

VMware AirWatch Product Provisioning for Windows Desktop Guide

Using Product Provisioning for managing Windows Desktop devices.

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

| | |
|--|-----------|
| Chapter 1: Introduction to Product Provisioning for Windows Desktop | 4 |
| Supported Devices, OS, and Agents | 4 |
| Chapter 2: Relay Servers | 5 |
| Relay Server Basics | 5 |
| Configure a Relay Server | 5 |
| Pull Relay Server Configuration | 6 |
| Bulk Importing | 6 |
| Remote Viewing of Files on a Relay Server | 6 |
| Relay Server Management | 6 |
| Configure a Relay Server | 6 |
| Batch Import Relay Servers | 9 |
| Pull Service Based Relay Server Configuration | 10 |
| Remote Viewing Files on Relay Server | 12 |
| Relay Server Management | 13 |
| Chapter 3: Product Provisioning | 15 |
| Product Provisioning Basics | 15 |
| Files/Actions | 15 |
| Product Conditions | 15 |
| Create a Product | 15 |
| Files/Actions for Products | 16 |
| Product Conditions | 18 |
| Custom Attributes | 22 |
| Create a Product | 27 |
| Product Verification | 30 |
| Chapter 4: Products Dashboard | 31 |
| Recent Product Status | 31 |
| Product Compliance | 32 |
| Top Job Compliance | 32 |
| Product Breakdown | 32 |

| | |
|---|-----------|
| Products List View | 33 |
| Products in the Device Details View | 34 |
| Product Job Statuses | 34 |
| Advanced Remote Management | 36 |
| Chapter 5: Device Dashboard | 37 |
| Device List View | 37 |
| Windows Desktop Device Details Page | 38 |
| Chapter 6: Create an XML Provisioning File | 40 |
| Chapter 7: Appendix: Batch File Guidelines | 42 |
| Accounting for Path | 42 |
| Writing Scripts for Registry | 42 |
| General Instructions | 43 |

Chapter 1:

Introduction to Product Provisioning for Windows Desktop

Product provisioning enables you to create, through Workspace ONE™ UEM, products containing profiles, applications, files/actions, and event actions (depending on the platform you use). These products follow a set of rules, schedules, and dependencies as guidelines for ensuring your devices remain up-to-date with the content they need.

Product provisioning also encompasses the use of relay servers. These servers are FTP(S) servers designed to work as a go-between for devices and the UEM console. Create these servers for each store or warehouse to store product content for distribution to your devices.

As this guide focuses on the functionality provided by product provisioning, it does not contain all the features and functionality that Workspace ONE™ UEM offers for managing Windows Desktop devices. For more information on general MDM functionality for Windows Desktop devices, see the **VMware AirWatch Windows Desktop Platform Guide** available on docs.vmware.com

Supported Devices, OS, and Agents

The product provisioning functionality supports different devices and operating systems. The functionality available changes based on the supported rugged device.

Workspace ONE™ UEM supports product provisioning for devices with the following operating systems.

- Windows 8.1 and Windows 10 devices with AirWatch Protection Agent installed.

Chapter 2:

Relay Servers

Relay servers act as a content distribution node that provides help in bandwidth and data use control. Relay servers act as a proxy between the Workspace ONE™ UEM server and the rugged device for product provisioning.

Relay Server Basics

The relay server acts as an FTP/Explicit FTPS/SFTP server that distributes products to the device for download and installation. You can distribute to all devices without consuming all the bandwidth to the main/central MDM server.

Push Relay Servers – This method is typically used in on-premises deployments. The UEM console pushes content and applications contained in the product or staging to the relay server.

Pull Relay Servers – This method is typically used in SaaS deployments. A web-based application stored in the relay server pulls content and applications contained in the product or staging from the UEM console through an outbound connection.

Relay servers are optional, but recommended, for pushing products to downloaded apps and content – as opposed to downloading directly from the server that hosts the Workspace ONE UEM console.

Relay servers also add redundancy through the fallback feature. If a device's relay server is down, the device falls back to the next relay server in the hierarchy system until it finds a working server or connects to the Workspace ONE UEM console server.

If you are not using a relay server, the device downloads apps and content directly from the UEM console server.

Source Server Versus Relay Server

A source server is the original location of the data, usually a database, or content repository. After the data is downloaded from the source server to the UEM console, it is then transferred to the relay server. The data is then downloaded from the relay server to devices.

Configure a Relay Server

Configure an FTP, Explicit FTPS, or SFTP file server to integrate with Workspace ONE UEM as a relay server. For more information, see [Configure a Relay Server on page 6](#).

Pull Relay Server Configuration

Relay servers either push or pull content based on the configuration. A pull relay server pulls content from Workspace ONE UEM based on certain variables established in the server configuration. A push server pushes content from Workspace ONE UEM to devices whenever it is published. For more information on installing a pull server, see [Pull Service Based Relay Server Configuration on page 10](#).

Bulk Importing

The Relay Server Import feature loads relay servers into the system in bulk. This feature simplifies the configuration of multiple relay servers. For more information, see [Batch Import Relay Servers on page 9](#).

Remote Viewing of Files on a Relay Server

After configuring a relay server and assigning products to use the relay server, you can view the files hosted on the server. For more information, see [Remote Viewing Files on Relay Server on page 12](#).

Relay Server Management

Maintaining Relay Servers keeps your products running smoothly so your devices remain up-to-date. Workspace ONE UEM offers several tools to ensure that your relay servers work as intended. For more information, see [Relay Server Management on page 13](#).

Configure a Relay Server

Configure a relay server by configuring an FTP, Explicit FTPS, or SFTP file server and integrating it with Workspace ONE UEM. Workspace ONE UEM console is not compatible with Implicit FTPS Push Relay Servers.

Important: If you use the pull service to create a pull-based relay server, you must give SYSTEM full access to the home directory. This configuration means the pull service stores and removes files from the directory.

Pull Relay Server Security

Client-server applications such as Workspace ONE UEM use the transport layer security (TLS) cryptographic protocol to communicate across a network. TLS is supported by the file transfer protocol (FTP), file transfer protocol over SSL (FTPS), and SSH file transfer protocol (SFTP).

These file transfer protocols only secure those parts of the process where data is in transit between the client and the server. Because of this limitation, VMware recommends the use of OS-level disk encryption. There are several operating system-specific tools available (for example BitLocker for Windows, GnuPG for Linux).

Requirements

- An FTP, Explicit FTPS, or SFTP server.
 - Pull service bandwidth needs and minimum hardware requirements are negligible when compared to pushing products to devices. Such needs are entirely dependent upon 1) the number of products you are pushing, 2) how often they are pushed, and 3) the size of the products in MBs.
 - When assessing hardware and bandwidth needs for FTP servers, consider following general guidelines and adjust their specifications as your needs change.
 - General FTP Server Guidelines: 2 GHz x86 or x64 processor and 4 GB RAM.
- You must create an FTP user with a home directory. This user must have read/write/delete permissions for both the directory and the files used in the relay server. This FTP user must have a user name and password for authentication.
- Workspace ONE UEM supports SFTP servers, however, the supported staging clients, Stage Now (Android), and Rapid Deployment, do not support SFTP servers for use with barcode staging.

