Provisioning for VMware Workspace ONE

VMware Workspace ONE UEM 2005

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 VMware Workspace ONE Provisioning Products for Windows 10 4

Factory Provisioning 4

Factory Provisioning Requirements 4

Install the Factory Provisioning Service 5

Create a Provisioning Package for Windows 10 Devices 6

Add an Encrypted PPKG During Out of Box Experience 9

Run an Encrypted PPKG on a Windows 10 Device 10

Managing Your Factory Provisioning Packages 10

Test a Factory Provisioning Configuration File 11

VMware Workspace ONE Provisioning Tool Considerations 12

Technical Preview: Workspace ONE Provisioning 15

Configure Workspace ONE Provisioning 15

Enable Offline Domain Join 16

VMware Workspace ONE Provisioning Products for Windows 10

1

Select from several Workspace ONE UEM Provisioning products for Windows 10 devices. Provisioning devices helps your end users by applying apps and configurations to devices so the user does not have to.

This chapter includes the following topics:

- Factory Provisioning
- Technical Preview: Workspace ONE Provisioning

Factory Provisioning

Workspace ONE UEM powered by AirWatch supports provisioning your Windows 10 devices with apps and configurations before they leave the factory. You do so by creating provisioning packages using Factory Provisioning.

Factory Provisioning requires on-premises customers to install the service onto an application server.

This service exports applications from the Workspace ONE UEM console and converts them into .PPKG files. You create this provisioning package in the Workspace ONE UEM console using a wizard. The wizard covers configuring the package, adding apps, and exporting the package.

Contact Your OEM for Availability

To use Factory Provisioning, contact your OEM (Original Equipment Manufacturer) Representative.

Provisioning Packages

You can also create encrypted PPKGs to provision devices yourself. This process does not use Factory Provisioning. You can provisioning devices either using the device OOBE or by running the PPKG on a device. For more information on provisioning devices yourself, see Create a Provisioning Package for Windows 10 Devices.

Factory Provisioning Requirements

Before creating provisioning packages, you must meet the Factory Provisioning requirements.

Factory Provisioning Requirements by Deployment Type

The following table shows the requirements for Factory Provisioning for each type of deployment. Consider these requirements before using Factory Provisioning.

Workspace ONE UEM Deployment	Software Distribution	File Storage	CDN
SaaS Shared	Enabled by Default	N/A	Enabled by Default
SaaS Dedicated version 9.7 and above	Enabled by Default	N/A	Enabled by Default
On-premises version 9.7	Disabled by default, but required	Required	Disabled by default, optional
On-premises version 1810 and later	Enabled by default	Required	Disabled by default, optional

Note Any application uploaded before you enable Software Distribution must be uploaded again.

Install the Factory Provisioning Service

Before you can use Factory Provisioning , you must install the Factory Provisioning Service in your environment.

Prerequisites

This process installs the Factory Provisioning Service into your environment. Only On-Premises customers must install this service. Consider reviewing the VMware Workspace ONE UEM Recommended Architecture Guide before installing the service.

Ensure that the servers the Factory Provisioning Service are installed on can reach and connect to your REST API server. The URL for REST API is set under **Groups & Settings > All Settings > System > Advanced > Site URLs > REST API URL**.

Use TLS to ensure that the traffic between the Factory Provisioning Service server and the Workspace ONE UEM console is secured. To use TLS, you must install a certificate for the Factory Provisioning Service server and enable HTTPS.

Procedure

1. On the server you want to install the Factory Provisioning Service onto, downloade the Factory Provisioning Service.

   If you are using a version of the Workspace ONE UEM console before 1811, download the installer from https://resources.workspaceone.com/view/cqp8nwklnmwnddgpphjv. If you are using version 1811 or later, download the installer from https://resources.workspaceone.com/view/gn7wrl7bbbtwzttgsm3r/en.

2. Run the Factory Provisioning Service installer.
3. In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs**.
4. Ensure that the correct URL is entered: `https://[FPS URL]/FactoryProvision/Package`.

Results

The Factory Provisioning Service is now installed. You can validate the installation by checking the communication between the various components used.

