

VMware AirWatch Product Provisioning and Staging for QNX Guide

Using Product Provisioning for managing QNX 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 QNX	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: Device Staging	15
Staging Basics	15
Staging Configuration	15
Advanced Staging	15
Sideload Staging	15
Create a Manual Staging Package	16
Configure Advanced Staging	16
Sideload Staging Packages	17
Chapter 4: Product Provisioning	19
Product Provisioning Basics	19
Profiles for Product Provisioning	19
Files/Actions	19
Product Conditions	20
Create a Product	20
Product Provisioning Profiles	20

Edit Product Provisioning Profiles	20
Files/Actions for Products	21
Product Conditions	24
Custom Attributes	25
Create a Product	29
Product Verification	32
Product Sets	32
Chapter 5: Product Management	37
Product Management Basics	37
Product Dashboard	37
Products List View	37
Device Details View	37
Product Job Status	38
Products Dashboard	38
Products List View	40
Products in the Device Details View	41
Product Job Statuses	42
Chapter 6: QNX Device Management	44
AirWatch Agent for QNX Settings	44
Device Dashboard	45
Device List View	45
Device Details Page	45
Advanced Remote Management	46
Appendix: AWTrigger Commands	47
Commands for AWTrigger	47

Chapter 1:

Introduction to Product Provisioning for QNX

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.

Another product provisioning feature is the staging methods of enrollment. Depending on the device type, you can perform device staging that quickly enrolls a device and downloads the AirWatch Agent, Wi-Fi profile, and any other important content. The methods of staging a device vary by platform.

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 QNX devices. For more information on general MDM functionality for QNX devices, see the **VMware AirWatch QNX 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.

- QNX 6.5 devices.

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	aaron		
							


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:

Device Staging

You can stage a device to enroll it and prepare it for production use quickly. A staging package installs the AirWatch Agent, and enrolls the device without end-user input.

Staging Basics

Staging packages are created as part of the product provisioning process. You can include profiles, applications, and files/actions as part of the staging package depending on the device platform.

Sideloaded packages are transferred to a device instead of being scanned or downloaded.

Staging Configuration

If you are not using the Rugged Enrollment Configuration Wizard, you must manually create a staging package. The staging package contains all the relevant enrollment information for devices. After creating a staging package, you install the package onto devices using barcode staging, sideload staging, or on-demand staging. For more information, see [Create a Manual Staging Package on page 16](#).

Advanced Staging

As part of creating a staging package, you can add more instructions and files to the staging package. These advanced components enhance the actions taken during enrollment. For more information, see [Configure Advanced Staging on page 16](#).

Sideload Staging

You can create a sideload staging package to install onto devices to begin the auto-enrollment process for your rugged devices. The sideload staging packages simplify enrollment by combining all the required components into one. For more information, see [Sideload Staging Packages on page 17](#).

Create a Manual Staging Package

Create a staging package to configure your devices to connect to Wi-Fi, download the AirWatch Agent, and enroll automatically. This method does not use the Rugged Enrollment wizard.

To create a staging configuration, follow these steps.

1. Navigate to **Devices > Staging & Provisioning > Staging** and select the **Add Staging** button.
2. Select the Platform for which you want to create a staging configuration. The **Staging Add** screen displays.
3. Complete the required text boxes on the **General** tab.

Settings	Description
Name	Enter the name of the staging configuration.
Description	Enter the description of the staging configuration.
Owned By	Select the organization group under which the staging package applies.
Enrollment User	Enter the user name of the enrollment user. You can search for and select an existing user by clicking the magnifying glass icon. You can also add a user by selecting Add User at the bottom of the drop-down menu.
Password	Enter the password for the enrollment user. You have the option of keeping the password redacted or displaying it as written.
Agent	Select an existing AirWatch Agent package from the drop-down listing to download during staging. You can also add an agent package by selecting Add AirWatch Agent at the bottom of the drop-down menu. These agents are uploaded as an Agent Package. See Upload the AirWatch Agent APF File on page 23 for more information.