Procedure

1. Navigate to **Devices > Staging & Provisioning > Relay Servers > List View** and select **Add**, followed by **Add Relay Server**.
2. Complete all applicable settings in the tabs that are displayed.

| Setting | Description |
|--------------------------|---|
| General | |
| Name | Enter a name for the relay server. |
| Description | Enter a description for the relay server. |
| Relay Server Type | <p>Select either Push or Pull as the relay server method.</p> <p>Push – This method is typically used in on-premises deployments. The UEM console pushes content and applications contained in the product or staging to the relay server.</p> <p>Pull – This method is typically used in SaaS deployments. A web-based application stored in the relay server pulls content and applications contained in the product or staging from the UEM console through an outbound connection.</p> <p>For more information on installing a pull server, see Pull Service Based Relay Server Configuration on page 10.</p> |

| Setting | Description |
|---|---|
| Restrict Content Delivery Window | <p>Enable to limit content delivery to a specific time window. Provide a Start Time and End Time to restrict the delivery of content.</p> <p>The start time and end time of the restriction window is based on Coordinated Universal Time (UTC), which the system obtains by converting the console server time into Greenwich Mean Time (GMT).</p> <p>Please set the system time on the console server accurately to ensure your content is delivered on time.</p> |
| Assignment | |
| Managed By | Select the organization group that manages the relay server. |
| Staging Server | <p>Assign the organization groups that use the relay server as a staging server.</p> <p>A staging server only works for the staging process involving the supported staging clients, Stage Now (Android) and Rapid Deployment.</p> |
| Production Server | <p>Assign the organization groups that use the relay server as a production server.</p> <p>A production server works with any device with the proper agent installed on it.</p> |
| Device Connection | |
| Protocol | <p>This is the information the device uses to authenticate with the FTP(s) server when downloading apps and content.</p> <p>FTP, Explicit FTPS, or SFTP as the Protocol for the relay server.</p> <p>If using Explicit FTPS, your Explicit FTPS server must have a valid SSL certificate. Configure the SSL certificate on the Explicit FTPS server.</p> |
| Hostname | Enter the name of the server that hosts the device connection. |
| Port | <p>Select the port established for your server.</p> <div> <p>Important: The ports you configure when you create your FTP, Explicit FTPS, Implicit FTPS (Android only), or SFTP server must be the same ports you enter when creating a relay server in the Workspace ONE UEM console.</p> </div> |
| User | Enter the server username. |
| Password | Enter the server password. |
| Path | <p>Enter the path for the server.</p> <p>This path must match the home directory path of the ftp user. For example, if the ftp user's home directory is C:\ftp\home\jdoe, the path entered into this field must be C:\ftp\home\jdoe.</p> |
| Passive Mode | Enable to force the client to establish both the data and command channels. |

| Setting | Description |
|----------------------|--|
| Verify Server | <p>This setting is only visible when Protocol is set to FTPS.</p> <p>Enable to ensure the connection is trusted and there are no SSL errors.</p> <p>If left unchecked, then the certificate used to encrypt the data can be untrusted and data can still be sent.</p> |

- For a push server, select the **Console Connection** tab and complete the settings. This is the information that the UEM console uses to authenticate with the FTP(S) server when pushing apps and content. The settings are typically identical to the **Device Connection** tab.

Press the **Test Connection** button to test your Console Connection to the push server. Each step of the connection is tested and the results are displayed to help with troubleshooting connection issues.

Press the **Export** button on the Test Connection page to export the data from the test as a CSV file.

- For a pull server, select the **Pull Connection** tab and complete the settings.

| Settings | Descriptions |
|-----------------------------|---|
| Pull Local Directory | Enter the local directory path for the server. |
| Pull Discovery Text | <p>Enter the IP addresses or the MAC addresses of the server. Separate each address with commas.</p> <p>IP addresses use periods as normal but MAC addresses do not use any punctuation in this form.</p> |
| Pull Frequency | Enter the frequency in minutes that the pull server should check with the UEM console for changes in the product. |

- Select **Save**.

Batch Import Relay Servers

The Relay Server Import feature loads relay servers into the system in bulk. Make sure to associate the relay server users with an organization group.

Save all files in CSV format before importing.

To bulk import relay servers, take the following steps.

- Navigate to **Devices > Staging & Provisioning > Relay Servers > List View** and select **Batch Import**.
- Enter a **Batch Name**.
- Enter a **Batch Description**.
- Select **Choose File** to upload the **Batch File**. Batch files must be in CSV format. Select the **Information** icon (i) to download a template.
- Select **Save** to upload the batch import.

Pull Service Based Relay Server Configuration

Pull service-based relay servers periodically contact the Workspace ONE™ UEM console to check for new products, profiles, files, actions, and applications assigned to devices under the pull relay servers purview. Configure a pull server to deliver content to devices without excessive bandwidth use.

If you make changes or additions, the server creates an outbound connection to the UEM console to download the new content to the server before pushing it to its devices. Pull service is best used when traversing any NAT firewall or SaaS to on-premises hybrid environments because SaaS customers typically do not want the service to tie-up bandwidth when content is delivered from Workspace ONE UEM to the store server.

Pull Relay Server Security

Client-server applications such as Workspace ONE UEM use the transport layer security (TLS) cryptographic protocol to communicate across a network. TLS is supported by the file transfer protocol (FTP), file transfer protocol over SSL (FTPS), and SSH file transfer protocol (SFTP).

These file transfer protocols only secure those parts of the process where data is in transit between the client and the server. Because of this limitation, VMware recommends the use of OS-level disk encryption. There are several operating system-specific tools available (for example BitLocker for Windows, GnuPG for Linux).

To create a pull relay server, you must first have an FTP, Explicit FTPS, or SFTP server to function as the relay server. FTP (S) servers must be compliant with RFC 959 and RFC 2228 set by the Internet Engineering Task Force.

Important: The ports you configure when you create your FTP, Explicit FTPS, Implicit FTPS (Android only), or SFTP server must be the same ports you enter when creating a relay server in the Workspace ONE UEM console.

The process covers the installation of one server at a time. For bulk installation, you must use a third-party application. Workspace ONE UEM supports importing servers in bulk through the Bulk Import option. See [Batch Import Relay Servers on page 9](#) for more information.

Create a Windows-Based Pull Service Relay Server

Configure a pull service relay server using a Windows FTP, Explicit FTPS, or SFTP server for use with product provisioning and staging. The pull service must be installed before you integrate the server with the Workspace ONE™ UEM console.

Prerequisites

- An FTP, Explicit FTPS, or SFTP server. Workspace ONE UEM does not support Implicit FTPS Windows-based relay servers.
- .NET must be installed on Windows-based servers.
- The relay server requires network access between the server (in-store, distribution center, and so on) and to the Workspace ONE UEM SaaS environment.
- Each server requires disk storage of 2 MB for the pull server installer and hard disk space for all the content pulled to the server.

Process

To create a windows-based pull relay server, take the following steps.

1. Configure an FTP, Explicit FTPS, or SFTP server. You must create an FTP user with read/write/delete permissions for both the directory and the files used in the relay server. This FTP user must have a user name and password for authentication. Note the home directory of the user for use in configuring the pull service.
2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Pull Service Installers**.
3. Download the Windows Pull Service Installer and the Configuration file onto the server using your preferred server management system.
4. Open the XML config file and update the IP Address with your console server FQDN, for example, cn274.awmdm.com.

```
<PullConfiguration>
<libraryPath>C:\AirWatch\PullService\</libraryPath>
<endPointAddress>https://[endpoint URL]/contentpull </endPointAddress>
</PullConfiguration>
```

5. Run the WindowsPullServiceInstaller.exe.
.NET is installed before the MSI is extracted.
6. Navigate to **Devices > Staging & Provisioning > Relay Servers > Undiscovered Pull Relay Servers**. If you have configured the FTP, Explicit FTPS, or SFTP server correctly, it provides feedback to this effect. If you do not see your server displayed, check your configuration settings.
7. Configure the relay server as a pull relay server in the UEM console. See [Configure a Relay Server on page 6](#) for more details.

If you are using the silent install from the command prompt, use the following commands:

- WindowsPullServiceInstaller.exe /s /v"/qn/"
- To include log: WindowsPullServiceInstaller.exe /s /v"/qn" /l WindowsPullServiceInstaller.txt"

The installer looks for the PullserviceInstaller.config file in the installer execution directory. If the file is missing, the installer prompts you to let you know the file is missing.

Create a Linux-Based Pull Service Relay Server

Configure a pull service relay server using a Linux FTP, Explicit FTPS, or SFTP server for use with product provisioning and staging. The pull service must be installed before you integrate the server with the Workspace ONE™ UEM console.

Prerequisites

- An FTP, Explicit FTPS, or SFTP server.
- Linux-based servers must run either CentOS or SLES 11 SP3.
- Java 8+ must be installed on Linux-based servers.
- The relay server requires network access between the server (in-store, distribution center, and so on) and to the Workspace ONE UEM SaaS environment.

- Each server requires disk storage of 2 MB for the pull server installer and hard disk space for all the content pulled to the server.

Process

To create a Linux-based pull relay server, take the following steps.