Factory Provisioning Service and the following:

- REST API over HTTPS
- Device Services over HTTPS
- CDN (if configured)
- Network file share access

The Workspace ONE UEM console and the REST API server communicate with the Factory Provisioning Service server over HTTPS.

What to do next

Configure a provisioning package. For more information, see Create a Provisioning Package for Windows 10 Devices

Create a Provisioning Package for Windows 10 Devices

Create a provisioning package for Windows 10 devices to use with Factory Provisioning or as an encrypted PPKG to install on devices yourself. This package contains the configuration file and the applications for your Windows 10 devices.

Prerequisites

Meet the Factory Provisioning Requirements. See Factory Provisioning Requirements.

Procedure

1. Navigate to **Devices > Lifecycle > Staging > Windows** and select **New**
2. Enter the general settings including the **Provisioning Package Name**, **Description**, and the smart group the package is **Managed By**.
3. Select **Next**.
4. Select the Onboarding Method. To create a PPKG for Factory Provisioning, select **Factory Provisioning**. To create an encrypted PPKG for your own use, select **Encrypted PPKG**. Select **Next**.

5 Configure the **Configurations** settings. The settings that display depend on the **Active Directory Type** selected. Consider the following information when configuring the settings:

Settings	Description
Domain Username	Enter the username that has Domain Join privileges. This setting displays when you set the **Active Directory Type** to **On-Prem AD Join**. **Note** This information is saved in plain text in the XML file. Ensure that this file is always secured and not sent over insecure connections.
Domain Password	Enter the password for the Domain Join user. This setting displays when you set the **Active Directory type** to **On-Prem AD Join**. **Note** This information saved in plain text in the XML file. Ensure that this file is always secured and not sent over insecure connections.
AD Organization Unit (OU)	Enter the organization unit for the AD. The OU must follow the correct formatting: `OU=,OU=,DC=Company,DC=com` This setting displays when you set the **Active Directory Type** to **On-Prem AD Join**.
Workgroup	Enter the name of the workgroup you want the client to join. The workgroup name must be 15 characters or fewer. This setting displays when you set the **Active Directory Type** to **Workgroup**.
Product Key	Enter the Windows 10 product key. You must follow the correct format: `12345-54CDE-XYZ78-ONM98-456TY`
Make Administrator?	You must make the local user account an administrator to start Workspace ONE enrollment automatically. During OOBE, the device prompts the user to enter their enrollment credentials. This setting displays when you set the **Active Directory Type** to **Workgroup** or **Azure AD**.
Computer Name	The computer name is randomly generated by default so that every system coming from the factory is unique. To create a naming convention, use the **Registered Owner** and **Registered Organization** settings. The computer name takes the first 7 characters from **Registered Organization** or **Registered Owner** as the prefix and then randomizes the rest of the characters up to the 15 character maximum.
Remove Windows 10 Consumer Apps	Select **Yes** to prevent consumer apps from appearing in Windows 10. This setting is only supported for Windows 10 Enterprise or Education. You must enter a Windows 10 Enterprise or Education key.
Additional Synchronous Commands	Add commands that automatically run at the end of the Windows setup process but before any user logs in.
First Logon Commands	Add commands that automatically run the first time a user logs in. This setting requires the user have local admin privileges.

Settings	Description
Enrollment Server	Enter your Workspace ONE UEM enrollment server URL. Find the enrollment URL by navigating in the Workspace ONE UEM console to **Groups & Settings > All Settings > System > Advanced > Site URLS**. This setting displays when you set the **Active Directory Type** to **On-Prem AD Join** or **Workgroup**.
Staging Account	Enter the username for the staging account. Find this username by navigating in the Workspace ONE UEM console to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Staging & Provisioning**. This setting displays when you set the **Active Directory Type** to **On-Prem AD Join** or **Workgroup**.
Device Services URL	Enter your device services URL. Find the device services URL by navigating in the Workspace ONE UEM console to **Groups & Settings > All Settings > System > Advanced > Site URLS**. This setting only displays when you set the **Active Directory Type** to **Azure AD - No Premium**.

