Introduction to the Windows Phone 8 Guide

Overview

Windows Phone 8 is Microsoft's operating system designed for smartphones and shares the “Modern UI” with other Windows 8 devices. Windows Phone 8 offers a high level of user personalization, which makes it a good choice for those who want the dual benefits of corporate owned and bring-your-own-device (BYOD). Although it shares the modern UI design with other Windows devices, it is a distinct operating system and has unique management functionality.

AirWatch can manage Windows Phone 8 devices from a central location. As an approved application in the phone's Device Management (DM) system, the AirWatch Agent can perform many device management functions that might not otherwise be available. For example, the AirWatch solution supports remote device configurations, including certificate-based authentication for email, as well as remote wipe commands and the installation of applications.

Note: It is often necessary to differentiate between the Windows Phone 8.0 and Windows Phone 8.1 because Microsoft added many new MDM features to Windows Phone 8.1. If the topic refers to Windows Phone 8 devices, the topic applies to all versions of Windows Phone 8 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 Phone 8 Device Enrollment – Explains the enrollment process and use of the autodiscovery service and agent needed to establish initial communications with AirWatch.
- Windows Phone 8 Device Profiles – Explores the AirWatch Admin Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, etc.
- Compliance – Explains how the AirWatch Compliance Engine works and how to create compliance policies.
- Apps for Windows Phone 8 – Leverages the DM functionality to distribute internal and public applications to devices and details how to push and manage these applications from the AirWatch Admin Console.
- Managing Windows Phone 8 Devices – Provides navigation for the AirWatch Admin Console and Self-Service Portal to features needed by administrators to manage devices.

Before You Begin

Overview

Prior to enrolling Windows Phone 8 devices, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section prepares you for a successful deployment of Windows Phone 8 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:

- Supported Devices, OS, Agents, Versions, and Browsers – Lists Windows Phone 8 devices and software versions supported by AirWatch.
- Requirements – Details useful and/or required information you need before continuing with this guide.
- Recommended Reading – Provides a list of helpful guides to better your understanding of mobile device management and Windows Phone 8 devices.

Supported Devices, OS, Versions, and Agents

Comprehensive list of supported devices, OS, versions, and agents.

Platforms and Devices Supported

AirWatch supports the use of all Windows Phone 8 devices.

Agents and Versions Supported

The latest agent and version found on the Windows Phone Store.

Requirements

For enrollment requirements, see the Windows Phone 8 Enrollment section.

Recommended Reading

Helpful background and supporting information available from alternate AirWatch guides.

- **AirWatch Mobile Device Management Guide** –Provides additional information regarding the general aspects of MDM.
- **AirWatch Mobile Application Management Guide** –Provides additional information regarding the general aspects of MAM.

Windows Phone 8 Device Enrollment

Overview

Each Windows Phone 8 device in your organization's deployment must be enrolled before it can communicate with AirWatch and access internal content and features. This is facilitated with the AirWatch Agent. Depending on the version of Windows Phone 8 your device is running, you can enroll it with different methods.

Windows Phone 8.0 devices can enroll with the DM client either using the AirWatch MDM Agent or not. Windows Phone 8.1 devices enroll using the Workplace app without the need of the agent.

You can associate an email domain to your environment, which requires users to enter only an email address and credentials (and in some cases select a Group ID from a list) to complete enrollment. This is a simplified approach that leverages information end users likely already know.

Alternatively, if you do not set up an email domain for enrollment, end users will be prompted for the Enrollment URL and Group ID, which must be provided to them by an administrator. The following steps explain how to set up email autodiscovery for your environment.

Windows Phone 8 devices must begin communicating with AirWatch to access internal content and features, which is facilitated using the AirWatch Agent. Available for download from the Windows Store , the AirWatch Agent provides a single resource to enroll a device as well as provide device and connection details.

Note: Windows Phone 8.1 devices use a different enrollment method than Windows Phone 8.0 devices.

Enrollment Requirements

- **Microsoft Developer's Account** –The AirWatch Admin must purchase an account, which consists of the following:
  - **Windows Account ID** –This account (different from the Windows Live ID) costs a fee and enables your company to add applications to the Windows Phone Development Center.
  - **Symantec Certificate** –Microsoft provides this code signing certificate in the Developer's package. You will use it for two purposes:
    - To code sign the AirWatch agent .xap file.
    - To generate an application enrollment token (AET) (.aetx file) that you upload into the AirWatch console, which is needed to distribute approved enterprise internal applications. For more information on this Enterprise Token, refer to the **AirWatch Mobile Application Management Guide.**

Caution: If you are considering the deployment of enterprise internal applications, make sure you generate and upload the AET before enrolling MDM devices. Otherwise, all devices enrolled before following the **Mobile Application Management Guide** will need to be re-enrolled again in order to access enterprise internal applications.

- **AirWatch Agent** –This is the AirWatch agent .xap file for the company Hub required for Windows Phone 8.0 enrollment.
- **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.

In This Section

- Allowing Enrollment Methods – Describes the requirements for enrolling Windows Phone 8.0 devices using either the AirWatch MDM Agent or Device Management (DM) only method.
- Enrolling through the DM Client – Explains how to enroll Windows Phone 8.0 devices using the AirWatch MDM Agent or without. Both enrollment methods use the Device Management method but using the Agent requires additional steps.
- Enrolling Windows Phone 8.1 Devices through Web-based Enrollment – Details how to enroll Windows Phone 8.1 devices using the Workplace Account on the device.

Allowing Enrollment Methods

When enrolling Windows Phone 8.0/8.1 devices, you can choose to enroll using the AirWatch MDM Agent or without. Both enrollment methods use the Device Management method but using the Agent requires additional steps.

Capabilities Based on Enrollment Type

The following capabilities matrix lists supported features for the Company Hub and DM/Workplace *only* Microsoft Phone 8 enrollment.

Feature	AirWatch MDM Agent	DM/Workplace only
Enrollment		
Requires Windows Account ID	Required	No
Force EULA/Terms of Use Acceptance	Yes	No
Active Directory/LDAP	Yes	Yes
SAML Integration	Yes	No
Token Based Enrollment	Yes	Yes
Device Staging Support	Yes	No
Support for Optional Prompts during Enrollment	Yes	No
Configuration Profile Management		
Certificate-based EAS Authentication	Yes	No for 8.0 Yes for 8.1
Security Settings (Data Encryption, Password Policy, etc.)	Yes	Yes

Feature	AirWatch MDM Agent	DM/Workplace only
Device Restrictions	Yes	Yes
Certificate Management	Yes	Yes
Email and Exchange ActiveSync management	Yes	Yes
Device Information		
Device Information (model, serial number, etc.)	Yes	No
GPS Tracking	Yes	No
Memory Information	Yes	No
Battery Information	Yes	No
UDID	Yes	Yes
Network Information		
IP Address	Yes	No
Bluetooth MAC address	Yes	No
Wi-Fi MAC address	Yes	No
Management Commands		
Full Device Wipe	Yes	Yes
Enterprise Wipe	Yes	Yes
Email Messaging	Yes	Yes
SMS Messaging	Yes	Yes
APNs Push Messaging	Yes	No
Application Management		
View and Manage Applications	Yes	No for 8.0 Yes for 8.1 (No App Catalog)
Application List	Yes	No
Compliance		
View Compliance Status	Yes	No

Feature	AirWatch MDM Agent	DM/Workplace only
View Compliance Policies	Yes	No

Note: Depending on the enrollment method you choose, you will need to navigate to **Device ▶Settings ▶Devices & Users ▶Windows ▶Windows Phone 8 ▶Company Hub Settings** and then either check **Enable Company Hub** for use during enrollment or deselect the checkbox if you do not wish to use the AirWatch MDM Agent.

Enrolling through the DM Client

Note: This enrollment method is for devices running Windows Phone 8.0 only. Devices running Windows Phone 8.1 must enroll using the Workplace enrollment.

This simplified enrollment process for Windows Phone 8 begins with approving the AirWatch MDM Agent as a company application on the device you are enrolling. To do this, you must have credentials provided by the AirWatch administrator. Additionally, if autodiscovery is not enabled, you must also know the server URL for the AirWatch environment into which you are enrolling your device. Next, to take full advantage of the device monitoring and management features and capabilities available for Windows Phone 8, you must also install the AirWatch MDM Agent, or Company Hub, following initial end user authentication. Additional information for AirWatch Administrators on uploading and enabling Company Hub can be found in Uploading and Enabling Company Hub.

