# Workspace ONE UEM Windows Phone

VMware Workspace ONE UEM 1903

**vm**ware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

# Contents

# Windows Phone Device Management

<span style="font-size:3em; color:#ccc;">1</span>

AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Windows Phone device deployment.

Through the AirWatch Console, you have several tools and features for managing the entire lifecycle of corporate and employee-owned devices. You can also enable end users to perform tasks themselves, for example, through the Self-Service Portal and user self-enrollment, which saves you vital time and resources.

AirWatch allows you to enroll both corporate and employee-owned devices to configure and secure your enterprise data and content. By using device profiles, you can properly configure and secure your Windows Phone devices.

Use AirWatch to manage Windows Phone devices from a central location. As an approved application in the Device Management (DM) system, the Workspace ONE Intelligent Hub can perform many device management functions that might not otherwise be available.

This chapter includes the following topics:

- Windows Phone Features Matrix
- Windows Phone Requirements

## Windows Phone Features Matrix

AirWatch features and functionality differ by each supported Windows Phone Platform.

| Feature | Windows 10 Mobile |
| --- | --- |
| Native Client Enrollment | ✓ |
| Hub Based Enrollment | ✓ |
| Native Enrollment with Web Dialog | ✓ |
| Force EULA/Terms of Use Acceptance | ✓ |
| Support for Option Prompts during Enrollment | ✓ |
| Active Directory/ LDAP | ✓ |
| Cloud Domain Join | ✓ |
| SMS | ✓ |
| Email Messages | ✓ |

| Feature | Windows 10 Mobile |
| --- | --- |
| Push Notifications | ✓ |
| Real Time Profile and Command Delivery | ✓ |
| Password Policy | ✓ |
| Lock, Ring, and Change Passcode Commands | ✓ |
| Enterprise Wipe | ✓ |
| Full Device Wipe | ✓ |
| Email & Exchange ActiveSync | ✓ |
| Wi-Fi | ✓ |
| VPN | ✓ |
| Root and CA Certificate Management | ✓ |
| Client Certificate Management (PFX) | ✓ |
| Client Certificate Management (SCEP) | ✓ |
| Device Restrictions and Settings | ✓ |
| Windows Hello | ✓ |
| Silent App Installation | ✓ |
| Silent App Update | ✓ |
| Silent App Removal | ✓ |
| App Whitelisting and Blacklisting | ✓ |
| Assigned Access (Kiosk Mode) | ✓ |
| VMware Browser | ✓ |
| VMware Content Locker | ✓ |
| Asset Tracking | ✓ |
| Device Status | ✓ |
| IP Address | ✓ |
| Location | ✓ |
| Network | ✓ |
| Send Support Message (Email and SMS only) | ✓ |
| Change Device Passcode | ✓ |

# Windows Phone Requirements

Before reading this guide, gather and prepare the requirements needed to use AirWatch with Windows Phone devices.

## Requirements for Internal Application Management

- **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.

    - **Signing Certificate** – You must use a certificate for code signing trusted by the devices you are install the app on. You can confirm this by ensuring that the root issuer of the cert is included in the device Trusted Root Store. Consider a publicly-trusted certificate.

    - **Trusted Code Signing Certificate** – Windows 10 supports signing internal apps with a Trusted Code Signing certificate. AirWatch also supports pushing root and intermediate certificates to establish the certificate trust chain.

**Important**   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.

## Enrollment Requirements

- **Active Environment** – This is your active Workspace ONE UEM environment and access to the Workspace ONE UEM console.

- **Appropriate Admin Permissions** – This type of permission allows you to create profiles, policies and manage devices within the UEM console.

- **Enrollment URL** – This URL is unique to your organization's enrollment environment and takes you directly to the enrollment screen. For example, **mdm.acme.com**.

- **Group ID** – This associates your device with your corporate role and is defined in the UEM console.

**Important**   If your enrollment server is behind a proxy, the Windows services need to be configured to be proxy-aware when configuring your network settings.

# Windows Phone Enrollment Overview

<div style="text-align: right">2</div>

Device enrollment establishes the initial communication with AirWatch to enable Mobile Device Management (MDM). Windows Phone devices enroll using MDM-functionality built into the Windows OS.

## Enrollment Basics

The enrollment methods for Windows Phone devices vary based on your AirWatch deployment, enterprise integrations, and device operating system. For more information, see Windows Phone Features Matrix.

Before enrolling devices, ensure that you have the required enrollment information. See Windows Phone Requirements for more information.

Simplify end-user enrollment by setting up the Windows Auto-Discovery Services (WADS) in your AirWatch environment. WADS supports an on-premises solution and cloud-based WADS.

The enrollment methods use either the native MDM functionality of the Windows operating system, the Workspace ONE Intelligent Hub for Windows, or Azure AD integration.

## Workspace ONE Intelligent Hub for Windows Enrollment

The simplest enrollment workflow uses the Workspace ONE Intelligent Hub for Windows to enroll devices. End users simply download the Workspace ONE Intelligent Hub from the Microsoft Store and follow the prompts to enroll. For more information on Hub-based enrollment, see Workspace ONE Intelligent Hub Enrollment for Windows Phone.

## Native MDM Enrollment

AirWatch supports enrolling Windows Phone devices using the native MDM enrollment workflow. The name of the native MDM solution varies based on the version of Windows. This enrollment flow changes based on the version of Windows and if you use WADS.

For more information, see Native MDM Client Enrollment for Windows Phone

# Azure AD Integration Enrollment

Through integration with Microsoft Azure Active Directory, Windows devices can automatically enroll into AirWatch with minimal end-user interaction. Azure AD integration enrollment simplifies enrollment for both end users and admins. Azure AD integration enrollment supports two different enrollment flows: Join Azure AD and Office 365 enrollment, and adding a work account. All methods require configuring Azure AD integration with AirWatch.

Before you can enroll your devices using Azure AD integration, you must configure AirWatch and Azure AD. For more information, see Configure Azure AD Identity Services Integration.

To enroll through Azure AD integration workflows, see Enrollment through Azure AD Integration.

This chapter includes the following topics:

- Workspace ONE Intelligent Hub Enrollment for Windows Phone

- Native MDM Client Enrollment for Windows Phone

- Enrollment through Azure AD Integration

# Workspace ONE Intelligent Hub Enrollment for Windows Phone

Use the Workspace ONE Intelligent Hub app to provide a single resource to enroll Windows Phone devices and facilitate communication between the device and the AirWatch Console.

Enrollment through the Workspace ONE Intelligent Hub provides simple step-by-step instructions for your end users. The app is downloaded through the Microsoft Store so end users can start enrollment whenever they are ready.

The Workspace ONE Intelligent Hub provides extra functionality to your Windows Mobile devices including location services.

**Note**   Windows 10 Mobile devices use the VMware Workspace ONE Intelligent Hub. Windows Phone 8.0 and 8.1 devices use the AirWatch MDM Agent.

## Enroll Windows 10 Mobile devices with the VMware Workspace ONE Intelligent Hub

Use the VMware Workspace ONE Intelligent Hub to enroll your Windows Mobile 10 devices. The VMware Workspace ONE Intelligent Hub provides a simplified enrollment flow for end users allowing for quick and easy enrollment.

**Procedure**

1   On the Windows 10 Mobile device, navigate to the Microsoft Store and search for VMware Workspace ONE Intelligent Hub and download it.

**2**    Install the application. Once installation finishes, start the app.

**3**    Select **Connect a work or school account** to the native Work Access enrollment client.

**4**    Select **Enroll in to device management**.

**5**    Enter the email address and select **Next**. If you are not using Windows Auto-Discovery, complete the following steps:

    a    Enter the **Server URL** and select**Next**.

    b    Enter the **Group ID** and select **Next**.

    c    Enter the **Username** and **Password**.

**6**    **Accept** the terms of use.

**7**    Select **Done**.

**8**    Open the VMware Workspace ONE Intelligent Hub to complete the enrollment. A second certificate pushes to the device to complete the enrollment. If the certificate has not installed after one minute, a link appears offering troubleshooting solutions.

# Native MDM Client Enrollment for Windows Phone

The native MDM Client for Windows Phone devices allows end users to enroll devices without downloading the Workspace ONE Intelligent Hub. End users enter their enrollment information into the MDM Client and the device enrolls into AirWatch.

The name of the native MDM client depends on the version of Windows Phone. The client is called Work Access for Windows 10 Mobile devices.

**Note**   Consider using the Workspace ONE Intelligent Hub enrollment method as it offers simple step-by-step instructions for the end user.

## Enroll Windows Phone Devices with Work Access

Work Access is the native MDM enrollment method for Windows 10 devices. Enrolling through Work Access and using Windows Auto Discovery provides a quick and easy enrollment flow for end users.

**Procedure**

**1**    On the Windows 10 Mobile device, navigate to **Settings > Accounts > Work Access**.

**2**    Select **Enroll in to device management**.

3   Enter the end user **Email Address** and select **Connect**. If you do not have Windows Auto-Discovery enabled, completed the following steps:

    a   Enter the **Server**, using the following format: <Device Services hostname> such as ds01.awmdm.com.

    b   Select **Connect**

    c   Enter the **Group ID**

4   Enter the end-user **Username** and **Password**, and then select **Next**.

5   Accept the **Terms of Use** if enabled.

**What to do next**

You can also download the VMware Workspace ONE Intelligent Hub from the Microsoft Store following enrollment to add extra functionality to your Windows 10 Mobile device.

# Enrollment through Azure AD Integration

Through integration with Microsoft Azure Active Directory, Windows devices can automatically enroll into AirWatch with minimal end-user interaction. Azure AD integration enrollment simplifies enrollment for both end users and admins.

Before you can enroll your devices using Azure AD Integration, you must configure AirWatch and Azure AD. The configuration requires entering information into your Azure AD and AirWatch deployments to facilitate communication.

Azure AD integration enrollment supports two different enrollment flows: Join Azure AD and Office365 enrollment. Both methods require configuring Azure AD integration with AirWatch.

For more information on configuring Active Directory in general, see the **Directory Services Guide**.

**Important**   Enrollment through Azure AD integration requires Windows Mobile 10 and Azure Active Directory Premium License.

## Configure Azure AD Identity Services Integration

Before you can use Azure AD to enroll your Windows devices, you must configure Workspace ONE UEM to use Azure AD as an Identity Service. Enabling Azure AD is a two-step process which requires the MDM-enrollment details to be added to Azure.

**Prerequisites**

You must have a Premium Azure AD P1 or P2 subscription to integrate Azure AD with Workspace ONE UEM. Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory (such as LDAP) is configured.

**Important**   If you are setting the **Current Setting** to **Override** on the Directory Services system settings page, the LDAP settings must be configured and saved before enabling Azure AD for Identity Services.

**Procedure**

1   Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.

2   Enable **Use Azure AD for Identity Services** under **Advanced** settings. Once enabled, take note of the MDM Enrollment and MDM Terms of Use URLs as they are needed when configuring the Azure directory.

3   Log in to the Azure Management Portal with your Microsoft account or organizational account.

4   Select your directory and navigate to the **Mobility (MDM and MAM)** tab. This tab was formerly the Applications tab.