6 Select **Next**.

7 Select the apps to include in the provisioning package. The apps that display are those apps available to the smart group set during the General settings step.

This screen only displays Win32 apps recognized through Software Distribution.

User context apps behave differently than device context apps. A provisioning package installs any device context apps in the factory, but user context apps install when a user signs in for the first time. These apps install using Software Distribution.

8 If the app requires transforms and patches (MST and MSP files), select the **Arrow** icon › to add the necessary transforms and patches. You must add these transforms from the **Edit Application** modal before creating a provisioning package.

9 Select **Next**.

10 Review the summary and either export the provisioning package or save it as a template.

a To export the provisioning package, select **Save and Export**.

b To save the package as a template, select **Save**. Templates do not create a PPKG file but save the settings for later creation and exporting. A template displays in the Windows list view with the Draft status.

You can only have one provisioning package PPKG stored at a time.

Results

Workspace ONE UEM exports the package or saves the template.

- If you created a Factory Provisioning PPKG, send the package to your OEM to provision your Windows 10 devices.

- If you created an Encrypted PPKG, you must save the PPKG to the root of a USB drive and install the package on the Windows 10 device. For more information, see Add an Encrypted PPKG During Out of Box Experience or Run an Encrypted PPKG on a Windows 10 Device.

If you want to change any settings in a provisioning package after creating one, you must either edit the existing package or export a template. Repeat the creation process and send the package to your OEM again. Exporting a new PPKG template overwrites any PPKGs currently available for download.

Add an Encrypted PPKG During Out of Box Experience

After creating an encrypted PPKG, you can add the package to devices using the Windows 10 Out of Box Experience (OOBE). This method installs your configurations and applications during the initial device setup.

Prerequisites

- Create an encrypted PPKG in the Workspace ONE UEM console. For more information, see Create a Provisioning Package for Windows 10 Devices.
- You need a USB drive to transfer the PPKG to the Windows 10 device. The USB drive must be formatted NTFS or FAT32.

Procedure

1. Navigate to **Devices > Lifecycle > Staging > Windows**.
2. Find the encrypted package and select **Download Encrypted PPKG**.
3. Save the PPKG to the root of a USB drive.

   If you save the PPKG to a subfolder, OOBE cannot detect the file.
4. On the Windows 10 device you want to provision, insert the USB drive at the **Select your Region** screen of the Out of Box Experience.

   If you save multiple PPKGs on the USB device, Windows prompts you to select the PPKG you want to apply. After selecting the PPKG, Windows automatically detects and begins processing the PPKG.
5. When prompted, enter the password used to encrypt the PPKG.
6. If you want to see the progress of the app installation, press **Shift + F10** to run a cmd window, press **Alt + Tab** and select the Provisioning Tool.

Results

The OOBE process runs the PPKG and installs the configuration and applications included in the package. The workflow changes based on the content of your PPKG:

- If you do not include configurations in your PPKG, the process completes and returns you to the **Select your Region** to complete the OOBE process.

- If you include configurations in your PPKG, Windows automatically runs Sysprep and reboots the device. After rebooting the device, Windows completes the device setup based on your configuration. After setup completes, Workspace ONE Intelligent Hub runs and completes device enrollment.

Run an Encrypted PPKG on a Windows 10 Device

After creating an encrypted PPKG, you can run the package on any Windows 10 device you want to configure. This method installs your configurations and applications on any Windows 10 device, even those already configured.

Prerequisites

- Create an encrypted PPKG in the Workspace ONE UEM console. For more information, see Create a Provisioning Package for Windows 10 Devices.
- You need a USB drive to transfer the PPKG to the Windows 10 device. The USB drive must be formatted NTFS or FAT32.
- Your devices must run Windows 10 1709 or later. They must also be unmanaged devices. If the device is already enrolled, the process does not apply any configurations or install any apps.

Procedure

1. Navigate to **Devices > Lifecycle > Staging > Windows**.
2. Find the encrypted package and select **Download Encrypted PPKG**.
3. Save the PPKG to a USB drive.
4. On the Windows 10 device you want to provision, insert the USB drive, open it, and double-click to run the PPKG.
5. Enter the password you used to encrypt the PPKG.
6. Confirm that you trust the source by selecting **Yes, Add It**.