1. Configure an FTP, Explicit FTPS, or SFTP server. You must create an FTP user with read/write/delete permissions for both the directory and the files used in the relay server. This FTP user must have a user name and password for authentication. Note the home directory of the user for use in configuring the pull service.
2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Pull Service Installers**.
3. Download the Linux Pull Service Installer and the Configuration file onto the server using your preferred server management system.
4. Open the XML config file and update the IP Address with your console server FQDN, for example, cn274.awmdm.com.

```
<PullConfiguration>
<libraryPath>C:\AirWatch\PullService\</libraryPath>
<endPointAddress>https://[endpoint URL]/contentpull /</endPointAddress>
</PullConfiguration>
```

5. In the command prompt, enter the following.

```
sudo ./LinuxPullServerInstaller.bin
```

Alternatively, enter the following command to install silently.

```
sudo ./LinuxPullServerInstaller.bin -I silent
```

6. Follow the instructions prompted by the installer, including the optional configuration of a proxy server. If you want to use a proxy server, supply the host, port, and authentication information when prompted.
7. Navigate to **Devices > Staging & Provisioning > Relay Servers > Undiscovered Pull Relay Servers**. If you have configured the FTP, Explicit FTPS, or SFTP server correctly, it provides feedback to this effect. If you do not see your server displayed, check your configuration settings.
8. Configure the relay server as a pull relay server in the UEM console. See [Configure a Relay Server on page 6](#) for more details.

The installer looks for the PullserviceInstaller.config file in the installer execution directory. If the file is missing, the installer prompts you to let you know the file is missing.

Remote Viewing Files on Relay Server

View files sent to a relay server for distribution to devices through the Remote File Viewer.

To access the Remote File Viewer, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Relay Servers > List View**.
2. Select the server you are interested in viewing by clicking the radio button to the left of the Active indicator, above the Edit pencil icon.
3. Select the **More Actions** button.
4. Select **Remote File List** to open the Remote File List for your selected relay server.

FTPS

Folders:

- /ftp_awtestact

RelayServerPath not found: /ftp_awtestact





















| RSFileName not found | RSFileSize not found | RSDateModified not found |
|--|----------------------|--------------------------|
| /ftp_awtestact/20g_63525421737000... | 419 | 2/20/2014 11:02:00 AM |
| /ftp_awtestact/ADV_20g_635254217... | 429 | 2/20/2014 11:02:00 AM |
| /ftp_awtestact/ADV_JAKE14_635282... | 432 | 2/20/2014 11:02:00 AM |
| /ftp_awtestact/ADV_PearceStagingA... | 387 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/ADV_PearceStagingA... | 387 | 2/24/2014 3:32:00 PM |
| /ftp_awtestact/ADV_stageStatus_63... | 436 | 2/20/2014 11:02:00 AM |
| /ftp_awtestact/AirWatchCoreAgentW... | 398 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/AirWatchCoreAgentW... | 674 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/AirWatchCoreAgentW... | 679 | 2/24/2014 3:32:00 PM |
| /ftp_awtestact/airwatch_client_4_5_... | 1055 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/AnandStaging_63521... | 357 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/AndroidStaging_6352... | 429 | 2/20/2014 2:51:00 PM |
| /ftp_awtestact/Android_awatl_1_325... | 411 | 2/24/2014 3:32:00 PM |

Relay Server Management




Maintaining Relay Servers keeps your products running smoothly so your devices remain up-to-date.

Relay Server Status

After creating a relay server, refresh the relay server detail page to get the status of the connection.

| | | | | | | | |
|---|---|----------------------|------|----------------------------|--------------|---|---|
|  |  | Primary Relay Server | Pull | FTP://11.111.1.111/Example | Akron |  |  |
|  | | | | | | | |
|  |  | Warehouse 1 | Push | FTP://11.111.1.111/Example | rickdr4 |  |  |
|  | | | | | | | |
|  |  | Warehouse 2 | Push | FTP://11.111.1.111/Example | aaron |  |  |
|  | | | | | | | |
|  |  | Warehouse 3 | Push | FTP://11.111.1.111/Example | <u>aaron</u> |  |  |
|  | | | | | | | |


The **Source Server** and **Relay Server** statuses are as follows:

| Settings | Descriptions | |
|---|---------------------------------------|---------------------------------------|
| Indicator | Source Server | Relay Server |
|  | Last retrieval from server succeeded. | Last file sync with server succeeded. |
|  | Retrieval from server in progress. | File sync with server in progress |
|  | Last retrieval failed. | Last file sync failed. |

Once the check mark displays for both source server and relay server, the product components are available for distribution to the end-user device.

Advanced Info

You can access the **Advanced Info** action for more detailed information pertaining to the server. This action can be found in the **More Actions** options drop-down available after selecting a relay server.. The Advanced Info action displays the **Queued Count** of files, the **Last Error Code** displayed, and the **Last Error Description**.

| Relay Server Advanced Information | |  |
|-----------------------------------|---------|--|
| Content Delivery Info | | |
| Queued Count | 0 | |
| Last Error Code | 0 | |
| Last Error Description | Success | |

Chapter 3:

Product Provisioning

The main feature of the Product Provisioning system is creating an ordered installation of profiles, applications, and files/actions into one product to be pushed to devices based on the conditions you create.

Product Provisioning Basics

Once products are created and activated, they are pushed to the device based on the conditions set. Conditions are an optional tool that determines when a product is downloaded and when it is installed. Content provisioning by products can be pushed to devices through optional relay servers.

Products are pushed to devices that are chosen by smart group assignments. These groups control which devices get which product based on how the group is created. You can also use Assignment Rules to further target your products to devices.

Important: You must upload the content of the product before a product can be created.

Files/Actions

You can install, configure, and upgrade devices by assigning files/actions to a product. The files/actions component also contains ways to manage the file system of a device. For more information, see [Files/Actions for Products on page 16](#).

Product Conditions

A condition determines when the product or OS upgrade package should be downloaded and installed. Conditions are checked when a product is pushed to a device. For more information, see [Product Conditions on page 18](#).

Create a Product

After creating the content you want to push to devices, create a product that controls when the content is pushed and the order of installation of the product. For more information, see [Create a Product on page 27](#).

Files/Actions for Products

You can install, configure, and upgrade devices by assigning files/actions to a product. The files/actions component also contains ways to manage the file system of a device.

A file/action is the combination of the files you want on a device and the actions you want performed on the device with the file. You cannot assign files/actions directly to a device. Instead, you assign a file/action to a product. The product is then assigned to the device using Smart Group assignment.

View the files/actions in the Files/Actions List View.

Create a Files/Actions Component

Create Files/Actions to install and configure files and upgrades onto your devices using product provisioning.

Windows Unified Agent is a 32-bit application, so when trying to run scripts in a 64-bit machine, proper redirections must be used to get access to the 64-bit folder or the registry hive.

To add files and actions to a Files/Actions component, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions** and select **Add Files/Actions**.
2. Select the device Platform for which you want to make the files/actions.
3. Complete the **General** text boxes.

| Settings | Descriptions |
|--------------------|--|
| Name | Enter a name for the files/actions. The name cannot be longer than 255 characters. |
| Description | Enter a short description for the files/actions. |
| Version | The UEM console pre-populates this setting. |
| Platform | Read-only setting displays the selected platform. |
| Managed By | Select the organization group that can edit the files/actions. |

4. Select the **Files** tab.
5. Select **Add Files**. The **Add Files** window displays.
6. Select **Choose Files** to browse for a file or multiple files to upload.
7. Select **Save** to upload the files. Once the files upload, the file grouping screen opens. File groups allow you to assign different download paths and settings to different groups of files you have uploaded to a single file/action.
8. Select uploaded files and select **Add** to move the files into a new file group.
9. Define the **Download Path** the device uses to store the file group in a specific device folder. If the download path entered does not exist, the folder structure is created as part of installation.
10. Select **Save**. You can repeat the previous steps for as many files as you want.
11. Select the **Manifest** tab. Actions are not required if you have at least one file uploaded.
12. Add actions to the **Install Manifest** or the **Uninstall Manifest** if needed.