To enroll your Windows Phone 8 devices:

1. On your Windows Phone 8 Device, navigate to **Settings ▶Company Apps**.
2. Select **Add Account**.
3. Enter the **Email Address** and **Password** and then select **Sign In**.
4. Enter the server URL for the AirWatch environment into which you are enrolling.

   Note: If your administrator has enabled autodiscovery, then AirWatch authenticates your identity using the credentials you entered and you will not be prompted to enter the URL of the server.

5. Ensure the **Install company app or Hub** checkbox is selected and select **Done**.

   Note: If you are not using the AirWatchMDM Agent, you have completed enrolling the Windows Phone 8 device.

Completing the Enrollment

Following the next DM sync, which can be initiated manually or occurs about every minute automatically, the AirWatch MDM Agent appears as an installed app on the device. At this point, the device remains in a quarantined state in AirWatch until you launch the Agent on the device and complete any additional prompts the administrator has configured as required for enrollment. This may include accepting a Terms of Use agreement, specifying device ownership category, or simply proceeding past a Welcome screen.

Note: If more than 10 minutes has elapsed between enrolling the device and launching the Agent for the first time, then a prompt asking for your credentials to access the application appears.

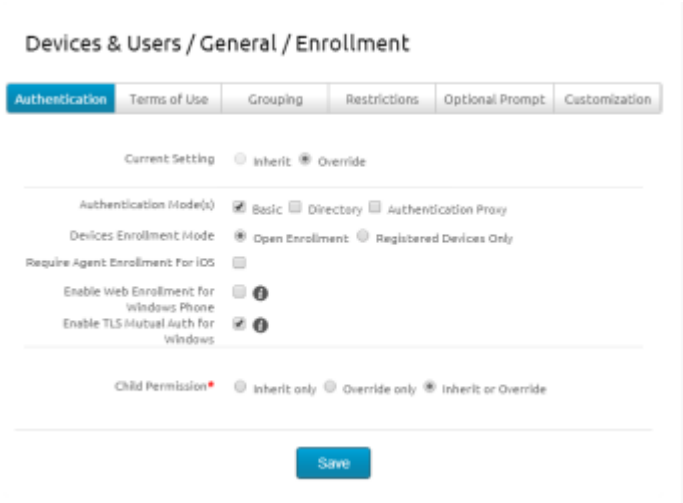
Enrolling Windows Phone 8.1 Devices through Workplace Enrollment

With Windows Phone 8.1, devices can be enrolled without downloading the AirWatch MDM Agent before or during enrollment. The Workplace Account provides a simple, easy way to enroll devices into AirWatch.

Note: This enrollment method only works with Windows Phone 8.1 devices.

Before you can begin using the workplace enrollment, you must configure the options listed below:

1. Navigate to **Devices ▶Settings ▶General ▶Enrollment**.



2. Under the **Authentication** tab, select the options you wish to use with your Windows Phone 8.1 Enrollments:
   - **Enable Web Enrollment for Windows Phone** – Enable to allow the native Workplace app on Windows Phone 8.1 devices to display the optional enrollment screens such as Terms of Use.
   - **Enable TLS Mutual Auth for Windows** – Enable to force Windows Phone 8.1 devices to use endpoints secured by TLS Muatual Authentication.

To enroll using workplace enrollment, follow the steps detailed below:

1. On your Windows Phone 8.1 device, navigate to **Settings ▶Workplace**.
2. Select **Add Account**.
3. Enter your **Email Address**.
4. If you are not using autodiscovery, a prompt for **Server URL** appears.
5. Enter you **Username** and **Password** and select **Sign In**.
6. Advance through any additional screens that are required by your company.

Your device is now enrolled and will begin receiving profiles, applications, etc. from the AirWatch Admin Console.

Windows Phone 8 Device Profiles

Overview

You can associate devices with profiles via the AirWatch Admin Console to help ensure the proper use of corporate-owned devices and protection of sensitive data. You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. The individual settings you configure, such as those for Wi-Fi, virtual private network (VPN), and restrictions, are referred to as **payloads**. It is recommended for profiles that only one payload is associated per profile, which means you will have multiple profiles for different settings you wish to establish. In addition to profiles, you can create compliance policies to detect Windows Phone 8-specific conditions and perform actions automatically.

In This Section

- Configuring General Settings – Details the options and settings found in the General settings you must configure for each profile. 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 Phone 8 devices available in the AirWatch Admin Console.
- Deploying a Wi-Fi Payload – Details the steps required to push Wi-Fi settings to devices.
- Configuring Virtual Private Network (VPN) Access – Describes how to configure your Windows Phone 8.1 device to access VPNs for secure access to corporate data.
- Deploying Email Payloads – Explains the steps in configuring user IMAP/POP3 email accounts.
- Deploying Exchange ActiveSync Payloads – Creates an Exchange ActiveSync profile to allow the end user to access corporate email infrastructures from the device.
- Configuring Application Control for Windows Phone 8.1 – Details how to create whitelists and blacklists for allowing and denying access to applications.
- Creating a Credential Profile –Covers certificate-based authentication for Windows Phone 8 devices and the configuration options available in the AirWatch Admin Console.
- Configuring a SCEP Payload – Details creating a SCEP profile to silently install certificates onto Windows Phone 8.1 devices.
- Securing Windows Phone 8 Devices by Time Schedules – Details 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

This payload requires 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. Consider the complexity of the passcode. Set simple passcodes so that users can quickly access device content or set complex alphanumeric passcodes to secure the device content.

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

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **Passcode** profile.
4. Configure the Passcode settings, including:
   - **Maximum Passcode Age** – Enforce users to renew passcodes at selected intervals.
   - **Maximum Number of Failed Attempts** – Reset the device to factory defaults if too many unsuccessful attempts have been made.
   - **Max Inactivity Time Device Lock** – Secure idle devices with short lock times.
5. Select **Save & Publish** when you are finished to push the profile to devices.

Deploying Restrictions Payloads

Deploy a restrictions payload for added security on Windows Phone 8 devices. Restrictions payloads for Windows Phone 8 devices can disable access to the SD card so unauthorized users cannot transfer sensitive data off the SD card.

Note: Windows Phone 8.0 does not support the same restrictions as Windows Phone 8.1. Check the version badges to the right of every restriction option in the AirWatch Admin Console.

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

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **Restrictions** profile.
4. Configure the Restrictions settings, including:

- Administration
  - **Allow User To Reset Phone** – Allow the end user to factory reset their device.
  - **Allow Manual MDM Enrollment** – Allow the end user to enroll into AirWatch through the Workplace Enrollment.
- Security and Privacy
  - **Allow Location** – Allow the use of location services.
  - **Allow Microsoft Account Connection** – Allow the use of MSA accounts for non-email related connection authentication and services.
  - **Allow Adding Non-Microsoft Accounts Manually** – Allow the end user to add accounts such as Facebook or Twitter manually.
  - **Allow Manual Root Certificate Installation** – Allow end user to manually install root and intermediate CAP certificates.
  - **Allow Developer Unlock** – Allow developer unlock to be used on the device.
- Device Functionality
  - **Allow Camera** – Allow end users to access the camera function of the device.
  - **Allow Screen Capture** – Allow end users to take screenshots of the device.
  - **Allow Storage Card** – Allow the use of a SD card.
  - **Require Device Encryption**– Encrypt all data being stored to the SD card to prevent an end user from accessing readable, sensitive information.

    Important: If you select this feature, you cannot return to not encrypting device data on the SD card by simply deselecting the checkbox. In order to return the device to that state, you would need to restore the device to factory settings (i.e., device wipe).
  - **Allow Browser** – Allow end users to use the native Internet Explorer browser.
  - **Allow App Store** – Allow access to the app store.
  - **Allow Voice Recording** – Allow the end users to record voice recordings.
  - **Allow Cortana** – Allow access to the Cortana application.
  - **Allow Copy and Paste** – Allow the end user to copy and paste on the device.
  - **Allow Bluetooth** – Allow the connection of devices through Bluetooth.
  - **Allow Telemetry** – Allow the device to send telemetry information (such as SQM or Watson) to the AirWatch Admin Console.
  - **Allow NFC** – Allow the use of the Near Field Communication chip on the device.
  - **Allow USB Connection** – Allow desktop to access phone storage via USB. Both MTP and IPoUSB are disabled when this restriction is enforced.
  - **Allow Search to Use Location** – Allow end user searches to use the device location services.
  - **Require Strict Safe Search** – Require searches to use the strict safe search setting.

