VMware AirWatch Product Provisioning and Staging for Windows Rugged Guide

Using Product Provisioning for managing Windows Rugged devices.

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

Table of Contents

Chapter 1:
Introduction to Product Provisioning for Windows Rugged

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 Windows Rugged devices. For more information on general MDM functionality for Windows Rugged devices, see the **VMware AirWatch Windows Rugged Platform Guide** available on docs.vmware.com.

Supported Devices, OS, and Agents

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

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

- Windows CE 5, 6, and 7.
- Windows Mobile 5.x/6.1/6.5 (Professional and Standard).
- Windows Embedded 6.5.

> **Important:** Motorola and Zebra Windows Rugged devices require the Rapid Deployment Client v2.0+.

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 required for Motorola Rapid Deployment Barcode Enrollment. Otherwise, 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 7.

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 11.

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 10.

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 14.

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 15.

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	Select either Push or Pull as the relay server method. **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. **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. For more information on installing a pull server, see Pull Service Based Relay Server Configuration on page 11.

Setting	Description
Restrict Content Delivery Window	Enable to limit content delivery to a specific time window. Provide a **Start Time** and **End Time** to restrict the delivery of content. 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). Please set the system time on the console server accurately to ensure your content is delivered on time.
Assignment	
Managed By	Select the organization group that manages the relay server. If you want to use the FTPS server for Barcode Enrollment only and not for Product Provisioning, remove all assigned organization groups under the Production Server section.
Staging Server	Assign the organization groups that use the relay server as a staging server. A staging server only works for the staging process involving the supported staging clients, Stage Now (Android) and Rapid Deployment.
Production Server	Assign the organization groups that use the relay server as a production server. A production server works with any device with the proper agent installed on it.
Device Connection	
Protocol	This is the information the device uses to authenticate with the FTP(s) server when downloading apps and content. **FTP**, **Explicit FTPS**, or **SFTP** as the Protocol for the relay server. If using Explicit FTPS, your Explicit FTPS server must have a valid SSL certificate. Configure the SSL certificate on the Explicit FTPS server.
Hostname	Enter the name of the server that hosts the device connection.
Port	Select the port established for your server. **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.
User	Enter the server username.
Password	Enter the server password.
Path	Enter the path for the server. 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.
Passive Mode	Enable to force the client to establish both the data and command channels.

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

3. 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.

   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	Enter the IP addresses or the MAC addresses of the server. Separate each address with commas. IP addresses use periods as normal but MAC addresses do not use any punctuation in this form.
Pull Frequency	Enter the frequency in minutes that the pull server should check with the UEM console for changes in the product.

4. Press the **Test Connection** button to test your Console Connection to the 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.

5. 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.

1. Navigate to **Devices > Staging & Provisioning > Relay Servers > List View** and select **Batch Import**.
2. Enter a **Batch Name**.
3. Enter a **Batch Description**.
4. Select **Choose File** to upload the **Batch File**. Batch files must be in CSV format. Select the **Information** icon ( ) to download a template.
5. 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 10 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 7 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 7 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.

Move an Existing Pull Relay Server From One Organization Group to Another

You can move an existing pull relay server installed with the Windows or new Linux installer by taking the following steps.

1. Delete the existing pull relay server from the original OG on the console.

   Once it is deleted, the pull discovery text that belongs to the pull service starts appearing on the undiscovered pull discovery page at Global OG.

2. Navigate to **Devices > Staging & Provisioning > Relay Servers > Undiscovered Pull Relay Servers** and locate the server by searching for your IP address (only available for dedicated SaaS or On-premises).

3. Copy the pull discovery text that includes the IP address of your selected server.

4. Create a relay server in the new OG and activate it.

   After activating the relay server in the new OG, the pull service discovery text listed in the Undiscovered Pull Relay Servers page disappears.

Remote Viewing Files on Relay Server

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

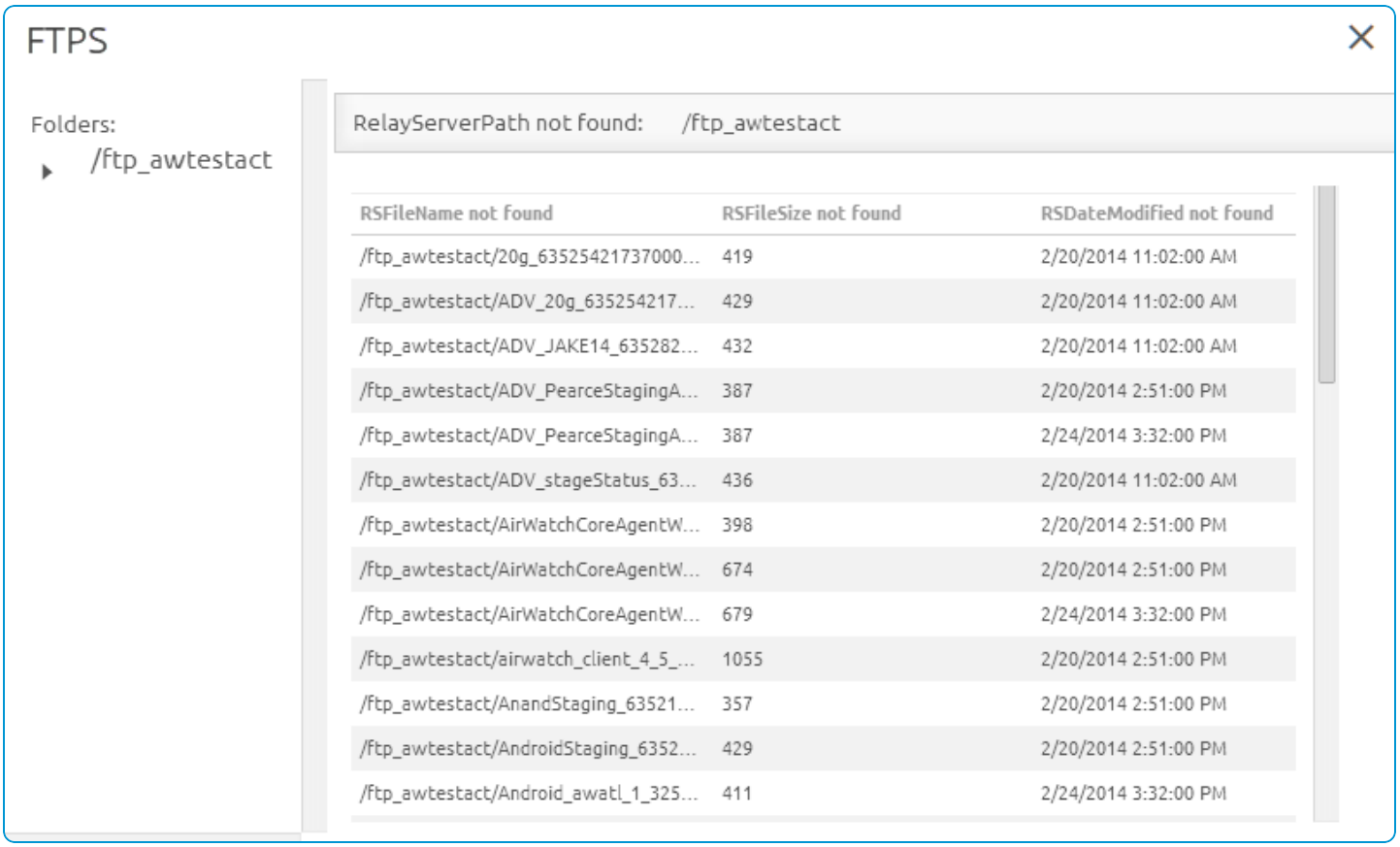
To access the Remote File Viewer, take the following steps.

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.

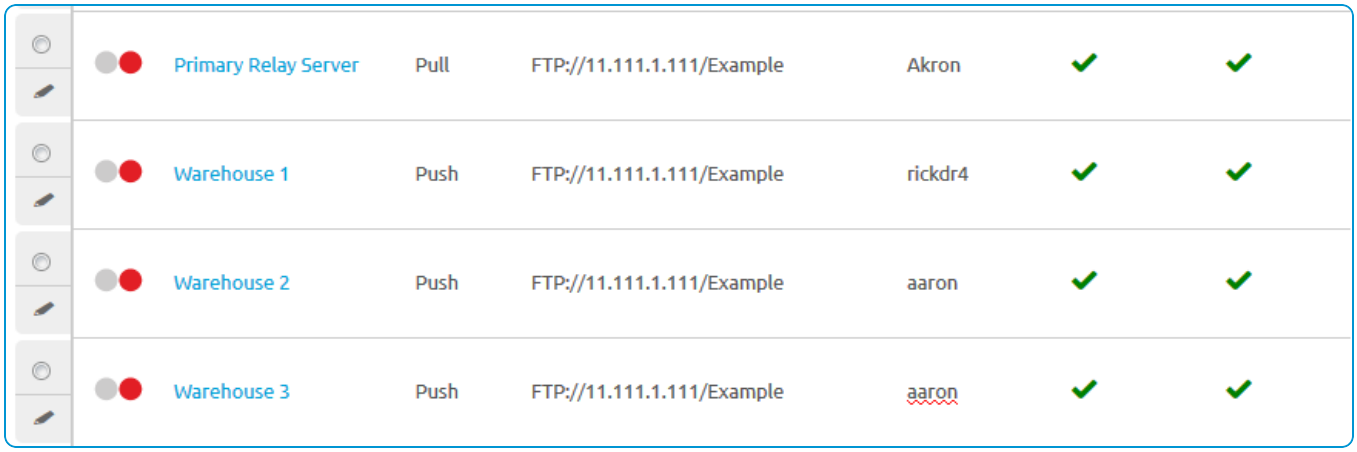


Relay Server Management

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.