The uninstall manifest only runs when the Uninstall action is added to the product. Also, if nothing is added to the Uninstall Manifest, uninstalling the file/action results in no effect.

| Settings | Descriptions |
|----------------------|--|
| Copy Files | Copy files from one location to another on the device. |
| Create Folder | Create a new folder on the device. |
| Delete Files | Delete folders from the device. |
| Install | <p>Install files on the device. You must use the Run manifest action to install files or applications. This is accomplished using command lines. Supports the following file types.</p> <ul style="list-style-type: none"> Windows Desktop: REG, CAB, MSI, and XML. <p>REG files require batch files and PowerShell commands.</p> |
| Move Files | Move files from one location to another on the device. |
| Remove Folder | Remove a folder from the device. |
| Rename File | Rename a file on the device. |
| Rename Folder | Rename a folder located in the device. |
| Run | <p>Use the manifest to run an application. This is accomplished using command lines. The Run command must use the syntax of "[full file path]". For example, \program files\program.exe.</p> <p>You must select the context of the command. Select whether the command runs at the system level, the user level, or the admin account level.</p> |
| Terminate | End a process or application running on the device. |
| Uninstall | <p>Uninstall a program or application on the device. You must enter the application name.</p> <p>The application name must match the name that appears in the Uninstall menu in the Control Panel.</p> <div> <p>Note: The Uninstall Manifest is for deleting files when a product is removed. If you remove a product from a device, any files installed remain on the device until uninstalled using an Uninstall Manifest.</p> </div> |

13. When finished adding actions to the **Manifest**, select **Save**.

Manage Files/Actions

Manage your created files/actions to keep products and devices up-to-date.

Edit Files/Actions

When you edit any existing files/actions, the version number increases. After saving the edits, Workspace ONE™ UEM runs a check against all active products to find any that contain the newly edited files/actions.

If any active products contain the files/actions, a warning prompt displays listing all active products affected by the edited files/actions. You can then choose to **Activate** or **Deactivate** a product using the files/actions.

Delete Files/Actions

Workspace ONE UEM checks any attempt to delete files/actions against the list of active products.

To delete files/actions, it must be detached from all products.

1. Select the **Files/Actions** listed in the Warning prompt.
2. Select **Edit**.
3. Remove the files/actions from the product.
4. Select **Save**.
5. Repeat for all products containing the files/actions.
6. Once the files/actions detaches from all products, you can delete the files/actions.

If the files/actions is part of an active product, a warning prompt displays listing any product that uses the files/actions.

Product Conditions

A condition determines when the product or OS upgrade package should be downloaded and installed. Conditions are checked when a product is pushed to a device.

Your device fleet is not always readily available for maintenance. You could have devices in different time zones or countries. Since you cannot always ensure that a device is not in use when you push a product, you can use conditions to delay the download and installation.

These conditions defer the product download or installation until the device meets the criteria of the assigned condition. You can set the products to only download based on battery life, power adapters, user confirmation, and other criteria. The available conditions for your products vary based on the device platform.

Conditions List View

You can view conditions from the list view by navigating to **Devices > Staging & Provisioning > Components > Conditions**. You can also edit and delete conditions from the list view.

Select the pencil icon () to the left of the name of the condition to open the **Edit Condition** screen.

Select the radio button to the far left of the condition to display the **Copy** and **Delete** buttons, offering more actions. Before you can delete a condition, you may have to detach it from one or more products.

Create a Condition

Conditions enable you to set products to download and install on your device only when preset conditions are met. Create a condition to determine when a product downloads and installs onto your devices.

To create a condition, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Conditions** and select **Add Condition**.
2. Select the Platform you want to create a condition for.
3. Complete the **Create Condition Type** settings.

| Settings | Description |
|--------------------|--|
| Name | Enter a name for the condition. The name cannot be longer than 255 characters. |
| Description | Enter a description for the condition. |
| Condition | <p>The type of condition affects the parameters on the Condition Details tab.</p> <ul style="list-style-type: none"> • Adapter Time. • Power. • Schedule. • SD Card Encryption. |
| Managed By | Select the organization group that manages the condition. |

4. Select **Next**.
5. Complete the **Create Condition Details** settings based on the condition type selected.

- **Adapter Time** – This condition type tests for various combinations of constraints related to **Network Adapters** including local date, time, and frequency on the device.

| Settings | Description |
|------------------------------------|--|
| Specify scenario #1? | <p>Set to Specify this scenario to begin configuring the condition scenario.</p> <p>Up to 5 scenarios may be entered, each with their own constraint choices.</p> <p>Each Scenario is an OR statement and each option inside a Scenario is an AND statement. For example, a device will check to see if Scenario #1 OR Scenario #2 is true. If Scenario #1 is true, it will check if all the constraints listed are true because they are AND statements.</p> |
| Scenario description | Enter a description for the adapter time scenario. |
| Constrain Network Adapters? | <p>Set to Constrain based on the Best Connected Network Adapter and configure the following.</p> <ul style="list-style-type: none"> ◦ Specify any Included or Excluded Network Adapters. <ul style="list-style-type: none"> ◦ Choose to either Select Network Adapter Class from a drop-down list or Type in a Network Adapter Name. ◦ Up to five network adapters may be selected in the Adapter selection method? setting. ◦ For each adapter you want to include/exclude, choose between Select a Network Adapter Class drop-down list and entering a specific Adapter name. <p>If you want to skip this kind of constraint, then select Don't constrain based on the Best Connected Network Adapter. Then you can proceed with defining another kind of constraint.</p> |
| Constrain days of week? | For each day of the week, choose whether it will be included or excluded. |
| Constrain months? | For each month, choose whether it will be included or excluded. |
| Constrain days of month? | Enter a Start day of month? and an End day of month? . |
| Constrain years? | Enter a Start year? and an Last year? . |
| Constrain time of day? | Enter the Start hour? , Start minute? , End hour? , and End minute? . |
| Set frequency limit? | Ranges from Every 15 Minutes to Every 1 Week . |

- **Power** – This condition type tests how a device is being powered, including whether the device is plugged in or

has a suitably high battery level. Use a **Power** condition type to prompt users to place the device into the cradle or to insert a charged replacement battery.

| Settings | Description |
|--------------------------------|---|
| Message to be displayed | |
| First line prompt | Enter a header for the prompt. |
| Second line prompt | Enter the body of the prompt. |
| Third line prompt | If you enable a countdown, you can enter a countdown phrase into the Third line prompt field. For example, "You have %count% seconds to comply" where %count% will be the countdown clock. |
| Condition | |
| Required power level | Enter the required power level for the condition to test true. <ul style="list-style-type: none"> ○ A/C. ○ A/C or Full Battery. |
| Delay | |
| Delay (seconds) | Use this to delay for a specified time or until the end user makes a selection. If you enter a non-zero value, the prompt will wait for that value worth of seconds. If the end user does not make a selection in the time allowed, the condition is automatically considered not met. If a value of zero is entered, then the prompt will display indefinitely until the end user makes a selection. |
| Enable countdown? | This allows delay time to be "counted" down on the device so the end user knows how much time is remaining for the user to make a selection. |

- **Schedule** – This condition type tests the device date and time against a specific date/time entered. When the date/time is met, the condition passes and allows the download.

| Settings | Description |
|-------------|--|
| Date | Select the specific date from the drop-down calendar. |
| Time | Select the specific hour and minute from the drop-down menu. |

- **SD Encryption** – This condition type tests whether the device's SD card is encrypted or not encrypted. This can be relevant if you need to wait for the SD card to be encrypted before downloading a file.

| Settings | Description |
|-------------------|--|
| SD card is | Select Encrypted or Unencrypted to limit the product based on the state of the SD card encryption. |

6. Select **Finish**.

Delete a Condition

Remove unwanted conditions from your product. Workspace ONE™ UEM checks any attempt to delete a condition against the list of active products.

To delete a condition, it must be detached from all products as detailed below.

1. Select the **Product** listed in the Warning prompt.
2. Select **Edit**.
3. Remove the condition from the product.
4. Select **Save**.
5. Repeat the steps above for all products containing the condition.
6. Once the condition detaches from all products, you can delete the condition.

If a condition is part of an active product, a warning prompt appears listing any product that uses the condition.

Custom Attributes

Custom attributes enable administrators to extract specific values from a managed device and return it to the Workspace ONE UEM console. You can also assign the attribute value to devices for use in product provisioning or device lookup values.

These attributes allow you to take advantage of the rules generator when creating products using Product Provisioning.

Note: Custom attributes (and the rules generator) are only configurable and useable at Customer-level organization groups.

Custom Attributes Database

Custom attributes are stored either as XML files on the device or in the custom attribute database on the Workspace ONE™ UEM console server. When using the database, custom attributes are sent as samples to Workspace ONE UEM periodically for asset tracking of key/value pairs. If a record in the device database is configured with 'Create Attribute' = TRUE, then the AirWatch Agent automatically retrieves the Name and Value sent with the custom attributes sample. The key/value pair displays in the Device Details page for the device in the Custom Attributes tab.