Results

The Provisioning Tool runs and begins installing the configuration and applications included in the package. If you included configurations in your PPKG, Sysprep runs and automatically reboots the device. After rebooting the device, Windows completes the device setup based on your configuration. After setup, Workspace ONE Intelligent Hub runs and completes device enrollment.

Managing Your Factory Provisioning Packages

After creating provisioning packages, you can manage your templates and package from the Windows list view. This page allows you to create, edit, and delete your existing packages.

Creating a Provisioning Package

Create a provisioning package to configure your Dell devices. To create a package, select **New**. For more information, see Create a Provisioning Package for Windows 10 Devices.

Provisioning Package Templates

After creating a provisioning package, you can choose to either export the package or save it as a template. The templates are the saved settings for provisioning packages. When you save a template, the settings you configured are saved, but templates do not generate PPKG files until you export the package. Use templates to save and edit packages without exporting them.

Workspace ONE UEM purges PPKG files from storage based on the Purge job in the scheduler. Once the Purge job initiates, PPKG files are deleted, but the template is saved and you can export the package again.

In the Windows list view, templates show a Draft status. Active exports show the status of the export (Queued, In Progress, and so on).

Editing a Provisioning Package

You can edit existing provisioning packages. Select a package to edit and then select **Edit**. From the editing page, you can edit any of the provisioning package settings. You can also export a saved template by selecting **Save and Export**.

Deleting a Provisioning Package

You can delete provisioning packages and templates as needed. To delete, select the package or template, and select **Delete**. When you delete a package, you also delete any stored PPKG files.

Test a Factory Provisioning Configuration File

After creating a configuration file for Factory Provisioning, test the file to ensure your devices are correctly configured. Testing configuration files requires a test device or virtual machine.

Prerequisites

You need the following:

- You must have a test device or virtual machine. To test the file, you must run the System Provisioning Tool in audit mode.
- You must have one of the following items to test:
  - A PPKG containing the apps you want to install onto the device.
  - A Factory Provisioning configuration file.

Procedure

1. Download the VMware Workspace ONE Provisioning Toolto the test device.
2. Start the VMware Workspace ONE Provisioning Tool.

3 In the tool, select a PPKG or a Configuration to test.

4 Select the test method you want to use. Select **Apply Apps Only** to only apply the apps in the PPKG to the device. Select **Apply Full Process** to apply the apps and the settings in the configuration file.

   a If you select a configuration file to test, you can select what happens after by setting **After Applying Sysprep**. You can choose to shutdown, restart, or quit after configuration. If you restart the machine, the OOBE runs. If you select quit, the VMware Workspace ONE Provisioning Tool closes after applying sysprep.

   Only device-context apps are applied during this test. As there is no user for the device, user-context apps do not apply. If an app requires a reboot to finish installation, the tool prompts you to schedule a reboot. During the reboot, the device is told to resume installation after reboot and the tool relaunches.

Results

The VMware Workspace ONE Provisioning Tool applies the PPKG and the configuration file based on the test method selected. On the right-side of the tool, you can see the status of each step. You can view the logs after running the tool. The logs are found in `C:\ProgramData\Airwatch\UnifiedAgent\Logs\PPKGFinalSummary.log`.

VMware Workspace ONE Provisioning Tool Considerations

The VMware Workspace ONE Provisioning Tool allows you to test your Factory Provisioning configuration files. The tool also allows you configure the tool settings and use command line actions to run tests.

Command Line Actions

You can choose to run your tests using command line actions.

Table 1-1. VMware Workspace ONE Provisioning Tool Command Line Actions

Command Line Action	Description
-a, --action	Required. Action to perform (AppsOnly, Full, or TrackOnly).
-p, --ppkg	Required. PPKG File path.
-u, --unattend	Unattend XML File path.
-s, --shutdown	Shuts down the computer after the Sysprep command finishes running.
-r, --reboot	Restarts the computer after Sysprep. You can use this option to audit the computer and to verify that the first-run experience operates correctly. The tool reboots by default if no option is specified.
-q, --quit	Closes the Sysprep tool without rebooting or shutting down the device after Sysprep finishes running the commands.