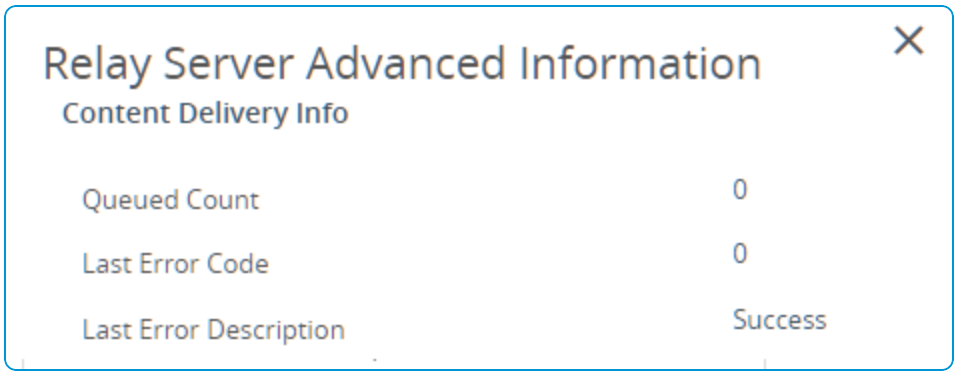
The **Source Server** and **Relay Server** statuses are as follows:

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**.



Chapter 3:
Device Staging

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

Staging Basics

The Rugged Enrollment Configuration Wizard simplifies creating staging packages. With the wizard, everything you need for a staging package is created in a step-by-step process.

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.

You have several methods for enrolling a rugged device through staging. Barcode Enrollment creates a staging package associated with a barcode that you scan to stage the device. On-Demand staging uses the Rapid Deployment Client (RD Client) to download the staging package to your Zebra Windows Rugged or Motorola devices. The Stage Now client is exclusive to Android devices with Zebra MX version 7.1+ under Android Nougat and later. Sideloading packages are transferred to a device instead of being scanned or downloaded.

Rugged Enrollment Configuration Wizard

Simplify rugged device enrollment through the Rugged Enrollment Configuration wizard. This wizard helps you complete each step in creating a staging package for your Android Rugged and Windows Rugged devices. The wizard supports QR code enrollment (Android only), barcode enrollment, sideload staging, and web enrollment (Windows Rugged only). For more information, see Use the Enrollment Configuration Wizard on page 18.

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 21.

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 22.

Staging Wi-Fi Profile

It is mandatory that your staging package includes a Wi-Fi profile. This profile configures the device to connect to the network the device uses to access the relay server to download the AirWatch Agent and enroll. For more information, see Create a Wi-Fi Profile for Staging on page 23.

Barcode Staging

You can create a barcode to scan to begin the auto-enrollment process for your Motorola and Zebra rugged devices. The barcodes simplify staging devices into a quick scan of a barcode to configure the device using a created staging package. For more information, see Barcode Staging on page 24.

On-Demand Staging

On-demand enrollment allows Motorola and Zebra rugged devices to scan a network or ActiveSync connection for a broadcast staging package. For more information, see On-Demand Staging on page 25.

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 26.

Use the Enrollment Configuration Wizard

Simplify rugged device enrollment through the Enrollment Configuration wizard. This wizard helps you complete each step in creating a staging package for your Android and Windows Rugged devices.

To use the Enrollment Configuration Wizard.

1. Navigate to **Devices > Staging & Provisioning > Staging** and select the **Configure Enrollment** button.
2. Select the device platform you want.
3. Select the staging enrollment type.
   - Barcode – Create a barcode to scan with your Zebra rugged devices to quickly stage the device. The wizard simplifies the barcode configuration process.

- Sideload – Create a sideload staging package to download and install onto a device to automatically configure and enroll the rugged device.
- Enroll Through Web Enrollment on page 21 – Create a staging package to download and install from a web URL onto a device to automatically configure and enroll the rugged device.

4. Select **Configure**.

The settings you must configure change based on the enrollment type selected.

Generate a Barcode Staging Package Using the Enrollment Configuration Wizard

After selecting Barcode enrollment in the Enrollment Configuration wizard, create a barcode to scan with your Zebra rugged devices to stage the device quickly. The wizard simplifies the staging configuration process.

To create a barcode using the wizard.

1. After taking note of the prerequisites, select **Configure** to begin.
2. Select the **Relay Server** to use to stage the devices.

   The list of relay servers populates from any relay servers created for the organization group or the parent organization groups. If you do not have a relay server created, select **Add Relay Server**.
3. Select **Next**.
4. Select a **Wi-Fi Profile** that devices use to connect to the relay server and download the AirWatch Agent.

   If you do not have a Wi-Fi profile created, select **Add Wi-Fi profile**. You cannot create a Wi-Fi profile through the wizard that uses certificate authentication. The Wi-Fi profile created is used for staging and remains on the device after enrollment.
5. Select **Next**.
6. Select the **AirWatch Agent** to push to devices during staging.

   If you do not have an AirWatch Agent added, select **Add AirWatch Agent** to upload an AirWatch Agent Package if necessary.

   Download the latest version of the AirWatch Agent. Contact your Account Manager or Workspace ONE ™ UEM Support for access.
7. Select **Next**.
8. Enter the **Stage User** credentials.

Settings	Descriptions
Name	Enter the name of the staging package.
Description	Enter a description of the staging package.
Owned By	Select the organization group that owns the staging package.
Enrollment User	Enter the user name of the user. If you do not have a user, select **Add User**. The user must be a basic user account. Do not use staging users or multi-user staging.

9. Select **Next**.
10. Set the **Barcode** settings.

Organization Group	Select the organization group the staging package uses.
Organization Group	Select the organization group the staging package uses.
Universal Barcode	Enable to create a universal barcode enrollment so devices can be enrolled without automatically assigning an organization group. This allows you to enroll devices without needing a Barcode enrollment for each organization group.
Require Password	Enable to create an alphanumeric password (maximum 99 characters) to use to unlock the staging package encryption on the end-user device immediately after enrollment.
Barcode Format	Select the barcode format for the devices you want to enroll.

11. Select **Save**.
12. The **Summary** page allows you to **Download File** of the PDF. You can also **View PDF** to see a preview of your **Barcode Format** selections.

Generate a Sideload Staging Package Using the Enrollment Configuration Wizard

After selecting Sideload enrollment in the Enrollment Configuration wizard, create a sideload staging package to configure and enroll the rugged device. The wizard simplifies the staging configuration process.

To create a sideload staging package using the wizard.

1. Select a **Wi-Fi profile** that devices use to connect to the relay server and download the AirWatch Agent.

   If you do not have a Wi-Fi profile created, select **Create Wi-Fi profile**. You cannot create a Wi-Fi profile that uses certificate authentication through the wizard. The Wi-Fi profile created is used for staging and remains on the device after enrollment.
2. Select **Next**.
3. Select the **AirWatch Agent** to push to devices during staging.

   If you do not have an AirWatch Agent added, select **Add AirWatch Agent** to upload an AirWatch Agent Package if necessary.

   Download the latest version of the AirWatch Agent. Contact your Account Manager or Workspace ONE ™ UEM Support for access.
4. Select **Next**.
5. Enter the Stage User credentials.

Settings	Descriptions
Name	Enter the name of the staging package.
Description	Enter a description of the staging package.
Owned By	Select the organization group that owns the staging package.

Settings	Descriptions
Enrollment User	Enter the user name of the user. The user must be a basic user account. Do not use staging users or multi-user staging.
Password	Enter the password of the user.

6. Select **Next**.
7. Enter the Sideload settings.

Settings	Descriptions
OG	Select the organization group the staging package uses.
Universal	Enable to create a universal enrollment so devices can be enrolled without automatically assigning an organization group. This option allows you to enroll devices without needing a Sideload enrollment for each organization group. The agent prompts you to enter an organization group after the staging process begins.

Enroll Through Web Enrollment

After selecting Web enrollment in the Rugged Enrollment Configuration wizard, create a staging package to enroll devices by sending end users to a URL to enroll. The wizard simplifies the staging configuration process.

To configure Web enrollment with the wizard.

1. Select **Configure Agent** to configure the AirWatch Agent for web enrollment.
2. The default file path to the AirWatch Agent CAB file displays. If you want to use a different CAB, select **Disable** and then select the CAB file you want to use. Select the CAB file for both Windows Mobile, Windows CE, and Windows x86 CE devices.

   To upload your own CAB file, select **Add Application**.
3. Select **Next**.
4. Send end users to the enrollment URL to begin enrollment.

The enrollment URL is configured on the Site URLS page.

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 51 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	Select one of the following action types. • **Install Profile** • **Uninstall Profile** • **Install Files/Actions** • **Uninstall Files/Actions** • **Warm Boot** • **Cold Boot** For more information on creating files, profiles, actions, see Product Provisioning on page 34.
Profile	Select the profile to use in the staging configuration.
Persistent through enterprise reset	Enable to keep the profile, application, or files/actions on the device through enterprise resets. For more information, see Product Persistence on page 38.

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.
   - Select **Barcode** and complete the text boxes on the **Generate Barcode** subpage.

Create a Wi-Fi Profile for Staging

It is mandatory that your staging configuration includes a Wi-Fi profile. This configuration is the network the device uses to connect to the relay server to download the AirWatch Agent.

A Wi-Fi profile is either a staging or production profile. The staging Wi-Fi profile is created under the Products section and connects the device to the relay server so the device can receive the staging configuration. The production Wi-Fi profile is a normal Wi-Fi profile used at the device's daily use locations.

To create a Wi-Fi profile, navigate to the **General** settings of the profile. Set the **Profile Scope** of the Wi-Fi profile:

- **Staging Wi-Fi Profile** – Connects a device to the Wi-Fi used for staging.
- **Production Wi-Fi Profile** – Connects a device to the Wi-Fi used for everyday use. Production Wi-Fi profiles are under **Device > Profiles > List View > Add**. You must use auto deployment and publish the profile before staging a device with it.

Barcode Staging

You can create a barcode and use it to auto-enroll your Motorola and Zebra rugged devices. Barcodes reduce the process to a quick scan which configures the device using a staging package.

You can also create universal barcode staging which does not automatically assign an organization group while enrolling the device. This generic barcode allows you to create one staging enrollment for all devices and assign the device to an organization group later, as needed.

Barcode enrollment is only available on devices running the Rapid Deployment Client or Zebra's Stage Now Client. These clients only support FTP and FTPS relay servers.