Create Custom Attributes

Create a custom attribute and values to push to devices. You create the attributes and values associated with them. For more information, see [Create Custom Attributes on page 23](#).

Importing Custom Attributes

The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters. For more information, see [Custom Attributes Importing on page 23](#).

Platform-Specific Custom Attributes Provisioning

You can push custom attributes to a device using XML provisioning for use with advanced product provisioning functionality. The method for pushing the XML varies based on the device platform.

Note: Custom Attribute values cannot return the following special characters: / \ " * : ; < > ? |. If a script returns a value which contains these characters, the value is not reported on the console. Trim these characters from the script's output.

Create Custom Attributes

Create a custom attribute and values to push to devices. These attributes and values control how product rules work and function as lookup values for certain devices.

1. Navigate to **Devices > Staging & Provisioning > Custom Attributes > List View**.
2. Select **Add** and then select **Add Attribute**.
3. Under the **Settings** tab, enter an **Attribute Name**.
4. Enter the optional **Description** of what the attribute identifies.
5. Enter the name of the **Application** that gathers the attribute.
6. Select **Collect Value for Rule Generator** to make the values of the attribute available in the drop-down menu of the rule generator.
7. Select **Use in Rule Generator** if you want to use the attribute in the rule generator.
8. Select **Persist** to prevent the removal of the custom attribute from the Workspace ONE™ UEM console unless an Admin or an API call explicitly removes it. Otherwise, the attribute is removed as normal.
If you delete a custom attribute reported from a device to the UEM console, a persisted custom attribute remains in the UEM console.
Custom attribute persistence is only available to Android and Windows Rugged devices.
9. Select **Use as Lookup Value** to use the custom attribute as a lookup value anywhere in the UEM console.
For example, you can use custom attributes as part of a device friendly name to simplify device naming.
10. Select the **Values** tab.
11. Select **Add Value** to add values to the custom attribute and then select **Save**.

Custom Attributes Importing

The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters.

With the templates, you can import custom attributes in different ways and with different information.

Caution: The syntax of the first column of each template must be replicated exactly. Failure to use the proper syntax can cause database issues and result in loss of data.

Template Types

- Custom Attributes Template – Allows you to define a custom attribute and its settings.

| | A | B | C | D | E | F | G |
|---|---------------------|----------------------------|-----------------|---------------------|-------------------------------|---------|-------------------|
| 1 | CustomAttributeName | Description | ApplicationName | UsedInRuleGenerator | CollectValuesForRuleGenerator | Persist | ShowOnDevicesGrid |
| 2 | AgentVersion1 | Airwatch Agent Description | Services1.exe | 1 | | 0 | 1 |
| 3 | AgentVersion2 | Airwatch Agent Description | Services1.exe | 1 | | 0 | 1 |
| 4 | AgentVersion3 | Airwatch Agent Description | Services1.exe | 1 | | 0 | 1 |
| 5 | AgentVersion4 | Airwatch Agent Description | Services1.exe | 1 | | 0 | 1 |

- Custom Attribute Values Template – Allows you to define the values of predefined custom attributes.

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|------------------|------------------|--------------------------|-------------------|---|---|---|---|---|---|---|---|---|
| 1 | SSID Bangalore | SSID Palo Alto | PreSharedKey AdminOffc | Custom Attributes | | | | | | | | | |
| 2 | Enterprise | PLTO_1 | ADMINS | | | | | | | | | | |
| 3 | BNG_Test | PLTO_Guest | ADM1N | Values | | | | | | | | | |
| 4 | AWT | | #Dm1N | | | | | | | | | | |

- Device Custom Attribute Values – Allows you to define the values of predefined custom attributes for individual devices based on the cross reference (Xref) value. The Xref values determine the individual devices receiving the value for each custom attribute.

| | A | B | C | D | E | F | G | H | I |
|---|----------|-----------|--------------|------------------|------------------|-------------|-------------------------------|---|---|
| 1 | XRefType | XRefValue | SSID Cust1 | USERNAME Cust2 | PASSWORD Cust3 | SSID CXXX | Services1.exe AgentVersion1 | | |
| 2 | 1 | 5263 | AW_BNG | DEV1 | XXXXXXXXXX | SS | 5.3.56.147 | | |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |

- DeviceID (Workspace ONE™ UEM assigned DeviceID when the device enrolls)
- Serial Number
- UDID
- MAC Address
- IMEI Number

Save the file as a .csv before you import it.

Assign Organization Groups Using Custom Attributes

Configure rules that control how devices are assigned to organization groups following enrollment. You can only create one custom attribute assignment rule for each organization group you run.

- Ensure that you are currently in a customer type organization group.
- Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.
- Set **Device Assignment Rules** to **Enabled**.
- Set the **Type** to **Organization Group by Custom Attribute**.

5. Select **Save**.
6. Navigate to **Devices > Staging & Provisioning > Custom Attributes > List View > Add > Add Attribute** and create a custom attribute if you have not already done so. See [Create Custom Attributes on page 23](#) for more information.
7. Navigate to **Devices > Staging & Provisioning > Custom Attributes > Custom Attributes Assignment Rules > Add Rule**.
8. Select the **Organization Group** to which the rule assigns devices.
9. Select **Add Rule** to configure the logic of the rule.

| Setting | Description |
|------------------------------|---|
| Attribute/Application | This custom attribute determines device assignment. |
| Operator | <p>This operator compares the Attribute to the Value to determine if the device qualifies for the product.</p> <p>When using more than one Operator in a rule, you must include a Logical Operator between each Operator.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Note: There is a limitation on the less than (<) and greater than (>) operators. This limitation includes "less than or equal to" and "greater than or equal to" variants. These operators are mathematical in nature, which means they are effective at comparing numbers including integers. They cannot be used to compare non-numeric text strings. And while it is common for software versions to be represented with numbers indicating a graded versioning system (for example, 6.14.2), such representations are not numbers because they have more than one decimal point. These representations are actually text strings. Therefore, any assignment rule that compares software version numbers with multiple decimal points using greater than or less than operators (and their variants) can result in an error message.</p> </div> |
| Value | All values from all applicable devices are listed here for the Attribute selected for the rule. |
| Add Logical Operator | Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules. |

10. Select **Save** after configuring the logic of the rule.

When a device enrolls with an assigned attribute, the rule assigns the device to the configured organization group.

Windows Desktop Custom Attributes

Use XML provisioning to collect custom attributes based on device details. Custom attributes enable you to use advanced product provisioning functionality.

Implementation





To begin collecting custom attributes, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions > Add** and select **Windows > Windows Desktop** as your platform.

2. Complete the steps to create an XML product as mentioned in Create an XML Provisioning File. Upload the XML file and specify the download path as **{installation path}\AirWatch\AgentUI\Cache\Profiles**.

Upon receiving the XML file, the AirWatch Unified Agent creates a custom attributes output file. During the next check-in with Workspace ONE™ UEM, the agent sends the output file to the UEM console.

Once the XML file installs, the custom attributes requested in the file are reported to the UEM console. These values display in the console in the Device Details page under custom attributes. This page allows you to view the name of the attribute and the values returned from each device. These values can be used to create product assignment rules using the Custom Rules system.

| Summary Compliance Profiles Apps Updates Content Location User Custom Attributes ▾ | | | | | |
|--|---|----------------|--------------|--|----------------------------------|
| | | | |   <input type="text" value="Search List"/> | |
| | | Source | Application | Attribute ▲ | Value |
| <input type="radio"/> |  | Device Sourced | services.exe | Device Model | Virtual Machine |
| <input type="radio"/> |  | Device Sourced | services.exe | Serial Number | 2021-07-14 08:00:00 AM UTC+08:00 |

Items 1 - 2 of 2

Page Size: 50 ▾

Note: Custom Attributes support the HKLM registry hive only.

You can also view existing custom attributes for all devices at a particular organization group and manually create custom attributes directly in the console. Navigate to **Devices > Staging & Provisioning > Custom Attributes > List View** to see these custom attributes listed. Any custom attribute created in this manner automatically associates with a device and its respective custom attribute value that is successfully transmitted to the console.