- **Allow Storing of Vision Search Images** – Allow the storage of Vision Search images onto the device.
- **Allow Sharing Office Files** – Allow end users to share Office files.
- **Allow Sync Settings Between Devices** – Allow end users to sync their settings preferences between Windows Phone 8.1 and Windows 8.1/RT devices.
- **Allow Action Center Notifications** – Allow app and device notifcations to display in the Action Center of the device.

- Network
  - **Allow Wi-Fi** – Allow end users to connect to Wi-Fi.
  - **Allow Manual Wi-Fi Configuration** – Allow connections to Wi-Fi outside of the MDM server installed networks.
  - **Allow Wi-Fi Hotspots Reporting** – Allow Wi-Fi Hotspots information reporting to Microsoft. Once disallowed, the user cannot turn this function on.
  - **Allow Internet Sharing** – Allow Internet sharing between devices.
  - **Allow VPN over Cellular** – Allow the device to create a VPN over cellular networks.
  - **Allow VPN Roaming over Cellular** – Allow the device to create a VPN while roaming over cellular networks.
  - **Allow Cellular Data Roaming** – Allow cellular data usage while roaming.

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

Deploying Wi-Fi Payloads

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 payload, follow the steps detailed below:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **Wi-Fi** profile.
4. Configure the Wi-Fi settings, including:
   - **Name** – Enter the name (SSID) of the desired Wi-Fi network.
   - **Service Set Identifier** – Enter an identifier that is associated with the Name (SSID) of the desired Wi-Fi network.
   - **Connection Type** – Use the dropdown menu to select Extended or Independent Basic Service Set as the Wi-Fi connection type.
   - **Security Type** – Use the dropdown menu to select the security type (e.g., WPA2 Enterprise) for the Wi-Fi network.
   - **Encryption** - Use the dropdown menu to specify if data transmitted using the Wi-Fi connection is encrypted using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES).

- **Password** – Enter the password required to join the Wi-Fi network. Select the Show characters check box to disable hidden characters within the field.
- **Identity Certificate** – Select (if desired) an Identity Certificate from the dropdown if you require the end user to pass a certificate in order to connect to Wi-Fi, otherwise select **None** (default). For more information needed to select a certificate for this payload, see Deploying Credentials Payloads.

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

Configuring Virtual Private Network (VPN) Access

Virtual private networks (VPNs) provide devices with a secure and encrypted tunnel to access internal resources. VPN profiles enable each device to function as if it were connected through the on-site network. Configuring a VPN profile ensures end users have seamless access to email, files and content.

Note: This payload is only available to devices using Windows Phone 8.1. If you wish to use this payload, you must download and install the free update.

To create a base VPN profile:

1. Navigate to **Devices ▶Profiles ▶List View ▶Add**. Select **Windows Phone 8**.
2. Configure General profile settings as appropriate.
3. Select the **VPN** payload.
4. Configure **VPN** settings, including:
   - **VPN Name** – Enter the name of the connection name to be displayed.
   - **Server** – Enter the hostname or IP address of the server to which to connect.
   - **Tunnel Type** – Select the type of VPN tunnel you wish to use.
   - **DNS Suffix** – Enter the DNS suffix for your VPN.
   - **Authentication Type** – Select the type of authentication from the drop-down menu.
     - **Certificate** – Select the Certificate created with the Certificate or SCEP profile.
   - **Proxy** – Select whether you wish to allow a **manual** proxy, a **bypass for local**, or **none**.
   - **Policies** – Select the checkbox if you wish to enable any of the following policies.
     - **Remember Credentials** – Enable to allow end users to save their credentials.
     - **Split Tunnel** – Enable to allow end users to use a split tunnel VPN.
     - **Bypass For Local** – Allow users to bypass the proxy server for local addresses.
     - **Trusted Network Detection** – Enable to use Trusted Network Detection when connection to VPN.
     - **Connection Type** – Select the connection type you wish to allow.
   - **Secured Resources** – Select if you wish to control what resources may have access to the VPN.
     - **Allowed Apps** – Add applications that are allowed access through the VPN.

- **Allowed Networks** – Add networks that are allowed access through the VPN.
- **Allowed Name Spaces** – Add name spaces that are allowed access through the VPN.
- **Excluded Apps** – Add apps that are not allowed access through the VPN.
- **Excluded Networks** – Add networks that are not allowed access through the VPN.
- **Excluded Name Spaces** – Add name spaces that are not allowed access through the VPN.
- **DNS Suffix Search List** – Add DNS suffixes to search for when connecting to the VPN.

5. Select **Save & Publish**.

Deploying Email Payloads

This payload configures user IMAP/POP3 email accounts and sends configurations directly to their devices. Consider the following options while setting email payloads:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **Email** profile.
4. Configure the Wi-Fi settings, including:
   - **Maximum Attachment Size** – Control the size of IMAP/POP3 email attachments to manage bandwidth on your mobile network.
   - **Use SSL** – Use the Secure Socket Layer (SSL) protocol to encrypt incoming and outgoing IMAP/POP3 emails on the mobile network.
   - **Enable Authentication** – Secure IMAP/POP3 email traffic on devices by enforcing authentication to access these email accounts.
5. Select **Save & Publish** to push the profile to devices.

Deploying 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 Phone 8**.
2. Configure General settings for the profile.
3. Select the **Exchange ActiveSync** profile.
4. Configure the Wi-Fi settings, including:

- **Exchange ActiveSync Host** – Enter the public host name or server name hosting your Exchange ActiveSync.
- **Use SSL** – Select to send all information through the Secure Socket Layer.
- Login Information
    - **Domain** – Enter the end-user's domain.
    - **Username** – Enter the end-user's username.
    - **Email Address** – Enter the end-user's email address.
    - **Password** – Enter the password for the end user.
    - **Identity Certificate** – Select (if desired) an Identity Certificate from the dropdown if you require the end user to pass a certificate in order to connect to the Exchange ActiveSync, otherwise select **None** (default). For more information needed to select a certificate for this payload, see Deploying Credentials Payloads.
- Settings
    - **Next Sync Interval (Min)** – Enter the number of minutes between syncs.
    - **Past Days of Mail to Sync** – Select the number of days worth of past mail to sync with device.
    - **Diagnostic Logging** – Select the type of diagnostic logging you wish to gather.
- Content Type
    - **Allow Email Sync** – Allow the syncing of email.
    - **Allow Contacts Sync** – Allow the syncing of contacts.
    - **Allow Calendar Sync** – Allow the syncing of calendars.

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

Configuring Application Control for Windows Phone 8.1

Note: This payload is only available to devices using Windows Phone 8.1. If you wish to use this payload, you must download and install the free update.

To allow or prevent installation of applications on devices, you can enable Application Control to whitelist and blacklist specific applications. While the Compliance Engine sends alerts and takes administrative actions when a user installs or uninstalls certain applications, Application Control prevents users from even attempting to make those changes. For example, prevent a certain game application from ever installing on a device, or allow only specific apps you've whitelisted to be installed on a device.

1. Navigate to **Devices ▶Profiles ▶List View ▶Add.** Select **Windows Phone 8**.
2. Configure General profile settings as appropriate.
3. Select the **Application Control** payload.
4. Enable or disable the following settings to set the level of control for your application deployments:
    - Enable **Prevent Installation of Blacklisted Apps** to enforce the automatic removal and/or prevent the installation of blacklisted apps defined in Application Groups.

- Enable **Only Allow installation of Whitelisted Apps** to prevent the installation of any application that is not a whitelisted app defined in Applications Groups.

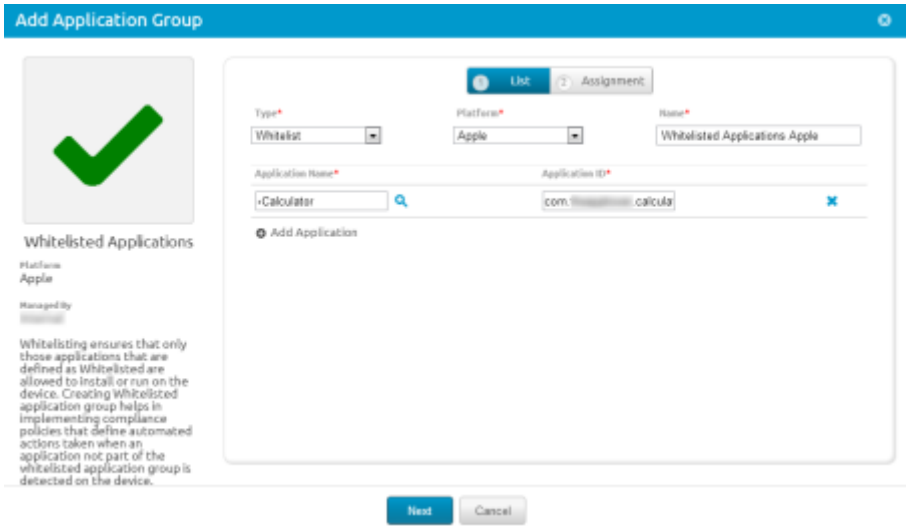
5. Select **Save & Publish**.