Use the Rugged Enrollment wizard to simplify the creation of barcode staging packages. The wizard enables you to create all the necessary components of a staging package in one place. For more information, see Use the Enrollment Configuration Wizard on page 18.

Barcode enrollment is only supported on the following devices.

- Windows Rugged devices with Rapid Deployment client.
  - MC45
  - MC55
  - MC65/67
  - MC75
  - MC3090
  - MC3190
  - MC9090
  - MC9190
  - MC92N0

Generate a Barcode Staging Package

Create a barcode to scan with your Zebra rugged devices to stage the device quickly.

Prerequisites

You must create a staging package before you generate a barcode. See Create a Manual Staging Package on page 21.

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

Procedure

To generate a barcode, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Staging**.
2. Select the radio button to the left of the name of the staging package. A new row of buttons displays under the **Add Staging** and **Configure Enrollment** buttons.
3. Select the **Barcode** button.

4. Select the **Staging Options**.

Settings	Descriptions
Organization Group	Select the organization group the staging package uses.
Universal Barcode	Enable to create a universal barcode enrollment so devices can be enrolled without automatically assigning an organization group. This allows you to enroll devices without needing a Barcode enrollment for each organization group. Enabling this box repopulates the **Staging Relay Server** and **Staging Profile** with applicable options.
Staging Relay Server	Select the staging relay server that hosts the staging content.
Staging Profile	Select the staging Wi-Fi profile to apply to the enrolled device.
Require Password	Enable to create an alphanumeric passphrase (maximum 99 characters) to use to unlock the staging package encryption on the end-user device.

5. Select the **Barcode Format** options.
6. Select **View PDF**. This generates a preview of the barcode PDF output page for end users to scan.
7. Select **Save** to save the PDF file.

On-Demand Staging

On-Demand enrollment allows you to use a staging profile to stage a device without the use of a barcode. The Motorola and Zebra rugged device scans the network connection or an ActiveSync connection for the broadcast On-Demand staging package.

You can also create universal On-Demand enrollment to stage devices without automatically assigning an organization group when enrolling the device. This option allows you to create one on-demand enrollment for all devices and assign the device to an organization group as needed.

On-demand enrollment is only available on devices running a compatible staging client. The compatible staging client can only support FTP and FTPS relay servers.

Create an On-Demand Staging Package

Create an on-demand staging package to stage a device over a network connection or an ActiveSync connection.

Prerequisites

You must create a staging package before you create an on-demand enrollment package. For more information, see Create a Manual Staging Package on page 21.

To use On-Demand Enrollment, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Staging**.
2. Find the staging configuration you want to use, select the radio button to the left of the Name, then select the **More Actions** button when it appears.

3. Select **On-Demand** from the drop-down menu.
4. Specify the staging options.

Settings	Description
Organization Group	Select the Workspace ONE ™ UEM organization group in which the device enrolls.
Universal Barcode	Enable to create a universal on-demand enrollment so devices can be enrolled without automatically assigning an OG. While the option is called universal barcode, there is no actual barcode in use in this functionality. Enabling universal barcode allows you to enroll devices without needing an on-demand enrollment for each OG. The agent will prompt you to enter an OG after beginning the staging process. Enabling this box repopulates the **Staging Relay Server** and **Staging Profile** with applicable options.
Staging Relay Server	Select the relay server from which the device retrieves the agent and other staging content.
Staging Profile	Select the Wi-Fi profile to use during staging to connect to the relay server.

5. Select the **On-Demand** button to start the On-Demand Enrollment screen.
6. Select **Turn staging server on**.
7. On the device you want to enroll, start the supported staging client and use the following settings.

Settings	Description
Search Connected Networks	The staging client searches for an On-Demand staging server over any Wi-Fi profiles that exist on the device, or through LAN if cradled. Motorola devices include a generic Wi-Fi profile out of the box, which you use when setting up a Wi-Fi access point.
Search Unconnected Networks	The staging client searches for an On-Demand staging server using ActiveSync. The device must be cradled and connected to the admin's machine hosting the On-Demand server through USB.

Once a device is connected to an On-Demand server, the staging profile configuration passes to the device. The device then retrieves all staging content from the relay server. Once all staging content has been retrieved and installed, the device enrolls in Workspace ONE UEM.

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.

Simplify creating a barcode staging package by using the Rugged Enrollment wizard. The wizard allows you to create all the necessary components of a staging package in one place. For more information, see Use the Enrollment Configuration Wizard on page 18.

You can use the Sideload Staging Utility for Windows Rugged devices to sideload a staging package easily. The utility simplifies the process of installing a sideloading package onto the device with simple step-by-step instructions.

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 21.

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. (Optional) Enable **Universal Barcode** to enable a universal enrollment so devices can be enrolled without automatically assigning an organization group. This allows you to enroll devices without needing a Sideload enrollment for each organization group. The agent will prompt you to enter an organization group after beginning the staging process.
5. Select **Download** to start downloading the zip file of the staging sideload.

Install a Sideload Staging Package

After creating a sideload staging package and downloading it, install it onto the rugged device to begin the enrollment process.

For Windows Rugged devices, follow the steps below:

1. Unzip the file and connect your device to the staging machine through USB once the download is complete.
2. Manually create "\Program Files\AirWatch\Staging" directory on your device. You must add both the AirWatch and staging directories.
3. Copy the content of the unzipped staging file (it should contain several directory folders) to the directory you created.
4. Open the "\Program Files\AirWatch\Staging\agent" directory and manually run the AirWatch Agent cab file.

The cab file installs the agent, then the enrollment process completes and the agent enrolls the device, assuming the device has network connectivity.

You can also use the Sideload Staging Utility for Windows Rugged devices to simplify the sideload staging process. See Use the Sideload Staging Utility on page 28 for more information.

Important: For sideload staging, if you want to preconfigure your Wi-Fi connection into the staging cab file, you must use the advanced staging feature (Manifest tab on the staging profile) and add a step for installing a production Wi-Fi profile. If this step is not done, then the Wi-Fi profile needs to be manually set up on the device (preferably before running the staging cab).

Use the Sideload Staging Utility

You can easily sideload your Windows Rugged device through the AirWatch Sideload Staging Utility. The utility simplifies the process of installing a sideloading package onto the device with simple step-by-step instructions.

To use the Sideload Staging Utility, follow the steps detailed below.

1. Download the Sideload Staging Utility from the my Workspace ONE ™ documentation repository.
2. Install the utility after the download completes.
3. Start the utility after the installation completes.
4. Connect the device to your computer. The **Choose Side Staging** and **Stage File to Device** buttons become available for use after the utility detects the device connection.

5. Select **Choose Side Staging** and select the .Zip file you want to stage to a device.

6. Select **Stage File to Device** to begin staging the device. The .Zip file unzips, folders and directories are created, and the CAB file installs.

Uninstall Sideload Staging for Windows Rugged

Use the Sideload Staging Utility for Windows Rugged to uninstall sideload staging packages from a device.

1. Start the Sideload Staging Utility.
2. Connect the device to your computer.
3. Once the Sideload Staging Utility detects connection with the device that has existing staging, select any of the following buttons:

Setting	Description
Uninstall AW Agent	Select to remove the AirWatch Agent for Windows Rugged from the device.
Remove Persistence	Select to remove any products marked for persistence through Enterprise Reset.
Remove Registry Key	Select to remove all registry key entries for the staging.

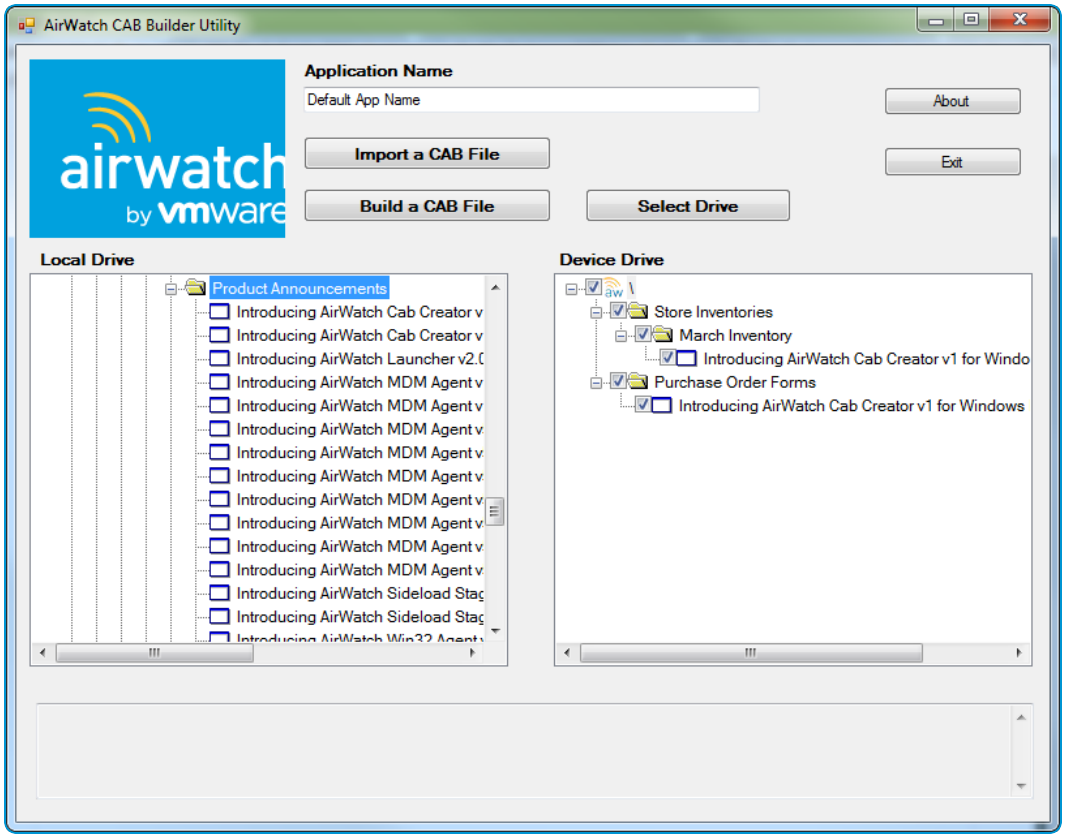
Selecting the uninstall options displays a status message when the action completes.

