Product Provisioning for Android

VMware Workspace ONE UEM 1903

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

Introduction to Product Provisioning for Android Rugged

1

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 Workspace ONE Intelligent Hub, 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 Android devices. For more information on general MDM functionality for Android devices, see the **Android 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.

Android Legacy

- Android Legacy devices running Android 4.1 (Jelly Bean) and later with Workspace ONE Intelligent Hub.
  - Zebra devices running Android 4.4 (Kit Kat) and later.

Android Enterprise

- Android Enterprise Work Managed devices running Workspace ONE Intelligent Hub.

Relay Servers 2

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.

This chapter includes the following topics:

Configure a Relay Server

Configure a relay server by configuring an FTP, Explicit FTPS, Implicit FTPS (Pull only), 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.

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).

Prerequisites

- An FTP, Explicit FTPS, Implicit FTPS (Pull only), 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 > 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
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.
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.
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 Hub installed on it.
Protocol	This is the information the device uses to authenticate with the FTP(s) server when downloading apps and content. **FTP**, **Explicit FTPS**, **Implicit FTPS (pull only)**, 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.

Setting	Description
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.
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.

a Press the **Test Connection** button to test your Console Connection to the push server.

Each step of the connection is tested and the results are displayed to help with troubleshooting connection issues.

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

4 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.

5 Select **Save**.

Batch Import Relay Servers

The Relay Server Import feature loads relay servers into the system in bulk. This is helpful if you have several relay servers to add. The **Batch Import** screen serves two purposes, 1) download a blank relay server batch file template and 2) import a completed relay server batch file.

Download a blank relay server batch file template and fill it out by taking the following steps.

Procedure

1 Select the Download template link and save the template to your device.

2 Open the template with Excel.

The template features two sample entries. These entries allow you to see what kinds of values and their formats the system expects to find in each field (or column) when you import your completed template.

3 You must associate the relay server users with an organization group (GroupID).

   The columns that feature an asterisk are required.

4 Remove the sample entries before you save your completed template.

5 Save the template in CSV format.

What to do next

For more information about importing a completed relay server batch file, see Bulk Import Relay Servers

Bulk Import Relay Servers

Procedure

1 Navigate to **Devices > Provisioning > Relay Servers > List View**. Select the **Add** button and then select **Batch Import**.

2 Enter a **Batch Name**.

3 Enter a **Batch Description**.

4 Select **Choose File** to upload the completed **Batch File**.

   Batch files must be in CSV format.

5 Select **Import** 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.

The server creates an outbound https connection on port 443 to the UEM console and periodically polls for changes or additions. If the server finds changes or additions, then it downloads the new content onto 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.

Note The IP configured in the pull connection / pull discovery must be an internal IP address for the server. The service does not configure correctly if an external IP or NAT IP address is used.

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 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 pull relay server requires outbound network access on https 443 to the Workspace ONE UEM console
- 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.

Procedure

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 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 > 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 for more details.

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

   a. WindowsPullServiceInstaller.exe /s /v"/qn/"

   b. 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, Implicit 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 pull relay server requires outbound network access on https 443 to the Workspace ONE UEM console
- 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.

Procedure

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. Note the home directory of the user for use in configuring the pull service.

   This FTP user must have a user name and password for authentication.

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.