Syncing Registry Settings

To synchronize the registry settings on a Windows 8 device with the console, which is likely the most common use of custom attributes for Windows 8 devices, you need to create a custom XML file. Below is an example of the format of an XML file that can pull information from the registry on a device:

Windows 8.1 Example

```
<?xml version="1.0"?>
-<wap-provisioningdoc>
  -<characteristic type="com.airwatch.getregistryinfo.winpc">
    <reg_value value_name="KeyName(i.e. CommonFilesDir)" key_name="RegistryPath(i.e.
Software\Wow6432Node\Microsoft\Windows\CurrentVersion)" custom_attribute_name="AttributeName"/>
    <reg_value value_name="Keyname ..." key_name="Path\..." custom_attribute_name="AttributeName">
```

```

    </characteristic>
</wap-provisioningdoc>

```

Windows 10 Example

```

<xml version="1.0">
  <wap-provisioningdoc name="System Info /V_1">
    <characteristic type="com.windowspc.getregistryinfo.managed">
      <reg_value
        custom_attribute_name="Hostname"
        key_name="SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName"
        value_name="ComputerName"/>
    </characteristic>
  </wap-provisioningdoc>

```

It must be in the previous format for the XML file to get correctly parsed and the registry settings to be outputted to a key value pair that can be exported back to the AirWatch Console. In this example, the registry key path is “HKEY_LOCAL_MACHINE\Ident” for two of the values and within that key path it is reading the values of “Username” and “OrigName”. The ‘custom_attribute_name’ parameter is the name of the custom attribute that displays in the console and corresponds to the value read from the device.

Create a Product

After creating the content you want to push to devices, create a product that controls when the content is pushed. Creation of the product also defines the order in which the product is installed.

To edit a product, the product must be deactivated in the list view first.

To create and configure a product.

1. Navigate to **Devices > Staging & Provisioning > Product List View > Add Product**.
2. Select the Platform you want to create a staging configuration for.
3. Complete the General text boxes.

| Setting | Description |
|------------------------------|--|
| Name | Enter a name for the product. The name cannot be longer than 255 characters. |
| Description | Enter a short description for the product. |
| Managed By | Select the organization group that can edit the product. |
| Assigned Smart Groups | Enter the smart groups the product provisions. |

4. Select **Add Rules** to use **Assignment Rules** to control which devices receive the product.

Application rules can be applied to unmanaged applications installed on the device. These rules allow you to use system apps and third-party apps that are not managed by Workspace ONE™ UEM.

| Setting | Description |
|------------------------------|---|
| Add Rule | Select to create a rule for product provisioning. Displays the Attribute/Application , Operator , and Value drop-down menus. |
| Add Logical Operator | Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules. |
| Attribute/Application | This is the custom attribute used to designate which devices receive the product. Custom attributes are created separately. For more information, see Custom Attributes on page 22 . |
| Operator | This operator compares the Attribute to the Value to determine if the device qualifies for the product. <div> <p>Note: There is a limitation on the less than (<) and greater than (>) operators. This limitation includes "less than or equal to" and "greater than or equal to" variants. These operators are mathematical in nature, which means they are effective at comparing numbers including integers. They cannot be used to compare non-numeric text strings. And while it is common for software versions to be represented with numbers indicating a graded versioning system (for example, 6.14.2), such representations are not numbers because they have more than one decimal point. These representations are actually text strings. Therefore, any assignment rule that compares software version numbers with multiple decimal points using greater than or less than operators (and their variants) can result in an error message.</p> </div> |
| Value | This is the value of the custom attribute. All values from all applicable devices are listed here for the Attribute selected for the rule. |

5. Select **Save** to add the **Assignment Rule** to the product.
6. Select the **Manifest** tab.
7. Select **Add** to add actions to the **Manifest**. At least one manifest action is required.

| Setting | Description |
|----------------------|--|
| Action Types | Select the Manifest action to add to the profile: <ul style="list-style-type: none"> • Install Files/Actions – This option runs the Install Manifest. • Uninstall Files/Actions – This option runs the Uninstall Manifest. |
| Files/Actions | Displays when the Action Type is set to Install Files/Actions or Uninstall Files/Actions. Enter the application name. |

8. Add additional **Manifest** items if desired.
9. You can adjust the order of manifest steps using the up and down arrows in the Manifest list view. You can also edit or delete a manifest step.
10. Select the **Conditions** tab if you want to use conditions with your product. These conditions are optional and are not

required to create and use a product.

11. Select **Add** to add either **Download Conditions**, **Install Conditions**, or both.
 - A **Download Condition** determines when a product should be downloaded but not installed on a device.
 - An **Install Condition** determines when a product should be installed on a device.
12. Select the **Deployment** tab if you want to control the time and date that products are activated and deactivated. This tab is optional and is not required to create and use a product.

| Setting | Description |
|--------------------------|--|
| Activation Date | <p>Enter the time when a product automatically activates for device job processing.</p> <p>If the activation date is defined and the product is saved, the product stays inactive until the activation date is met according to the Workspace ONE UEM server time. The policy engine wakes up and automatically activates the product. You can manually activate products with activation dates beforehand. Manually activating a product overrides the activation date.</p> |
| Deactivation Date | <p>Enter the time when a product automatically deactivates from current and new device job processing.</p> <p>If the deactivation date is defined and the product is saved and currently active, it stays active until the deactivation date is met according to the Workspace ONE UEM server time. The policy engine wakes up and automatically deactivates the product. You can manually deactivate products with deactivation dates beforehand. Manually deactivating a product overrides the deactivation date.</p> <p>A deactivation date cannot be set earlier than the activation date.</p> |
| Pause/Resume | <p>Enable to ensure that an interrupted product provisioning due to Wi-Fi connectivity issues will be retried.</p> <p>Enabling this feature sets the product to retry for up to 50 attempts before marking the product as failed and alerting you. If this is not enabled, the product keeps retrying indefinitely and will not alert you that there is an error.</p> |
| Product Type | <p>Determine if a product is Required or Elective.</p> <p>A required product provisions to assigned devices when deployment settings are met. An elective product is only provisioned when it is manually activated on the Device Details View of a provisioned device.</p> |
| Deployment Mode | <p>Select from the following how the product is to be deployed.</p> <p>Relay Server with Device Services Backup – This is the default deployment mode. The device attempts to receive the product from the relay server initially, making 5 separate attempts, then falling back to device services as a secondary source.</p> <p>Relay Server Only – The device only makes attempts to receive the product from the relay server. The device never requests this product from device services.</p> |

13. Select the **Dependencies** tab if you want to set the product to only provision devices that have other products provisioned as well.
 - Select **Add** to add a dependent product. You can add as many dependent products as you want.

14. Select to deploy the product immediately by selecting **Activate** or wait to deploy later and select **Save**.

Product Verification

You can ensure the product you provision from the console or from an API call is the exact same product that gets received by the device. This product verification is built into the provisioning process. Verification happens on the device agent side but both the device end user and the administrator on the console side is made aware of the product's status.

Chapter 4:

Products Dashboard

View and manage products from the Products Dashboard. Navigate to **Devices > Staging & Provisioning > Products Dashboard**.

The dashboard provides an easy method of viewing the status of your products and the devices they provision. The charts of information allow you to examine specific products or devices so you can remain informed about your device fleet.

Recent Product Status

This chart displays the 10 most recently created products and the status for each product. You can select any section of the bar graph to view the devices to which that product status applies.

- **Compliant** – The product installed on the device and the inventory data of the product reported by the device matches the requirements of the product.
- **In Progress** – The product has been sent to the device and is pending a compliance check based on inventory.
- **Must Push** – The product deployment type is set to elective. The admin on the console side must initiate product installation.
- **Dependent** – The product depends on another product installation before installing onto devices.
- **Failed** – The product reached maximum attempts to install on the device and is no longer attempting to install.

Filters

You can filter the Recent Product Status chart to refer to specific device platforms that support product provisioning. To filter your results, select the **Menu** icon (☰) in the top right corner. Select the platforms you want to filter by.

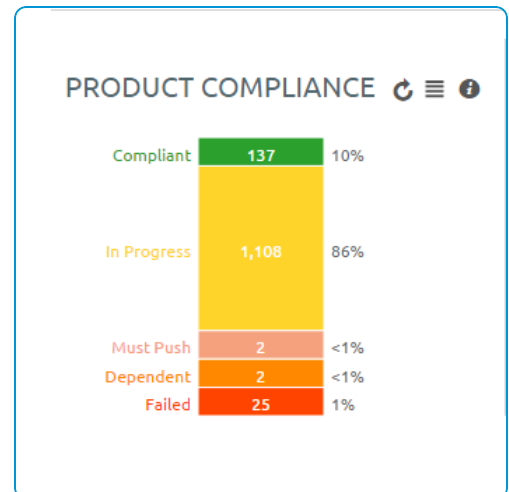
Product Compliance

The Product Compliance chart shows the total percentage of each compliance status. The number displayed in each status is the total number of product statuses reported from each device.

