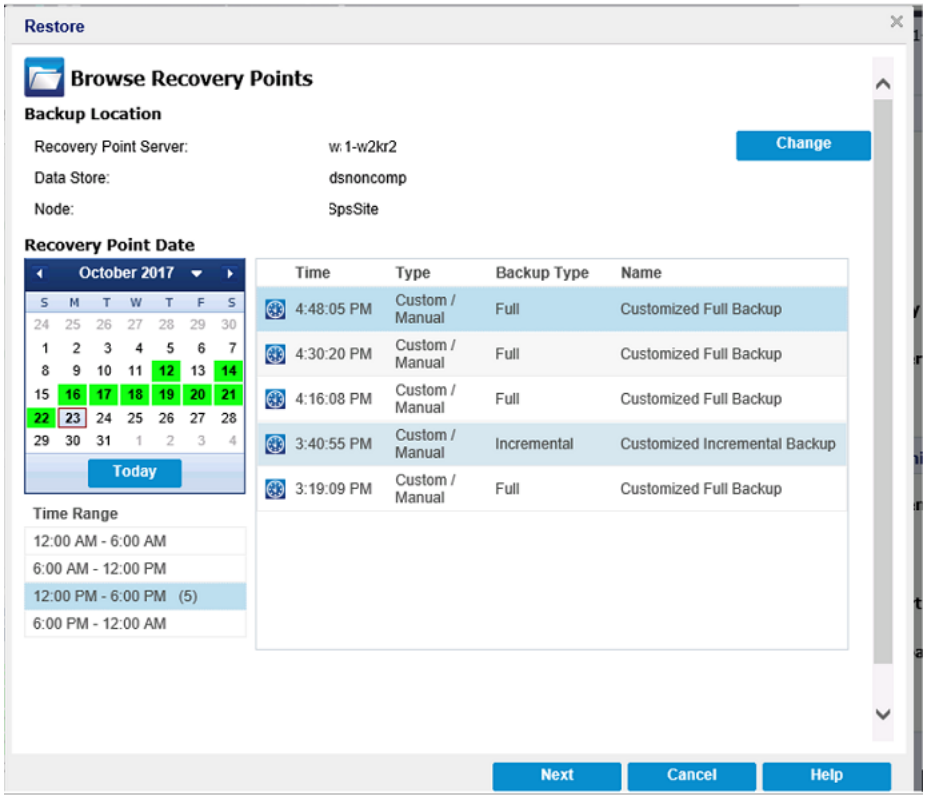
   Select **SharePoint Online Nodes** group.

   All the added SharePoint nodes are displayed in the center pane.
4. In the center pane, select the SharePoint Online node and click **Actions**.
5. Click **Restore** from the **Actions** drop-down menu.

   The **Restore SharePoint Item** dialog opens.

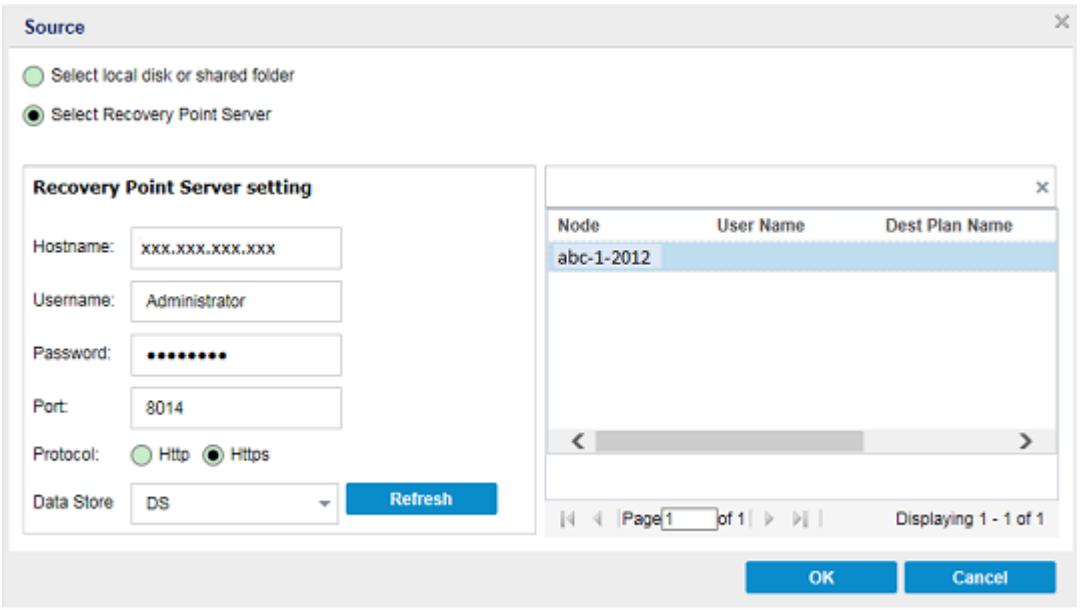
   Note: You are automatically logged into the agent node and the **Restore SharePoint Item** dialog opens.

   The **Backup Location** displays the **Recovery Point Server** details.



6. (Optional) Click **Change** to modify the backup location.

   The **Source** dialog opens. You can select the backup location in this dialog.



7. To specify Source, select one of the following options, and click **OK**:

   Select local disk or shared folder

Note: In Arcserve UDP, we do not recommend to select the **Select local disk or shared folder** option.

