

Windows 7 Device Management

VMware Workspace ONE UEM 1907



vmware®

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	Introduction to Windows 7	5
	Windows 7 Requirements	5
2	Windows 7 Enrollment Overview	7
	Windows Desktop and Windows 7 Devices	8
	Workspace ONE Intelligent Hub for Windows Enrollment	8
	Enroll Windows 7 Devices with the Workspace ONE Intelligent Hub	9
	Install the Workspace ONE Intelligent Hub on a Base Operating System Image	10
	Enroll Windows 7 Devices Through a Proxy	10
	Windows 7 Silent Enrollment	11
	Enroll Windows 7 Devices Silently	12
	Silent Enrollment Parameters and Values	12
3	Windows 7 Profiles Overview	15
	Configure a Wi-Fi Profile (Windows 7)	16
	Enforce a VPN Profile (Windows 7)	17
	Credentials Profile (Windows 7)	17
	Create a Credentials Profile (Windows 7)	18
	Configure a Shortcuts Profile (Windows 7)	19
	Create an Exchange Web Services Profile (Windows 7)	19
	Encryption Profile (Windows 7)	20
	Configure an Encryption Profile (Windows 7)	21
	Configure a Passcode Profile (Windows 7)	22
	Configure an Automatic Updates Profile (Windows 7)	23
	Configure a Firewall Profile (Windows 7)	24
4	Compliance Policies	26
5	Windows 7 Application Overview	27
	Configure the Workspace ONE Intelligent Hub for Windows 7	27
	Workspace ONE Intelligent Hub for Windows Upgrades	28
	VMware Content Locker for Windows 7	29
6	Product Provisioning Overview	30
7	Windows 7 Device Management	31
	Device Dashboard	31
	Device List View	32

Device Details Page, Win7	33
Advanced Remote Management	34

Introduction to Windows 7

Workspace ONE UEM powered by AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Windows 7 device deployment. Use Workspace ONE UEM to ensure that your device fleet remains secured.

Through the Workspace ONE UEM 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. Workspace ONE UEM provides complete management solutions for enterprise-managed Windows laptop devices running Windows 7, 8, and 10.

Workspace ONE UEM allows you to enroll both corporate and employee-owned devices to configure and secure your enterprise data and content. By using of our device profiles, you can properly configure and secure your Windows devices.

This chapter includes the following topics:

- [Windows 7 Requirements](#)

Windows 7 Requirements

Before reading this guide, gather and prepare the requirements Workspace ONE UEM requires for Windows 7 devices.

Platforms Supported

Windows 7 interchangeably refers to the following supported Windows Operating Systems.

Microsoft Windows	
Operating System	
32-bit	Windows 7, Windows 8, or Windows 10
64-bit	Windows 7, Windows 8, or Windows 10

Silent Enrollment Agent Requirements

Win32Agent_installer.exe file version 3.8.2 to 6.0.4 or AirwatchAgent.msi version 7.0.0 or later must be downloaded or accessible to the Windows device.

Encryption

- **Supported OS:** Windows 7 Enterprise and Ultimate, 32-bit or 64-bit with .NET 4.5 framework.

- **Levels of Encryption:** System partition and complete hard disk.
- **Default Encryption Type:** BitLocker native encryption.

Enrollment Requirements for All Windows 7 Devices

- **Enrollment URL** – The web address entered into the Internet browser to begin the enrollment procedure. This location is specific to your company's enrollment environment.
- **Group ID** – The unique identifier specific to the organization group within the environment which defines all configurations that devices receive.
- **Credentials** – The username and password used to authenticate the end-user's account and to access the Workspace ONE UEM environment. These credentials can be identical to the end-user's directory services credentials or specific to Workspace ONE UEM.
- **Local Administrator Privileges** – End users must have Admin Rights or be part of the Administrator Group to properly run the Workspace ONE Intelligent Hub EXE on their device.

Workspace ONE Intelligent Hub Prerequisites

Before using the Workspace ONE Intelligent Hub for Windows 7, you must download the following:

- Microsoft Visual C++ 2015 Redistributable (x86)
- Microsoft Visual C++ 2015 Redistributable (x64)

If you do not have .NET 4.5 or above installed before beginning the device enrollment process, the Workspace ONE Intelligent Hub prompts you to install it before continuing enrollment.

