Windows Rugged Platform

VMware Workspace ONE UEM 2102

vmware®

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

https://docs.vmware.com/

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

Contents

The Windows Rugged Platform 1

Workspace ONE UEM provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Windows Rugged devices. Through the UEM console, you have several tools and features for managing the entire lifecycle of corporate and employee-owned devices.

Windows Mobile and Windows CE devices and their operating systems are proven performers in rugged environments like warehouses, courier services, and healthcare facilities. These devices represent most mobile devices in these environments and can perform many functions such as sales, inventory, scanners, and more. With the Workspace ONE UEM solution, you can manage these devices and integrate them with your other mobile platforms, which give you a central location for mobile device management.

Platforms Supported

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

Agents and Versions Supported

Consider using version 5.X.X of the Workspace ONE Intelligent Hub for Windows Rugged. Workspace ONE UEM no longer supports bug reports, code changes, or new enhancements for previous versions of the Workspace ONE Intelligent Hub for Windows Rugged.

Product Provisioning

Product provisioning in Workspace ONE UEM enables you to create products containing profiles, applications, files/actions, and event actions for Windows Rugged devices. These products follow a set of rules, schedules, and dependencies as guidelines for ensuring your devices remain up-to-date with the content they need.

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

For details, see the **Product Provisioning Documentation**, found on docs.vmware.com.

Windows Rugged Enrollment 2

Enroll Windows Rugged devices into Workspace ONE UEM to access internal content and features using Web enrollment. Web enrollment directs the user to an enrollment URL to complete enrollment and download the Workspace ONE Intelligent Hub for your devices.

Device enrollment is required for all Windows Rugged devices you want managed by Workspace ONE UEM.

If you use the Product Provisioning functionality, you can enroll your Windows Rugged devices through additional enrollment methods. These additional methods, including sideload staging, require product provisioning.

Enroll Windows Rugged Devices Through Web Enrollment

Simplify device enrollment with Web Enrollment instead of downloading the Workspace ONE Intelligent Hub manually. Send end users to a URL to enroll their devices into Workspace ONE UEM.

1 Go to the enrollment URL using the native browser on the device. This URL is built into your environment and is accessible by appending "/enroll/welcome" onto your active environment.

   For example, the Web Enrollment URL for mdm.saas.acme.com is the following:

   ```
   https://mdm.saas.acme.com/enroll/welcome
   ```

2 Enter the applicable Workspace ONE UEM solution information in the **Group ID**, **Username**, and **Password** text boxes.

3 Optionally, select the **Device Ownership** type (**Employee Owned**, **Corporate-Dedicated**, or **Corporate-Shared**) and select **Enroll**.

4 Accept the **Terms of Use** if this option is configured.

5 Select **Accept** to download the Workspace ONE Intelligent Hub to the device.

6 Select **Continue** to complete the enrollment.

Unenroll Windows Rugged Devices

When the time comes to unenroll a device from Workspace ONE UEM, ensure that you select the best method for your situation. Unenroll devices using enterprise wipe from the UEM console or remove the Workspace ONE Intelligent Hub from the Windows Rugged device.

Enterprise wipe enables you to clear corporate data, applications, and profiles from a device without removing personal data. This action enables you to unenroll an employee-owned device without clearing the personal data.

1 Navigate to **Devices > List View** and select the Windows Rugged device you want to unenroll.

2 From the Device Detail page, select the **More** option.

3 Select the **Enterprise Wipe** option under **Management**.

4 Enter your Admin PIN and confirm the Enterprise Wipe.

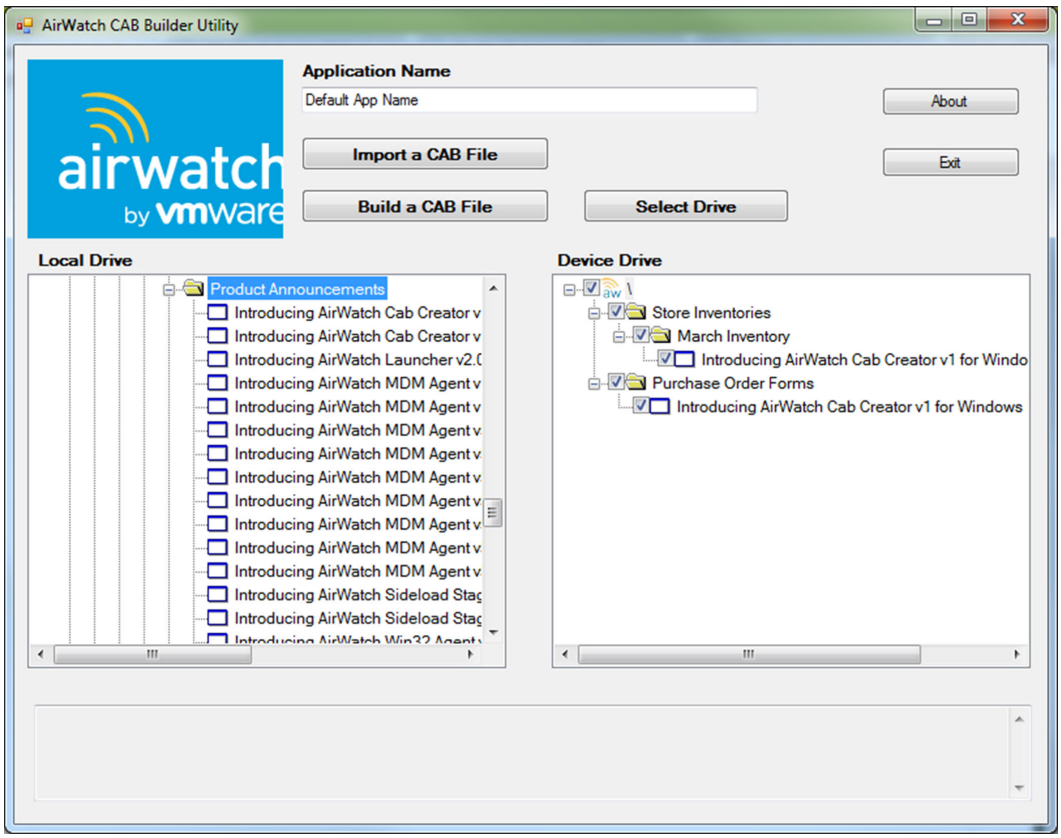
The device undergoes an enterprise wipe to remove corporate data and unenroll the device from Workspace ONE UEM.

AirWatch Cab Creator for Windows Rugged

The AirWatch Cab Creator allows you to create custom CAB files for use on Windows Rugged devices under Workspace ONE UEM. These custom CAB files consist of files and applications you add from your computer.

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

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



Create a Custom CAB

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

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

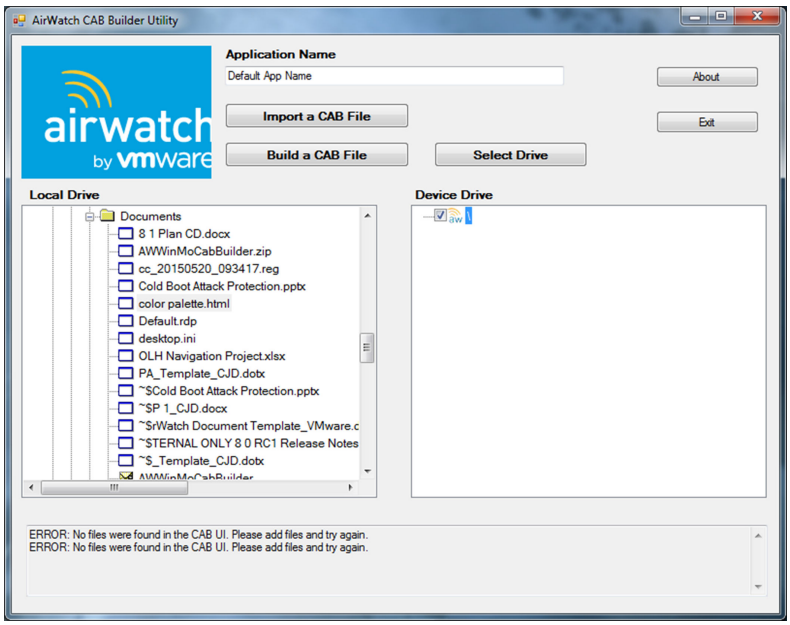
- A Windows device running Windows 7+
- .NET Framework 4.5

Take the following steps to create a custom CAB.

1 Download the "AirWatch Cab Creator" for Windows Rugged from the MyWorkspaceONE portal.

2 Unzip the file to your preferred directory.

3 Double-click CabBuilder.exe to start the app.



4 Navigate to a file on your **Local Drive** you want to add to the custom CAB file. You can select a different drive by selecting **Select Drive**.

5 Enter an **Application Name**. This text box is the name of the CAB file after installation.

Remember the name for use in Uninstall Manifest items.

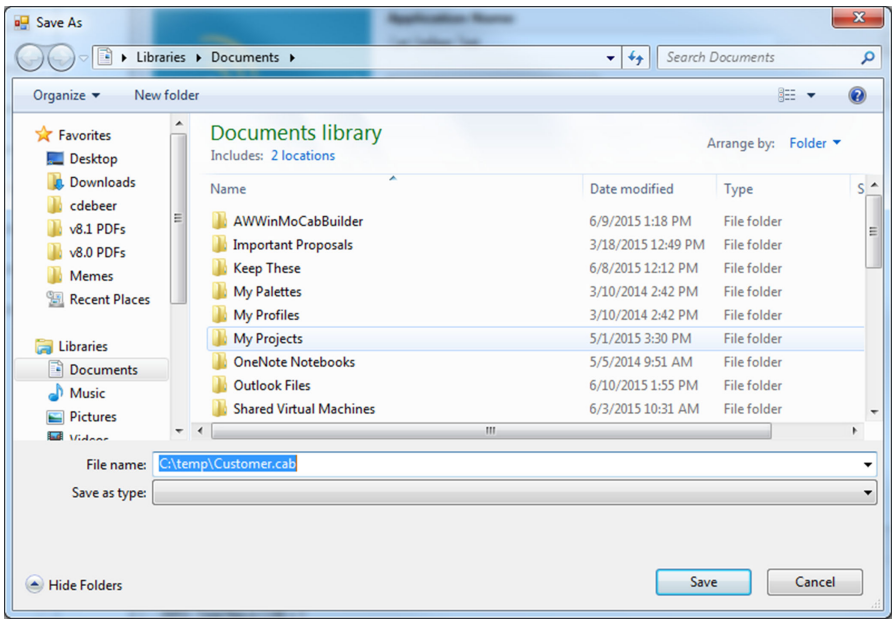
6 Select the file and drag it to the **Device Drive** pane.

