Introduction to the Windows Mobile Guide

Overview

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 the majority of mobile devices in these environments and can perform many functions such as sales, inventory, scanners, and more. With the AirWatch solution, you can manage these devices and integrate them with your other mobile platforms, which give you a central location for mobile device management.

This Platform Guide describes the following processes:

- Enrolling devices with AirWatch
- Using AirWatch Utilities
- Configuring AirWatch options
- Securing and managing devices

In This Guide

You will find in this guide the following procedures that were arranged in a logical sequence to guide you from enrolling to managing devices:

- Before You Begin – Details device hardware and software supported, requirements, recommended reading, and things you should know and do before proceeding .
- Windows Mobile Device Enrollment – Explains the enrollment process needed to establish initial communications with AirWatch.
- AirWatch Windows Mobile Agent – Describes the use of the AirWatch Application Manager and AirWatch Diagnostics utilities to provision devices with packages and view device status.
- Windows Mobile Device Profiles – Explores the AirWatch Admin Console features, such as enabling services for the agent, provisioning packages, deploying profiles and credentials, controlling profile time schedules, etc.
- Managing Windows Mobile Devices – Provides AirWatch Admin Console and Self-Service Portal navigation to features needed by administrators to manage devices.
- Appendix A - Over-the-Air Migration – Describes how to perform over-the-air (OTA) migration from an older WinMo/WinCE Agent to a newer one or from Athena to the latest Agent through package provisioning.
- Appendix B – XML Provisioning – Details how to use Product Provisioning to download and install XML updates to a Windows Mobile devce.
- Appendix – Custom Variables – Details how to configure, gather, and apply custom variables from Windows Mobile devices for use with Product Provisioning.

Before You Begin

Overview

This Windows Mobile guide was written for AirWatch administrators and explains the complete process from enrolling to managing those devices in AirWatch. This guide simplifies the entire process by explaining each process step-by-step in a logical sequence. By following procedures in this guide, you can ensure a successful deployment of Windows Mobile devices.

In this Section

You will find in this section all the information you need to know prior to advancing to the procedures in this guide:

- Requirements – Details useful and/or required information you need before continuing with this guide.
- Supported Devices, OS, Agents, Versions, and Browsers – Lists Windows Mobile devices and software versions supported by AirWatch.
- Recommended Reading – Provides a list of helpful guides to better your understanding of mobile device management and Windows Mobile devices.

Requirements

Before reading this guide, perform actions needed to gather and prepare the following requirements:

Enrollment Requirements for Windows Mobile

- **AirWatch Admin Console Credentials** – These credentials allow access to the AirWatch environment.
- **Host Name** – This enrollment URL is unique to your organization's environment and is defined in the AirWatch Admin Console.
- **Group ID** – This ID associates your device with your corporate role and is defined in the AirWatch Admin Console.
- **ScanToConnect and EnrollmentBarcode Applications** (Optional) – These applications help to enroll Windows Mobile devices if using the scan-to-connect method of enrollment. Ask your AirWatch Account Manager for these applications.

Supported Devices, OS, Agents, Versions, and Browsers

Platforms and Devices 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

Choose the method for installing the agent by referring to Enrolling Windows Mobile Devices.

Recommended Reading

Through the AirWatch Resource Portal , AirWatch provides many documents, videos, and webinars on a multitude of related subjects that give you additional background and knowledge to aid you in the processes explained within this guide. If this is the first time using this guide, you might find the following information helpful:

- **AirWatchMobile Device Management Guide** – Provides additional information regarding the general aspects of MDM.

Windows Mobile Device Enrollment

Overview

Windows Mobile devices can enroll with the AirWatch Agent by three methods: sideloading, web enrollment, and scan-to-connect. Each method has its uses.

Note: For those using agent 4.0.0.20 or greater, AirWatch supports the cold boot persistence storage feature on Motorola devices so if the device is wiped (reset) and the AirWatch Windows Mobile agent is removed, the agent remains in the non-volatile memory and automatically reinstalls itself upon device startup.

- **Sideloading** stages the AirWatch Agent on to the device so the user has no interaction with the enrollment process. The device is ready to use immediately.
- **Web enrollment** directs the user to an enrollment URL to complete enrollment.
- **ScanToConnect** is available for Motorola and Symbol devices only. Users scan to enroll and to put the following configurations on the device:
  - Wireless local area network (WLAN)
  - AirWatch Environment information
  - User authentication information
  - AirWatch Organization Group

In This Section

- Enrolling Using Sideloading – Details how to sideload the agent to enroll a device.
- Enrolling Using the Web – Explains how to enroll by sending a URL and Group ID to the device.
- Enrolling Using Scan-To-Connect – Summarizes how to scan barcodes to configure the AirWatch Agent and the WLAN on Motorola and Symbol devices.
- Unenrolling Windows Mobile Devices – Details the different methods of unenrollment that allow you to remove corporate data from the device and the device from AirWatch.

Enrolling Using Sideloading

Use the following steps to sideload the AirWatch Agent.

1. Navigate to **Groups & Settings ▶All Settings ▶Devices & Users ▶Windows ▶Windows Mobile ▶Agent Settings** in the AirWatch Admin Console.
2. In the Sideloading CAB section, select the **Request Enrollment Cab** check box.
3. Select the **Platform**, **Windows Mobile**, or **Windows CE**.

4. Enter your user ID to receive the CAB file in the **Enrollment User** field.
5. Enter your AirWatch user credentials.
6. Select **Download** to install the AirWatch Agent on a computer.

Note: Sideloading the agent requires CAB Creation Templates for the agent version to build on the server.

7. Connect the Windows Mobile device to the computer using a USB connection and copy the AirWatch Agent CAB file from the computer to the device.
8. Ensure the device is connected to the WLAN.
9. Double-tap the AirWatch Agent on the device to complete enrollment.

Enrolling Using the Web

Enrolling using the web requires sending the enrollment URL and their Group ID to end users. Use the following steps to enroll using the web:

1. Go to the enrollment URL using the native browser on the device.
2. Enter the applicable AirWatch solution information in the **Group ID**, **Username**, and **Password** fields.
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 AirWatch Agent to the device.
6. Select **Continue** to complete the enrollment.

Enrolling Using Scan-To-Connect

Scan-to-connect allows end users to scan barcodes to configure the AirWatch Agent and the WLAN on Motorola and Symbol devices. Use the following steps to enroll using the scan-to-connect process.

1. Get the ScanToConnect application, EnrollmentBarcode application, and AirWatch Agent CAB file from your AirWatch Services Account Representative.
2. Create a barcode using the EnrollmentBarcode application. Include the WLAN settings, AirWatch environment settings and username and password in the barcode. Print the barcode.
3. Connect the scanning device to a computer using a USB connection.
4. Copy the AirWatch Agent CAB and the ScanToConnect application to the scanning device.
5. Tap the AirWatch Agent CAB file on the scanning device to install it.
6. Tap the ScanToConnect application on the scanning device to start the scanning utility.
7. Scan the barcodes from top to bottom to configure the WLAN settings and to complete the enrollment process.

Unenrolling Windows Mobile Devices

When it becomes time to unenroll a device from AirWatch, you want to ensure that you choose the best method for your situation. This section covers the different unenrollment methods available to you.

Enterprise Wipe

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

To perform an enterprise wipe from the AirWatch Admin Console, follow the steps detailed below:

1. Navigate to **Devices ▶List View** and select the Windows Mobile device you wish 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 to confirm the Enterprise Wipe.

The device now enterprise wipes to remove corporate data and unenroll the device from AirWatch.

You can also perform an enterprise wipe from the device through the AirWatch MDM Agent. To perform a device-side enterprise wipe, follow the steps detailed below:

1. On the device, open the AW Diagnostics app.
2. Navigate to the **Advanced** tab.
3. Select **Enterprise Wipe**.

The device removes corporate data and unenroll from AirWatch.

Uninstalling the AirWatch Agent

You can also unenroll a device from AirWatch by uninstalling the AW Core Agent CAB. To unenroll through uninstall, follow the steps detailed below:

1. On the device, navigate to **Settings ▶Remove Programs**.
2. Find the AW Core Agent CAB and uninstall the program.

While the device removes corporate data, the device remains enrolled with AirWatch. This uninstall method is not the preferred method.

Windows Mobile Device Profiles

Overview

Profiles are the primary means by which you can manage devices. 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 those for Wi-Fi, VPN and passcodes, are referred to as **payloads**. It is recommended for security profiles that only one payload is associated per profile, which means you have multiple security profiles for different settings you wish to establish.

In This Section

- Configuring Profile General Settings – Each profile has General settings you must configure. This section explains the options and settings you can configure as part of the General tab.
- Deploying Passcode Payloads – Covers the multiple fields and levels of complexity for a passcode policy in the AirWatch Admin Console.
- Deploying Restrictions Payloads – Details the restriction payloads used to secure and protect Windows Mobile devices available in the AirWatch Admin Console.
- Configuring a Wi-Fi Profile – Details the steps required to push Wi-Fi settings to devices.
- Deploying Exchange ActiveSync Payloads – Creates an Exchange ActiveSync profile to allow the end user to access corporate email infrastructures from the device.
- Creating a Credential Profile – Covers certificate-based authentication for Windows Mobile devices and the configuration options available in the AirWatch Admin Console.
- Deploying and Configuring a Launcher Profile – Details configuring the Launcher profile to limit access to applications and features of a device.
- Enforcing a VPN Profile – Details deploying corporate VPN settings directly to managed devices so end users can remotely and securely access corporate infrastructure.
- Deploying Time Sync Profile – Summarizes how to sync devices with the Time Sync server to ensure all device times are accurate.
- Configuring a Shortcuts Profile – Explains the steps to create a URL Shortcuts for end users.
- Deploying a Time Zone Profile – Details how to create a Time Zone profile so end user devices are properly assigned a time zone.
- Securing Windows Mobile Devices by Time Schedules – Learn how to configure time schedules to set time-based rules to govern profile pushes and when the device user can access corporate data from their device.

Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the **General** settings for the profile. The **General** settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the payload for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed. The general settings listed below apply to any profile:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**.
2. Select the appropriate platform for the profile you wish to deploy.
3. Configure **General** settings on the applicable tab. These include:
    - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
    - **Description** – A brief description of the profile that indicates its purpose.
    - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
        - **Managed** – The profile is removed.
        - **Manual** – The profile remains installed until removed by the end user.
    - **Assignment Type** – Determines how the profile is deployed to devices:
        - **Auto** – The profile is deployed to all devices automatically.
        - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
        - **Interactive** – This is a unique assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
        - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
    - **Minimum Operating System** – The minimum operating system required to receive the profile.
    - **Model** – The type of device to receive the profile.
    - **Ownership** – Determines which ownership category receives the profile:
    - **Allow Removal** – Determines if the profile can be removed by the device's end user:
        - **Always** – The end user can manually remove the profile at any time.
        - **With Authorization** – The end user can remove the profile with the authorization of the administrator.
        - **Never** – The end user cannot remove the profile from the device.
    - **Managed By** – The Organization Group with administrative access to the profile.
    - **Assigned Organization Groups** – The Organization Groups that receive the profile.
    - **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
        - **Publish only to users in selected User Groups** – Specify one or more User Groups to receive the profile.