Windows 7 Enrollment Overview

2

Device enrollment establishes the initial communication with Workspace ONE UEM to enable Mobile Device Management (MDM). Windows 7 requires the Workspace ONE Intelligent Hub for Windows devices to enroll.

Enrollment Basics

Windows 7 must begin communicating with Workspace ONE UEM to access internal content and features. This communication uses the Workspace ONE Intelligent Hub. The Workspace ONE Intelligent Hub provides a single resource to enroll a device and provides device details.

The Windows 7 enrollment methods all use the Workspace ONE Intelligent Hub to complete enrollment. End users enroll using the Workspace ONE Intelligent Hub enrollment flow. You can also enroll devices using the silent enrollment or device imaging enrollment.

The Windows 7 platform supports Windows 7, Windows 8.1, and Windows 10 devices. The functionality changes when enrolling devices as Windows 7 devices. For more information, see [Windows Desktop and Windows 7 Devices](#).

Workspace ONE Intelligent Hub 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 www.awagent.com and follow the prompts to enroll. For more information on Agent-based enrollment, see [Workspace ONE Intelligent Hub for Windows Enrollment](#).

If you use a proxy server, you must configure the Workspace ONE Intelligent Hub proxy settings. For more information, see [Enroll Windows 7 Devices Through a Proxy](#).

Silent Enrollment

You can bypass end-user interaction and simplify enrollment using the silent enrollment work flow. This enrollment method uses BAT files and command-line entries to download and configure the Workspace ONE Intelligent Hub and complete enrollment. For more information, see [Windows 7 Silent Enrollment](#).

Device Imaging Enrollment

If you are imaging Windows 7 devices, you can download and configure the Workspace ONE Intelligent Hub onto the base operating system image. With this enrollment method, you can ship devices to end users with the Workspace ONE Intelligent Hub preinstalled, only requiring the end users to enter their user credentials. For more information, see [Install the Workspace ONE Intelligent Hub on a Base Operating System Image](#).

This chapter includes the following topics:

- [Windows Desktop and Windows 7 Devices](#)
- [Workspace ONE Intelligent Hub for Windows Enrollment](#)
- [Install the Workspace ONE Intelligent Hub on a Base Operating System Image](#)
- [Enroll Windows 7 Devices Through a Proxy](#)
- [Windows 7 Silent Enrollment](#)

Windows Desktop and Windows 7 Devices

You can enroll your Windows devices into one of two platforms. The platform determines the available device management functionality for your Windows devices.

The Windows Desktop platform supports Windows 8.1 and Windows 10 devices using the native MDM enrollment. The Windows 7 platform supports Windows 7, Windows 8, and Windows 10 devices enrolled using the Workspace ONE Intelligent Hub for Windows.

The table shows the differences in enrollment methods. Consider enrolling Windows 8 and Windows 10 devices as Windows Desktop devices because of the increased device management functionality.

Functionality	Windows 7	Windows Desktop
Native MDM Enrollment Method		✓
Workspace ONE Intelligent Hub Enrollment	✓	✓
AirWatch Protection Agent Support	✓	✓
Supports Full Windows 10 functionality		✓
Supports SCCM Managed Devices	✓	✓
Supports Windows 7 Devices	✓	

Workspace ONE Intelligent Hub for Windows Enrollment

The Workspace ONE Intelligent Hub, available through the Windows Store, provides a single resource for enrollment and facilitates communication between the device and the Workspace ONE Intelligent Hub Console. Use the Workspace ONE Intelligent Hub to simplify enrollment and enable full MDM functionality.

Consider using the Workspace ONE Intelligent Hub for Windows to enroll your Windows 7 devices as the Workspace ONE Intelligent Hub provides the simplest enrollment flow for users. You may also consider awagent.com to start enrollment.