`cn274.awmdm.com`

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

5 In the command prompt, enter the command.

```
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.

a If you want to use a proxy server, supply the host, port, and authentication information when prompted.

7 Navigate to **Devices > 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 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.

Procedure

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 > 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

You can view files sent to a relay server for distribution to devices through the Remote File Viewer.

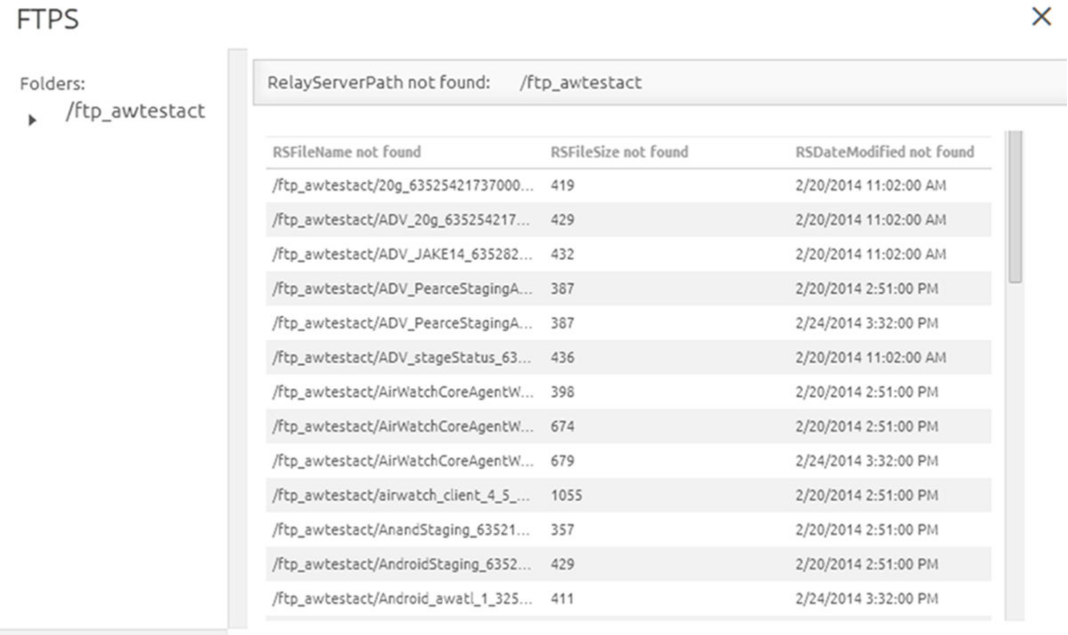
Procedure

1 Navigate to **Devices > 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.



RelaySeverPath not found: /ftp_awtestact

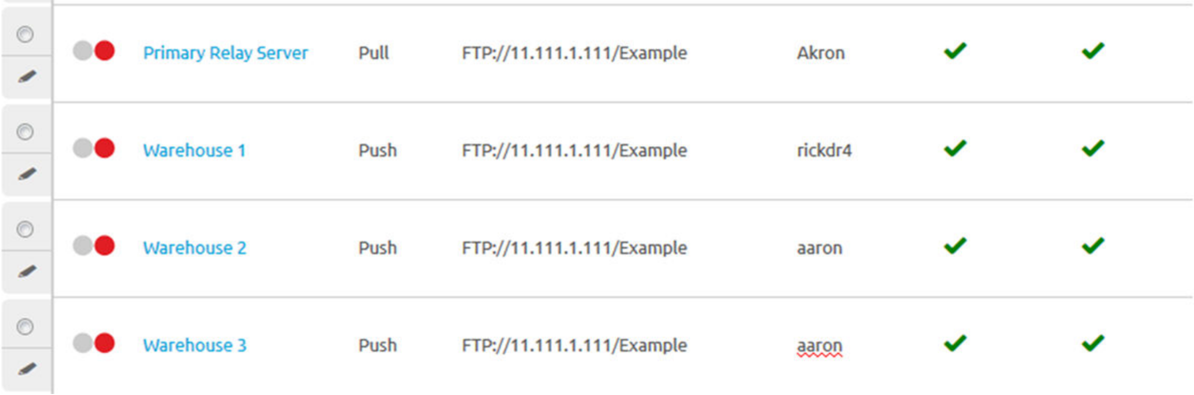
RSFileName not found	RSFileSize not found	RSDateModified not found
/ftp_awtestact/20g_63525421737000...	419	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_20g_635254217...	429	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_JAKE14_635282...	432	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_PearceStagingA...	387	2/20/2014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

Relay Server Management

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

Relay Server Status

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



●●	Primary Relay Server	Pull	FTP://11.111.1.111/Example	Akron	✓	✓
●●	Warehouse 1	Push	FTP://11.111.1.111/Example	rickdr4	✓	✓
●●	Warehouse 2	Push	FTP://11.111.1.111/Example	aaron	✓	✓
●●	Warehouse 3	Push	FTP://11.111.1.111/Example	aaron	✓	✓

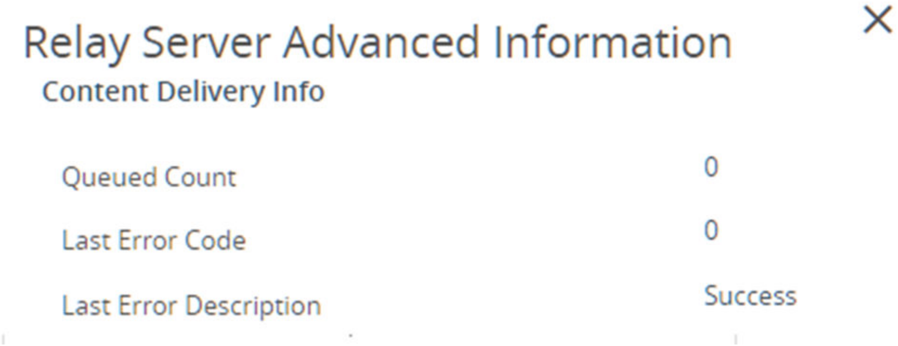
The **Source Server** and **Relay Server** statuses are as follows:

Settings	Descriptions	
Indicator	**Source Server**	**Relay Server**
✓	Last retrieval from server succeeded.	Last file sync with server succeeded.
•••	Retrieval from server in progress.	File sync with server in progress.
⚠	Last retrieval failed.	Last file sync failed.

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

Advanced Info

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



Relay Server Advanced Information

Content Delivery Info

Queued Count 0

Last Error Code 0

Last Error Description Success

Device Staging

3

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 Workspace ONE Intelligent Hub, 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. 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.

For more information on the Stage Now client for Android devices, see Zebra Stage Now.

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.

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 or sideload staging. For more information, see Create a Manual Staging Package.

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.

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 Workspace ONE Intelligent Hub and enroll. For more information, see Create a Wi-Fi Profile for Staging.

QR Code Staging

You can create a QR Code to scan to begin the auto-enrollment process for your Android 7.0 or later Work Managed devices. These codes simplify staging devices into a quick scan of a QR Code to configure the device using a created staging package. For more information, see Generate a QR Code Using the Enrollment Configuration Wizard.

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.

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.

This chapter includes the following topics:

- Zebra Stage Now
- Use the Enrollment Configuration Wizard
- Create a Manual Staging Package
- Configure Advanced Staging
- Create a Wi-Fi Profile for Staging
- Barcode Staging
- Sideload Staging Packages
- Android Device Enrollment with the Workspace ONE Intelligent Hub

Zebra Stage Now

The Stage Now staging client is Zebra's next generation Android solution for staging Zebra devices and preparing them for production use.

Workspace ONE UEM supports Stage Now given the following conditions and limitations.

For more information on Zebra Mobility, see Zebra Mobility Extensions (MX) and Full MX Feature Matrix.

If you plan to enroll Zebra devices in Work Managed Device Mode with a Stage Now barcode, take the following steps.

Prerequisites

- Zebra devices must be running Android Nougat with MX version 7.1 or later.
- If you want to enroll your Zebra devices using a Stage Now barcode, you must have Android Hub version 8.2 or later uploaded to the console as the Workspace ONE Intelligent Hub Package.
- Zebra devices running Android Marshmallow and below must continue to use Rapid Deployment as the default staging client.
- Relay Servers set to passive mode only are supported. Relay servers in active mode are not supported and do not function with the Stage Now client.
- Ensure the **Stage Now URL** setting, found in **Groups & Settings > All Settings > System > Advanced > Site URLs**, is set to the appropriate URL.
  - If your on premises environment is configuring your own Stage Now server, then place your custom URL in this field.
  - If your on premises environment is not configuring your own Stage Now server, then you simply must open your networks to allow access to the URL listed here.
  - SaaS environments do not need to change this text box.
- There must be no Google account present on the device while attempting Stage Now enrollment in Work Managed Mode.

Procedure

1. Use the Organization Group selector to select the OG you want to configure for your Android devices.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration** and select the **Enrollment Restrictions** tab.

3 Complete the following settings.

Setting	Description
Current Setting	Select **Override** to affect changes to the OG you selected in step 1.
Define devices that will use Android (Legacy) in this organization group	This setting determines how this OG treats Android (Legacy) devices. Select from among the following settings. **Don't use Android (Legacy)** – This setting enables the **Device Owner Mode** slider on the **Generate Stage Now Barcode** screen and makes it uneditable. This forces all Android (Legacy) devices that enroll in this OG to be in Device Owner Mode (or Work Managed Device Mode). **Always use Android (Legacy)** – This setting disables the **Device Owner Mode** slider from the **Generate Stage Now Barcode** screen and makes it uneditable. This forces all Android (Legacy) devices that enroll in this OG to be in Device Admin Mode. **Exempt smart groups from Android (Legacy)** – This setting enables the **Device Owner Mode** slider on the **Generate Stage Now Barcode** screen and makes it editable, allowing you the choice of enrolling Android devices in Device Owner Mode (Work Managed Device Mode) or enrolling them in Device Admin Mode.

4 Direct your end-user to take the following steps once they take possession of the newly-enrolled device.

   a Start the device from a "factory settings" state.

   b Ensure there is no Google account on the device.

   c Proceed through the Setup Wizard or scan the "skip setup wizard" barcode provided by Zebra.

   d Open the Stage Now app.

   e Scan the barcode.

   The device is automatically enrolled into Work Managed mode.

What to do next

You can optionally continue to the next step of making a Stage Now barcode by proceeding to the next step, Generate a Barcode Staging Package Using the Enrollment Configuration Wizard.

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.

Procedure

1 Navigate to **Devices > Lifecycle > Staging** and select the **Configure Enrollment** button.

2 Select the device platform you want.

3 Select the staging enrollment type.

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

- Generate a QR Code Using the Enrollment Configuration Wizard – Create a QR Code to scan with your Android Work Managed devices to quickly stage the device. The wizard simplifies the configuration process.
- Generate a Barcode Staging Package Using the Enrollment Configuration Wizard – Create a barcode to scan with your Zebra rugged devices to quickly stage the device. The wizard simplifies the barcode configuration process.
- Generate a Sideload Staging Package Using the Enrollment Configuration Wizard – Create a sideload staging package to download and install onto a device to automatically configure and enroll the rugged device.

4 Select **Configure**.

Generate a QR Code Using the Enrollment Configuration Wizard

After selecting QR Code enrollment in the Enrollment Configuration wizard, create a QR Code to scan with your Android 7.0 or later devices to stage the device quickly. The wizard simplifies the staging configuration process.

Procedure

1 After taking note of the prerequisites, select **Configure** to begin.

2 You can connect the device to **Wi-Fi** prior to enrollment by enabling the Wi-Fi toggle. This enabling action displays the following options.

Setting	Description
SSID	Enter the Service Set Identifier, more commonly known as the name of the Wi-Fi Network.
Password	Enter the Wi-Fi password for the entered SSID.

3 Select **Next**.

4 Select the Workspace ONE Intelligent Hub to push to devices during staging. The default selection is Use latest Workspace ONE Intelligent Hub.

If you do not have an Workspace ONE Intelligent Hub added, select **Hosted on an external URL** and enter the address in the **URL** text box to point to an externally-hosted Workspace ONE Intelligent Hub Package.

5 Select **Next**.

6 Set the **Enrollment Details** settings. To use token-based authentication, leave both options disabled.

Setting	Description
Organization Group	Enable and select the organization group the QR Code staging package uses.
User name	Enable to configure login credentials. Enter the Workspace ONE UEM account user name.
Password	Enter the corresponding password.

7 Select **Next**.

8 The **Summary** page allows you to **Download File** of the PDF. You can also **View PDF** to see a preview of your **QR Code Format** selections.

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.

Procedure

1 After taking note of the prerequisites, select **Configure** to begin.

2 Select the **Relay Server** to use to stage the devices.

   a If you do not have a relay server created, select **Add Relay Server**.

   The list of relay servers populates from any relay servers created for the organization group or the parent organization groups.

3 Select **Next**.

4 Select a **Wi-Fi Profile** that devices use to connect to the relay server and download the Workspace ONE Intelligent Hub.

   a 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 Workspace ONE Intelligent Hub to push to devices during staging.

   a If you do not have an Workspace ONE Intelligent Hub added, select Add Workspace ONE Intelligent Hub to upload an Workspace ONE Intelligent Hub Package if necessary.

   b Download the latest version of the Workspace ONE Intelligent Hub.

   c 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.
Password	Enter the password of the user.

9 Select **Next**.

10 Set the **Barcode** settings.

Setting	Description
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. With this setting enabled, the Workspace ONE Intelligent Hub prompts you to enter an organization group after beginning the staging process. If you are enrolling devices into Android (Legacy) with this barcode, care should be taken to only select an OG that is configured for Android (Legacy) enrollment.
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**.

What to do next

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.

If you want to make a Stage Now barcode for Zebra devices using the options you have selected above, you must close the Enrollment Wizard and proceed to the Generate a Barcode Staging Package step.

Generate a Sideload Staging Package Using the Enrollment Configuration Wizard

You can create a sideload staging package to configure and enroll the rugged device for Android legacy devices only. The wizard simplifies the staging configuration process.

After selecting Sideload enrollment in the Use the Enrollment Configuration Wizard, create a sideload staging package using the wizard.

Procedure

1 Select a **Wi-Fi profile** that devices use to connect to the relay server and download the Workspace ONE Intelligent Hub.

   a 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 Workspace ONE Intelligent Hub to push to devices during staging.

   a If you do not have an Workspace ONE Intelligent Hub added, select Add Workspace ONE Intelligent Hub to upload an Workspace ONE Intelligent Hub Package if necessary.

   b Download the latest version of the Workspace ONE Intelligent Hub.

   c 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.
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 Hub prompts you to enter an organization group after the staging process begins.

Create a Manual Staging Package

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

Procedure

1. Navigate to **Devices > Lifecycle > 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.
Hub	Select an existing Workspace ONE Intelligent Hub package from the drop-down listing to download during staging. You can also add the Workspace ONE Intelligent Hub package by selecting Add Workspace ONE Intelligent Hub at the bottom of the drop-down menu. These agents are uploaded as the Workspace ONE Intelligent Hub Package. See Upload the Workspace ONE Intelligent Hub APF File 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.

Establish a list of ordered steps during staging.

Procedure

1. After finishing the **General** tab of the Staging window, navigate to **Devices > Lifecycle > 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 Application** ■ **Uninstall Application** ■ **Install Files/Actions** ■ **Uninstall Files/Actions** ■ **Reboot** For more information on creating files, profiles, actions, see Chapter 4 Product Provisioning.
Profile	Select the profile to use in the staging configuration.
Application	Select the application 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.

4 Select **Add** again to add additional actions to the manifest.

5 When you are finished adding actions, select **Save**.

What to do next

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 Workspace ONE Intelligent Hub.

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.

Barcode enrollment is only supported on the following devices.

- Android
  - Zebra Rugged devices with MX running Android Marshmallow and earlier (Rapid Deployment barcodes only).
  - Zebra Rugged devices with MX version 7.1 or later running Android Nougat (Stage Now barcodes only).
  - Zebra Rugged devices with Android Hub version 8.2 or later (Stage Now barcodes only).

You can create barcodes to enroll Honeywell Android rugged devices in the Workspace ONE UEM console by using the EZconfig utility for Android legacy devices only.

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.

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

Procedure

1. Navigate to **Devices > Lifecycle > Staging**.
2. Select the radio button to the left of the name of the staging package you created in step 8 with the Generate a Barcode Staging Package Using the Enrollment Configuration Wizard.

   A new row of buttons displays under the **Add Staging** and **Configure Enrollment** buttons.
3. Select the **Barcode** or **Stage Now 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. With this setting enabled, the Workspace ONE Intelligent Hub prompts you to enter an organization group after beginning the staging process. If you are enrolling devices into Work Managed Mode with this barcode, care should be taken to select only an OG that has configured Android EMM Registration settings. 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.
Device Owner Mode	Enable to enroll the device into Android Work Managed mode. This option can only be enabled when the **Universal Barcode** option is enabled.

5 Select the **Barcode Format** options.

Android admins can enter the optional **Barcode Instructions** to be included on the barcode PDF output page.

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.

Sideload Staging Packages

You can create a sideload staging package to download and install onto devices to begin the auto-enrollment process for your Android legacy rugged devices only. 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.

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.

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

Procedure

1. Navigate to **Devices > Lifecycle > 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 Hub 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.

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).

Procedure

1. Download and install the Android Debug Bridge to the computer you want to use for staging devices.
2. Unzip the downloaded Sideload Staging ZIP file.

3 Depending upon the version of the OS that your device is running, you might need to download an updated stage.bat file from my Workspace ONE ™ Resource Portal.

   a Visit `https://my.workspaceone.com`.

   b Search for "VMware AirWatch Stage.bat for Zebra Sideload Staging" and download this file.

   c Verify that this stage.bat file is in the root folder of the unzipped Sideload Staging ZIP file.

4 Establish a USB debug connection to the Android device.

   USB debugging must be enabled on the Android device. The setting to enable this is in the device system settings under Developer Options.

5 Start the stage.bat file from the root folder of the unzipped Sideload Staging ZIP file.

   The stage.bat file copies files to the device and then uses intents to start the auto-enrollment process.

   The Workspace ONE UEM auto-enrollment screen displays on the device and shows progress.

   When auto-enrollment is complete, the Workspace ONE Intelligent Hub displays the main details screen.

This script installs the MX Service and Hub then applies the Wi-Fi profile you defined in the staging manifest and any other manifest items. Once the Wi-Fi connects, the device auto-enrolls into Workspace ONE UEM.

Enroll with Sideload Staging for Honeywell Devices

Enroll your Honeywell Android Rugged devices using a sideload staging package. Sideload staging configures your Honeywell Android Rugged devices to download the Workspace ONE Intelligent Hub and enroll automatically.

Prerequisites

- You must create a staging package before you create a sideload staging package. See Create a Manual Staging Package.
- Download the staging package and unzip the file to access the credentials.bin file.
- Download the latest Hub APK available on Workspace ONE UEM Resources. Contact your Workspace ONE UEM account manager for access to the APK.
- Download the latest Honeywell APK available on Workspace ONE UEM Resources. Contact your Workspace ONE UEM account manager for access to the APK.
- Download and install the Android Debug Bridge (ADB).

Procedure

1 Create a folder containing the following.

   - Latest Workspace ONE Intelligent Hub for Android APK.
   - Latest Honeywell APK.

- Credentials.bin from the staging package.

2 Open a text editor such as Notepad. Copy the following chunk of text and paste it into the blank notepad.