Select Recovery Point Server

a. Specify the Recovery Point Server setting details and click **Refresh**.

   All the agents are listed in the Data Protection Agent column in the **Source** dialog.

b. Select the agent from the displayed list/library and click **OK**.

   The recovery points are listed in the **Restore SharePoint Item** dialog.

8. Select the calendar date for the backup image to restore and click **Next**.

   All the dates containing recovery points for the specified backup source are high-lighted in green.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed (Full or Incremental), and the name of the backup.

9. From the **Restore SharePoint Online items** dialog, expand the site collection.

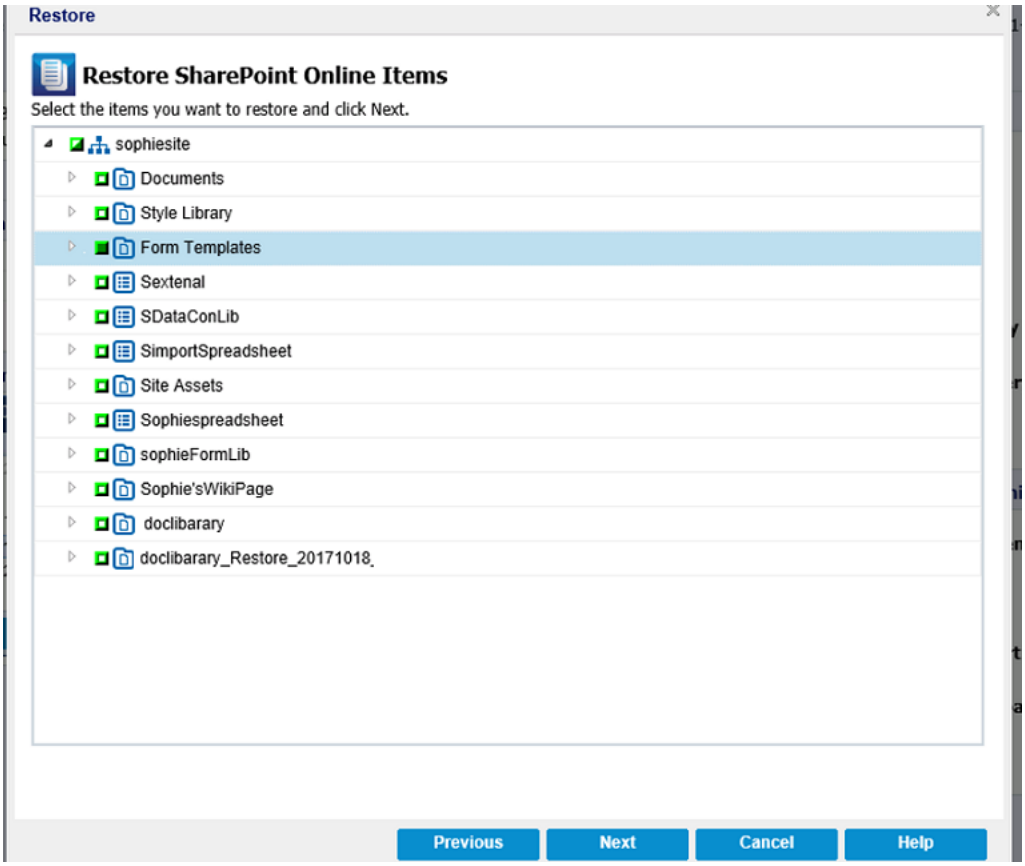
   All lists/Libraries and list are displayed.

10. Select the List/Library or item available in the Site collection that you want to restore from SharePoint site collection and click **Next**.

    Notes:

    - You can select the entire content or partial content of the SharePoint object to restore. To select partial content, expand the object, and click the check box of that content.
    - You can select multiple SharePoint lists/Libraries or list items to restore.

    The **Restore Options** dialog opens.



