VMware AirWatch Product Provisioning and Staging for Android Guide

Using Product Provisioning for managing Android devices.

AirWatch v9.3

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

Table of Contents

Chapter 1:
Overview

Introduction to Product Provisioning for Android Rugged

Product provisioning allows you to create, through AirWatch, products containing profiles, applications, and files/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 AirWatch Console. Create these servers for each store or warehouse to store product content for distribution to your devices.

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

As this guide focuses on the functionality provided by product provisioning, it does not contain all the features and functionality that AirWatch offers for managing Android devices. For more information on general MDM functionality for Android devices, see the **Android Platform Guide** available on AirWatch Resources.

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.

AirWatch supports product provisioning for devices with the following operating systems:

- Android devices v4.1 (Jelly Bean) and higher with AirWatch Agent.

Chapter 2:
Relay Server Configuration

Relay Servers Overview

Relay servers act as a content distribution node that provides help in bandwidth and data utilization control. Relay servers act as a proxy between the AirWatch server and the rugged device for product provisioning.

Relay Server Basics

This proxy basically serves as an FTP/Explicit FTPS/SFTP server that distributes products to the device for download and installation. Using relay servers allows the product to distribute to all devices without consuming all of the bandwidth to the main/central MDM server.

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

Note: Relay servers, both push and pull configurations, fall back to the next available relay server in its hierarchy and continue to fall back until the device finds a suitable server or reaches AirWatch. This ensures devices with products provisioned to them have access to their content.

Source Server vs Relay Server

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

Configure a Relay Server

Configure an FTP, Explicit FTPS, Implicit FTPS, or SFTP file server to integrate with AirWatch as a relay server. For more information, see Configure a Relay Server on page 8.

Pull Relay Server Configuration

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

Bulk Importing

The Relay Server Import feature loads relay servers into the system in bulk. This feature simplifies the configuration of multiple relay servers. For more information, see Batch Import Relay Servers on page 10.

Remote Viewing of Files on a Relay Server

After configuring a relay server and assigning products to use the relay server, you can view the files hosted on the server. For more information, see Remote Viewing Files on Relay Server on page 13.

Relay Server Management

Maintaining Relay Servers keeps your products running smoothly so your devices remain up to date. AirWatch offers several tools to ensure your relay servers work as intended. For more information, see Relay Server Management on page 14.

Configure a Relay Server

Configure a relay server by configuring an FTP, Explicit FTPS, Implicit FTPS, or SFTP file server and integrating it with AirWatch.

> **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 allows the pull service to store and remove files from the directory.

Requirements

- An FTP, Explicit FTPS, Implicit FTPS, or SFTP server.
- 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 username and password for authentication.
- While SFTP servers are supported by AirWatch, the supported staging clients, Stage Now (Android) and Rapid Deployment, do not support SFTP servers for use with barcode staging.

Procedure

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

Setting	Description
	General
Name	Enter a name for the relay server.
Description	Enter a description for the relay server.
Relay Server Type	Select either Push or Pull as the relay server method. **Push** – This method is typically used in on-premises deployments. The AirWatch 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 AirWatch Console through an outbound connection. For more information on installing a pull server, see Pull Service Based Relay Server Configuration on page 10.

Setting	Description
Restrict Content Delivery Window	Enable to limit content delivery to a specific time window. Provide a **Start Time** and **End Time** based on the relay server time.
Assignment	
Managed By	Select the organization group that manages the relay server. If you want to use the FTP(S) server for Barcode Enrollment only and not for Product Provisioning, remove all assigned organization groups under the Production Server section.
Staging Server	Assign the organization groups that use the relay server as a staging server. A staging server only works for the staging process involving the supported staging clients, Stage Now (Android) and Rapid Deployment.
Production Server	Assign the organization groups that use the relay server as a production server. A production server works with any device with the proper agent installed on it.
Device Connection	
Protocol	This is the information the device uses to authenticate with the FTP(s) server when downloading apps and content. **FTP**, **Explicit FTPS**, **Implicit FTPS**, or **SFTP** as the Protocol for the relay server. If using Explicit FTPS, your Explicit FTPS server must have a valid SSL certificate. Configure the SSL certificate on the Explicit FTPS server.
Hostname	Enter the name of the server that hosts the device connection.
Port	Select the port established for your server. **Important:** The ports you configure when you create your FTP, Explicit FTPS, or SFTP server must be the same ports you enter when creating a relay server in the AirWatch Console. AirWatch does not support Implicit FTPS relay servers.
User	Enter the server username.
Password	Enter the server password.
Path	Enter the path for the server. This path must match the home directory path of the ftp user. For example, if the ftp user's home directory is C:\ftp\home\jdoe, the path entered into this field must be C:\ftp\home\jdoe.
Passive Mode	Enable to force the client to establish both the data and command channels.
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 AirWatch Console uses to authenticate with the FTP(S) server when pushing apps and content. The settings are typically identical to the **Device Connection** tab.

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

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

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

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

5. Select **Save**.

Batch Import Relay Servers

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

Save all files in .csv format before importing.

To bulk import relay servers, take the following steps.

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

Pull Service Based Relay Server Configuration

Pull service based relay servers periodically contacts the AirWatch Console to check for new products, profiles, files, and actions, and applications assigned to devices under the pull relay servers purview. Configure a pull server to deliver content to devices without excessive bandwidth use.

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

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. The instructions below detail how to create a pull relay server from an Explicit FTP(S) server.

> **Important:** The ports you configure when you create your FTP, Explicit FTPS, or SFTP server must be the same ports you enter when creating a relay server in the AirWatch Console. AirWatch does not support Implicit FTPS relay servers.

This process covers the installation of one server at a time. For bulk installation, you must use a third-party application. AirWatch supports importing servers in bulk through the Bulk Import option. See Batch Import Relay Servers on page 10 for more information.

Create a Windows-Based Pull Service Relay Server

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

Prerequisites

- An FTP, Explicit FTPS, or SFTP server. AirWatch recommends using FTP or Explicit FTPS servers, as SFTP is not a standardized format. AirWatch does not support Implicit FTPS relay servers.
- .NET must be installed on Windows-based servers.
- The relay server requires network access between the server (in-store, distribution center, etc.) and to the AirWatch SaaS environment.
- Each server requires disk storage of 2 MB for the pull server installer as well as storage space for all the content pulled to the server.

Process

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

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

```
<PullConfiguration>
    <libraryPath>C:\AirWatch\PullService\</libraryPath>
```

```
        <endPointAddress>https://[endpoint URL]/contentpull/</endPointAddress>
</PullConfiguration>
```

5. Run the WindowsPullServiceInstaller.exe.

   .NET will be installed before the MSI is extracted.

6. Follow the instructions prompted by the installer.

7. Navigate to **Devices >Staging & Provisioning > Relay Servers > Undiscovered Pull Relay Servers**. If you have configured the FTP, Explicit FTPS, or SFTP server correctly, it will display on this screen. If you do not see your server, check your configuration settings.

8. Configure the relay server as a pull relay server in the AirWatch Console. See Configure a Relay Server on page 8 for more details.

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

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

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

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

Create a Linux-Based Pull Service Relay Server

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

Prerequisites

- An FTP, Explicit FTPS, Implicit FTPS, or SFTP server. AirWatch recommends using FTP or Explicit FTPS servers, as SFTP is not a standardized format. AirWatch does not support Implicit FTPS relay servers.

- Linux-based servers must run either CentOS or SLES 11 SP3.

- Java 8+ must be installed on Linux-based servers.

- The relay server requires network access between the server (in-store, distribution center, etc.) and to the AirWatch SaaS environment.

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

Process

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

1. Configure an FTP, Explicit FTPS, or SFTP server. You must create an FTP user with read/write/delete permissions for both the directory and the files used in the relay server. This FTP user is must have a username and password for authentication. Note the home directory of the user for use in configuring the pull service.

2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Pull Service Installers**.

3. Download the Linux Pull Service Installer and the Configuration file onto the server using your preferred server management system.

4. Open the XML config file and update the IP Address with your console server FQDN, for example, cn274.awmdm.com.

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

5. In the command prompt, enter:

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

   a. Alternatively, enter the following command to silently install:

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

6. Navigate to **Devices > Staging & Provisioning > Relay Servers > Undiscovered Pull Relay Servers**. If you have configured the FTP, Explicit FTPS, or SFTP server correctly, it will display on this screen. If you do not see your server, check your configuration settings.

7. Configure the relay server as a pull relay server in the AirWatch Console. See Configure a Relay Server on page 8 for more details.