```
adb push credentials.bin /sdcard/credentials.bin
adb install HoneywellService.apk
adb shell am start -a android.intent.action.MAIN -n com.airwatch.admin.honeywell/.HoneywellActivity
adb install Hub.apk
adb shell am start -a android.intent.action.MAIN -n
com.airwatch.androidagent/com.airwatch.agent.ui.activity.SplashActivity -e hideui true
adb shell pm grant com.airwatch.androidagent android.permission.READ_EXTERNAL_STORAGE
adb shell am broadcast -a com.airwatch.agent.action.IMPORT_CREDENTIAL_XML -e
file /sdcard/credentials.bin --user 0
adb shell am broadcast -a com.airwatch.agent.action.AUTO_ENROLL --user 0
```

a Change the filenames and storage locations as needed.

3 Save the file as autoenroll_Honeywell.bat in the same directory as the other files.

4 Connect a Honeywell Android Rugged device to your PC using an ADB connection. Ensure that the device is connected to Wi-Fi.

5 Run the autoenroll_Honeywell.bat file.

Sideload Staging with Platform OEM Service

You can set up a Sideload Staging bundle for devices using the Generic OEM Service. This procedure is not supportive of Advanced Staging.

Procedure

1 Get the enrollment credentials.

a Create a Staging bundle in the console.

b Download the Sideload Staging Package.

c Unzip the Sideload Staging Package file and copy the 'credentials.bin' file inside the enrollment folder. Save this file for later.

2 Collect the necessary files for the device,

a Get the latest Hub APK.

b Get the OEM Service APK for your device.

c Get the credentials.bin from the preceding Step 1, number 3.

d Place all these files in a folder on your PC.

3 Create your auto-enroll BAT file.

a Using a text editor, add the following lines (change the filenames and storage locations based on your own configuration).

```
adb push credentials.bin /sdcard/credentials.bin
  adb install OEMService.apk
  adb shell am start -a android.intent.action.MAIN -n com.airwatch.admin.awoem.
[OEM_NAME]/com.airwatch.admin.awoem.PlatformOEMActivity -e hideui true
```

```
*If you are using POEM v3.2 or higher, use this intent instead:
  adb shell am start -a com.airwatch.START_AIRWATCH_SERVICE
```