Note: For instructions on creating application groups, see Configuring an Application Group.

Configuring an Application Group

The AirWatch Admin Console provides the ability to group applications into blacklisted, whitelisted, and required applications. These groups are called **Application Groups** and each application group is tied to an Organization Group. Use application groups to assign whitelists and blacklists to users.

1. Navigate to **Apps & Books ▶Applications ▶Settings ▶App Groups.**
2. Select **Add Group**.



- **List** tab:
  - Select **Type** as **Whitelist**, **Blacklist**, **Required** or **MDM Application**. On selecting the **Type**, the **Name** field is automatically populated.

    Note: Select **MDM Application** for custom MDM applications.
  - Select **Platform** as either **Apple**, **Android** or **Windows Phone 8**.
  - Enter the **Application Name** and the **Application ID**. The **Application ID** automatically completes when you use the search function to search for the app from an app store.
  - Select **Add Application** to add multiple applications and then select **Next** to navigate to the **Assignment** tab. Add exceptions to your application group to create detailed whitelists and blacklists.
- **Assignment** tab:
  - Enter a **Description** for the application group.
  - Define the **Device Ownership** as **Corporate-Dedicated**, **Corporate-Shared**, **Employee Owned**, or **Undefined**.
  - Assign the device **Model** and the **Operating System**.
  - Select the **Organization Group** and **User Group** for the application group to be assigned to and then select **Finish** to complete the process.

Deploying a Credentials Profile

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

Note: Windows Phone 8.0 or 8.1 devices using the Credentials payload will need to have the AirWatch MDM Agent downloaded. End users will be required to install any certificates as mentioned in Installing a Certificate on Windows Phone 8 Devices.

To push certificates down to devices, you need to configure a **Credentials** payload as part of the profiles you created for EAS, Wi-Fi and VPN settings. Use the following instructions to create a certificate-enabled profile:

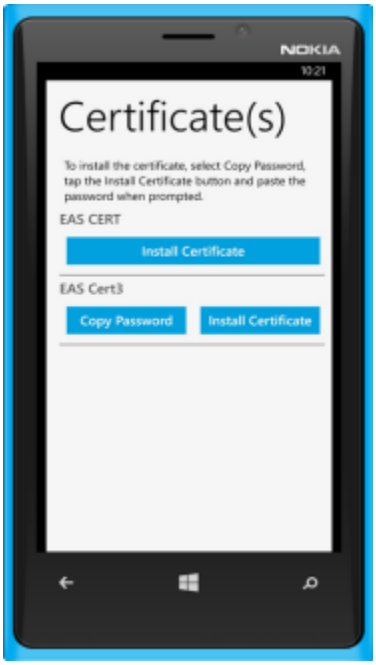
1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **Credentials** profile.
4. Configure the Credentials settings, including:
    - **Credential Source** – **Upload** a certificate from your local machine or define a **Defined Certificate Authority**.
        - If you choose to **Upload** your certificate, complete the following:
            - **Credential Name** – Enter the name of the credential or select on the information symbol to view acceptable lookup values like {EmailDomain} and {DeviceModel} to find the credential file to use.
            - **Upload** – Upload the new certificate or lookup values.
        - If you choose to use a **Defined Certificate Authority**, complete the following:
            - **Certificate Authority** for the **Defined Certificate Authority** – Select the external or internal CA issuing encryption keys for the PKI.
            - **Certificate Template** for the **Defined Certificate Authority** – Select the predefined template for the CA to use when requesting a certificate.
    - **Certificate Store** – Select the store on the device where the certificate is located. Choose from **Personal Certificates**, **Intermediate Certification Authorities Store**, or **EAS Certificate**.
5. Select **Save & Publish** when you are finished to push the profile to devices.

Installing a Certificate on Windows Phone 8 Devices

To install a credential on a Windows Phone 8 device, follow the steps detailed below:

1. Open the AirWatch MDM agent on the device.
2. Navigate to the **My Device** section of the agent.
3. Tap on the **Contextual** menu (three dots) at the bottom right corner of the screen.

4. Tap **install certificate(s)**. The **Certificate(s)** screen displays, listing all the certificates the AirWatch Admin pushed in a payload to that device, as shown.

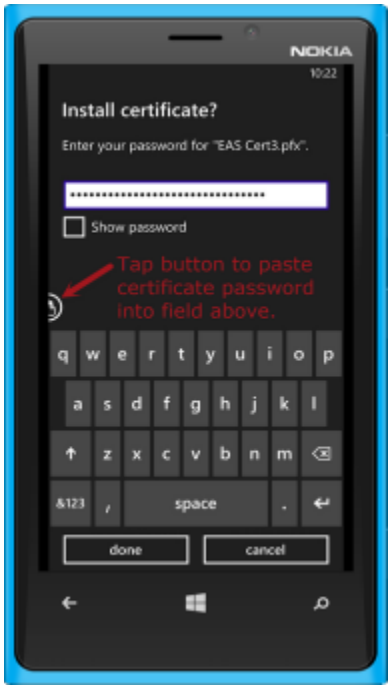


Note: If the certificate contains a password, a **Copy Password** button displays. Tapping **Copy Password** copies the password to the device's clipboard.

Note: If the email certificate does not display, verify it was pushed to the device from the AirWatch Admin Console.

5. Tap on the **Install Certificate** button shown under the certificate you want to install on the device. If the certificate does not require a password, the certificate installs. Otherwise, the device advances to the **Install Certificate?** screen as shown.

6. If you copied a certificate password, tap on the **Paste** button located to the left side of the screen. This inserts the certificate password you copied from the device's clipboard into the password field as shown.



7. Tap **Done**. The **Your certificates are installed** screen displays.

8. Tap **Ok**.

The email certificate is now installed on the device and displays on the **Certificate(s)** page of the device. Installation is successful when the device user can authenticate their email client with their Exchange server.

Configuring a SCEP Payload

Even if you protect your corporate email, Wi-Fi, and VPN with strong passcodes and other restrictions, your infrastructure still remains vulnerable to brute force and dictionary attacks, in addition to employee error. For greater

security, you can implement digital certificates to protect corporate assets. Simple Certificate Enrollment Protocol (SCEP) profiles allow you to silently install these certificates onto devices without the need of end-user interaction. To do this, you must first define a certificate authority, then configure a **SCEP** payload alongside your **EAS**, **Wi-Fi** or **VPN** payload. Each of these payloads has settings for associating the certificate authority defined in the SCEP payload.