To create a folder on the device drive, right-click the root drive and select **Add Folder**.

7 Repeat Step 5 for each file or application you want to add to the custom CAB file.

8 **OPTIONAL:** Add an existing CAB file to your custom CAB file by selecting **Import a CAB File**.

9 Select **Build a CAB File** to save the CAB file and select a name for the file.



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

Windows Rugged Profiles

3

Profiles are the primary means to manage devices in Workspace ONE UEM. Configure profiles so your Windows Rugged devices remain secure and configured to your settings.

Overview

You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices.

The individual settings you configure, such as the settings for Wi-Fi, VPN, and passcodes, are called payloads. Consider associating only one payload per profile. Create multiple profiles for the different settings you want to establish.

Device Access

Some device profiles configure the settings for accessing a Windows Phone device. Use these profiles to ensure that access to a device is limited only to authorized users.

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Create a Passcode Profile (Windows Rugged).
- Configure the device launcher and layout. For more information, see Launcher Profile (Windows Rugged).

Device Security

Ensure that your Windows Phone devices remain secure through device profiles. These profiles configure the native Windows security features or configure corporate security settings on a device through Workspace ONE UEM.

Some examples of device security profiles include:

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see Dynamic Wi-Fi Profiles (Windows Rugged).

- Ensure access to internal resources for your devices with the VPN profile. For more information, see Create a VPN Profile (Windows Rugged).

Device Configuration

Configure the various settings of your Windows Phone devices with the configuration profiles. These profiles configure the device settings to meet your business needs.

Some examples of device configuration profiles include:

- Set up an Exchange account on a device with an Exchange ActiveSync profile. For more information, see Configure an Exchange ActiveSync Profile (Windows Rugged).
- Configure the device time zone. For more information, see Create a Time Zone Profile (Windows Rugged).

Profiles and Product Provisioning

If you plan on using these profiles for product provisioning, see the topic "Profiles for Product Provisioning" in the **Product Provisioning** documentation in docs.vmware.com.

This chapter includes the following topics:

Create a Passcode Profile (Windows Rugged)

Deploy a Passcode payload to require users to protect their devices with passcodes each time they return from an idle state in Workspace ONE UEM powered by AirWatch. This action ensures that all sensitive corporate information on managed devices remains protected.

Important Passcode payloads apply only to Windows Rugged devices and not Windows CE devices.

Procedure

1. Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.
2. Select **Windows Rugged**.
3. Configure the profile's **General** settings.
4. From the left panel, select the **Passcode** payload and click the **Configure** button.
5. Configure the Passcode settings:

Settings	Descriptions
Maximum Passcode Age	Requires users to renew passcodes at selected intervals.
Passcode	Sets a specific passcode for the device.
Maximum Passcode Length	Sets the maximum number of characters for your passcode.
Minimum Passcode Length	Sets the minimum number of characters for your passcode.
Minimum Number of Upper Case Letter	Sets the minimum number of upper case letters a passcode must contain.
Minimum Number of Lower Case Letter	Sets the minimum number of lower case letters a passcode must contain.
Minimum Number of Numerical Digits	Sets the minimum number of numerical digits a passcode must contain.
Grace period for device lock	Specifies a period of inactivity before locking a device.
Maximum Number of Failed Attempts	Sets a limit on failed passcode attempts before wiping a device.

6. Select **Save & Publish** to push the profile to devices.

Create a Restrictions Profile (Windows Rugged)

Deploy a Restrictions payload to restrict the options end users have on devices in Workspace ONE UEM powered by AirWatch. Restrictions allow you to ensure that your device is secure by controlling what an end user can use to save and store data.

Important You can use a Restriction payload only on Windows Rugged devices and not on Windows CE devices.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Restrictions** payload and click the **Configure** button.

5 Configure the Restrictions settings.

Settings	Descriptions
Allow Camera.	Allow access to the camera application.
Allow External Storage.	Allow use of external storage memory.
Remove Encryption on External Storage.	Allow the removal of encryption on external storage.
Enable On-Device Encryption.	Allow encryption on the device.
Allow Bluetooth.	Allow the use of Bluetooth.

6 Select **Save & Publish** when you are finished to push the profile to devices.

Dynamic Wi-Fi Profiles (Windows Rugged)

Using custom attributes, you can create dynamic Wi-Fi profiles in Workspace ONE UEM powered by AirWatch that allow you to configure device Wi-Fi settings across smart groups and OGs without creating multiple profiles. The custom attributes can use device-side values or override device values with a specific value.

This feature works best when managing many different Wi-Fi networks across your mobile fleet. When updating the access credentials for all your Wi-Fi networks, import a batch of custom attributes (using the .csv batch import process). Using the Device Custom Attribute Values template, you can upload specific values to individual devices. This process allows you to update the credentials across your mobile fleet quickly without having to create hundreds of different Wi-Fi profiles.

Dynamic Wi-Fi profiles allow you to specify certain text boxes in the profile as a dynamic value. For example, the **Service Set Identifier** can be set to a dynamic value so devices can use their own value as opposed to one service set identifier per profile. If you have devices in one OG that use different Wi-Fi credentials, use dynamic Wi-Fi profiles to create one profile that configures the different settings required.

To use a custom attribute in your Wi-Fi Profile, enable the check box next to a text box. Enabling the text box allows you to select the custom attribute, enter a default value, and set the default value to override device values for the attribute.

For more information on custom attributes and instructions for creating them, see Chapter 6 Custom Attributes.

Configure a Wi-Fi Profile (Windows Rugged)

Create a Wi-Fi profile in Workspace ONE UEM powered by AirWatch to connect devices to hidden, encrypted, or password-protected corporate networks. Wi-Fi profiles are useful for end users who need access to multiple networks or for configuring devices to connect automatically to the appropriate wireless network.

Important Zero Wireless Config is not available for Windows CE devices except Psion CE devices. You can provision Wi-Fi profiles using Zero Wireless Config to Psion CE devices only but not any other Windows CE devices.

Procedure

1. Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.
2. Select **Windows Rugged**.
3. Configure the profile's **General** settings.
4. From the left panel, select the **Wi-Fi** payload and click the **Configure** button.
5. Configure the Wi-Fi settings:

Settings	Descriptions
Network Adapter Type	Select the adapter type. ■ Standard Microsoft (Zero Wireless Config). ■ Motorola Fusion – For more information, see Configure a Motorola Fusion Wi-Fi Profile (Windows Rugged). ■ Honeywell DeviceScope – Network Adapter Type for Honeywell devices.
Service Set Identifier	Enter an identifier that is associated with the name (SSID) of the desired Wi-Fi network.
Wi-Fi Meta Network	Select whether you are connecting through a proxy with **Work** or connecting directly to the **Internet**.
RFBand	Honeywell Network Adapter Type only.
IP Addressing Mode	Select the type of IP Addressing mode used.
Operating Mode	Select the type of operating mode used.
Security Type	Select your Wi-Fi security type. The type selected determines which additional text boxes display.
Authentication Type	Select the Authentication type to be used with enterprise applications.
Encryption	Select the encryption type for traffic over the Wi-Fi connection.
Pre Shared Key	Enter the Pre Shared Key for your Wi-Fi. Displays when **Security type** is set to **WPA Personal** or **WPA2 Personal**.
Domain Name	Enter the Domain name for your certificates. Displays when **Security type** is set to **WPA Enterprise** or **WPA2 Enterprise**.
Username	Enter the user name for the domain. Displays when **Security type** is set to **WPA Enterprise** or **WPA2 Enterprise**.

Settings	Descriptions
Password	Enter the password used for the domain. Displays when **Security type** is set to **WPA Enterprise** or **WPA2 Enterprise**.
Identity Certificate	Select the certificate used to identify the end user to the server.
Server Certificate	Select the certificate used to identify the server to the end user.

6 Select **Save & Publish** to push the profile to devices.

Configure a Motorola Fusion Wi-Fi Profile (Windows Rugged)

The Windows Rugged Wi-Fi profile in Workspace ONE UEM powered by AirWatch allows you to specify the network adapter to support the Motorola Fusion type of network adapter. These settings allow you to control when and how often the device connects to Wi-Fi.

The settings differ based on the Motorola adapter type selected.

Note The settings that follow are based on the specific Motorola adapter type selected.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Wi-Fi** payload and click the **Configure** button.

5 Configure the Wi-Fi settings.

Settings	Descriptions
Network Adapter Type	Set to Motorola Fusion. For other adapter types, see Configure a Wi-Fi Profile (Windows Rugged).
Motorola Adapter Type	These options change the text boxes available. Text boxes that are tied to a specific Motorola adapter type are noted. Scroll down to view the settings specific to the WLAN of your choice, WLANFusionPublic, WLANFusion3xPublic, and WLANFusionX2Public.
Set Fusion Options.	Set to **Yes** to list extra network options.
Enable 80211d.	Set to **Change** to enable 802.11d wireless specification for operation in extra regulatory domains.
Change Regulatory Country Code	Set to **Change** to select the Country Code for the device.
Set RFBand	Set to **Change** to specify the RF Band for the device.
Enable Auto Time Config.	Set to **Change** to enable automatic time configuration.
Set FAPI Access Password	Set to **Change** to select a FAPI access code.
Set FAPI Access Code	Enter the FAPI Access Code you want for the device.

Settings	Descriptions
Set Profile Configuration	Set to **Yes** to set the profile settings.
Service Set Identifier	Identifies the wireless network to be connected. This text box includes an option to set its value dynamically with custom attributes. You can also use lookup values. For more information, see Chapter 8 Lookup Values.
Profile Country Code	Enter the country code to use with the profile.
Wi-Fi Meta Network	Select whether you are connecting through a proxy with **Work** or connecting directly to the **Internet**.
IP Addressing Mode	Select to use **DHCP** or **Static** IP Addressing. If you select **Static**, enter the settings for your static IP address.
Disable all other Profiles.	Set to **Yes** to disable all other Wi-Fi profiles on the device.
Operating Mode	Select the operating mode.
Transmit Power Level.	Select the transmit power level.
Power Level	Select the balance of power use.
Security Type	Select the encryption type for the network connection.
Authentication Type	Select an authentication type to be used with enterprise applications. Additional text boxes display depending on the type selected. The FAST authentication types (EAP-FAST-MSCHAPV2, EAP-FAST-TLS, and EAP-FAST-GTC) add the following additional text boxes: ■ **Auto PAC Refreshing** ■ **Auto PAC Provisioning** ■ **PACFile Name** ■ **PACFile Password** ■ **Use GTC Token**
Encryption	Select the encryption type used for the Wi-Fi connection.
Pre Shared Key	Enter the Pre Shared Key used for the Wi-Fi Connection.
Change CCKM Setting.	Enable to change the CCKM Mode.
Domain Name	Enter the domain name used in authentication.
User name	Enter the user name used for authentication.
Password	Enter the password used for authentication.
Identity Certificate	Set to **Other** and enter the certificate name used for authentication.
Server Certificate	Set to **Other** and enter the certificate name used for authentication.
Set Fusion Options.	Set to **Yes** to list extra network options.
Enable 80211d.	Set to **Change** to enable 802.11d wireless specification for operation in additional regulatory domains.
Change Regulatory Country Code	Set to **Change** to select the Country Code for the device.
Set RFBand	Set to **Change** to specify the RF Band for the device.
Enable Auto Time Config.	Set to **Change** to enable automatic time configuration.
Set FAPI Access Password	Set to **Change** to select an FAPI access code.