5   Select **Add Application** and select the AirWatch by VMware application.

You can use the default URLs if the user scope is set to none. If needed, you can also use placeholder URLs.
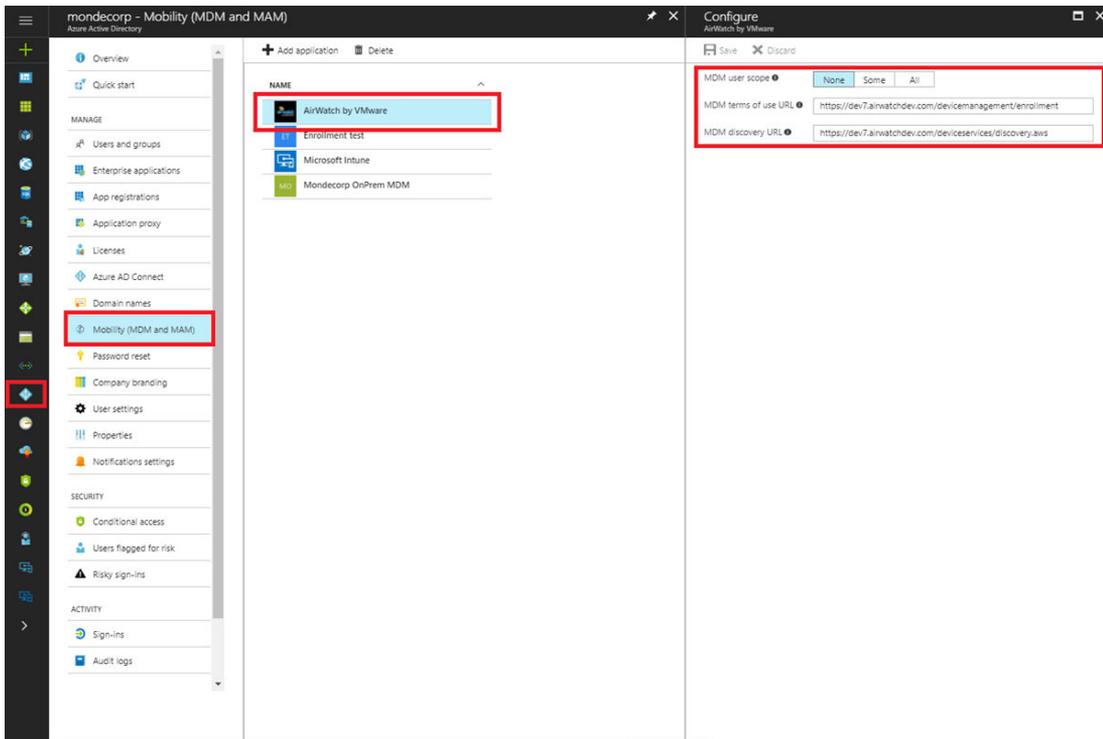
**6** Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **None**.
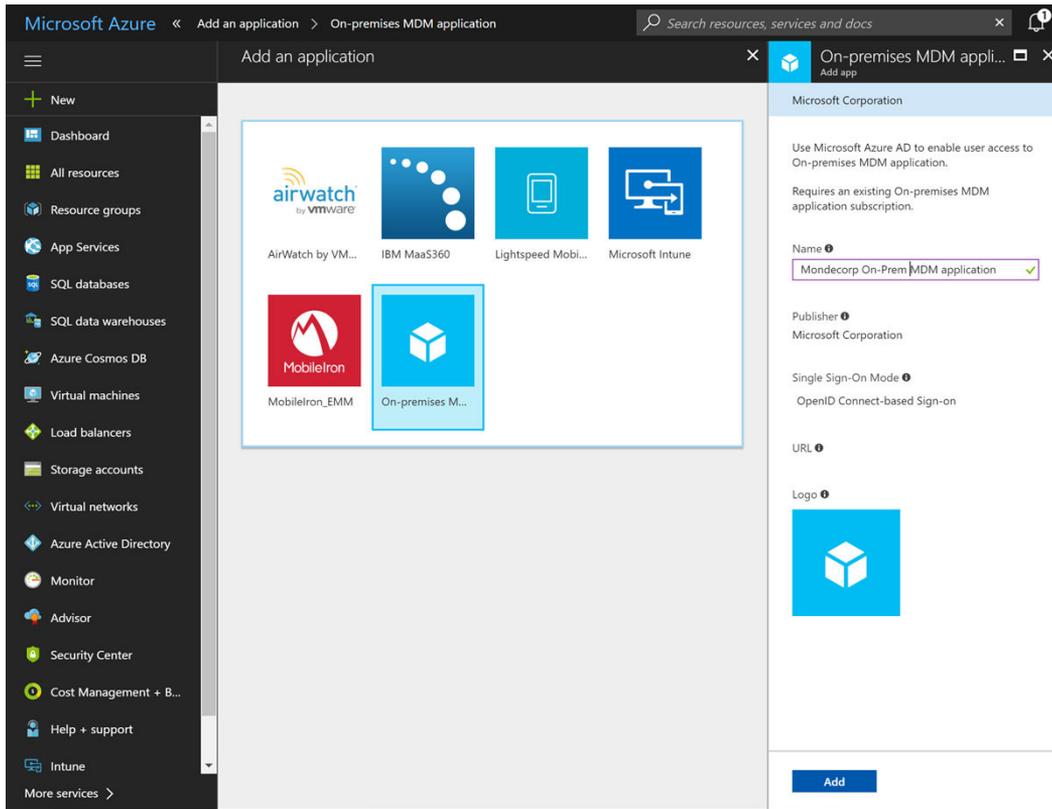


**7** Select **Add Application** again and select the **On Premises MDM application**. You can rename the application when you add it.

**8** Configure the On-Premises MDM application by entering the **MDM Enrollment URL** and **MDM Terms of Use** URLs from the Workspace ONE UEM Console.

**9** Select **On-premises MDM application settings** then select **Required Permissions > Windows Azure Active Directory**.

**10** Change the Application Permissions as follows:

   a   Select **Read and write directory data**.

   b   Select **Read and write devices**.

**11** Change the Delegated Permissions as follows:

   a   Select **Access the directory as the signed-in user**.

   b   Select **Read directory data**.

   c   Select **Sign in and read user profile**.

**12** Select the Properties settings and enter your device services host in the **APP ID URI** text box.

Use the same host that you used in the **MDM Enrollment URL** and **MDM Terms of Use** text boxes.

https:// <MDM DS SERVER>

**13** Set **MDM user scope** to **All** to apply these settings to all users.

You can also limit the OOBE enrollment to selected Azure AD groups by selecting **Some** and adding the preferred groups.

**14** Select **Save** to continue.

**15** Navigate to the Properties tab and find the Azure Directory ID. This setting was formerly called the **Tenant ID**.
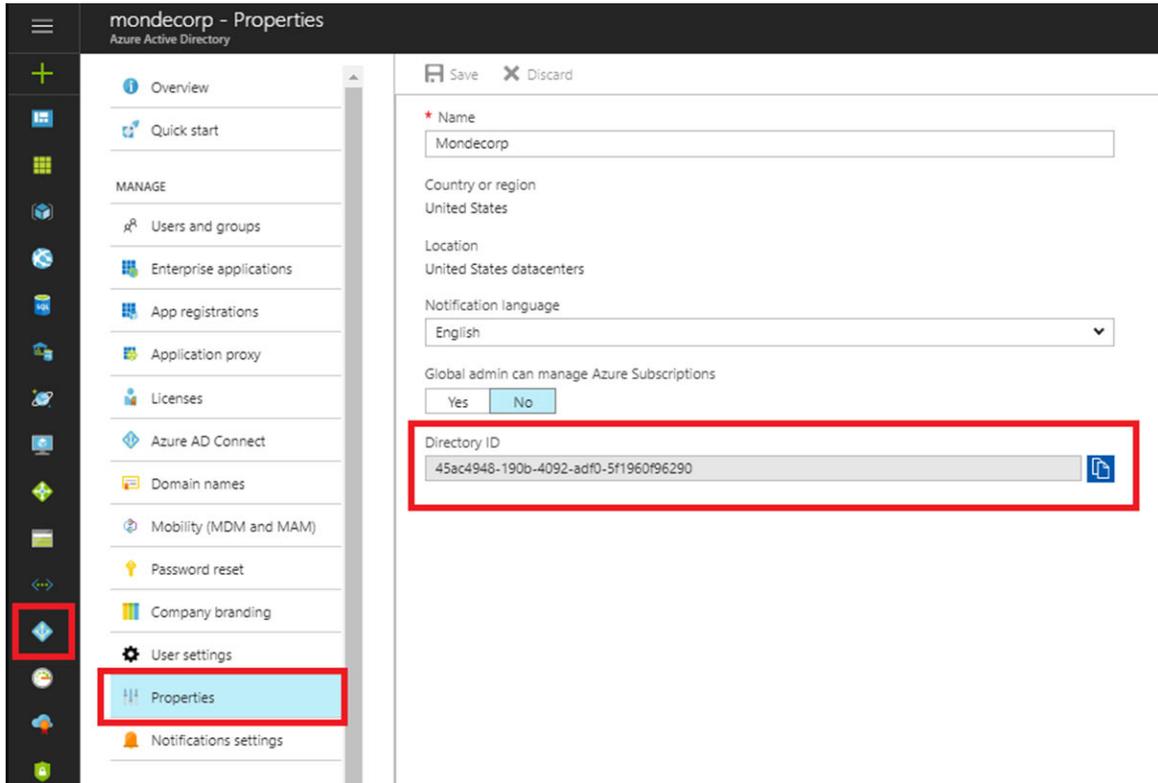


**16** Select **User Account Details** in the top right corner. The Azure **Tenant Name** is the name of your Azure Directory. You can find the name under the **Domain** tab.

**17** Return to the UEM Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.

**18** Enter the **Azure Directory ID** as the **Tenant Identifier**. Enter the default domain as your Azure Directory **Tenant Name**.

**19** Select **Save** to finish the process.

## Enroll a Windows Phone Device with Cloud Domain Join

Cloud domain join enrollment uses Azure AD integration to enroll a device into the correct organization group in AirWatch automatically. Devices enrolled through the cloud domain join method are joined completely. This method means all users on the device join the domain.

**Procedure**

1   Navigate on the Windows 10 Mobile device to **Settings > Accounts > Your Account > Add a work or school account**.

2   Enter your **Email Address** and **Password**.

3   Select **Sign In**.

4   Ensure that the AirWatch welcome page displays and then select **Continue.**.

5   Select **Next**.

6   Select **Accept** if terms of use are enabled.

7   Select **Join** to confirm that you want to enroll in AirWatch.

8   Select **Finish** to complete joining your device to AirWatch. Your device now downloads the applicable policies and profiles.

# Enroll Windows Phone Devices through Office 365 Apps

If your company uses Office 365 and Azure AD integration, end users can enroll their own devices the first time they open an Office 365 app.

**Procedure**

1   Select **Add a Work Account** the first time you open an Office365 application.

2   Enter your **Email Address** and **Password**.

3   Select **Sign In**.

4   Ensure that the AirWatch welcome page displays.

5   Select **Continue**.

6

7   Select **Next**.

8   Select **Accept** if terms of use are enabled

9   Select **Join** to confirm that you want to enroll in AirWatch.

10  Select **Finish** to complete joining your device to AirWatch. Your device now downloads the applicable policies and profiles.

# Windows Phone Profiles Overview

<span style="color:#888">3</span>

Profiles are the primary means by which you can manage devices. Configure profiles so your Windows Phone devices remain secure and can access your data.

## Overview

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

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

## Device Access

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

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Configure a Passcode Profile (Windows Phone)

- Configure the native Passport functionality. For more information, see Configure a Windows Hello Profile (Windows Phone)

- Configure how the device home screen looks and control access to apps and settings. For more information, see Configure an Assigned Access Profile (Windows Phone).

## Device Security

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

Some examples of device security profiles include:

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

- Keep corporate data secure with the Data Protection profile. For more information, see Data Protection Profile (Windows Phone).

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

# Device Configuration

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

Some examples of device configuration profiles include:

- Set up an Exchange account on a device with an Exchange ActiveSync profile. For more information, see Exchange ActiveSync Profiles (Windows Phone).