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

Remote Viewing Files on Relay Server

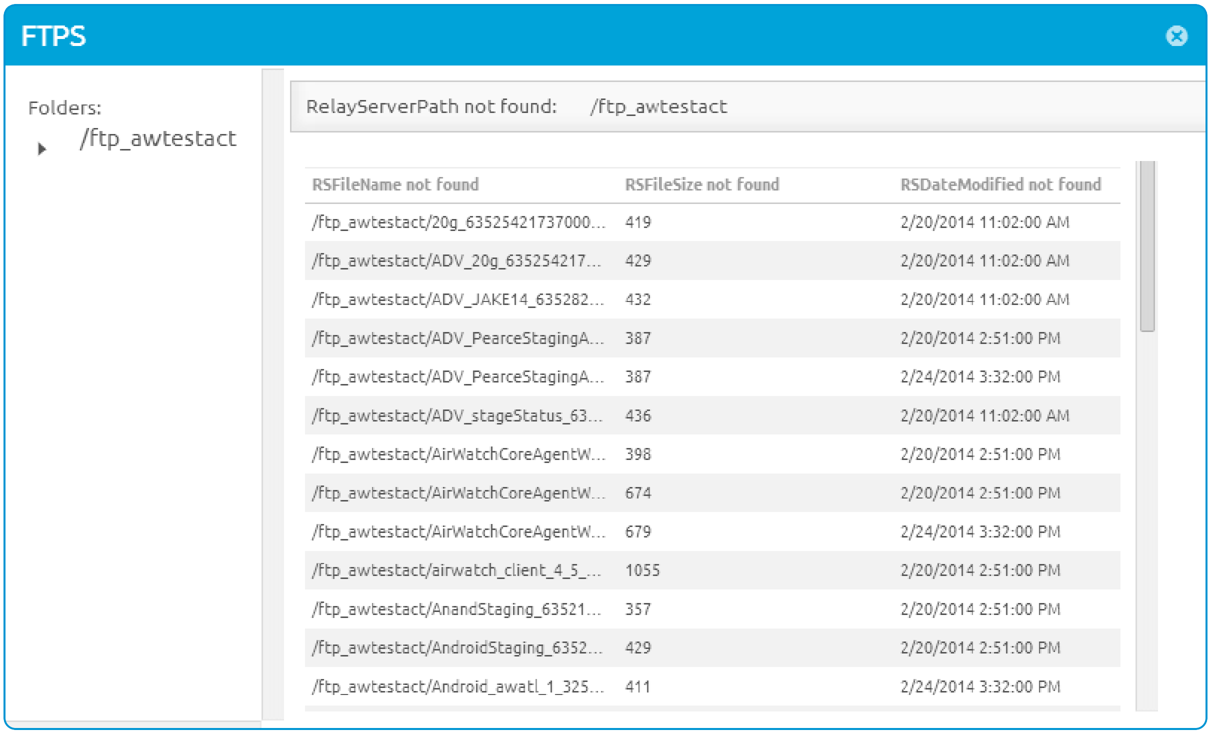
View files sent to a relay server for distribution to devices through the Remote File Viewer.

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

1. Navigate to **Devices > Staging & Provisioning > Relay Servers > List View**.

2. On the far right of a server listing, select the **More** option.

3. Select **Remote File List** to open the Remote File List for your viewing. You can see the files are on a relay server.



FTPS

Folders:

/ftp_awtestact

RelayServerPath not found: /ftp_awtestact

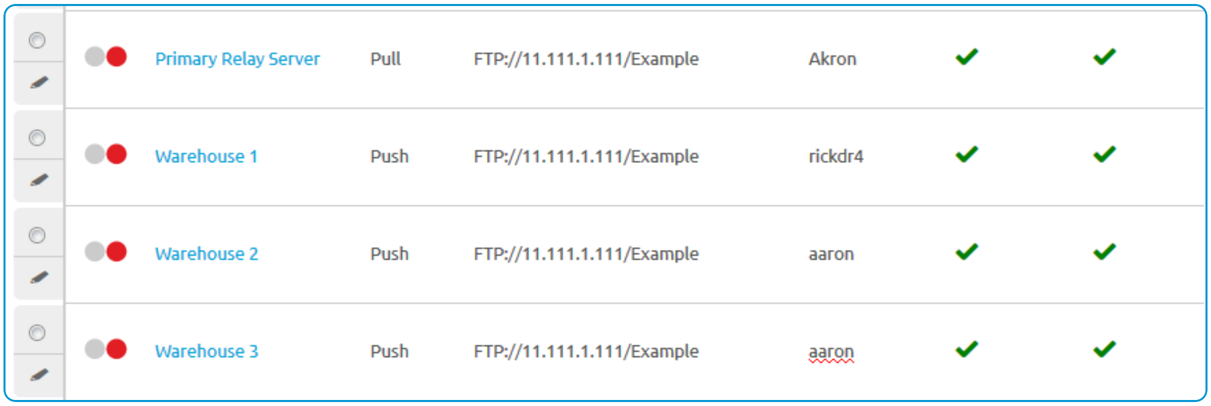
RSFileName not found	RSFileSize not found	RSDateModified not found
/ftp_awtestact/20g_63525421737000…	419	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_20g_635254217…	429	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_JAKE14_635282…	432	2/20/2014 11:02:00 AM
/ftp_awtestact/ADV_PearceStagingA…	387	2/20/2014 2:51:00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

Relay Server Management

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

Relay Server Status

After creating a relay server, refresh the relay server detail page to get the real-time 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	✓	✓

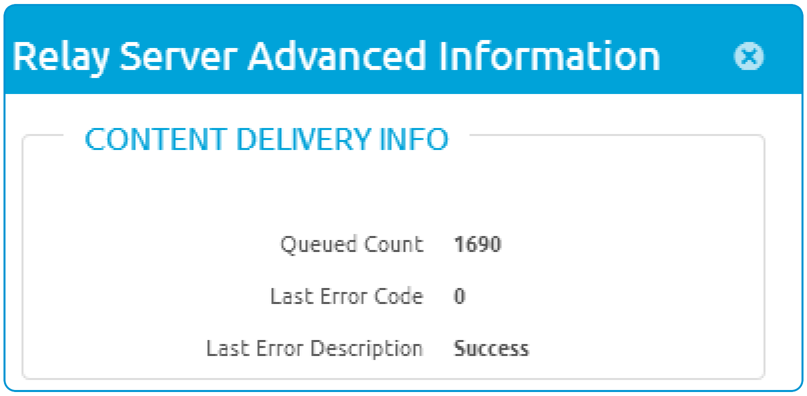
The **Source Server** and **Relay Server** statuses are as follow:

Settings	Descriptions	
	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

Along with the Relay Server Status, 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 1690

Last Error Code 0

Last Error Description Success

Chapter 3:
Device Staging

Staging Overview

Staging enables you to enroll a device quickly. A Staging package connects a device to a Wi-Fi connection, installs the AirWatch Agent and enrolls the device without end-user input.

Staging Basics

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

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

You have several methods for enrolling a rugged device through staging. Barcode Enrollment creates a staging package associated with a barcode that you scan to stage the device. On-Demand staging uses the Rapid Deployment Client (RD Client) to download the staging package to your Zebra Windows Rugged or Motorola devices. Sideloading packages are transferred to a device instead of being scanned or downloaded.

Rugged Enrollment Configuration Wizard

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

Staging Configuration

If you are not using the Rugged Enrollment Configuration Wizard, you must manually create a staging package. The staging package contains all the relevant enrollment information for devices. After creating a staging package, you install the package onto devices using barcode staging, sideload staging, or on-demand staging. For more information, see Create a Manual Staging Package on page 20.

Advanced Staging

As part of creating a staging package, you can add more instructions and files to the staging package. These advanced components enhance the actions taken during enrollment. For more information, see Configure Advanced Staging on page 21.

Staging Wi-Fi Profile

It is mandatory that your staging package include a Wi-Fi profile. This profile configures the device to connect to the network the device uses to access the relay server to download the AirWatch Agent and enroll. For more information, see Create a Wi-Fi Profile for Staging on page 22.

Barcode Staging

You can create a barcode to scan to begin the auto-enrollment process for your Motorola and Zebra rugged devices. The barcodes simplify staging devices into a quick scan of a barcode to configure the device using a created staging package. For more information, see Barcode Staging on page 23.

On-Demand Staging

On-demand enrollment allows Motorola and Zebra rugged devices to scan a network or ActiveSync connection for a broadcast staging package. For more information, see On-Demand Staging on page 24.

Sideload Staging

You can create a sideload staging package to install onto devices to begin the auto-enrollment process for your rugged devices. The sideload staging packages simplify enrollment by combining all the required components into one. For more information, see Sideload Staging Packages on page 25.

Use the 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.

To use the Rugged Enrollment Configuration Wizard.

1. Navigate to **Devices > Staging & Provisioning > Staging > Configure Enrollment**.
2. Select the device platform you want.
3. Select the staging enrollment type.
    - Generate a Barcode Staging Package using the Rugged Enrollment Configuration Wizard on page 18 – 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 Rugged Configuration Wizard on page 26 – Create a sideload staging package to download and install onto a device to automatically configure and enroll the rugged device.
4. Select **Configure**.

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

Generate a Barcode Staging Package using the Rugged Enrollment Configuration Wizard

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

To create a barcode using the wizard.

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

   The list of relay servers populates from any relay servers created for the organization group or the parent organization groups. If you do not have a relay server created, select **Create a new Relay Server**.