Table 1-1. VMware Workspace ONE Provisioning Tool Command Line Actions (continued)

Command Line Action	Description
-g, --gui	Run the application with GUI. The default is `false`.
-l, --autologin	Enable auto login after reboot. The default is `false`.
-n, --username	Username for auto login.
-w, --password	Password for auto login.
--help	Display the help screen.
--version	Display the version information.

After running the action, exit codes display. These codes report the outcome of the action. The exit codes are as follows:

- 0 - Success
- 1 - Failure
- 2 - Reboot Required
- 3 - Timeout

Some examples include:

- Display the help screen: `VMwareWS1ProvisioningTool –-help`
- Apply apps only (PPKG): `VMwareWS1ProvisioningTool –a appsonly –p "C:\MyProvisioningPackage.ppkg"`
- Apply full process (ppkg & XML) - shutting down the system at the end: `VMwareWS1ProvisioningTool –a full –p "C:\MyProvisioningPackage.ppkg" –u "C:\MyAnswer.xml" –s`
- Apply full process (ppkg & XML) - rebooting the system at the end: `VMwareWS1ProvisioningTool –a full –p "C:\MyProvisioningPackage.ppkg" –u "C:\MyAnswer.xml" –r`
- Track only the application queue with GUI: `VMwareWS1ProvisioningTool –a trackonly –-gui`
- Track the application queue with GUI with the auto login enabled: `VMwareWS1ProvisioningTool –a trackonly –-gui –-autologin –n myuser –w mypassword`

VMware Workspace ONE Provisioning Tool Configuration Options

You can change the configuration settings for the VMware Workspace ONE Provisioning Tool to meet your needs. To change the settings, you must edit the VMwareWS1ProvisioningTool.exe.config file.

The config file contains the settings that control how the VMware Workspace ONE Provisioning Tool runs. Here are some commonly used settings for consideration. More settings are found in the config file. Consider reviewing the following settings to best meet your needs.

Table 1-2. VMware Workspace ONE Provisioning Tool Configuration Settings

Setting	Description
`loggingConfiguration`	Enter the file path, logging level, file size, and maximum number of archived files. The `level=` value controls the log level. The default value is `"Information"`. For troubleshooting, consider changing the level to `"Verbose"`.
`"TimeoutMinutes"`	Enter a value, in minutes, for how long the tool should attempt to apply the PPKG before timing out. Consider keeping this value below 90 minutes.
`"RefreshRateSeconds"`	Enter a value, in seconds, for how frequently the tool refreshes the installation progress of the PPKG.
`"BitLockerDecryptionTimeoutMinutes"`	Enter a value, in minutes, for how long the tool should wait for BitLocker Decryption to finish before timing out.
`"UnattendXmlCleanup"`	Set to True to remove the source Unattended XML file from the system drive after staging the device. If the Unattended XML is not present on the device, the file is only copied.
`"PpkgCleanup"` added in v2.2	Set to true to delete all PPKG files in the specified cleanup file path.
`"PpkgCleanupPath"` added in v2.2	Enter the file path to clean up any PPKG after staging. Any file with the PPKG extension is deleted.

Reading the PPKG Final Summary Log

After the VMware Workspace ONE Provisioning Tool finishes applying the PPKG to the device, a summary log generates. You can find the logs in `C:\ProgramData\Airwatch\UnifiedAgent\Logs\PPKGFinalSummary.log`. These logs are useful for troubleshooting. Dell may ask for these logs if there are issues provisioning devices.

The logs cover important information such as the OS details, client network details, device model and manufacturer, and PPKG details. If you do not set the device into audit mode, a note will be made in the log to help troubleshoot why the process failed. You can also see a log of the status updates that displayed in the tool during processing.

Technical Preview: Workspace ONE Provisioning

Workspace ONE Provisioning simplifies the provisioning process. With Workspace ONE Provisioning, you can dynamically apply assigned applications to devices before they leave the factory.