- Restrict what applications can install on a device with the Application Control profile. For more information, see Configure Application Control (Windows Phone).

This chapter includes the following topics:

- Configure a Passcode Profile (Windows Phone)
- Configure a Restrictions Payload (Windows Phone)
- Configure Wi-Fi Payloads (Windows Phone)
- VPN Profile (Windows Phone)
- Configure an Email Profile (Windows Phone)
- Exchange ActiveSync Profiles (Windows Phone)
- Configure Application Control (Windows Phone)
- Assigned Access Profile (Windows Phone)
- Credentials Profile (Windows Phone)
- SCEP Profile (Windows Phone)
- Windows Hello Profile (Windows Phone)
- Create a Windows Licensing Profile (Windows Phone)
- Data Protection Profile (Windows Phone)
- Create Custom Settings Profile (Windows Phone)

# Configure a Passcode Profile (Windows Phone)

Enforce a Passcode profile to protect end user devices with passcodes each time they return from an idle state. A passcode ensures that all sensitive corporate information on managed devices remains protected.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and then select **Windows Phone**.

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

4   Select the **Passcode** profile.

5   Configure the Passcode settings, including:

| Settings | Descriptions |
| --- | --- |
| Password Complexity | Set whether required passcode is **Simple** or **Complex**. |
| Alphanumeric Password | Set whether the passcode must be alphanumeric or let the end user decide. |
| Require Idle State PIN or Password | Set whether the passcode or PIN must be entered when resuming the device from an idle state. |
| Minimum number of complex characters | Enter the minimum number of complex characters (lowercase, uppercase, symbols, numbers, etc.) required for a passcode. |
| Minimum Password Length | Enter the minimum number of characters a passcode must have. |
| Maximum Passcode Age (days) | Enforce users to renew passcodes at selected intervals. |
| Passcode History | Enter the number of passwords remembered. The end user cannot reuse a previous password. For example, if you entered 12 in this field, an end user cannot re-use the past twelve passwords. |
| 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. The time set here is the maximum amount of a time before the device requires a passcode to be entered. The end users may shorten that time in the device settings but cannot lengthen the time past the amount entered in this payload. |

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

# Configure a Restrictions Payload (Windows Phone)

Deploy a restrictions payload for added security on Windows Phone devices. Restrictions payloads for Windows Phone devices can disable end user access to device features to ensure devices are not tampered with.

**Procedure**

1  Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2  Select **Windows** and then select **Windows Phone**.

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

4  Select the **Restrictions** profile.

5  Configure the **Administration** settings:

| Settings | Descriptions |
|---|---|
| Allow Manual MDM Enrollment | Allow the end user to enroll into AirWatch through the native MDM enrollment. This restriction applies to all Windows Phone devices. |
| Allow User To Reset Phone | Allow the end user to factory reset their device. This restriction applies to all Windows Phone devices. |
| Allow Adding Non-Microsoft Accounts Manually | Allow the end user to add accounts such as Facebook or Twitter manually. |
| Experimentation | Allow Microsoft to experiment with the product to study user preferences or device behavior. This restriction applies to Windows 10 Mobile devices only. |
| Location | Allow the use of location services. This restriction applies to all Windows Phone devices. |
| Allow Manual Root Certificate Installation | Allow end user to manually install root and intermediate CAP certificates. This restriction applies to all Windows Phone devices. |
| User Decryption | Allow users to decrypt the device. This restriction applies to Windows 10 Mobile devices only. |
| Allow Telemetry | Allow the device to send telemetry information (such as SQM or Watson) to the AirWatch Console. |
| Allow User to Change Data Sense Settings | Allows the user to change the Data Sense application settings. |
| Date/Time | Allows the user to change the Date and Time settings. |
| VPN | Allows the user to change the VPN configuration. |
| Allow User to Change Account Settings | Allows the user to change the Account settings. |
| Allow Action Center Notifications | Allow app and device notifications to display in the Action Center of the device. |
| App Store | Allow access to the app store. |

| Settings | Descriptions |
|---|---|
| App Store Auto Update | Allows applications from the app store to automatically update. |
| Bluetooth | Allow the connection of devices through Bluetooth. |
| Allow Browser | Allow end users to use the native Internet Explorer browser. |
| Camera | Allows the user to access the camera function of the device. |
| Allow Copy and Paste | Allows the user to copy and paste on the device. |
| Cortana | Allow access to the Cortana application. |
| Direct Memory Access | Allows direct memory access. |
| Indexing of Encrypted Stores or Items | Allows the indexing of encrypted stores or items for faster searching. |
| Allow NFC | Allow the use of the Near Field Communication chip on the device. |
| Allow Save as of Office Files | Allows the user to Save as Office files and change the file name and location. |
| Allow Sharing Office Files | Allows the users to share Office files. |
| Allow Search to Use Location | Allows the user searches to use the device location services. |
| Screen Capture | Allows the user to take screenshots of the device. |
| Allow Storage Card | Allow the use of a SD card. |
| Allow Storing of Vision Search Images | Allow the storage of Vision Search images onto the device. |
| Allow Sync Settings Between Devices | Allows the users to sync their settings preferences between Windows 10 Mobile and Windows Desktop devices. |
| Allow Task Switching | Allows the users to use the task switcher to switch between apps. |
| Allow USB Connection | Allow desktop to access phone storage through USB. Both MTP and IPoUSB are disabled when this restriction is enforced. |
| Use Diacritics | Allows the use of diacritics for languages such as the accent or cedilla. |
| Automatic Language Detection | Specifies whether to always use automatic language detection when indexing content and properties. |
| Allow Voice Recording | Allow the end users to record voice recordings. |
| Require Device Encryption | Encrypt all data stored on the device to prevent an end user from accessing readable, sensitive information.<br><br>**Important**  If you select this feature, you cannot return to not encrypting device data by simply deselecting the checkbox. In order to return the device to an unencrypted state, you must restore the device to factory settings (i.e., device wipe). |
| Require Strict Safe Search | Require searches to use the strict safe search setting. |
| Allow Non-Microsoft Store Trusted Applications | Allows the downloading and installation of applications that are not trusted by the Microsoft Store. |
| Allow Developer Unlock | Allows the user of the Developer Unlock setting for sideloading applications onto devices. |

| Settings | Descriptions |
|---|---|
| Allow Shared Among Multiple Users of the Same App | Allows sharing of data between multiple users of an app. |
| Restrict App Data to System Volume | Restricts app data to the same volume as the OS instead of secondary volumes or removable media. |
| Restrict Installation of Applications to System Drive | Restricts the installation of apps to the system drive instead of secondary drives or removable media. |
| Allow Auto Connect to Wi-Fi Sense Hotspots | Allow the device to automatically connect to Wi-Fi hotspots using the Wi-Fi Sense functionality. |
| Allow Cellular Data Roaming | Allow cellular data usage while roaming. |
| Allow Internet Sharing | Allow Internet sharing between devices. |
| Allow Manual VPN Configuration | Allow creation of VPN connections. |
| Allow Manual Wi-Fi Configuration | Allow connections to Wi-Fi outside of the MDM server installed networks. |
| VPN Over Cellular | Allow the device to create a VPN over cellular networks. |
| VPN Roaming over Cellular | Allow the device to create a VPN while roaming over cellular networks. |
| Wi-Fi | Allows the users to connect to Wi-Fi. |
| Allow Wi-Fi Hotspots Reporting | Allow Wi-Fi Hotspots information reporting to Microsoft. Once disallowed, the user cannot turn this function on. |
| WLAN Scan Frequency | Select the frequency of scans when the device searches for Wi-Fi networks to connect to. |
| Cellular App Download Limit | Set the application file size limit to prevent the users from downloading large apps over cellular data. |
| Cookies | Allows the use of cookies. |
| Do Not Track | Allows the sending of Do Not Track requests. |
| Password Manager | Allows the use of the password manager to store website credentials. |
| SmartScreen Filter | Allows the use of the SmartScreen Filter to protect devices from malicious sites and downloads. |

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

# Configure Wi-Fi Payloads (Windows Phone)

Create a Wi-Fi profile to connect devices to hidden, encrypted, or password-protected corporate networks. Wi-Fi profiles are useful for end users who travel to various office locations that have unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network.

**Procedure**

1    Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2    Select **Windows** and then select **Windows Phone**.

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

4    Select the **Wi-Fi** profile.

**5** Configure the **General** settings, including:

| Settings | Descriptions |
| --- | --- |
| Service Set Identifier | Enter an identifier that is associated with the name (SSID) of the desired Wi-Fi network. |
| Hidden Network | Enable if the network is not open to broadcast. |
| Auto-Join | Enable to set the device to automatically join the network. |
| Security Type | Use the drop-down menu to select the security type (e.g., WPA2 Personal) for the Wi-Fi network. |
| Encryption | Use the drop-down menu to specify if data transmitted using the Wi-Fi connection is encrypted.<br>Displays based on the **Security Type**. |
| Password | Enter the password required to join the Wi-Fi network.<br>Select the **Show Characters** check box to disable hidden characters within the field.<br>Displays based on the **Security Type**. |
| Proxy | Enable to configure proxy settings for the Wi-Fi connection. |
| URL | Enter the URL for the proxy. |
| Port | Enter the port for the proxy. |
| Protocols | Select the type of protocols to use:<br>• **Certificate**<br>• **EAP-TTLS**<br>• **PEAP-MsChapv2**<br>• **Custom**<br>This section displays when the **Security Type** is set to WPA Enterprise or WPA2 Enterprise. |
| Inner Identity | Select the method of authentication through EAP-TTLS:<br>• **Username/Password**<br>• **Certificate**<br>This section displays when the **Protocols** field is set to EAP-TTLS or PEAP-MsChapv2. |
| Require Crypto Binding | Enable to require cryptographic binding on both authentications.<br>This limits man-in-the-middle attacks. |
| Use Windows Log On Credentials | Enable to use the Windows log on credentials are the username/password to authenticate.<br>Displays when **Username/Password** is set as the **Inner Identity**. |
| Identity Certificate | Select an Identity Certificate, which you can configure using the Credentials payload. For more information, see Configure a Credentials Profile (Windows Phone)<br>Displays when **Certificate** is set as the **Inner Identity**. |

| Settings | Descriptions |
|---|---|
| Trusted Certificates | Select **Add** to add Trusted Certificates to the Wi-Fi profile.<br><br>This section displays when the **Security Type** is set to WPA Enterprise or WPA2 Enterprise. |
| Allow Trust Exceptions | Enable to allow trust decisions to be made by the user through a dialog. |

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

# VPN Profile (Windows Phone)

AirWatch supports configuring device VPN settings so end users can remotely and securely access your organizations internal network. The VPN profile provides granular VPN settings control including specific VPN provider settings and Per-App VPN access.

AirWatch supports specific VPN connection types for various third-party VPN providers, including:

| | |
|---|---|
| ▪ IKEv2 | ▪ F5 Edge Client |
| ▪ L2TP | ▪ Juniper Pulse |
| ▪ PPTP | ▪ Sonic Wall Mobile Connect |
| ▪ Check Point Mobile | ▪ Automatic |
| ▪ Cisco AnyConnect | ▪ VMware Tunnel |

## Per-app VPN

Per-app VPN allows you to configure VPN traffic rules based on specific applications. When configured, the VPN can automatically connect when a specified app is launched and send the application traffic through the VPN traffic but no traffic from other applications. With this flexibility, you can ensure that your corporate data remains secure while not limiting devices access to the Internet at large.