AirWatch Cab Creator for Windows Rugged

The AirWatch Cab Creator for Windows Rugged allows you to create custom CAB files for use on Windows Rugged devices. These custom CAB files consist of any files or applications you add from your computer.

Simplify the install process combining all the files and applications you want on your Windows Rugged device into a custom CAB file. You can import CAB files into your own custom CAB file.

This feature allows you to create one custom CAB file that contains all the CAB files you must install on a device. You can also use the AirWatch Cab Creator to edit any existing CAB file on your PC. The AirWatch Cab Creator also supports importing files that you can then convert to CAB file upon saving.



Create a Custom CAB

Simplify installation of files onto your Windows Rugged devices by creating custom CAB files using the AirWatch Cab Creator for Windows Rugged. These custom CABS can contain your business files or the files necessary to upgrade your Windows Rugged devices.

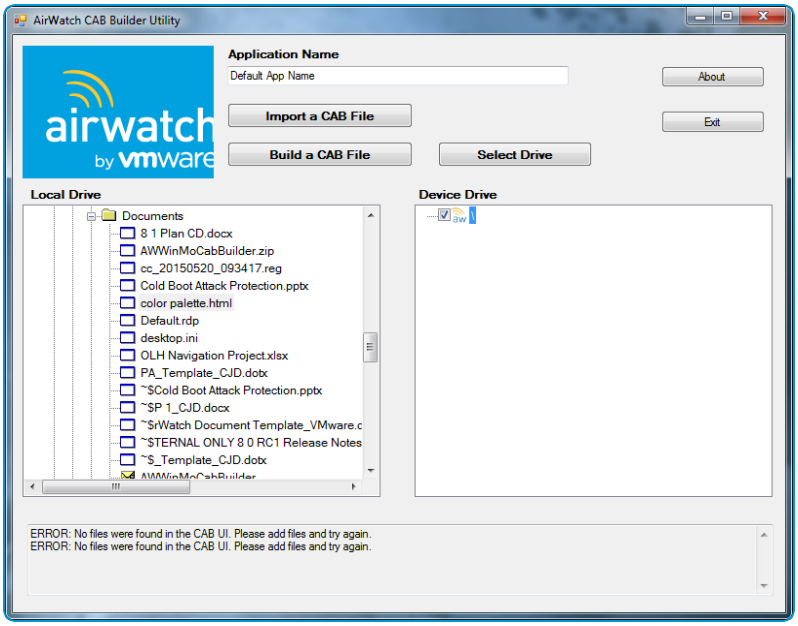
Requirements

To use the AirWatch Cab Creator for Windows Rugged, you must meet the following requirements:

- A Windows device running Windows 7+
- .NET Framework 4.5

To create a custom CAB file:

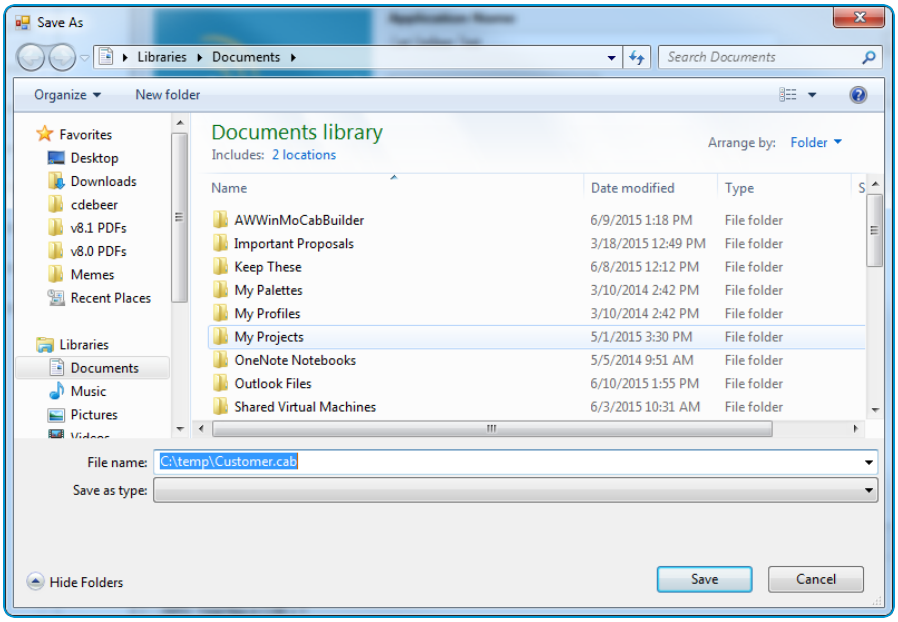
1. Download the "AirWatch Cab Creator" for Windows Rugged from the my Workspace ONE documentation repository.
2. Unzip the file to your preferred directory.
3. Double-click CabBuilder.exe to start the app.



4. Navigate to a file on your **Local Drive** you want to add to the custom CAB file. You can select a different drive by selecting **Select Drive**.
5. Enter an **Application Name**. This text box is the name of the CAB file after installation.

   Remember the name for use in Uninstall Manifest items.
6. Select the file and drag it to the **Device Drive** pane.

   To create a folder on the device drive, right-click the root drive and select **Add Folder**.
7. Repeat Step 5 for each file or application you want to add to the custom CAB file.
8. (Optional) Add an existing CAB file to your custom CAB file by selecting **Import a CAB File**.
9. Select **Build a CAB File** to save the CAB file and select a name for the file.



10. Select **Save** to create a custom CAB file.

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.

In addition, 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; if the product status is Compliant, then the product on the device matches the product provisioned. If file validation discovers a mismatch, the console pushes the content to the device again to ensure compliance between the product and the device. In this way, the product ensures that your devices remain up-to-date.

With the AirWatch Agent for Android v5.1+ or the AirWatch Agent for Windows Rugged v5.5+, interrupted products, known as orphaned products, automatically restarts and continues from where they were interrupted. This means that if a device shuts down or reboots for whatever reason during the middle of the processing of the product, the product automatically restarts.

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 57.

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 47.

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 39.

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 35.

Product Persistence

Product Provisioning allows you to enable profiles, files/actions, and applications to remain on a device following an enterprise reset. Content marked to persist following an enterprise reset reinstalls following the device restart after the agent installs. Product Persistence only applies to specific Windows Rugged and Android devices. For more information, see Product Persistence on page 38.

Create a Product

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

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

To create and configure a product.

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

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

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

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

Setting	Description
Add Rule	Select to create a rule for product provisioning. Displays the **Attribute/Application**, **Operator**, and **Value** drop-down menus.
Add Logical Operator	Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.
Attribute/Application	This is the custom attribute used to designate which devices receive the product. Custom attributes are created separately. For more information, see Custom Attributes on page 58.
Operator	This operator compares the **Attribute** to the **Value** to determine if the device qualifies for the product. **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.
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: • **Install Profile**. • **Uninstall Profile**. • **Install Files/Actions** – This option runs the Install Manifest. • **Uninstall Files/Actions** – This option runs the Uninstall Manifest. • **Warm Boot**. • **Cold Boot**.

Setting	Description
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.
Persistent through Enterprise Reset	Select whether you want the Profile to be **Persistent through enterprise reset** or not. For more information, see Product Persistence on page 38.

Note: Profiles and files/actions that were selected to persist through an Enterprise Reset are stored in the flash memory of the device upon install. Once a device initiates the restore process from an Enterprise Reset and installs the AirWatch Agent, any persisted files/actions will be restored after Profiles are installed even if they were previously uninstalled. For more information, see Product Persistence on page 38.

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.

Setting	Description
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.
Pause/Resume	Enable to ensure that an interrupted product provisioning due to Wi-Fi connectivity issues will be retried. 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.
Product Type	Determine if a product is **Required** or **Elective**. 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.

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 Persistence

Product Provisioning allows you to enable profiles, files/actions, and applications to remain on a device following an enterprise reset. Content marked to persist following an enterprise reset reinstalls following the device restart after the agent installs.

Product Persistence is ideal for help-desk type support as it allows the device to be wiped to clear away any problems without needing the device to be re-enrolled and products provisioned again.

Product Persistence for Windows Rugged only applies to Motorola, Honeywell, Psion, Pideon, and Intermec devices running Windows Mobile.

Persistence works as follows.

1. A device must contain a staging configuration so that the agent and enrollment reinstall following the enterprise reset.

   Staging configurations automatically persist on a device.
2. Set to persist any profiles, files/actions, or apps that you want to remain on the device after the enterprise reset.
3. The device resets when the Enterprise Reset command is sent (see Product Management). After resetting, the restore process starts.

4. The AirWatch Agent for the device reinstalls during the restore process.
5. After the agent is installed, any persisted profiles, such as Wi-Fi, reinstall.
6. Any persisted files/actions or apps are reinstalled.

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.

Settings	Description
Condition	The type of condition affects the parameters on the **Condition Details** tab. • **Adapter**. • **Adapter Time**. • **Battery Threshold***. • **Connectivity State***. • **Confirm**. • **File**. • **Memory Threshold***. • **Power**. • **Time**. * Condition is only available for use in Event Actions. For more information, see Event Actions on page 45.
Managed By	Select the organization group that manages the condition.

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

- **Adapter** – This condition type tests to see which, if any, **Network Adapters** are connected. This can be relevant if network connectivity is a scarce or expensive resource and certain operations should be limited to use over certain **Network Adapters** or prohibited from use over certain **Network Adapters**.

Settings	Descriptions
What would you like to do with the adapters?	Select to use the adapters you define or exclude them. ◦ Only use these adapters to connect. ◦ Exclude these adapters from connecting.
Adapter 1	Select to select an adapter from the list or enter the adapter by name. ◦ Select From List. ◦ Enter name.
Select adapter	Select the network adapter from the drop down list.
Specify Adapter	Enter the adapter name to use or exclude.
Adapter 2/Adapter 3	Select to use or exclude additional adapters.