4. Select **Save**.

Configure Advanced Staging

After creating a staging package, install product components as part of a staging package using the advance staging options.

To establish a list of ordered steps during staging, take the following steps.

1. After finishing the **General** tab of the Staging window, navigate to **Devices > Staging & Provisioning > Staging** then select the **Add Staging** button and continue to the **Manifest** tab.
2. Select the **Add** button.
3. Select the action you want to take place during staging.

Settings	Description
Action Types	<p>Select one of the following action types.</p> <ul style="list-style-type: none"> • Install Profile • Uninstall Profile • Install Files/Actions • Uninstall Files/Actions <p>For more information on creating files, profiles, actions, see Product Provisioning on page 19.</p>
Profile	Select the profile to use in the staging configuration.

4. Select **Add** again to add additional actions to the manifest.
5. When you are finished adding actions, select **Save**.
6. View the newly created staging profile in the List View. Take additional actions on the profile from the menus on the right.
 - **Edit** your configuration.
 - **Copy** your profile.

Sideload Staging Packages

You can create a sideload staging package to download and install onto devices to begin the auto-enrollment process for your rugged devices. The sideload staging packages simplify enrollment by combining all the required components into one.

You can also create universal barcode staging to stage devices with a generic barcode that does not automatically assign an organization group when enrolling the device. This allows you to create one staging enrollment for all devices and assign the device to an organization group as needed.

Generate a Sideload Staging Package Using the Configuration Wizard

After selecting Sideload as the staging enrollment type in the Enrollment Configuration wizard, create a sideload staging package to download and install onto a device to configure and enroll the rugged device automatically.

Prerequisites

You must create a staging package before you create a sideload staging package. See [Create a Manual Staging Package on page 16](#).

The staging user for the staging package must be a basic user account. Do not use staging users or multi-user staging.

Procedures

To create a side staging package, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Staging**.
2. Select a previous staging package that you want to create a sideloaded staging package for. Select the **More** option

and select **Staging Side Load** from the drop-down.

3. Select the **Organization Group** to which this staging applies.
4. Select **Download** to start downloading the zip file of the staging sideload.

Chapter 4:

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.

Profiles for Product Provisioning

The product provisioning system allows you to create profiles for your rugged devices. The profiles created for rugged devices are installed or uninstalled as part of a product. Profiles created under Products (**Devices > Staging & Provisioning > Components > Profiles**) are different than those created through the non-products process (**Devices > Profiles**). For more information, see [Product Provisioning Profiles on page 20](#).

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 21](#).

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 24](#).

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 29](#).

Product Provisioning Profiles

The product provisioning system allows you to create profiles for your rugged devices. The profiles created for rugged devices are installed or uninstalled as part of a product.

Profiles created under Products are different than those created through Workspace ONE™ UEM. This section lists the differences between profiles created for normal device use and those created for use in product provisioning.

Profile Creation and General Settings

Profiles for use with product provisioning must be created by navigating to **Devices > Staging & Provisioning > Components > Profiles** and select **Add**.

While creating these product provisioning profiles, the general tab will be different than the normal general tab for profiles.

Note: Assignment of profiles happens at the product level and not at the profile level as it is in smartphone profiles.

Saving Product Provisioning Profiles

After configuring your product provisioning profile, select **Save** instead of **Save & Publish**.

Profiles names cannot be longer than 255 characters.

Edit Product Provisioning Profiles

Unlike profiles created for typical MDM deployments, profiles for product provisioning have different rules governing editing or deleting.

Update Profiles

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

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

Delete Profiles

Workspace ONE UEM checks any attempt to delete a profile against the list of active products.

To delete a profile, you must detach it from all products.

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

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

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.

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	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.
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	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. 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.
Terminate	End a process or application running on the device.

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.

Upload the AirWatch Agent APF File

The Agent Package can be uploaded only in specific organization group types, for example, in organization groups of type 'Customer'. Upload the Agent Package at the highest organization group level. You can find the file specific to your OEM located in Workspace ONE™ UEM Resources.