Watch a tutorial video explaining how to configure the Windows VPN profile for Per-app VPN: https://support.air-watch.com/articles/115001664668

Each rule group under the Per-App VPN Rules section uses the logical OR operator. So if traffic matches any of the set policies, it is allowed through the VPN.
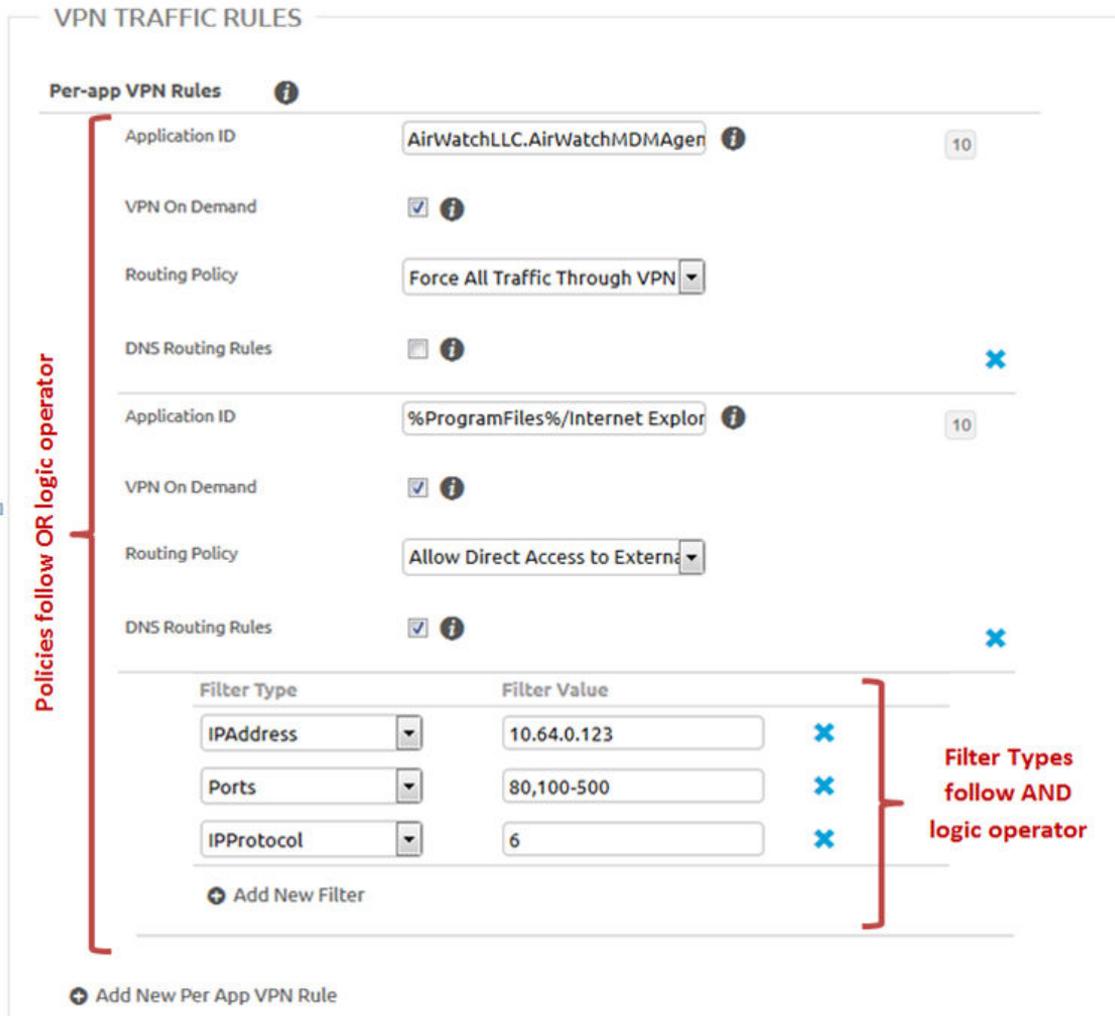
The applications for which Per-app VPN traffic rules apply can be legacy Windows applications such as EXE files or modern apps downloaded from the Microsoft Store. By designating specific applications to start and use the VPN connection, only the traffic from those apps uses the VPN and not all device traffic. This logic allows you to keep corporate data secure while reducing the bandwidth sent through your VPN.

To help you reduce VPN constraint, you can set DNS routing rules for the Per-app VPN connection. These routing rules limit traffic sent through the VPN to only that traffic that matches the rules. The logic rules use the AND operator so if you set an IP Address, Port, and IP Protocol, the traffic much match EACH of these filters to pass through the VPN.

Per-app VPN allows you to create granular, detailed control over your VPN connections on an app by app basis.

## Configure a VPN Profile (Windows Phone)

Configure device VPN settings to remotely and securely access corporate infrastructure. You can also configure Per-app VPN connections that limit traffic through the VPN to specific applications and set the VPN to automatically connect whenever the specified application is launched.

This payload is only available to devices using Windows 10 Mobile or Windows 10 Mobile. If you want to use this payload, you must download and install the free update.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and then select **Windows Phone**.

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

4   Select the **VPN** payload.

5   Configure the VPN settings.

| Settings | Description |
|---|---|
| Connection Name | Enter the name of the VPN connection. |
| Connection Type | Select the type of VPN connection: |
| | The connection type will support all third-party VPN providers available on the Windows store. |
| Server | Enter the VPN server, hostname, or IP Address. |
| Advanced Connection Settings | Enable to configure advanced routing rules for device VPN connections. |
| Routing Addresses | Select **Add** to enter the IP Addresses and Subnet Prefix Size of the VPN server. |
| | You may add additional routing addresses as needed. |
| DNS Routing Rules | Select **Add** to enter the **Domain Name** on which the VPN server is hosted. Enter the **DNS Servers** and **Web Proxy Servers** to use for each specific domain. |
| Routing Policy | Select **Split Tunnel** to allow traffic to use the VPN or the local network connection. Select **Force Tunnel** to force all traffic through the VPN. |
| Proxy | Select **Auto Detect** to automatically detect any proxy servers used by the VPN. Select **Manual** to configure the proxy server. |
| Server | Enter the IP Address for the proxy server. |
| | Displays when **Proxy** is set to **Manual**. |
| Proxy Server Config URL | Enter the URL for the proxy server configuration settings. |
| | Displays when **Proxy** is set to **Manual**. |
| Bypass proxy for local | Enable to bypass the proxy server when the device detects it is on the local network. |
| Authentication Type | Select the authentication protocol for the VPN: |
| | ■ EAP – Allows for various authentication methods. |
| | ■ Machine Certificate – Detects a client certificate in the device certificate store to use for authentication. |

| Settings | Description |
|---|---|
| Protocols | Select the type of EAP authentication: |
| | <ul><li>EAP-TLS – Smart Card or client certificate authentication</li><li>EAP-MSCHAPv2 – Username and Password</li><li>EAP-TTLS</li><li>PEAP</li><li>Custom Configuration – Allows all EAP configurations</li></ul> |
| Credential Type | Select **Use Certificate** to use a client certificate. Select **Use Smart Card** to use a Smart Card to authenticate. |
| | Displays when **EAP Type** is set to **EAP-TLS**. |
| Simple Certificate Selection | Enable to simplify the list of certificates from which the user selects. The certificates are grouped by the entity that the certificate was issued for and the most recently issued certificate is presented. |
| | Displays when **EAP Type** is set to **EAP-TLS**. |
| Use Windows Log On Credentials | Enable to use the same credentials as the Windows device. |
| | Displays when **EAP Type** is set to **EAP-MSCHAPv2**. |
| Identity Privacy | Enter the value to send servers before the client authenticates the server's identity. |
| | Displays when **EAP Type** is set to **EAP-TTLS**. |
| Inner Authentication Method | Select the authentication method for inner identity authentication. |
| | Displays when **EAP Type** is set to **EAP-TTLS**. |
| Enable Fast Reconnect | Enable to reduce the delay in time between an authentication request by a client and the response from the server. |
| | Displays when **EAP Type** is set to **PEAP**. |
| Enable Identity Privacy | Enable to protect the user identity until the client authenticates with the server. |
| Per-app VPN Rules | Select **Add** to add traffic rules for specific Legacy and Modern applications. For more information on Per-app VPN, see VPN Profile (Windows Phone). |
| Application ID | Enter the application package family name to specify the app the traffic rules apply to. |
| | <ul><li>Package Family Name example: AirWatchLLC.AirWatchMDMAgent_htcwkw4rx2gx4</li></ul> |
| VPN On Demand | Enable to have the VPN connection automatically connect when the application is launched. |
| Routing Policy | Select the routing policy for the app. |
| | <ul><li>**Allow Direct Access to External Resources** allows for both VPN traffic and traffic through the local network connection.</li><li>**Force All Traffic Through VPN** forces all traffic through the VPN.</li></ul> |

| Settings | Description |
|---|---|
| DNS Routing Rules | Enable to add DNS routing rules for the app traffic. |
| | Select **Add** to add **Filter Types** and **Filter Values** for the routing rules. Only traffic from the specified app that matches these rules can be sent through the VPN. |
| | ■ **IP Address**: A list of comma separated values specifying remote IP address ranges to allow. |
| | ■ **Ports**: A list of comma separated values specifying remote port ranges to allow. For example, 100-120, 200, 300-320. Ports are only valid when the protocol is set to TCP or UDP. |
| | ■ **IP Protoco**l: Numeric value from 0-255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17. |
| | For more information on how these filters and policies function and the logic used, see VPN Profile (Windows Phone). |
| Device Wide VPN Rules | Select **Add** to add traffic rules for the entire device. |
| | Select **Add** to add **Filter Types** and **Filter Values** for the routing rules. Only traffic that matches these rules can be sent through the VPN. |
| Remember Credentials | Enable to remember the end user's login credentials. |
| Always On | Enable to force the VPN connection to always be on. This will turn the VPN connection back on when the network connection disconnects and reconnects. |
| VPN Lockdown | Enable to force the VPN to always be on, never be disconnected, disable any network access if the VPN is not connected, and prevent connection or modification to other VPN profiles. |
| Trusted Network | Enter, separated by commas, trusted network addresses. The VPN does not connect when a trusted network connection is detected. |
| WP8 Split Tunnel | Enable to allow end users to use a split tunnel VPN. |
| | This field applies to Windows 10 Mobile devices only. |
| Bypass for Local | Enable to bypass the VPN connection for local intranet traffic. For example, you do not use the VPN connection if you are also connected to your work network connection at the office. |
| | This field applies to Windows 10 Mobile devices only. |
| Connection Type | Select the connection type you want to allow. |
| | Always ON leaves the VPN connection running at all times. |
| | This field applies to Windows 10 Mobile devices only. |
| Trusted Network Detection | Enable to use Trusted Network Detection when connecting to the VPN. |
| | This field applies to Windows 10 Mobile devices only. |
| Idle Disconnection Time | Set the maximum amount of time that can pass without connectivity requests before automatically disconnecting the VPN. |
| | This field applies to Windows 10 Mobile devices only. |

| Settings | Description |
|---|---|
| Allows Apps | Select **Add** to define apps to have all their traffic secured over the VPN. |
| | You may add as many apps as you like. |
| Allowed Networks | Select **Add** to define networks. |
| | All traffic over configured networks are secured over the VPN. |
| | You may add as many networks as you like. |
| Excluded Apps | Select **Add** to define excluded apps. |
| | All traffic to these apps are NOT secured over the VPN. |
| | You may add as many excluded apps as you like. |
| Excluded Networks | Select **Add** to define excluded networks. |
| | All traffic over excluded networks are NOT secured over the VPN. |
| | You may add as many excluded networks as you like. |
| DNS Suffix Search List | Select **Add** to define the DNS Suffix Search List. |
| | DNS suffixes are appended to short name URLs for DNS resolution and connectivity. |
| | You may add as many DNS suffixes as you like. |

6  Select **Save & Publish**.

# Configure an Email Profile (Windows Phone)

The Email profile sets up end user IMAP/POP3 email accounts and sends configurations directly to their devices.