The same Workspace ONE Intelligent Hub works for both Windows Desktop and Windows 7 devices. When the Workspace ONE Intelligent Hub installer runs on a device, the Workspace ONE Intelligent Hub checks the enrollment status of the device. If the device is enrolled through Windows Desktop, the Workspace ONE Intelligent Hub acts as the AirWatch Protection Agent and installs onto the device. If the device is not enrolled, the Workspace ONE Intelligent Hub begins the enrollment process to enroll the device as a Windows 7 device.

Note If the enrollment process is interrupted, launching the Workspace ONE Intelligent Hub again automatically re-initiates the enrollment process. To relaunch the Workspace ONE Intelligent Hub, double-click the icon.

Enroll Windows 7 Devices with the Workspace ONE Intelligent Hub

Use the Workspace ONE Intelligent Hub to start enrollment of your Windows Desktop devices. The Workspace ONE Intelligent Hub provides a simplified enrollment flow for end users that is quick and easy to follow.

Procedure


- 1 Navigate to www.awagent.com. The Workspace ONE Intelligent Hub Installer begins downloading.
- 2 Start the installer once the download completes.
- 3 Select **Run** to begin the installation.
- 4 Select **Email** if you have AirWatch Auto-Discovery enabled, otherwise select **Server Detail**.
- 5 Complete the settings required based on the authentication type selected.
 - a Enter the email address to auto-fill the server details screen. Select **Next** and the details are entered.
 - b Enter the Server Name and Group ID if you are not using AirWatch Auto-Discovery to complete the settings. Select **Next**.
- 6 Enter the **Username** and **Password** and select **Next** (Windows 7 images only).
- 7 Complete any optional screens.
- 8 Select **Finish** to complete the enrollment.

Once completed, Workspace ONE UEM pushes profiles and products to the device.

Install the Workspace ONE Intelligent Hub on a Base Operating System Image

Download the Workspace ONE Intelligent Hub onto a device and configure the Workspace ONE Intelligent Hub for use on a base operating system image for deployment. This enrollment flow allows you to ship devices to users with the Workspace ONE Intelligent Hub preinstalled, only requiring end users to enter their user credentials.

Procedure

- 1 Navigate to awagent.com. The agent downloads immediately.
- 2 Run the Workspace ONE Intelligent Hub installer (`AirWatchAgent.msi`) and, if prompted, accept any security warnings.
- 3 Click **Run** to begin the Workspace ONE Intelligent Hub installation wizard.
- 4 After installation and the Workspace ONE Intelligent Hub starts, select the Settings icon ()
- 5 Select the operating system the image uses.

If you are enrolling a Windows 8.1 or Windows 10 device using the Workspace ONE Intelligent Hub for Windows, you must select **This is for Windows 7 Image**. If you select **This is for Windows 8.1/10**, the device must be enrolled using MDM enrollment.

- 6 Enter the **Server URL** and **Group ID**.
- 7 Select **Save**.

The Workspace ONE Intelligent Hub is now installed into the system image and starts on any imaged device so end users can enter their credentials.

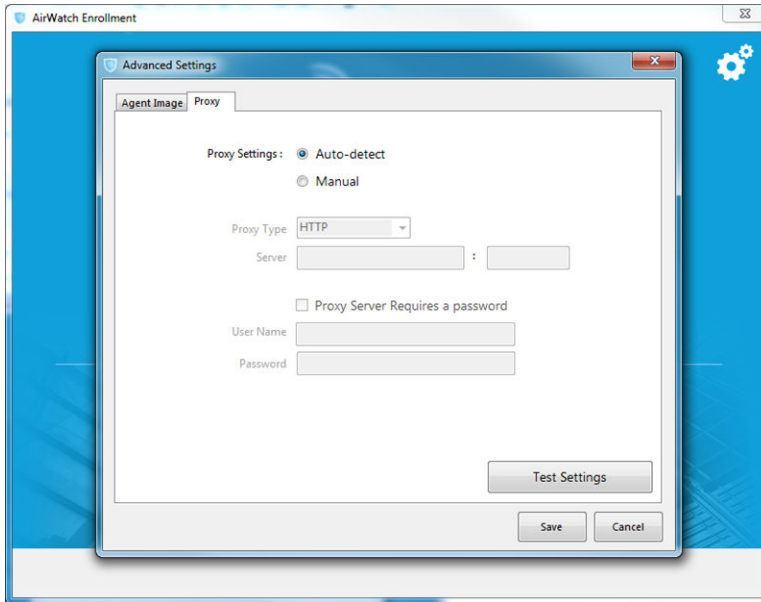
Enroll Windows 7 Devices Through a Proxy

A Windows 7 might be behind a proxy server that may prevent you from enrolling devices. If you use a proxy server, configure the proxy settings for the Workspace ONE Intelligent Hub.