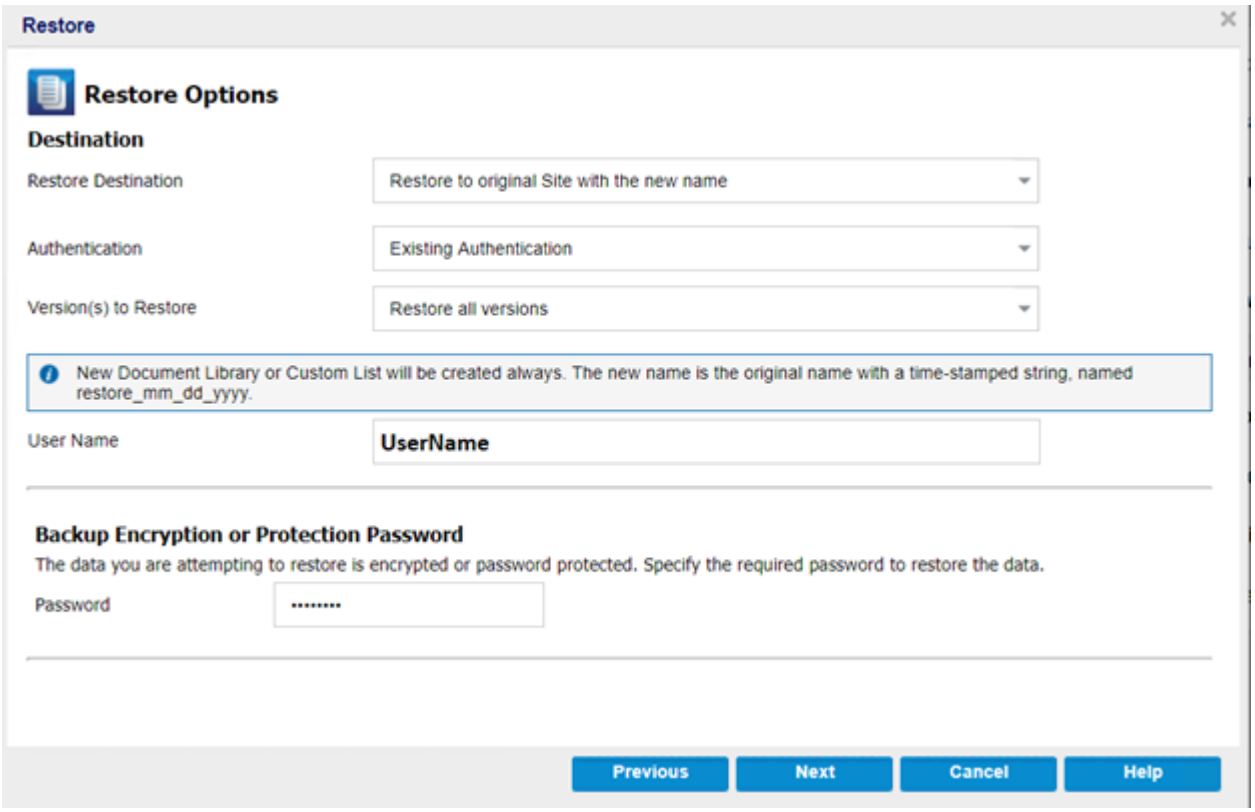
The SharePoint Online lists/Libraries or list items to restore are selected. Now, you can define the restore options.

Define the Restore Options

After you specify the SharePoint Online information to restore, define the restore options for the selected content.

Follow these steps:

1. On the **Restore Options** dialog, select the restore destination.



The available destination options are:

Restore to original Site with the new name

Restores the list/Library and list items data to the same site with new list name from where you took a backup.

Restore to the original location

Restores the list/Library and list items data to the same location from where you took a backup.

2. Specify one of the following options from the **If Item already exists in the Destination** drop-down:

Append as new version if versioning is enable

This option works when your version setting is enabled from library setting in SharePoint Site. Once you choose this option, new version is appended to the current versions of the list items if the list items are existing.

Skip the item and do not restore

Skips over the items and does not restore.

Overwrite the item in the destination

Overwrites the item in the destination.

Export to disk

Restores the lists/Libraries or list items in the site collection to folder or share folder in disk.

Note: For lists restore when selecting restore option of Export to disk, only export attachment(s) of list to disk.

Authentication

Validates and identifies the user account. Select one of the following options:

- **Existing Authentication**

  When you select Existing Authentication, the authentication type that was selected during Node creation is used.

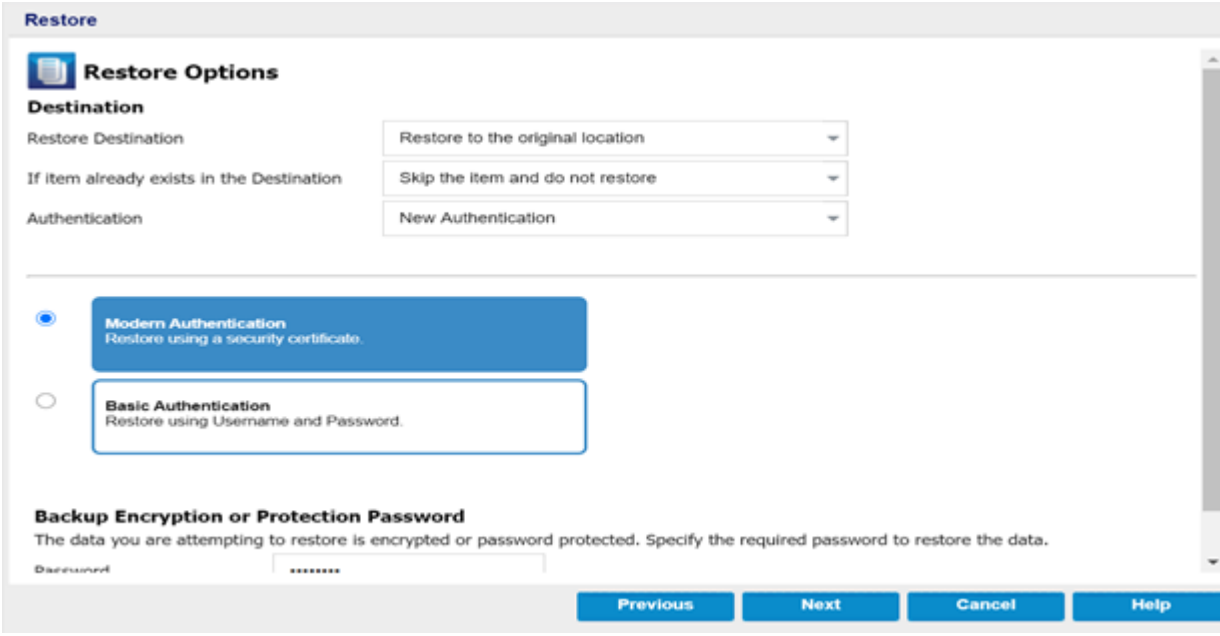
  - If the Node Authentication is basic, parameters such as Username, Password and Backup Encryption or Protection Password [If Encrypted] are loaded automatically to proceed with the restore.
  - If the Node Authentication is modern, parameters such as Username and Backup Encryption or Protection Password [If Encrypted] are loaded automatically to proceed with the restore.