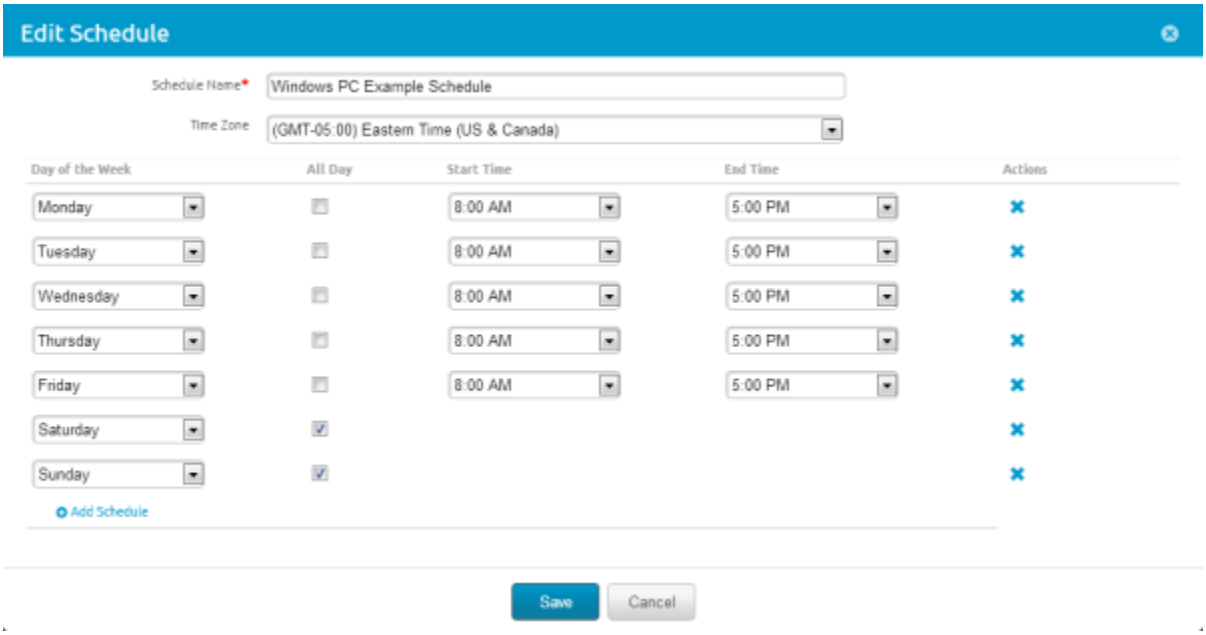
Note: SCEP profiles are for Windows Phone 8.1 devices only.

To push certificates down to devices, you need to configure a **SCEP** payload as part of the profiles you created for EAS, Wi-Fi, and VPN settings. Use the following instructions to create a certificate-enabled profile:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add** and then select **Windows Phone 8**.
2. Configure General settings for the profile.
3. Select the **SCEP** profile.
4. Configure the SCEP settings, including:
    - **Credential Source** – This drop-down menu is always set to Defined Certificate Authority.
    - **Certificate Authority** – Select the certificate authority you wish to use.
    - **Certificate Template** – Select the template available for the certificate.
5. Configure the Wi-Fi, VPN, or EAS profile.
6. Select **Save & Publish** when you are finished to push the profile to devices.

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.

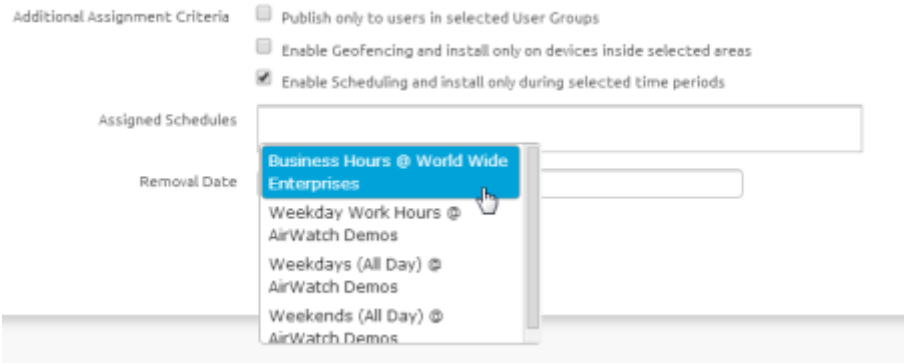
6. Select the **Day of the Week**, **Start Time** and **End Time** using the applicable drop-down menus. You can also select the **All Day** check box to disable start and end times for the schedule.
   To remove a day from the schedule, select the applicable **X** under **Actions**.
7. Repeat steps 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	Mac OS X	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.

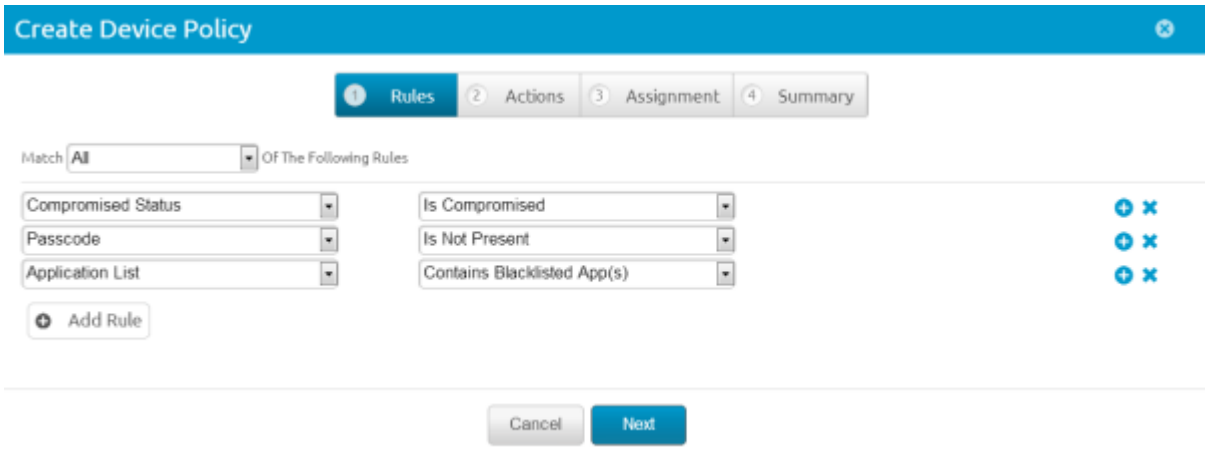
- **Compromised Status** – Select if the device is non-compliant when compromised.

  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.

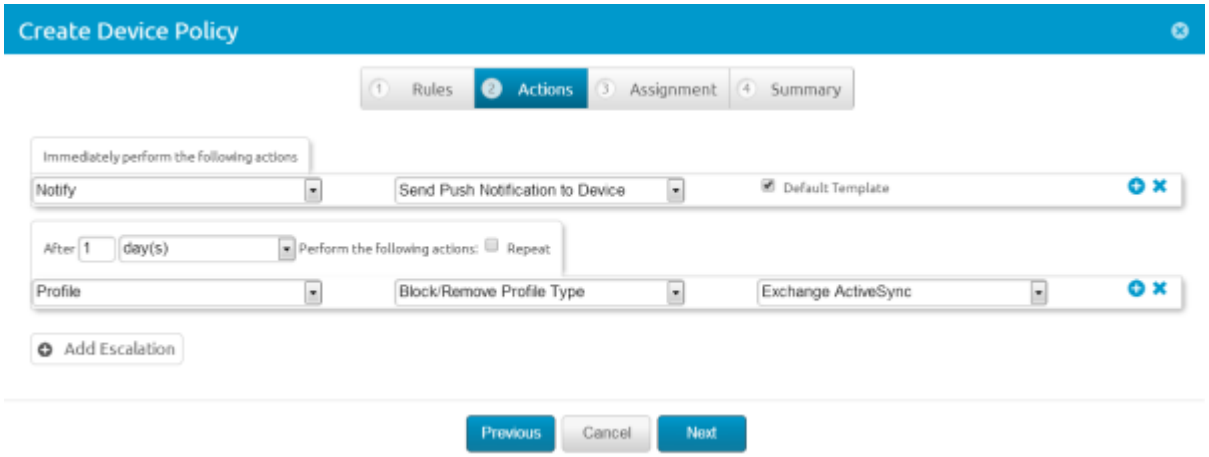
- **Interactive Profile Expiry** – Select if the device is non-compliant when an installed profile expires within the specified length of time.
- **Last Compromised Scan** – Select if the device is non-compliant when AirWatch is unable to successfully query the device on schedule.
- **MDM Terms of Use 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**.

Apps for Windows Phone 8

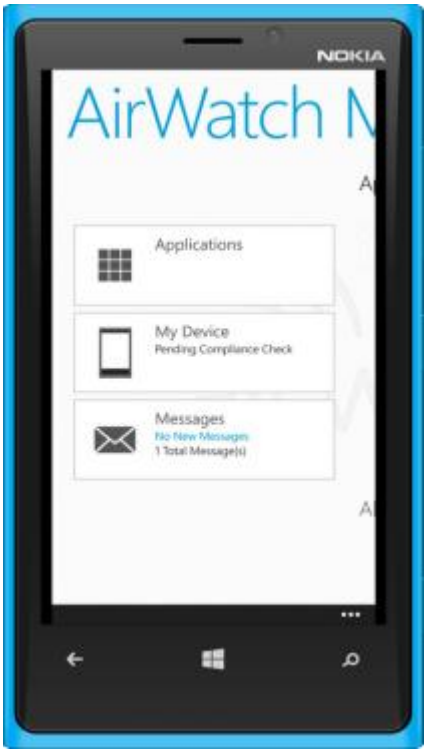
Overview

You can use AirWatch applications in addition to AirWatch MDM features to further secure devices and configure them with added functionality.The AirWatch MDM Agent allows you to secure devices and configure settings. Deploy the AirWatch Browser to enable secure web browsing for your end users.