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

   If you do not have a Wi-Fi profile created, select **Create Wi-Fi profile**. You cannot create a Wi-Fi profile through the wizard that uses certificate authentication. The Wi-Fi profile created is used for staging and remains on the device after enrollment.

4. Select **Next**.
5. Select the **AirWatch Agent** to push to devices during staging.

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

   Download the latest version of the AirWatch Agent from AirWatch Resources. Contact your Account Manager or AirWatch Support for access.
6. Select **Next**.
7. 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 username of the user. If you do not have a user, select **Create a New 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. Android Rugged devices only.

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

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

10. Select **Save**.

Generate a Sideload Staging Package using the Rugged Enrollment Configuration Wizard

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

To create a sideload staging package using the wizard.

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

If you do not have a Wi-Fi profile created, select **Create Wi-Fi profile**. You cannot create a Wi-Fi profile that uses certificate authentication through the wizard. The Wi-Fi profile created is used for staging and remains on the device after enrollment.

2. Select **Next**.
3. Select the **AirWatch Agent** to push to devices during staging.

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

   Download the latest version of the AirWatch Agent from Accessing Other Documents on page 81. Contact your Account Manager or AirWatch 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 username of the user. The user must be a basic user account. Do not use staging users or multi-user staging.
Password	Enter the password of the user.

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

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

Create a Manual Staging Package

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

To create a staging configuration, follow these steps.

1. Navigate to **Devices > Staging & Provisioning > Staging > Add Staging**.
2. Select the Platform type you want to create a staging configuration for.

3. Complete the required fields 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 username of the enrollment user. You can search for and select an existing user by clicking the magnifying glass icon. You can also add a new user by selecting **Add User** at the bottom of the drop-down menu.
Password	Enter the password for the enrollment user. You have the option of keeping the password redacted or displaying it as written.
Agent	Select an existing AirWatch Agent package from the drop-down listing to download during staging. You can also add a new agent package by selecting **Add AirWatch Agent** at the bottom of the drop-down menu. These agents are uploaded as an Agent Package. See Upload the AirWatch Agent APF File on page 39 for more information.

4. Select **Save**.

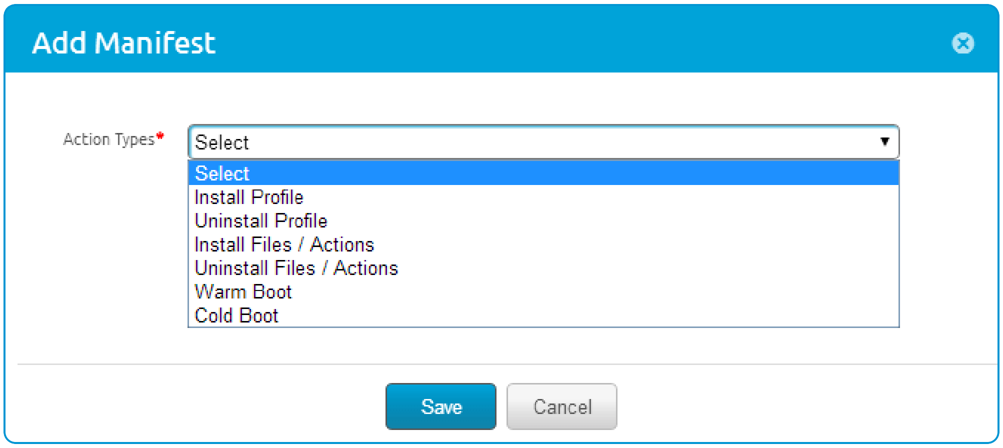
Configure Advanced Staging

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

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

1. After completing the **General** tab of the Staging window, select the **Manifest** tab.

2. Select **Add**.



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 Product Provisioning Overview on page 31.
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 on page 60.

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

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

6. View the newly created staging profile in the List View. Take additional actions on the profile from the menus on the right.

   - **Edit** your configuration.
   - **Copy** your profile.
   - Select **Barcode** and complete the fields on the **Generate Barcode** subpage.

Create a Wi-Fi Profile for Staging

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

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

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

- **Staging Wi-Fi Profile** – Connects a device to the Wi-Fi used for staging.

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

Barcode Staging

You can create a barcode and use it to auto-enroll your Motorola and Zebra rugged devices. The barcodes make staging devices fast and easy by reducing the process down 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. These clients only support FTP and FTPS relay servers.

Barcode enrollment is only supported on the following devices.

- Android
  - Zebra Rugged devices

Barcode Enrollment for Honeywell Android Devices

You can create barcodes to enroll Honeywell Android rugged devices in the AirWatch Console by using the EZconfig utility. For more information, see the Knowledgebase Article on Honeywell Barcode Staging Package at https://support.air-watch.com/articles/115001664568.

Generate a Barcode Staging Package

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

Prerequisites

You must create a staging package before you generate a barcode. See Create a Manual Staging Package on page 20.

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

Procedure

To generate a barcode, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Staging**.
2. Select **Barcode** (▥) located in the menu to the right of a staging configuration.
3. Select the **Staging Options**.

Settings	Descriptions
Organization Group	Select the organization group the staging package uses.

Settings	Descriptions
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. The agent prompts you to enter an organization group after beginning the staging process. 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.

4. Select the **Barcode Format** for the device you want to enroll.

5. Select **View PDF**. This generates the barcode for end users to scan.

On-Demand Staging

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

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

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

Create an On-Demand Staging Package

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

Prerequisites

You must create a staging package before you create an on-demand enrollment package. For more information, see Create a Manual Staging Package on page 20.

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

1. Navigate to **Devices > Staging & Provisioning > Staging**.

2. Find the staging configuration you want to use, select the radio button to the left of the Name, then select the **More Actions** button when it appears.

3. Select **On-Demand** from the drop-down menu.

4. Specify the staging options.

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

5. Select the **On-Demand** button to launch the On-Demand Enrollment screen.

6. Select **Turn staging server on**.

7. On the device you want to enroll, start the supported staging client and use the following settings.

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

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

Sideload Staging Packages

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

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

Generate a Sideload Staging Package using the Rugged Configuration Wizard

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

Prerequisites

You must create a staging package before you create a sideload staging package. See Create a Manual Staging Package on page 20.

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

Procedures

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

1. Navigate to **Devices > Staging & Provisioning > Staging**.
2. Choose 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. Choose the **Organization Group** to which this staging applies.
4. (Optional) Enable **Universal Barcode** to enable a universal enrollment so devices can be enrolled without automatically assigning an organization group. This allows you to enroll devices without needing a Sideload enrollment for each organization group. The agent will prompt you to enter an organization group after beginning the staging process.
5. Select **Download** to start downloading the zip file of the staging sideload.

Install a Sideload Staging Package

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

For Android device staging, follow the steps below:

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. Verify the 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. Launch the stage.bat file from the root folder of the unzipped Sideload Staging ZIP file.
6. The stage.bat file will copy files to the device and then use intents to start the auto-enrollment process.
7. The AirWatch auto-enrollment screen displays on the device and shows progress.
8. When auto-enrollment is complete, the AirWatch Agent displays the main details screen.

This script installs the MX Service and agent then applies the Wi-Fi profile you defined in the staging manifest as well as any other manifest items. Once the Wi-Fi connects, the device auto-enrolls into AirWatch.

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 AirWatch Agent and enroll automatically.

Prerequisites

- You must create a staging package before you create a sideload staging package. See Create a Manual Staging Package on page 20.
- Download the staging package and unzip the file to access the credentials.bin file.
- Download the latest Agent APK available on AirWatch Resources. Contact your AirWatch account manager for access to the APK.
- Download the latest Honeywell APK available on AirWatch Resources. Contact your AirWatch account manager for access to the APK.
- Download and install the Android Debug Bridge (ADB).

Procedures

1. Create a folder containing the following.
   - Latest AirWatch Agent 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 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 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
   ```

   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.

Step 1 - Get the Enrollment Credentials

1. Create a Staging bundle in the console.
2. Download the Sideload Staging Package.
3. Unzip the Sideload Staging Package file and copy the 'credentials.bin' file inside the enrollment folder. Save this file for later.

Step 2 - Collect the Necessary Files for the Device

1. Get the latest Agent APK.
2. Get the OEM Service APK for your device.
3. Get the credentials.bin from the preceding Step 1, number 3.
4. Place all these files in a folder on your PC.

Step 3 - Create Your Auto-Enroll BAT File

1. 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
```

2. 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.

Step 4 - Auto-Enroll the Device

1. Connect the device to Wifi.
2. Connect the device to the PC via an ADB connection.

3. Run the autoenroll_OEM.bat file.

Android Device Enrollment with the AirWatch Agent

The AirWatch Agent 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 AirWatch environment.