Settings	Descriptions
Set FAPI Access Code	Enter the FAPI Access Code for the device.
Set WLAN Management Mode	Set to **Change** to configure the WLAN Management Mode settings.
WLAN Management Mode	Select either the **Wireless Zero Config** or **Fusion Management State** modes.
Set Profile Configuration	Set to **Yes** to set the profile settings.
Handle Error By.	Select to **Ignore Error** or **Stop On Error**.
Set Current Management Mode Option	Set to **Change** to configure the management mode.
Apply Profile Regardless of Device's Current Management Mode Configuration.	Enable to apply the Wi-Fi profile regardless of current management mode.
Service Set Identifier	Enter the identification of the wireless network the device connects with.
Profile Country Code	Enter the country code to use with the profile.
Wi-Fi Meta Network	Select whether you are connecting through a proxy with **Work** or connecting directly to the **Internet**.
IP Addressing Mode	Select to use **DHCP** or **Static** IP Addressing. If you select **Static**, enter the settings for your static IP address.
Disable all other Profiles.	Set to **Yes** to disable all other Wi-Fi profiles on the device.
Operating Mode	Select the operating mode. **Transmit Power Level**: Select the transmit power level. **Adhoc Channel**: Select the Ad Hoc channel the devices use. **Encryption**: Select the encryption type for the Wi-Fi network. **Pre Share Key**: Enter the Pre Shared Key used for the network.
Transmit Power Level.	Select the transmit power level.
Power Level	Select the balance of power use.
Security Type	Select the encryption type for the network connection.
Pre Shared Key	Enter the Pre Shared Key used for the Wi-Fi Connection.
Change CCKM Setting.	Enable to change the CCKM Mode.
Domain Name	Enter the domain name used in authentication.
User name	Enter the user name used for authentication.
Password	Enter the password used for authentication.
Identity Certificate	Set to **Other** and enter the certificate name used for authentication.
Server Certificate	Set to **Other** and enter the certificate name used for authentication.
Enable 80211d.	Set to **Change** to enable 802.11d wireless specification for operation in additional regulatory domains.
Set RFBand	Set to **Change** to specify the RF Band for the device.
Enable Auto Time Config.	Set to **Change** to enable automatic time configuration.
Set FAPI Access Password	Set to **Change** to select an FAPI access code.
Enable IPv6.	Set to **Change** to enable IPv6 settings.

Settings	Descriptions
Set WLAN Management Mode	Set to **Change** to configure the WLAN Management Mode settings.
WLAN Management Mode	Select either the **Wireless Zero Config** or **Fusion Management State** modes.
Enable FIPS Mode.	Set to **Change** to enable FIPS mode.
Change PreAuth	Enable PreAuth to allow access points to authorize devices before they officially switchover to the new access point.
Reset Fusion Options.	Set to **Reset** to reset the device's Fusion options when pushing this profile to the device.
Reset Fusion Data Store	Set to **Reset** to reset the Fusion data store on a device.
Set Profile Configuration	Set to **Yes** to set the profile settings.
Handle Error By.	Select to **Ignore Error** or **Stop On Error**.
Service Set Identifier	Enter the identification of the wireless network the device connects with.
Profile Country Code	Enter the country code to use with the profile.
Wi-Fi Meta Network	Select whether you are connecting through a proxy with **Work** or connecting directly to the **Internet**.
IP Addressing Mode	Select to use **DHCP** or **Static** IP Addressing. If you select **Static**, enter the settings for your static IP address.
Disable all other Profiles.	Set to **Yes** to disable all other Wi-Fi profiles on the device.
Operating Mode	Select the operating mode. ■ **Transmit Power Level**: Select the transmit power level. ■ **Adhoc Channel**: Select the Ad Hoc channel the devices use. ■ **Encryption**: Select the encryption type for the Wi-Fi network. ■ **Pre Share Key**: Enter the Pre Shared Key used for the network.
Transmit Power Level.	Select the transmit power level.
Power Level	Select the balance of power use.
Security Type	Select the encryption type for the network connection.
Pre Shared Key	Enter the Pre Shared Key used for the Wi-Fi Connection.
Change CCKM Setting.	Enable to change the CCKM Mode.
Domain Name	Enter the domain name used in authentication.
User name	Enter the user name used for authentication.
Password	Enter the password used for authentication.

6 After setting the Motorola adapter type specific settings, select **Save & Publish** to push the profiles to devices.

Exchange ActiveSync Profiles (Windows Rugged)

The Exchange ActiveSync profiles enable you to configure your Windows Rugged devices in Workspace ONE UEM to access your Exchange ActiveSync server.

Strongly consider only using certificates signed by a trusted third-party certificate authority (CA). Mistakes in your certificates expose your otherwise secure connections to potential man-in-the-middle attacks. Such attacks degrade the confidentiality and integrity of data transmitted between product components, and might allow attackers to intercept or alter data in transit.

The Exchange ActiveSync profile supports the native mail client for Windows Desktop. The configuration changes based on which mail client you use.

Important You can use an EAS payload only on Windows Mobile devices and not on Windows CE devices.

Configure an Exchange ActiveSync Profile (Windows Rugged)

Create an Exchange ActiveSync profile to give Windows Phone devices access to your Exchange ActiveSync server for email and calendar use.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Exchange ActiveSync** payload and click the **Configure** button.

5 Configure the Exchange ActiveSync settings.

Settings	Descriptions
Domain	Enter the domain for the Exchange account. You can use lookup values to create dynamic profiles. For more information, see Chapter 8 Lookup Values.
Exchange ActiveSync Host	Enter the hostname or IP address for the Exchange ActiveSync server.
User	Enter the user name for the Exchange account. You can use lookup values to create dynamic profiles.
Use SSL.	Enable to send all communications through the Secure Socket Layer.
Max Body Truncation	Select the maximum amount an email body is truncated in bytes.
Past Days of Calendar to Sync	Enter the number of days of Calendar events to download when the account syncs for the first time on the device.
Past Days of Mail to Sync	Enter the number of days of emails to download when the account syncs for the first time on the device.
Max HTML Truncation	Select the level of truncation for HTML emails.
Max Email Truncation	Select the maximum amount an email is truncated in bytes.
Max Email File Attachment Size (MB)	Select the max size (in MB) that a file can be when attached.
Allow Sync When Roaming.	Enable to allow the email client to sync when the device is roaming.

Settings	Descriptions
Allow Calendar Sync.	Enable to allow the syncing of calendars.
Allow Contacts Sync.	Enable to allow the syncing of contacts.
Allow Tasks.	Enable to allow the syncing of tasks.
Allows Text Messages	Enable to allow the syncing of text messages.
Allow Email Sync.	Allow the syncing of email. Disabling this setting removes access to email through Exchange Active Sync.
Sunday	Enable to allow schedule of syncing on Sundays.
Monday	Enable to allow schedule of syncing on Mondays.
Tuesday	Enable to allow schedule of syncing on Tuesdays.
Wednesday	Enable to allow schedule of syncing on Wednesdays.
Thursday	Enable to allow schedule of syncing on Thursdays.
Friday	Enable to allow schedule of syncing on Fridays.
Saturday	Enable to allow schedule of syncing on Saturdays.
Peak Start Time	Select the start time of the peak time period.
Peak End Time	Select the end time of the peak time period.
Sync Schedule Peak	Select what level of syncing happens during the peak time period.
Sync Schedule Off Peak	Select what level of syncing happens outside the peak time period.

6 Select **Save & Publish** to push the profile to devices.

Credentials Profile (Windows Rugged)

A Credentials profile allows you to push Root, Intermediate, and Client certificates to support any Public Key Infrastructure (PKI) and certificate authentication use case. The profile pushes configured credentials to the proper credentials store on the Windows Rugged device in Workspace ONE UEM.

Even with strong passcodes and other restrictions, your infrastructure remains vulnerable to brute force, dictionary attacks, and employee error. For greater security, you can implement digital certificates to protect corporate assets. To use certificates in this way, you must first configure a Credentials payload with a certificate authority, and then configure your Wi-Fi and VPN payloads. Each of these payloads has settings for associating the certificate authority defined in the Credentials payload.

Create a Credentials Profile

A Credentials profile pushes certificates to devices for use in authentication. With Workspace ONE UEM, you can configure credentials for intermediate, trusted root, trusted publisher, and trusted people certificate stores.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Credentials** payload and click the **Configure** button.

5 Configure the Credentials settings.

Settings	Description
Credential Source	Use the drop-down menu to select either **Upload** or **Defined Certificate Authority**.
Credential Name	Enter a name for the credentials certificate. Displays if the **Credential Source** is **Upload**.
Certificate	Select **Upload**, navigate to the desired credential certificate file, and select **Save**. Displays if the **Credential Source** is **Upload**.
Certificate Authority	Use the drop-down menu to select a predefined certificate authority. Displays if the **Credential Source** is **Define Certificate Authority**.
Certificate Template	Use the drop-down menu to select a predefined certificate template specific to the selected certificate authority. Displays if the **Credential Source** is **Define Certificate Authority**.
Store Location	Use the drop-down menu to select to save the certificate on the specific user account level or on the Computer Store for all users of a computer.
Certificate Store	Select the certificate store folder location from the drop-down menu. ■ Trusted Root Certification Authorities ■ Trusted Publishers ■ Untrusted Certificates ■ Trusted People

6 Select **Save & Publish** to push the profile to devices.

Launcher Profile (Windows Rugged)

The Workspace ONE UEM App Launcher restricts user access to a list of allowed applications and native features on the device. Use the App Launcher to control the apps available to end users and the layout of the device home screen.