- **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. See Time Schedules for more information.

4. Configure a payload for the device platform.

   Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable **Platform Guide**.

5. Select **Save & Publish**.

Deploying Passcode Payloads

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

Note: As of AirWatch v6.5, the **Clear Passcode** button is no longer on the **Device Dashboard**. To perform this function, create a profile that clears the passcode. This is accomplished by navigating to **Devices ▶Profiles ▶List Views**, selecting **Add**, and then selecting **Passcode** and modifying the profile.

To enforce a Passcode profile, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Passcode** profile.
4. Configure the Passcode settings, including:
   - **Maximum Passcode Age** – Requires users to renew passcodes at selected intervals.
   - **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.
5. Select **Save & Publish** to push the profile to devices.

Deploying Restrictions Payloads

Deploy a Restrictions payload to restrict the options end users have on devices. Restrictions allow you to ensure your device is secure by controlling what a end user can use to save and store data.

To enforce a Restrictions profile, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Restrictions** profile.
4. Configure the Restriction settings, including:
   - Allow the use of the following options:
     - **Camera**

    - **External storage**
    - **Bluetooth**
- Stop the removal of the encryption on the external storage
- Require the user to encrypt the device

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

Note: You can use a Restriction payload only on Windows Mobile devices and not on Windows CE devices.

Configuring a Wi-Fi Profile

Configuring a Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted, or password protected. This can be useful for end users who travel to various office locations that have their own unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network while in an office.

To configure a Wi-Fi profile, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**. Select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Wi-Fi** profile.
4. Configure the Wi-Fi settings, including:
    - **Service Set Identifier**
    - **Network Adapter Type**
        - Standard Microsoft (Zero Wireless Config)
        - Motorola Fusion
        - Motorola Fusion (Legacy)
    - **Wi-Fi Meta Network**
        - Internet
        - Work
    - **Peer-to-peer networks**
    - **Security Type**
        - Open Authentication
        - Shared Authentication
        - WPA, WPA-PSK, WPA NONE
        - WPA2, WPA2-PSK
        - WPA Enterprise (Fusion only)
        - WPA2 Enterprise (Fusion only)
    - **Encryption**

    - WEP
    - TKIP
    - AES
- **Authentication Type**
    - EAP-TLS
    - EAP-FAST
    - PEAP
    - LEAP
    - TTLS
- **Allow Network Key**
- **Network Key**
- **Key Index**
- **Hidden**

5. If you select an **Authentication Type**, you must complete the authentication section including:
    - **Tunnel Authentication** (If applicable to your Authentication Type)
    - **Domain Name**
    - **Username**
    - **Password**
    - **Identity Certificate**
    - **Server Certificate**
6. Select **Save & Publish** to push the profile to devices.

Note: You can use a Wi-Fi payload only on Windows Mobile devices and not on Windows CE devices.

MorDeploying Exchange ActiveSync Payloads

This payload allows users to access corporate push-based email infrastructures. Use this payload to set the sync frequency for calendar and email systems.

You can use identity certificates or public key certificates with the Exchange ActiveSync payload. If supported by the network, this profile can include ad-hoc certificate requests, too.

To configure Exchange ActiveSync payloads, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Exchange Active Sync** profile.

4. Configure the Exchange ActiveSync settings, including:
    - **Login Information** – Specifies the EAS host and you can leverage user account information with look-up values, such as domain information {EmailDomain}, username information {EmailUserName} and email addresses {EmailAddress}.
    - **Settings** – Sets the Secure Socket Layer (SSL) protocol to encrypt mail traffic over port 443. Also, define intervals to sync mail and to control the size of email attachments.
    - **Restrictions** – Enables the device to use calendar, contacts, tasks, text messages, and email.
    - **Peak Days for Sync Schedule** – Creates a schedule to sync email during specific hours.
5. Select **Save & Publish** to push the profile to devices.

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

Creating a Credentials Payload

Deploy a Credentials payload to use certificates to authenticate the device with various corporate resources. The AirWatch Admin Console integrates with your public key infrastructure (PKI) so that devices can communicate securely on public networks.

As part of the Credentials payload, choose to upload certificates or distribute certificates from a defined certificate authority (CA). You can assign a certificate authority in **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Certificate Authorities**.

Note: You can use a Credential payload only on Windows Mobile devices and not on Windows CE devices.

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**. Select **Windows PC**.
2. Configure General settings for the profile.
3. Select the **Credentials** profile.
4. Configure the Credentials settings, including:
    - **Credential Source** – Uploads a certificate from your local machine or defines a **Defined Certificate Authority**.
    - **Certificate Authority** for the **Defined Certificate Authority** – Defines the external or internal CA issuing encryption keys for the PKI.
    - **Certificate Template** for the **Defined Certificate Authority** – Specifies the predefined template for the CA to use when requesting a certificate.
    - **Certificate Store** – Defines the store on the device where the certificate is located. Choose from **Personal Certificates**, **Intermediate Certification Authorities Store**, **Trusted Root Certification Authorities**, and **Software Publisher Certificates**.
5. Select **Save & Publish** to push the profile to devices.

Note: The latest versions of the AirWatch MDM Agent for Windows Mobile fully support the silent installation of certificates. This allows certificates to be installed on a device without requiring the end user to approve the installation of the certificate.

Deploying and Configuring the Launcher Payload

Configure the AirWatch App Launcher with a profile in the AirWatch Admin Console. You can also configure it on the device if you have the Admin passcode.

Configuring the Launcher Payload

The AirWatch App Launcher restricts user access to a list of allowed applications as well as other native features on the device.

Note: For more on applicable AirWatch profiles for Windows Mobile devices, see Deploying Profiles.

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Launcher** profile.
4. Enter a **Title** for the launcher profile. You can use the supported AirWatch Lookup Values. Select for a list of all AirWatch supported Lookup Values.
5. Define an **Administrative Passcode** for setting configurations on the device.
6. Enter the **Allowed Applications**, including the following options:
   - **Application Name** – Specifies the application name that displays in the AirWatch App Launcher.
   - **File Path to Exe** – Defines the file path of the application and includes the executable file.
   - **Arguments** (Optional) – Enter any command line arguments to run the application.
   - **Hide** – Masks the application on the device.
   - **Launch On Start** – Launches the application when the AirWatch App Launcher starts.
   - **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 being able to close the app. Select this only for dedicated use applications.
   - **Enable Home Button** – Allows you to minimize a whitelisted application and return to the main App Launcher page while keeping the current session active for that program. If you want to return to the minimized program, 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 using **Upload Icon** below.
   - **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 field as described above.
7. Enter the application **Settings**.
   - **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.

Note: When selected, all other settings, except for **View Time**, **Disable Active Sync**, **Disable Keyboard**, and **View IP Address** are disabled since 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.
- **View Wifi Signal** – Displays the signal strength of the Wi-Fi signal.
- **View Cell Signal** – Displays the signal 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.

8. Choose the Tools to be available in the **Tools Menu** of the launcher:
Allows the user to customize and manage the contents of the Tools Menu on the Launcher. The admin 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 directly configure this on a device, provided the **Configure** option is enabled.

   - **Restart AW Agent** – 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.
   - **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. Prior versions are capable of only supporting the last profile published.

     Note: Multiple Profile Support requires Windows Mobile AirWatch Agent version 4.0.0.13 or above as prior versions are capable of *only* supporting the last profile published.

   - **Configure** – Allows the user to configure all areas of the Launcher directly on the device, including **Allowed Applications**, **Settings**, and **Tools Menu**.

Configuring the AirWatch App Launcher on the Device

To make Admin configurations in the AirWatch App Launcher, follow the steps detailed below:

1. Open the AirWatch App Launcher application on the device.
2. Enter the Admin passcode in the **Password** field and Select **Accept**.
3. Select the applicable option according to what you want to do on the **Allowed Applications** tab. Your options include to **Import**, **Export** and **Add** applications from and to the list.
4. Select **Add** to add an application and complete the following options on the **Add Application** screen:
    - **Application Location** – Defines the file path of the application or select the **Browse** option.
    - **Application Name** – Defines the name of the application to display in the AirWatch App Launcher.
    - **Arguments** – Defines command line arguments to run the application.
    - **Launch On Start** – Launches the application when the AirWatch App Launcher is started.
    - **Hide from User** – Masks the application in the user interface.
    - **Console Application** – Defines the application as not having a user interface or as a background process.

Enforcing a VPN Profile

Create a VPN Profile to deploy corporate VPN settings directly to managed devices. This allows end users to remotely and securely access corporate infrastructure.

To enforce a VPN profile, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **VPN** profile.
4. Configure the VPN settings, including:
    - **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.
    - **Authentication** – Defines the authentication for the VPN.
        - **Certificate** – Use this option to deploy certificate-based authentication for your VPN connections. You must choose this option if you select the **Connection Type, IPSec/L2TP** in your VPN profile. You must also use this option for authentication if you select the Wi-Fi profile with the **EAP Type, Smart Card, or Certificate**.
        - **Pre Shared Key** – Use the PSK option when you have a shared secret that device users utilize to access the VPN. This authentication type often uses symmetric key algorithms for security.

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

Note: You can use a VPN profile only on Windows Mobile devices, but not on Windows CE devices.

Deploying Time Sync Payloads

Deploy Time Sync payloads to synchronize the system time on Windows Mobile devices with primary and secondary time server to ensure that the device fleet runs on the same clock. This is useful for global networks with devices in numerous time zones.

nDeploying Shortcut Profiles

Deploy custom labeled icons that are associated to a specific URL. The admin has the ability to add as many icons as needed to a shortcut payload. The admin uploads the icon image file into the AirWatch Admin Console. Once the payload is published, the icon is pushed to the user's device. When the user selects the start button, the shortcut icon appears on the user's main programs screen.

Configuring a Shortcuts profile allows you to save URLs for your end users to access.

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**. Select **Windows Mobile**.
2. Configure General settings for the profile.
3. Select the **Shortcuts** profile.
4. Configure the Shortcuts settings, including:
   - **Label** – Name associated to the icon that displays on the user's device.
   - **URL** – URL for the website in which the user is advanced to when user taps on the icon.
   - **Icon** – Image file that displays on the user's device that is associated to the URL.
5. Select **Save & Publish** to push the profile to devices.