Note Workspace ONE UEM offers Workspace ONE Provisioning as a technical preview for our SaaS customers. Technical preview features are not fully tested and some functionality may not work as expected. However, these previews help Workspace ONE UEM improve current functionality and develop future enhancements.

To use a technical preview feature, contact your VMware Workspace ONE representative and ask to have several feature flags enabled at the listed OG levels.

- WindowsConnectedProvisioningFeatureFlag at the applicable OG level
- WindowsOEMProvisioningServiceFeatureFlag at the Global OG level
- WindowsDomainJoinScheduledJobFeatureFlag at the Global OG level

Workspace ONE Provisioning is an alternate method to provision devices before they ship to your workplace. This method provides a more flexible and powerful way to provision your devices. With Workspace ONE Provisioning, you do not need to create and export provisioning packages or share XML files with the hardware manufacturer. To use Workspace ONE Provisioning, you must configure autodiscovery for your OG and enable Workspace ONE Provisioning.

Workspace ONE Provisioning currently only supports assigning apps to your Windows 10 devices. To assign apps to the device, you must assign the apps to the staging user created when enabling Workspace ONE Provisioning. To see the staging user information, navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Staging & Provisioning**.

Configure Workspace ONE Provisioning

Configure Workspace ONE Provisioning to provision your Dell Windows 10 devices before they leave the factory. Workspace ONE Provisioning simplifies the provisioning process compared to Factory Provisioning.

Prerequisites

You must meet the following requirements before you can use Workspace ONE Provisioning:

- Workspace ONE UEM 1912 or later
- App Deployment Agent v3.8 or later
- Workspace ONE Provisioning Agent v3.0 or later
- Configure Software Distribution for the Organization Group
- Configure autodiscovery for the Organization Group

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Staging & Provisioning**
2. In the **Dell Connected Provisioning** section, select **Enable**.
3. If you want to use Offline Domain Join to add devices to your domain after a user signs in for the first time, enable **Offline Domain Join**.
   a. Enter the **Computer Name**.

      You can use variables to create the computer names. `%SERIAL%` creates a name using the device serial number. `%RAND:[#]%` creates a name using random characters based on the number entered.

   b. Enter the **Organization Unit Distinguished Name**.
4. Select **Save**.

What to do next

If you do not want to use Offline Domain Join, you must create an Administrator account on the device after receiving it from Dell. To create the administrator account, create a Custom Settings profile using the Accounts CSP. For easy access to the SyncML for this profile, see VMware Policy Builder.

Enable Offline Domain Join

Run the AirWatch Cloud Connector under a user who has Windows Server delegate permissions. This configuration sets the AirWatch Cloud Connector to add devices to domains in Active Directory for Workspace ONE Provisioning for Windows 10 devices.

You need the MMC snap-in called Active Directory Users and Computers (ADUC) to configure offline domain join. This snap-in is part of Remote Server Administration Tools (RSAT). See Microsoft | Docs for the latest documentation on Windows Server.

You must use AirWatch Cloud Connector to configure offline domain join. If you do not use this product, then create an admin account on the device to use Workspace ONE Provisioning.