The Launcher profile enables you to customize the look and layout of the Windows Rugged device home screen. You can configure the launcher profile to start when the device starts to limit end-user access to the entire device. To limit end-user access to the correct apps on a shared device, you can set the launcher profile to display based on the user group of the end user. This functionality allows you to tailor the launcher to the role of the end user using a shared device.

Customize the launcher to display different settings and apps based on the layout you want. To manage the device, the launcher profile includes different tools for admins to troubleshoot the device.

Create a Launcher Profile

Configure the Workspace ONE UEM App Launcher profile to customize the layout and apps of a Windows Rugged device using the App Launcher. This customization allows you to control end-user access to the device settings and applications based on the roles of the user.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Workspace ONE Launcher** payload and click the **Configure** button.

5 Enter a **Title** for the Workspace ONE Launcher profile. You can use the supported Workspace ONE UEM Lookup Values. Select the plus sign **(+)** for a list of all Workspace ONE UEM supported Lookup Values. For more information, see Chapter 8 Lookup Values.

6 Define an **Administrative Passcode** for setting configurations on the device.

7 Define the **User Category** of the end user if Shared Devices are enabled in the Windows Rugged Hub Settings page. The user category ties end users to specific Launcher profiles allowing you to tailor Launcher layout and configuration to individual end users. Consider creating user groups based on the end user's role.

8 Configure the remaining options:

Settings	Descriptions
Application Name	Specifies the application name that displays in the Workspace ONE UEM App Launcher.
File Path to Exe	Defines the file path of the application and includes the executable file.
Arguments	Enter any command-line arguments to run the application.
Hide	Masks the application on the device.
Launch On Start	Starts the application when the Workspace ONE UEM App Launcher starts. For best results, enable this option for a single application.
Start Up Options	Select the condition that triggers the launcher starting.
Delayed Launch	Select the time (in seconds) that the launcher is delayed from starting following device boot. This setting requires **Start Up Options** to be set to **Delayed Start**.
Console Application	Defines the application as not having a user interface or as a background process.
Tools Menu	Lists applications on the Tools menu for the App Launcher.
Background Application	Select if the application requires no user interaction and you want it to run in the background.
Disable App Close	Removes the close button from the application preventing the user from closing the app. Select this option only for dedicated use applications.

Settings	Descriptions
Enable Home Button.	Allows you to minimize an allowlisted application and return to the main App Launcher page while keeping the current session active for that app. If you want to return to the minimized app, select the icon on the App Launcher screen.
Application Icon Path	Defines the path to the location of the application icon that resides on the device. If the desired icon does not reside on the device, then you can upload an image.
Upload Icon	Allows you to upload an image (icon) that can be associated to an application by entering the path in the Application Icon Path text box.
View Time	Displays the time for application processes.
Disable Active Sync.	Disables the use of the Exchange ActiveSync protocol for application transactions.
Disable Keyboard.	Disables the use of the device keyboard to perform application processes.
View IP Address	Displays the device's IP address within application processes.
Enable Native Taskbar.	Uses the default taskbar for that device instead of the custom launcher taskbar. *When selected, these settings are disabled except for **View Time**, **Disable Active Sync**, **Disable Keyboard**, and **View IP Address**. These exceptions exist because the native taskbar only displays the icons/settings that are available to that device.
View Connection Status	Displays the connection status of the device.
Show Message Notification	Displays a message indicator for unviewed messages from a third-party application.
Display Organization Group	Displays the Organization Group of the signed-in user.
View Wi-Fi Signal	Displays the strength of the Wi-Fi signal.
View Cell Signal	Displays the strength of the cell signal.
View Battery Icon	Displays the amount of power remaining in the battery.
View Volume	Displays the level the volume is set to on the device.
Display Missed Call Notification	Displays a notification when an incoming call was not answered/missed.
Display SMS/Text Notification	Displays a notification when the device received a text message.
Tools	The following settings allow the user to customize and manage the contents of the Tools Menu on the Launcher. You can select any combination of the following options to make those options available to the user on the Tools Menu. A second option is to whitelist the application under the **Allowed Application** section by selecting the **Tools Menu** option next to that application. A third option is to configure apps directly on a device, provided the **configure** option is enabled.
Restart AW Hub.	Allows the user to restart the AirWatch Service on the device.
Restart AWCM.	Allows the user to restart the AWCM Service on the device.
Start AW Diagnostics.	Allows the user to open and access the AirWatch Diagnostics utility.

Settings	Descriptions
Start App Manager.	Allows the user to open and access the Application Manager utility. The Launcher is capable of **multiple profile support**. Profiles that are active and meet the assignment criteria for that device. Multiple profile support requires Workspace ONE Intelligent Hub version 4.0.0.13 or higher.
Configure	Allows the user to configure all areas of the Launcher directly on the device, including **Allowed Applications**, **Settings**, and **Tools Menu**.
Select Launcher View/Layout Style.	Select the format for the view/layout. ■ **Grid** – Traditional grid layout of applications. ■ **List** – List of applications with a small thumbnail of the app icon. ■ **Plain List** – List of applications with no thumbnail of app icon. ■ **None** – No preset view/layout. End users can select the view/layout they want. If you select a view/layout other than **None**, end users cannot change the view/layout.
Enable Wallpaper.	Enable to set a wallpaper for the Launcher. You must select a **Landscape** and **Portrait** mode image. **Important** Wallpapers cannot exceed 640x480 or be more than 20 KB. Images larger than 20 KB cannot display.

9 Select **Save & Publish**.

Update the Launcher Profile from the Windows Rugged Device

You might need to change the applications included in the Workspace ONE UEM App Launcher. This action requires admin credentials to perform.

1 Open the Workspace ONE UEM App Launcher application on the device.

2 Enter the Admin passcode in the **Password** text box and select **Accept**.

3 Select the option to **Import**, **Export**, or **Add** applications from and to the list.

4 Select **Add** to add an application and complete the following options on the **Add Application** screen:

   a **Application Location** – Defines the file path of the application or select the **Browse** option.

   b **Application Name** – Defines the name of the application to display in the Workspace ONE UEM App Launcher.

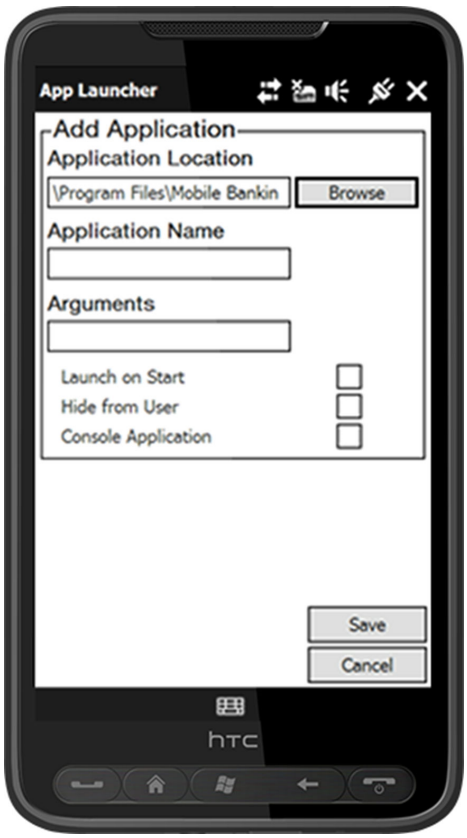
   c **Arguments** – Defines command-line arguments to run the application.

   d **Launch On Start** – Starts the application when the Workspace ONE UEM App Launcher is started.

   e **Hide from User** – Masks the application in the user interface.

   f **Console Application** – Defines the application as not having a user interface or as a background process.

5 Select **Save**.



Configure Shared Device Launcher Profiles

Workspace ONE UEM allows you to configure Launcher profiles to support multiple end users sharing a single device. Use this feature to customize the Launcher for individual users and their different applications to meet their individual roles.

Important You must enroll the device into the Parent organization group for the Launcher profiles for various User Categories to push to the device.

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Rugged > Hub Settings**.

2 Navigate to **Accounts > Users > User Settings > Categories > Add** and enter the Name and Description.

Consider creating the User Categories based on the various roles end users have that require different applications on the device. For example, basic users require different applications than a shift supervisor or manager. To accommodate this requirement, create different User Categories for the basic user, shift supervisor, and manager.

3 Select **Enable Shared Device Mode**.

4 Navigate to **Accounts > Users > List View** and **Add** new user or **Edit** an existing one.

5 Enable **Show Advanced User Details** and select the applicable **Category** based on the role of the user.

6 Create and configure a Launcher Profile. Select the applicable **User Category** based on the role of the user for this specific Launcher profile.

7 Configure a Launcher profiles for each end-user role.

8 End users must enter their credentials and their group ID. To remove the need to enter the group ID, navigate to **Settings > All Settings > Devices & Users > General > Shared Device** and set the **Group Assignment Mode** to **Fixed Organization Group**.

Create a VPN Profile (Windows Rugged)

Create a VPN Profile to deploy corporate VPN settings directly to managed devices in Workspace ONE UEM powered by AirWatch. This profile enables end users to access corporate infrastructure remotely and securely.

Important You can use a VPN profile only on Windows Rugged devices, but not on Windows CE devices.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **VPN** profile and click the **Configure** button.

5 Configure the VPN settings.

Settings	Descriptions
Connection Type	Defines the connection for the VPN. Both of these types rely on the encryption protocol to be passed within the tunnel because they do not inherently have their own encryption methods. ■ **PPTP** – Point-to-Point Tunneling Protocol. ■ **IPSec/L2TP** – Layer 2 Tunneling Protocol.
Connection Name	Enter the connection name.
Server	Enter the hostname of IP address of the VPN server.
Username	Enter the user name for the VPN. You can use lookup values to use the device-specific value.
Domain	Enter the domain for the VPN. You can use lookup values to use the device-specific value.

Settings	Descriptions
Authentication	Defines the authentication for the VPN. ■ **Certificate** – Use this option to deploy certificate-based authentication for your VPN connections. You must select this option if you select the **Connection TypeIPSec/ L2TP** ■ **Pre Shared Key** – Use the PSK option when you have a shared secret that device users use to access the VPN. This authentication type often uses symmetric key algorithms for security.
Shared Secret	Enter the shared secret for the connection. Displays when **Authentication** is set to **Pre Shared Key**.

6 Select **Save & Publish** to push the profile to devices.

Create a Time Sync Profile (Windows Rugged)

Deploy Time Sync payloads to synchronize the system time on Windows Rugged devices with time servers to ensure that the device fleet runs on the same clock. This profile within Workspace ONE UEM powered by AirWatch is useful for global networks with devices in numerous time zones.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Time Sync** payload and click the **Configure** button.