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

Settings	Description
Specify scenario #1?	Set to **Specify this scenario** to begin configuring the condition scenario. Up to 5 scenarios may be entered, each with their own constraint choices. Each Scenario is an OR statement and each option inside a Scenario is an AND statement. For example, a device will check to see if Scenario #1 OR Scenario #2 is true. If Scenario #1 is true, it will check if all the constraints listed are true because they are AND statements.
Scenario description	Enter a description for the adapter time scenario.
Constrain Network Adapters?	Set to **Constrain based on the Best Connected Network Adapter** and configure the following. ◦ Specify any **Included or Excluded Network Adapters**. ◦ Choose to either **Select Network Adapter Class from a drop-down list** or **Type in a Network Adapter Name**. ◦ Up to five network adapters may be selected in the **Adapter selection method?** setting. ◦ For each adapter you want to include/exclude, choose between **Select a Network Adapter Class** drop-down list and entering a specific **Adapter name**. If you want to skip this kind of constraint, then select **Don't constrain based on the Best Connected Network Adapter**. Then you can proceed with defining another kind of constraint.
Constrain days of week?	For each day of the week, choose whether it will be included or excluded.
Constrain months?	For each month, choose whether it will be included or excluded.
Constrain days of month?	Enter a **Start day of month?** and an **End day of month?**.
Constrain years?	Enter a **Start year?** and an **Last year?**.
Constrain time of day?	Enter the **Start hour?**, **Start minute?**, **End hour?**, and **End minute?**.
Set frequency limit?	Ranges from **Every 15 Minutes** to **Every 1 Week**.

- **Battery Threshold** - This condition type tests the device to see what level battery charge remains. You can

test for charge levels *under* a defined threshold or *over* a defined threshold.

Settings	Description
Battery Level	Select between **Less than or Equal To**, **Greater Than or Equal To**, and **Between** to define a range of charge levels.
Battery Percentage	Enter a percentage between 1 and 100. When **Between** is selected, you must enter a range comprised of two percentage levels.

- **Connectivity State** - This condition tests the device for the type of connection and the length of time it has been connected.

Settings	Description
the device is connected to	Select between **Wi-Fi** and **Cellular**.
the device is continuously	Two selections must be made. First, select whether to test if the device has been Connected or Disconnected. Next, select the length of time it has been in such a state.

- **Confirm** – This condition type prompts the end user to determine whether or not the condition is met. This prompt is customizable so you can control what displays on the prompt.

Settings	Description
	Message to be displayed
First line prompt	Enter a header of the prompt
Second line prompt	Enter the body of the prompt.
Third line prompt	If you enable a countdown, you can enter a countdown phrase into this setting. For example, "You have %count% seconds to comply" where %count% is the countdown.
Allow users to cancel action (s)?	Select **Yes** if you want to give users a chance to opt out of the action upon which this condition is placed. Select **No** to obligate users to accept the action.

Settings	Description
	Delay
Delay (seconds)	Use this to delay for a specified time or until the end user makes a selection. If you enter a non-zero value, the prompt will wait for that value worth of seconds. Then if the end user does not make a selection in the time allowed, the condition is automatically considered not met. If a value of zero is entered, then the prompt displays indefinitely until the user makes a selection.
Enable countdown?	Select **Yes** to allow the delay time to be "counted" down on the device so the end user knows how much time is remaining to make a selection. Select **No** to hide the delay countdown.
	Defer Action
Defer time	This controls the minimum time after the condition is not met before the end user will be prompted again to determine the state of this condition. If a non-zero value is entered, the end user will not be prompted again for at least that number of seconds. If a value of zero is entered, then the end user could be prompted again as soon as the next execution of the Check-In command.
Maximum number of defers	This controls the maximum number of times the condition is not met. Once the condition has not been met this number of times, it will either be met or failed, depending on the setting of the next feature. If a value of zero is entered, then the condition will be met or failed on the first time.
Action after maximum defers	Select the action to trigger after the maximum number of defers is met. ○ **Fail Condition**. ○ **Display Cancel Button**. ○ **Pass Condition**.

- **Memory Threshold** - This condition type tests the device for available memory level.

Settings	Description
Available memory is less than	Enter a percentage of available memory such that your action only executes if the device has less than the indicated amount.

- **Power** – This condition type tests how a device is being powered, including whether the device is plugged in or has a suitably high battery level. Use a **Power** condition type to prompt users to place the device into the cradle or to insert a charged replacement battery.

If your testing needs are particular, the **Battery Threshold** condition offers more granular battery tests than Power offers.

Settings	Description
Message to be displayed	
First line prompt	Enter a header for the prompt.
Second line prompt	Enter the body of the prompt.
Third line prompt	If you enable a countdown, you can enter a countdown phrase into the **Third line prompt** field. For example, "You have %count% seconds to comply" where %count% will be the countdown clock.
Condition	
Required power level	Enter the required power level for the condition to test true. ◦ **A/C**. ◦ **A/C or Full Battery**.
Delay	
Delay (seconds)	Use this to delay for a specified time or until the end user makes a selection. If you enter a non-zero value, the prompt will wait for that value worth of seconds. If the end user does not make a selection in the time allowed, the condition is automatically considered not met. If a value of zero is entered, then the prompt will display indefinitely until the end user makes a selection.
Enable countdown?	This allows delay time to be “counted” down on the device so the end user knows how much time is remaining for the user to make a selection.

- **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.

Settings	Description
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.

Event Actions

Event actions allow you to take action on a device when predetermined conditions are met. The Event Actions wizard guides you through creating the conditions and actions together.

In cases where you want to perform a device action only when certain conditions are met, event actions allow you to control the timing of these actions. For example, your devices might need new files download to them but only until the device is not in use. A device event can wait until the device is connected to its charger before installing files. In another example, you can set a connectivity condition to wait for the device to connect to Wi-Fi before sending in a device check-in.

Event actions act as a device-based "if-this-then-that" configuration which controls the recurrence of actions on a device. A product only processes once on a device. Event actions, however, process any time the conditions are met.

Push event actions to devices as a component of a product.

Create an Event Action

You can create event actions that run on a device when certain conditions are met.

1. Navigate to **Devices > Staging & Provisioning > Components > Event Actions** and select the **Add Event Actions** button. The **Add Event Action** wizard displays.
2. Select your device platform. The available conditions and actions for the platform display. Select **Next**.
3. Complete the **Details** settings and select **Next** when complete.

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

4. Select a **Condition** to trigger the device action.

   You can select a previously created condition or create a new one. To create a condition, select **Create Condition** from the drop-down menu. Select **Next** when complete. For more information, see Create a Condition on page 39.

   You can select multiple conditions, but only one condition of each type can be selected.

   - **Adapter** – select which network adapters to allow/disallow.
   - **Battery Threshold** – select to take actions for specified battery limits.
   - **Connectivity** – select to take actions when connectivity requirements are met.
   - **Memory** – select to take actions when the available memory of the device is lower than a specific limit.
   - **Time** – Schedule your actions to take place on certain dates, days of the week, and within time-slots.

5. Select an **Action** to perform. The actions available depend on the device platform.

Action	Description
Copy Files	Copy files from one location to another on the device.
Create Folder	Create a folder on the device.
Delete Files	Delete folders from the device.
Device Check-In	Command the AirWatch Agent to check in with the Workspace ONE ™ UEM console for updates.
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: Windows Rugged: .reg, .cab, and .xml.
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.

Action	Description
Run	Run command lines and arguments on the device. If you want to install executable files (EXE), then you must use the Run manifest action on Windows Rugged devices. This is accomplished using command lines. The Run command must use the syntax of "\[full file path]". For example, \program files\program.exe.
Send Sample Data	Send the device data sample to the UEM console.
Terminate	End a process or application running on the device.
Uninstall	Uninstall a program or application on the device. You must enter the application name. **Note:** The Uninstall Manifest is for deleting files when a product is removed. If you remove a product from a device, any files installed remain on the device until uninstalled using an Uninstall Manifest.
Warm Boot	Restart the device.

6. Select **Update** to add the action to the event action. You can add additional actions to the event action. Select **Next**.
7. Review the **Summary** and select **Save**.

To push event actions to devices, add them as a component to a product. For more information, see Create a Product on page 35.

Files/Actions for Products

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

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

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

Create a Files/Actions Component

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

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

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

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

3. Complete the **General** text boxes.

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

4. Select the **Files** tab.
5. Select **Add Files**. The **Add Files** window displays.
6. Select **Choose Files** to browse for a file or multiple files to upload.

   Windows Rugged devices can use the files/actions option to install XML onto a device. For more information, see Create an XML Provisioning File on page 50.
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. Windows Rugged devices can enable **Relay Server Only** to ensure that the device only receives the files/actions from a Relay Server and not from other sources. This option applies to Windows Rugged devices only.
11. Select **Save**. You can repeat the previous steps for as many files as you want.
12. Select the **Manifest** tab. Actions are not required if you have at least one file uploaded.
13. 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
AirWatch Agent Upgrade	Install the new AirWatch Agent to the device. Before using this file/action, see Upload the AirWatch Agent APF File on page 51 for more information.
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.

Settings	Descriptions
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. • Windows Rugged: REG, CAB, and XML. Workspace ONE UEM recommends using the Workspace ONE UEM CAB Creator to create CAB files that combine multiple files into one CAB file.
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.
Uninstall	Uninstall a program or application on the device. You must enter the application name. **Note:** The Uninstall Manifest is for deleting files when a product is removed. If you remove a product from a device, any files installed remain on the device until uninstalled using an Uninstall Manifest.
Warm Boot	Restart the device.

14. 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.

Import Packages in Files/Actions

AirWatch allows you to import MSP (Motorola Services Platform) packages. The packages import and unpack into proper files/actions for use in products.

To import an MSP package, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions** and select **Add**.
2. Select the Platform you want to create a staging configuration for.
3. Select **Import Package**.
4. Select **Upload** to add an APF file.

   Once the file is uploaded, the required text boxes are auto-completed.
5. Select **Save**.