Deploying Time Zone Profiles

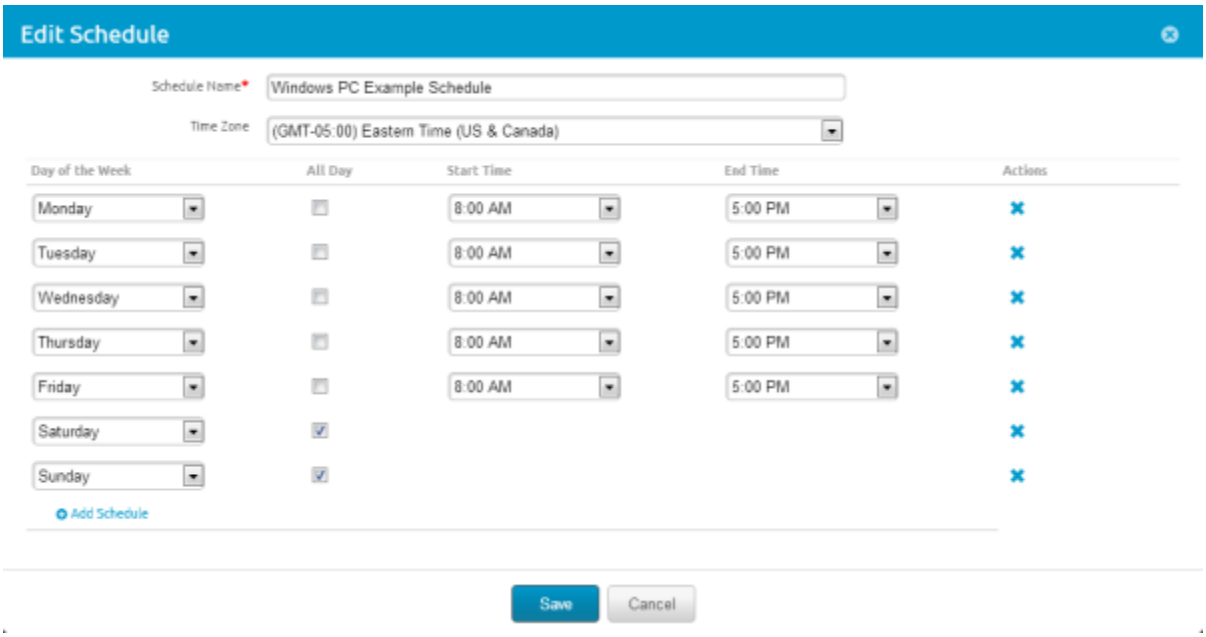
Allows the AirWatch admin to configure time zones by pushing a profile to the user's device from the console. This eliminates having to remote control into the end-user's device to manually set the time zone. The profile allows you to manage times zones on the user's devices based on their Organization group or by setting it manually. Once the payload is published, the time zone is pushed to the user's device, the device displays the time zone, and all device activity is time stamped based on that time zone regardless of the actual device location.

Set a Time Zone in the AirWatch Admin Console by performing the following steps:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**. Select **Windows PC**.
2. Configure General settings for the profile.
3. Select the **Time Zone** payload, Select on the **Time Zone Setup** dropdown, and select **Set Time Zone Manually**.
4. Select the **Time Zone** dropdown and select the appropriate time zone from the list.

Time Schedules

In addition to simply assigning applicable profiles, you have the ability to enhance device management further by controlling when each profile assigned to the device is active. Configure and apply time schedules to restrict when profiles are active on the device. Applying time schedules to profiles secures your corporate resources by only allowing employees access during the specific days and time frames. Conversely, applying time schedules can also limit personal content and access during work hours.



In This Section

- Defining Time Schedules – See how to create a time schedule, which allows or denies access to internal content and features based on the day and time.
- Applying a Time Schedule to a Profile – See how to apply a time schedule to a profile, which lets you control when and how a particular profile is activated.

Defining Time Schedules

To create a time schedule:

1. Navigate to **Devices ▶Profiles ▶Settings ▶Time Schedules**.
2. Select **Add Schedule** to launch the **Add Schedule** window.
3. Enter a name for the schedule in the **Schedule Name** field.
4. Select the applicable **Time Zone** using the drop-down menu.
5. Select the **Add Schedule** hyperlink.
6. Select the **Day of the Week**, **Start Time** and **End Time** using the applicable drop-down menus. You can also select the **All Day** check box to disable start and end times for the schedule.
   To remove a day from the schedule, select the applicable **X** under **Actions**.

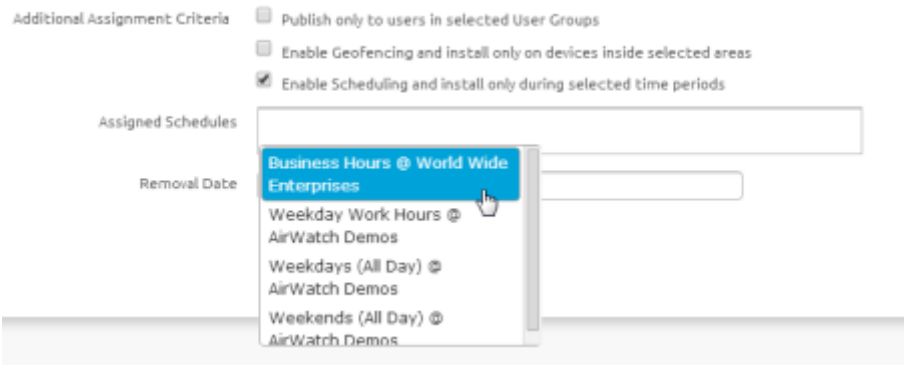
7. Repeat steps 5 and 6 as many times as is necessary to add additional days to the schedule.
8. Select **Save**.

Applying a Time Schedule to a Profile

Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles. For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming or YouTube content based on ratings and other settings.

Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

1. Navigate to **Devices ▶Profiles ▶List View ▶Add** and select your platform.
2. Select **Enable Scheduling and install only during selected time periods** on the **General** tab. An **Assigned Schedules** box displays.



3. Enter one or multiple Time Schedules to this profile.
4. Configure a payload, such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the time frames.
5. Select **Save & Publish**.

Compliance

The **Compliance Engine** is an automated tool by AirWatch that ensures all devices abide by your policies. Your policies may include basic security settings such as requiring a passcode and having a minimum device lock period. You may also decide to set password strength, blacklist certain apps and require device check-in intervals to ensure devices are safe and in-contact with the AirWatch servers.

Once configuration is complete and devices are out of compliance, the Compliance Engine begins to warn the user to fix compliance errors to prevent disciplinary action on the device. For example, if a user loads blacklisted games or social media apps onto their device, the Compliance Engine sends a message to notify the user that their device is out of compliance. If the errors are not corrected in the amount of time specified, the device loses access to certain content and applications.

You may even automate the escalation process if corrections are not made. Lock down the device and notify the user to contact you to unlock the device. These escalation steps, disciplinary actions, grace periods and messages are all completely customizable with the AirWatch Admin Console.

Enforcing mobile security policies is as easy as:

- **Building your policies** – Customize your policy to cover everything from application list, compromised status, encryption, model and OS version, passcode and roaming.
- **Defining escalation** – Configure time-based actions in minutes, hours or days and take a tiered approach to those actions.
- **Specifying actions** – Send SMS, email or push notifications to the user's device or send an email only to an Administrator. Request device check-in, remove or block specific profiles, install compliance profiles, remove or block apps and perform an enterprise wipe.

In This Section

- Enforcing Device Compliance – Details the general process for setting up Compliance policies and the Compliance Engine.

Enforcing Device Compliance

Follow the steps below to set up and initiate the Compliance Engine complete with profiles and automated escalations:

1. Navigate to **Devices ▶Compliance Policies ▶List View** and select **Add**. Match **Any** or **All** rules to detect conditions. Select **Next** when rule definition is complete. The supported compliance policies by Platform are as follows:

Compliance Policy	Apple iOS	Android	Windows Mobile (Motorola)	Windows Phone 8
Application List	✓	✓		
Compromised Status	✓	✓		✓
Device Last Seen	✓	✓	✓	
Encryption	✓	✓		✓
Interactive Certificate Profile Expiry	✓	✓		
Last Compromised Scan	✓	✓		
MDM Terms of Use Acceptance	✓	✓		
Model	✓	✓		✓
OS Version	✓	✓		✓
Passcode	✓	✓		✓
Roaming	✓	✓		
SIM Card Change	✓	✓		

- **Application List** – Detect specific, blacklisted apps that are installed on a device, or detect all apps that are not whitelisted.

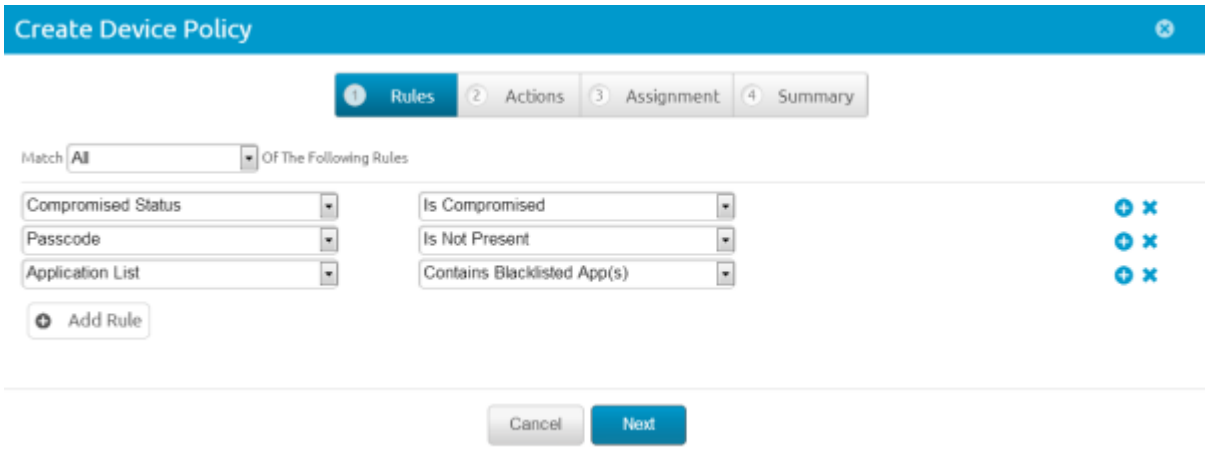
  You can either specifically prohibit certain apps, such as social media or entertainment apps, or specifically permit only the apps you specify, such as internal applications for business use.

- **Compromised Status** – Select if the device is non-compliant when compromised.

  Prohibit the use of jailbroken devices that are enrolled with AirWatch. Jailbroken devices strip away integral security settings and may introduce malware in your network and provide access to your enterprise resources. Monitoring for compromised device status is especially important in BYOD environments where employees have various versions of devices and operating systems. For more information, refer to the **Detecting Compromised Devices** document available on the AirWatch Resources Portal.

- **Device Last Seen** – Select if the device is non-compliant when the device fails to check in within an allotted time window.