5 Configure the Time Sync settings:

Settings	Descriptions
Time Sync Method	Select the preferred method of time sync. ■ **Time Server** – Select to use a Network Time Protocol server with which to sync devices such as pool.ntp.org. ■ **HTTP** – Select to enter a URL. This URL can be any URL. For example, you can use www.google.com. ■ **SNTP** – Select to enter a Simple Network Time Protocol such as time.nist.gov. ■ **Console** – Select to sync the device with the UEM console.
Primary Time Server	Enter the URL of the time server with which the device syncs.
Port	Enter the port the device uses to sync with the secondary server.
Secondary Server	Enter an optional secondary server the device can use if the primary is unavailable. Displays when **Time Server** is selected as the **Time Sync Method**.

Settings	Descriptions
Port	Enter the port the device uses to sync. Displays when **Time Server** is selected as the **Time Sync Method**.
Sync Time Every	Enter the number of minutes, hours, or days.

6 Select **Save & Publish**.

Create a Shortcut Profile (Windows Rugged)

Create a Shortcut profile in Workspace ONE UEM powered by AirWatch to push custom icons associated with URLS. These icons provide your end users with the shortcuts to websites they need.

You can add as many icons as needed to a shortcut payload. Upload the icon image file into the Workspace ONE UEM console.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Shortcut** payload and click the **Configure** button.

5 Configure the Shortcut settings.

Settings	Descriptions
Label	Enter the name associated to the icon that displays on the user's device.
URL	Enter the URL for the website in which the user is advanced to when the user taps on the icon.
Icon	Upload the image file that displays on the user's device that is associated to the URL.

6 Select **Save & Publish** to push the profile to devices.

Create a Time Zone Profile (Windows Rugged)

Create a Time Zone profile to configure your Windows Rugged device time zone settings in Workspace ONE UEM powered by AirWatch. This profile eliminates having to remote control into the end user's device to set the time zone manually.

After pushing the profile, the device displays the time zone, and all device activity is time stamped based on that time zone regardless of the actual device location.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **Time Zone** payload and select the **Configure** button.

5 Select the **Time Zone Setup** drop-down, and select **Set Time Zone Manually**.

6 Select the **Time Zone** drop-down and select the appropriate time zone from the list.

Create a Custom Attribute Payload

Workspace ONE UEM powered by AirWatch allows you to create and deploy custom attributes that collect and compare custom-made values from device. Custom attributes are used to manage devices using attributes assigned to or gathered from the devices.

These attributes can be collected or created by third-party applications for use with the UEM console. By using custom attributes, you can ensure that only the devices whose attribute values match the ones you set are selected.

Custom attributes are used by the rules generator of product provisioning to provision products to specific devices. Ensure that your devices are provided the correct values to prevent incorrect products from being provisioned to them. See Chapter 6 Custom Attributes for more information.

Procedure

1 Navigate to **Devices > Products > Profiles > List View** and select **Add** and then select the device platform.

2 Configure the profile's **General** settings.

These settings determine how the profile deploys and who receives it.

3 Select the **Custom Attribute** profile.

4 Select **Add** to configure the custom attributes you want to use.

Settings	Descriptions
Application	Select the application (grouping of custom attributes) that contain the attributes you want to configure.
Custom Attributes	Select the specific custom attributes for the profile to configure.
Value	Enter the custom attribute value to assign to the device.
Is Dynamic	Enable to allow the custom attribute's value to change and be changed based on permissions. If selected, this looks up the custom attribute value for an individual device when the command is queued instead of using the default value specified in the payload. If no value is found, the device's default value is used.

Settings	Descriptions
Permission	Set the permission of the custom attribute. ■ **Read/Write** allows the applications to change the attribute value. ■ **Read Only** restricts applications from changing the value.
Sync	Enable to push the attribute value back to the UEM console to be displayed in the Device Details page.

You can add additional attributes as necessary.

5 Select **Save & Publish** to push the profile to devices.

Create a GPRS Profile (Windows Rugged)

The General Packet Radio Service (GPRS) allows mobile data on 2G and 3G cellular communication system for GSM devices. The GPRS payload allows you to configure and control how the device uses GPRS in Workspace ONE UEM powered by AirWatch.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.

2 Select **Windows Rugged**.

3 Configure the profile's **General** settings.

4 From the left panel, select the **GPRS** payload and click the **Configure** button.

5 Configure the GPRS settings.

Settings	Descriptions
Enabled	Select to enable GPRS management.
Connection Name	Enter the GPRS connection name.
Destination	Select whether the GPRS connection is to the **Internet** or a **Work** intranet.
GPRS Info Access Point Name	Enter the APN the device must connect to. The APN must follow the correct format: <network identifier>.mnc<MNC>.mcc<MCC>.gprs
User name	Enter the user name for connecting to the network.
Password	Enter the password for connecting to the network.
Domain	Enter the network domain.
Advanced	Enable to configure advanced options.
Specific Name Servers	Enable to enter specific name servers to use.
Country Code	Enter the network country code.
Area Code	Enter the device area code.
Use Country and Area Codes.	Enable to use Country and Area codes.
Phone	Enter the device phone number.

Settings	Descriptions
Device Name	Enter the device name for use in phone books.
Device Type	Select the RAS device type.
Use Software Compression.	Allows for faster connection speeds on low-bandwidth networks by compressing the phone book entries.
Use IP Header Compression.	Allows for faster connection speeds on low-bandwidth networks by compressing the IP Header.
Specific IP Address	Enable to connect to a specific IP Address.
Read Only.	Enable to restrict the device to reading data only.
Authentication Type	Select the type of authentication the network uses.

6 Select **Save & Publish**.

Compliance Policies

4

The compliance engine is an automated tool by Workspace ONE UEM powered by AirWatch that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period.

Compliance Policies in Workspace ONE UEM

For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, blocking certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM. Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

Dell BIOS Verification for Workspace ONE UEM

Ensure that your Dell Windows Desktop devices remain secure with Dell Trusted Device (formerly, Dell BIOS Verification). This service analyses the BIOS of your Dell devices and reports the status to Workspace ONE UEM so you can act against any compromised devices.

Benefits of Dell Trusted Device

The BIOS is a part in maintaining the overall device health and security. Modern computer systems rely on BIOS firmware to initialize hardware during the boot process and for runtime services that support the operating system and applications. This privileged position within the device architecture makes unauthorized modification of the BIOS firmware a significant threat. The Dell Trusted Device service provides secure BIOS validation using a secure signed response model. The status of the secure validation helps you act on compromised devices with the compliance policy engine.

Prepare Your Devices for Dell Trusted Device

To use Dell Trusted Device on your Windows Desktop devices, you must install the Dell Trusted Device service on the device. You must download the latest client from Dell (https://www.dell.com/support/home/product-support/product/trusted-device/drivers). Consider using Software Distribution to install the client on your Dell Windows Desktop devices.

Dell BIOS Verification Statuses

After you install the client onto your devices, you can see the reported status in the Device Details page. The statuses are as follows:

- Pass - The Dell Trusted Device client is installed on the device and the device is secure.
- Fail - The Dell Trusted Device client is installed and one of the following issues is present:
  - The Pre-Check event returns a fail result. This result happens when the client detects an invalid binary signature.
  - The BIOS Utility event returns a fail result for the validation test.
  - The BIOS Server Processing event returns a fail result for an invalid signature, invalid exit code, or the payload status is out of sync.
- Warning - The Dell Trusted Device is installed and the client detects an issue. The device might not be secured, so investigate the issue. Causes for a Warning status might include the following list.
  - No network connection
  - Invalid command-line argument
  - Application is running with insufficient privileges.
  - Internal errors in the client
  - Server responds with an error.
  - Driver issues with the client
  - Unknown results in the BIOS verification
- If you see a gray warning icon, the Dell Trusted Device client is not installed on the device.

Compromised Device Detection with Health Attestation

In both BYOD and Corporate-Owned device deployments, it is important to know that devices are healthy when accessing corporate resources. The Windows Health Attestation Service accesses device boot information from the cloud through secure communications. This information is measured and checked against related data points to ensure that the device booted up as intended and is not victim to security vulnerabilities or threat. Measurements include Secure Boot, Code Integrity, BitLocker, and Boot Manager.

Workspace ONE UEM enables you to configure the Windows Health Attestation service to ensure device compliance. If any of the enabled checks fail, the Workspace ONE UEM compliance policy engine applies security measures based on the configured compliance policy. This functionality allows you to keep your enterprise data secure from compromised devices. Since Workspace ONE UEM pulls the necessary information from the device hardware and not the OS, compromised devices are detected even when the OS kernel is compromised.

Configure the Health Attestation for Windows Desktop Compliance Policies

Keep your devices secured by using Windows Health Attestation Service for compromised device detection. This service allows Workspace ONE UEM to check the device integrity during startup and take corrective actions.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Windows Health Attestation**.

2 (Optional) Select **Use Custom Server** if you are using a custom on-premises server running Health Attestation. Enter the **Server URL**.

3 Configure the Health Attestation settings.

Settings	Descriptions
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the Server URL field.
Server URL	Enter the URL for your custom Health Attestation server.
Secure Boot Disabled	Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.

Settings	Descriptions
Data Execution Prevention (DEP) Policy Disabled	Enable to flag compromised device status when the DEP is deacivated on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. Hardware and software both enforce DEP.
BitLocker Disabled	Enable to flag compromised device status when BitLocker encryption is deactivated on the device.
Code Integrity Check Disabled	Enable to flag compromised device status when the code integrity check is deactivated on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.
Early Launch Anti-Malware Disabled	Enable to flag compromised device status when the early launch anti-malware is deactivated on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.

4 Select **Save**.

Configure the Workspace ONE Intelligent Hub for Windows Rugged

5

The Workspace ONE Intelligent Hub for Windows Rugged devices is pre-configured with Workspace ONE UEM. Change these settings when you need the Workspace ONE Intelligent Hub to meet certain business needs.

Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Rugged > Hub Settings**.

Upgrade the Workspace ONE Intelligent Hub

When a new version of the Workspace ONE Intelligent Hub releases, upgrade your devices remotely and easily. With product provisioning, devices receive the Workspace ONE Intelligent Hub CAB file and install it based on directions. For more information, see the Product Provisioning Guide for Windows Rugged available on Workspace ONE UEM Resources.

If you are using a legacy Workspace ONE Intelligent Hub older than version 5.2.x, you must use the legacy Over-the-Air Migration method. For more information, see https://support.air-watch.com/articles/115001664548.

Device-Side Scripting

The AirWatch AWScript component allows you to configure your Windows Rugged devices through device-side scripting. The script file uses a dialect of BASIC as its core scripting language and adds Workspace ONE UEM-specific extensions on top.