To upload an APF file, follow these steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Agent Packages** and select **Add AirWatch Agent**. Make sure that you are using the top-level organization group.
2. Select the platform for which you are adding the agent package. The Add AirWatch Agent screen displays.
3. Select the **Upload** button next to the **Application File** setting. Next, select **Choose File** to browse for the APF file of the agent version you want to upload.
4. Select the APF file and select **Open** to select the file.
5. Select **Save** to close the upload dialog.
6. With the uploading of the APF file, the settings are automatically populated with data. You can make desired edits to **File Name**, **Package Name**, and **Version** for the agent.
7. Select **Save** to upload the APF file to the UEM console.

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	The type of condition affects the parameters on the Condition Details tab. <ul style="list-style-type: none"> • File. • Time.
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.

Settings	Description
----------	-------------

- **Time** – This condition type tests the local date and time on a device.

Settings	Description
First Time Slot	
Select the month, day and year Start Finish	Select Month , Day , and Year for both Start and Finish.
Select hour and minute Start Finish	Select Hour and Minute for Start and Finish.
Second Time Slot	
Enable time check 2?	Select Yes to display a second set of options identical to the First Time Slot.
Third Time Slot	
Enable time check 3?	Select Yes to display a third set of options identical to the First Time Slot.

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 26](#).

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 27](#).

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.

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 Cust	PASSWORD Cust3	SSID CXXX	Services1.exe	AgentVersion1	
2	1	5263	AW_BNG	DEV1	XXXXXXXXXX	SS	5.3.56.147		
3									
4									

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

4. MAC Address
5. 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.

1. Ensure that you are currently in a customer type organization group.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.
3. Set **Device Assignment Rules** to **Enabled**.
4. 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 26](#) 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> <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.

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.

Setting	Description
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 25 .
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 Profile. • Uninstall Profile. • Install Files/Actions – This option runs the Install Manifest. • Uninstall Files/Actions – This option runs the Uninstall Manifest.
Profile	Displays when the Action Type is set to Install Profile or Uninstall Profile. Enter the profile name.
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	Enter the time when a product automatically activates for device job processing. 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.
Deactivation Date	Enter the time when a product automatically deactivates from current and new device job processing. 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. A deactivation date cannot be set earlier than the activation date.

Setting	Description
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.

Product Sets

Occasionally there are conflicting products provisioned to devices due to similar grouping in smart groups and custom attributes. Product sets allow you to group conflicting products and rank the products based on business needs.

Product Sets Basics

Product sets contain multiple products that you want to keep mutually exclusive. Product sets are useful for situations where the products contained inside the product set consist of content that should only apply to specific devices within the parameters set by the rules engine using custom attributes.

The products in the product set follow a hierarchy based on ranking according to business needs. From a given product set, a device receives only one product that applies to the device. This product is the highest ranked product where the device meets the smart group and custom attribute rules criteria. Once a device receives a product from a product set,

the device will not receive any other products from the set unless the rank of a subsequent product is elevated or a new product is created in the set with a higher rank.

Important: A product must exist as either a standalone product or as part of a product set. The product set ensures the integrity of mutual exclusivity of products for a given device.

Create a Product Set

Create a product set to control the delivery of multiple products so a device receives only the specific product that applies to the device based on your business rules. For more information, see [Create a Product Set on page 33](#).

Product Set Management

Managing product sets includes more requirements and actions from you than other management functionality in the Workspace ONE™ UEM console. As product sets create complicated relationships between smart groups and products, removing and editing product sets cause multiple reactions for each action taken. For more information, see [Product Sets Management on page 34](#).

Create a Product Set

Create a product set to control the delivery of multiple products so a device receives only the specific product that applies to the device based on your business rules.

To create a product set, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Product Sets** and select the **Add Product Set** button.
2. Select the platform for which you want to create the product set.
3. Complete the **General** text boxes.

Settings	Descriptions
Name	Enter a name for the product sets. The name cannot be longer than 255 characters.
Description	Enter a short description for the product sets.
Managed By	Select the organization group that can edit the product sets.