Procedure

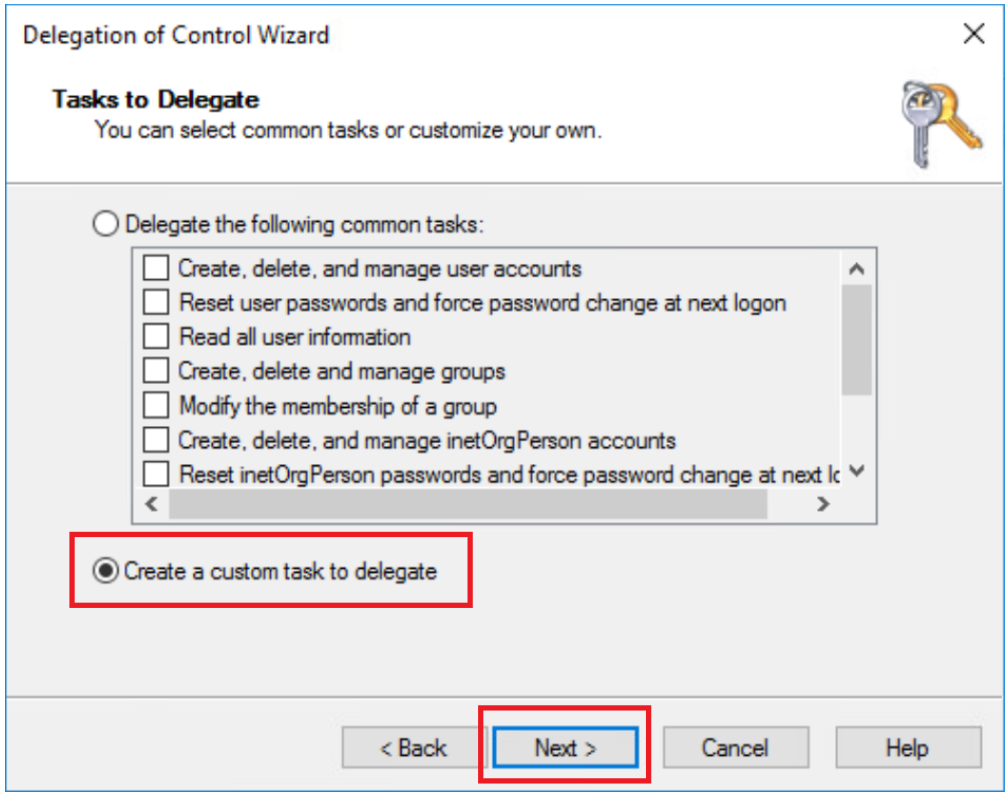
1. In ADUC, select the user with Windows Server delegate permissions, create a custom delegate task, and configure permissions.
   a. Right-click the container or folder where you want to add devices and select **Delegate Control**.

      This selection displays the **Delegation fo Control Wizard**.

   b. Select **Next** in the **Delegation fo Control Wizard**.

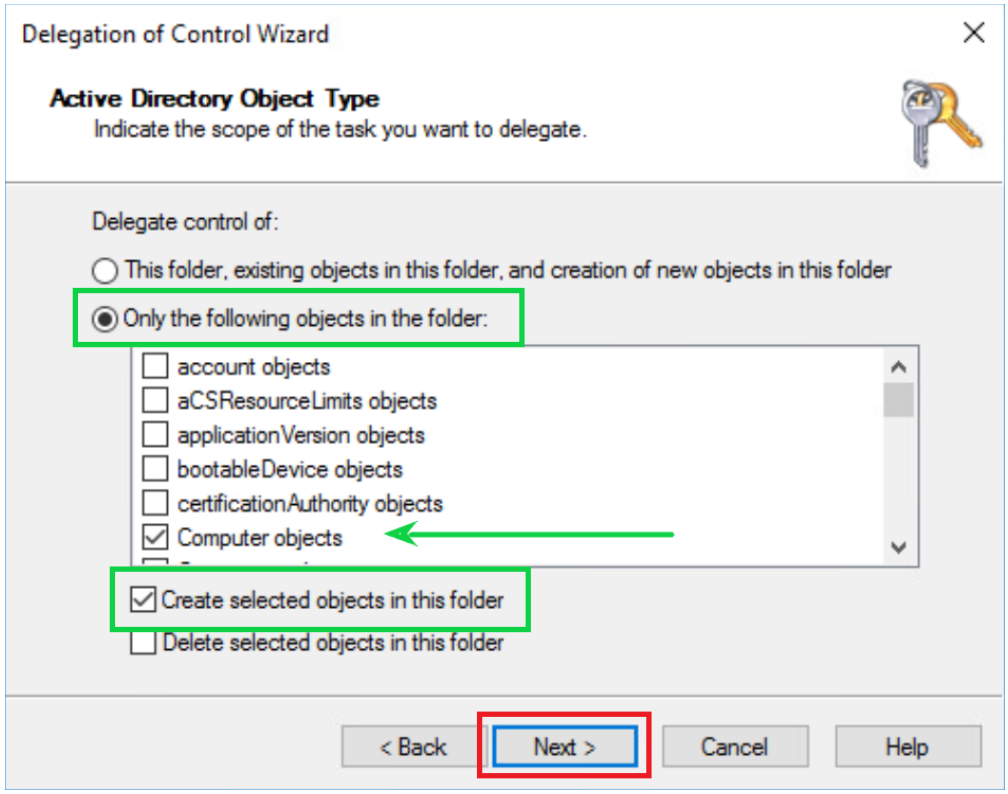
   c. On the **Users or Groups** window, select the user with Windows Server delegate permissions from the list, select **Add**, and then select **Next**.