**Procedure**

1  Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2  Select **Windows** and then select **Windows Phone**.

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

4  Select the **Email** profile.

5  Configure the Email settings.

| Settings | Descriptions |
|---|---|
| Email Service Name | Enter the email service provider. |
| Name | Enter the name of the email account to appear in the mail client. |
| Email Address | Enter the user email address. |
| | You can use lookup values to use the device specific value. |
| Domain | Enter the user's domain. |
| Reply Address | Enter the email address that replies are sent from. |
| | You can use lookup values to use the device specific value. |

| Settings | Descriptions |
|---|---|
| Maximum Email Truncation Size (bytes) | Enter the maximum amount an email is truncated in bytes. |
| Maximum Attachment Size (KB) | Enter the maximum attachment size allowed to be sent. |
| Past Days of Emails to Download | Enter the number of days of past emails to download when the account syncs for the first time on the device. |
| Use SSL | Enable to use Secure Socket Layer when receiving emails. |
| Protocol | Select the email protocol for incoming mail. |
| Host Name | Enter the email server URL for incoming mail. |
| Use SSL | Enable to use Secure Socket Layer when sending emails. |
| Protocol | Select the email protocol for outgoing mail. |
| Host Name | Enter the email server URL for outgoing mail. |
| Enable Authentication | Enable to secure IMAP/POP3 email traffic on devices by enforcing authentication to access these email accounts. |
| Allow Alternative SMTP Domain | Enable to configure an alternative SMTP domain. |
| Alternative SMTP Domain | Enter the alternate SMTP domain. Displays when **Allow Alternative SMTP Domain** is enabled. |
| Alternative SMTP Username | Enter the username for the alternate SMTP domain. Displays when **Allow Alternative SMTP Domain** is enabled. |
| Alternative SMTP Password | Enter the password for the alternative SMTP domain. Displays when **Allow Alternative SMTP Domain** is enabled. |

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

# Exchange ActiveSync Profiles (Windows Phone)

The Exchange ActiveSync profiles allow you to configure your Windows Phone devices to access your Exchange ActiveSync server for email and calendar use.

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

The Exchange ActiveSync profile supports the native mail client and AirWatch Inbox for Windows Phone. The configuration changes based on which mail client you use.

## Configure an Exchange ActiveSync Profile (Windows Phone)

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

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

**Procedure**

1    Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

**2** Select **Windows** and then select **Windows Phone**.

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

**4** Select the **Exchange ActiveSync** profile.

**5** Configure the Exchange settings:

| Settings | Descriptions |
|---|---|
| Mail Client | Select the mail client for the exchange profile. |
| Account Name | Enter the name for the account to display in the mail client. |
| 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. |
| Domain | Enter the end-user's domain. You can use the Lookup Values instead of creating individual profiles for each end user. |
| Username | Enter the end-user's username. You can use the Lookup Values instead of creating individual profiles for each end user. |
| Email Address | Enter the end-user's email address. You can use the Lookup Values instead of creating individual profiles for each end user. |
| Password | Enter the password for the end user. You can use the Lookup Values instead of creating individual profiles for each end user. |
| Identity Certificate | Select (if desired) an Identity Certificate from the drop-down 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 Configure a Credentials Profile (Windows Phone). |
| Next Sync Interval (Min) | Enter the number of minutes between syncs. |
| Past Days of Mail to Sync | Select the number of days of past mail to sync with device. |
| Diagnostic Logging | Select the type of diagnostic logging you want to gather. |
| Require Data Protection Under Lock Configuration | Enable to protect data when a device is pin locked. When the device is configured to use a pin lock, the protected data is encrypted using a separate enterprise key at all times. If someone gains access to the device pin lock, your organization's email and data are protected by a separate key. |
| Allow Email Sync | Allow the syncing of email. Disabling this setting will remove access to email through Exchange Active Sync. |
| Allow Contacts Sync | Allow the syncing of contacts. |
| Allow Calendar Sync | Allow the syncing of calendars. |

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

# Configure an EAS Profile for AirWatch Inbox (Windows Phone)

Create an Exchange ActiveSync profile to give Windows Phone devices access to your Exchange ActiveSync server for email and calendar use. The settings change when you use the AirWatch Inbox as your Windows Phone email client.

**Procedure**

**1**    Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

**2**    Select **Windows** and then select **Windows Phone**.

**3**    Select **Windows** and then select **Windows Phone**.

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

**5**    Select the **Exchange ActiveSync** payload.

| Settings | Descriptions |
|---|---|
| **Mail Client** | Set to AirWatch Inbox. |
| **Exchange ActiveSync Host** | Enter the public host name or server name hosting your Exchange ActiveSync. |
| **Use SSL** | Select the checkbox to send all information through the Secure Socket Layer. |
| **Use S/MIME** | Select the checkbox to store an end user's S/MIME certificate to be used with S/MIME enabled profiles. |
| **Ignore SSL** | Select the checkbox to allow the devices to ignore Secure Socket Layer errors from Hub processes. |
| **Domain** | Enter the end-user's email domain. You can use the Lookup Values instead of creating individual profiles for each end user. |
| **Username** | Enter the end-user's email username. You can use the Lookup Values instead of creating individual profiles for each end user. |
| **Email Address** | Enter the end-user's email address. You can use the Lookup Values instead of creating individual profiles for each end user. |
| **Password** | Enter the password for the end user. You can use the Lookup Values instead of creating individual profiles for each end user. |
| **Identity Certificate** | Select (if desired) an Identity Certificate from the drop-down 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 to select a certificate, see Configure a Credentials Profile (Windows Phone). |
| **Enable Calendar** | Enable to allow the syncing of calendar events. |
| **Enable Contacts** | Enable to allow the syncing of contacts. |

| Settings | Descriptions |
|---|---|
| Sync Interval | Select the time interval between syncs to the EAS server. |
| Email Notifications | Select the type of notifications that display on the device. |
| Past Days of Mail to Sync | Select the number of days of past mail to sync with device. |
| Past Days of Calendar to Sync | Select the number of days of past calendar events to sync with device. |
| Email Signature | Enter the signature to use with all emails sent from this device. |
| Enable Signature Editing | Enable to allow end users to edit their signature. |
| Require Passcode | Enable to enter a passcode to protect the AirWatch Inbox application. |
| Type | Select the type of passcode security.<br>■ **Passcode** requires a string of numbers and letters to unlock the app.<br>■ **Username and Password** requires the end user to enter their login credentials to unlock the app. |
| Complexity | Select the level of complexity of the passcode as either a simple numeric passcode or a more complex alphanumeric.<br>Displays when the passcode **Type** is set to **Passcode**. |
| Minimum Length | Select the minimum number of characters the passcode can be.<br>Displays when the passcode **Type** is set to **Passcode**. |
| Allow Simple Value | Enable to allow end users to create a simple passcode regardless of the passcode settings configured.<br>Displays when the passcode **Type** is set to **Passcode**. |
| Maximum Age | Select the number of days until the passcode must be changed.<br>Displays when the passcode **Type** is set to **Passcode**. |
| History | Select the number of previous passcodes to remember. A new passcode may not match a previous passcode that is stored in the history.<br>Displays when the passcode **Type** is set to **Passcode**. |
| Auto Lock When Device Locks | Enable to automatically lock the application when the device is locked. |
| Grace Period | Enter time in minutes that pass before the app automatically locks. |
| Maximum Number of Failed Attempts | Select the maximum number of failed attempts allowed before all data on the device is wiped. |
| Disable Copy-Paste | Enable the checkbox to disable the copy-paste functionality while using the application. |
| Disable Screen Capture | Enable the checkbox to disable the screenshot functionality while using the application. |
| Disable Attachments | Enable the checkbox to disable the use of attachments when sending emails. |
| Maximum Attachment Size (MB) | Enter the maximum size (in MB) of an attachment that can be uploaded. |

| Settings | Descriptions |
|---|---|
| Content Locker Only Attachments | Enable the checkbox to open the attachments that are attached only through Content Locker. |
| Restrict Domains | Enable to restrict the domains through whitelisting or blacklisting specific domains. |

**6** Select **Save & Publish**.

# Configure Application Control (Windows Phone)

Create a profile of blacklisted and whitelisted applications to limit app access to your Windows Phone devices.

**Procedure**

**1** Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

**2** Select **Windows** and then select **Windows Phone**.

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

**4** Select the **Application Control** payload.

**5** Enable or disable the following settings to set the level of control for your application deployments:

| Settings | Descriptions |
|---|---|
| Prevent Installation of Blacklisted Apps | Enable to prevent the installation enforce and the automatic removal of blacklisted apps defined in Configure an Application Group. |
| Only Allow installation of Whitelisted Apps | Enable to prevent the installation of any application that is not a whitelisted app defined in Configure an Application Group. |

**6** Select **Save & Publish**.

If you update your Application Group after publishing the profile, you must republish the profile for it to take effect on devices.

## Configure an Application Group

Configure application groups, or app groups, so that you can use the groups in your compliance policies. Take set actions on devices that do not comply with the installing, updating, or removing applications.

You assign application groups to organization groups. When you assign the application group to a parent organization group, the child organization groups inherit the application group configurations.

**Procedure**

**1** Navigate to **Apps & Books > Applications > Applications Settings > App Groups**.

**2** Select **Add Group**.

**3** Complete options on the **List** tab.

| Setting | Description |
| --- | --- |
| Type | Select the type of application group you want to create depending on the desired outcome: allow applications, block applications, or require application installations.<br><br>If your goal is to group custom MDM applications, select**MDM Application**. You must enable this option for it to display in the menu. |
| Platform | Select the platform for the application group. |
| Name | Enter a display name for the application group in the Workspace ONE UEM console. |
| Add Application | Display text boxes that enable you to search for applications to add to the application group. |
| Application Name | Enter the name of an application to search for it in the respective app store. |
| Application ID | Review the string that automatically completes when you use the search function to search for the application from an app store. |
| Add Publisher - Windows Phone | Select for Windows Phone to add multiple publishers to application groups.<br><br>Publishers are organizations that create applications.<br><br>Combine this option with **Add Application** entries to create exceptions for the publisher entries for detailed whitelists and blacklists on Windows Phone. |

**4** Select **Next** to navigate to an application control profile. You must complete and apply an application control profile for Windows Phone. You can use an application control profile for Android devices.

**5** Complete settings on the **Assignment** tab.

| Setting | Description |
| --- | --- |
| Description | Enter the purpose of the application group or any other pertinent information. |
| Device Ownership | Select the type of devices to which the application group applies. |
| Model | Select device models to which the application group applies. |
| Operating System | Select operating systems to which the application group applies. |
| Managed By | View or edit the organization group that manages the application group. |
| Organization Group | Add more organization groups to which the application group applies. |
| User Group | Add user groups to which the application group applies. |

**6** Select **Finish** to complete configurations.

# Assigned Access Profile (Windows Phone)

The Assigned Access profile limits access to specific functions and control features of Windows Phone 8.1 and Windows 10 Mobile devices. Use this profile to control the apps displayed on the front page or app list, the settings accessed, and the function of each hardware key.

Assigned Access enables an enterprise to provision a device into a state with a locked down user experience. The start screen can be customized with pinned applications, and the system buttons can be disabled or configured to have custom actions. You can also customize the settings panel to display only certain settings to the user.

Consider using the Application Control and the Assigned Access payloads together to ensure that your devices are controlled.

**Caution**   The Assigned Access profile may cause devices to fail or lose connectivity and requires that the device is serviced at a repair center to reset it to factory settings. This profile is a one-way action and cannot be removed. Once this profile is published, your devices must be factory-reset to regain normal functionality.