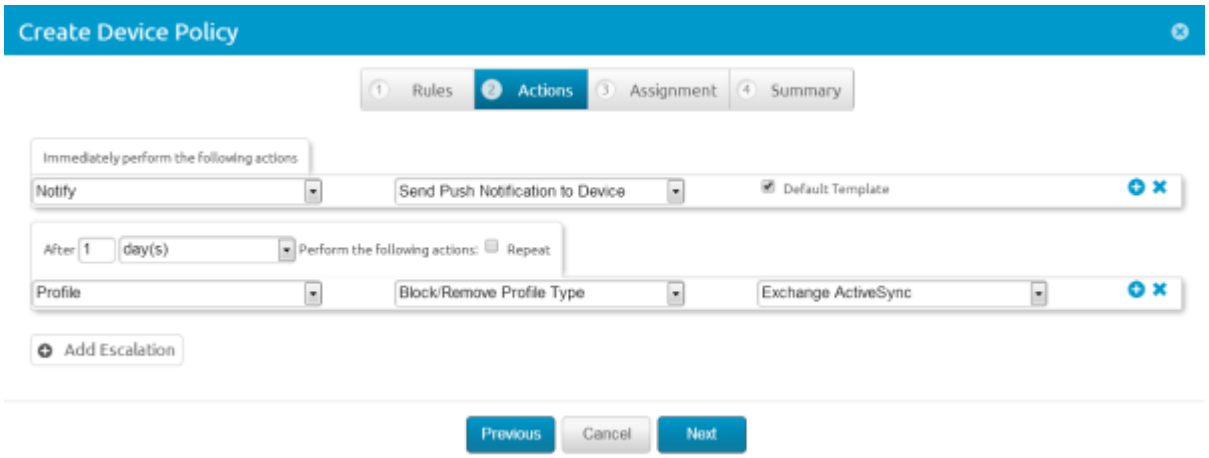
- **Encryption** – Select if the device is non-compliant when Encryption is not enabled.
- **Interactive Profile Expiry** – Select if the device is non-compliant when an installed profile expires within the specified length of time.
- **Last Compromised Scan** – Select if the device is non-compliant when AirWatch is unable to successfully query the device on schedule.
- **MDM Terms of Use Acceptance** – Select if the device is non-compliant when the current MDM Terms of Use have not be accepted by the end user within a specified length of time.
- **Model** – Select if the device is non-compliant based on a specific platform.
- **OS Version** – Select if the device should be marked as non-compliant when it is within a certain window of OS versions that you configure.
- **Passcode** – Select if the device is non-compliant when a passcode is not present.
- **Roaming** – Detect if the device is roaming.
- **SIM Card Change** – Select if the device is non-compliant when the SIM Card has been replaced.



2. Specify **Actions** and **Escalations** that occur. Select the type of action to perform: **Application**, **Command**, **Notify**, **Profile**, or **Email**.

Note: Block Email applies if you are using Mobile Email Management and the Email Compliance Engine, which is accessed by navigating to **Email ▶Compliance Policies ▶Email Policies**. This lets you use Device Compliance policies such as blacklisted apps in conjunction with any Email Compliance Engine policies you configure. With this Action selected, email compliance is triggered with a single device policy update if the device falls out of compliance.

Increase security of actions over time by adding Escalations. Select **Next** when all actions and escalations are added.



3. Configure **Assignment** and **Activate Policy**. Define the devices, Organization Groups and user groups to receive the policy. Enter a policy name, view a snapshot and select **Finish & Activate** to launch the new rule.

You can enforce application compliance as well by establishing a whitelist, blacklist or required list of applications. For more information on establishing a robust and effective Mobile Application Management (MAM) plan, please see the **AirWatch MAM Guide**.

AirWatch Windows Mobile Agent

Overview

You can use AirWatchAgent for Windows Mobile devices to add additional functionality to the devices. This section covers configuring and using the Agent to get the most out of your device.

In This Section

- Configuring the AirWatch Agent – Explains how to deploy the agent as a .CAB file to enroll a device.
- Configuring More Windows Mobile Options – Details how to configure additional settings in the AirWatch MDM Agent including advance settings and power on password.
- Using the Application Manager and the Diagnostics Utility – Explains that using these tools help provision devices with packages and help view the status of devices.
- Product Provisioning – Summarizes the Product Provisioning system that allows you to provision profiles, files/actions, and/or applications to a Windows Mobile device.

Configuring the AirWatch Agent

The AirWatch solution deploys the AirWatch Agent as a CAB file to Windows Mobile and Windows CE devices.

1. Use the **APPLICATION MANAGER PACKAGE SCHEDULER** to define a schedule for devices with the AirWatch Agent v3.3 to retrieve products provisioned on schedule.
    - The **Application Manager Scheduler** defines when the AirWatch Application Manager utility on the device synchronizes with the AirWatch Admin Console.
    - The **Randomization Windows** option sets a time range to push applications randomly to manage traffic and bandwidth on the mobile network.

Notes: The application manager package scheduler for the AirWatch Agent v4.0 is built into the **Manifest** and you define it when you create the provisioning package. For information about the AirWatch Application Manager, see the **Mobile Application Management Guide**.

Configuring More Windows Mobile Options

Configure other options for Windows Mobile devices to prepare for possible issues. Find these options in **Groups & Settings ▶All Settings ▶Devices & Users ▶Windows ▶Windows Mobile**.

- **Power on Password** – Protects Windows Mobile devices during loss or theft.

Note: Power on Password is *only* for Athena and requires the PoP CAB, which is a separate CAB component. You can perform a similar function through the AirWatch agent by pushing down a "Passcode" profile.

- **Advance Settings** – Installs a loader for Windows Mobile devices and a warm boot file.

Configuring Power on Password

Use the **Power on Password** option to control system BIOS password options to secure the device from unauthorized users when they turn on the device.

To configure the Power on Password option, follow the steps details below:

1. Navigate to **Groups & Settings ▶All Settings ▶Devices & Users ▶Windows ▶Windows Mobile**.
2. Select **Power on Password** and set the options, including:
   - **Force Password Expiration** – Forces the password to expire so that the user must change the password.
   - **View Power On Password** – Enables the user to see the password they enter.
3. Select **Save**.

Configuring Advanced Settings

Use these options to update applications on Windows Mobile devices and to reset devices.

- **Path to App Update** – Enter the path to the AppUpdate.exe file so that this loader can check for updates, install the updates and load and run the applications it updates.
- **Intermec Reboot Exe** – Enter the path to the Reboot.exe file on Intermec devices used to warm boot the device.

Using the AirWatch Application Manager and the AirWatch Diagnostics Utility

Installing the AirWatch Agent on to Windows Mobile devices adds the AirWatch Application Manager and the AirWatch Diagnostics utility. These tools help provision Windows Mobile devices with packages and help view the status of devices using the AirWatch Admin Console.

Using the AirWatch Application Manager

The AirWatch Application Manager processes provisioning packages that come from the AirWatch Admin Console. It also reports the status of the provision process. Control the sync schedule for communicating with the AirWatch Admin Console.

To configure, go to **Groups & Settings ▶All Settings ▶Devices & Users ▶Windows ▶Windows Mobile ▶Agent Settings**. Navigate to the **Application Manager Package Scheduler** section. The Application Manager distinguishes provisioned package using the following categories:

- **Required** – View packages that are required for the mobile device.
- **Interactive** – View optional packages that you can provision to the device.
- **Installed** – View packages that are provisioned and installed on the device.

Note: Use the **Install** and **Refresh** options to put optional packages on the device and to refresh package lists.

Using AirWatch Diagnostics

The AirWatch Diagnostics utility provides data about the Windows Mobile device to the AirWatch Admin Console. This utility can send the following information:

- System data
- AirWatch Cloud Messaging (AWCM) Service information
- GPS data
- Enterprise Wipe and Device Wipe commands

Product Provisioning

Product Provisioning allows you to create products to configure and update devices. These products push profiles, files/actions, and/or applications to a device based on the configuration of the product. Profiles provide Wi-Fi, VPN, Credentials, and more for the device so it can remain connected and up-to-date. The files/actions and applications download and install what the device needs to perform it's job. Products can check the device against a list of user-defined conditions for the proper time to download and install the product onto the device. This allows you to ensure a device is ready for the files and updates you wish to push to them.

Through the use of relay servers, products can be periodically pinged to ensure compliance between device and the product. The relay servers allow you to create a FTP or FTPS server to push or pull products to a device. Relay servers can also be used to create staging profiles that use the Motorola Rapid Deployment Barcode Enrollment method or other staging methods to quickly and easily stage a device for later use by the end user.

For more information on creating and using Product Provisioning, please see the **AirWatch Product Provisioning Guide.**

Managing Windows Mobile Devices

Overview

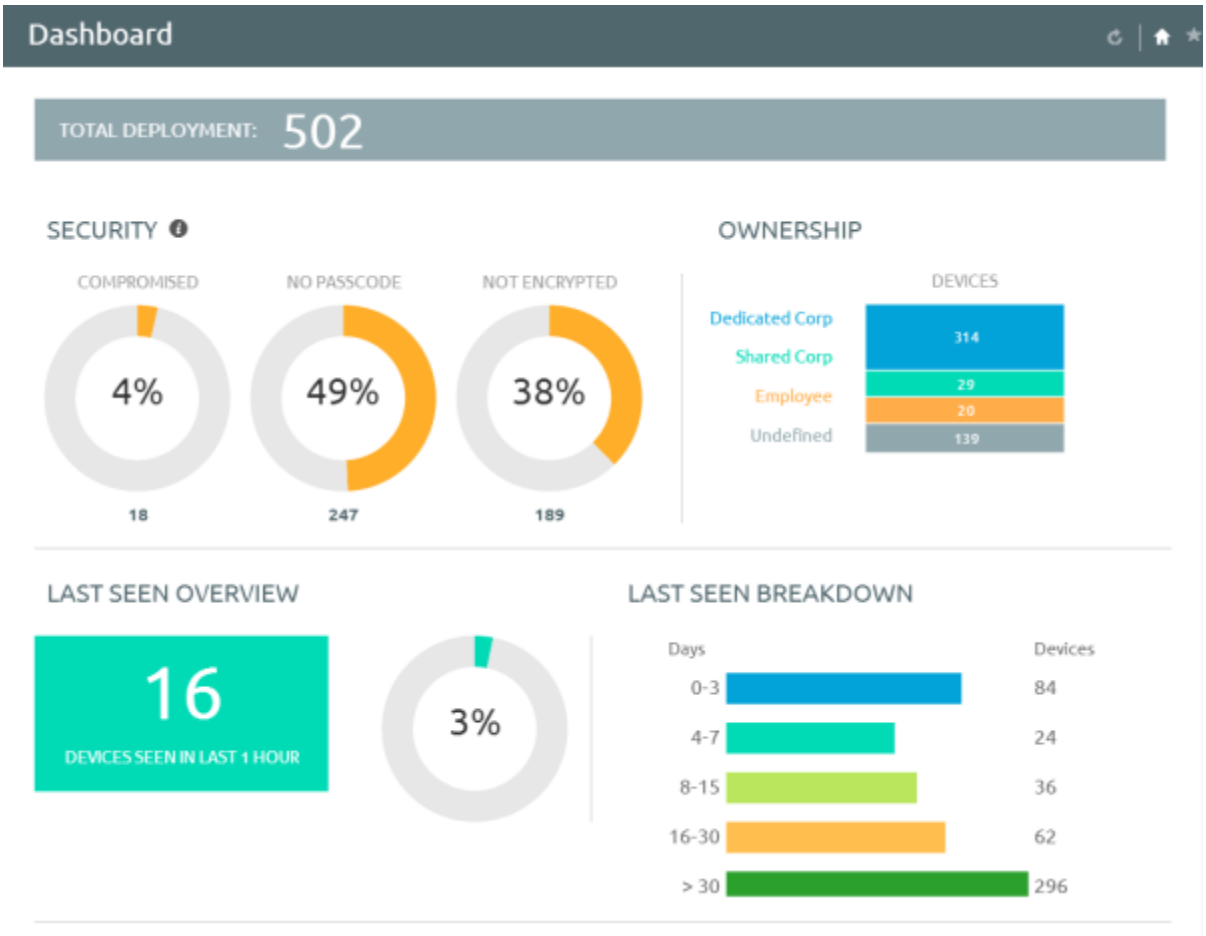
You can manage all of your deployment's devices from the AirWatch **Dashboard**. The **Dashboard** is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. In addition, you can set up the **Self-Service Portal** (SSP) to empower end users to manage their own devices and reduce the strain on Help Desk personnel.