d On the **Tasks to Delegate** window, select **Create a custom task to delegate** and then select **Next**.



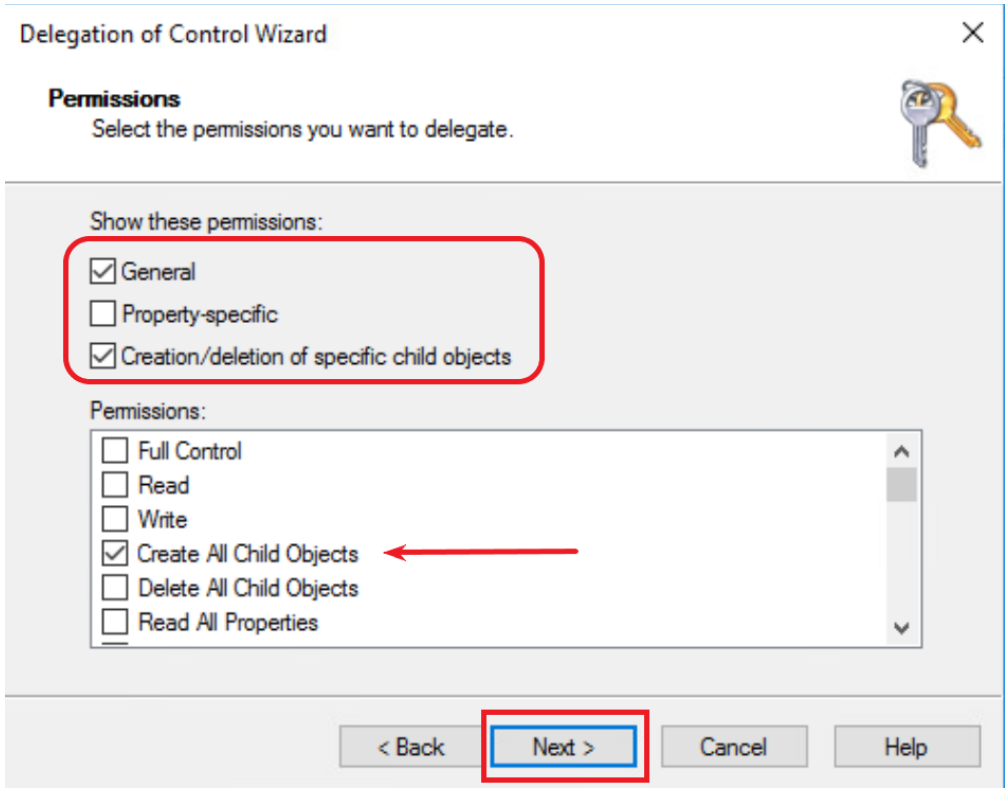
e On the **Active Directory Object Type** window, select the listed settings, and then select **Next**.

- **Only the following objects in the folder:**
- **Computer Objects**
- **Create selected objects in this folder**



f On the **Permissions** window, select the listed settings, and then select **Next**.

- **General**
- **Creation/deletion of specific child objects**
- **Create All Child Objects**



g Select **Finish**.

2 In AirWatch Cloud Connector, update the login and add write permissions.

a Change the **Log On As** for the AirWatch Cloud Connector to the user configured with Windows Server delegate permissions.

b In the AirWatch Cloud Connector **Advanced Security Settings** area, give the user `WRITE` permissions for the AirWatch Cloud Connector folder at `<Drive>:\VMware\AirWatch\CloudConnector`.