- **New Authentication**

  During restore, you can select one of the following to change the authentication type:

  - Modern Authentication

- Basic Authentication

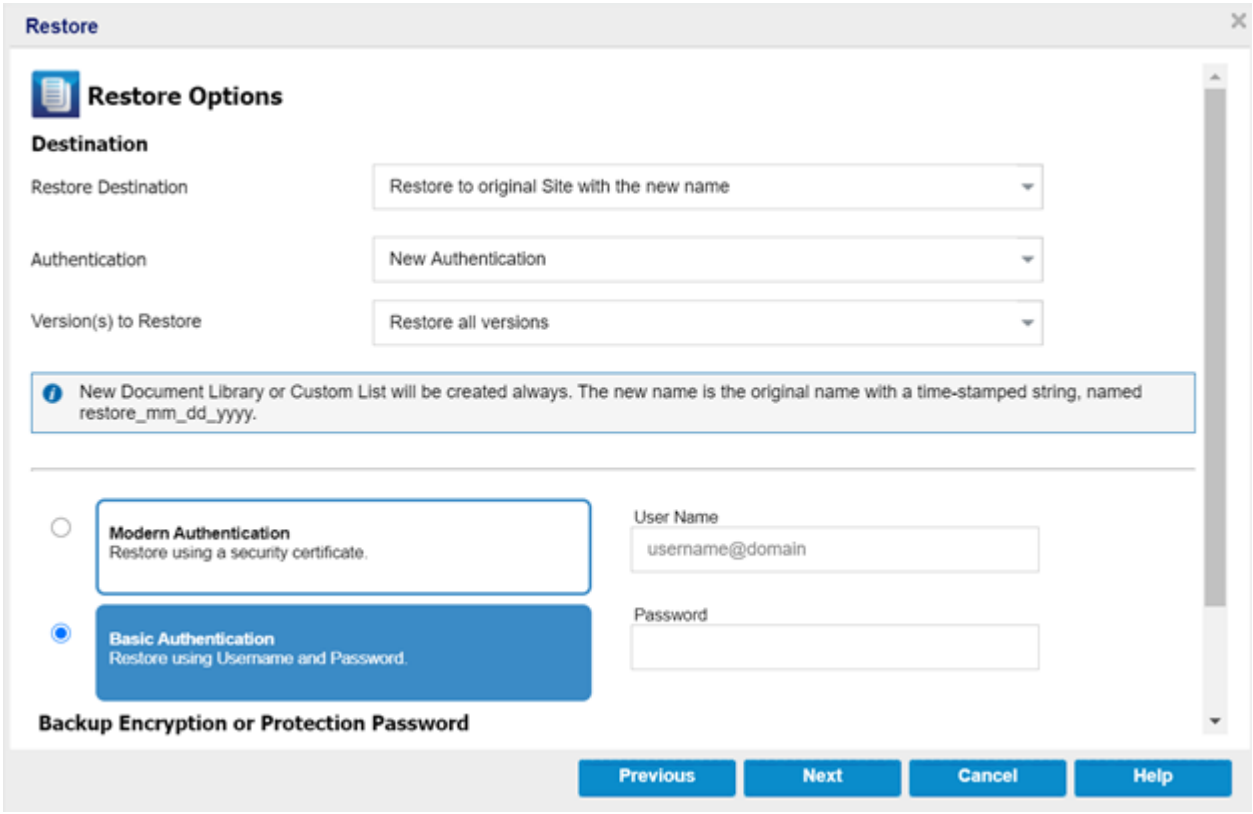


3. To apply authentication, do one of the following:
   - Modern Authentication

     For more information, see How to Use Security Certificates.
   - Basic Authentication

     For Basic Authentication, to proceed with the restore, enter UserName and Password.

     Note: This option fails if you have Modern Authentication enabled on the Tenant or Account.



Specify **Username** and **Password** of the site owner that performs backup.

4. Specify the list item Versions that you want to restore when your version setting is enabled from library setting in SharePoint Site.

   Restore all versions

   Restores all versions on backup.