```
adb install Agent.apk
  adb shell am start -a android.intent.action.MAIN -n
com.airwatch.androidagent/com.airwatch.agent.ui.activity.SplashActivity -e hideui true
  adb shell am broadcast -a com.airwatch.agent.action.IMPORT_CREDENTIAL_XML -e
file /sdcard/credentials.bin --user 0
  adb shell am broadcast -a com.airwatch.agent.action.AUTO_ENROLL --user 0
```

b Save the file as autoenroll_OEM.bat in the same directory as the other files.

*On Mac, it must be an SH file and run in Terminal.

4 Auto-enroll the device.

a Connect the device to Wifi.

b Connect the device to the PC via an ADB connection.

c Run the autoenroll_OEM.bat file.

Android Device Enrollment with the Workspace ONE Intelligent Hub

The Workspace ONE Intelligent Hub application facilitates enrollment and allows for real-time management and access to relevant device information. The enrollment process secures a connection between Android devices and your Workspace ONE UEM environment.

Android Rugged devices also support using the Workspace ONE Intelligent Hub to enroll Android devices. Workspace ONE UEM recommends using the Product Provisioning system to enroll devices through staging packages as the Workspace ONE Intelligent Hub enrollment method does not support some Product Provisioning functionality.

- WifiConfig cannot configure Fusion settings for Motorola devices. You must push the WifiConfig.apk as an internal app after enrollment to configure the settings. Extract the WifiConfig.apk from a sideload staging bundle inside the Workspace ONE Intelligent Hub folder of a device and upload it to the Workspace ONE UEMconsole as an internal app.

- Product Persistence does not support Workspace ONE Intelligent Hub enrollment method. Products marked for persistence still download to the device but an Enterprise Reset removes all products. Persisted products do not automatically reinstall following an Enterprise Reset when the device reboots.
- Android Work Managed enrollment is supported provided Zebra's Stage Now staging client is used.

For additional enrollment considerations and details about configuring enrollment options including enforcing enrollment restrictions, please see Device Enrollment Overview.

Product Provisioning

4

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 and Application 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.

With the Workspace ONE Intelligent Hub for Android v5.1+ or the Workspace ONE Intelligent Hub 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 > Provisioning > Components > Profiles**) are different than those created through the non-products process (**Devices > Profiles**). For more information, see Product Provisioning Profiles.

Applications

Product provisioning allows you to upload applications to the console for distribution as part of a product. Through product provisioning, you can upgrade applications and remove them remotely. For more information, see Application Provisioning.

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 Workspace ONE Intelligent Hub installs. Product Persistence only applies to specific Windows Rugged and Android devices. For more information, see Product Persistence.

This chapter includes the following topics:

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.

Prerequisites

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

Procedure

1 Navigate to **Devices > 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 console.

Setting	Description
Add Rule	Select to create a rule for product provisioning. Displays the **Attribute/Application**, **Operator**, and **Value** drop-down menus.
Add Application Rule	Select to create an application rule for product provisioning. This allows you to require applications to have specific versions install on the device for the rule to pass. 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 or application used to designate which devices receive the product. Custom attributes are created separately. Only internal applications display in the drop-down menu. You can use **Enter Manually** to enter the package ID of any application that should be present on the device. For more information, see Custom Attributes.
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 Applications**. ■ **Uninstall Application**. ■ **Install Files/Actions** – This option runs the Install Manifest. ■ **Uninstall Files/Actions** – This option runs the Uninstall Manifest. ■ **Reboot**.
Profile	Displays when the **Action Type** is set to Install Profile or Uninstall Profile. Enter the profile name.
Application	Displays when the **Action Type** is set to Install Application or Uninstall Application. Enter the application 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.

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 Workspace ONE Intelligent Hub, any persisted files/actions will be restored after Profiles are installed even if they were previously uninstalled. For more information, see Product Persistence.

8 Add additional **Manifest** items if desired.

9 You can adjust the order of manifest steps using the up and down arrows in the Manifest list view. You can also edit or delete a manifest step.

10 Select the **Conditions** tab if you want to use conditions with your product.

These conditions are optional and are not required to create and use a product.

11 Select **Add** to add either **Download Conditions**, **Install Conditions**, or both.

- A **Download Condition** determines when a product should be downloaded but not installed on a device.
- An **Install Condition** determines when a product should be installed on a device.

12 Select the **Deployment** tab if you want to control the time and date that products are activated and deactivated.

This tab is optional and is not required to create and use a product.

Setting	Description
Activation Date	Enter the time when a product automatically activates for device job processing. If the activation date is defined and the product is saved, the product stays inactive until the activation date is met according to the Workspace ONE UEM server time. The policy engine wakes up and automatically activates the product. You can manually activate products with activation dates beforehand. Manually activating a product overrides the activation date.
Deactivation Date	Enter the time when a product automatically deactivates from current and new device job processing. If the deactivation date is defined and the product is saved and currently active, it stays active until the deactivation date is met according to the Workspace ONE UEM server time. The policy engine wakes up and automatically deactivates the product. You can manually deactivate products with deactivation dates beforehand. Manually deactivating a product overrides the deactivation date. A deactivation date cannot be set earlier than the activation date.
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.
Deployment Mode	Select from the following how the product is to be deployed. **Relay Server with Workspace ONE Server as Backup** – This is the default deployment mode. The device attempts to receive the product from the relay server initially, making 5 separate attempts, then falling back to device services as a secondary source. **Relay Server Only** – The device only makes attempts to receive the product from the relay server. In a scenario where the relay server is not configured or deactivated, the fallback source is device services.
Auto Retry	Enables the automatic retry of a product push when it detects a push failure rate of up to 5%, making a maximum of three retries per device. For details, see Product Push Automatic Retry.

13 Select the **Dependencies** tab if you want to set the product to only provision devices that have other products provisioned as well.

   a 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 Workspace ONE Intelligent Hub 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.
- Product Persistence for Android only applies to legacy Motorola, Zebra, and Honeywell devices.

Persistence works as follows.

1. A device must contain a staging configuration so that the Workspace ONE Intelligent Hub 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 Chapter 5 Product Management). After resetting, the restore process starts.
4. The Workspace ONE Intelligent Hub for the device reinstalls during the restore process.
5. After the Workspace ONE Intelligent Hub is installed, any persisted profiles, such as Wi-Fi, reinstall.
6. Any persisted files-actions or apps are reinstalled.

Product Push Automatic Retry

When a device fails to process a provisioned product for whatever reason, the product push is automatically retried up to three times per device.

The product push automatic retry helps to minimize the amount of force reprocessing you must request. Enable this feature when you make a new product by navigating to **Devices > Provisioning > Product List View** and select the **Add Product** button followed by the platform selection. The **Auto Retry** check box is in the **Deployment** tab.

Automatic Retry Trigger

The automatic retry trigger audits each product job by making a rolling calculation of the product push failure rate. If the amount of failed product pushes is 5% or less, then an automatic retry is triggered. At this stage, individual devices are sampled and if the auto retry fails again, then another retry is attempted. This retry happens a maximum of three times per device.

If the amount of failed pushes is greater than 5% (or the rolling calculation increases to greater than 5%), then automatic retry is not triggered or the retry stops.

Manual Force Reprocess

You can monitor for product push failures by navigating to **Devices > Provisioning > Product Dashboard**. The product data that is displayed on the Product Dashboard can help you determine when to request a manual force reprocess, no matter at which stage the push fails.

For details on how to request a Force Reprocess, see Products List View.

Application Provisioning

Product provisioning allows you to upload applications to the console for distribution as part of a product. Through product provisioning, you can upgrade applications and remove them remotely.

Silent install of applications is supported on Android Legacy devices with an OEM service application and Android Work Managed devices.

Note Smart group assignment happens on the Product level and not on the Application level.

Upload an Application

Applications added through product provisioning use the rules and restrictions of the product to manage installation. Add applications that you want installed onto devices as part of a product.

Procedure

1. Navigate to **Devices > Provisioning > Components > Applications** and select **Add Application**.
2. Enter who the application is **Managed By**.
3. Select **Upload** to browse for the **Application File**.
4. Select **Choose File** to add a local file or select **Link** to enter a link.
5. Select **Save** to finish uploading the application.
6. Select **Continue** to add the application to the Product Provisioning application list.

Add New Application Versions

You can add a new version of an already uploaded application. This action enables you to push the newest version of an application to end users using the existing products you have already created.

Procedure

1. Navigate to **Devices > Provisioning > Components > Applications** and select **More**.
2. Select the **Add Version** option from the drop-down menu.
3. Upload the new version of the application as described in Upload an Application.
4. Select **Save**.
5. Navigate to **Devices > Provisioning > Product List View** and find the product that contains the app you want to update. If necessary, use the filters to narrow your search.
6. Select the radio button to the left of the product name.

   This radio button selection displays some action buttons at the top of the **List View**.

7 Select the **Edit** action button.

The **Edit product** screen displays.

8 In the **Manifest** tab, find the **Install Application** Action Type that contains the app you want to update and select the small blue pencil icon to the right of the **Description** column.

The **Edit Manifest** screen displays.

9 In the **Application** text box, delete the app name.

This action causes the drop-down menu to appear which now displays all versions of all applications in your entire Applications library.

10 Select the new version of the app that you uploaded in step 3 above.

11 Select the **Save** button.

The **Edit product** screen now shows the **Manifest** that includes the new version of the app.

12 Select the **Activate** button.

This action pushes the new version of the app to the devices provisioned with this product.

Delete Applications

Remove unwanted applications from your products. The Workspace ONE UEM console checks any attempt to delete an application against the list of active products.

Prerequisites

Before you are able to delete an application, it must be detached from all products.

Procedure

1 Navigate to **Devices > Provisioning > Applications**.

2 Locate the Application you want to delete from the List View.

3 Select the down arrow button to the far-right of the row belonging to the application.

4 Select **Delete**.

5 The Restricted Action screen displays. This is a security feature designed to prevent accidental application deletions. Enter your 4-digit security PIN to proceed with the deletion.

6 If the application you selected is part of a product, then you are not allowed to delete it until the application is detached from the product. A green warning prompt appears. At the bottom of the warning prompt lists all the products to which the selected application belongs. Take note of these products.

7 Navigate to **Devices > Provisioning > Product List View**.

8 Select the **Product** listed in the warning prompt.

9 Select the **Edit** button. The Edit Product screen displays.

10 Switch to the **Manifest** tab.

11 Select the delete button (**x**) to detach the application from the product. You are prompted to confirm.

12 Select **Save**.

13 Repeat steps 8 to 12 for all products containing the application.

What to do next

Once the application detaches from all products, you can delete the application by returning to complete steps 1 to 5.

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.

Condition	Android	macOS	QNX	Windows 7 / Windows Desktop	Windows Rugged
Adapter Time	✓	✓		✓	✓
Adapter					✓
Battery Threshold					✓
Confirm	✓	✓			✓
Connectivity State					✓
File	✓		✓		✓
Memory Threshold					✓
Power	✓			✓	✓
SD Card Encryption	✓			✓	
Schedule	✓			✓	
Time	✓		✓		✓

Conditions List View

You can view all conditions in a list view. You can also edit and delete conditions from the list view.

Procedure

1 Navigate to **Devices > Provisioning > Components > Conditions**.

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

3 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.

Procedure

1 Navigate to **Devices > Provisioning > Components > Conditions** and select **Add Condition**.

2 Select the Platform you want to create a condition for.

3 Complete the **Create Condition** Type settings.

Settings	Description
Name	Enter a name for the condition. The name cannot be longer than 255 characters.
Description	Enter a description for the condition.
Condition	The type of condition affects the parameters on the **Condition Details** tab. ■ **Adapter Time**. ■ **Battery Threshold***. ■ **Confirm**. ■ **File**. ■ **Power**. ■ **Recurring Schedule***. ■ **Schedule**. ■ **SD Card Encryption**. ■ **Time**. * Condition is only available for use in Event Actions. For more information, see Event Actions.
Managed By	Select the organization group that manages the condition.

4 Select **Next**.

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

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

Settings	Description
Specify scenario #1?	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**. **Set frequency limit** is a mandatory setting. The Adapter Time condition will not function correctly without it.

Note ActiveSync and VPN Network Adapters are not supported under the Android platform.

- **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.

- **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.