Procedure

- 1 Start the Workspace ONE Intelligent Hub.

- 2 Select the **Settings** icon ().



- 3 Select the appropriate **Proxy Settings**.

Settings	Descriptions
Auto-detect	Select to have the Workspace ONE Intelligent Hub automatically detect the proxy settings configured on the device browser and use those settings for communication with the Workspace ONE UEM Console.
Manual	Select to configure the proxy settings manually for the Workspace ONE Intelligent Hub.
Proxy Type	Displays HTTP as the proxy type.
Server	Enter the proxy server URL and port number.
Proxy Server Requires a Password	Enable to enter the Username and Password for the proxy server.

- 4 Select **Save** to apply the Proxy Settings.
- a Use **Test Settings** before saving and applying the proxy settings.
- 5 Select **Finish** to apply the settings and close the Workspace ONE Intelligent Hub.

Windows 7 Silent Enrollment

You can silently download the Workspace ONE Intelligent Hub onto devices using BAT files and command-line entries. This enrollment method bypasses end-users interactions and simplifies enrollment.

Running a command-line installation eliminates all InstallShield prompts so the admin does not need to select acknowledgment buttons continuously. This installation method reduces the time it takes to install the Workspace ONE Intelligent Hub and simplifies the process.

Installation of Workspace ONE Intelligent Hub using silent enrollment assumes that the user accepts the EULA by default since all acknowledgment screens are automatically bypassed. The EULA is automatically accepted and not displayed.

Silent enrollment supports the following use cases:

- On a base OS image without enrolling the device.
- On a PC using command line switches to complete silent enrollment.

Important Devices behind a proxy cannot be enrolled through Silent Enrollment.

Enroll Windows 7 Devices Silently

Download and install the Workspace ONE Intelligent Hub onto a device without requiring end-user interaction. This enrollment flow allows you to bypass end users and enroll devices quickly and easily.

Note If you are storing the Workspace ONE Intelligent Hub on a network drive for later use, ensure that you are downloading the latest version of the Workspace ONE Intelligent Hub from awagent.com.

Procedure

- 1 Navigate to awagent.com to download the Workspace ONE Intelligent Hub.

Only download the Workspace ONE Intelligent Hub. Do not start the executable or select **Run** as that initiates a standard enrollment process and defeats the purpose of silent enrollment.

If necessary, move the Workspace ONE Intelligent Hub from the download folder to a local or network drive folder.

- 2 Open a command line or create a BAT file and enter all the necessary paths, parameters, and values using information shown in [Silent Enrollment Parameters and Values](#).

- 3 Run the command.

For examples of typical syntax, see [Silent Enrollment Parameters and Values](#).

The Workspace ONE Intelligent Hub is installed on the Windows device without requesting you to select any acknowledgment buttons.

Silent Enrollment Parameters and Values

Silent enrollment requires command-line entries or a BAT file to control how the Workspace ONE Intelligent Hub downloads and installs onto the device.

The following table lists all the possible enrollment parameters you can enter into a command line or into a BAT file, and the respective values for each parameter.