4. Select the **Products** tab.
5. Select **Add** to add products to the product set.
6. Create a product including manifest items, conditions, and deployment settings. See [Create a Product on page 29](#) for more information on creating a product. Ensure that you use the rules engine to create custom attribute-based rules for each product so the policy engine can properly assign the products.
7. Use the **Up** and **Down** arrows to adjust product ranking based on business needs.
8. Set products to **Active** if needed.
9. Select **Save** to create the product set.

Product Sets Management

Managing product sets includes more requirements and actions from you than other management functionality in the Workspace ONE™ UEM console. As product sets create complicated relationships between smart groups and products, removing and editing product sets cause multiple reactions for each action taken.

- [Product Sets in Device Details on page 34.](#)
- [Add a Product to a Product Set on page 34.](#)
- [Change the Product Ranking in a Product Set on page 35.](#)
- [Removing Products from Product Sets on page 36.](#)

Activating and Deactivating Products in a Product Set

When you select to activate or deactivate a product that is part of a product set, a series of reactions take place.

- Deactivating a product in a product set sends a removal command to all devices with that product, and the next highest ranked product is installed.
- Activating a product in a product set might trigger other products to be removed on devices, and the newly activated product to be installed.

Product Sets in Device Details

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 **Products** tab displays all the products in a product set that is assigned to a device. The status of the products in relation to the device is displayed as well. Not all the displayed products from a product set are applicable for the device viewed.

To see the product sets in the Device Details, navigate to **Devices > List View** and select the device you want to view. Then select the **More** option and select **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**.

Add a Product to a Product Set

Add a product to an existing product set. This action requires following specific rules due to the complicated relation between products and business rules.

A new product in a product set is added with the lowest ranking in the set by default. If the new product should be a higher rank, you must edit the ranking. See [Change the Product Ranking in a Product Set on page 35](#) for more information on what happens when product ranks are adjusted.

To add a product, take the following steps.


1. Navigate to **Devices > Staging & Provisioning > Product Sets**.
2. Find the product set you want to add a product to and select the **Edit** icon ().
3. Select the **Products** tab.
4. Select **Add Product**.
5. Manually adjust the product rank as needed according to your business needs.
6. Select **Save** to add the product to the product set.

Any modifications made during the edit of a product set do not take effect until you save the product set. Once saved, the product set enters the policy engine for evaluation.

Change the Product Ranking in a Product Set

Product set ranking controls which product of a product set is sent to a device. Since the ranking is the key feature of product sets, changes in ranking cause a series of reactions in the product set.

To change product ranking, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Product Sets**.
2. Find the product set you want to add a product to and select the **Edit** icon ().
3. Select the **Products** tab.
4. Manually adjust the product rank as needed according to your business needs.
5. Select **Save** to apply the rank changes.

Listed below are examples of rank changes and what happens to the product, product set, and devices as a result.

Reason for Edit	Effect of Edit
Adding a new product.	The new product is set at the lowest rank. You must manually change the rank of the new product as needed.
Changing rank of existing products	<p>Increasing the rank (selecting Up arrow) of a product decreases the rank of all subsequent products by one.</p> <p>Decreasing the rank (selecting Down arrow) of a product increases the rank of previously lower-ranked products.</p> <p>After you complete the rank changes and save the product, the product set enters the policy engine for evaluation. The engine assesses the custom attribute for each device against the new device rankings.</p> <p>If you reorder the Products priority within a Product Set, then the Products are reassigned based on the new priority order. As a result, the Workspace ONE™ UEM console sends removal commands for all devices affected by the reorder and assign Products based on the new order.</p> <p>After editing product ranking, only the products affected by the new ranking receive removal and install commands. Products outside the change in ranking are not affected.</p>


Removing a Product	<p>Removing a product increases the rank of all products previously ranked below the deleted product by one. If multiple products were removed, the ranking increases by one for each product removed.</p> <p>All products that preceded the deleted product's rank remain unchanged.</p> <p>Any products that had the removed product installed receives a new product based on the new rankings.</p>
---------------------------	--

Removing Products from Product Sets

Remove a product from an existing product set. This action requires following specific rules due to the complicated relation between products and business rules.