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**.

- **File** - This condition type tests the device to see if a file is present or not. You can set the condition to test if the file is on the device, and if it is, test true. You may also set the condition to test true if a file is not on the device.

Settings	Description
File Name	Enter the name of the file the system searches for, including device path. The system searches for this file before it downloads or installs product components.
Condition Met When	Select whether the system downloads or installs based on the existence of the file (File Found) or nonexistence of the file (File Not Found).
Frequency	Select how often the system searches for this file.
Duration	Select how long this condition performs the action.
After Duration Exceeded	Choose how to proceed after the condition duration period elapses.

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

Settings	Description
Message to be displayed	
First line prompt	Enter a header for the prompt.
Second line prompt	Enter the body of the prompt.
Third line prompt	If you enable a countdown, you can enter a countdown phrase into the **Third line prompt** field. For example, "You have %count% seconds to comply" where %count% will be the countdown clock.
Condition	
Required power level	Enter the required power level for the condition to test true. ■ **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.

- **Recurring Schedule** – Rather than set an event action to begin based on a specific device condition, you can simply assign it to a recurring schedule.

Settings	Description
Scheduled Interval	Select from **Hourly**, **Daily**, and **Weekly** as the basis for the recurrence.
Events Interval	Enter the length of time you want each recurring schedule to be. For example, if you want an event action to start every other day, then select Daily and enter 2 in this field. Alternatively, you could select Weekly and select the two specific days you want the event action to start. To start an event action twice a day, then select Hourly and enter 12 in this field.
Days of event occurrence (Weekly only)	
Sunday through **Saturday**	Select **Yes** for each day you would like the event action to start.
Start and End Time (Daily and Weekly only)	
Start Time.	Enter the time of day the event action starts.
End Time.	Many things can delay an event action from starting such as the device being offline or a previous event still in progress. When the device is ready, you can allow the event action to always start or set an end time at which point the device waits until the next start time. Enter the time of day the event action will stop making attempts to start until the next scheduled start time.
Disable end time.	Select **Yes** to disable end time. This causes the device to make continued attempts to start the event action until it succeeds.

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

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

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

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

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

Settings	Description
First Time Slot	
Select the month, day and yearStartFinish.	Select **Month**, **Day**, and **Year** for both Start and Finish.
Select hour and minuteStartFinish.	Select **Hour** and **Minute** for Start and Finish.
Second Time Slot	

Settings	Description
Enable time check 2?.	Select **Yes** to display a second set of options identical to the First Time Slot.
Third Time Slot	
Enable time check 3?.	Select **Yes** to display a third set of options identical to the First Time Slot.

6 Select **Finish**.

Delete a Condition

Remove unwanted conditions from your product. The Workspace ONE UEM console 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.

Procedure

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. An 'event' ocurrs followed by the prescribed 'action'. 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.

Procedure

1 Navigate to **Devices > Provisioning > Components > Event Actions** and select the **Add Event Action** button.

The **Add Event Action** wizard displays.

2 Select your device platform.

The available conditions and actions for the platform display.

3 Select **Next**.

4 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.

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

You can select a previously created condition or create a new one.

a To create a condition, select **Create Condition** from the drop-down menu.

b Select **Next** when complete.

For more information, see Create a Condition.

- **Battery Threshold** – select to take actions for specified battery limits.
- **Schedule** – Schedule your actions to run on a recurring basis.

6 Complete the required option **Minimum Time Between Actions (hours)**.

This option limits the number of times the action is run when triggered by the prescribed event.

This option is not available when **Recurring Schedule** is included in the selected conditions.

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

Action	Description
Custom Settings	Apply custom, OEM-specific device settings based on the selected XML file, which must be delivered to the device through a separate File/Action. If the file entered in the **File Path** text box is not found, then the Event Action does not run. However, the Event Action remains active, making attempts to run the custom setting XML file each time the condition is met. Supported Devices: ■ Android MSI devices with the Android Hub v7.1+ ■ Upload the ZIP file created by MSI. ■ Android Zebra devices with the Android Hub v7.2+ ■ Upload the XML configuration file created by the Zebra Stage Now program.
Files	You can download a file from the selected File Server source path onto the selected Destination folder of your device. For details, see Configure Download and Upload Actions for Event Action.
Reboot	Restart the device.
Run Intent	Run command lines and arguments on the device. See RunIntent Action for more information.
Files	You can upload a file from a source file path on your device to the selected File Server destination folder. For details, see Configure Download and Upload Actions for Event Action.

8 Select **Update** to add the action to the event action. You can add additional actions to the event action. Select **Next**.

9 Review the **Summary** and select **Save**.

What to do next

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

Configure Download and Upload Actions for Event Action

You must select a previously configured file server when you make Download Files or Upload Files the action of your Event Action. Making such a selection provides a source and destination for these files.

If you have not yet configured a file server for this purpose, see Add a File Server.

You can only see these options in the **Actions** tab of the **Add Event Action** screen, and only when you select as your action either **Download Files** or **Upload Files**.

Procedure

1 Complete the following options to configure the Download Files or Upload Files action.

Setting	Description
Select Action	This option is pre-populated with either Download Files or Upload Files.
File Server	Select from the list of **Existing** file servers you have configured previously. If no file servers are configured, select the **Create New** button followed by **New File Server** to add a file server and consult Add a File Server.
Source	For Download Files, the source is a file on the file server. Enter the path on the file server where the file can be found. For Upload Files, the source is a file on your device. Enter the directory or file path on your device where the file can be found.
Destination	For Download Files, the destination is your device. Enter the directory or file path on your device where the file is going. For Upload Files, the destination is the file server. Enter the path on the file server where the file is going.
Folder Naming	This option is available only when Upload Files is the **Select Action**. When multiple Upload Files actions use the same destination folder, there is a risk that identically named files might overwrite each other. To reduce this risk, files can be uploaded into dynamically generated child folders for each assigned device. You can use a lookup value to give identically named files a unique folder name. When you review the uploaded files on the file server, the folder name identifies the user or device from which it came. Select one or more of the following lookup values to make the destination folder name unique. ■ DeviceAssetNumber ■ DeviceUid ■ DeviceFriendlyName ■ User name ■ UserEmailAddress For more information, see Chapter 7 Lookup Values. You can also perform a search on docs.vmware.com.

2 Select the **Update** button to save your configuration.

File Servers

You can configure a file server as a staging and provisioning component. This file server component is in support of the Upload File and Download File actions in Event Actions.

You can coordinate this file server with an organization group and content gateway in Workspace ONE UEM console.

Add a File Server

File servers are used as the source or destination of a download files or upload files event action.

Procedure

1 Navigate to **Devices > Provisioning > Components > File Servers** and then select **Add File Server**.

2 Complete all applicable settings in the tabs that are displayed.

Setting	Description
Name	Enter a name for the file server.
Link	Enter the path of the source or destination of files. For example, \\home\NetworkFileShare
Organization Group	Enter the organization group you want to coordinate with for the File Server.
Content Gateway	Select the content gateway that is reachable from this resource. The selection of a content gateway is required.
User name	Enter the user name that is recognized by the file server.
Password	Enter the password that accompanies the user name.
Test Connection Status	Select the **Test Connection** button to test whether the file server can be connected to with the user name and password entered.

Files/Actions for Products

A file/action is the combination of the files you want on a device plus 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.

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.

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

Actions	Android	macOS	QNX	Windows Rugged	Windows 7	Windows Desktop
Copy Files.	✓	✓	✓	✓	✓	✓
Create Folder.	✓	✓	✓	✓	✓	✓
Delete Files.	✓	✓	✓	✓	✓	✓
Execute Script.		✓				
Install		✓	✓	✓	✓	✓
Move Files.	✓	✓	✓	✓	✓	✓
Remove Folders.	✓	✓	✓	✓	✓	✓
Rename File.	✓	✓	✓	✓	✓	✓
Run.		✓	✓	✓	✓	✓
Run Intent.	✓					
Reboot	✓					
Terminate.			✓	✓	✓	✓

Uninstall.		✓	✓	✓	✓
Warm Boot			✓		
OS Upgrade	✓				
Workspace ONE Intelligent Hub Upgrade.	✓				

Create a Files/Actions Component

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.

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

Procedure

1 Navigate to **Devices > 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.

There is a 2 GB limit on uploads.

7 Select **Save** to upload the files.

Once the files upload, the file grouping screen opens. File groups allow you to assign different download paths and settings to different groups of files you have uploaded to a single file/action.

8 Select uploaded files and select **Add** to move the files into a new file group.

9 Define the **Download Path** the device uses to store the file group in a specific device folder.

If the download path entered does not exist, the folder structure is created as part of installation.

10 Select **Save**.

You can repeat the previous steps for as many files as you want.

11 Select the **Manifest** tab.

Actions are not required if you have at least one file uploaded.

12 Add actions to the **Install Manifest** or the **Uninstall Manifest** if needed.

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

Settings	Descriptions
Workspace ONE Intelligent Hub Upgrade	Install the new Workspace ONE Intelligent Hub to the device. Before using this file/action, see Upload the Workspace ONE Intelligent Hub APF File for more information.
Apply Custom Settings	Apply custom, OEM-specific device settings based on the selected XML file. You must upload the custom XML or ZIP file as part of the file/action. Supported Devices: ■ Android Motorola Solutions devices with the Android Hub v7.1+ ■ Upload the ZIP file created by MSI. ■ Android Zebra devices with the Android Hub v7.2+ and Zebra's MX Service App installed on the device. ■ Create your XML configuration file using Zebra Stage Now. ■ Upload the XML configuration file and select it from the drop-down menu. ■ After pushing the product containing an Apply Custom Setting file/action, the status information reports in the Job Log. If an error occurs, the failed response XML is reported in the Job Log. For more information, see Product Job Statuses.
Copy Files	Copy files from one location to another on the device.
Create Folder	Create a new folder on the device.
Delete Files	Delete folders from the device.
Install Unmanaged Application	Install an unmanaged .APK file. Workspace ONE UEM does not add the app to the managed app list. Enterprise wipes or unenrollment do not remove the app from the device. You must use the Uninstall Unmanaged Application file/action. Consider adding Uninstall Unmanaged Application to the uninstall manifest of any product including the Install Unmanaged Application file/action.
Move Files	Move files from one location to another on the device.
OS Upgrade	Install a new OS upgrade and the relevant Workspace ONE Intelligent Hub. For more information on this option, see Create an Android OS Upgrade File/Action.
Reboot	Restart 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.

Settings	Descriptions
Run Intent	Run command lines and arguments on the device. See RunIntent Action for more information.
Uninstall Unmanaged Application	Uninstall an unmanaged application. Enter the package ID of the app.

- **Path Variables** – For all file management-related actions listed above (copy files, create folder, delete files, move files, remove folder, rename file, and rename folder), you have the option of inserting a path variable for both source and target, as applicable. The use of these variables in your Files/Actions path means you do not need to account for the randomly generated OEM-specific path definitions in the creation of your Files/Actions.
- **$internal$** – Use this variable at the beginning of your path to indicate your source/target path to be read from/written to the internal storage space. Supports read and write actions. For example: `/$internal$/agreement/license.txt` addresses the file `license.txt` in the agreement folder on the device's internal storage space.

  Note $internal$ does not work with all Files/Actions.
- **$external$** – Use this variable at the beginning of your path to indicate your source path to be from the external memory card storage, which the device must feature. External storage supports read-only access so any usage must involve a memory card that has been properly formatted and furnished with the correct files in the correct locations. For example: `/$external$/sdcard/license.txt` reads the file `license.txt` from the `sdcard` folder found on the device's external memory card storage.

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

Manage Files/Actions

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

Edit Files/Actions

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

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

Delete Files/Actions

Workspace ONE UEM checks any attempt to delete files/actions against the list of active products. To delete files/actions, it must be detached from all products.

Procedure

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

You can import MSP (Motorola Services Platform) packages, which can be unpacked into proper files/actions for use in products.

Procedure

1 Navigate to **Devices > 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.

Procedure

1 Navigate to **Devices > 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 > 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.

The following is a sample of an XML file which updates a registry setting that can be installed on a device through product provisioning.

Android Example