## Configure an Assigned Access Profile (Windows Phone)

Create an Assigned Access profile to limit access to the device settings and functions and set the location of applications on the start screen.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and then select **Windows Phone**.

3   Configure the profile **General** settings.

4   Select the **Assigned Access** profile and configure the following settings:

| Settings | Descriptions |
| --- | --- |
| **Add Application** | Select to add a Windows 10 Mobile app to the device screen. |
| **Application Name** | Enter the name of the application that you want to configure and add to the device. Select the Search icon(🔍) to select the application from a list. |
| **Identifier** | Enter the alphanumeric identifier for the Windows app. This text box is automatically populated if you use the app lookup. |
| **Pin to Start** | Enable to pin the Live Tile to the Start screen. If the app is added but not pinned, it appears on the app list. |
| **Size** | Select the size of the Live Tile used on the front screen. |
| **Column** | Set the X-axis location of the Live Tile. |

| Settings | Descriptions |
| --- | --- |
| Row | Set the Y-axis location of the Live Tile. |
| Add Application | Select to add a Windows 10 Mobile app to the device screen. |
| Application Name | Select the application that you want to configure and add the device. |
| Pin to Start | Enable to pin the Live Tile to the Start screen. If the app is added but not pinned, it appears on the app list. |
| Size | Select the size of the Live Tile used on the front screen. |
| Column | Set the X-axis location of the Live Tile. |
| Row | Set the Y-axis location of the Live Tile. |
| Airplane Mode | Enable to allow access to the Airplane Mode settings screen. |
| Backup | Enable to allow access to the Backup settings screen. |
| Bluetooth | Enable to allow access to the Bluetooth settings screen. |
| Cellular & SIM | Enable to allow access to the Cellular & SIM settings screen. |
| Data Sense | Enable to allow access to the Data Sense settings screen. |
| Feedback | Enable to allow access to the Feedback settings screen. |
| Internet Sharing | Enable to allow access to the Internet Sharing settings screen. |
| NFC | Enable to allow access to the NFC settings screen. |
| Phone Update | Enable to allow access to the Phone Update settings screen. |
| Sync My Settings | Enable to allow access to the Sync My Settings settings screen. |
| VPN | Enable to allow access to the VPN settings screen. |
| Wi-Fi | Enable to allow access to the Wi-Fi settings screen. |
| About | Enable to allow access to the About settings screen. |
| Advertising ID | Enable to allow access to the Advertising settings screen. |
| Battery Saver | Enable to allow access to the Battery Saver settings screen. |
| Colors | Enable to allow access to the Colors settings screen. |
| Brightness | Enable to allow access to the Brightness settings screen. |
| Date and Time | Enable to allow access to the Date and Time settings screen. |
| Driving Mode | Enable to allow access to the Driving Mode settings screen. |
| Ease of Access | Enable to allow access to the Ease of Access settings screen. |
| Find My Phone | Enable to allow access to the Find My Phone settings screen. |
| Keyboard | Enable to allow access to the Keyboard settings screen. |
| Project My Screen | Enable to allow access to the Project My Screen settings screen. |

| Settings | Descriptions |
| --- | --- |
| Ringtones & Sounds | Enable to allow access to the Ringtones & Sounds settings screen. |
| Screen Rotation | Enable to allow access to the Screen Rotation settings screen. |
| Start and Theme | Enable to allow access to the Start and Theme settings screen. |
| USB | Enable to allow access to the USB settings screen. |
| Language | Enable to allow access to the Language settings screen. |
| Location | Enable to allow access to the Location settings screen. |
| Email and Accounts | Enable to allow access to the Email and Accounts settings screen. |
| Kids Corner | Enable to allow access to the Kids Corner settings screen. |
| Lock Screen | Enable to allow access to the Lock Screen settings screen. |
| Notifications & Actions | Enable to allow access to the Notifications & Actions settings screen. |
| Quiet Hours | Enable to allow access to the Quiet Hours settings screen. |
| Region | Enable to allow access to the Region settings screen. |
| Storage Sense | Enable to allow access to the Storage Sense settings screen. |
| Workplace | Enable to allow access to the Workplace settings screen. |
| Cortana | Enable to allow access to the Cortana settings screen. |
| Internet Explorer | Enable to allow access to the Internet Explorer settings screen. |
| Maps | Enable to allow access to the Maps settings screen. |
| Messaging | Enable to allow access to the Messaging settings screen. |
| Office | Enable to allow access to the Office settings screen. |
| People | Enable to allow access to the People settings screen. |
| Phone | Enable to allow access to the Phone settings screen. |
| Photos and Camera | Enable to allow access to the Photos and Camera settings screen. |
| Search | Enable to allow access to the Search settings screen. |
| Microsoft Store | Enable to allow access to the Microsoft Store settings screen. |
| Wallet | Enable to allow access to the Wallet settings screen. |
| Narrator | Enable to allow access to the Narrator settings screen. |
| Magnifier | Enable to allow access to the Magnifier settings screen. |
| High Contrast | Enable to allow access to the High Contrast settings screen. |
| Closed Captions | Enable to allow access to the Closed Captions settings screen. |
| More Options | Enable to allow access to the More Options settings screen. |

| Settings | Descriptions |
|---|---|
| Camera | Enable to allow use of the Camera hardware key. |
| | You can set different behavior for Windows 10 Mobile devices and Windows 10 Mobile devices. |
| Search | Enable to allow use of the Search hardware key. |
| | Enable **Remap** to change what application the hardware key starts when pressed. |
| | You can set different behavior for Windows 10 Mobile devices and Windows 10 Mobile devices. |
| Start | Enable to allow use of the Start hardware key. |
| | You can set different behavior for Windows 10 Mobile devices and Windows 10 Mobile devices. |
| Start Menu Grid Layout> | Choose the layout option for the start screen. |
| | This option controls the number of columns visible on the start menu. |
| | High-resolution devices have the option of 4 or 6 columns while lower resolutions display 4 columns. |
| Action Center | Enable to allow the use of the Action Center. |
| Allow User to Resize Tiles | Enable to allow the user to resize tiles on the home screen. |
| Menu Items | Enable to allow the user to access the context menu, which is displayed when a user presses and holds an application in the All Programs list. |
| Theme Background & Color | Select **Admin Enabled** to set the theme background and color for the device. |
| Background Color | Select **Light** or **Dark** for the device background color. |
| | This option displays if **Theme Background & Color** is set to **Admin Enabled**. |
| Foreground Accent Color | Select the foreground accent color from the available drop-down menu. |
| | This option displays if **Theme Background & Color** is set to **Admin Enabled**. |
| Time Zone Settings | Set to **Admin Enabled** to set the time zone for the device. |
| Time Zone | Select the device time zone from the available drop-down menu. |
| | This option displays if **Time Zone Settings** is set to **Admin Enabled**. |

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

# Windows Phone Assigned Access Start Screen Layout

The Assigned Access profile supports pinning applications to specific location on the device start screen.

To pin or allow certain applications to the start screen, you must select the application from the drop-down menu in the Assigned Access payload and then configure their placement. Refer to the image to the right to understand how to place an application on the start screen.

The start screen can be either small or large size (configurable in the Assigned Access payload). The small screen size has a total of 4 columns, while the large screen size has 6 columns.

The rows on a start screen are infinite. You can have as few or as many applications on the start screen as you want. Applications can have the sizing option of small, medium, or large:

- Small applications are 1x1
- Medium applications are 2x2
- Large applications are 4x2
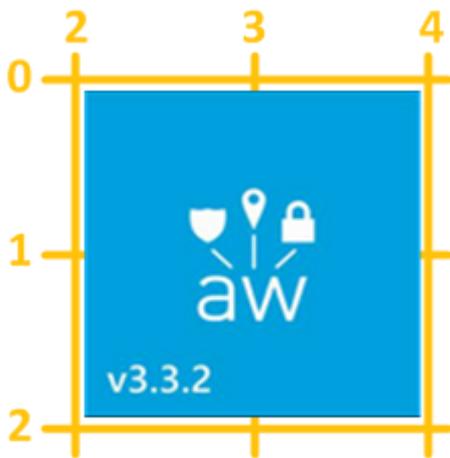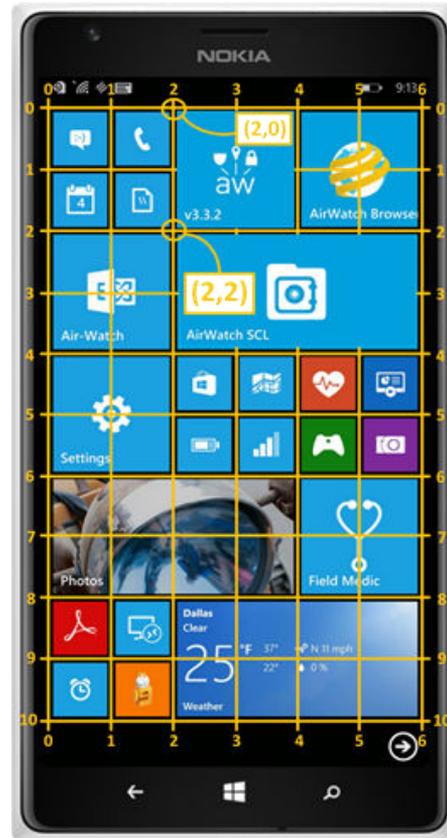


In the image to the left, the Workspace ONE Intelligent Hub is placed on the start screen. Measure the column and row values for where this application is placed. Referring to the coordinate system, the top left corner (used to place the apps position) is located at (2,0). When the Assigned Access profile is configured, input the column value of 2 and row value of 0.



# Credentials Profile (Windows Phone)

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

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

The Credentials profile also allows you to push S/MIME certificates to devices. These certificates are uploaded under each user account and controlled by the Credentials profile.

Windows Phone 8.0 or 8.1 devices using the Credentials payload to push Personal Certificates need the Workspace ONE Intelligent Hub downloaded. End users are required to install any certificates as mentioned in Install a Personal Certificate on a Windows 10 Mobile Device. The Root and Intermediate certificates install silently onto the device without the Workspace ONE Intelligent Hub or the end-user interaction.

## Configure a Credentials Profile (Windows Phone)

A Credentials profile pushes certificates to devices for use in authentication. AirWatch supports configuring credentials for personal, intermediate, trusted root, trusted publisher, and trusted people certificate stores.

### Prerequisites

To push certificates onto the devices, you need to configure a Credentials payload as part of the profiles that you create for EAS, Wi-Fi, and VPN settings.

**Note** For Windows 8.0 and 8.1, the Root and Intermediate certificates silently install to the device without interaction from the end user. The Personal Certificates cannot be installed silently with the Credentials payload and require end-user interaction. Please see Install a Personal Certificate on a Windows 10 Mobile Device section for more information. To silently install Personal Certificates without end-user involvement, see the Configure a SCEP Payload (Windows Phone).

### Procedure

1    Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2    Select **Windows** and then select **Windows Phone**.