In This Section

- Using the Device Dashboard – Covers stats and data about your devices available in the Device Dashboard.
- Using the Device List View – Details how to use the Devices List View to search for, filter, and perform remote actions on multiple Windows Mobile devices.
- Using the Device Details Page – Walks through the ways you can manage Windows Mobile devices from using the Device Details Page in the AirWatch Admin Console.
- Utilizing Reports – Presents reports and collected data within the AirWatch Admin Console featuring detailed information on all aspects of your deployment.
- Using the Hub – Presents the data flow within AirWatch Hub and how to use the data within.
- Using the Self-Service Portal (SSP) – View relevant device information for enrolled devices and perform remote actions such as clear passcode, lock device, or device wipe from your device or PC.

Using the Device Dashboard

As devices are enrolled, view and manage them from the AirWatch **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet of mobile devices while allowing a quick and easy way to drill down to individual devices and take MDM actions. View graphical representations of relevant statistics, including important device information for your fleet, such as device ownership type, compliance statistics and platform breakdown.



Select any of the available data views from the **Device Dashboard** to quickly access each set of devices in the **List View**. From this **List View**, take administrative action, including send a message, lock devices, delete devices and change groups associated with the device.

Using the Device List View

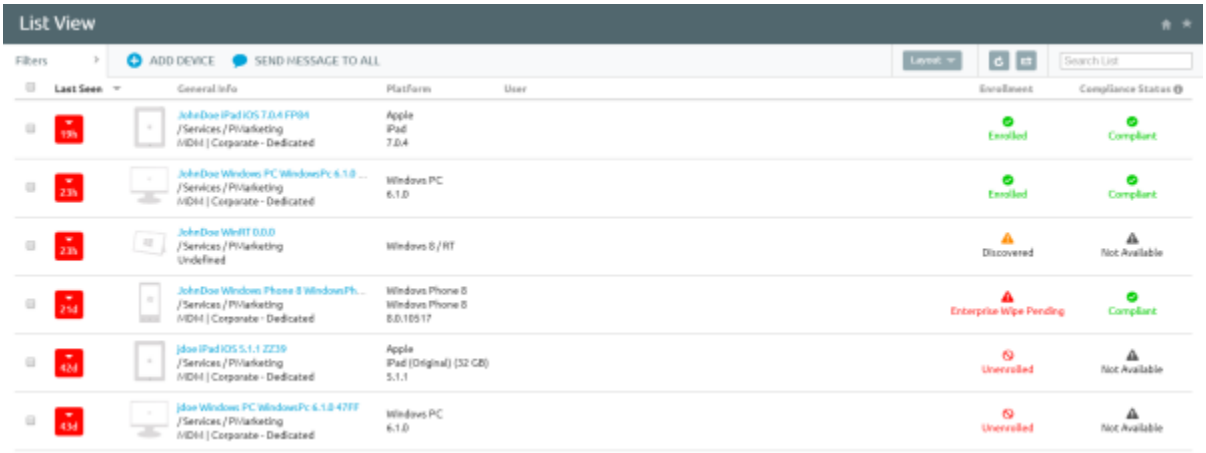
Switch to **List View** (**Devices ▶List View**) at any time to sort and manage devices by filtering the columns and fields available in the **Device Dashboard**, including:

- Last Seen
- Friendly Name
- Ownership
- Username
- Display Name
- Platform/OS/Model

- Corporate - Dedicated
- Corporate - Shared
- Employee-Owned

- Organization Group
- Compliance Status

Select on a device Friendly Name at any time to open up the device details page for that device.



Sort columns and configure information filters to gain insight on device activity based on specific information you are curious about. For example, sort the **Compliance Status** column to view only devices that are currently out-of-compliance and take action or message only those specific devices. Search all devices for a friendly name or user's name to isolate one device or user. Once you have sorted or filtered dashboard information, export, save and send the data for review.

Using the Search List, Filters, and Bulk Messaging

At times, you will need to search for a single device for quick access to its information and take remote action on the device. For example, search for a specific device, platform or user. Navigate to **Devices ▶List View ▶Search List** and search for all devices within the current Organization Group and all child groups.

You can also drill down to specific sets of devices by filtering device criteria, including by **Platform**, **Ownership Type**, **Passcode**, **Last Seen**, **Enrollment**, **Encryption** and **Compromised** status.

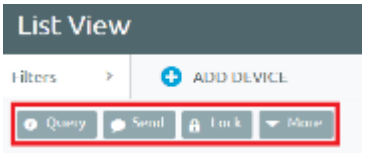
You can also search specific information across all fields associated with devices and users, allowing you to search user name ("John Doe") or device type.

Once you have applied a filter to show a specific set of devices, perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the **Management** tabs.

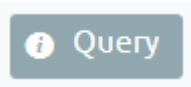
Using the Management Tabs

With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

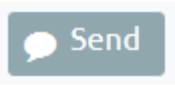
Note: The actions listed below vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.



With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:



Query – Query all selected devices for current device info, including last seen, OS, model and compliance status.



Send – Access Send Message menu and compose message to send to selected devices.

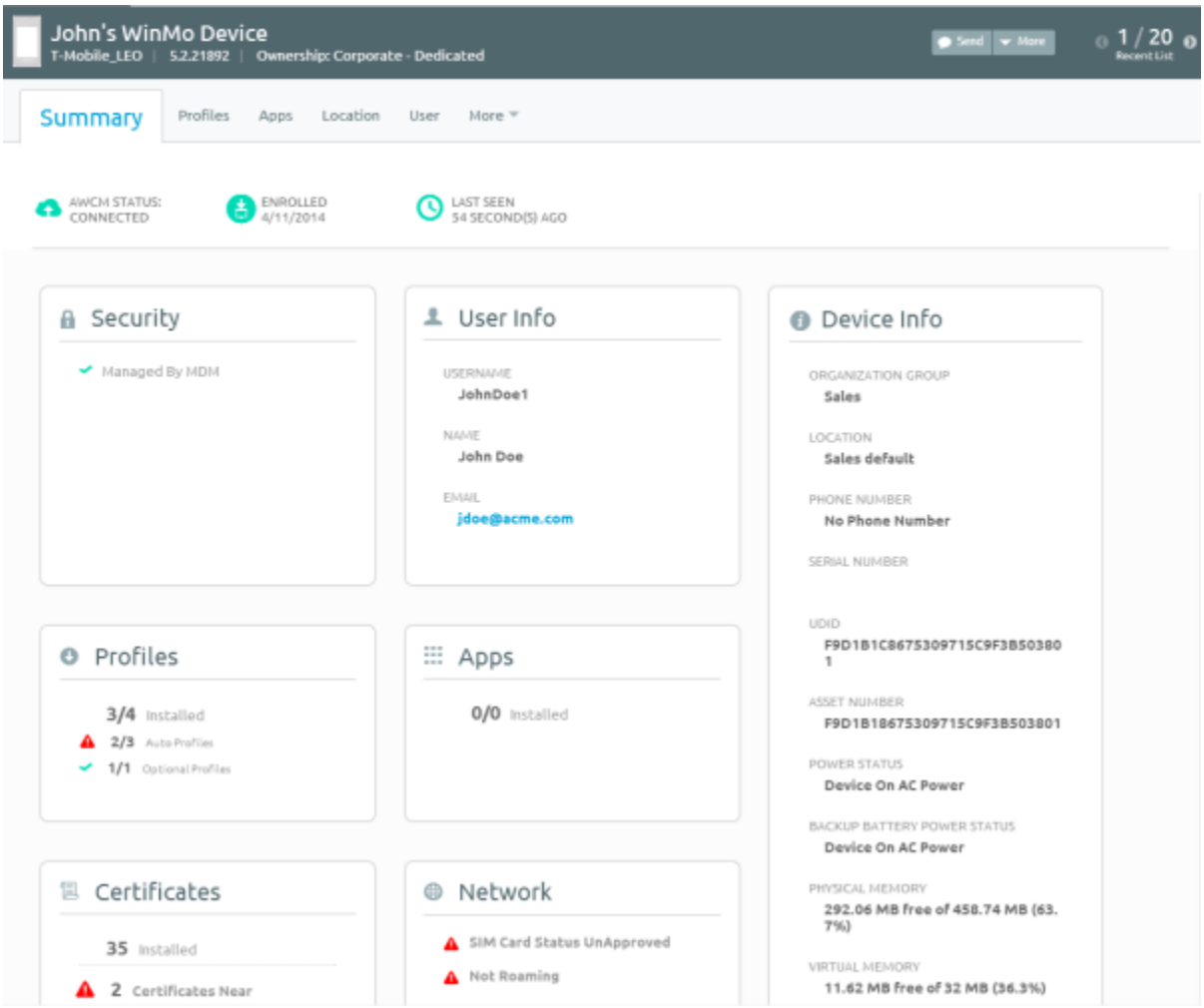
Lock – Lock all selected devices and force users to re-enter device security PIN.

More – View commands that you can perform on all selected devices. For example:

- **Management** – Query, lock or perform Enterprise Wipe on all selected devices.
- **Support** – Send a message to a device with instructions or communication to end user. Locate current GPS location of all selected devices.
- **Admin** – Change AirWatch Admin Console settings, including changing Organization Group, Ownership type or device group of selected devices or deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices. Select Provision Now to perform a number of configuration for selected devices. Select Install Product to install a particular apps to selected devices.

Using the Device Details Page

Use the Device Details page to track detailed device information and quickly access user and device management actions. You can access the Device Details page by either selecting a device's Friendly Name from the Device Search page, from one of the available Dashboards or by using any of the available search tools with the AirWatch Admin Console.