```
<?xml version="1.0"?>
<attributes>
    <attribute name="attribute 1" value="value 1"/>
    <attribute name="attribute 2" value="value 2"/>
    <attribute name="attribute 3" value="value 3"/>
</attributes>
```

Workspace ONE Intelligent Hub Upgrade File/Action

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

Use this option to enroll devices with older Hub versions installed. You can enroll the devices then upgrade the device to the new Hub 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 Hub 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 Hub Packages screen is only accessible in Customer type organization groups.

Upload the Workspace ONE Intelligent Hub APF File

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

Procedure

1 Navigate to **Devices > Provisioning > Components > Hub Packages** and select Add Workspace ONE Intelligent Hub. Make sure that you are using the top-level organization group.

2 Select the platform for which you are adding the Workspace ONE Intelligent Hub package.

The Add Workspace ONE Intelligent Hub screen displays.

3 Select the **Upload** button next to the **Application File** setting.

4 Select **Choose File** to browse for the APF file of the Workspace ONE Intelligent Hub version you want to upload.

5 Select the APF file and select **Open** to select the file.

6 Select **Save** to close the upload dialog.

With the uploading of the APF file, the settings are automatically populated with data.

7 Make any desired edits to **File Name**, **Package Name**, and **Version** for the Workspace ONE Intelligent Hub.

8 Select **Save** to upload the APF file to the UEM console.

RunIntent Action

The runIntent action starts an Android intent that facilitates late runtime binding between the code in different applications. Use these intents to accomplish actions on your Android devices.

The most significant use of runIntent is the launching of activities, where it can be thought of as the glue between activities. It is a passive data structure holding an abstract description of an action to be performed. The runIntent action supports both explicit and implicit intents.

Depending on the arguments used, the Workspace ONE Intelligent Hub uses either of the following to start the specified intent.

- android.content.Context.startActivity(Intent intent)
- android.content.Context.sendBroadcast(Intent intent) to run the specified intent.

RunIntent Syntax

The argument syntax changes depending on whether explicit or implicit mode is specified.