Removing a product from a product set raises the rank of all products previously ranked below the removed product by one. If multiple products are removed, the remaining products are adjusted by one rank for each product removed. See [Change the Product Ranking in a Product Set on page 35](#) for more information on what happens when product ranks are adjusted.

To remove a product, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Product Sets**.
2. Find the product set you want to add a product to and select the **Edit** icon ().
3. Select the **Products** tab.
4. Select the check box for each product you want to remove from the product set.
5. Select the **Delete** button to remove the products.
6. Manually adjust the product rank as needed according to your business needs.
7. Select **Save** to add the product to the product set.

Any modifications made during the edit of a product set do not take effect until you save the product set. Once saved, the product set enters the policy engine for evaluation.

Chapter 5:

Product Management

Manage products using the product provisioning management functionality. Use these tools in addition to the tools mentioned in the **Workspace ONE™ UEM Mobile Device Management Guide** to manage your rugged devices.

Product Management Basics

Product management uses the Products Dashboard, Products List View, and Device Details View to manage how devices use products. Rugged devices have different device actions and options than consumer devices. Some actions, such as Remote Management, require additional configuration before using with devices.

Products must be deactivated before most device actions work. You must also disable any components before using device actions.

Product Dashboard

View and manage products from the 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 select specific products or devices so you can remain informed about your device fleet. For more information, see [Products Dashboard on page 38](#).

Products List View

The Product List view allows you to view, edit, copy, and delete products. From this view, you can also see the devices assigned the product. For more information, see [Products List View on page 40](#).

Device Details View

You can use the Device Details View to see the products, files/actions, apps, and profiles pushed to a device. For more information, see [Products in the Device Details View on page 41](#).

Product Job Status

Product provisioning works by handling each item in a product as a different job. As a product is pushed to a device, the UEM console updates the status of each job to display any errors or issues in the process. For more information, see [Product Job Statuses on page 42](#).

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.

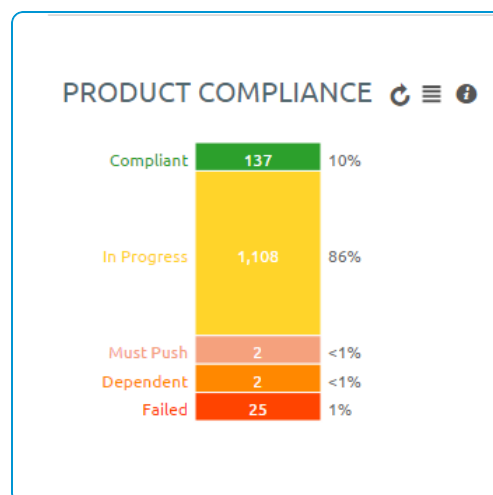
Product Compliance

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

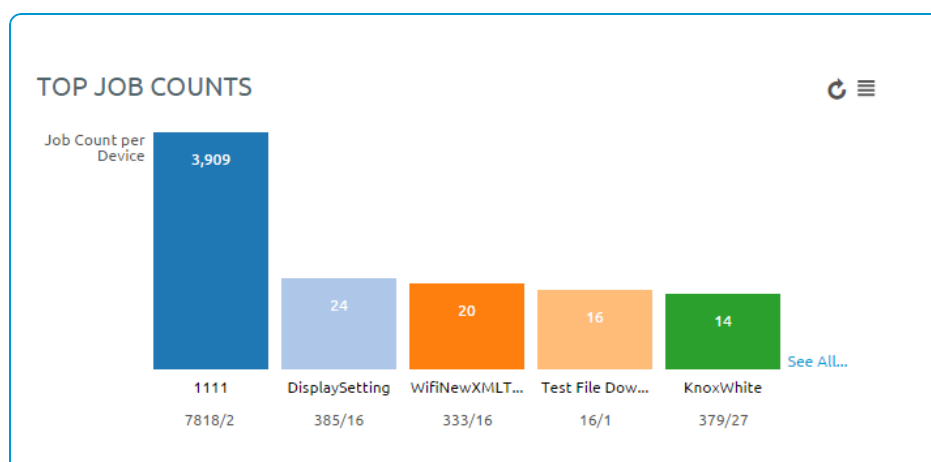
You can filter the Product Compliance chart to display specific device platforms that support product provisioning and the total percentage of each compliance status for a specific products.