For more information on the AWscript and its capabilities, see https://support.air-watch.com/articles/115001664528

General

Setting	Description
Device ID Algorithm	Set the unique device identification algorithm used on the device. ■ Device ID Algorithm 3 – Hub uses the OS-provided API to generate the UDID. ■ Device ID Algorithm 5 – Along with the OS-provided API, the Workspace ONE Intelligent Hub uses the MAC ID of the device to generate the UDID. ■ Device ID Algorithm 6 – Together with the OS-provided API and the MAC ID of the device, the Workspace ONE Intelligent Hub also uses the serial number of the device to generate the UDID.
Heartbeat Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking in with the Workspace ONE UEM console.
Data Sample Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device.
Data Transmit Time Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to send data collected from the device to the UEM console.
Check-In on Condition (Event)	Enable to limit the Workspace ONE Intelligent Hub to check-in or beacon to the UEM console only when certain conditions (Wi-Fi connection, AC Power, or NW Adapter) are met. This helps reduce bandwidth issues as devices typically meet the condition when they are stored for after hours.

Shared Devices

Setting	Description
Enable Shared Device Mode	Select this check box to enable shared device functionality.

Notifications

Setting	Description
Enable Hub Installation Complete Notification	Select this check box to enable or disable notifications for Hub installation completion.
Enable Product Install Status Notification	Select this check box to enable or disable notifications through the Workspace ONE Intelligent Hub for product installation completion.

Location

Setting	Description
Collect Location Data	Enable to allow the to determine the device location based on a device's Wi-Fi network. When available, the Workspace ONE Intelligent Hub will report the location to the Workspace ONE UEM console using the Data Transmit Interval.

Application List

Setting	Description
Applications Poll Interval (min)	Set the time interval (in minutes) at which the applications list for each device will refresh on the Workspace ONE UEM console.

Certificate List

Setting	Description
Certificate Poll Interval (min)	Set the time interval at which the certificate list for each device will refresh on the Workspace ONE UEM console.

Proxy

Setting	Description
Proxy Configuration	Enable to allow the configuration of a proxy settings.

Application Manager Package Scheduler

These settings are for the legacy Workspace ONE Intelligent Hub v3.3.

Use the **APPLICATION MANAGER PACKAGE SCHEDULER** to define a schedule for devices with the Workspace ONE Intelligent Hub v3.3+ to retrieve products provisioned on schedule.

Setting	Description
Add	Select to create schedules for provisioning products using Products (Legacy).
Application Manager Scheduler	Select the hour the product begins to push to devices.
Randomization Window (min)	Select the amount of time the product is pushed. The order of devices is randomized.

Sideloading Cab

Setting	Description
Request Enrollment Cab	Enable to create a side loading cab to quickly enroll devices.
Platform	Select the operating system for the cab file.
Enrollment User	Select a user for the cab file to use during enrollment. The cab file can be used on multiple devices regardless of the user selected.

Setting	Description
Enrollment User Password	Enter the password for the user for enrolling with the cab file.
Show Characters	Select to show password characters.

Windows Rugged Device Logging with the Workspace ONE Intelligent Hub

All device log settings in Workspace ONE UEM are configured through the log_config.cfg file located in the "\Program Files\AirWatch" directory. When this file is opened up and viewed in Notepad, it appears with the following text and options.

```
       [*]
       trace_level=5
       max_file_size_kb=256
       files_to_keep=2
       log_file_path=\Program Files\AirWatch\Logs
       use_local_time=false [aw_setup]trace_level=5max_file_size_kb=256files_to_keep=2log_file_path=
\use_local_time=false [awregisterdevice.exe]trace_level=3max_file_size_kb=256files_to_keep=2log_file_path=
\Program Files\AirWatch
\Logsuse_local_time=false [awapplyprofile.exe]trace_level=5max_file_size_kb=256files_to_keep=2log_file_path=
\Program Files\AirWatch
\Logsuse_local_time=false [awremotecontrol.exe]trace_level=1max_file_size_kb=256files_to_keep=2log_file_path=
\Program Files\AirWatch\Logsuse_local_time=false
```

The first setting group that appears under the asterisk is the default configuration settings for all logs available on the device.

Trace levels vary from 1 to 5. A level of 1 provides the most basic and least amount of information. Developers use Level 5 for debugging purposes since it provides all available messaging. There is a tradeoff between the trace level and the log size. A higher trace level increases the size of the log files due to messaging increase. The trace level that is set in the default section applies to all log files on a device.

You can keep the default log level low and still increase the log level for the four options below the default log level. Specify the log level for each of the options if you select to use a different trace level than the default level.

The logs available on a device vary based on what is configured and the OEM of the device. The following log files are generally available on Windows Rugged devices.

- aw_setup – Provides logging information relating to the AWMasterSetup utility. The AWMasterSetup utility initiates the Workspace ONE Intelligent Hub install and uninstall process on a device. This log file is the only log file that is not located in the "\Program Files \AirWatch" directory. The log is instead located in the root of the file system.
- awacmclient – Provides logging information relating to the AWCM client on the device.

- awapplicationmanager – Provides logging information relating to product provisioning.
- awprocesscommands – Provides logging information relating to the execution of MDM commands and installation of profiles.
- AWService – Provides information about the AWService.exe component, which is responsible for managing beacon and interrogator samples.
- awapplyprofile – Relates to installation of the Workspace ONE Intelligent Hub settings XML file which occurs during the enrollment process.
- awregisterdevice – Provides information about the registering of the device that occurs during the enrollment process.
- awapplauncher – Provides information about the Application Launcher executable. This log only applies to devices using the App Launcher.
- fusionwlansetup – Provides information about configuring and setting up the Fusion Wi-Fi driver on Motorola devices.

Configure Log Files

You can configure the trace level behavior of device log files in Workspace ONE UEM by doing some tweaking with notepad.

1 Transfer the log file to your PC using the file manager utility in device details or through remote management.

2 Open the log file using a basic text editor such as Notepad.

3 Edit the desired trace level to the needed value.

4 Save the log file.

5 Transfer the log file back to the "Program Files\AirWatch" directory on the device.

   Consider first deleting the old log_config.cfg file from the device.

6 Restart the AWService on the device once it has the updated log_config.cfg file. Use the Restart Workspace ONE Intelligent Hub or the **Warm Boot** device actions available in the UEM console.

Once the AWService restarts, the new logging configuration takes effect.

Custom Attributes

6

Custom attributes in Workspace ONE UEM enable you to extract specific values from a managed device (for example IMEI, location, among many others) and use it as assignment criteria for products. You can also configure a 3rd party application to create custom attributes and display them on the launcher.

What Is A Custom Attribute?

A custom attribute is a placeholder for additional device information collected by Workspace ONE Intelligent Hub or by a third party application. This placeholder can be used in many different ways.

- It can be used to assign content such as provisioned products.
  - *...for example, you can provision product XYZ to only devices that are checked out and in the field.*
- It can provide information to the admin on the UEM console or to the end user on the device.
  - *...for example, a delivery driver can view an in-house developed app to determine their next stop, furnished by a custom attribute that collects the location of the device*.
- It can be used to move newly enrolled devices to a specific organization group.
  - *...for example, you can move all newly enrolled devices whose model number equals Zebra VC80 to an organization group that is designed to serve that specific model.*

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

Create a Custom Attribute

Create a custom attribute and values to push to devices in Workspace ONE UEM. You can create assignment rules for products to provision based on these attributes and their values.

1 Navigate to **Devices > Provisioning > Custom Attributes**.

2 Select **Add** and then select **Add Attribute**.

3 Under the **Settings** tab, enter an **Attribute Name**.

4 Enter the optional **Description** of what the attribute identifies.

5 Enter the name of the **Application** that gathers the attribute. The application can be a third-party app or Workspace ONE Intelligent Hub.

6 Select **Collect Value for Rule Generator** to make the values of the attribute available in the drop-down menu of the rule generator.

7 Select **Use in Rule Generator** if you want to use the attribute in the rule generator.

8 Select **Persist** to prevent the removal of the custom attribute from the Workspace ONE UEM console unless an Admin or an API call explicitly removes it.

   Otherwise, the attribute is removed as normal. If you delete a custom attribute reported from a device to the UEM console, a persisted custom attribute remains in the UEM console. Custom attribute persistence is only available to Android and Windows Rugged devices.

9 Select **Use as Lookup Value** to use the custom attribute as a lookup value anywhere in the UEM console.

   Example: You can use custom attributes as part of a device friendly name to simplify device naming.

10 Select the **Values** tab.

11 Select **Add Value** to add values to the custom attribute.

   You do not need to enter all possible values of the attribute. The list of attributes entered here is not a requirement or constraint on what values the device *can* report. Instead, enter only expected values used to pre-define organization group assignment rules.

12 Select **Save**.

Custom Attributes Database

Custom attributes are stored as XML files and in the Workspace ONE Intelligent Hub database, each stored on the device. When using the database, custom attributes are sent as samples to Workspace ONE UEM periodically for asset tracking of key/value pairs.

If a record in the device database is configured with 'Create Attribute' = TRUE, then the Workspace ONE Intelligent Hub automatically retrieves the Name and Value sent with the custom attributes sample. The key/value pair displays in the Device Details page for the device in the Custom Attributes tab.

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

Assign Organization Groups Using Custom Attributes

Configure rules that control how devices are assigned to organization groups following enrollment in Workspace ONE UEM. You are limited to one custom attribute assignment rule per organization group (OG).

1 Ensure that you are currently in a customer type organization group.

2 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.

3 Set **Device Assignment Rules** to **Enabled**.

4 Set the **Type** to **Organization Group by Custom Attribute**.

5 Select **Save**.

6 Navigate to **Devices > Provisioning > Custom Attributes > Add > Add Attribute** and create a custom attribute if you have not already done so.

See the section on this page entitled **Create a Custom Attribute**.

7 Navigate to **Devices > Provisioning > Custom Attributes > Custom Attributes Assignment Rules > Add Rule**.

8 Select the **Organization Group** to which the rule assigns devices.

9 Select **Add Rule** to configure the logic of the rule.

Setting	Description
Attribute/ Application	This custom attribute determines device assignment. Select from among Device Model, Serial Number, and any custom attribute or XML file that is available in the customer OG you are in.
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** When making an assignment rule, comparisons using the less than (<) and greater than (>) operators (and their variants) can only be used to compare numerical values including integers. The exception is when you are comparing OEM build versions, you can apply < and > operators on non-numerical ASCII strings. An example is when an OEM update filename includes hyphens, periods, and other characters together with numbers. Such assignment rules must identify a device manufacturer in the rule logic and that comparison is deemed accurate when the format on the device matches the one specified on the server.
Value	All values from all applicable devices are listed here for the **Attribute** selected for the rule.
Add Logical Operator	Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.