Create an XML Provisioning File

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

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

10. Select **Install Files/Actions** and select the files and actions just created.
11. **Save** and **Activate** the product.

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

XML Provisioning is for Windows Mobile devices only and not Windows CE.

AirWatch Agent Upgrade File/Action

When you upgrade your devices, you can seed the AirWatch Agent in the Workspace ONE ™ UEM console for use in products. The file/action AirWatch Agent Upgrade then grabs the list of seeded APF files when creating a manifest action for products.

Use this option to enroll devices with older agent versions installed. You can enroll the devices then upgrade the device to the new agent version you want to use.

When using this upgrade option, be alert for failed upgrades. A failed upgrade can cause the product to push repeatedly as the console recognizes the older agent version. This can cause additional strain on the network and much greater battery consumption on the device. If the upgrade fails, deactivate the product and look over the configuration to ensure that the settings are correct.

Note: The Agent Packages screen is only accessible in Customer type organization groups.

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.

Windows Rugged OS Upgrade Process

You can Upgrade your Motorola and Zebra Windows Rugged devices remotely to a new version of the OS using product provisioning. This process allows you to keep your entire device fleet up-to-date without needing to have the devices shipped back to you.

All OS upgrade files are restricted access files and require a valid user account with Motorola to log in with a valid device serial number. The OS upgrade files are specific to both device model and OS version. The Workspace ONE ™ UEM OS upgrade process uses the APF files and requires the administrator to first install the MSP Package Builder utility.

This utility is required to extract the contents of the APF file into individual components that are then pushed to the device and used to upgrade the OS.

Important: The Windows Rugged OS Upgrade method requires the AirWatch Agent v5.3+ for Windows Rugged devices.

Upgrade a Windows Rugged Device

Using the Windows OS Upgrade file/action, upgrade your Motorola and Zebra Windows Rugged devices remotely. By creating a product containing the OS Upgrade file/action, you can upgrade all your devices without having them shipped back to you.

Prerequisites

To use the Windows Rugged OS Upgrade, you must have the following:

- The MSP Package Builder utility installed on your computer.
- A Motorola user account to download the OS Upgrade.
- The serial number for the device you want to upgrade.
- The OS update utility, included with the extracted APF files.
  This file can be downloaded from the Zebra support website.
- A relay server configured to deliver the product to the device.

To upgrade your Windows Rugged devices using Windows OS Upgrade:

1. Extract the Required OS Update Files on page 52
2. Create an OS Upgrade File/Action on page 53.
3. Create a Product on page 35.

Extract the Required OS Update Files

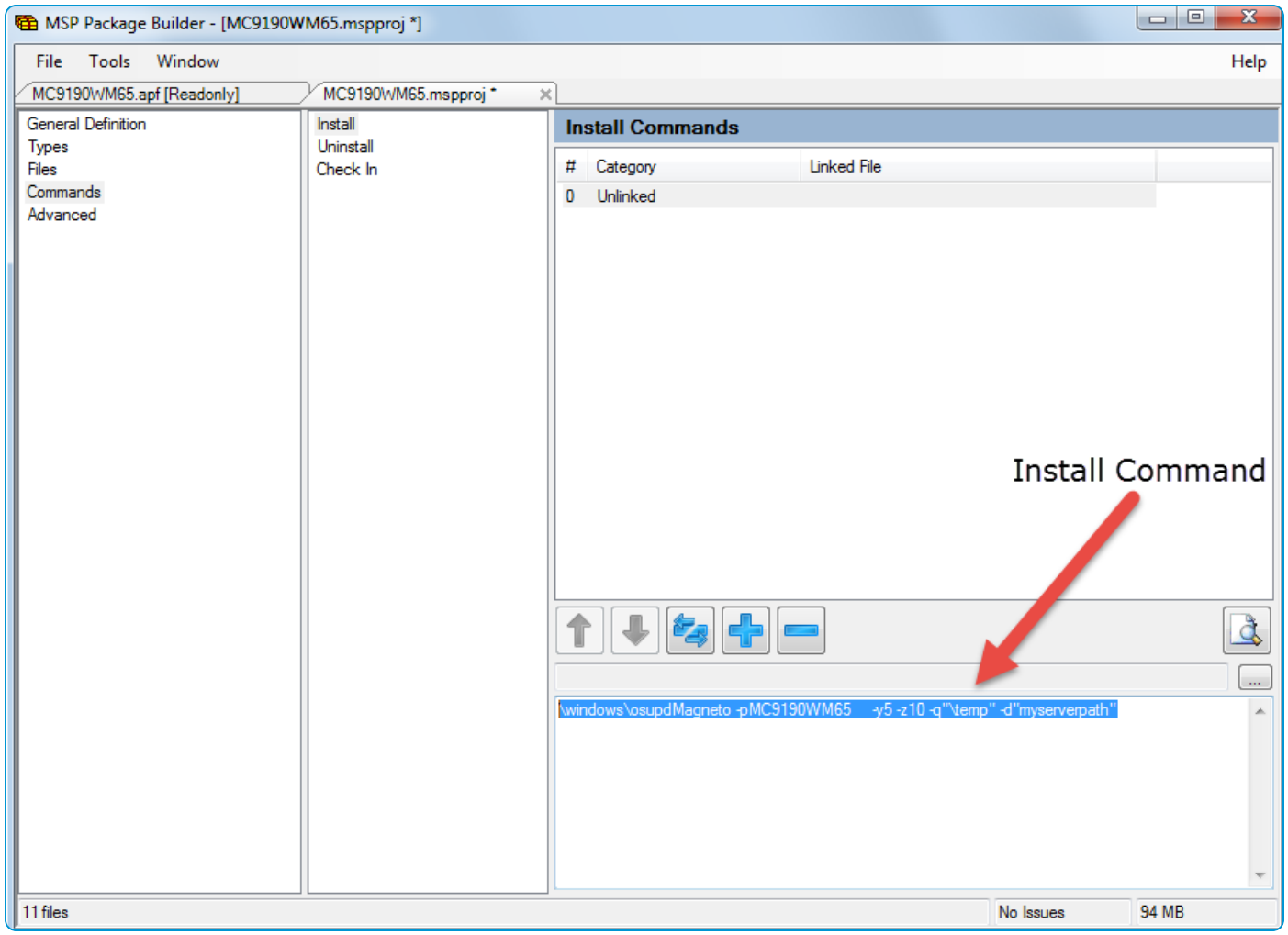
Before you can create an OS Upgrade file/action, you must extract the required files from the APF files. These files are extracted using the MSP Package Builder Utility.

To extract the OS update files:

1. Start the MSP Package Builder Utility.
2. Navigate to **File > Open Project** and select the appropriate APF file and open it in MSP Package Builder.
3. Navigate to **Tools > Convert Project** to open the **Convert to Project** dialog box.

4. Complete the following text boxes:
   - **Name** – Enter the name for the OS Upgrade project.
   - **Extract FilesTo** – Enter the location the files should be saved to or select the Browse button to select the location.
5. Select **OK** to close the Convert to Project dialog box.
6. Select **Command** from the left window pane.
7. Select **Install** and copy the install command from the bottom right window pane.

   You might want to paste and save this install command to a file (Notepad, Word, and so on) so you can access this command while creating the File/Action for the OS Upgrade.



Create an OS Upgrade File/Action

Once you extract the OS upgrade files from the APF file, create an OS Upgrade file/action.

If you must update the device registry, create a separate files/actions for the Registry Edit file and list that Files/Action first in the product manifest.

To create a product for OS Upgrade:

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions** and select the **Add Files/Actions** button.
2. Select the **Windows Rugged** platform.
3. Complete the **General** text boxes.
4. Select the **Files** tab and select **Add Files**.
5. Select **Choose Files** and upload the extracted OS update files.
6. Specify the **Download Path** as:

```
\[directory]\[full file name]
```

7. Enable **Relay Server Only** to ensure that the files are all successfully downloaded and processed on the device. Large image files that are part of the OS Update remain on the Relay Server until needed by the OSUpdate utility.
8. Select **Add** to add additional files.
9. Upload the OS Update Utility EXE and the "package.TXT" manifest file.

   Windows Mobile devices always use a file named "osupdMagneto.exe." For Windows CE devices, the filename varies with the device.

   Windows CE devices also require a package .APD. The contents of this file are not important and can be a simple text format file containing something benign. It can even be empty.
10. Specify the separate **Download Paths** for both the OS Update Utility and the package .TXT manifest file.

    The **Download Path** for the OS Update utility and the package.TXT manifest file must be: "\Windows\".

    The Windows CE .APD file must be placed in: "\Application\AirBeam\PKG."

    Important: Do not select **Relay Server Only**. These files need to be delivered directly to the device.
11. (Optional) Create a files/actions to download and install the REG file to the device.

    This step is only necessary if the registry settings are not already correctly updated on the device.

    Download the REG file to the '\Temp' directory specifying the full filename. On the manifest tab, add an **Install** action type and specify the directory location and the filename of the REG file to be run on the device.
12. Once all the files have been uploaded, select the **Manifest** tab and select **Add Action** to add **Install Actions**.
13. Select the **Run** action in the **Action Types** text box.
14. Copy the Install Command from the MSP Package Builder utility and paste it into the **Command Line and Arguments to Run**.

    For more information, see Create an OS Upgrade File/Action on page 53.