   Restore only the latest version

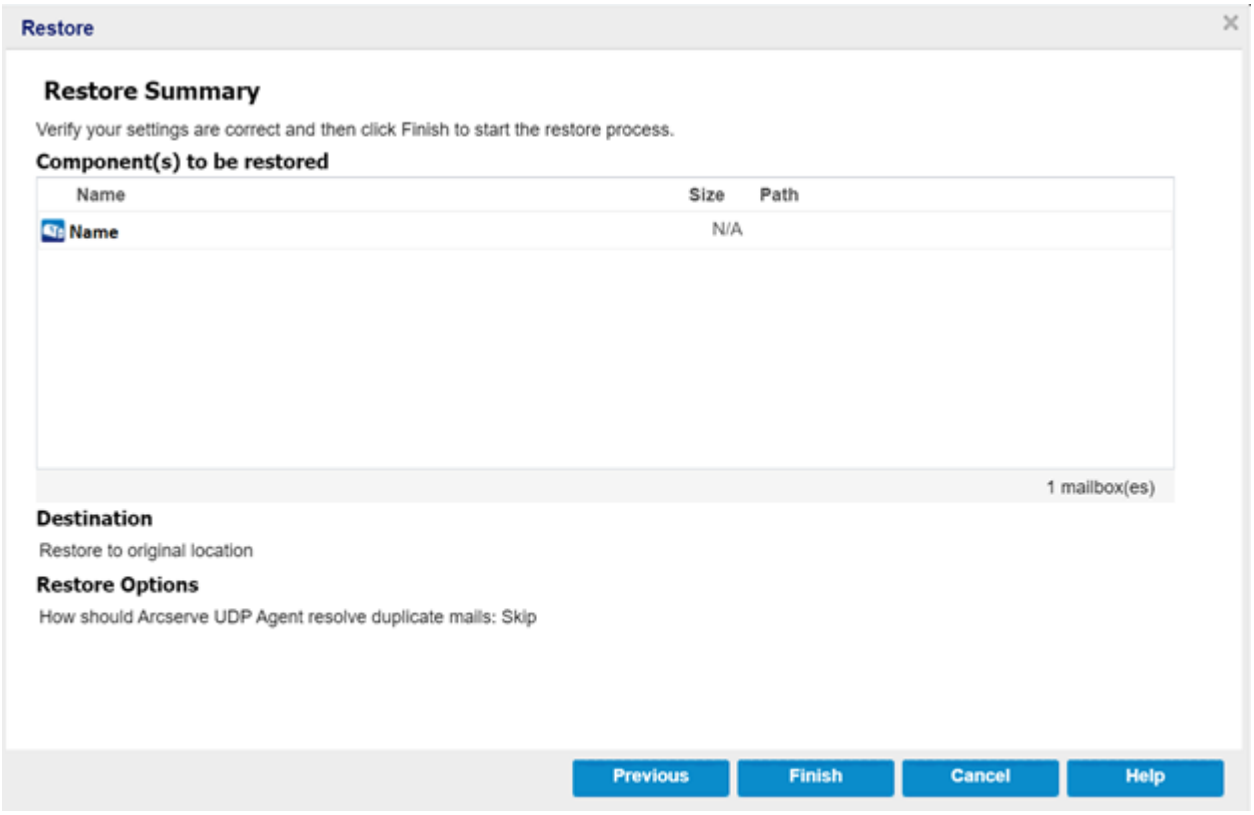
   Restores only the latest version on backup.

   Restore only the latest major version

   Restores only the latest major version on backup.

5. Specify the Session password if have.
6. Click **Next**.

   The **Restore Summary** dialog opens.



You can verify the restore information form Restore Summary dialog.

7. Click **Finish** to submit the restore job.

   The restore options are defined to restore the SharePoint Online information.

Verify that Content is Restored

After the completion of the restore process, verify that content was restored to the specified destination.

Follow these steps:

1. Log into the SharePoint site collection.
2. Verify the list/Library and list items.
3. Verify the restored content.

   The restored content is successfully verified.

How to Restore OneDrive Data

You can restore OneDrive data (files, folders, and so on) using any computer. You can restore using the restore option or also by using Mount Volume option from agent user interface.

Perform the following tasks to restore OneDrive data the restore option:

1. Select the OneDrive Items to Restore
2. Define the Restore Options
3. View Restore Summary
4. Verify that Content is Restored

Or else

Restore OneDrive data using the Mount Volume option.

Select OneDrive Items to Restore

You can restore OneDrive data from a recovery point. When you select a recovery date, and then specify the time, all the associated recovery points for that duration are displayed. You can then browse and select the backup content (including applications) to restore.

Follow these steps:

1. Log into Arcserve UDP.
2. Click the **resources** tab.
3. Select **All Nodes** in the left pane.

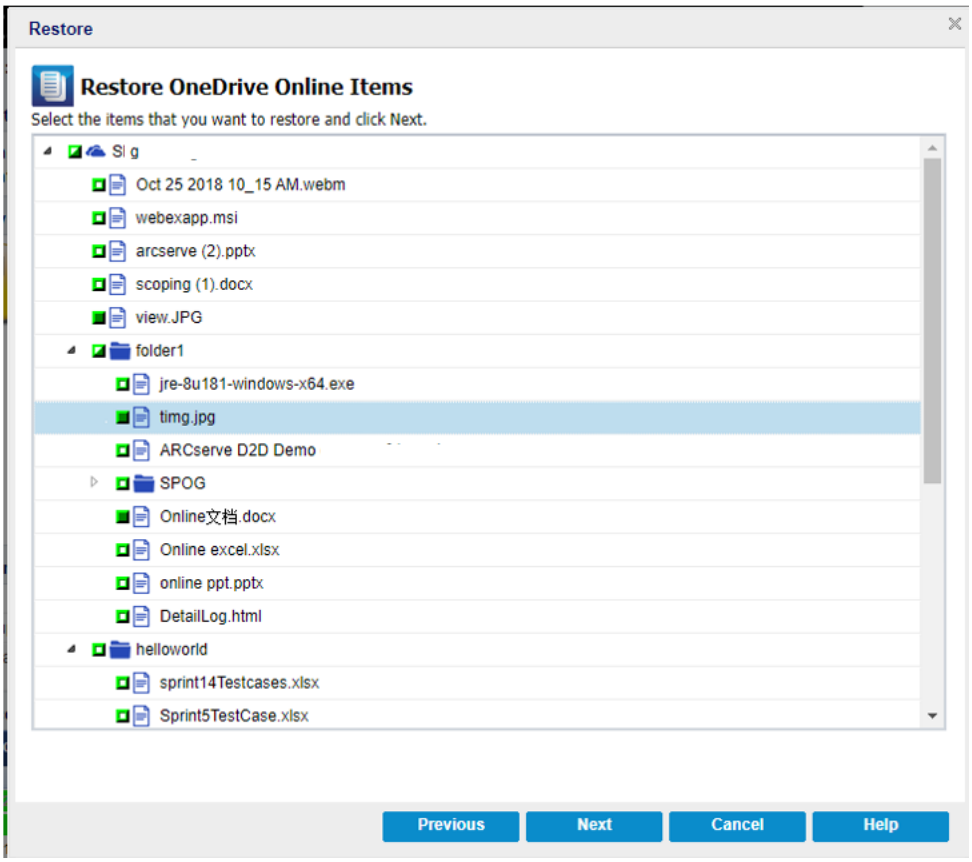
   All the added nodes are displayed in the center pane.
4. In the center pane, select the OneDrive node and click **Actions**.
5. Click **Restore** from the **Actions** drop-down menu.

   Note: You are automatically logged in to the agent node and the **Node** dialog opens.

   You can view the **Browse Recovery Points** details in the Backup Location. The name of selected *Recovery Point Server* is displayed. If desired, click **Change** and modify **Recovery Point Server setting** from the **Source** pop-up.
6. Select the calendar date for the backup image to restore and click **Next**.

   All the dates containing recovery points for the specified backup source are highlighted in green.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed (Full or Incremental), and the name of the backup.
7. From the **Restore OneDrive Node Items** pane, select the check boxes of related items or folders that you want to restore from Folders, and click **Next**.



Notes:

- You can select the entire content or partial content of the OneDrive object to restore. To select partial content, expand the object, and click the check box of that content.
- You can select multiple OneDrive objects to restore.

The **Restore Options** dialog opens.

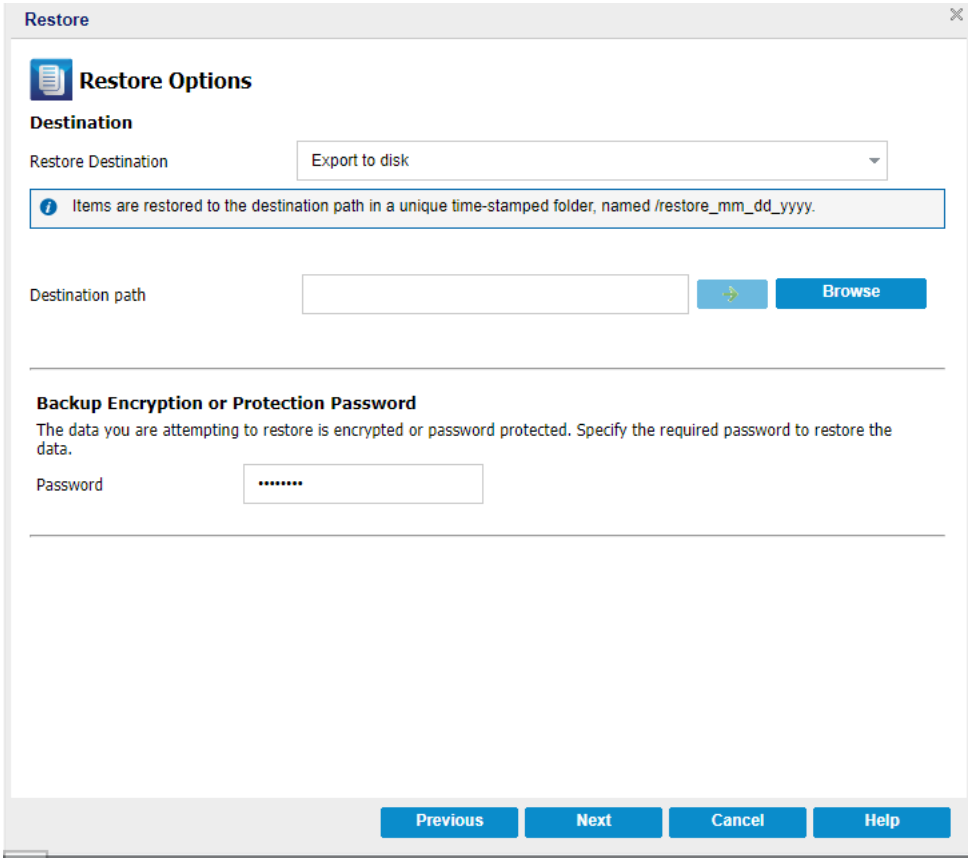
The OneDrive Node items to restore are selected. Now, you can define the restore options.

Define the Restore Options

After you specify the OneDrive information to restore, define the restore options for the selected content.