Enrollment Parameters	Values to Add to Parameter
/ENROLL	Select 'Y' to enroll. Select 'N' for image only.
/IMAGE	Select 'Y' for image. Select 'N' for enrollment.
/SERVER	Enter the enrollment URL.
/LGName	Enter organization group name.
/USERNAME	Enter the user name for the user being enrolled or the staging user name if staging the device on the behalf of a user.
/PASSWORD	Enter the password for the user being enrolled or the staging user password if staging the device on the behalf of a user.
ASSIGNTOLOGGEDINUSER	Select 'Y' to assign the device to the logged in domain user.
/STAGEUSERNAME	Enter user name for the enrolling user.
/SECURITYTYPE	Needed if user account is added to Workspace ONE UEM console during enrollment process: <ul style="list-style-type: none"> ■ Select 'D' for Directory. ■ Select 'B' for Basic User type.
/STAGEEMAILUSRNAME*	Enter the email user name for the user being enrolled.
/STAGEPASSWORD	Enter the password for the user being enrolled.
/STAGEEMAIL*	Enter the email address for the user being enrolled.
/DEVICEOWNERSHIPTYPE*	Select 'CD' for Corporate Dedicated. Select 'CS' for Corporate Shared. Select 'EO' for Employee Owned. Select 'N' for None.
/INSTALLDIR*	Enter the directory path if you want to change installation path. Note If this parameter is not present, the Workspace ONE Intelligent Hub uses the default path: C:\Program Files (x86)\AirWatch.

Items denoted with an asterisk (*) are optional.

Examples of Silent Enrollment

Below are examples of various use cases using enrollment parameters and the values that you can enter into a command line or use to create a BAT file. Initiating any one of these examples silently enrolls the Windows device without prompting the user to select any of the acknowledgment buttons.

Agent Install for Image Only Without Enrollment

The following is an example of installing the Workspace ONE Intelligent Hub for image only without enrollment using minimum parameters required for image only.

```
AirwatchAgent.msi /quiet ENROLL=N IMAGE=Y
```

Basic User Enrollment

The following is an example of using minimum parameters required for basic enrollment only:

```
AirwatchAgent.msi /quiet ENROLL=Y IMAGE=n SERVER=companyURL.com LGName=locationgroupid
USERNAME=TestUsr PASSWORD=test
```

Workspace ONE Intelligent Hub Installed Elsewhere

The following is an example of the AirwatchAgent.msi located in a different location:

```
C:\AirwatchAgent.msi /quiet ENROLL=Y IMAGE=n SERVER=companyURL.com
LGName=locationgroupid USERNAME=TestUsr PASSWORD=test
```

Installation Directory and Workspace ONE Intelligent Hub on Network Drive

The following is an example of the installation directory parameter with the Workspace ONE Intelligent Hub on a network drive.

Important Add extra quotes for the INSTALLDIR parameter when there is space within the parameter.

```
Q:\AirwatchAgent.msi /quiet INSTALLDIR="E:\Install Win32\" ENROLL=Y IMAGE=n
SERVER=companyURL.com LGName=locationgroupid USERNAME=TestUsr PASSWORD=test
```

All Available Parameters and Values

The following is an example of the syntax using all available parameters and values shown in the previous table.

```
<AirwatchAgent.msi>/quiet INSTALLDIR="<Directory Path>" ENROLL=<Y/N>IMAGE=<Y/
N>SERVER=<CompanyURL>LGNAME=<Location Group
ID>USERNAME=<Username>PASSWORD=<Username Password>STAGEUSERNAME=<Stager
Username>SECURITYTYPE=<D/B>STAGEEMAILUSRNAME=<User
Enrolling>STAGEPASSWORD=<Password for User Enrolling>STAGEEMAIL=<Email Address for User
Enrolling>DEVICEOWNERSHIPTYPE<CD/CS/EO/N>ASSIGNTOLOGGEDINUSER=<Y/N>
```

Windows 7 Profiles Overview

Profiles are the primary means to manage devices. Configure profiles so your Windows 7 devices remain secure and configured to your settings.

Overview

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

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

Device Security

Ensure that your Windows 7 devices remain secure through device profiles. These profiles configure the native Windows security features or configure corporate security settings on a device through Workspace ONE UEM.

Some examples of device security profiles include:

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see [Configure a Wi-Fi Profile \(Windows 7\)](#).
- Ensure access to internal resources for your devices with the VPN profile. For more information, see [Enforce a VPN Profile \(Windows 7\)](#).
- Secure a device with a Passcode profile. For more information, see [Configure a Passcode Profile \(Windows 7\)](#).

Device Configuration

Configure the various settings of your Windows 7 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 [Create an Exchange Web Services Profile \(Windows 7\)](#).