Android Rugged devices also support using the AirWatch Agent for Android to enroll devices. AirWatch recommends using the Product Provisioning system to enroll devices through staging packages as the AirWatch Agent enrollment method does not support some Product Provisioning functionality. The issues are listed below:

- 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 Agent folder of a device and upload it to the AirWatch Console as an internal app.
- Product Persistence does not support AirWatch Agent 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 devices use the Enrollment URL to first check and then download the AirWatch Agent. The AirWatch Agent provides a single resource to enroll a device as well as provides device and connection details. Additionally, the enrollment process allows you to:

- Authenticate users using basic or directory services, such as AD/LDAP/Domino, SAML, tokens or proxies.
- Authenticate users using pass through authentication using Single Sign On.
- Register devices in bulk or allow users to self-register.
- Define approved OS versions, models and maximum number of devices per user.

Chapter 4: Products

Product Provisioning Overview

The main feature of the Product Provisioning system is creating an ordered installation of profiles, applications, and files/actions (depending on the platform used) 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 determine when a product is downloaded as well as 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 AirWatch Agent for Android v5.1+ or the AirWatch Agent for Windows Rugged v5.5+, interrupted products, known as orphaned products, will automatically restart and continue 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 are different than those created through AirWatch MDM. For more information, see Product Provisioning Profiles on page 32.

Files/Actions

You can install, configure, and upgrade devices by assigning files/actions to a product. The files/actions component also contains ways to manage the file system of a device. For more information, see Files/Actions for Products on page 33.

Applications

Product provisioning allows you to upload applications to the console for distribution as part of a product. Through product provisioning, you can upgrade and downgrade applications and remove them remotely. For more information, see Application Provisioning on page 43.

Product Conditions

A condition determines when the product or OS upgrade package should be downloaded and installed. Conditions are checked when a product is pushed to a device. For more information, see Product Conditions on page 45.

Create a Product

After creating the content you want to push to devices, create a product that controls when the content is pushed as well as the order of installation of the product. For more information, see Create a Product on page 57.

Product Persistence

Product Provisioning allows you to enable profiles, files/actions, and applications to remain on a device following an enterprise reset. Content marked to persist following an enterprise reset reinstalls following the device restart after the agent installs. Product Persistence only applies to specific Windows Rugged and Android devices. For more information, see Product Persistence on page 60.

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 AirWatch MDM. This section lists the differences between profiles created for normal device use and those created for use in product provisioning.

Auto-Renewal of Certificates Not Supported

If you include a certificate profile in your product, the certificate does not auto-renew.

You can get around this limitation by pushing a product with a full manifest (minus the wifi cert profile) then assigning a separate MDM wifi cert profile by navigating to **Devices > Profiles & Resources > Profiles > ADD**.

Profile Creation and General Settings

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

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

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

Saving Product Provisioning Profiles

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

Profiles names cannot be longer than 255 characters.

Edit Product Provisioning Profiles

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

Update Profiles

When you edit an existing profile, the version number automatically increases. After saving the edits, AirWatch 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 choose to **Activate** or **Deactivate** a product using the profile.

Delete Profiles

AirWatch checks any attempt to delete a profile against the list of active products.

In order to delete a profile, you must detach it from all products.

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

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

Files/Actions for Products

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

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

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

Create a Files/Actions Component

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

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

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

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	This setting is automated by the AirWatch Console.
Platform	Read-only setting displays the chosen platform.
Managed By	Select the organization group that can edit the files/actions.

4. Select the **Files** tab.
5. Select **Add Files**. The **Add Files** window displays.

6. Select **Choose Files** to browse for a file or multiple files to upload.
7. Select **Save** to upload the files. Once the files upload, the file grouping screen opens. File groups allow you to assign different download paths and settings to different groups of files you have uploaded to a single file/action.
8. Select an uploaded file(s) 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 may repeat the previous steps for as many files as you want.
11. Select the **Manifest** tab. Actions are not required as long as you have at least one file uploaded.
12. Add actions to the **Install Manifest** or the **Uninstall Manifest** if needed.

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

Settings	Descriptions
AirWatch Agent Upgrade	Install the new AirWatch Agent to the device. Before using this file/action, see Upload the AirWatch Agent APF File on page 39 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 MSI devices with the Android Agent v7.1+ ○ Upload the ZIP file created by MSI. • Android Zebra devices with the Android Agent v7.2+ ○ 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 a Apply Custom Setting file/action, the status information reports in the Job Log. The failed response XML is reported in the Job Log. For more information, see Product Job Statuses on page 78.
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. AirWatch 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.

Settings	Descriptions
OS Upgrade	Install a new OS upgrade as well as the relevant AirWatch Agent. For more information on this option, see Create an Android OS Upgrade File/Action on page 37.
Reboot	Restart the device.
Remove Folder	Remove a folder from the device.
Rename File	Rename a file located on the device.
Rename Folder	Rename a folder located in the device.
Run Intent	Run command lines and arguments on the device. See Example RunIntent on page 41 for more information.
Uninstall Unmanaged Application	Uninstall an unmanaged .APK file.

- **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.

  - **$external$** – 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 automatically increases. After saving the edits, AirWatch 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

AirWatch checks any attempt to delete files/actions against the list of active products.

In order to delete files/actions, it must be detached from all products.

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

Android OS Upgrade File/Action

You can upgrade your Android devices remotely to a new version of the OS using product provisioning. Support includes Zebra devices using the Zebra MX Service and any OEM supporting the Platform OEM Service v3.0 or higher. This process allows you to keep your entire device fleet up to date without needing to have the devices shipped back to you.

For more information about the Platform OEM Service, see the **VMware AirWatch Android Platform Guide** topic titled "Android OEM Services" available in Accessing Other Documents on page 81.

Note: Before updating your Motorola device to a new Zebra OS, you must have the AirWatch Agent for Android v5.1.4+ installed as well as the 1.9 MX service. For information on upgrading the OS for Honeywell devices, see the KB article :https://support.air-watch.com/articles/115001664568.

Device Side OS Update Process

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

1. Device receives the product which you can verify in **Agent > Products**.
2. Download all the files including the OS update zip which you can verify in the Product logs found in **Agent > Product > Product Name**.
3. Once the downloads complete, the AirWatch Agent backs up its data and any installed managed applications to the device enterprise folder which is persistent.
4. The agent then fires the intent to start the OS update by passing the OS Upgrade zip file.
5. Device then applies the OS upgrade.
6. Once complete, the device reboots.
7. Upon reboot, the Rapid Deployment client re-installs the agent applications and launches them.
8. Upon launch, the agent restores its data and re-installs managed apps.

Import Packages in Files/Actions

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

To import an MSP package, take the following steps.

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

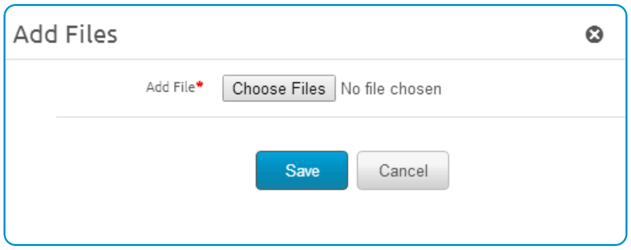
   Once the file is uploaded, the required fields are auto-completed.
5. Select **Save**.

Create an Android OS Upgrade File/Action

Upgrade all of 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 manually update them.

To create an OS Upgrade File/Action:

1. Navigate to **Devices > Staging & Provisioning > Components > Files/Actions** and select **Add**.
2. Select **Android** as your device platform.
3. Complete the General fields.
   - Enter a **Name**.
   - Enter a **Description**.
   - View the **Version** automated by AirWatch.
   - Enter who the files/actions are **Managed By**.
4. Select the **Files** tab.
5. Select the **Add Files** button.

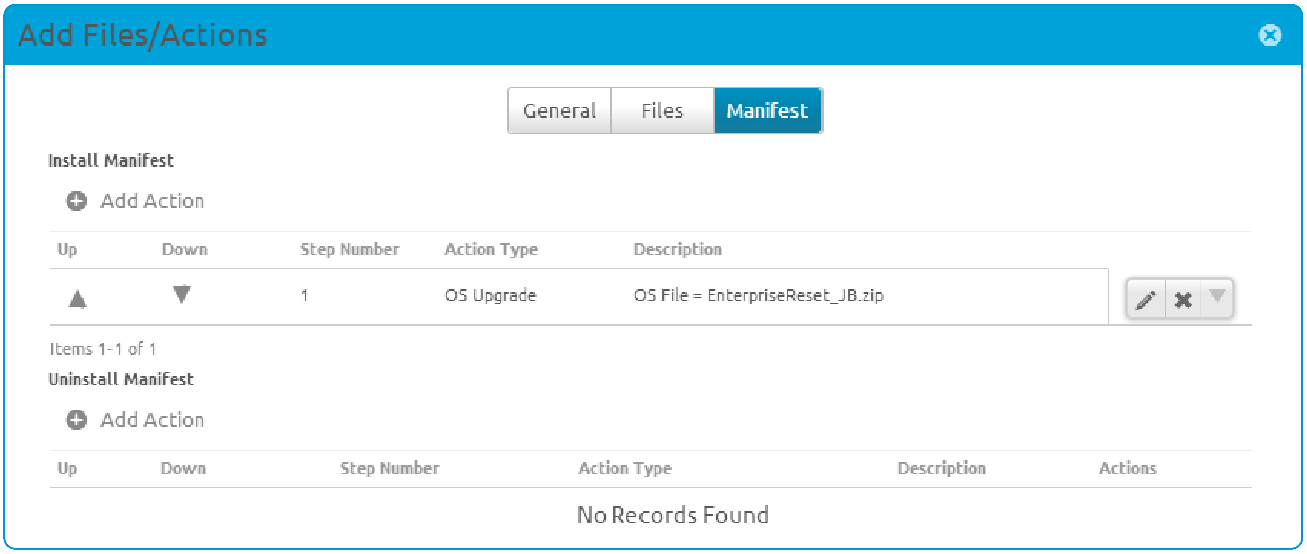


6. For Zebra devices, upload the following files and specify the path as `/data/tmp/`. For other devices, specify a known internal storage path on the device, such as `/sdcard/`.
   - OS Update zip file – This file can be a major or minor OS upgrade file. The file can also be an enterprise reset package.