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

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, Organization Group, contact information, serial number, power status, storage capacity, physical memory and virtual memory.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View all apps currently installed or pending installation on the device.
- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

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

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Security** – View current security status of a device based on security settings.
- **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
- **Certificates** – Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
- **Products** – View complete history and status of all packages provisioned to the device and any provisioning errors.

- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Alerts** – View all alerts associated with the device.
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.
- **Status History** – View history of device in relation to enrollment status.
- **Targeted Logging –** Enable and view logging for this device.
- **Attachments –** Add files associated to the device.
- **Advanced Metrics –** View advanced metrics for the device.

Performing Remote Actions

The **More drop-down** on the Device Details page enables you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.

Note: The actions listed below vert depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.

- **Query –** Query the device for specific information.
- **Clear Passcode –** Clear the device passcode.
- **Management –** Perform an enterprise wipe to clear corporate data or an enterprise reset enabling you to reset a device while allowing persistent agents, profiles, and file/actions to remain and reinstall. For more information on persisting agents, profiles, and files/actions, see the **AirWatch Product Provisioning Guide**.
- **Support –** Perform support actions such as sending the device a message, remote view, requesting a check-in, and remote control.
- **Admin –** Change AirWatch Admin Console settings, including changing Organization Group, and editing/deleting devices from AirWatch MDM.
- **Advanced –** Access the file manager, task manager, or registry manager, perform a warm boot, start and stop AWCM, and more.

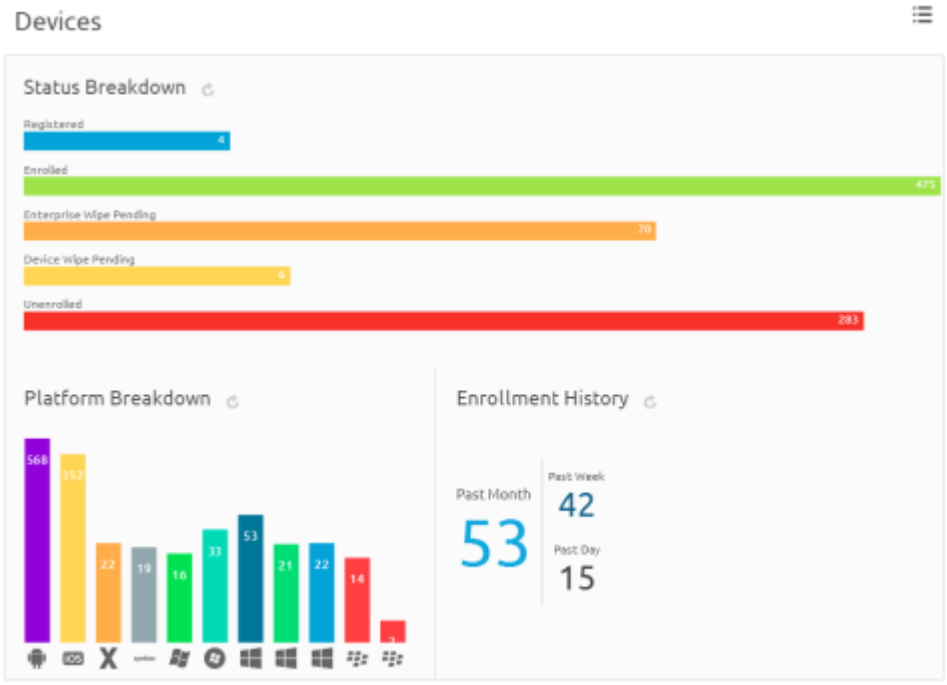
Utilizing Reports

AirWatch has extensive reporting capabilities that provide administrators with actionable, result-driven statistics about their device fleets. IT administrators can leverage these pre-defined reports or create custom reports based on specific devices, User Groups, date ranges or file preferences.

In addition, the administrator can schedule any of these reports for automated distribution to a group of users and recipients on either a defined schedule or a recurring basis. For example, you can run reports to see the number of compromised devices, how many devices there are for a specific make or model, or the total amount of devices running a particular version of an operating system.

Using the Hub

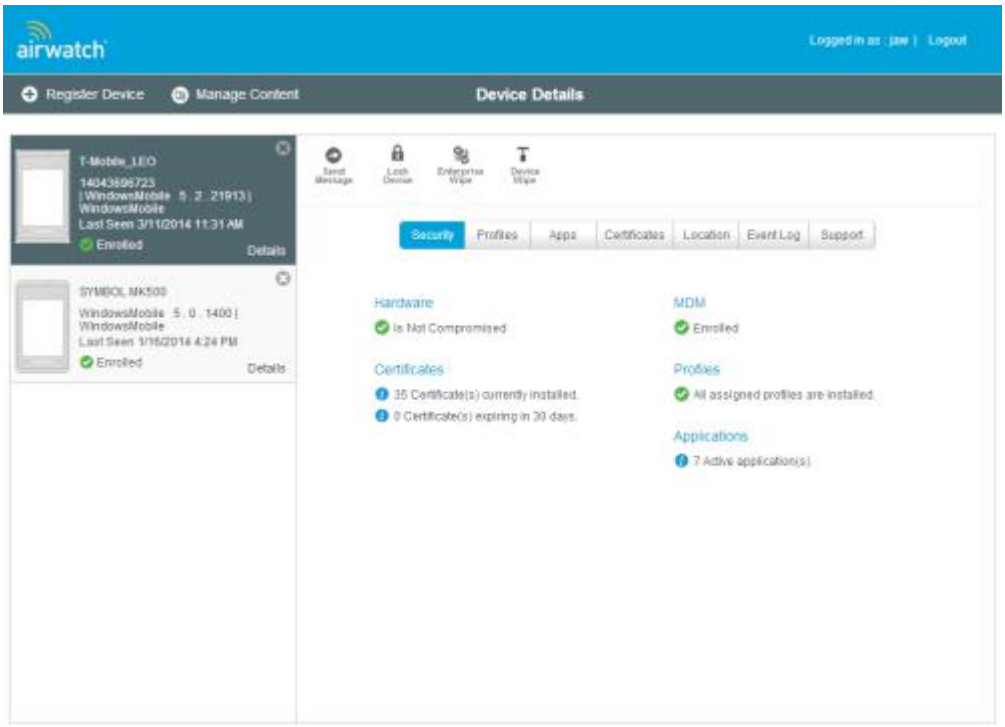
Utilize the AirWatch Hub as your central portal for fast access to critical information. Quickly identify important issues or devices and take action from a single location in the AirWatch Admin Console. Select any metric to open the **Device List View** for that specific set of devices, where you can perform actions such as sending a message to those devices.



For more information about using the Hub to filter and view specific information, refer to the Managing Devices section of the **AirWatch Mobile Device Management Guide**.

Using the Self-Service Portal (SSP)

The **AirWatch Self-Service Portal** (SSP) allows end users to remotely monitor and manage their smart devices. The Self-Service Portal lets you view relevant device information for enrolled devices and perform remote actions such as clear passcode, lock device, or device wipe.



Using the SSP

Logging into the SSP

You can access the SSP by logging in through a browser. To do this, navigate to the SSP website using the URL provided to you. It should look similar to this format: **https://mdm.acme.com/mydevice**. Once you launch the SSP, you can log in using the same credentials (**Group ID**, **username** and **password**) you used to enroll in AirWatch. Optionally, if Email Domain registration is configured, you can log in using your corporate email address.

Selecting a Device in the SSP

After logging in to the SSP, a list of all devices tied to your user account displays on the left. Select the device you want to manage. The **Device Details** screen displays.

Viewing Device Information

The following tabs display device-related information:

- **Security** – This tab displays the information specific to security controls currently in place for the device, including: enrollment status, assigned profile status, installed certificate status, certificates nearing expiry and installed applications.
- **Compliance** – This tab shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure devices remain compliant and operate as intended.
- **Profiles** – This tab shows all of the MDM profiles that have been sent to the devices enrolled under your user account and the status of each profile. From the Profiles view, you can select the install icon ( )to install a profile or the delete icon ( ) to remove it from the device.
- **Apps** – This tab displays all applications that have been installed on the selected device and provides basic application information.

- **Certificates –** This tab displays a detailed listing of certificates currently assigned to and installed on the device. From the Certificates view, you can deactivate, renew or remove a certificate, if allowed.
- **Event Log** – This tab contains a comprehensive log of all interactions between the AirWatch Admin Console and the device.
- **Support** – This tab contains detailed device information and contact information for your organization's support representatives.

Perform Remote Actions

The **Remote Actions** enable you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.

Note: All remote action permissions are determined by your administrator and therefore you may not be able to perform all listed actions.

- **Device Query** – Requests the device to send a comprehensive set of MDM information to the AirWatch Server.
- **Send Message** – Sends an Email, SMS (text) or Push Notification over-the-air to the selected device.
- **Lock Device** – Locks the selected device so that an unauthorized user cannot access it. This feature is useful if the device is lost or stolen.
- **Enterprise Wipe** – Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies and internal applications. The device returns to the state it was in prior to the installation of AirWatch MDM.

Appendix A – Over-the-Air Migration

Overview

You can perform over-the-air (OTA) migration from an older WinMo/WinCE Agent to a newer one or from Athena to the latest Agent through package provisioning.

In This Section

- Migrating from an Older Agent – Explains how to migrate from an older agent to a newer agent.

Migrating from an Older Agent

Migrate by following these steps:

1. Download the Installer CAB for the appropriate platform.

   Some of the older releases followed a different software naming convention. The name of the agent to uninstall can be specified as a registry entry within the Installer CAB [HKEY_LOCAL_MACHINE\Software\AirWatch\AWInstall]. This could be any of AirWatch Device Agent, AirWatch Core Agent, or AirWatch Interrogator Device Agents 3.x and needs to be customized before deployment.

2. Create a provisioning package with the following manifest actions. For replacing Athena, The agent type should be **Legacy**.

   a. Create the Folder: **\Program Files\AWAgentInstall**.

   b. Download the latest Agent CAB to **\Program Files\AWAgentInstall\Airwatch-CoreAgent.cab**. The target must be named exactly as stated.

   c. Download the **AirWatch Agent Installer WinMo.cab** to **\Temp\AW.cab**.

   d. Install **\Temp\AW.cab**.

   e. Process Run **"\Program Files\AWAgentInstall\AWAgentInstallStart.exe"**.

   Note: Make sure you type double quotes around the path above.

   f. Set the timeout to -1.

   Note: Entering -1 for the timeout causes the application to never timeout while it is running so it will run until it is complete.

Appendix B – XML Provisioning

Overview

The 5.X version of the AirWatch MDM Agent for Windows Mobile now supports XML provisioning. XML provisioning allows a client admin to take a custom designed XML file and download it to a device in a provisioning product. After the file is downloaded, it will execute an install command to extract the settings from the XML file and install them on the device. This feature provides added flexibility in terms of implementing custom configuration options for Windows Mobile devices which are currently enrolled in AirWatch.