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

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

Custom Attributes Importing

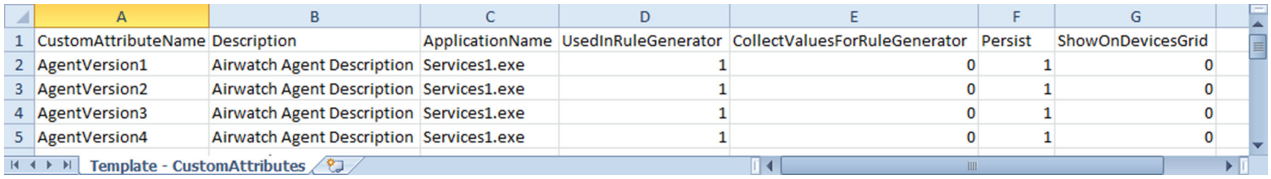
The custom attribute batch import feature in Workspace ONE UEM allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters.

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

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

Template Types

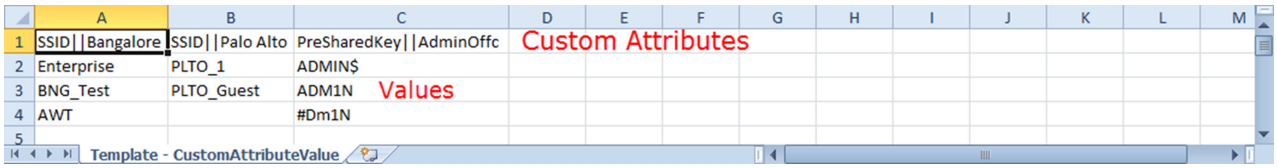
- Custom Attributes Template – Allows you to define a custom attribute and its settings.



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

Template - CustomAttributes

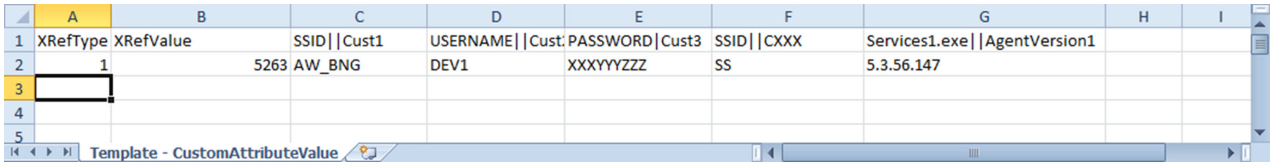
- Custom Attribute Values Template – Allows you to define the values of predefined custom attributes.



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

Template - CustomAttributeValue

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



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

Template - CustomAttributeValue

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

  b Serial Number

  c UDID

  d MAC Address

  e IMEI Number

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

This chapter includes the following topics:

XML Provisioning, WinRugg

XML provisioning in Workspace ONE UEM powered by AirWatchcan collect custom attributes based on device details for your Windows Rugged device. You can use custom attributes to unlock product provisioning's more advanced functionality.

Procedure

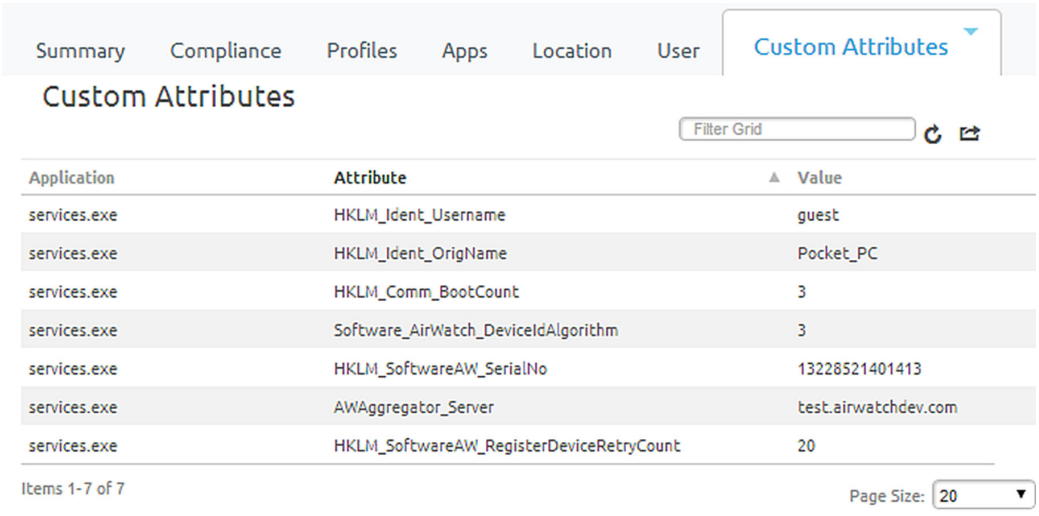
1. Navigate to **Devices > Provisioning > Components > Files/Actions**, then select the **Add Files/Actions** button, and then select **Windows Rugged** as your platform.
2. Create an XML product.

   For more information, see Create an XML Provisioning File, WinRugg. The manifest includes an action to download the XML file to **\Program Files\Airwatch\Cache\Profiles**.

Results

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

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



Example

Syncing Registry Settings

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

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

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

Using Third-Party Applications to Create Custom Attributes

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

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

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

What to do next

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

Create an XML Provisioning File, WinRugg

XML provisioning allows you to push a custom-designed XML file to a device in Workspace ONE UEM powered by AirWatch. After the file is uploaded, it runs an install command to extract the settings from the XML file and install them on the device.

Procedure

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

Results

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

Example

Windows Rugged

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

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

```
<?xml version="1.0"?>
<wap-provisioningdoc name="desiredDocName /V_1">
```

```
<characteristic type="com.windowspc.getregistryinfo.managed">
<reg_value value_name="KeyName"
<!-- (i.e. CommonFilesDir) --
key_name="RegistryPath"
<!-- (i.e.Software\Wow6432Node\Microsoft\Windows\CurrentVersion) --
custom_attribute_name="AttributeName"/>
<reg_value value_name="Keyname ..." key_name="Path\...."
custom_attribute_name="AttributeName2"/>
</characteristic>
</wap-provisioningdoc>
```

Windows Rugged Device Management

7

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

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

Device Dashboard

The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

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

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

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.

  - **Not Encrypted** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.
- **Ownership** – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.
- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send out a query command so that the devices can check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for each supported OS. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Workspace ONE Assist

Workspace ONE Assist, previously named Advanced Remote Management (ARM), allows you to connect remotely to end-user devices so you can help with troubleshooting and maintenance. The Assist Server facilitates communication between the Workspace ONE UEM and the "host" device.

For more information, see VMware Workspace ONE Assist Documentation.

Device Details Page

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

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

Remote Actions

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

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

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed applications.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **Change Organization Group** – Change the device's home organization group to another existing OG. Includes an option to select a static or dynamic OG.
  - If you want to change the organization group for multiple devices at a time, you must select devices for the bulk action using the Block selection method (using the shift-key) instead of the Global check box (next to the Last Seen column heading in the device list view).
- **Clear Passcode (Device)** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as **Delete In Progress** on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the console.
- **Device Information (Query)** – Send an MDM query command to the device to return information on the device such as friendly name, platform, model, organization group, operating system version, and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group Device Category**.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.
  - **Windows Desktop Only:** Enterprise Reset restores a device to a Ready to Work state when a device is corrupted or has malfunctioning applications. It reinstalls the Windows OS while preserving user data, user accounts, and managed applications. The device will resync auto-deployed enterprise settings, policies, and applications after resync while remaining managed by Workspace ONE.

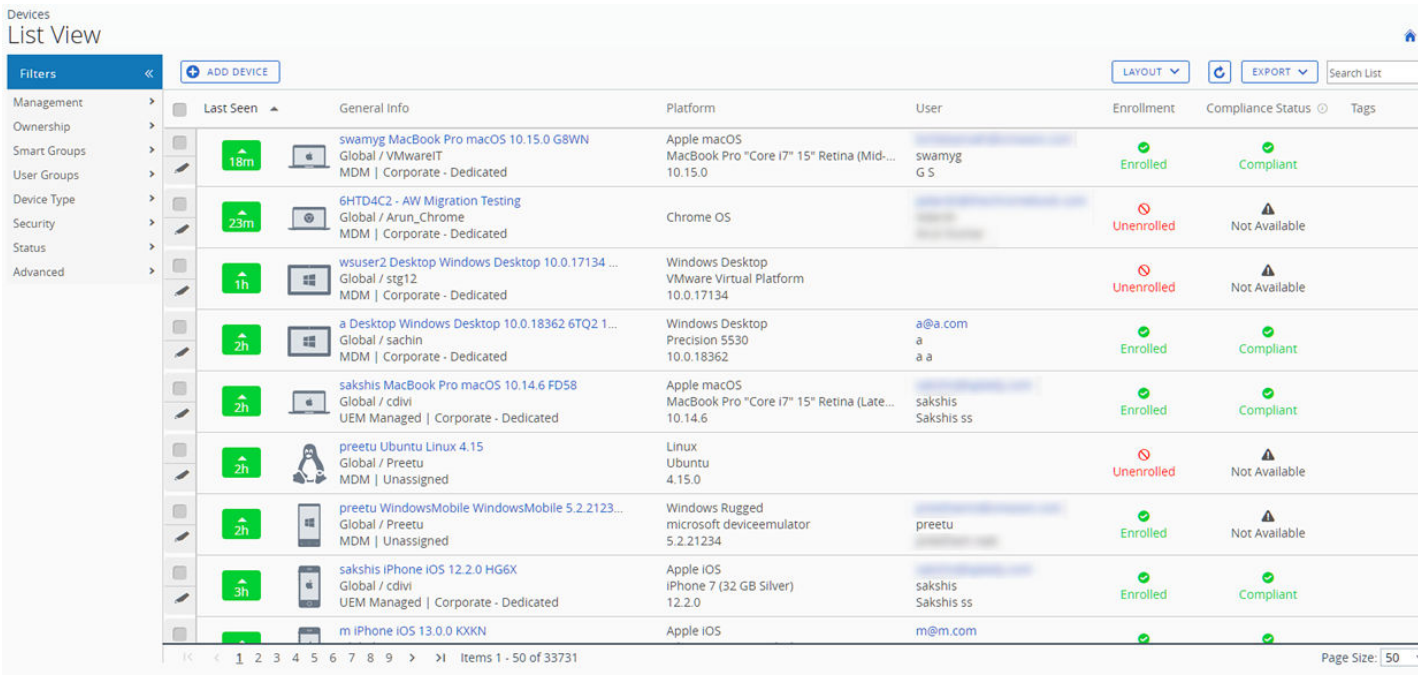
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment is required before Workspace ONE UEM can manage this device again. This device action includes options to prevent future re-enrollment and a **Note Description** text box for you to add information about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **File Manager** – Start a File Manager within the UEM console that enables you to view remotely a device's content, add folders, conduct searches, and upload files.
- **Provision Now** – Provision products to a device. Provisioning is the ability to create an ordered installation of files, actions, profiles, and applications into a single product that can be pushed to devices.
- **Query All** – Send a query command to the device to return a list of installed applications (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles, and security measures.
- **Registry Manager** – Start a Registry Manager within the UEM console that enables you to view remotely a device's OS registry, add keys, conduct searches and add properties.
- **Remote Assist** – Take control of a supported device remotely using this action, which offers platform-specific tools that allow you to perform support and troubleshooting on the device. Android devices require Remote Control Service to be installed on the device.
- **Remote Management** – Take control of a supported device remotely using this action, which starts a console application that enables you to perform support and troubleshoot on the device. Android devices require Remote Control Service to be installed on the device.
- **Request Device Check-In** – Request that the selected device check itself in to the UEM console. This action updates the **Last Seen** column status.
- **Restart Workspace ONE Intelligent Hub** – Restart the Workspace ONE Intelligent Hub. This option is used during troubleshooting for when the enrollment process or submodule installation process is interrupted.
- **Send Message** – Send a message to the user of the selected device. Select between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**. Push notification requires Airwatch applications like Hub, Boxer etc which must have been launched at least once.
- **Start/Stop AWCM** – Start/Stop the Cloud Messaging service for the selected device. VMware AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Admin Console. The AWCM eliminates the need for end users to access the public Internet or use consumer accounts such as Google IDs.
- **Task Manager** – Run a Task Manager within the UEM console that enables you to view remotely a device's currently running tasks, including task **Name**, **Process ID**, and applicable **Actions** you can take.
- **View Manifest** – View the device's **Package Manifest** in XML format from the UEM console. The manifest on Windows Rugged devices lists metadata for widgets and applications.