- [optional] AirWatch Agent update package (apf) – This optional file can be specified in order to update the AirWatch Agent prior to initiating the actual OS update. AirWatch 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 should look similar to below:



Install Manifest

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

Items 1-1 of 1

Uninstall Manifest

Up	Down	Step Number	Action Type	Description	Actions

No Records Found

9. Select **Save**.

After creating an OS Upgrade file/action, create a product to push the upgrade to your devices. See Create a Product on page 57 for more information.

> **Note:** Before installing an OS Update, the device checks the battery level. If the level is below a threshold, the product will fail. This failure will display in the log.

Create a Honeywell Android OS Upgrade File/Action

Upgrade all of 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 manually update them.

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 AirWatch Service for Honeywell must be installed on the device.

Procedures

To upgrade Honeywell Android Rugged device OS:

1. Navigate to **Devices** > **Staging & Provisioning** > **Components** > **Files/Actions** and select **Add**. Create a file/action component. See Create a Files/Actions Component on page 33 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.

AirWatch Agent Upgrade File/Action

When you upgrade your devices, you can seed the AirWatch Agent in the AirWatch Console for use in products. The file/action AirWatch Agent Upgrade then grabs the list of seeded .apf files when creating a manifest action for products.

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

When using this upgrade option, you should be alert for failed upgrades. A failed upgrade can cause the product to push over and over again as the console recognizes the older agent version. This could 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 the settings are correct.

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

Upload the AirWatch Agent APF File

The Agent Package can be uploaded only in specific organization group types, for example, in organization groups of type ‘Customer’. It is recommended to upload the Agent Package at the highest organization group. You can find the file specific to your OEM located in AirWatch Resources.

To upload an APF file, follow these steps.

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

Arguments

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.examples.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.

- **$external$** – 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.

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 executes an install command to extract the settings from the XML file and install them on the device.

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

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

```
<?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>
```

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 and downgrade applications and remove them remotely.

Internal Applications silently push to the following devices:

- Concierge
- Zebra (MX)
- Unitech
- Getac
- Honeywell
- Intermec

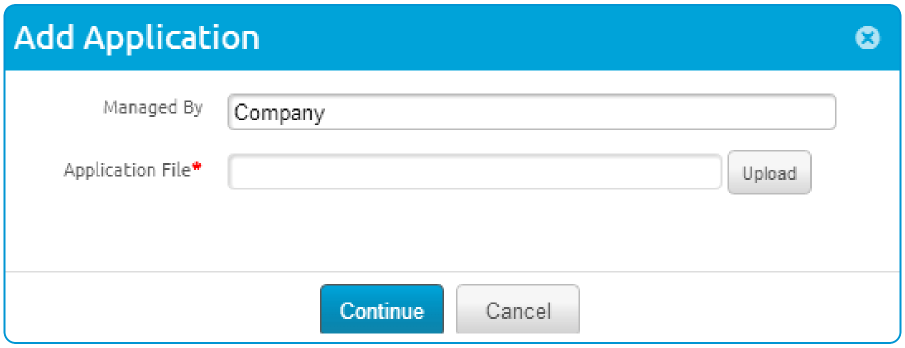
Note: Smart group assignment happens on the Product level and not on the Application level.

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.

To add an Application, follow the steps detailed below:

1. Navigate to **Devices > Staging & Provisioning > Components > Applications** and select **Add Application**.



Add Application

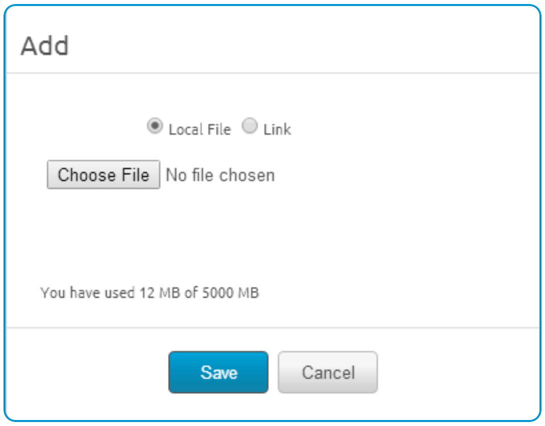
Managed By: Company

Application File*:

2. Enter who the application will be **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.



Add

● Local File ○ Link

No file chosen

You have used 12 MB of 5000 MB

5. Select **Save** to finish uploading the application.

6. Select **Continue** to add the application to the Product Provisioning application list.

For more information on adding applications, please consult the **Mobile Application Management Guide**.

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.

To add a new version of an app to a product, follow the steps detailed below.

1. Navigate to **Devices > Staging & 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 on page 43.

4. Select **Save**.

5. Navigate to **Devices > Staging & 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.

Downgrade Applications through Products

You can quickly rollback applications that have bugs or major issues through with product provisioning. Upload and assign multiple versions of the same application to devices to meet your organization needs.

Only Product Provisioning allows you to upload two versions of the same application as separate application items. Mobile Application Management through the AirWatch Console does not support this functionality.

To push previous versions of an app to a device through product provisioning, follow the steps detailed below:

1. Navigate to **Devices > Staging & Provisioning > Components > Applications** and select **Add Application**.
2. Upload the previous version of the application you want on devices. See Upload an Application on page 43 for more information.
3. Create a Product containing the downgrade version of the app. See Create a Product on page 57.
4. Activate the new product to push the downgrade version of the app to provisioned devices.

> **Important:** AirWatch recommends deactivating the product with the newer version of the app before activating the downgrade product. If both products are active at the same time, the products will attempt to keep pushing both versions.

Delete Applications

Remove unwanted applications from your products. AirWatch checks any attempt to delete an application against the list of active products.

In order to delete an application, it must be detached from all products.

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

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

Product Conditions

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

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

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

Conditions List View

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

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

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

Create a Condition

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

To create a condition, take the following steps.

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

Settings	Description
Name	Enter a name for the condition. The name cannot be longer than 255 characters.
Description	Enter a description for the condition.
Condition	The type of condition affects the parameters on the **Condition Details** tab. The following types are supported by this platform. • **Adapter Time** • **Confirm** • **Power** • **Schedule** • **SD Card Encryption**
Managed By	Select the organization group that manages the condition.

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

- **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 constrain 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	Choose 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.

Settings	Description
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**

- **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**

Settings	Description
Delay	
Delay (seconds)	Use this to delay for a specified time or until the end user makes a selection. If you enter a non-zero value, the prompt will wait for that value worth of seconds. If the end user does not make a selection in the time allowed, the condition is automatically considered not met. If a value of zero is entered, then the prompt will display indefinitely until the end user makes a selection.
Enable countdown?	This allows delay time to be “counted” down on the device so the end user knows how much time is remaining for the user to make a selection.

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

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

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

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

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

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

6. Select **Finish**.

Delete a Condition

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

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

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

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

Event Actions

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

In cases where you want to perform a device action only when certain conditions are met, event actions allow you to control the timing of these actions. For example, your devices could 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 could 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 control the recurrence of actions on a device. A product only processes once on a device. Event actions, however, process any time the conditions are met.

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

Create an Event Action

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

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

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 **Next**.
6. Select a **Condition** to trigger the device action.

   You can select a previously created condition or create a new one. To create a new condition, select **Create Condition** from the drop-down menu. For more information, see Create a Condition on page 46.

   - **Battery Threshold** – Choose to take action(s) for specified battery limit(s).
7. Select **Next**.
8. Complete the required option **Minimum Time Between Actions (hours)**. This option limits the number of times the action is triggered by the prescribed event.
9. Select an **Action** to perform. The actions available depend on the device platform.

Action	Description
Reboot	Restart the device.
Run Intent	Run command lines and arguments on the device. See Example RunIntent on page 41 for more information.

10. Select **Update** to add the action to the event action. You can add additional actions to the event action.
11. Select **Next**.
12. Review the **Summary** and select **Save**.

To push event actions to devices, add them as a component to a product. For more information, see Create a Product on page 57.

Custom Attributes Overview

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

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

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

Custom Attributes Database

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

Create Custom Attributes

Create a custom attribute and values to push to devices. You create the attributes and values associated with them. For more information, see Create Custom Attributes on page 53.