In This Section

- Using the AirWatch MDM Agent for Windows Phone 8 – Learn more about how the AirWatch Agent is used to secure devices and how to configure its settings for Windows Phone 8 devices.
- Using the AirWatch Browser for Windows Phone 8 – Learn more about the AirWatch Browser for Windows Phone 8 devices.
- Enforcing Application-Level Single Sign On Passcodes – Learn more about how you can apply a single app-level SSO passcode for end users to access applications without having to authenticate each time.

Using the AirWatch Agent



The AirWatch Agent for Windows Phone 8 devices has many management functions as well as self-service features. It includes the Enterprise App Catalog, information about the device, and notifications.

The AirWatch Agent includes the following sections. You can tap on each of these icons for detailed information or swipe to the left for the same detailed information:

Option	Description
Applications	Access and download applications from the integrated Enterprise App Catalog. Access both internal and public applications as follows: • **All Internal** – Access internal applications highlighted by the company. • **All Public** – Access all public application available to the end user. **Note:** If you add an app to one of the categories listed in the AirWatch Admin Console, the category is pushed to the device and displays under **All Internal** and **All Public**. If you tap on that category, the app you pushed to the device displays.
My Device	View current MDM details for the device as follows: • **Connection** – View connection status. • **Location** – View the current GPS location of the device. • **Enrollment** – View the enrollment status of the device. **Note:** If you swipe to the left, the **Details** page appears showing you the **Agent Version** and other useful information.
Messages	View messages sent to the device from the AirWatch Admin Console. These messages include new application update announcements, company meeting information, out-of-compliance warnings, and other company announcements.
Contextual Menu ...	View and configure MDM settings on the device by tapping on the Contextual menu (three dots ...) located at the bottom right corner of the screen as follows: **Settings** **Note:** Tapping on **Settings** advances you to a screen where you must enter the Admin passcode to view a page that contains **Settings** and **Services**. • **Group** – View the current Group ID in which the device is enrolled. • **DM URL** – View the current Host Name (enrollment URL) associated with enrollment. • **Username** – View the current user of the device. **Services** • **Location Services** – Configure Location Services and GPS tracking on the device. • **Push Notification Services** – Configure MPNs on the device. **About** • Displays information about AirWatch and MDM. The information displayed on the device is entered in the AirWatch Admin console by navigating to **Groups & Settings ▶All Settings ▶Devices & Users ▶**

Windows ▶Windows Phone 8 ▶Agent Settings and then select **About Page Configuration** and enter information in the dialog box.

Terms of Use

- Displays the current Terms of Use.

Enabling Services

In the AirWatch Admin Console, enable the following features so that there is communication between the AirWatch Agent and the AirWatch Admin Console.

1. In the AirWatch Admin Console, select the applicable **Organization Group** to apply settings to.
2. Go to **Groups & Settings ▶All Settings ▶Device & Users ▶Windows ▶Windows Phone 8 ▶Agent Settings**.
3. Enable the following options in the **AirWatch Agent Settings** section:
   - **Collect Location Data** – This setting enables the AirWatch Admin Console to locate the device for Location Services.
   - **Enable Push Notification Services** – This setting enables the AirWatch Admin Console to send notifications to the device using WNS.

Uploading and Enabling Company Hub

For Windows Phone 8, you must install the AirWatch MDM Agent (also known as the Company Hub) on the device to take full advantage of the monitoring and management capabilities available following enrollment. The Company Hub is a .xap application file that you must first upload to the AirWatch Admin Console as an internal application. You must then enable the Company Hub configuration setting in order for the application to be made available for deployment to devices enrolling into your AirWatch environment.

To code sign the AirWatch Agent .xap application file:

1. Obtain the Symantec certificate that Microsoft provided in the Microsoft Developer's Account kit.
2. Obtain the AirWatch Agent .xap application file downloaded from your support hotline team.
3. Code sign the .xap application file with your Symantec certificate.

To upload the .xap application file:

1. Navigate to **Apps & Books ▶Applications ▶List View** from the AirWatch Admin Console main menu. By default, the internal application tab is selected.
2. Select **Add Application**.
3. Select **Upload**, navigate to the AirWatch MDM Agent .xap application file, and select **Open**.
4. Select **Save**.

5. Ensure the correct Organization Group displays in the **Add Application** window and select **Continue**.
6. Add or modify any application information as needed and then select **Save & Publish**.

Note: Once installed on the device, updates to the Company Hub application deploy automatically without user interaction.

To enable Company Hub:

1. Navigate to **Groups & Settings ▶All Settings ▶Devices & Users ▶Windows ▶Windows Phone 8** and select **Company Hub Settings**.
2. Select the **Override** radio button.
3. Select the **Enable Company Hub** checkbox.
4. Enter the name of the application in the **Company Hub Name** field.
5. Select the application you uploaded previously from the **Company Hub Application** drop-down menu.
6. Select **Save**.

Using the AirWatch Browser for Windows Phone 8

The AirWatch Browser is a safe, accessible and manageable Internet browser for your devices. You can customize and configure the AirWatch Browser to meet unique business and end user needs, restrict web access to certain websites, provide a secure Internet portal for devices used as a mobile point-of-sale, and more. Provide users with a standard browsing experience, including support of multi-tabbed browsing and Javascript pop-ups.

For additional information about preparing and configuring the AirWatch Browser for deployment, refer to the **AirWatch Browser Guide**.

Enforcing Application-Level Single Sign On Passcodes

AirWatch's single sign on (SSO) feature allows end users to access all AirWatch apps without having to enter login credentials for each application. Using either the AirWatch MDM Agent or the AirWatch Workspace as a "broker application", end users can authenticate once using either their normal credentials or an SSO Passcode and then gain access to other applications so long as the SSO session is active.

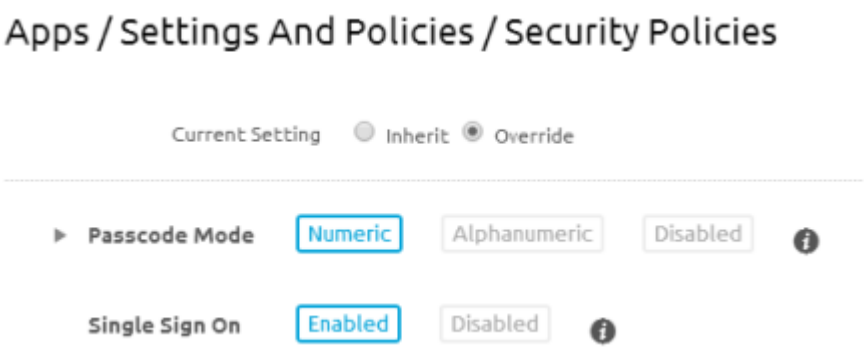
Enabling Single Sign On

Enable SSO as part of the **Security Policies** that you configure to apply to all AirWatch apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile. To enable SSO:

1. Navigate to **Groups & Settings ▶All Settings ▶Apps ▶Settings and Policies ▶Security Policies**.
2. Set **Single Sign On** to **Enabled** to allow end users to access all AirWatch applications and maintain a persistent login.

3. Optionally set **Passcode Mode** to either **Numeric** or **Alphanumeric** to require an SSO Passcode on the device. If you enable SSO but do not enable a Passcode Mode, end users will use their normal credentials (either directory service or AirWatch account) to authenticate, and an SSO Passcode will not exist.

   Note: Wrapped apps must have a passcode, either numeric or alphanumeric. Without this passcode, wrapped apps do not display true SSO functionality.



SSO Session

Once an end user authenticates with either the Workspace or the Agent, an SSO session is opened. It lasts so long as the Workspace is running in the background or until the **Passcode Timeout** value defined in the **Passcode Mode** settings is exceeded. With an active session, end users can access managed applications without having to enter their SSO Passcode.