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

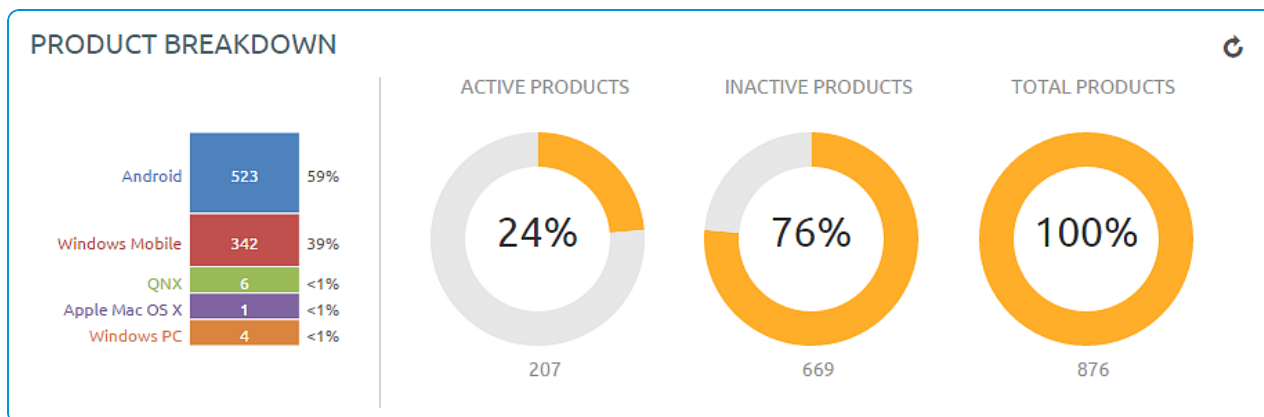
You can filter the Total Job Compliance chart to refer to specific device platforms that support product provisioning.

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.

Profiles

Navigate to **Devices > Details View > Additional Options > Profiles** to access the Profiles 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.

Chapter 6:

QNX Device Management

After your devices are enrolled and configured, manage the devices using the Workspace ONE™ UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

AirWatch Agent for QNX Settings

The AirWatch Agent for QNX devices is pre-configured with Workspace ONE™ UEM. Change these settings when you need the AirWatch Agent to meet certain business needs.

Navigate to **Groups & Settings > All Settings > Devices & Users > QNX > Agent Settings** to edit the AirWatch Agent Settings.

General Settings

Setting	Description
Device ID Algorithm	Set the unique device identification algorithm used on the device.
Heartbeat Interval (min)	Set the time (in minutes) the agent waits before checking-in with the Workspace ONE UEM console.
Data Sample Interval (min)	Set the time (in minutes) the agent waits to collect data from the device.
Data Transmit Time Interval (min)	Set the time (in minutes) the agent waits to send data to the UEM console.

Advanced Remote Management

See [Advanced Remote Management on page 46](#).

Job Notifications

The AirWatch Agent for QNX devices supports Job notifications for products provisioned to the device. Any job that completes displays the device side through the AirWatch Agent for QNX devices.

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.

Device Details Page

The Device Details page displays detailed device information and lets you quickly access user and device management actions.

You can access the Device Details page by selecting a device's Friendly Name from the Device Search page. You can also use one of the available Dashboards or any of the available search tools with the Workspace ONE™ UEM console.

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.

Performing Remote Actions

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

The actions listed below vary depending on factors such as device platform, 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.
- **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.
- **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.
- **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.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.

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.

Appendix:

AWTrigger Commands

AWTrigger allows third-party applications to interact with the AirWatch Agent for QNX.