- **Warm Boot** – Initiate a restart of the operating system without performing a power-on self-test (POST).
- **Workspace ONE Intelligent Hub Query** – Send a query command to the Workspace ONE Intelligent Hub on the device to ensure it has been installed and is functioning normally.

This chapter includes the following topics:

Device List View

Use the Device List View in Workspace ONE UEM to see a full listing of devices in the currently selected organization group.



The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on how long the device is inactive. The default value is 480 minutes (8 hours) but you can customize this by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced** and change the **Device Inactivity Timeout (min)** value.

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

Sort by columns and configure information filters to review 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.

Hover-Over Pop-Up Window in Device List View

Each device in the **General Info** column features a tool tip icon in the shape of a folder located in the upper-right corner next to the device friendly name. When this icon is tapped (mobile touch device) or hovered-over with a mouse pointer (PC or Mac), it displays a Hover-Over pop-up window. This pop-up window contains information such as **Friendly Name**, **Organization Group**, **Group ID**, **Management**, and **Ownership**.

Similar tool tip icons are found in the **Enrollment** and **Compliance Status** columns in the Device List view. These tool tip icons feature Hover-Over Pop-Up windows displaying **Enrollment Date** and **Compliance Violations** respectively.

Customize Device List View Layout

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

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

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

Some notable device list view custom layout columns include the following.

- Android Management
- SSID (Service Set Identifier or Wi-Fi network name)
- Wi-Fi MAC Address
- Wi-Fi IP Address
- Public IP Address

Exporting List View

Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

Search in Device List View

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

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

Device List View Action Button Cluster

With one or more devices selected in the Device List View, you can perform common actions with the action button cluster including Query, Send [Message], Lock, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer, model, enrollment status, and the specific configuration of your Workspace ONE UEM console.

Remote Assist

You can start a **Remote Assist** session on a single qualifying device allowing you to remotely view the screen and control the device. This feature is ideal for troubleshooting and performing advanced configurations on devices in your fleet.

To use this feature, you must satisfy the following requirements.

- You must own a valid license for Workspace ONE Assist.
- You must be an administrator with a role assigned that includes the appropriate Assist permissions.
- The Assist app must be installed on the device.
- Supported device platforms:
  - Android
  - iOS
  - macOS
  - Windows 10
  - Windows Mobile

Select the check box to the left of a qualifying device in the **Device List View** and the **Remote Assist** button displays. Select this button to initiate a Remote Assist session.

For more information, see the Workspace ONE Assist Guide.

Unenrolled Devices

Unenrolled devices may or may not be viewed in the Workspace ONE UEM console depending upon whether they were registered or held an enrolled status in the past. You can also get access to troubleshooting logs made before a device's unenrollment from the UEM console.

Unenrolled Status

An unenrolled device is a device in one of three possible scenarios.

1 The device is new to Workspace ONE UEM and is not registered, not enrolled, and therefore not managed. A device in this scenario cannot be seen in the UEM console.

2 The new device has begun the Workspace ONE enrollment process and is registered with the UEM console but not yet fully enrolled. This scenario normally occurs during a wave of new enrollments where devices are registered as a way of restricting enrollment. The mechanism that allows registered devices to enroll is a device allowlist. A device in this state can be seen by the UEM console with the status 'unenrolled'. Given that a registered device is traditionally a part of the enrollment process, a device does not remain in this scenario for long.

3 A device can also become unenrolled if the device end user manually removes the MDM profile from the device.

For more information, see the section on this page entitled **Deleting Devices**.

Access Troubleshooting Logs Made Before Unenrollment

You can access Troubleshooting/Commands logs made before the device was unenrolled. These logs can be useful to get a full picture of the device's history.

1 Navigate to **Devices > List View**.

2 Select a device you know to have been unenrolled in the past. You have the option to **Filter** the list view to show only devices with a **Status** of **Unenrolled**.

Result: When you select a device, the **Details View** displays.

3 Select the **More** tab drop-down, then select **Troubleshooting**, followed by the **Commands** tab.

What to do next: If you do not intend to re-enroll a previously unenrolled device to the same customer organization group again, consider deleting the device record permanently so the device history is clear upon re-enrollment. Contact Workspace ONE Support to make this arrangement.

Bulk Actions in Device List View

Once you filter a subset of devices, you can perform bulk actions to multiple devices by selecting devices and then selecting from the action button cluster.

Bulk actions are only available in the Device List View if they are enabled in the system settings (**Groups & Settings > All Settings > System > Security > Restricted Actions**). Password Protect Actions require a PIN to perform.

With devices selected in the **List View**, the number of devices selected is displayed next to the action buttons. This number includes filtered devices that are selected as well.

Note In the Device List View, the bulk actions available when you select a block of devices with the shift key may be different than the bulk actions available when you use the Global check box.

Selecting Devices in Device List View

You can select individual devices on a page by ticking individual check boxes to the left of each device. You can also select a block of devices across multiple pages. You can even select all devices in your entire fleet, which might trigger the restricted actions warning.

Selecting a Block of Devices

You can select a contiguous block of devices, even across multiple pages, by selecting the device check box at the beginning of the block. Next, hold down the shift key, then select the device check box at the end of the block. This action is similar to the block-selection in the Windows and Mac environments and it allows you to apply bulk actions to those selected devices.

Selecting All Devices

The Global check box, located to the left of the **Last Seen** column header, can be used to select or deselect all devices in the listing. If your **List View** contains a filtered listing of devices, the Global check box can be used to select or deselect all filtered devices.

When the Global check box features a green minus sign (), it means at least one but not all devices are selected. Select this icon again and it changes to a check mark sign (), indicating that all devices in the listing (either filtered or unfiltered) have been selected. Select it a third time and it changes again to an empty check box (), indicating that no devices in the listing are currently selected.

Note In the Device List View, the bulk actions available when you select a block of devices with the shift key may be different than the bulk actions available when you use the Global check box.

Deleting Devices

You can delete an enrolled device from the Workspace ONE UEM console.

Deleting a device has the following three impacts.

1 It removes the device from the Device List View.

2 An *Enterprise Wipe is executed, removing any sensitive corporate content from the device.

3 The device is thereby excluded from all device management functions and features.

However, a deleted device is still registered with the UEM console and gets added to the allowlist. This addition means the deleted device can be re-enrolled easily. A device can remain in this scenario indefinitely. You can retain up to approximately 150,000 devices on this allowlist. Contact support if your needs exceed this amount.

You can remove the registration record of any allowlisted device at any time, which makes the device unseen and unknown by the UEM console. A device in this scenario can be enrolled at a future date.

Alternately, you can remove the device from the allowlist and add the device to a denylist, preventing future enrollment and effectively banning the device from your fleet.

You can delete a device from the Device List View or the Device Details View.

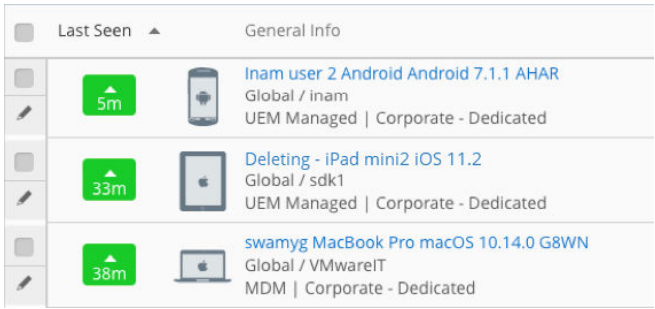
1 Navigate to **Devices > List View** and select the device you want to delete by clicking the check box to the left of the device listing.

   a Some devices cannot be deleted from the list view. If you want to delete such a device, navigate to **Devices > List View** and instead, select the device **Friendly Name** in the **General Info** column. This action displays the **Details View**. The **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

2 Locate the **More Actions** button and select it.

3 Select **Delete Device** and select **OK** at the confirmation prompt.

Results: the Device List View entry for the deleted device includes the "Deleting" indicator.



* When you select multiple devices to be deleted, you may trigger the Wipe Protection feature. Any devices wiped after the wipe protection is unlocked must be manually deleted.

For example, if you select 25 devices to be deleted and Wipe Protection is activated after 10 deletions, the remaining 15 devices are enterprise wiped after you unlock wipe protection but they are not deleted from UEM as the first 10 were. You must delete these 15 remaining devices manually.

Lookup Values

8

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

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

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

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

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

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

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

```
jsmith iPad iOS GHKD
```

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

Data Overhead

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

Static Strings Versus Lookup Values

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

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

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