Managing Windows Phone 8 Devices

Overview

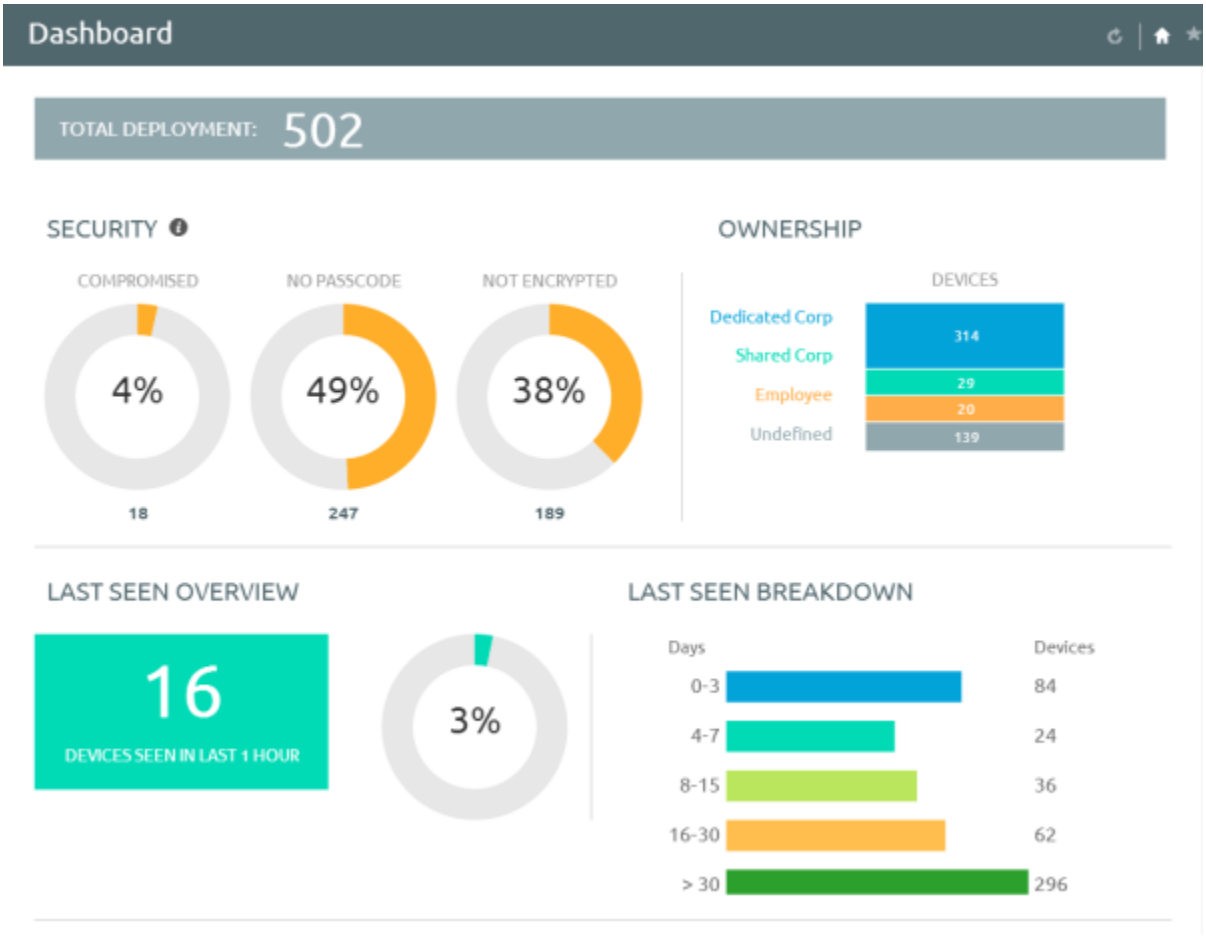
You can manage all of your deployment's devices from the AirWatch **Dashboard**. The **Dashboard** is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. 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

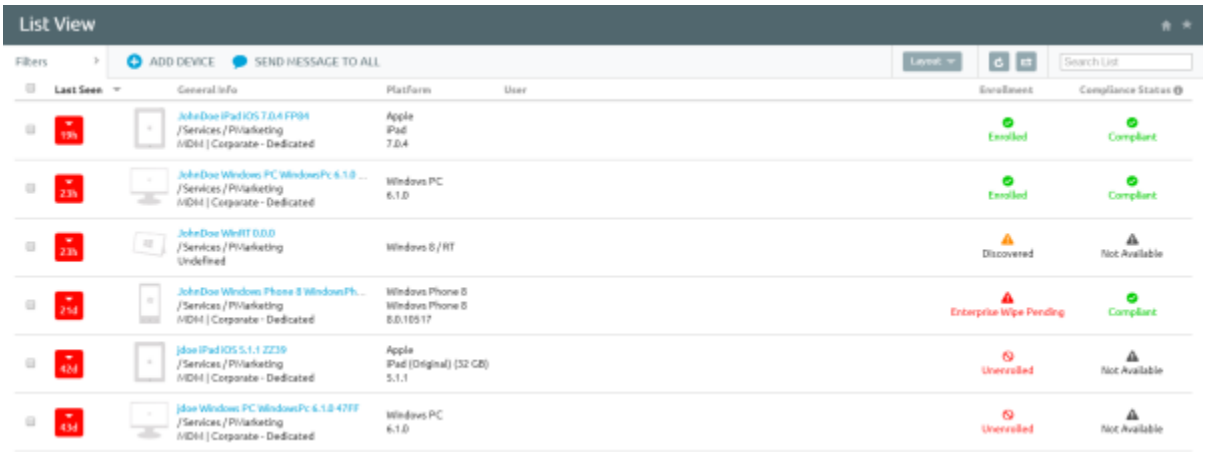
Switch to **List View** (**Devices ▶List View**) at any time to sort and manage devices by filtering the columns and fields available in the **Device Dashboard**, including:

- 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.

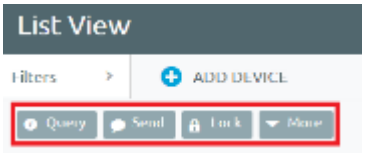
You can also drill down to specific sets of devices by filtering device criteria, including by **Platform**, **Ownership Type**, **Passcode**, **Last Seen**, **Enrollment**, **Encryption** and **Compromised** status.

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.

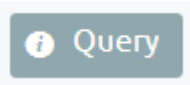
Once you have applied a filter to show a specific set of devices, perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the **Management** tabs.

Using the Management Tabs

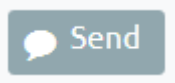
Note: The actions listed below will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.



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.

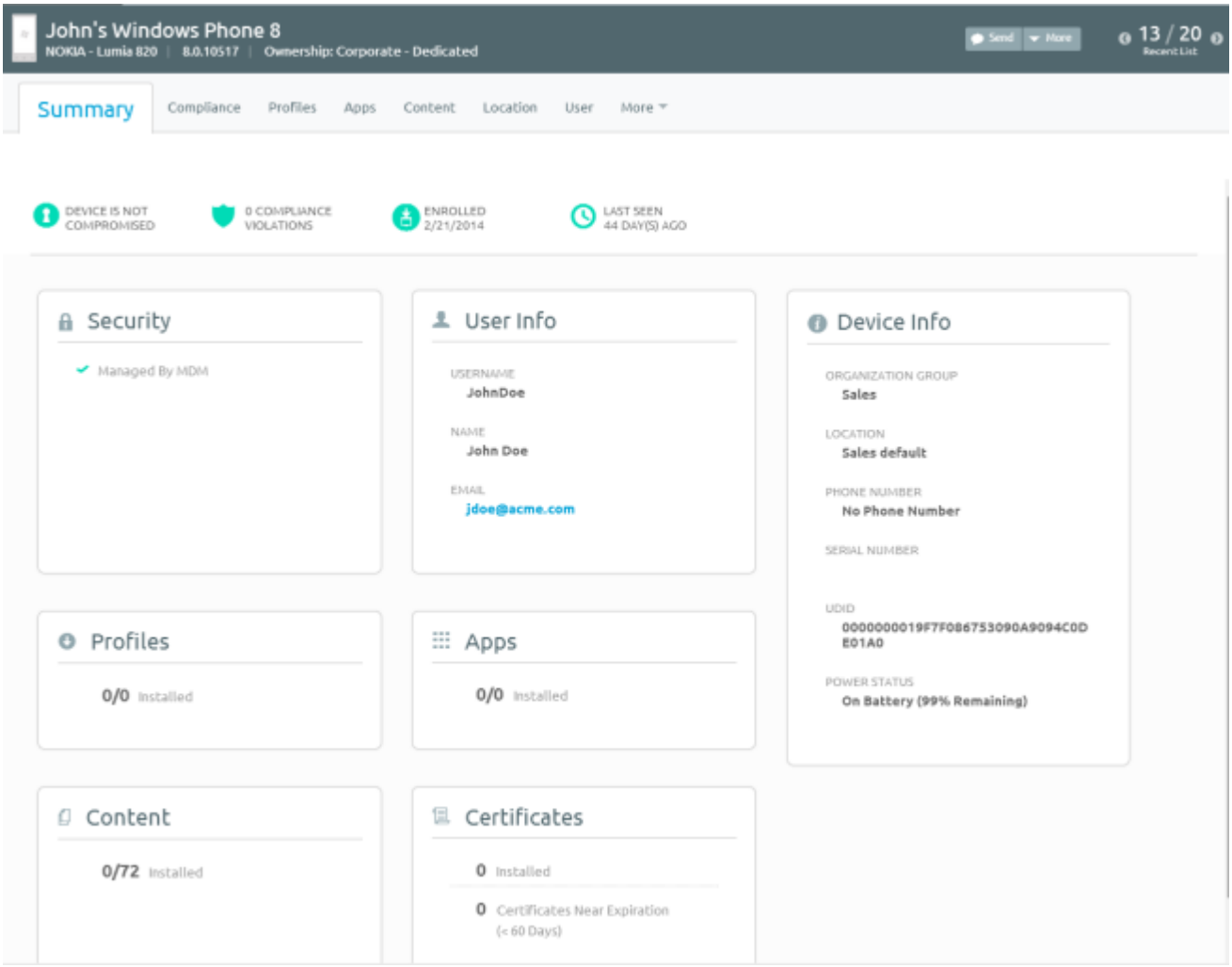
Lock – Lock all selected devices and force users to re-enter device security PIN.