The applications interact in two ways. The first interaction is the ability to enable/disable the process of products using the fast track. This setting allows you to evaluate products regardless of any conditions enabled for the product. For example, you can install all products available for a device immediately instead of waiting for conditions or dependencies.

The second interaction ability allows you to evaluate all device readiness and detached conditions immediately. This interaction circumvents the normal check-in interval for the agent and will check all conditions at that moment as opposed to waiting for the normal interval.

This appendix lists the commands available for use while using the Workspace ONE™ UEM Installation Directory Command-Line entries.

Commands for AWTrigger

AWTrigger –installnow true

This command processes all the jobs that have already reached the device (and also all the jobs that reach the device after this command has been successfully run) to be processed with immediate effect by disabling all conditions.

AWTrigger –installnow false

This command will disable the installnow functionality. All the jobs that reach the device after this command has been run, will be processed normally (by evaluating conditions).

AWTrigger –condition true

This command causes all the deferred jobs on the device to be reevaluated again with immediate effect to see if the condition specified (in each job) has been met or not. Useful in the case of file conditions.

For example, suppose that a job has been pushed onto the device which has a file condition associated with it and the file condition specifies to check for the presence of a test file. If the test file is missing on the device, AWApplicationManager creates a flag file. Agent defers this job by 5 minutes. After 5 minutes, the AWApplicationManager will again check for the presence of the test file. If the application creates a test file after 2 minutes (of deferring the job) and if the technician does not want to wait for another 3 minutes for the job to be processed, he can run this command and the job will be immediately evaluated. This command causes ALL the deferred jobs to be evaluated with immediate effect.

AWTrigger –h

This prints the usage of the utility into the respective log file.

AWTrigger -migrateca true

This migrates your XML custom attribute files to the new custom attribute database.

In order for the new text boxes to be present in a custom attribute XML file created from a profile, the UEM console version must be at least 8.1, and the AirWatch Agent version must be at least 5.4.66.98.

For clean migration of custom attribute data from XML files to the database, Workspace ONE UEM recommends repushing any profiles that are already installed on any devices so that the new text boxes are present.

Migrating from XML to CA Database

1. Repush existing profiles to update XML files with data for all profile text boxes.
2. Update configuration file "`~/airwatch/General-Config.cfg`" to use `DB_BASED_CA`.

```
[CustomAttributes]
Type = DB_BASED_CA
```

3. Run command for custom attribute migration utility.

```
~/airwatch/AWTrigger -migrateca true
```

4. Check Status

```
~/airwatch/AWStatusFinder -migrateca
```

Migrating AirWatch v8.0 XML files to CA Database

Workspace ONE UEM recommends re-pushing the custom attribute profile from the UEM console after upgrading to AirWatch v8.1. If you choose to migrate to a CA Database without pushing the updated profile, the following decisions are made by the migration process.

- Importing Application values.
 - If an Application value does exist for a custom attribute record in an XML file, then the existing value is used as the value for application when the record is inserted into the database.
 - If an Application value does not exist for an attribute record in an XML file, then the **File Name** is used as the Application value when the record is inserted into the database.
- Importing Attribute Name values.
 - The name of the custom attribute record in the XML element is imported as the name of the custom attribute database record.
- Importing value.
 - The value of the custom attribute record in the XML element is imported as the value of the custom attribute database record.
- Importing is_dynamic values.
 - If an is_dyanmic value does exist for a custom attribute record in an XML file, then the existing values are imported as the is_dynamic value for the database record.

- If an `is_dynamic` value does not exist for a custom attribute record in an XML file, then the `is_dynamic` value is set to "True" for the database record.
- Importing Permission values:
 - If a Permission value does exist for a custom attribute record in an XML file, then the existing value is imported as the Permission value for the database record.
 - If a Permission value does not exist for a custom attribute record in an XML file, then the Permission value is set to "read/write" for the database record.
- Importing sync.
 - If a Sync value does exist for a custom attribute record in an XML file, then the existing value is imported as the Sync value for the database record.
 - If a Sync value does not exist for a custom attribute record in an XML file, then the Sync value is set to "True" for the database record.