Importing Custom Attributes

The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to different parameters of custom attribute. For more information, see Custom Attributes Importing on page 53.

Platform-Specific Custom Attributes Provisioning

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

Create Custom Attributes

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

1. Navigate to **Devices > Staging & Provisioning > Custom Attributes > List View**.
2. Select **Add** and then select **Add Attribute**.
3. Under the **Settings** tab, enter an **Attribute Name**.
4. Enter the optional **Description** of what the attribute identifies.
5. Enter the name of the **Application** that will gather 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 AirWatch Console unless an Admin or an API call explicitly removes it. Otherwise, the attribute is removed as normal.

   If you delete a custom attribute that reported from a device to the AirWatch Console, a persisted custom attribute still remains in the AirWatch 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 AirWatch Console.

   For example, you could 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

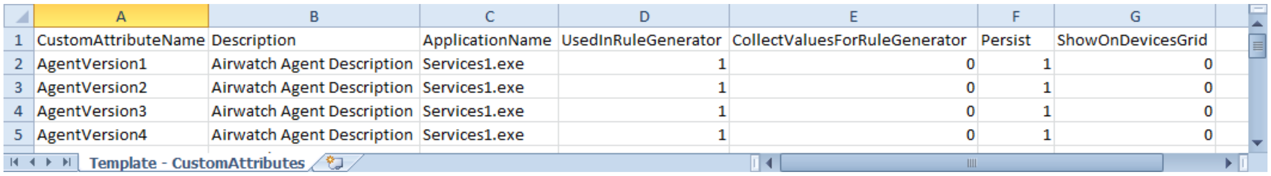
The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to different parameters of custom attribute.

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 proper syntax can cause database issues and result in loss of data.

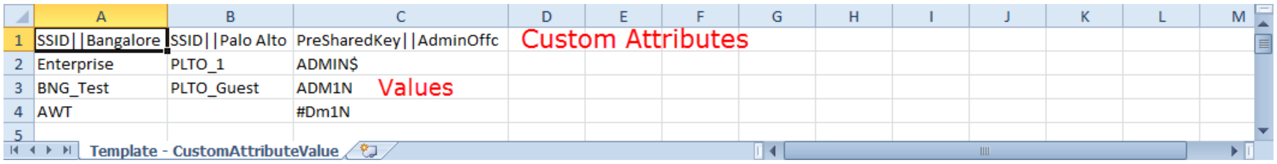
Template Types

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



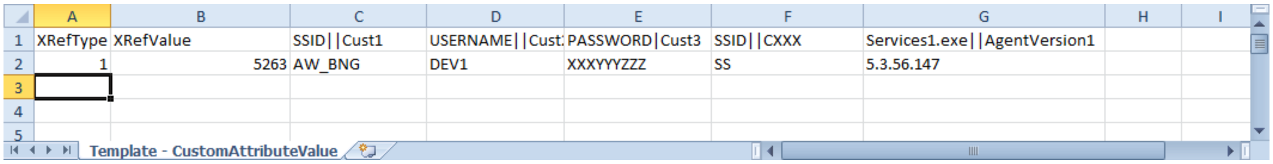
	A	B	C	D	E	F	G
1	CustomAttributeName	Description	ApplicationName	UsedInRuleGenerator	CollectValuesForRuleGenerator	Persist	ShowOnDevicesGrid
2	AgentVersion1	Airwatch Agent Description	Services1.exe	1	0	1	0
3	AgentVersion2	Airwatch Agent Description	Services1.exe	1	0	1	0
4	AgentVersion3	Airwatch Agent 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	D	E	F	G	H	I	J	K	L	M
1	SSID||Bangalore	SSID||Palo Alto	PreSharedKey||AdminOffc										
2	Enterprise	PLTO_1	ADMIN$										
3	BNG_Test	PLTO_Guest	ADM1N										
4	AWT		#Dm1N										
5													

- 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									

  - 1 – DeviceID (AirWatch assigned DeviceID when the device enrolls)
  - 2 – Serial Number
  - 3 – UDID
  - 4 – MAC Address
  - 5 – IMEI Number

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

Assign Organization Groups Using Custom Attributes

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

To create assignment rules, follow the directions below.

1. Ensure you are currently in a customer type organization group.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.
3. Set **Device Assignment Rules** to **Enabled**.
4. Set the **Type** to **Organization Group by Custom Attribute**.
5. Select **Save**.
6. Navigate to **Devices > Staging & Provisioning > Custom Attributes > List View > Add > Add Attribute** and create a custom attribute if you have not already done so. See Create Custom Attributes on page 53 for more information.
7. Navigate to **Devices > Staging & Provisioning > Custom Attributes > Custom Attributes Assignment Rules > Add Rule**.
8. Select the **Organization Group** to which the rule assigns devices.
9. Select **Add Rule** to configure the logic of the rule.

Setting	Description
Attribute/Application	This is the custom attribute with corresponding values for determining 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 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 intended to portray 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) may 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.
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 with an assigned attribute enrolls, the rule assigns the device to the configured organization group.

Android Custom Attributes

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

To begin collecting custom attributes, take the following steps.

1. Navigate to **Devices** > **Staging & Provisioning** > **Components** > **Files/Actions** > **Add** and select **Android** as your platform.
2. Create an XML provisioning file. See Create an XML Provisioning File on page 42. 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/**.

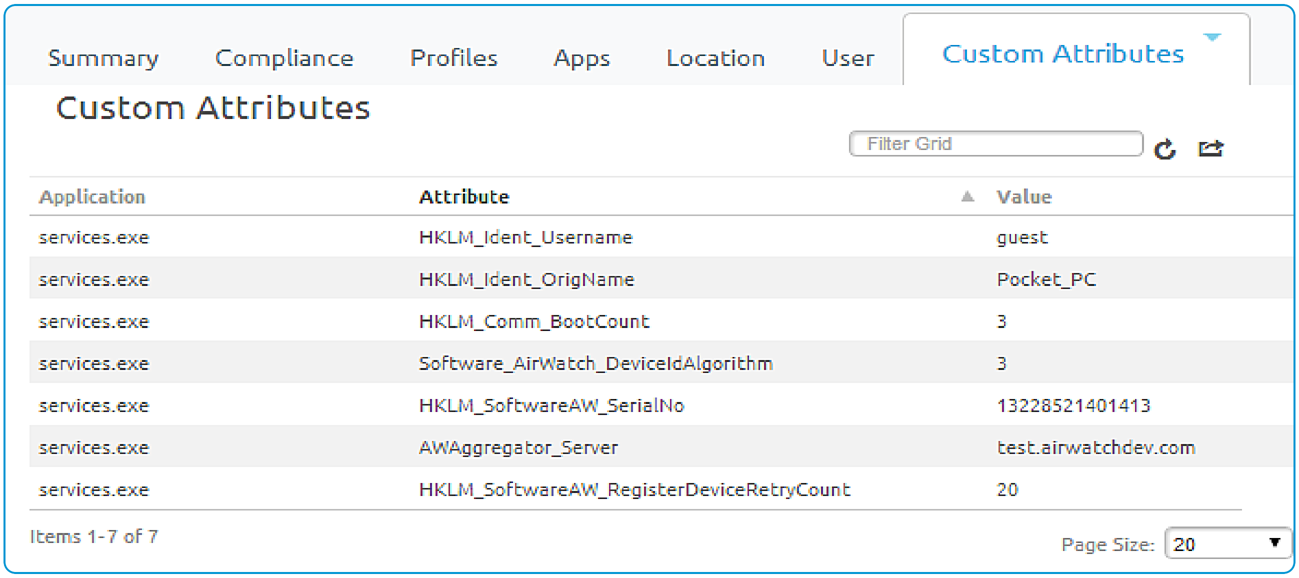
Upon receiving the XML file, the AirWatch Agent for Android creates a custom attributes output file.

During the next check-in with AirWatch, the agent sends the output file to the AirWatch 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 as well as the values returned from each device. These values can be used to create product assignment rules using the Custom Rules system.