    You must edit the syntax of the Install Command to match Workspace ONE ™ UEM run syntax:

- Windows Mobile
  - You must use double quotes around "\windows\osupdMagento" and add the .exe to the end of osupdMagento.
  - -d"myserverpath" must be updated in the following format: "[path of your relay server]/PFILES/[file action name]_version/". So if the directory on the relay server that you are using for OS Update is /Motorola/OSUpdateFiles, the name of the OS Update file/action is "OSUpdate" and the "OSUpdate" file/action is on version 5, then the -d argument might look like: -d"/Motorola/OSUpdateFiles/PFILES/OSUpdate_5/".
    - The full run command syntax with all the arguments looks similar to this:

      "\windows\osupdMagneto.exe" -p"MC9190WM65" -o -y5 -z10 -q"\temp\" -d"/Motorola/OSUpdateFiles/PFILES/OSUpdate_5/"

- Windows CE
  - You must use double quotes around "\windows\ [OS Update Utility filename]" and add the .exe to the end of the filename.
  - -d"myserverpath" must be updated in the following format: "[path of your relay server]/PFILES/[file action name]_version/". So if the directory on the relay server that you are using for OS Update is /Motorola/OSUpdateFiles, the name of the OS Update file/action is "OSUpdate" and the "OSUpdate" file/action is on version 5, then the -d argument might look like: -d"/Motorola/OSUpdateFiles/PFILES/OSUpdate_5/".
    - The full run command syntax with all the arguments looks similar to this:

      "\windows\[OS Update filename].exe" -p"WT41N0" -o -y5 -z10 -d"/Motorola/OSUpdateFiles/PFILES/OSUpdate_5/"

15. Select **Save**.
16. Add the OS Upgrade file/action to a product and assign the product to all applicable devices.

Once the device receives the product, the OS Update process initiates. A notification screen displays when the upgrade is complete.

Windows Rugged OS Upgrade Resources

The Windows Rugged OS Upgrade file/action might require Run command arguments to process the action on the device. You can also change the device registry settings.

Check Device Registry Settings

If at any point an error occurs, check the device registry settings. The 5.x agent has been designed to update these settings based on the Workspace ONE ™ UEM console configuration settings. The relay server settings are a part of the job XML and are applied during provisioning just before processing the job.

If the OS Update process does not complete successfully, the following settings are checked as part as any troubleshooting effort.

HKEY_LOCAL_MACHINE\SOFTWARE\AIRBEAM\	
IGNORESERVER	string “1”

HKEY_LOCAL_MACHINE\SOFTWARE\AIRBEAM\	
SERVERRIP	string [Enter the Server URL or IP Address]
FTPUSER	string [Enter the FTP (s) username]
FTPPASSWORD	string [Enter the FTP (s) password] - THIS FIELD MUST BE ENCRYPTED
TFTP	string "0"
PASSIVEMODE	string "1"
FTPPORT	string "21"
FTPS	string "0" or "1"
VERIFYSERVER	string "0"
SOFTKEY1	number "123"
SOFTKEY2	number "124"
ENTERKEY	number "13"

Run Command Argument Information

-d option describes the Workspace ONE UEM relay server folder path containing files required to update the device. It uses the following format (with forward slashes and double quotes): "[path of your relay server]/PFILES/[file action name]_version/"

-y option describes the maximum number of retry attempts while the –z option describes the retry delay.

-q is the folder on the device that is used to download the files from the FTP server when updating Windows Mobile. This location is typically “\Temp” or “\Storage Card”. In CE updates, the files are downloaded one at a time into memory so the parameter is not used in that case.

-p is the OSUpdate project name. The project name can be whatever the user wants it to be but is usually something to indicate what the update package contains. This name should be the same as the Motorola APF file. The project (APF) should be named in such a way as to be able to identify the target device, OS type, and so forth.

For the Workspace ONE UEM process, this name will be the same as whatever you call the dummy APD file (which can be an empty text file).

- If your command line contained –p”WT41N0”, you need to have a WT41N0.apd file put down to the device prior to doing the update. This is only needed for CE devices.
- For Windows Mobile devices –p”MC9190WM65” is required by the command line parsing, but in effect will not be used.

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.

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 58.

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 59.

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

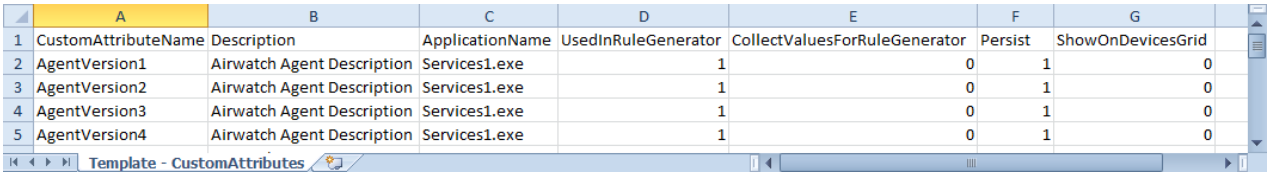
The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters.

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

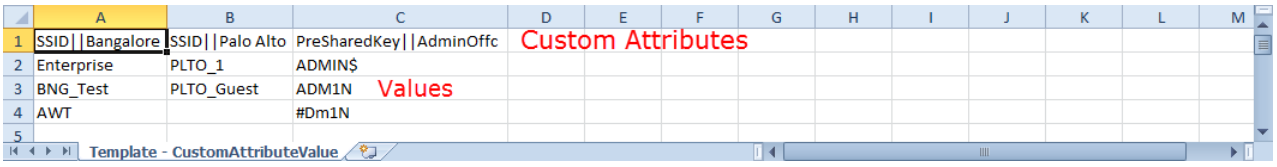
- Custom Attributes Template – Allows you to define a custom attribute and its settings.



	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	0
3	AgentVersion2	Airwatch Agent Description	Services1.exe	1	0	1	0
4	AgentVersion3	Airwatch Agent Description	Services1.exe	1	0	1	0
5	AgentVersion4	Airwatch Agent Description	Services1.exe	1	0	1	0

Template - CustomAttributes

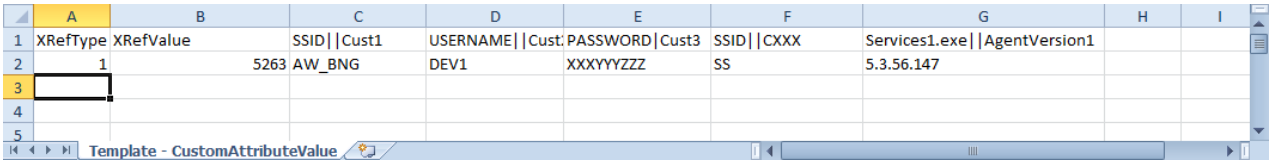
- Custom Attribute Values Template – Allows you to define the values of predefined custom attributes.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	SSID||Bangalore	SSID||Palo Alto	PreSharedKey||AdminOffc										
2	Enterprise	PLTO_1	ADMIN$										
3	BNG_Test	PLTO_Guest	ADM1N										
4	AWT		#Dm1N										
5													

Template - CustomAttributeValue

- 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	XXXYYYZZZ	SS	5.3.56.147		
3									
4									
5									

Template - CustomAttributeValue

1. DeviceID (Workspace ONE ™ UEM assigned DeviceID when the device enrolls)
2. Serial Number
3. 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 58 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	This operator compares the **Attribute** to the **Value** to determine if the device qualifies for the product. When using more than one Operator in a rule, you must include a **Logical Operator** between each **Operator**. **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.
Value	All values from all applicable devices are listed here for the **Attribute** selected for the rule.
Add Logical Operator	Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.

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

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

Windows Rugged Custom Attributes

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

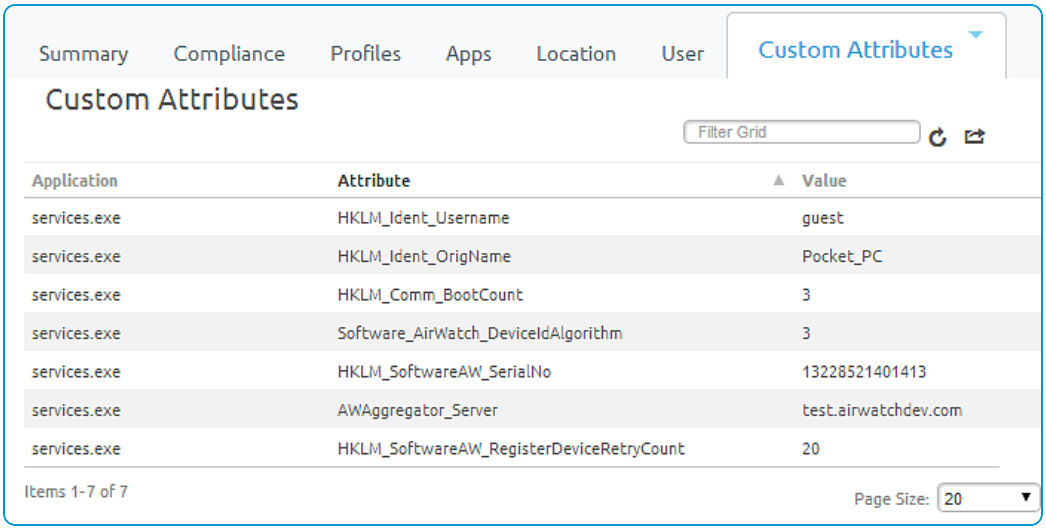
Implementation

To begin collecting custom attributes, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions**, then select the **Add Files/Actions** button, and then select **Windows Rugged** as your platform.
2. Create an XML product. For more information, see Create an XML Provisioning File on page 50. The manifest includes an action to download the XML file to **\Program Files\Airwatch\Cache\Profiles**.

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

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



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

Syncing Registry Settings

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

```
<?xml version="1.0"?>
-<wap-provisioningdoc allowRemoval="True" name="GetTypicalRegValues/V_1" id="5a63204f-848c-42d5-9c14-4ca070743920">
    -<characteristic uuid="f49a9cb5-48e9-47cd-84cc-ef122dcb5d50" type="com.airwatch.getregistryinfo.winmo">
        <reg_value value_name="Username" key_name="HKEY_LOCAL_MACHINE\Ident" custom_attribute_name="HKLM_Ident_Username"/>
        <reg_value value_name="OrigName" key_name="HKEY_LOCAL_MACHINE\Ident" custom_attribute_name="HKLM_Ident_OrigName"/>
        <reg_value value_name="BootCount" key_name="HKEY_LOCAL_MACHINE\Comm" custom_attribute_name="HKLM_Comm_
BootCount"/>
        <reg_value value_name="DeviceIdAlgorithm" key_name="HKEY_LOCAL_MACHINE\Software\AirWatch" custom_attribute_
name="Software_AirWatch_DeviceIdAlgorithm"/>
    </characteristic>
</wap-provisioningdoc>
```

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

Using Third-Party Applications to Create Custom Attributes

If you want to create custom attributes using a third-party application, you need that application to export an XML file with a key value pair to the **Program Files\AirWatch\Cache\CustomAttributes** directory on the device. Once an XML file with a key value pair is present in this directory, it is parsed by the agent and included in the next interrogator sample. The XML key/value pair must be in the following format.

```
<?xml version="1.0"?>
-<attributes>
    <attribute name="HKLM_Ident_Username" value="guest"/>
    <attribute name="HKLM_Ident_OrigName" value="Pocket_PC"/>
    <attribute name="HKLM_Comm_BootCount" value="1"/>
    <attribute name="Software_AirWatch_DeviceIdAlgorithm" value="3"/>
    <attribute name="HKLM_SoftwareAW_SerialNo" value="13233521403231"/>
</attributes>
```

'Attribute name' is the name of the attribute in the console while 'value' is the corresponding value that is associated with that attribute.