```
mode=explicit, broadcast=[true|false] , action=< action>, package=<package>, class=<class> [,
data=<data>][, extraString=<stringname>=<string value>[,...]][, extraInt=<int name>=<int value>[,…]]
```

```
mode=implicit, broadcast=[true|false] , action=<action> [,category=<category>][, uri=<uri>] [,
data=<data>] [, extraString=<string name>=<string value>[,...]][, extraInt=<int name>=<int value>[,…]]
```

Argument	Explanation
mode=[explicit|implicit]	Specifies whether the intent is explicit or implicit.
broadcast=[true|false]	Specifies whether the intent to be launched using startActivity() or sendBroadcast().
action=<action>	Specifies the Android action string for the intent. An example of an Android action string is android.intent.action.MAIN.
package=<package >	Specifies the Android package name of the java class to be explicitly run. Android package names are generally of the format com.mycompany.myapplication.
class=<class>	Specifies the java class in the specified package that is to be explicitly launched.
uri=<uri>	Specifies the URI that is to be passed with the implicitly launched intent.

category =<category>	Specifies the Android category string that is to be passed with the implicitly launched intent. An example of an Android category string is android.intent.category.DEFAULT
data=<data>	Specifies the value of the Android data parameter that is to be passed with the explicitly or implicitly launched intent.
extraString=<string name>=<string value>	Specifies the name of an extra string parameter that is to be passed with the explicitly or implicitly launched intent. string value specifies the value of the extra string. The extraString argument can be used multiple times to specify additional extra string name/values.
extraInt=<int name>=<int value>	Specifies the name of an extra int parameter that is to be passed with the explicitly or implicitly launched intent. int value specifies the value of the extra int. The extraInt argument can be used multiple times to specify additional extra int name/values.

The following table indicates which arguments are required, optional, or not applicable for the explicit and implicit modes.

mode	explicit	implicit
broadcast	required	required
action	required	required
package	required	n/a
class	required	n/a
uri	n/a	optional
category	n/a	optional
data	optional	optional
extraString	optional	optional
extraInt	optional	optional

Example RunIntent

```
mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.examples.myappl,class=com.e
xamples.myappl.MainActivity
```

APK File Installation

You can use a runIntent action on an APK file on the device's local storage which instals an application on the device.

RunIntent Syntax for APK File Installation

```
mode=implicit,broadcast=false,action=com.airwatch.android.provisioning.INSTALL_APKS_FROM_FOLDER,package
=com.airwatch.androidagent,extraString=path=/storage/emulated/Download
```

- You must customize the path in the highlighted portion to account for your specific file and folder structure.
- You can specify an individual APK file in this path on the runIntent which installs an app on the device.

- You can also specify a folder in the path of the runIntent, which runs all APK files found in that folder.
- Apps installed on a device using APK files via a runIntent are unmanaged.
- You can also use a path variable in the runIntent to represent the device's internal or external storage.

Path Variable Usage in RunIntent for APK Installation

$internal$ – Use this variable at the beginning of your path to indicate your source/target path to be read from/written to the internal storage space. Supports read and write actions. For example: `/$internal$/agreement/license.txt` addresses the file `license.txt` in the agreement folder on the device's internal storage space.

Note $internal$ does not work with all Files/Actions.

$external$ – Use this variable at the beginning of your path to indicate your source path to be from the external memory card storage, which the device must feature. External storage supports read-only access so any usage must involve a memory card that has been properly formatted and furnished with the correct files in the correct locations. For example: `/$external$/sdcard/license.txt` reads the file `license.txt` from the `sdcard` folder found on the device's external memory card storage.

Upgrade Android OS Using File/Action

You can upgrade your Android 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.

After an Android device receives an Android OS Upgrade file/action, the device processes the command in the following order.

Prerequisites

- Support includes Zebra devices using the Zebra MX Service and any OEM supporting the Platform OEM Service v3.0 or later. For more information about the Platform OEM Service, see the **VMware Workspace ONE UEM Android Platform Guide** topics titled **Android OEM Services** and **Platform OEM Service Overview**.
- **Note** Before updating your Motorola device to a new Zebra OS, you must have the Workspace ONE Intelligent Hub for Android v5.1.4+ installed and the 1.9 MX service.

Procedure

1. The device receives the product which you can verify on the device by navigating to **Hub > Products**.
2. Download all the files including the OS update zip which you can verify in the Product logs found on the device in **Hub > Products > Product Name**.
3. Once the downloads complete on a Zebra device, the Workspace ONE Intelligent Hub backs up its data and any installed managed applications to the device enterprise folder which is persistent.
4. The Hub then reboots the device into recovery mode to install the update.

5 Device then applies the OS update.

6 Once complete, the device reboots.

After reboot, the Workspace ONE Intelligent Hub validates that the OS update is successful before reporting that the job completed successfully.

What to do next

If the OS update fails, you can investigate the reasons why by using the Workspace ONE UEM console to navigate to **Devices > Provisioning > Product Dashboard**. Select the failed product in **Recent Product Status** that contains the OS upgrade. In the **View Devices** screen, select the magnifying glass icon to view history, then select the magnifying glass icon again to view the **Job Log**.

Create an Android OS Upgrade File/Action

Upgrade all your Android Rugged devices remotely with the Android OS Upgrade File/Action. Add the file/action to a product to push an OS Upgrade to your devices without needing to update them manually.

Procedure

1 Navigate to **Devices > Provisioning > Components > Files/Actions** and select the **Add Files/Actions** button.

2 Select **Android** as your device platform.

3 Complete the General text boxes.

   a Enter a **Name**.

   b Enter a **Description**.

   c View the **Version** automated by Workspace ONE ™ UEM.

   d Enter who the files/actions are **Managed By**.

4 Select the **Files** tab.

5 Select the **Add Files** button.

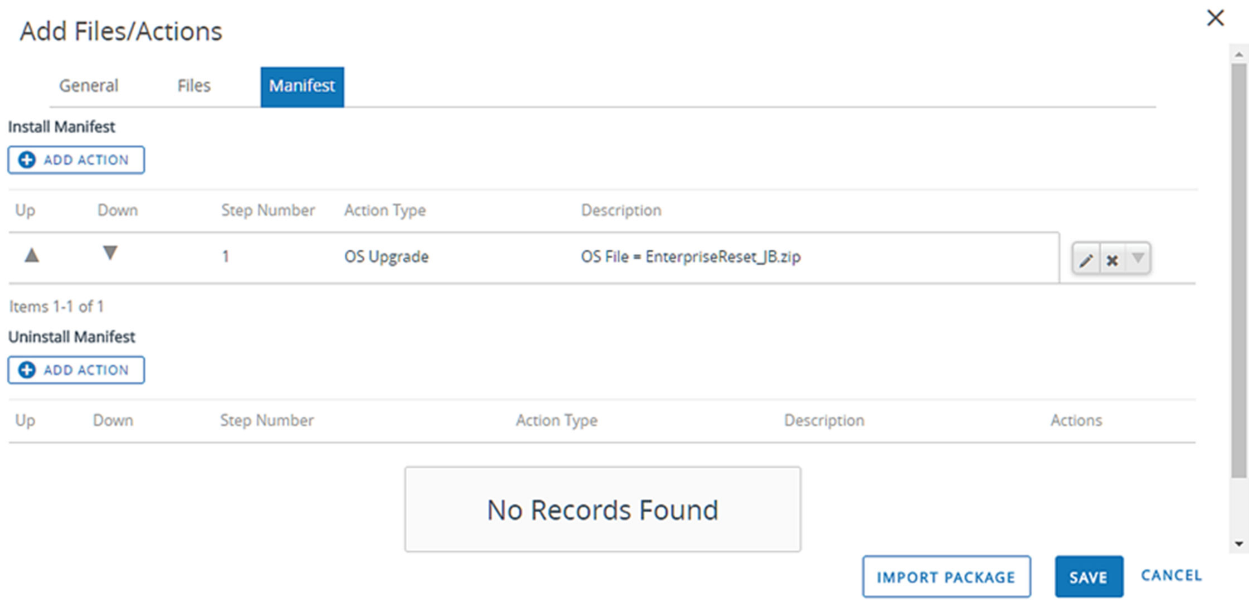
6 For Zebra devices, upload the following files and specify the path as either /data/tmp/ to store the file on the data partition, or as a known internal path to store it on the internal storage. For other devices, specify a known internal storage path on the device, such as /sdcard/.

   - OS Update ZIP file – This file can be a major or minor OS upgrade file. The file can also be an enterprise reset package.
   - [optional] Workspace ONE Intelligent Hub update package (APF) – This optional file can be specified to update the Workspace ONE Intelligent Hub before initiating the actual OS update. Workspace ONE UEM can provide this APK.

7 Select the **Manifest** tab and select **Add Action** under the **Install Manifest**.

8 Add OS Upgrade command to the manifest and select the corresponding OS upgrade file that was uploaded earlier.

Your Manifest tab looks similar to the following.



Up	Down	Step Number	Action Type	Description
▲	▼	1	OS Upgrade	OS File = EnterpriseReset_JB.zip

Items 1-1 of 1

Up	Down	Step Number	Action Type	Description	Actions

No Records Found

9 Select **Save**.

What to do next

After creating an OS Upgrade file/action, create a product to push the upgrade to your devices. See Create a Product for more information.

Note Before installing an OS Update, the device checks the battery level. If the level is below a threshold, the product fails. This failure displays in the log.

Create a Honeywell Android OS Upgrade File/Action

Upgrade all your Honeywell Android Rugged devices remotely through product provisioning. Add the file/action to a product to push the upgrade to your devices without needing to update them manually.

Honeywell Android Rugged devices do not use the OS Upgrade file/action to upgrade. The Honeywell OS uses an autoinstall feature to upgrade the device.

Prerequisites

Download the OS Update.zip from Honeywell before beginning this process.

The VMware Workspace ONE UEM Service for Honeywell must be installed on the device.

Procedure

1 Navigate to **Devices > Provisioning > Components > Files/Actions** and select **Add**. Create a file/action component.

See Create a Files/Actions Component for more information.

2. Upload the OS Update.zip to the file/action. Set the download location to **/storage/IPSM/honeywell/autoinstall/**.
3. Add a Reboot action in the file/action install manifest.
4. Create a product including the file/action you created and push the product to your Honeywell devices.

When the device processes the product job, the file is installed into the download location. When the device reboots, the OS autoinstalls the ZIP file and upgrades the device.

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 > 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 a Product Provisioning Profile

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.

Procedure

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 you to extract specific values from a managed device and return it to the Workspace ONE UEM console. You can also assign the attribute value for device lookup values.

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 Workspace ONE Intelligent Hub 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.

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

Create Custom Attributes

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

Procedure

1. Navigate to **Devices > 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.

   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

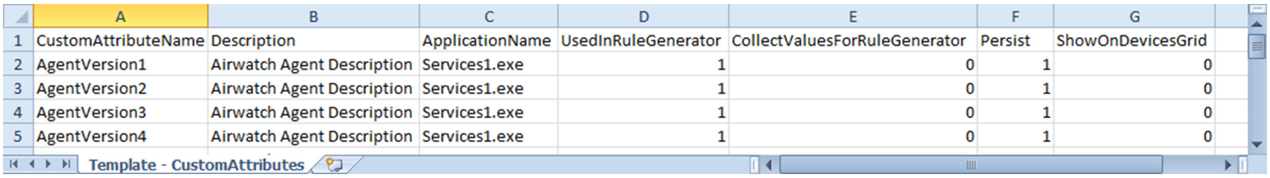
The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters.

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.

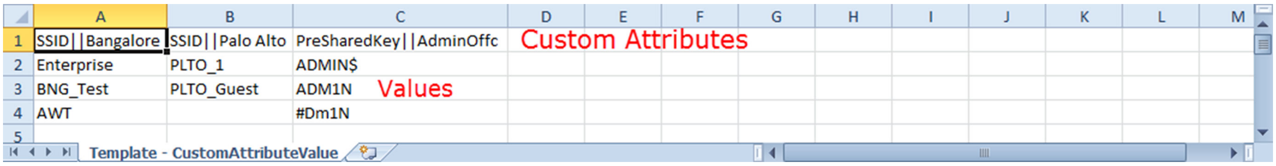
Template Types

- 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

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

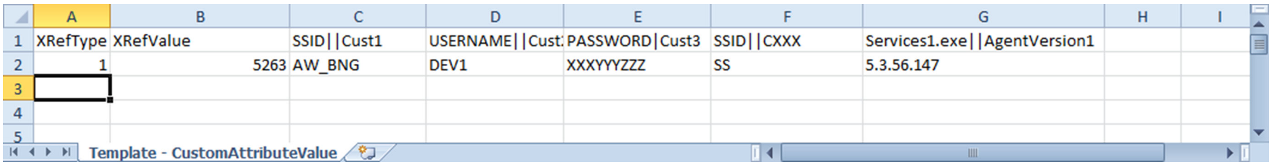


	A	B	C
1	SSID||Bangalore	SSID||Palo Alto	PreSharedKey||AdminOffc
2	Enterprise	PLTO_1	ADMIN$
3	BNG_Test	PLTO_Guest	ADM1N
4	AWT		#Dm1N
5			

Custom Attributes

Values

- 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									

a DeviceID (Workspace ONE UEM assigned DeviceID when the device enrolls)

b Serial Number

c UDID

d MAC Address

e 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.

Procedure

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 > Provisioning > Custom Attributes > List View > Add > Add Attribute** and create a custom attribute if you have not already done so.

   See Create Custom Attributes for more information.
7. Navigate to **Devices > 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.

Custom Attributes, Android

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

Procedure

1 Navigate to **Devices > Provisioning > Components > Files/Actions > Add** and select **Android** as your platform.

2 Create an XML provisioning file.

See Create an XML Provisioning File. The manifest must include an action to download the XML file to the Zebra device location **/enterprise/usr/attributes**.

For non-Zebra Android devices, the XML file location is **/sdcard/Android/data/com.airwatch.androidagent/files/attributes/**.

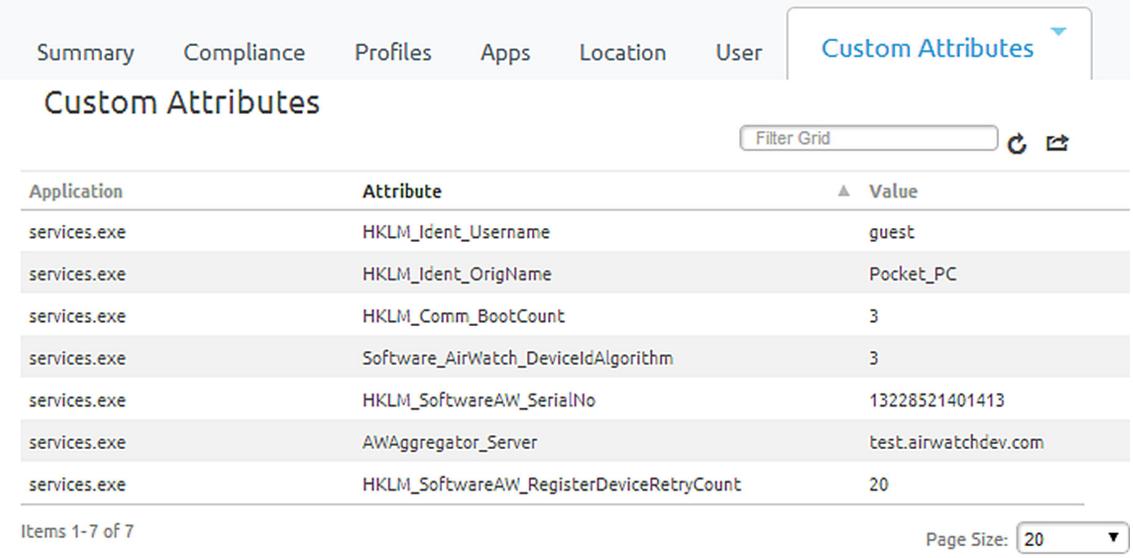
Upon receiving the XML file, the Workspace ONE Intelligent Hub for Android creates a custom attributes output file.

During the next check-in with AirWatch, the Workspace ONE Intelligent Hub sends the output file to the Workspace ONE UEM console.

Once the XML file installs, the custom attributes requested in the file exported to the console. These values display in the console in 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.

Android