Here is an example of the Android XML.

```
<?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

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

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.

In order to edit a product, the product must be deactivated in the list view first.

To create and configure a product.

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

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. This allows you to use system apps as well as third party apps that are not managed by AirWatch.

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 may use **Enter Manually** to enter the package ID of any application that should be present on the device. For more information see Custom Attributes Overview on page 52.

Setting	Description
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 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 intended to portray 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) may 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 Applications**. • **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.

Setting	Description
Persistent through Enterprise Reset	Select whether you want the Profile to be **Persistent through enterprise reset** or not. For more information, see Product Persistence on page 60.

Note: Profiles and files/actions that were selected to persist through an Enterprise Reset are stored in the flash memory of the device upon install. Once a device initiates the restore process from an Enterprise Reset and installs the AirWatch Agent, any persisted files/actions will be restored after Profiles are installed even if they were previously uninstalled. For more information, see Product Persistence on page 60.

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 may 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 AirWatch 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 AirWatch 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 fifty attempts before marking the product as failed and alerting you. If this is not enabled, the product will keep retrying indefinitely and will not alert you that there is an error.

Setting	Description
Device Policy Type	Determine if a product is **Required** or **Elective**. A required product provisions to assigned devices when deployment settings are met. An elective product is only provisioned when it is manually activated on the Device Details View of a provisioned device.

13. Select the **Dependencies** tab if you want to set the product to only provision devices that have other products provisioned as well.
    - Select **Add** to add a dependent product. You may add as many dependent products as you want.
14. Choose to deploy the product immediately by selecting **Activate** or wait to deploy later and select **Save**.

Product Persistence

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

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

Product Persistence for Android only applies to Motorola or Zebra devices.

Persistence works as follows:

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

   Staging configurations automatically persist on a device.
2. Set to persist any profiles, files/actions, or apps that you want to remain on the device after the enterprise reset.
3. The device resets when the Enterprise Reset command is sent (see Product Management). After resetting, the restore process starts.
4. The AirWatch Agent for the device reinstalls during the restore process.
5. After the agent is installed, any persisted profiles, such as Wi-Fi, reinstall.
6. Any persisted files/actions or apps will be reinstalled.

Product Sets

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

Product Sets Basics

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

The products in the product set follow a hierarchy based on ranking according to business needs. From a given product set, a device receives only one product that applies to the device. This product is the highest ranked product where the device meets the smart group and custom attribute rules criteria. Once a device receives a product from a product set, the device will not receive any other products from the set unless the rank of a subsequent product is elevated or a new product is created in the set with a higher rank.

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

Create a Product Set

Create a product set to control the delivery of multiple products so a device receives only the specific product that applies to the device based on your business rules. For more information, see Create a Product Set on page 61.

Product Set Management

Managing product sets includes more requirements and actions from you than other management functionality in the AirWatch Console. As product sets create complicated relationships between smart groups and products, removing and editing product sets cause multiple reactions for each action taken. For more information, see Product Sets Management on page 62.

Create a Product Set

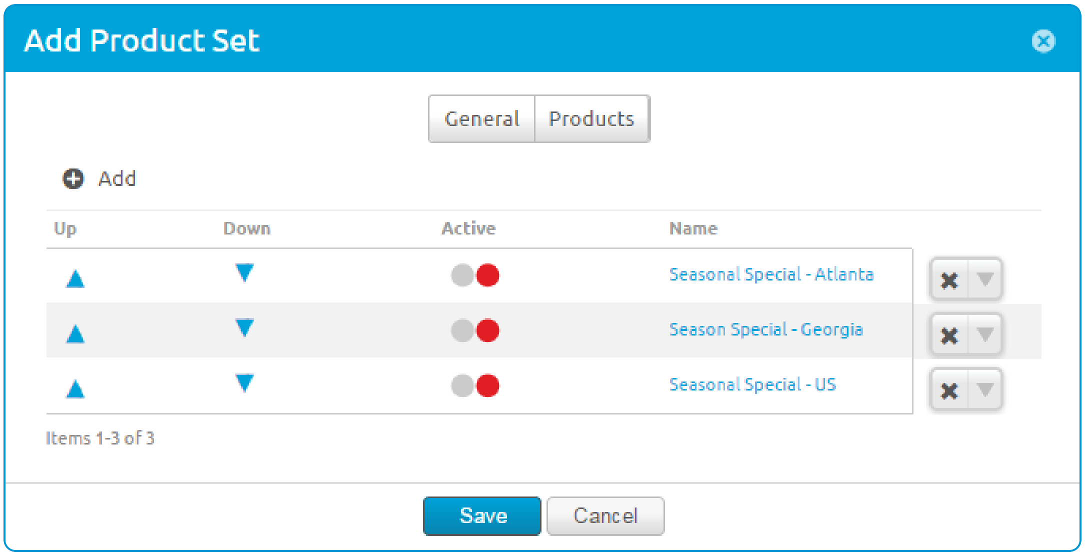
Create a product set to control the delivery of multiple products so a device receives only the specific product that applies to the device based on your business rules.

To create a product set, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Product Sets > Add Product Sets**.
2. Select the platform you want to create the product set for.
3. Complete the General fields.

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(s) including manifest items, conditions, and deployment settings. See Create a Product on page 57 for more information on creating a product. Ensure 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.



Up	Down	Active	Name
▲	▼	●	Seasonal Special - Atlanta
▲	▼	●	Season Special - Georgia
▲	▼	●	Seasonal Special - US

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 AirWatch Console. As product sets create complicated relationships between smart groups and products, removing and editing product sets cause multiple reactions for each action taken.

The actions that you can use to manage your product sets are:

- Product Sets in Device Details on page 62.
- Add a Product to a Product Set on page 63.
- Change the Product Ranking in a Product Set on page 63.
- Removing Products from Product Sets on page 64.

Activating and Deactivating Products in a Product Set

When you choose 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 will send a removal command to all devices with that product, and the next highest ranked product will be installed.
- Activating a product in a product set may 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 as well as 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. Note that not all of 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 fields display relevant product set information:

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

Add a Product to a Product Set

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

A new product in a product set is added with the lowest ranking in the set by default. If the new product should be a higher rank, you must edit the ranking. See Change the Product Ranking in a Product Set on page 63 for more information on what happens when product ranks are adjusted.

To add a product, take the following steps.

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

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

Change the Product Ranking in a Product Set

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

To change product ranking, take the following steps.

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

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

Reason for Edit	Effect of Edit
Adding a new product.	The new product is set at the lowest rank. You must manually change the rank of the new product as needed.
Changing rank of existing products	Increasing the rank (selecting **Up** arrow) of a product will decrease the rank of all subsequent products by one. Decreasing the rank (selecting **Down** arrow) of a product will increase 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 will be reassigned based on the new priority order. As a result, the AirWatch Console will send 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 automatically 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 will receive a new product based on the new rankings.

Removing Products from Product Sets

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

Removing a product from a product set automatically raises the rank of all products previously ranked below the removed product by one. If multiple products are removed, the remaining products are adjusted by one rank for each product removed. See Change the Product Ranking in a Product Set on page 63 for more information on what happens when product ranks are adjusted.

To remove a product, take the following steps.

1. Navigate to **Devices > Staging & Provisioning > Product Sets**.
2. Find the product set you want to add a product to and select the **Edit** icon (✎).
3. Select the **Products** tab.
4. Select the checkbox for each product you want to remove from the product set.
5. Select the **Delete** button to remove the products.

6. Manually adjust the product rank as needed according to your business needs.
7. Select **Save** to add the product to the product set.

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

Chapter 5:
Product Management

Products Dashboard

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

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

Recent Product Status

This chart displays the ten 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 is dependent on another product(s) installation before installing onto devices.
- Failed – The product reached maximum attempts to install on the device and is no longer attempting to install.

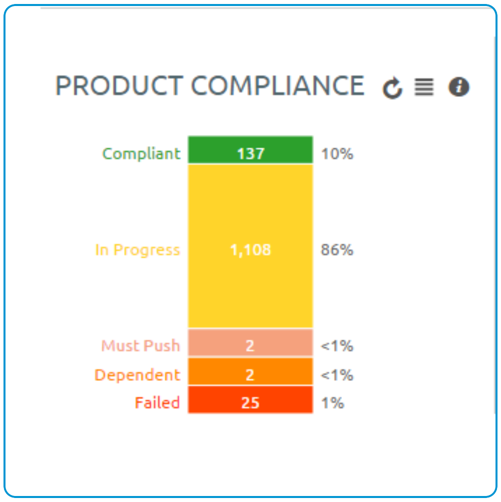
Filters

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. This information allows you to drill down to the Products List View that is filtered by the compliance status you select.



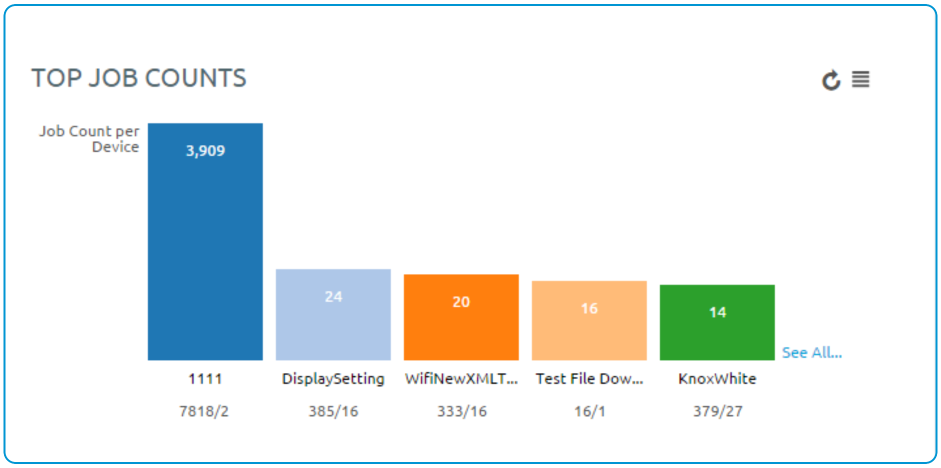
Filters

You can filter the Product Compliance chart to display specific device platforms that support product provisioning as well as the total percentage of each compliance status for a specific product(s).

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

Top Job Compliance

This chart displays a ratio of total job count to number of devices the product is provisioned to. This ratio gives you information on what products are having issues executing. For example, if the number shown is a 3, then you know that an average of 3 jobs per device happen 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 drill down further to find which jobs are failing and the reason for those failures.