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

Creating an XML Product

1. Navigate to **Devices ▶Product (New) ▶File/Actions ▶Add**.
2. Select **Windows Mobile**.
3. Enter in the required settings on the **General** tab then select the **Files** tab and upload the desired XML file and enter in 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 ▶Product (New) ▶List View ▶Add**.
7. Select **Windows Mobile.**
8. Enter the **General** information.
9. Select the **Manifest** tab.
10. Select **Install Files/Actions** and choose the files and actions just created.
11. **Save** and **Activate** the product.

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

Note: The old product provisioning should also work with XML provisioning as long as the 5.X agent is installed on the device.

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

```
<?xml version="1.0"?>
-<wap-provisioningdoc>
  -<characteristic type="Registry">
    -<characteristic type="HKLM\Software\AirWatch\Test">
      <parm datatype="integer" value="5" name="TestValue"/>
      <parm datatype="boolean" value="1"name="TestValueBoolean"/>
```

```
      </characteristic>
   </characteristic>
</wap-provisioningdoc>
```

Appendix C – AWScript Reference

Overview

AWScript is a component that implements device-side scripting capabilities for Windows Mobile and Windows CE devices. It uses a dialect of BASIC as its core scripting language and adds AirWatch specific extensions on top. An AWScript script is a plain ascii or utf-8 text file with an extension of .aws. This file extension is handled specially by the other agent components like the Application Manager.

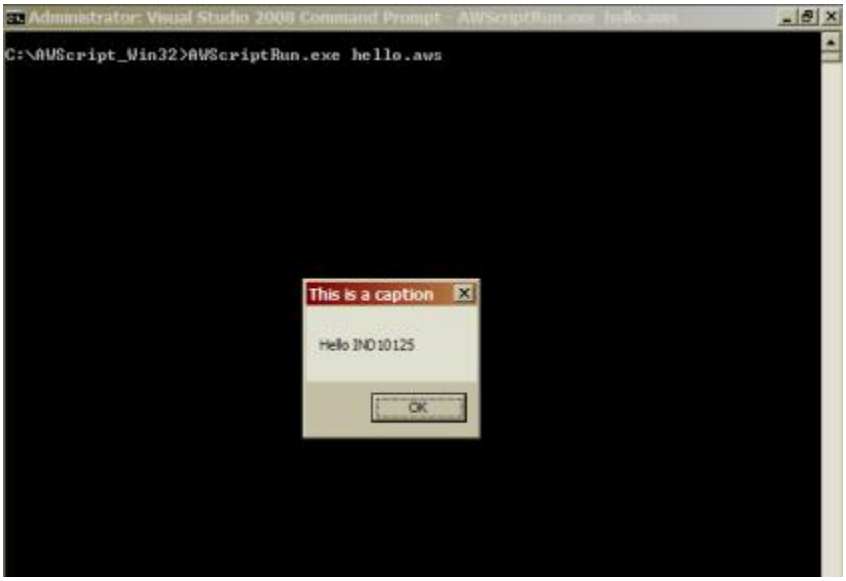
For testing and development, there is a Win32 port of AWScript that can be downloaded from this location:

http://atlp-tfs01.airwatch.corp/Sites/Devices/Releases/AWScript%20Win32/AWScript_Win32_1.0.0.4.7z

Extract the 7z archive to a directory on your computer. Now create the following file using Notepad or another Text editor.

```
'
' Hello AWScript
 '
ComputerName = regreadstring("HKLM","System\\CurrentControlSet\\
Control\\ComputerName\\ComputerName", "ComputerName")
Message = "Hello " + ComputerName
MessageBox("This is a caption", Message, 0)
```

Now open up a command prompt and execute AWScriptRun.exe with the above file as argument. You should see a message box with your computer name.



Language Reference

Keywords

The following are reserved keywords and may not be used as variable or function names:

- MOD
- AND
- OR
- NOT
- LET
- DIM
- IF
- THEN
- ELSE
- FOR
- TO
- STEP
- NEXT
- WHILE
- WEND
- DO
- UNTIL
- EXIT
- GOTO
- GOSUB
- RETURN
- END
- TRUE
- FALSE

Built-In Functions

Function	Description
ABS(num)	Returns the absolute value of a specified number.
SGN(num)	Returns an Integer value indicating the sign of a number.
SQR(num)	Returns the square root of a number.
FLOOR(num)	Returns the largest integer less than or equal to the given numeric expression.
ROUND(num)	Returns a numeric value, rounded to nearest integer.
RND	Returns a random value in the range 0.0 to 0.99.
SIN(rads), COS(rads), TAN(rads)	Returns trigonometric ratios of the angle specified in radians.
ASIN(num), ACOS(num), ATAN(num)	Returns angles from ratios specified.
EXP(num)	Returns a Double value containing e (the base of natural logarithms) raised to the specified power.
LOG(num)	Returns natural logarithm of a specified number.
ASC(char)	Returns an Integer value representing the character code corresponding to a character.
CHR(num)	Returns the character associated with the specified character code.
LEFT(string, len)	Returns a string containing a specified number of characters from the left side of a string.
LEN(string)	Returns an integer containing the number of characters.
MID(string, start, len)	Returns a string containing a specified number of characters from a string. Start position is indexed from zero.
RIGHT(string, len)	Returns a string containing a specified number of characters from the right side of a string.
STR(num)	Returns a String representation of a number.
VAL(string)	Returns the number contained in the string.
PRINT param1, param2 . .paramN	Formats and Prints the parameters to standard output. This is not available on Windows Mobile/CE. End the statement with a semi-colon to append a new-line.

Control Structures

Branching

The GOTO statement transfers control to a labelled statement. The GOSUB statement transfers control to a sub-routine

GOTO *label*

```
first:
print "Hello "
print "World "
goto first
```

GOSUB *label*

```
GOSUB PrintMessage1
GOSUB PrintMessage2
end

PrintMessage1:
   print "Hello "
return

PrintMessage2:
    print "World";
return
```

If Statements

The syntax for a single line If statement has the form:

IF *condition* THEN *statement* ELSE *statement2*

```
if (rnd * 100.0) <= 50 then print "Heads !"; else print "Tails!";
```

While there is no direct support for multi-line if blocks, it can be simulated using the single line IF and GOTO as illustrated below:

```
IF x <= 1- THEN GOTO line 10
   statement1
   statement2
Line10:
```

For Loops

The syntax of a FOR statement is illustrated below:

```
For i = 1 TO 10 Step 1
   Print i
Next i
```

While Loops

WHILE statements are terminated by a WEND keyword.

```
a = 1
WHILE a <= 10
   Print a
WEND
```

Do Until Loops

```
b = 1
DO
   Print b
UNTIL a > 10
```

AirWatch Extensions

A set of additional functions are available for use with Provisioning and general device side scripting.

Function	Description
beep()	Plays a notification alert sound.
udid()	Returns a string representing the AirWatch Device UDID which is a unique identifier for each device.
crlf	Represents a platform specific line ending, can be used in print statements and message boxes.
instr(sTarget, sSearch, iCaseSensitive)	Returns the position of the search string within the target string. Set iCaseSensitive to 1 to do a case sensitive search, 0 to ignore case. Returns -1 if the search string is not found.
filecopy(sSrc, sDest, iFail_if_exists)	Copies a File. Specify source and destination paths for a file copy. iFail_if_exists indicates if the function should fail if the destination file already exists. (Valid values are 1 and 0) Returns 1 on success, 0 on failure.
filemove(sSrc, sDest)	Moves a file to a different path. Specify source and destination paths for moving the file. Returns 1 on success, 0 on failure.
filedelete(sSrc)	Path to a file to be deleted. Returns 1 on success, 0 on failure.
dircreate(sSrc)	Full Path to a directory to be created, intermediate missing directories will also be created. Returns 1 on success, 0 on failure.
dirrename(sSrc, sDest)	Moves a directory, Specify source and target directories. Returns 1 on success, 0 on failure.
dirremove(sSrc)	Deletes a directory and all its contents, specify the full path to the directory. Returns 1 on success, 0 on failure.
abort(sMessage)	Deletes a directory and all its contents, specify the full path to the directory. Returns 1 on success, 0 on failure.
run(sExe, sArguments, iTimeout)	Runs an executable on the device, specify complete path to the executable, any arguments it takes or an empty string if there are no arguments. Timeout in seconds to wait for process to finish. Returns 1 if program was started successfully, 0 on error.
wakeup()	Wakes up the device from sleep. No arguments and return values.
regaddkey(sHive, sPath)	Adds a key to the registry, specify hive which can be any of HKCU, HKLM. Path to the new key (Example: Software\AirWatch) Returns 1 on success, 0 on Error
regremovekey(sHive, sPath)	Removes a key from the registry, the key must not have any child keys. Specify Registry Hive and Path. Returns 1 on success, 0 on Error.
regwritestring(sHive, sPath, sName, sValue)	Adds a string property to the registry. Specify hive, registry key, property name and property value Returns 1 on success, 0 on Error.
regreadstring(sHive, sPath, sPropertyName)	Read a string from the registry. Specify hive, registry key, property name Returns string value, empty string if property doesn't exist.
regwritedword(sHive, sPath, sName, sValue)	Adds an Integer property to the registry. Specify hive, registry key, property name and property value. Returns 1 on success, 0 on

	Error.
regreaddword(sHive, sPath, sPropertyName, iDefaultValue)	Read an integer from the registry. Specify hive, registry key, property name Returns an integer, returns iDefaultValue if property is not present.
mergetemplate(sTemplatePath, sMergedTarget, sHive, sRegPath)	Merge a template with parameters from the registry and write to a target file. sTemplatePath - Path to the template file on the file system (Example: \Program Files\wifi.settings.template) sMergedTarget - Path to a target file to be written (Example : \Program Files\wifi.settings) sHive - Registry Hive where parameters are to be sourced (Example: HKLM) sRegPath - Registry Key under which configuration sections and parameters are stored (Example : Software\Walmart) Parameters in the template file will have to be enclosed within a double brace (Example {{General\Country}} or {{WiFi\SSID}}) .
messagebox(sCaption, sMessage, iButtons)	Display a MessageBox, iButtons has the same value as the argument to the Win32 MessageBox API (0 for just an OK button, 1 for an OK and CANCEL button).
fileexists(sBasePath, sFileName)	Checks if a file exists under the specified base directory.
direxists(sBasePath, sSubDir)	Checks if a subdirectory exists under the specified base directory.
fileversion(sFilePath)	Returns the version of a DLL or EXE. Takes file path as argument.
filesize(sFilePath)	Computes a hash of the file contents, Hash Algorithm must be either of "md5" or "sha1."
filehash(sFilePath, sHashAlgorithm)	Computes a hash of the file contents, Hash Algorithm must be either of "md5" or "sha1."
downloadfile(sURL, ignoreSSLErrors, sTargetFile)	Downloads a file through http/https and saves it to sTargetFile. Specify if certificate errors should be ignored by setting ignoreSSLErrors to 1 or 0 Returns 1 on success, 0 on error.
uploadfile(sURL, ignoreSSLErrors, sSourceFile)	Posts a file from the device to a http/https URL. Specify if certificate errors should be ignored by setting ignoreSSLErrors to 1 or 0 Returns 1 on success, 0 on error.
httppost(sURL, ignoreSSLErrors, sContent, sContentType)	Post a message to an HTTP URL. Specify if certificate errors should be ignored by setting ignoreSSLErrors to 1 or 0. Pass the body of the message in sContent.set sContentType to the MIME type of the message Returns response as a string.
sleep(iMilliseconds)	Suspend execution for specified millseconds.
oeminfo()	Returns the model and make of the Windows Mobile/CE device as a string.
gzip(sUncompressedFile, sGZFileName)	Compresses a single file using the gzip algorithm.
gunzip(sGZFileName, sUncompressedFile)	Uncompress a gz file using the gzip algorithm. Only single file archives are supported.
createshortcut(shortcut, target)	Creates a shortcut for the target.
diskfreespace(driveName)	Returns the free space available in the mentioned drive.
installcertificate(certificate , certificateStore)	Installs the certificate in the specified store.
installpfx(pfxCertificate, password, certificateStore)	Installs the pfx certificate in the specified store.