Follow these steps:

1. On the **Restore Options** dialog, select the restore destination.



Export to disk

Restores to folder or share folder in disk.

2. Specify a **Destination path** to define alternate restore locations.
3. (Optional) Specify **Backup Encryption Password or Protection password**.

   Note: This option is displayed only when the session password is already set while defining Destination in the Backup Plan.

4. Click **Next**.

   The **Restore Summary** dialog opens.

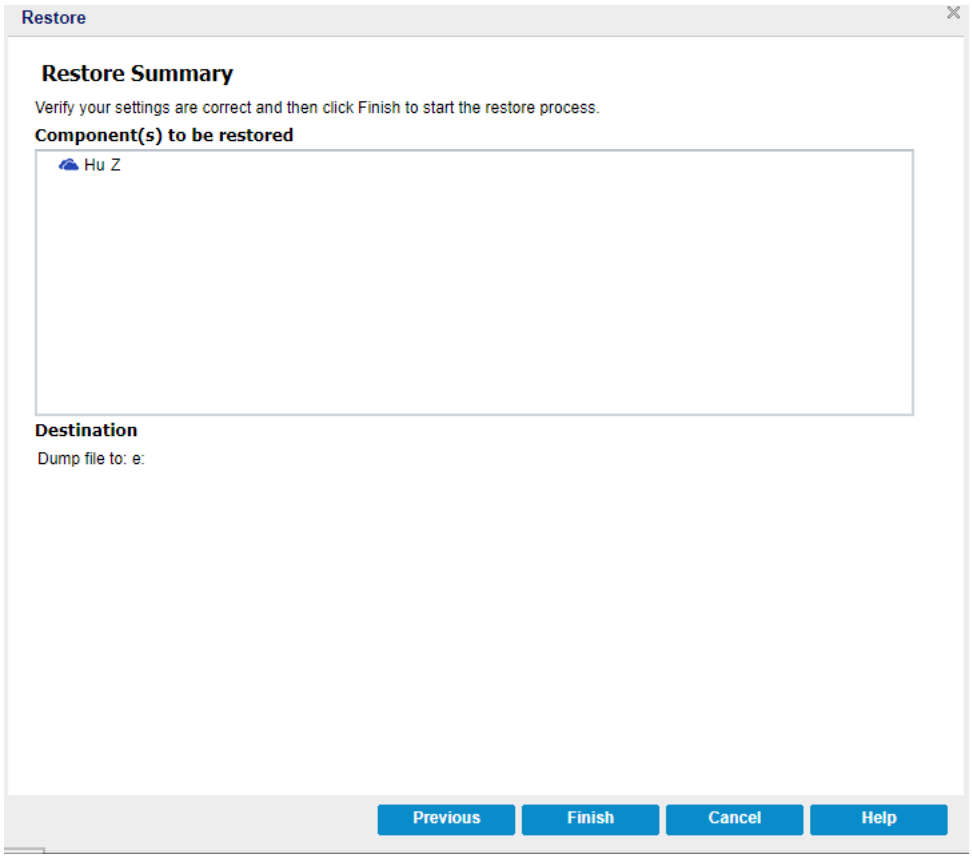
   The restore options are defined to restore the OneDrive information. Now, you can view restore summary.

View Restore Summary

After you define the restore options, verify that your settings are correct and confirm the restore process. **Restore Summary** helps you to review all the restore options and destination path that you defined. If you need to modify, click **Previous**.

Follow these steps:

1. On the **Restore Summary** dialog, review the displayed information to verify that all the restore options and settings are correct.

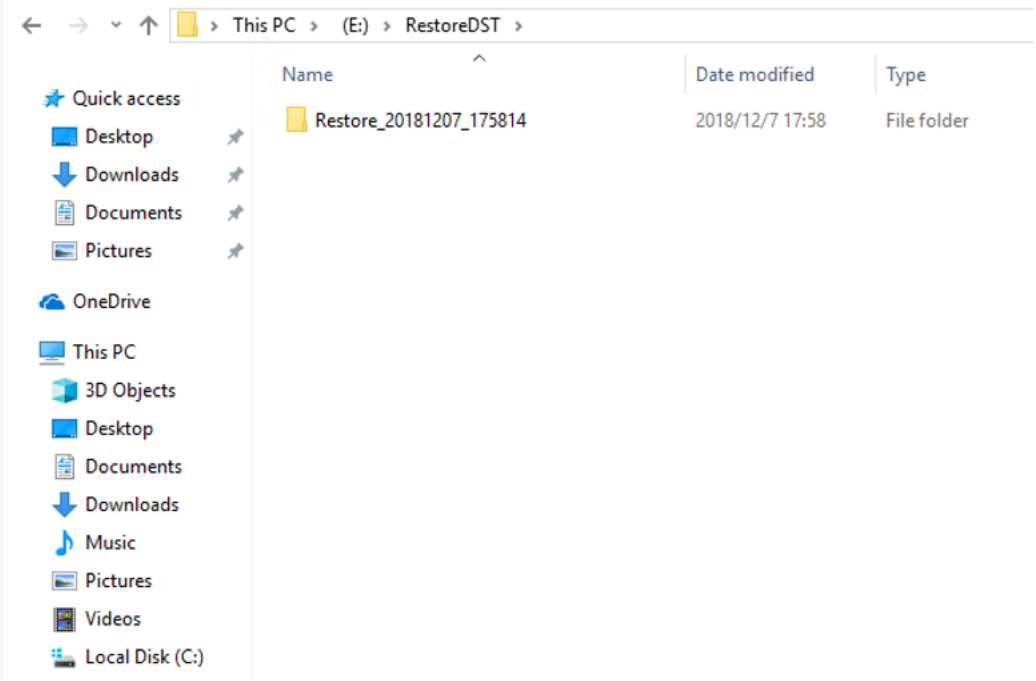


   - If the summary information is incorrect, click **Previous** and go back to the applicable dialog to modify the setting.
   - If the summary information is correct, click **Finish** to launch the restore job.