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

- **Management** –Lock or perform Enterprise Wipe or Device Wipe on all selected devices. You can also change the device passcode.
- **Support** – Send a message to a device with instructions or communication to end user. You can also Ring the device to help locate it.
- **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 configurations 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.
- **Compliance** – Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View all apps currently installed or pending installation on the device.
- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

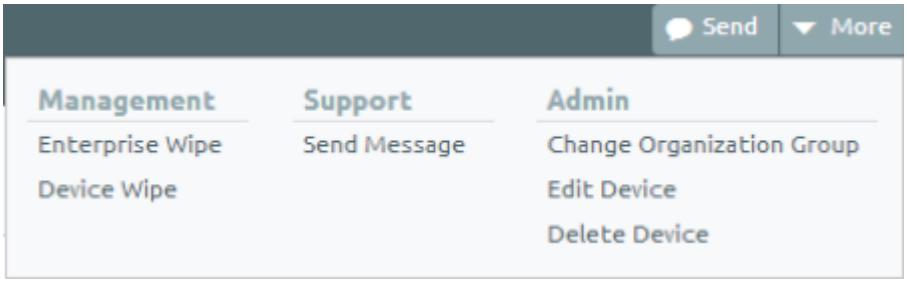
The menu tabs below are accessed by selecting **More** from the main Device Details tab (More).

- **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.

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 will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.

- **Management –** Perform an enterprise or device wipe.
- **Support –** Perform support actions such as sending the device a message.
- **Admin –** Change AirWatch Admin Console settings, including changing Organization Group, and editing/deleting devices from AirWatch MDM.

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.

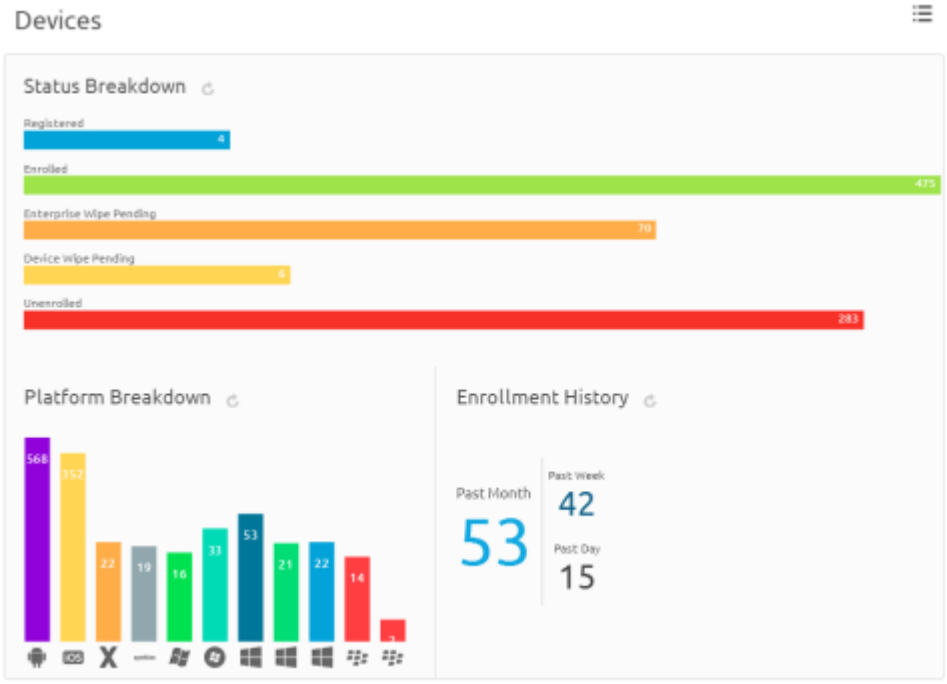
In addition, the administrator can schedule any of these reports for automated distribution to a group of users and recipients on either a defined schedule or a recurring basis. For example, you can run reports to see the number of

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.

For more information about generating custom reports, compiling a list of personalized bookmarked reports, and creating report subscriptions, refer to the **AirWatch Reporting Analytics Guide**.

Using the Hub

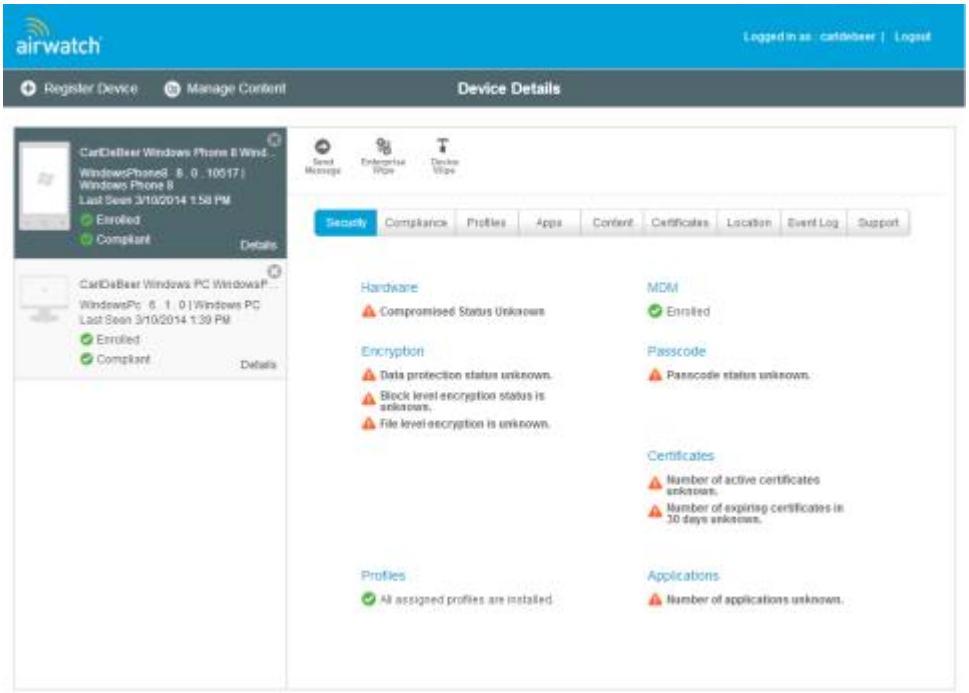
Utilize the AirWatch Hub as your central portal for fast access to critical information. Quickly identify important issues or devices and take action from a single location in the AirWatch Admin Console. Select any metric to open the **Device List View** for that specific set of devices, where you can 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.
- **Location** – This tab displays the coordinates of the selected device, if enabled.
- **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.

- **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 (In this case, you may also want to use the GPS feature to locate the device.)
- **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 will return to the state it was in prior to the installation of AirWatch MDM.
- **Device Wipe –** Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.
- **Find My Device –** Display a message along with an optional sound chime.