Provisioning Functions	Descriptions
provisioning_getactioncount()	Returns the number of actions defined in the manifest for the current product.
provisioning_getactiontype(iActionIndex)	Return the stringified action type (Ex: Download, MoveFile) for the specified action index.
provisioning_getfirstactionparam(iActionIndex)	Returns the first parameter of an action if present. The value depends on the type of action. For instance a CopyFile action will have the source file as its first parameter while the WarmBoot action has no parameters and will return an empty string.
provisioning_getsecondactionparam(iActionIndex)	Returns the second parameter of an action if present.
provisioning_isactionenabled(iActionIndex)	Returns 1 if the Action is enabled, 0 if it is disabled.
provisioning_setactionstate(iActionIndex, iState)	Enables/Disables the specified action. Set iState to 1 for enabling an action, 0 for disabling the action.
provisioning_getproductname()	Returns the name of the provisioning product.
provisioning_getproductversion()	Returns the version of the provisioning product.

Examples

Picking a file based on a stanza parameter

- Based on the encryption setting of a symbol 9090g, pick either a wpa2 or a wep setting file and copy it to 9090g-ce5_irr.apd.
- Based on the country setting, pick a country specific configuration.
- Based on the number of sessions for the gls application.

```
if regreadstring("HKLM", "Software\\Walmart\\Wireless", "symbol-9090g-ce5_
encryption") = "wpa2" then filecopy("9090g-ce5_irr_wpa2.apd", "9090g-
ce5_irr.apd", 0)
if regreadstring("HKLM", "Software\\Walmart\\Wireless", "symbol-9090g-ce5_
encryption") = "wep" then filecopy("9090g-ce5_irr_wep.apd", "9090g-ce5_irr.apd",
0)

 if regreadstring("HKLM", "Software\\Walmart\\General", "country") = "US" then
filecopy("9090g-ce5_reg.apd.default", "9090g-ce5_reg.apd", 0)
if regreadstring("HKLM", "Software\\Walmart\\General", "country") = "JP" then
filecopy("9090g-ce5_reg.apd.japan", "9090g-ce5_reg.apd", 0)

ansi_reg_src = ansi.reg + regreadstring("HKLM", "Software\\Walmart\\Apps",
"gls_num_of_sessions") + "_sessions"; if fileexists("\\Program Files",
ansi_reg_src) then filecopy(ansi_reg_src, "ansi.reg", 0)
```

Generate a configuration file based on stanza settings

```
if regreadstring("HKLM", "Software\\Walmart\\Wireless", "symbol
   -9090g-ce5_ encryption") <> "wpa2" then goto end_encrypret
   = mergetemplate("\\Program Files\\fusion.ini.wpa2tmp", "\\Program
```

```
        Files\\fusion.ini", "HKLM", "Software\\Walmart")
    end_encryp:
```

The fusion.ini.wpa2tmp is listed below:

```
# FUSION CONFIG FILE
# This defines a configuration file for the Fusion Radio
#######################################
"Profile Name"="DC"                                  #(wpa2_essid from stanza file goes here)
"ESS_ID"={{WIRELESS\wpa2_essid}}
#Parameters for IP Addressing Type selection
#Type: zero bit=0 for DHCP, zero bit=1 for Static IP
"IPAddressType"=dword:00000000                       #30mW, 15mW, 5mW, 1mW, 0= full power
"Transmit Power"=dword:00000000                      #0=CAM, 1=Fast Power Save, 2=Max Power Save
"BatteryUsage"=dword:00000001                        #0=Infrastructure, 1=Ad-Hoc
"OperatingMode"=dword:00000000                       #1=2412 MHz, 2=2417MHz, 3=2422MHz, 4=2427MHz, 5=2432MHz,
                                                     6=2437MHz, 7=2442MHz, 8=2447MHz, 9=2
"Channel"=dword:00000001
"Authentication"=dword:00000000                      #0=None, 1=LEAP, 2=PEAP, 3=TTLS
#Key to selectencryption type
"Encryption"=dword:00000006                          #0=open, 1=40bit WEP, 2=128bit WEP, 3=TKIP
"PassKey"={{WIRELESS\wpa2_psk}}
#EOF cfg
```

...And the generated file fusion.ini has the replaced values

```
# FUSION CONFIG FILE
# This defines a configuration file for the Fusion Radio
#######################################
"Profile Name"="DC"
"ESS_ID"=VZkBobWwB6Tz                                #(wpa2_essid from stanza file goes here)
#Parameters for IP Addressing Type selection
#Type: zero bit=0 for DHCP, zero bit=1 for Static IP
"IPAddressType"=dword:00000000
"Transmit Power"=dword:00000000                      #30mW, 15mW, 5mW, 1mW, 0= full power
 "BatteryUsage"=dword:00000001                       #0=CAM, 1=Fast Power Save, 2=Max Power Save
"OperatingMode"=dword:00000000                       #0=Infrastructure, 1=Ad-Hoc
"Channel"=dword:00000001                             #1=2412 MHz, 2=2417MHz, 3=2422MHz,
                                                     4=2427MHz, 5=2432MHz, 6=2437MHz, 7=2442MHz,
```

"Authentication"=dword:00000000

#Key to selectencryption type

"Encryption"=dword:00000006
"PassKey"=2CQH74VfWV3AJ3vgcceZ8Jegu
Mi87FIlj58TNfLix395OZOB30LjXSNk3Lw7yzO

#EOF cfg

8=2447MHz, 9=2

#0=None, 1=LEAP, 2=PEAP, 3=TTLS

#0=open, 1=40bit WEP, 2=128bit WEP, 3=TKIP

Provisioning Conditional Execution

Skip all download actions for a product

```
count = provisioning_getactioncount();
for i = 0 to count - 1
 if provisioning_getactiontype(i) = "Download" then provisioning_
setactionstate(i, 0)
next i
```

Appendix – Custom Attributes

Overview

Custom attributes enable administrators to extract particular values from a managed device and return it to the AirWatch Admin Console. Apply these attributes to other uses such as associating them with rules to further assign products to devices.

For the Windows Mobile platform the most common application will be through the syncing of registry settings, which allows administrators to specifically assign products to devices based on common registry settings.

Implementation

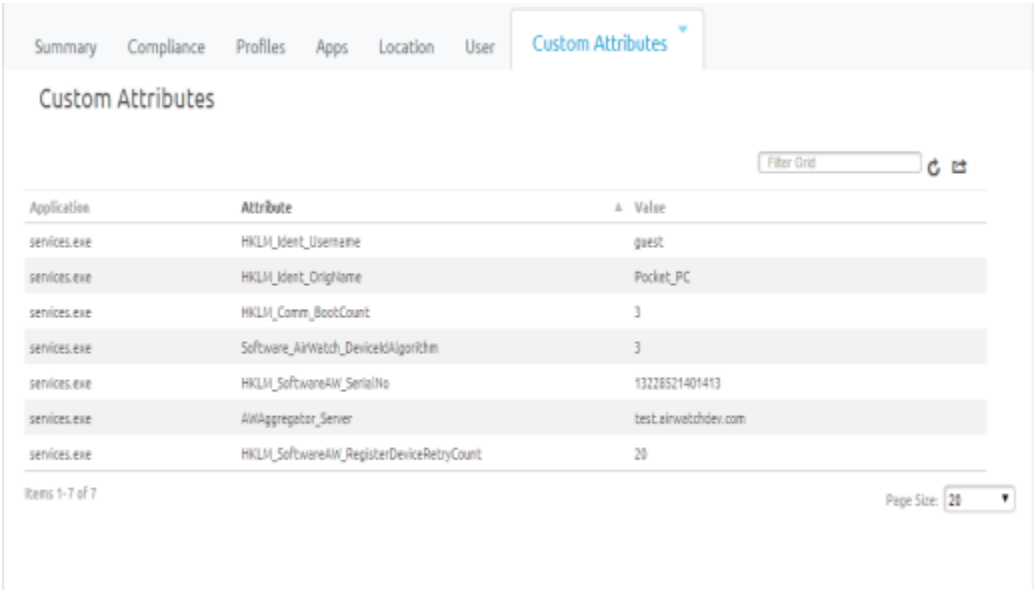
To begin collecting custom attributes, follow the steps detailed below:

1. Navigate to **Devices ►Product (New) ►File/Actions ►Add** and select **Windows Mobile** as your platform.
2. Complete the steps to create an XML Product as mentioned in Appendix B – XML Provisioning. The Manifest should include an action to download the XML file to **\Program Files\Airwatch\Cache\Profiles**.

Upon receiving the XML file, the AirWatch MDM Agent for Windows Mobile creates a custom attributes output file.

During the next check-in with AirWatch, the agent will send the output file to the AirWatch Admin Console.

Once the XML file installs, the custom attributes requested in the file exported to the console. These values display in the console in the Device Details page under Custom Attributes.This page allows you to view the name of the attribute as well as the values returned from each device. These values can be used to create product assignment rules using the Custom Rules system.



You may also view existing custom attributes for all devices at a particular Organization Group as well as manually creating custom attributes directly in the console. Navigate to **Groups & Settings ►All Settings ►Devices & Users ► Advanced ►Custom Attributes** to see these custom attributes listed. Any custom attribute created in this manner automatically associates with a device and its respective custom attribute value that is successfully transmitted to the console.

Syncing Registry Settings

In order to synchronize the registry settings on a Windows Mobile device with the console, which most likely is the most common use of custom attributes for Windows Mobile devices, the you need to 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 AirWatch 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 “Username” 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 will 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 will be parsed by the agent and included in the next interrogator sample. The XML key/value pair should 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’ will simply be the name of the attribute in the console while ‘value’ will be the corresponding value that will be associated with that attribute.