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 64.

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 64.

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 35 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 65.
- Add a Product to a Product Set on page 65.
- Change the Product Ranking in a Product Set on page 66.
- Removing Products from Product Sets on page 66.

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 66 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	Increasing the rank (selecting **Up** arrow) of a product decreases the rank of all subsequent products by one. Decreasing the rank (selecting **Down** arrow) of a product increases the rank of previously lower-ranked products. 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. 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. 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.
Removing a Product	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. All products that preceded the deleted product's rank remain unchanged. Any products that had the removed product installed receives a new product based on the new rankings.

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 66 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 69.

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 71.

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 72.

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 are in the process. For more information, see Product Job Statuses on page 73.

Enterprise Reset

Enterprise Reset enables you to reset a device similar to an enterprise wipe, but with one important difference. Profiles and files/actions set to persist on a device are not removed and automatically reinstall on a device following the first reboot after an enterprise reset. For more information, see Perform an Enterprise Reset on page 75.

XML Provisioning

XML provisioning allows you to download a custom-designed XML file to a device in a provisioning product. After the file is downloaded, it runs an install command to extract the settings from the XML file and install them on the device. For more information, see Create an XML Provisioning File on page 50.

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. The product also passes a file hash validation, ensuring the product on the device is the exact same product provisioned by the console or API call.
- In Progress – The product has been sent to the device and is pending a compliance check based on inventory and file hash data to be received from the device.
- 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.

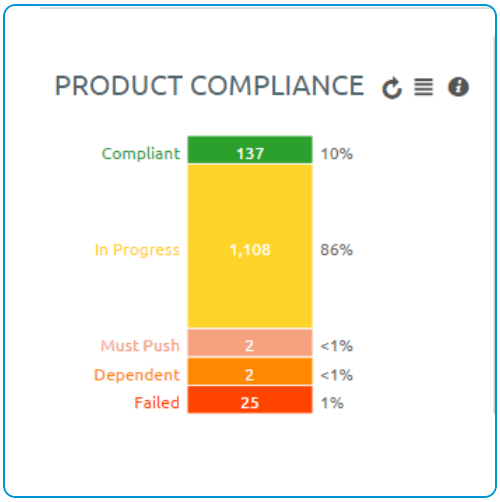
Filters

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.



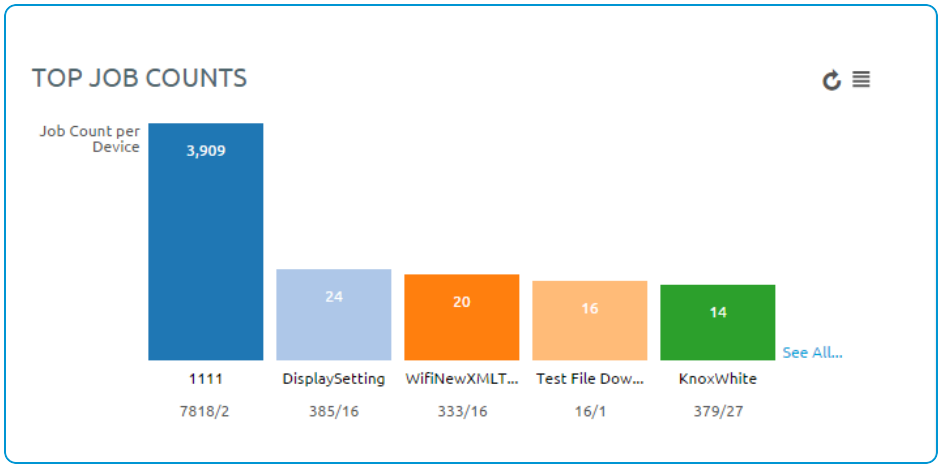
Filters

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

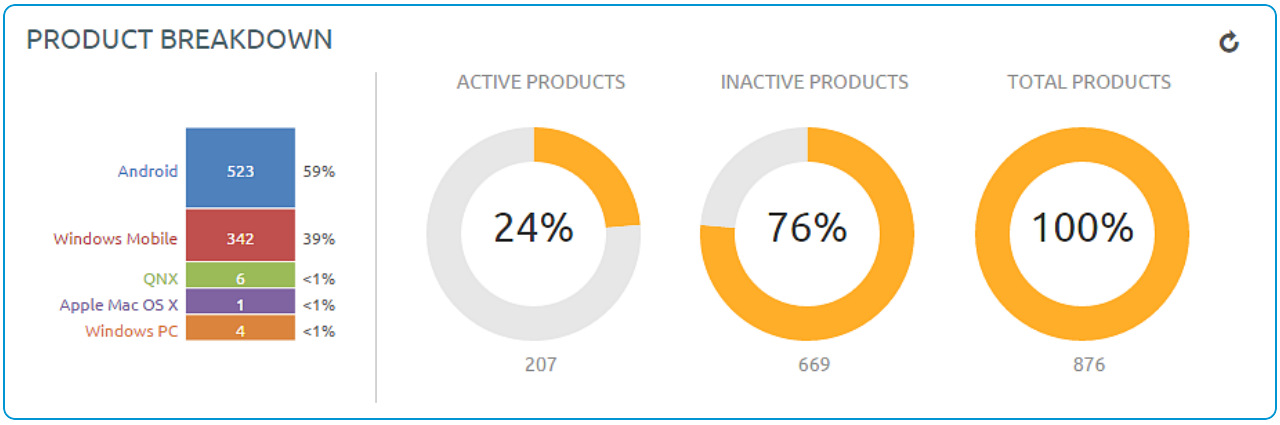
You can filter the Total Job Compliance chart to refer to specific device platforms that support product provisioning.

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.

Job Log Detail Level

You can set the amount of detail captured in the Job Log by navigating to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Rugged > Agent Settings** then scroll down to the **Product Provisioning** section and select the **Job Log Level** you prefer.

You can also Target a Device Log Level for Troubleshooting Purposes on page 73.

Target a Device Log Level for Troubleshooting Purposes

You can target an individual device and temporarily change its logging level for troubleshooting purposes.

1. Navigate to **Devices > List View**, locate the device you want to troubleshoot and select the device friendly name to display the **Device Details**.
2. Click the **More** tab and select **Targeted Logging**.
3. Select **Create New Log** and select the length of time you want the log to capture data.
4. Select **Start** to begin the logging.

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.

Next, you can target an individual device for troubleshooting purposes. See Target a Device Log Level for Troubleshooting Purposes on page 73.

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.

Perform an Enterprise Reset

Enterprise Reset enables you to reset a device similar to an enterprise wipe, but with one important difference. Profiles and files/actions set to persist on a device are not removed and automatically reinstall on a device following the first reboot after an enterprise reset.

To perform an Enterprise Reset, take the following steps.

1. Navigate to **Devices > List View** and select a device you want to Enterprise Reset.
2. On the Device Details View, select the **More Actions** button.
3. Select **Enterprise Reset**, located under Management section.
4. Enter your **Security Pin** in the **Restrict Action** prompt to perform the Enterprise Reset.

Chapter 6:
Device Dashboard

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

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

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

Device List View

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

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

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

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

Customize Device List View Layout

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

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

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

Search in Device List View

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

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

Windows Rugged Device Details Page

Use the Device Details page to track detailed device information and quickly access user and device management actions.

You can access Device Details by selecting a device Friendly Name from the Device List View, using one of the Dashboards, or with any of the search tools.

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

Remote Actions

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

The actions vary depending on factors such as the device platform, 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.
- **AirWatch Agent (Query)** – Send a query command to the device's AirWatch Agent to ensure it has been installed and is functioning normally.
- **App Remote View** – Take a series of screenshots of an installed application and send them to the Remote View screen in the UEM console. You may choose the number of screenshots and the length of the gap, in seconds, between the screenshots.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed apps.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **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.
- **Clear Passcode (Device)** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM console.
- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.

- **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.
- **File Manager** – Launch a File Manager within the UEM console that enables you to remotely view a device's content, add folders, conduct searches and upload files.
- **Provision Now** – Provision products to a device. Provisioning is the ability to create an ordered installation of files, actions, profiles and applications into a single product that can be pushed to devices.
- **Query All** – Send a query command to the device to return a list of installed apps (including AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Registry Manager** – Launch a Registry Manager within the UEM console that enables you to remotely view a device's OS registry, add keys, conduct searches and add properties.
- **Remote Control** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshooting on the device.
- **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.
- **Request Device Check-In** – Request that the selected device check itself in to the UEM console. This action updates the **Last Seen** column status.
- **Restart AirWatch Agent** – Restart the AirWatch Agent. To be used during troubleshooting for when the enrollment process or submodule installation process is interrupted.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.
- **Start/Stop AWCM** – Start/Stop the Cloud Messaging service for the selected device. VMware AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Admin Console by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs.
- **Task Manager** – Launch a Task Manager within the UEM console that enables you to remotely view a device's currently-running tasks, including task **Name**, **Process ID** and applicable **Actions** you may take.
- **View Manifest** – View the device's **Package Manifest** in XML format from the UEM console. The manifest on Windows Rugged devices lists metadata for widgets and apps.
- **Warm Boot** – Initiate a restart of the operating system without performing a power-on self-test (POST).

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.