- Ensure that the devices remain up to date with the Windows Updates profile. For more information, see [Configure an Automatic Updates Profile \(Windows 7\)](#).
- Keep your data secure with the Encryption profile. For more information, see [Encryption Profile \(Windows 7\)](#).

This chapter includes the following topics:

- [Configure a Wi-Fi Profile \(Windows 7\)](#)
- [Enforce a VPN Profile \(Windows 7\)](#)
- [Credentials Profile \(Windows 7\)](#)
- [Configure a Shortcuts Profile \(Windows 7\)](#)
- [Create an Exchange Web Services Profile \(Windows 7\)](#)
- [Encryption Profile \(Windows 7\)](#)
- [Configure a Passcode Profile \(Windows 7\)](#)
- [Configure an Automatic Updates Profile \(Windows 7\)](#)
- [Configure a Firewall Profile \(Windows 7\)](#)

Configure a Wi-Fi Profile (Windows 7)

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 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Wi-Fi** profile.
- 5 Configure the Wi-Fi settings.

Settings	Descriptions
Wi-Fi Network Name	Enter the name (SSID) of the desired Wi-Fi network.
Connection Type	Use the drop-down menu to select the Wi-Fi connection type as Ad Hoc or Infrastructure .
Connection Mode	Use the drop-down menu to specify automatic or manual joining of the network.
Security Type	Use the drop-down menu to select the security type for the Wi-Fi network.
Encryption	Use the drop-down menu to select the encryption method for the connection. Choosing WPA or WPA2 Enterprise adds the Authentication section that must be completed.

Settings	Descriptions
Password	Enter the password required to join the Wi-Fi network. Select Show Characters to disable hidden characters within the text box.
Authentication	If needed, choose the Root Certificate and enable AD authentication. Displays only if Security Type is set to WPA Enterprise or WPA2 Enterprise .
Enable AD Authentication	Select to use user AD credentials to authenticate instead of using a certificate. Displays only if Security Type is set to WPA Enterprise or WPA2 Enterprise .
Root Certificate	Select the certificate used to authenticate.

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

Enforce a VPN Profile (Windows 7)

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

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **VPN** profile.
- 5 Select **Enable VPN** to configure the VPN settings.

Settings	Descriptions
Connection Type	Use the drop-down menu to select the network connection method.
Connection Name	Enter the name of the connection.
Server	Enter the hostname or IP address of the server to which to connect.
Username	Enter the user name required for VPN authentication.
Domain	Enter the name of the domain to which the VPN connects.
Password	Enter the password required to join the VPN. Select Show Characters to disable hidden characters within the text box.

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

Credentials Profile (Windows 7)

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 7 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 of these payloads has settings for associating the certificate authority defined in the Credentials payload.

Create a Credentials Profile (Windows 7)

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

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Credentials** profile.
- 5 Configure the Credentials settings.

Settings	Description
Credential Source	Use the drop-down menu to select either Upload or Defined Certificate Authority .
Credential Name	Enter a name for the credentials certificate. Displays if the Credential Source is Upload .
Certificate	Click Upload , navigate to the desired credential certificate file, and then select Save . Displays if the Credential Source is Upload .
Certificate Authority	Use the drop-down menu to select a predefined certificate authority. Displays if the Credential Source is Define Certificate Authority .
Certificate Template	Use the drop-down menu to select a predefined certificate template specific to the selected certificate authority. Displays if the Credential Source is Define Certificate Authority .
Store Location	Use the drop-down menu to choose to save the certificate on the specific User account level or on the Computer Store for all users of a computer.
Certificate Store	Select the certificate store folder location from the drop-down menu. <ul style="list-style-type: none"> ■ Personal (Default) ■ Trusted Root Certification Authorities ■ Intermediate Certificate Authorities ■ Trusted Publishers ■ Untrusted Certificates ■ Trusted People

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

Configure a Shortcuts Profile (Windows 7)

A Shortcuts profile allows you to save URLs for your end users to access. Use the Shortcuts profile when you want to push specific URLs such as an internal website to your end users.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Shortcuts** profile.
- 5 Configure the Shortcuts settings.