The recovery point content is stored.

Verify that Content is Restored

After completion of the restore job, the file/folder is saved in a temp folder with prefix Restore.



The restored file/folder maintains the same layout as available in OneDrive.

Restore OneDrive Data Using Mount Volume Option

OneDrive Protection uses the universal backup session format. You can mount the backup session as a drive letter and then copy the file/folder from the mounted volume.

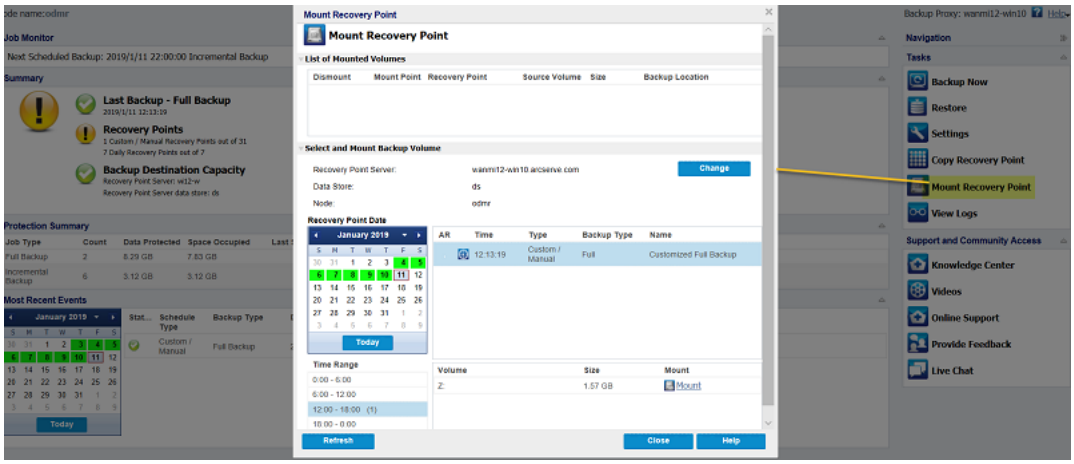
Follow these steps:

1. Log into Arcserve UDP.
2. Click the **resources** tab.
3. Select **All Nodes** in the left pane.

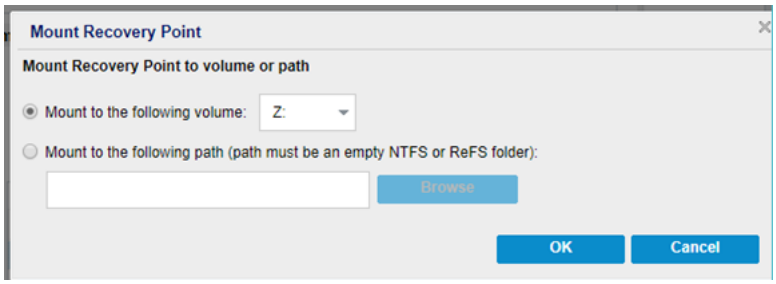
   All the added nodes are displayed in the center pane.
4. In the center pane, select the OneDrive node and click **Actions**.
5. Click **Log into Agent** from the **Actions** drop-down menu.

   Note: You are automatically logged in to the agent node. You can view complete details about the node and also on the right pane view the list of tasks that you can perform.
6. From the right pane under **Tasks**, click **Mount Recovery Point**.

   The **Mount Recovery Point** dialog opens. You can select the backup session in this dialog.



7. Select the destination and mount the session as a Drive Letter or Mount into an empty NTFS folder.



You can browse the volume. In the Volume, Arcserve UDP saved all the meta data of OneDrive. Each Account will have a related folder in the root volume. The folder is named according to the account name.

You can open the folder created by that account name and verify if the OneDrive data is backed up.

Recover Protected Microsoft Office 365 Data from Arcserve Cloud backup instance

This section contains the following topics:

How to Restore Microsoft SharePoint Online Site Collection Data

You can restore SharePoint Online List/Library or List item in Site. You can restore the data to original site using new name, restore the data to original location and export to disk from the recovery points.

For more information, see How to Restore SharePoint Online Site Collection Data.

How to Restore Microsoft Office 365 Exchange Mailbox Data

You can restore Exchange Online Mailbox data such as emails, calendars, contacts, notes, tasks, and so on from the Microsoft Cloud. You can restore the data to original or alternate location and export to disk from the recovery points.

For more information, see How to Restore Exchange Online Mailbox Data.

How to Restore Microsoft OneDrive Data

You can restore Microsoft OneDrive Data using the restore option or the Mount Volume option from the agent user interface. You can export Microsoft OneDrive files and folders to a local disk.

For more information, see How to Restore Microsoft OneDrive Data.