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

**4** Select the **Credentials** payload and configure the following settings:

| Settings | Descriptions |
|---|---|
| Credential Source | Select the credential source as either an **Upload** or a **Defined Certificate Authority**, or **User Certificate**<br><br>The remaining payload options are source-dependent.<br><br>▪ If you select **Upload**, you must upload a new certificate. If you select **Defined Certificate Authority**, you must choose a predefined certificate authority and Template.<br><br>▪ If you select **User Certificate**, you must select how the **S/MIME** certificate is used. |
| Upload | Select to navigate to the desired credential certificate file and upload it to the AirWatch Console.<br><br>This setting displays when **Upload** is selected as the **Credential Source**. |
| Certificate Authority | Use the drop-down menu to select a predefined certificate authority.<br><br>This setting displays when **Defined Certificate Authority** is selected as the **Credential Source**. |
| Certificate Template | Use the drop-down menu to select a predefined certificate template specific to the selected certificate authority.<br><br>Displays when **Defined Certificate Authority** is selected as the **Credential Source**. |
| Export Private Key | Select **Allow** to let end users export certificates using Windows Certificate Manager or select **Don't Allow** to prohibit end users from exporting certificates. |
| Key Location | Select the location for the certificate private key:<br><br>▪ **TPM If Present** – Select to store the private key on a Trusted Platform Module if one is present on the device, otherwise store it in the software.<br><br>▪ **TPM Required** – Select to store the private key on a Trusted Platform Module. If a TPM is not present, the certificate does not install and an error displays on the device.<br><br>▪ **Software** – Select to store the private key in the device software.<br><br>▪ **Passport** – Select to save the private key within Microsoft Passport. This requires the AirWatch Protection Agent to be installed on the device. |
| Certificate Store | Select from the drop-down menu the appropriate certificate store for the credential to reside in on the device:<br><br>▪ **Personal** – Select to store personal certificates.<br><br>▪ **Intermediate** – Select to store certificates from Intermediate Certificate Authorities.<br><br>▪ **Trusted Root** – Select to store certificates from Trusted Certificate Authorities as well as root certificates from your organization and Microsoft.<br><br>▪ **Trusted Publisher** – Select to store certificates from Trusted Certificates Authorities that are trusted by software restriction policies.<br><br>▪ **Trusted People** – Select to store certificates from trusted people or end entities that are explicitly trusted. Often these are self-signed certificates or certificates explicitly trusted in an application such as Microsoft Outlook. |
| Store Location | Use the drop-down menu to select **User** or **Machine** to define where the certificate is located. |
| S/MIME | Select whether the S/MIME certificate is for encryption or signing. |

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

# Install a Personal Certificate on a Windows 10 Mobile Device

After you configure a Credentials profile for a certificate in the personal store, install the certificate onto a Windows 10 Mobile device. Credentials provide authentication for end users to access corporate resources.

**Procedure**

1   Open the Workspace ONE Intelligent Hub on the device.

2   Navigate to the **My Device** section of the Workspace ONE Intelligent Hub.

3   Tap 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 that the AirWatch Admin pushed in a payload.

   a   If a certificate contains a password, **Copy Password** option is displayed. Tap **Copy Password** to copy the password to the device's clipboard.

   b   If an email certificate does not display, verify if it was pushed to the device from the AirWatch Console.

5   Tap **Install Certificate** 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 in the image.

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

7   Tap **Ok** on the **Your certificates are installed** screen.

   The email certificate is now installed on the device and displays on the Certificate(s) screen of the device. The installation is successful when the device user can authenticate an email client with the Exchange server.

# SCEP Profile (Windows Phone)

Simple Certificate Enrollment Protocol (SCEP) profiles allow you to install certificates onto devices silently without the need of end-user interaction.

Even if you protect your email, Wi-Fi, and VPN with strong passcodes, your infrastructure remains vulnerable to brute force, dictionary attack, and employee error. For greater security, you can implement digital certificates to protect corporate assets. To use SCEP to install these certificates to devices silently, you must first define a certificate authority, then configure a **SCEP** payload alongside your **EAS**, **Wi-Fi**, or **VPN** payload. Each payload has settings for associating the certificate authority defined in the SCEP payload.

To push certificates to devices, you must configure a **SCEP** payload as part of the profiles you created for EAS, Wi-Fi, and VPN settings.

## Configure a SCEP Payload (Windows Phone)

A SCEP profile silently installs certificates onto end user devices for use with device authentication.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and then select **Windows Phone**.

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

4   Select the **SCEP** profile.

5   Configure the SCEP settings, including:

| Settings | Descriptions |
| --- | --- |
| Credential Source | This drop-down menu is always set to defined certificate authority. |
| Certificate Authority | Select the certificate authority you want to use. |
| Certificate Template | Select the template available for the certificate. |
| Issuer | Enter the issuer of the certificate. The issuer can be found in the subject line of the certificate. |
| Store Location | Select where the SCEP stores on the machine:<br>■ **Context User** – Stores the SCEP with the specific user.<br>■ **Context Machine** – Stores the SCEP for all users on the machine. |

6   Configure the Wi-Fi, VPN, or EAS profile.

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

8

**What to do next**

Combine SCEP payloads with a Wi-Fi, VPN, or an EAS payload when you create a profile.

For more information on these payloads:

■   Exchange ActiveSync Profiles (Windows Phone)

■   VPN Profile (Windows Phone)

■   Configure Wi-Fi Payloads (Windows Phone)

# Windows Hello Profile (Windows Phone)

Microsoft Passport provides a secure alternative to using passwords for security. The Windows Hello profile configures Microsoft Passport for your Windows 10 Mobile devices so end users can access your data without sending a password.

Protecting devices and accounts with a user name and password creates potential security exploits. Users can forget a password or share it with non-employees, putting your corporate data at risk. Using Passport, Windows Mobile 10 devices securely authenticate the user to applications, Web sites, and networks on the behalf of the user without sending a password. The user does not need to remember passwords, and man-in-the-middle attacks are less likely to compromise your security.

Passport requires users to verify possession of a Windows 10 device before it authenticates with either a PIN or Windows Hello biometric verification. Once authenticated with Passport, the device gains instant access to Web sites, applications, and networks.

**Important**  Windows Hello requires Azure AD integration to work.

## Configure a Windows Hello Profile (Windows Phone)

Microsoft Passport provides a secure alternative to using passwords for security. The Windows Hello profile configures Microsoft Passport for your Windows 10 Mobile devices so end users can access your data without sending a password.

Create a Windows Hello profile to configure Microsoft Passport for your Windows Phone devices so end users can access your organization's applications, websites, and networks without entering a password.

**Procedure**

1    Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2    Select **Windows** and then select **Windows Phone**.

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

4    Select the **Windows Hello** profile.

5    Configure the **Passport** settings:

| Settings | Descriptions |
|---|---|
| Biometric Gesture | Enable to allow end users to use the device biometric readers. |
| TPM | Set to **Require** to disable Passport use without a Trusted Protection Module installed on the device. |
| Minimum PIN Length | Enter the minimum number of digits a PIN must contain. |
| Maximum PIN Length | Enter the maximum number of digits a PIN can contain. |
| Digits | Set the permissions level for using digits in the PIN. |
| Upper Case Letters | Set the permissions level for using upper case letters in the PIN. |
| Lower Case Letters | Set the permissions level for using lower case letters in the PIN. |
| Special Characters | Set the permissions level for using special characters (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~) in the PIN. |

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

# Create a Windows Licensing Profile (Windows Phone)

Configure a Windows Licensing profile to provide your Windows 10 devices with a license key. This license key upgrades a consumer device to Windows 10 Mobile Enterprise edition and allows you to use additional functionality.

This upgrade process cannot be revered. Use caution before pushing this profile to employee-owned devices.

**Prerequisites**

For Windows 10 Mobile devices, you must acquire a valid XML License file from the Microsoft Volume Licensing Service Center.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and then select **Windows Phone**.

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

4   Select the **Windows Licensing** profile.

5   Select **Upload** to select a valid XML license file.

   Acquire this file from the Microsoft Volume Licensing Service Center.

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

   To check if the licensing upgrade was successful, navigate on the phone to **Settings > System > About** and check under **Device Information** for **Software: Windows 10 Mobile Enterprise**.

# Data Protection Profile (Windows Phone)

The Data Protection profile configures rules to control how enterprise applications access data from multiple sources in your organization. Using Data Protection ensures that your data is only accessible by secured, approved applications.

**Important**   Data Protection is currently a tech preview feature. Consider limiting your use of this feature for testing purposes only. Data Protection should not be used in a production environment. Features are not final and are subject to change at any time.

With personal and work data on the same device, accidental data disclosure is possible through services that your organization does not control. With the Data Protection payload, AirWatch controls how your enterprise data moves between applications to limit leakage with a minimal impact on end users. AirWatch uses the Microsoft Windows Information Protection (WIP) feature to protect your Windows 10 Mobile devices.

Data Protection works by whitelisting enterprise applications to give them permission to access enterprise data from protected networks. If end users move data to non-enterprise applications, you can act based on the selected enforcement policies.

WIP treats data as either unencrypted personal data or corporate data to protect and encrypt. Applications whitelisted for Data Protection fall into four different types. These types determine how the app interacts with protected data.

- Enlightened Apps – These apps fully support WIP functionality. Enlightened apps can access both personal and corporate data without issues. If data is created with an enlightened app, you can save the data as unencrypted personal data or encrypted corporate data. You can restrict users from saving personal data with enlightened apps using the Data Protection profile.

- Allowed – These apps support WIP-encrypted data. Allowed apps can access both corporate and personal data but the apps save any accessed data as encrypted corporate data. Allowed apps save personal data as encrypted corporate data that cannot be accessed outside of WIP-approved apps. Consider slowly whitelisting allowed apps on a case-by-case basis to prevent issues accessing data. Reach out to software providers for information on WIP approval.

- Exempt – You determine which apps are exempt from WIP policy enforcement when you create the Data Protection profile. Exempt any apps that do not support WIP-encrypted data. If an app does not support WIP-encryption, the apps break when attempting to access encrypted corporate data. No WIP policies apply to exempt apps. Exempt apps can access unencrypted personal data and encrypted corporate data. Because exempt apps access corporate data without WIP policy enforcement, use caution when whitelisting exempt apps. Exempt apps create gaps in data protection and leak corporate data.

- Not Allowed – These apps are not whitelisted or exempted from WIP policies and cannot access encrypted corporate data. Not allowed apps can still access personal data on a WIP-protected device.

**Important**   The Data Protection profile requires Windows Information Protection (WIP). This feature requires the Windows Anniversary Update. Consider testing this profile before deploying to production.

## Configure a Data Protection Profile (Windows Phone)

Create the Data Protection (Preview) profile to use the Microsoft Windows Information Protection feature to limit user and application access to your organizational data to approved networks and applications. You can set detailed controls over data protection.

Data Protection is currently a tech preview feature. AirWatch recommends limiting your use of this feature for testing purposes only. Data Protection should not be used in a production environment. Features are not final and are subject to change at any time.

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and choose **Windows Phone** as the platform.