Filters

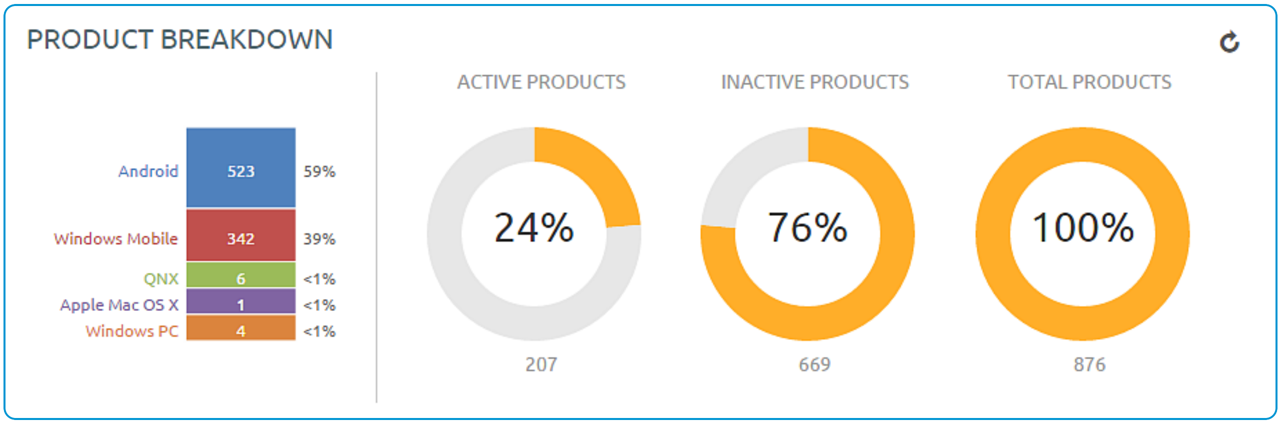
You can filter the Total Job Compliance chart to refer to specific device platforms that support product provisioning.

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 allows you to quickly see the products available for each platform.

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



Products List View

The Product List view allows you to view, edit, copy, and delete products as well as view the devices a product is provisioning.

Navigate to **Devices > Staging & Provisioning > Product List View**. This is the Products List View. Listed here are all the available products for the current organization group. The products can be sorted using the columns.

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

Actions

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

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

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

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

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

View Product

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

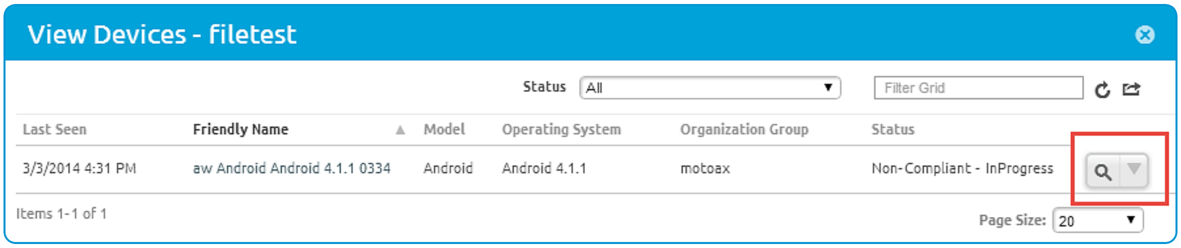
Select the **Edit** button to change any of the product settings.

View Devices

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

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

The **Log** listing shows the actions taken by the AirWatch Console to keep the product and device in sync.



View Devices - filetest

Status: All

Last Seen	Friendly Name	Model	Operating System	Organization Group	Status
3/3/2014 4:31 PM	aw Android Android 4.1.1 0334	Android	Android 4.1.1	motoax	Non-Compliant - InProgress

Items 1-1 of 1

Page Size: 20

Inherited Products

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

Products in the Device Details View

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

Products

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

Any product that fails to push to devices may 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 as well as the deployment status of the products.

The following fields 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

Navigate to **Devices > Details View > Apps** to access the Applications on the device.

Profiles

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

Product Job Statuses

Product provisioning works by handling each item in a product as a different job. As a product is pushed to a device, the AirWatch Console updates the current 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.

Job Status	Description
Paused	Job was previously started but a failure occurred. Job will resume before other jobs are processed.
Download Pending	The download is pending 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 the process was a success. Failed means the process failed.
Canceled	Job canceled while deferred or waiting.
Orphaned	Job being process by device uncompleted when jobs reprocessed. Job will automatically restart when able.
Deleted	The job was canceled by the user on the device.

Product Job Logs

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

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

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

Configure Targeted Job Log Collection

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

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

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

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

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

Define How Much Data to Collect

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

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

Job logs older than the selected number of days are purged from the AirWatch Console.

Perform an Enterprise Reset

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

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

To perform an Enterprise Reset, take the following steps.

1. Navigate to **Devices > List View** and select a device you want to Enterprise Reset.
2. On the Device Details View, select the **More Actions** button.

3. Select **Enterprise Reset**, located under Management section.
4. Enter your **Security Pin** in the **Restrict Action** prompt to perform the Enterprise Reset.

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.

Chapter 6:
Android Device Management

Product Management Overview

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

Product Management Basics

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

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

Product Dashboard

View and manage products from the Products Dashboard. The dashboard provides an easy method of viewing the status of your products and the devices they provision. The charts of information allow you to drill down to specific products or devices so you can remain informed about your device fleet. For more information, see Products Dashboard on page 67.

Products List View

The Product List view allows you to view, edit, copy, and delete products. From this view you can also see the devices assigned the product. For more information, see Products List View on page 68.

Device Details View

You can use the Device Details View to see the products, files/actions, apps, and profiles pushed to a device. For more information, see Products in the Device Details View on page 70.

Product Job Status

Product provisioning works by handling each item in a product as a different job. As a product is pushed to a device, the AirWatch Console updates the current status of each job to display any errors or issues are in the process. For more information, see Product Job Statuses on page 78.

Enterprise Reset

Enterprise Reset enables you to reset a device similar to an enterprise wipe, but with one important difference. Profiles and files/actions set to persist on a device are not removed and automatically reinstall on a device following the first reboot after an enterprise reset. For more information, see Perform an Enterprise Reset on page 72.

XML Provisioning

XML provisioning allows you to download a custom-designed XML file to a device in a provisioning product. After the file is downloaded, it executes an install command to extract the settings from the XML file and install them on the device. For more information, see Create an XML Provisioning File on page 42.

Device Dashboard

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

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

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

Device List View

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

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

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

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

Customize Device List View Layout

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

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

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You may 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.

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 AirWatch 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 AirWatch 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 AirWatch 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 AirWatch Agent 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 (More ▾).

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Security** – View current security status of a device based on security settings.
- **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.
- **Provisioning** – View complete history and status of all packages provisioned to the device and any provisioning errors.

- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Alerts** – View all alerts associated with the device.
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.
- **Status History** – View history of device in relation to enrollment status.
- **Management** – Lock or perform Enterprise Wipe on all selected devices.

  When you lock a SAFE 4 device, you can configure a customized lock screen. Set the **Message Template** to **Custom Message**. Then, in the **Message** field, provide your text and provide a **Phone Number**.
- **Support** – Send a message to email AirWatch Technical Support regarding selected device. Also, locate the device according to its current GPS location.
- **Admin** – Change AirWatch Console settings, including changing organization group of selected devices or deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices. Select **Provision Now** to perform a number of configurations for selected devices.

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 AirWatch Console updates the current 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. Job will resume before other jobs are processed.
Download Pending	The download is pending 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.

Job Status	Description
Completed/ Failed	Job processing complete. Complete means the process was a success. Failed means the process failed.
Canceled	Job canceled while deferred or waiting.
Orphaned	Job being process by device uncompleted when jobs reprocessed. Job will automatically restart when able.
Deleted	The job was canceled by the user on the device.

Product Job Logs

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

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

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

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire AirWatch 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 > Agent 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.

Remote Management

The Remote Management Service allows you to remotely connect to end-user devices so you can assist in troubleshooting and maintenance. The Remote Management Service requires your computer and the end user device to connect to the Remote Management Server to facilitate communication between the AirWatch Console and the end user device.

For more information on installing, configuring, and using the Remote Management Service, please see the **VMware AirWatch Remote Management Guide**, available on AirWatch Resources.

Overview Service Kit Overview

The OEM Service Kit is an additional app that allows AirWatch to provide extended management capabilities to any Android device.

The app uses platform key signing by the OEM to enable these features. AirWatch works with each Android device OEM to achieve this functionality. Here is a list of features and a list of the OEM Service Kits.

OEM Service Kit 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

OEM Service Kit Versions

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

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.