Filters

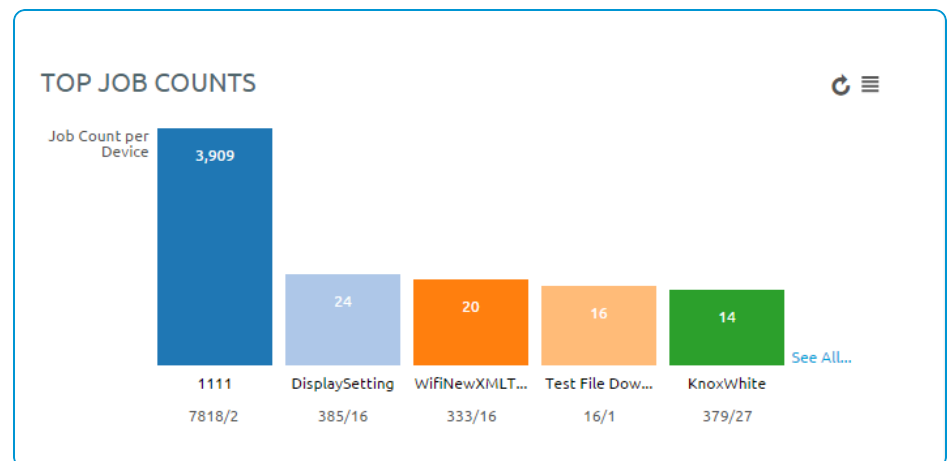
You can filter the Product Compliance chart to display specific device platforms that support product provisioning and the total percentage of each compliance status for a specific products.

To filter your results, select the **Menu** icon (☰) in the top right corner. Select the platforms you want to filter by or enter the products you want to filter by.



Top Job Compliance

This chart displays a ratio of total job count to the number of devices the product is provisioned to. This ratio gives you information on what products are having issues running. For example, if the number shown is a 3, then you know that an average of 3 jobs per device happens for this product. If you select the bar for each product, the View Devices screen displays with all devices currently assigned the product. You can then determine which jobs are failing and the reason for those failures.



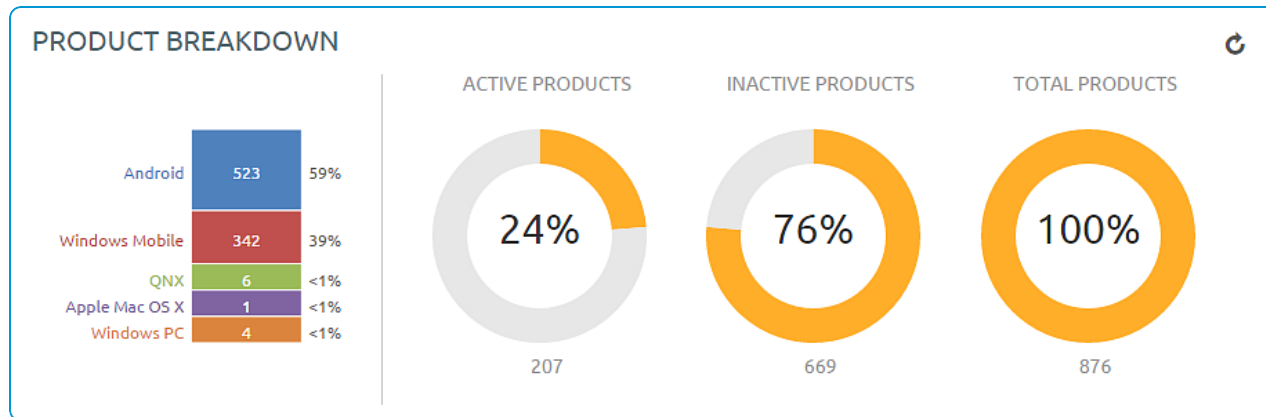
Filters

You can filter the Total Job Compliance chart to refer to specific device platforms that support product provisioning. To filter your results, select the menu icon (☰) in the top right corner. Select the platforms you want to filter by.

Product Breakdown

This section shows you the breakdown of your products. The first chart shows the breakdown of products by platform. Selecting a platform displays the Products List View filtered by that product. This arrangement allows you to see the products available for each platform quickly.

The second chart displays the percentage of your products that are active vs. inactive and a total number of products. Selecting a chart displays the Products List View page filtered by the status of the product.



Products List View

The Product List view allows you to view, edit, copy, and delete products and view the devices a product is provisioning. Navigate to **Devices > Staging & Provisioning > Product List View**. This is the Products List View. Listed here are all the available products for the current organization group. The products can be sorted using the columns.

- **Platform** sorts by the device platform.
- **Managed By** sorts by the organization group the product is assigned to.
- **A/D** sorts by if the product uses activation/deactivation dates or manual.
- **Compliant, In Progress, Failed, and Total Assigned** sort by the status of the product on devices.

Actions

By selecting the **Edit** icon, you can edit a product. You can only edit products after they are deactivated. **Edit** displays the Product Wizard allowing you to change any part of a product.

You can attempt to fix non-compliant products and push the product to the device again by selecting the **Reprocess** button.

The **Force Reprocess** action resends Products to all assigned devices regardless of compliance status. The devices fully download and install every component of the Product manifest, even if it exists on the device already. You can perform this action on multiple products simultaneously.

Select the **Relay Server Status** button (located under the **More** button) to see the status of the relay server associated with the product. Only active products have the **Relay Server Status** button


You can also view history from the View Devices page to see the past and future products pushed to the device based on Product sync.

View Product

Select a product to view the details and settings of the product. The View Product screen displays the general settings, manifest items, conditions, deployment settings, and product dependencies for the product.

Select the **Edit** button to change any of the product settings.

View Devices

From the Products List View, select the **View Devices** icon () to view all devices the product provisions. A quick summary of information on each device allows you to see which devices are at specific statuses.

Select a device **Friendly Name** to open the Device Details Page for that device.

The **Log** listing shows the actions taken by the Workspace ONE™ UEM console to keep the product and device in sync.

Inherited Products

The Product List View displays all inherited products a child organization group receives from the parent organization groups. As products are provisioned based on smart groups and not organization groups, your devices can receive products from a parent organization group.

Products in the Device Details View

You can use the Device Details View to see the products, files/actions, apps, and profiles pushed to a device.

Products

To view the products on a device, navigate to **Devices > List View > Select a device > More > Products**. This displays the products available on a specific device.

Any product that fails to push to devices can be reprocessed by selecting the **Reprocess** button next to the failed product.

Product Sets

Product Sets display on individual device detail pages to show the status of the products' deployments to the device. The products listed that are part of a product set display the product set they pertain to and the deployment status of the products.

The following text boxes display relevant product set information.

- **Product Set** – Displays the product set that contains the product. Select the product set to view the product set details.
- **Status** – Displays the status of the product. For products in a product set, the appropriate product deployed to the device is labeled as **Compliant**. The other products contained in the product set that are eligible for deployment but are not deployed to the device are labeled as **Outranked**. Any product that is not eligible for deployment to the device is labeled as **Not Applicable**.

Files/Actions

Navigate to **Devices > List View > Select a device > More > Files/Actions** to access the files/actions on the device.

Product Job Statuses

Product provisioning works by handling each item in a product as a different job. As a product is pushed to a device, the Workspace ONE™ UEM console updates the status of each job to display any errors or issues that are in process.

Each job follows a workflow and the statuses reflect the position in the process.

| Job Status | Description |
|----------------------|---|
| Queued | The job is created but not yet started. |
| Delivered | Job initially delivered to device database. |
| Paused | Job was previously started but a failure occurred. Jobs resume before other jobs are processed. |
| Download Pending | The download remains in a pending state until download conditions are met. |
| Downloaded | The job downloaded to the device. |
| Install pending | The install is pending until install conditions are met. |
| Installed | The job installed on the device. |
| Deferred | Job download conditions not yet met. |
| Waiting | Job is processing on the device but the status of the job is not confirmed. |
| Completed/ Failed | Job processing complete. Complete means that the process was a success. Failed means that the process failed. |
| Canceled | Job canceled while deferred or waiting. |
| Orphaned | Job being process by device uncompleted when jobs reprocessed. Job will automatically restart when able. |
| Deleted | The job was canceled by the user on the device. |

Product Job Logs

You can view more detail about product jobs by viewing the job logs.