```
<?xml version="1.0"?>
<attributes>
    <attribute name="attribute 1" value="value 1"/>
    <attribute name="attribute 2" value="value 2"/>
    <attribute name="attribute 3" value="value 3"/>
</attributes>
```



Custom Attributes

Application	Attribute	Value
services.exe	HKLM_Ident_Username	guest
services.exe	HKLM_Ident_OrigName	Pocket_PC
services.exe	HKLM_Comm_BootCount	3
services.exe	Software_AirWatch_DeviceIdAlgorithm	3
services.exe	HKLM_SoftwareAW_SerialNo	13228521401413
services.exe	AWAggregator_Server	test.airwatchdev.com
services.exe	HKLM_SoftwareAW_RegisterDeviceRetryCount	20

Items 1-7 of 7

Page Size: 20

What to do next

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

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.

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.

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.

Procedure

1. Navigate to **Devices > 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 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.
- Add a Product to a Product Set.
- Change the Product Ranking in a Product Set.
- Removing Products from Product Sets.

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

You can add a product to an existing product set. This action requires following specific rules due to the complicated relationship 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 for more information on what happens when product ranks are adjusted.

Procedure

1. Navigate to **Devices > 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.

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

Table 4-4. Rank Changes

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.

Procedure

1 Navigate to **Devices > 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.

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 for more information on what happens when product ranks are adjusted.

Any modifications made during the edit of a product set do not take effect until you save the product set.

Procedure

1 Navigate to **Devices > 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.

Once saved, the product set enters the policy engine for evaluation.

Product Management 5

Manage products using the product provisioning management functionality. 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.

XML Provisioning

For Windows Rugged, Windows Desktop, and Android devices only, 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.

This chapter includes the following topics:

Products Dashboard

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

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

Recent Product Status

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

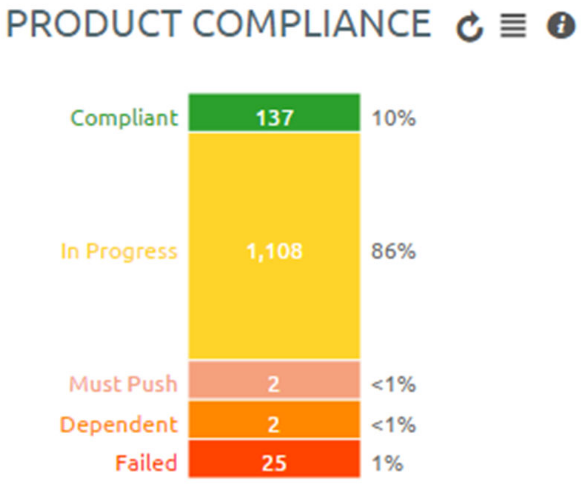
- Compliant – The product installed on the device and the inventory data of the product reported by the device matches the requirements of the product.
- In Progress – The product has been sent to the device and is pending a compliance check based on inventory.
- Must Push – The product deployment type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

Filters

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

Product Compliance

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



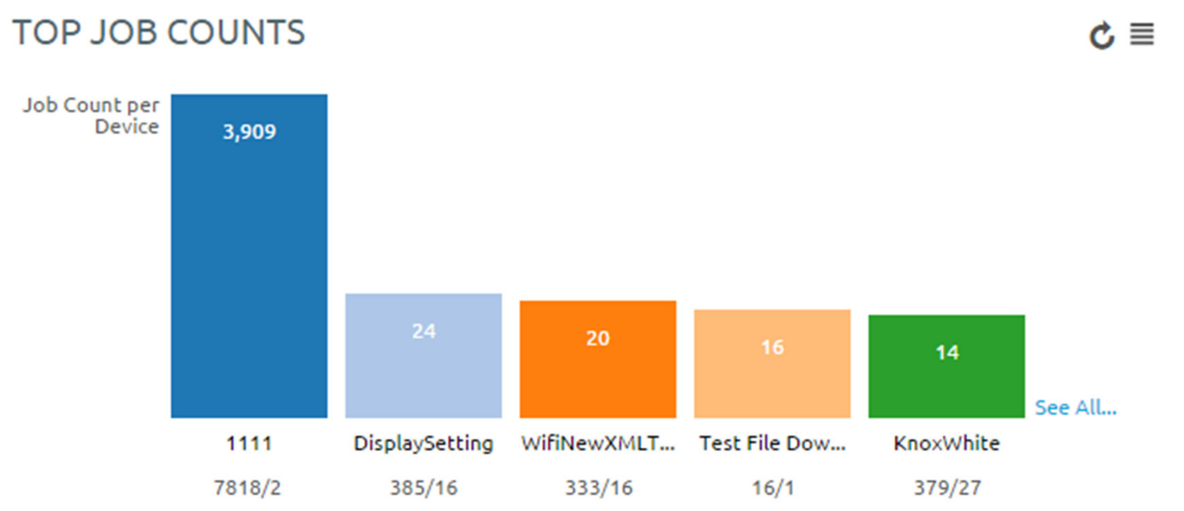
Filters

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

To filter your results, select the **Menu** icon (≣) in the top right corner. Select either the platform or the product by which you want to filter.

Top Job Compliance

This chart displays a ratio of total job count to the number of devices to which the product is provisioned. 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.

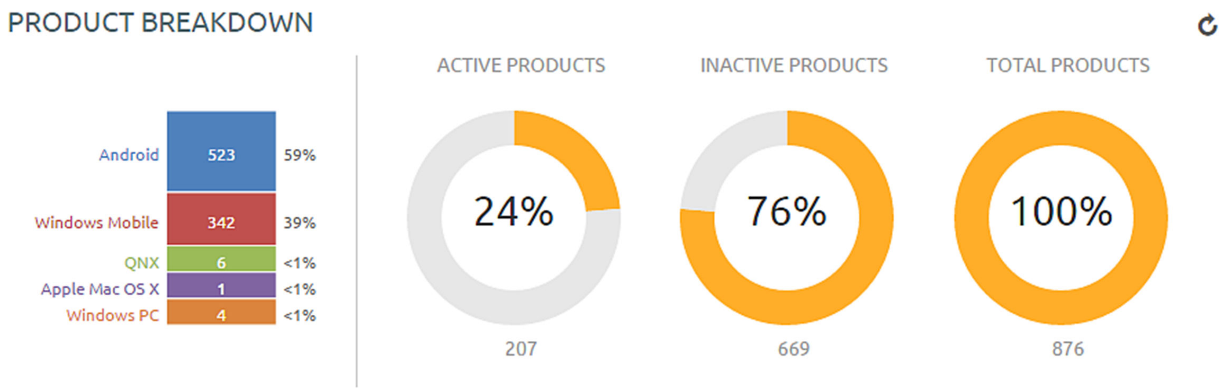
Filters

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, reprocess, and delete products and view the devices a product is provisioning.

Navigate to **Devices > 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.

Select a product by name 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. You can also select the number links in the **Compliant**, **In Progress**, **Failed**, **Has Dependency**, **Must Push**, **Offline**, and **Total** columns, allowing you to see device details as they pertain to these product provisioning statuses.

Select the edit radio button to the left of each product name and you have access to the following actions.

- You can **Deactivate** a product, making it no longer accessible. Deactivating the product also clears all pending provisioning commands.
- Select the **Edit** button to 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.
- Select the **View Devices** button to view all devices to which 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.

More Actions

- You can view the **Activation Log** for the selected product, which displays detailed information about the product including date of activation and the name of the admin who initiated the activation.
- You can make a **Copy** of a product. If one of your products has detailed and intricate parameters, you can save time programming them from the beginning by making a copy of an existing product. You could then, for example, change the application in the manifest of the copy, thus making an entirely new product that shares the same detailed parameters.
- 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 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.
- The **Inherited Products** option 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.

Applications

For Android devices only, navigate to **Devices > Details View > Apps** to access the Applications on the device.

Profiles

For Windows Rugged devices, Windows Desktop devices, QNX devices, and Android devices only, 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.

Job Status	Description
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 for Android and Windows Rugged devices only by navigating to **Groups & Settings > All Settings > Devices & Users > Android** or **Windows > Windows Rugged** then continue on to **Hub 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.

Target a Device Log Level for Troubleshooting Purposes

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

Procedure

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.

Procedure

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.

What to do next

For Android and Windows Rugged only, you can target an individual device for troubleshooting purposes. See Target a Device Log Level for Troubleshooting Purposes.

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.

Procedure

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.

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.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.

  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.

  - **No Passcode** – The number and percentage of devices without a passcode configured for security.

  - **No Encryption** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.

  Ownership – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.

- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send them a message requesting that they check in.

- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.

- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.

- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for Apple iOS, Android, Windows Phone, and Windows Rugged. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

This chapter includes the following topics:

Device List View

Use the UEM console's Device List View to see a full listing of all devices in the currently selected organization group.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on the number of minutes defined in **Device Inactivity Timeout (min)**. This indicator can be set by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.

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** views of the current OG and of all the OGs underneath.

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, within the current organization group and all child groups.

Using the Device Details Page

The **Device Details** page allows you to track detailed device information and quickly access user and device management actions.

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

Android devices running Android M utilize power saving options for idle apps and devices. If a user unplugs a device and leaves it stationary, with its screen off, for a period of time, the device goes into **Doze** mode, where it attempts to keep the device in a sleep state. There will be no network activity during this time.

Additionally, **App Standby** mode allows the device to determine that an app is idle when the user is not actively using it. When devices are in either state, the Workspace ONE UEM console will not receive reports on device details. When the user plugs a device in to charge or opens an app, the device will resume normal operations and reporting from AirWatch apps installed on the device to the Workspace ONE UEM console resumes.

Use the **Device Details** menu tabs to access specific device information, including:

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, organization group, contact information, serial number, power status including battery health, storage capacity, physical memory and virtual memory. Zebra devices feature a panel displaying detailed battery information. You can also view the Workspace ONE Intelligent Hub and which version of any applicable OEM is currently installed on the device.
- **Compliance** – Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View all apps currently installed or pending installation on the device.
- **Content** – View status, type, name, priority, deployment, last update, and date and time of views, and provide a toolbar for administrative action (install or delete content).
- **Location** – View current location or location history of a device.
- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

The menu tabs below are accessed by selecting **More** from the main Device Details tab.

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Telecom** – View all amounts of calls, data and messages sent and received involving the device.

- **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
- **Certificates** – Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
- **Products** –View complete history and status of all packages provisioned to the device and any provisioning errors.
- **Custom Attributes** – Enable you to use advanced product provisioning functionality.
- **Files/Actions** – View the files and other actions associated with the device.
- **Event Actions** – Allows you to take action on a device when predetermined conditions are met
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Troubleshooting** – View **Event Log** and **Commands** logging information. This page features export and search functions, enabling you to perform targets searches and analysis.
  - **Event Log** – View detailed debug information and server check-ins, including a **Filter** by **Event Group Type**, **Date Range**, **Severity**, **Module**, and **Category**.

    In the **Event Log** listing, the **Event Data** column may display hypertext links that open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install.
  - **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a **Filter** enabling you to filter commands by **Category**, **Status**, and specific **Command**.
- **Compromised Detection** – View details about the compromised status of the device including the specific **Reason** for the status and how **Severe** the status is.
- **Status History** – View history of device in relation to enrollment status.
- **Targeted Logging** - View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the **Create New Log** button and select a length of time the log is collected.
- **Attachments** – Use this storage space on the server for screenshots, documents, and links for troubleshooting and other purposes without taking up space on the device itself.

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.

Enterprise Reset is only available for Windows Rugged Devices and Android legacy Motorola, Zebra, and Honeywell devices.

Note Enterprise Reset cannot run on devices with low battery levels. If you attempt an Enterprise Reset on a device with low battery level, a warning displays alerting to you about potential issues with the Enterprise Reset. On Android devices, the Enterprise Reset command is held until the device reaches sufficient battery level. Once the device is charged, the Reset occurs automatically.

Procedure

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.

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire Workspace ONE UEM solution as a comprehensive replacement for Google Cloud Messaging (GCM).

AWCM provides real-time device management status and command pushes for:

- Devices that cannot be configured with a Google Account.
- Devices restricted to internal network communication.
- Devices without public Internet access.

Enable AWCM by navigating to **Devices > Device Settings > Android > Hub Settings > AirWatch Cloud Messaging**.

Select **Enabled** on **Use AWCM Instead of C2DM** to enable AWCM. Selecting this option locks the deployment type to **Always Running** so that the system and device have a constant and ongoing line of communication. You may also choose to leave the **Use AWCM Instead of C2DM** check box unchecked and decide to make the deployment type **Always Running** or **Manual**, with an associated timeout value.

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 Advanced Remote Management Server to facilitate communication between the Workspace ONE UEM console and the end-user device.

For more information, see **VMware Workspace ONE Advanced Remote Management Documentation** on docs.vmware.com.

Platform OEM Service

The Platform OEM (POEM) Service is an additional app that allows the Workspace ONE UEM console to provide extended management capabilities to Android legacy devices only.

After you enroll, the Workspace ONE UEM console automatically detects if the device can take advantage of additional device capabilities, and deploys an Original Equipment Manufacturer (OEM) specific service application to your Android. The OEM Service app is a plug-in app that is only installed and used in combination with Workspace ONE Intelligent Hub enrollment.

It allows for additional MDM capabilities that only pertain to a specific OEM device. All of these APKs are available through AirWatch Resources by request. There are a few service apps that we publish to the Google Play Store (see list below).

Here is a sample of supported features and available OEMs for the Platform OEM Service.

POEM Service Features

- Silent App installation, uninstallation, and updates
- Silent Device Administrator Activation on launch
- Date/Time configuration (date format, time format, time zone, server time, SNTP, HTTP URL, or Auto)
- Toggle Bluetooth on/off with the Disable Bluetooth restriction
- Disable installation from unknown sources on 5.0 Lollipop and above
- Device Reboot

POEM Service Versions

- Bluebird
- Kube
- Getac
- Honeywell
- HP
- Intermec
- Lenovo
- Mediawave
- Panasonic
- Sonim
- Zebra CC5000

POEM Service Version Available on the Google Play Store

- Samsung
- Sony
- LG
- Huawei
- Zebra
- Honeywell

Lookup Values

7

A lookup value is a variable that represents a particular data element of a device, user, or admin account. Lookup values can be invaluable in completing a process or a form.

In several different text boxes in the Workspace ONE UEM console, you can add lookup values in place of manually entered or static values. In most cases, lookup values function as a stand-in for a piece of information you do not know or do not have access to.

For example, the **Add Device** screen is used to add a device to your fleet. One of the text boxes on this screen that can be completed with lookup values is the **Expected Friendly Name**.

The friendly name represents the device on many different screens in the UEM console including the **Device List View** and the **Details View**. And while you can enter a static friendly name manually, you can instead use lookup values to standardize the friendly name and make it a valuable identifier.

A common friendly name format can be constructed with the following lookup values.

{EnrollmentUser} {DeviceModel} {DeviceOperatingSystem} {DeviceSerialNumberLastFour}

If you enter the above in the **Expected Friendly Name** text box, it produces a friendly name that looks like this on the **Device List View**.

jsmith iPad iOS GHKD

This friendly name instantly provides you with at least three useful pieces of information. And with the last four digits of the device serial number at the end, it is virtually guaranteed to be unique.

Data Overhead

When used, lookup values do not add to the device's memory with an extra load. Lookup values are a construct of the UEM console itself, not something that is transferred to the device.

Static Strings Versus Lookup Values

Lookup values cannot be applied once a static string has been entered in a text box.

For example, assume that you have 100 devices to enroll. You add the first 50 devices using a manually entered static string for **Expected Friendly Name**. For the next 50 devices, you opt to use a lookup value for **Expected Friendly Name** instead. Those 100 devices, half with static friendly names and the other half with lookup values, can coexist perfectly well. There is no issue with mixing and matching static strings and lookup values.

However, you cannot return to the first 50 devices and replace the static string friendly name with a lookup value.

Custom Lookup Values

You can use the Custom Attributes feature to make your own lookup values. You can then use these custom lookup values in the same manner as ordinary lookup values. For details, see Create Custom Attributes.

Lookup Values Listing

To reference a full listing of lookup values including the locations in Workspace ONE UEM from which they are accessed, see https://support.workspaceone.com/articles/115001663908.