**3**    Select **Device Profile**.

**4**    Configure the profile **General** settings.

**5**    Select the **Data Protection** payload.

**6**    Configure the Enterprise Data Protection settings:

| Settings | Descriptions |
|---|---|
| **Add** | Select to add enterprise applications to the enterprise allowed list. |
| | Applications added here are trusted to use enterprise data. |
| **App Type** | Select either Store App or Store App Publisher. |
| | Selecting a publisher whitelists all apps from the publisher. |
| **Name** | Enter the app name. If the app is a Microsoft Store app, select the Search icon (🔍) to search for the app Package Family Name (PFN). |
| **Identifier** | Enter the package family name for the store app or the app publisher name. |
| **Exempt** | Select the check box if the app does not support full data protection but still needs access to enterprise data. Enabling this option exempts the app from data protection restrictions. These apps are often legacy apps not yet updated for data protection support. |
| | Creating exemptions creates gaps in data protection. Only create exemptions when necessary. |
| **Primary Domain** | Enter the primary domain that your enterprise data uses. |
| | Data from protected networks is accessible by enterprise applications only. Attempting to access a protected network from an application not on the enterprise allowed list results in enforcement policy action. |
| | Enter domains in lowercase characters only. |
| **Enterprise Protected Domain Names** | Enter a list of domains (other than your primary domain) used by the enterprise for its user identities. Separate the domains with the vertical bar character (\|). |
| | Enter domains in lowercase characters only. |
| **Enterprise IP Ranges** | Enter the enterprise IP ranges that define the Windows 10 devices in the enterprise network. |
| | Data that comes from the devices in range are considered part of the enterprise and are protected. These locations are considered a safe destination for enterprise data sharing. |
| **Enterprise Network Domain Names** | Enter the list of domains that are the boundaries of the enterprise network. |
| | Data from a listed domain that is sent to a device is considered enterprise data and is protected. These locations are considered a safe destination for enterprise data sharing. |
| **Enterprise Proxy Servers** | Enter the list of proxy server that the enterprise can use for corporate resources. |

| Settings | Descriptions |
| --- | --- |
| Enterprise Cloud Resources | Enter the list of enterprise resource domains hosted in the cloud that need to be protected by routing through the enterprise network through a proxy server (on port 80). |
| | If Windows cannot determine whether to allow an app to connect to a network resource, it will automatically block the connection. If you want Windows to default to allow the connections, add the `/*AppCompat*/` string to the setting. For example: |
| | `www.air-watch.com | /*AppCompat*/` |
| | Only add the `/*AppCompat*/` string once to change the default setting. |
| Application Data Protection Level | Set the level of protection and the actions taken to protect enterprise data. |
| Show EDP Icons | Enable to display an EDP icon( ) in the Web browser, file explorer, and app icons when accessing protected data. The icon also displays in enterprise-only app tiles on the Start menu. |
| Revoke on Unenroll | Enable to revoke Data Protection keys from a device when the device unenrolls from AirWatch. |
| Protection Under Lock | Enable to cryptographically protect enterprise data while the device is locked. |
| User Decryption | Enable to allow users to select how data is saved using an enlightened app. They can select **Save as Corporate** or **Save as Personal**. |
| | If this option is not enabled, all data saved using an enlightened app will save as corporate data and encrypt using the corporate encryption. |
| Direct Memory Access | Enable to allow users direct access to device memory. |
| Data Recovery Certificate | Upload the special Encrypting File System certificate to use for file recovery if your encryption key is lost or damaged. For more information, see Create an Encrypting File System Certificate (Windows Phone). |

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

# Create an Encrypting File System Certificate (Windows Phone)

The Data Protection profile encrypts enterprise data and restricts access to approved devices. Create an EFS certificate to encrypt your enterprise data protected by a Data Protection profile.

**Procedure**

1   On a computer without an EFS certificate, open a command prompt (with admin rights) and navigate to the certificate store you where you want to store the certificate.

**2**   Run the command:

cipher /r:<EFSRA>

The value of <EFSRA> is the name of the .cer and .pfx files that you want to create.

**3**   When prompted, enter the password to help protect your new .pfx file.

**4**   The .cer and .pfx files are created in the certificate store you selected.

**5**   Upload your .cer certificate to devices as part of a Data Protection profile. For more information, see Configure a Data Protection Profile (Windows Phone).

# Create Custom Settings Profile (Windows Phone)

The **Custom Settings** payload provides a way to use Windows Phone functionality that AirWatch does not currently support through its native payloads. If you want to use the new features, you can use the **Custom Settings** payload and XML code to manually enable or disable certain settings.

**Procedure**

**1**   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

**2**   Select **Windows** and then select **Windows Phone**.

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

**4**   Configure the applicable payload (for example, Restrictions or Passcode).

You can work on a copy of your profile, saved under a "test" organization group, to avoid affecting other users before you are ready to Save and Publish.

**5**   **Save**, but do not publish, your profile.

**6**   Select **View XML** from the actions menu in the **Profiles List View** for the row of the profile you want to customize.
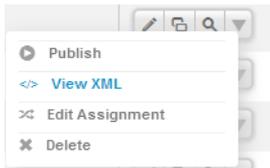


**7**   Find the section of text starting with <characteristic> ... <characteristic> that you configured previously, for example, Restrictions or Passcode. The section contains a configuration type identifying its purpose, for example, restrictions.

**8**   Copy this section of text and close the XML View. Open your profile.

**9**   Select the **Custom Settings** payload and select **Configure**. Paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from <characteristic> to <characteristic>.

**10** Remove the original payload you configured by selecting the base payload section and selecting the minus [-] button. You can now enhance the profile by adding custom XML code for the new functionality.

Any device not upgraded to the latest version ignores the enhancements you create. Since the code is now custom, you should test the profile devices with older versions to verify expected behavior.

**11** Select **Save & Publish**.

# Compliance Policies

<span style="color: gray; font-size: 3em; float: right;">4</span>

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

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

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

For more information about compliance policies, including which policies and actions are supported for a particular platform, see the **Managing Devices** documentation on docs.vmware.com.

## Configure Health Attestation for Windows Phone Compliance Policies

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

Compromised status compliance policy is applicable to Windows 10 Mobile devices with a Trusted Platform Module (TPM) 1.2 or higher.

**Procedure**

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

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

**3** Configure the Health Attestation settings:

| Settings | Descriptions |
|---|---|
| **Compromised Status Definition** | |
| **Use Custom Server** | Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the **Server URL** field. |
| **Server URL** | Enter the URL for your custom Health Attestation server. |
| **Secure Boot Disabled** | Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files. |
| **Attestation Identity Key (AIK) Not Present** | Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate. |
| **Data Execution Prevention (DEP) Policy Disabled** | Enable to flag compromised device status when the DEP is disabled on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. DEP is enforced by both hardware and software. |
| **BitLocker Disabled** | Enable to flag compromised device status when BitLocker encryption is disabled on the device. |
| **Code Integrity Check Disabled** | Enable to flag compromised device status when the code integrity check is disabled on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software. |
| **Early Launch Anti-Malware Disabled** | Enable to flag compromised device status when the early launch anti-malware is disabled on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize. |
| **Code Integrity Version Check** | Enable to flag compromised device status when the code integrity version check fails. |
| **Boot Manager Version Check** | Enable to flag compromised device status when the boot manager version check fails. |
| Boot App Security Version Number Check | Enable to flag compromised device status when the boot app security version number does not meet the entered number. |
| Boot Manager Security Version Number Check | Enable to flag compromised device status when the boot manager security version number does not meet the entered number. |
| **Advanced Settings** | Enable to configure advance settings in the Software Version Identifiers section. |
| Software Version Identifiers | |
| **Code Integrity Policy Hash Check** | Enable to define a whitelist of known, valid hash values for the **Code Integrity** software. If the hash is not a whitelisted value, health attestation compliance fails. |

| Settings | Descriptions |
|---|---|
| **Secure Boot Config Policy Hash Check** | Enable to define a whitelist of known, valid hash values for the **Secure Boot Config** software. If the hash is not a whitelisted value, health attestation compliance fails. |
| **PCR0 Check** | Enable to define a whitelist of known, valid measurements for the **PRC0 Check** software. This measurement checks the BIOS trusted code to ensure that it has not been compromised. If the measurement is not a whitelisted value, health attestation compliance fails. |

## What to do next

For more information, see the Microsoft TechNet article on Health Attestation.

# AirWatch Applications for Windows Phone

<span style="float:right; font-size:4em; color:#bbb;">5</span>

You can use AirWatch applications in addition to AirWatch MDM features to further secure devices and configure them with added functionality.

Use the VMware Content Locker to safeguard corporate content on mobile devices and deploy the VMware Browser to enable secure Web browsing for your end users. Download the Workspace ONE Intelligent Hub for Windows to monitor your devices on a more granular level.

For more information about deploying public, internal, and purchased applications, including an App Catalog, see the comprehensive **AirWatch Mobile Application Management Guide**.

This chapter includes the following topics:

- Configure the Workspace ONE Intelligent Hub (Windows Phone)

- Application-Level Single Sign On Passcodes

- VMware Content Locker for Windows Phone

- VMware Browser for Windows Phone

## Configure the Workspace ONE Intelligent Hub (Windows Phone)

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

**Procedure**

**1**   In the AirWatch Console, select the applicable **Organization Group** to apply settings to.

**2**   Navigate to **Groups & Settings > All Settings > Device & Users > Windows > Windows Phone > Hub Settings**.

**3** Enable the following options in the **Hub Settings** section:

| Setting | Description |
|---|---|
| Heartbeat Interval (min) | Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking in with the UEM console. |
| Data Sample Interval (min) | Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device. |
| Profile Refresh Interval (min) | Set the frequency (in minutes) the profile list of each device refreshes on the server. |
| Enable Passcode | Enable the use of a passcode to access the Workspace ONE Intelligent Hub settings on the device. |
| Administrative Passcode | Enter the administrative passcode to enter for access to Hub settings on the device. |
| Collect Location Data | Enable to collect the location data from the device. The location is determined based on the Wi-Fi network of the device. When located data is available, the Workspace ONE Intelligent Hub sends the location data to the console at the Transmit Interval. |
| GPS Sample Interval (min) | Set the time (in minutes) the Workspace ONE Intelligent Hub waits before collecting GPS data from the device. |
| Enable Push Notification Services | Enable to allow the console to send Push Notifications to devices. |

# Application-Level Single Sign On Passcodes

Single sign on (SSO) allows end users to access Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps without entering credentials for each application. Using the Workspace ONE Intelligent Hub or the AirWatch Container as a "broker application," end users authenticate once per session using their normal credentials or an SSO Passcode.

Enable SSO as part of the **Security Policies** that you configure to apply to all Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile.

**Procedure**

**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 Workspace ONE UEM applications and maintain a persistent login.

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

Once an end user authenticates with an application participating in SSO, a session establishes. The session is active until the **Authentication Timeout** defined in the SDK profile is reached.

# VMware Content Locker for Windows Phone

VMware Content Locker is an application that enables your end users to access important content on their devices while ensuring file safety for your organization.

From the VMware Content Locker, end users can access content you upload in the UEM console, content from synced corporate repositories, or their own personal content.

Use the UEM console to add content, sync repositories and configure the actions that end users can take on content opened within the application. These configurations prevent content from being copied, shared, or saved without approval.

# VMware Browser for Windows Phone

VMware Browser is an application that provides a manageable and secure alternative to native Web browsers. You can secure the browsing experience on an application, tunnel, and Web site level.

You can configure the VMware Browser to meet unique business needs by restricting Web access to Web sites and providing a secure Internet portal for mobile point-of-sale devices. Provide users with a standard browsing experience, including support of multi-tabbed browsing and JavaScript dialog box.

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

# Windows Phone Device Management Overview

<span style="font-size:3em; color:#999;">6</span>

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

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

This chapter includes the following topics:

- Device Dashboard

- Device List View

- Windows Phone Device Details

## Device Dashboard

As devices are enrolled, you can manage them from the Workspace ONE UEM **Device Dashboard**.

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

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

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

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.

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

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

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

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

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

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

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

# Device List View

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

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

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

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

## Customize Device List View Layout

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

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

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

## Search in Device List View

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

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

# Windows Phone Device Details

Use the Device Details page to track detailed device information and quickly access user and device management actions.

You can access Device Details by selecting a device Friendly Name from the Device List View, using one of the Dashboards, or with any of the search tools.

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

## Remote Actions

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

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

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.

- **Change Device Passcode** – Replace any existing device passcode used to access the selected device with a new passcode.

- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.

- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as **Delete In Progress** on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the console.

- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.

- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.

- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.

- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.

    - Enterprise Wipe is not supported for cloud domain-joined devices.

- **Find Device** – Send a text message to the applicable Workspace ONE UEM application together with an audible sound (with options to repeat the sound a configurable number of times and the length of the gap, in seconds, between sounds). This audible sound should help the user locate a misplaced device.

- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.

- **Rename Device** – Change the device friendly name within the UEM console.

- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.

- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.