Navigate to **Devices > List View** and select the friendly name of a device that has been provisioned with a product. Next, select the **More** tab, select **Products**, then select the magnifying glass icon to the right of the **Last Job Status** column. This action displays the **Jobs** screen which provides access to the contents of the Job logs.

The Job logs provide a detailed history of events that have elapsed for the device in question as it pertains to the assigned product. This history includes timestamps, progress, error messages, and pause/resume history.

Configure Targeted Job Log Collection

You can target individual devices for job log collection. To activate this option, take the following steps.

1. Navigate to **Groups & Settings > All Settings > Admin > Diagnostics > Logging**.
2. Select the **Enabled** slider for each component and **Scheduled Services** for which you want to collect data.


3. Scroll down to the **Targeted Logging** section, Enable the **Targeted Logging** slider, and complete the settings.

| Setting | Description |
|---|--|
| Organization Group(s) | Select the organization group(s) where the device(s) reside(s). |
| Device ID(s) | Enter the device ID(s) for which you want to enable targeted logging. Use commas to separate multiple device IDs. |
| File Storage Impersonation Enabled | Enable if you are using a file storage server to store these targeted logs and enter the appropriate authentication credentials. |
| File Path | Enter the path and filename of the LOG file where you would like the data saved. |
| File Storage Impersonation User Name | This option appears only when File Storage Impersonation Enabled is checked. Enter the username of the storage server where you targeted logs are saved. |
| File Storage Impersonation Password | This option appears only when File Storage Impersonation Enabled is checked. Enter the corresponding password of the username of the storage server where you targeted logs are saved. |
| Test Connection (button) | Select this button to test the connection. It tests various possible scenarios which the logging process uses and makes sure it is working as expected. |

4. **Save** to apply Targeted Logging.

Define How Much Data to Collect

You can define the length of time job log data is collected. Define this timescale by taking the following steps.

1. Navigate to **Groups & Settings > All Settings > Admin > Data Purging**.
2. Locate the purge module named **DevicePolicyJobPurge** and select the pencil icon () to open the **Data Purging** screen.
3. Complete the **Purge older than (days)** setting with the length of time in days that you want to keep job log data.
4. Select **Save**.

Job logs older than the selected number of days are purged from the Workspace ONE™ UEM console.

Advanced Remote Management

Advanced Remote Management (ARM) allows you to connect remotely to end-user devices so you can help with troubleshooting and maintenance. ARM requires your computer and the end-user device to connect to the Remote Management Server to facilitate communication between the Workspace ONE UEM console and the end-user device.

For more information on installing, configuring, and using Advanced Remote Management, see the **VMware Workspace ONE UEM Advanced Remote Management Guide**, available on docs.vmware.com.

Chapter 5:

Device Dashboard

As devices are enrolled, you can manage them from the Workspace ONE™ UEM **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators. For instance, you can hide 'Asset Number' from the **Device List**.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter.

Windows Desktop Device Details Page

Use the Device Details page to track detailed device information and quickly access user and device management actions. You can access Device Details by selecting a device Friendly Name from the Device List View, using one of the Dashboards, or with any of the search tools.

From the Device Details page, you can access specific device information broken into different menu tabs. Each menu tab contains related device information depending on your Workspace ONE UEM deployment.

Remote Actions

The **More Actions** drop-down on the Device Details page enables you to perform remote actions over the air to the selected device.

The actions vary depending on factors such as the device platform, Workspace ONE UEM console settings, and enrollment status:

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed apps.

The Apps (Query) action requires an active enrolled user login.

- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.

The Certificates (Query) requires an active enrolled user login.

- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM console.
- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.
 - For iOS 11 and below devices, the device wipe command would also wipe the Apple SIM data associated with the devices.
 - For iOS 11+ devices, you have the option to preserve the Apple SIM data plan (if existed on the devices). To do this, select the **Preserve Data Plan** checkbox on the Device Wipe page before sending the device wipe command.
 - For iOS 11.3+ devices, you have an additional option to enable or disable to skip the **Proximity Setup** screen while sending down the device wipe command. When the option is enabled, the Proximity Setup screen will be skipped in the Setup Assistant and thus preventing the device user from seeing the Proximity Setup option.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.

- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.
 - Enterprise Wipe is not supported for cloud domain-joined devices.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.

Important: When locking a device, an enrolled user must be signed into the device for the command to process. The lock command locks the device and any user signed in must reauthenticate with Windows. If an enrolled user is signed-in to the device, a lock device command locks the device. If an enrolled user is not signed in, the lock device command is not processed.

- **Query All** – Send a query command to the device to return a list of installed apps (including AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again.
- **Remote Management** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshoot on the device.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.

Chapter 6:

Create an XML Provisioning File

XML provisioning allows you to download a custom-designed XML file to a device in a provisioning product. After the file is downloaded, it runs an install command to extract the settings from the XML file and install them on the device.

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions** and select **Add Files/Actions**.
2. Select your platform.
3. Enter the required settings on the **General** tab, then select the **Files** tab and upload the desired XML file and enter the destination path on the device.
4. Select the **Manifest** tab and **Add an Install Action** for the XML file.
5. Select **Save**.
6. Navigate to **Devices > Staging & Provisioning > Products List View**, and select **Add Product**.
7. Select your platform.
8. Enter the **General** information.
9. Select the **Manifest** tab.
10. Select **Install Files/Actions** and select the files and actions just created.
11. **Save** and **Activate** the product.

The product downloads to all assigned devices and the XML file successfully installs.

```
<?xml version="1.0"?>

-<wap-provisioningdoc>

  -<characteristic type="com.airwatch.getregistryinfo.winpc">
    <reg_value value_name="KeyName(i.e. CommonFilesDir)" key_
      name="RegistryPath(i.e.
        Software\Wow6432Node\Microsoft\Windows\CurrentVersion)" custom_
```



```
attribute_name="AttributeName"/>

<reg_value value_name="Keyname ..." key_name="Path\...." custom_
attribute_name="AttributeName2"/>

</characteristic>

</wap-provisioningdoc>
```

Chapter 7:

Appendix: Batch File Guidelines

While writing and running batch (BAT) files when working with rugged devices, you should follow some best practices.

Accounting for Path

Windows Unified Agent is a 32-bit application, so when trying to run scripts in a 64-bit machine, proper redirections must be used to get access to the 64-bit folder or the registry hive.

There are two %windir%\System32 on a Windows x64 system.

- **%windir%\System32** directory is for 64-bit applications. This directory contains a 64-bit cmd.exe.
- **%windir%\SysWOW64** directory is for 32-bit applications. This directory contains a 32-bit cmd.exe.

Since AirWatch Agent is a 32-bit application, it can access %windir%\System32 for running 64-bit applications by using **%windir%\Sysnative** in path.

Admin must use **%windir%\Sysnative** in script to access any 64-bit applications.

For example,

```
%windir%\Sysnative\manage-bde -on c: -skiphardwaretest
```

- **manage-bde** is a 64-bit application and it can be accessed only by providing proper path **%windir%\Sysnative**.
- **Certutil** is part of both folders (32-bit and 64-bit), so no need to give %windir%\Sysnative in the script.

Writing Scripts for Registry

Since Windows Unified Agent is a 32-bit application, it always creates a record or performs any action on WOW6432 Node.

On 64-bit Windows, HKLM\Software\Wow6432Node contains values used by 32-bit applications running on the 64-bit system.

32-bit applications do not create records in HKLM\Software directly.

To write explicitly to a 64-bit hive, add the `/reg:64` modifier to the end of your REG ADD command in scripts to create a record in the HKLM\Software registry path.

For example, `REG ADD HKLM\Software\MyApp /reg:64`

General Instructions

- Running scripts in admin context when Standard User is logged in performs actions for Admin User.

For example,

Running a script in User context installs a certificate for a standard user in the Current user store.

Running a script in Admin context installs a certificate for an Admin in the Current user store.

- Path should be quoted while passing arguments to batch files.

For example,

```
"C:\Passing_Argument.bat" Hello World
```

- The BAT file extension must always be included in the file path. Omitting the extension causes the script not to run. This causes a file not found error.
- It is always recommended to have file action as run while deploying batch files.