Settings	Descriptions
Label	Enter a descriptive name for the shortcut.
URL	Enter the target Web address for the shortcut to use.
Icon	Upload an image to serve as a visual representation for the shortcut on the desktop. The file type must be .ico.

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

Create an Exchange Web Services Profile (Windows 7)

Create an Exchange Web Services profile to allow the end user to access corporate email infrastructures and Microsoft Outlook accounts from the device.

Important During initial configuration, the device must have access to the Internal Exchange Server.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Exchange Web Services** profile.
- 5 Configure the Exchange Web Services settings.

Settings	Descriptions
Domain	Enter the name of the email domain to which the end user belongs.
Email Server	Enter the name of the Exchange server.
Email Address	Enter the address for the email account.

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

Removing an Exchange Web Services profile removes all Outlook accounts from the device.

Encryption Profile (Windows 7)

Secure your organization data on Windows 7 devices using the native BitLocker encryption with the Encryption profile. BitLocker encryption policy is only available on Windows 7 Ultimate and Enterprise, Windows 8 Enterprise and Pro, and Windows 10 Enterprise, Education, and Pro devices.

Because laptops and tablets are mobile devices by design, they risk your organization data being lost or stolen. By enforcing a BitLocker encryption policy through Workspace ONE UEM, you can protect data on the hard drive. BitLocker is the native Windows encryption that Workspace ONE UEM supports. The Encryption profile continually checks the encryption status of the device. If the profile finds that the device is not encrypted, it automatically encrypts the device.

If you decide to encrypt with BitLocker, a recovery created during encryption is stored in the Workspace ONE UEM console.

Note The BitLocker Encryption profile requires the Workspace ONE Intelligent Hub to be installed on the device.

Deploying an Encryption Profile

The Windows native BitLocker encryption secures data on Windows 7. Deploying the encryption profile requires more actions from the end user.

Note For BitLocker encryption to take place, the device must have Trusted Platform Module (TPM) enabled. The exact process to enable and activate TPM may vary from one system to another but is typically done by restarting the device and accessing the BIOS security settings.

Pushing BitLocker Profiles

The BitLocker encryption uses a wizard to enable and activate the encryption on end-user devices. Note the following important points when pushing BitLocker to end users:

- If **Enforce Encryption PIN to Login** is enabled, end users are prompted to create a 4–20 digit PIN that is used every time the machine is restarted.
 - This PIN is required even during restarts required by encrypting and decrypting the drive.
- The end users are prompted to select a local recovery key storage path. The recovery key is saved as a TXT file at the selected path.
- If TPM is not enabled, BitLocker encryption cannot take place. If TPM is enabled but not active, the wizard restarts the device to activate it. This reboot requires the end user to accept the change.

BitLocker and the UEM console

If BitLocker is enabled and in use, you can see encryption status reports in the following areas:

- Workspace ONE UEM Dashboard
 - Device Details displays recovery key information.
 - Encryption progress (percentage) or completion at the time of the device sample displays.
 - BitLocker protection displays as enabled.
- Workspace ONE UEM Self-Service Portal (SSP)
 - Self-Service Portal displays that the recovery key is stored in Workspace ONE UEM, but does not display recovery key details.
 - Encryption progress (percentage) or completion displays.
 - BitLocker protection displays as enabled.

Note During device encryption, the profile may display as **Not Installed** in the Workspace ONE UEM console. Once encryption of the device reaches 100%, the profile displays as installed.

Removal Behavior

If the profile is removed from the UEM console, Workspace ONE UEM no longer enforces the encryption and the end user is free to decrypt. Enterprise wiping or manually uninstalling the Workspace ONE Intelligent Hub from the Control Panel does not turn off BitLocker. The device end user must decrypt from the Control Panel.

If the end user decides to unenroll during the BitLocker encryption process, the encryption process continues unless it is turned off manually from the Control Panel.

Encryption Warnings

Only manage BitLocker encryption with the Encryption profile, or the device may report incorrect information and become unmanageable. Some sample scenarios include:

- If the user decrypts BitLocker from the entire system or any drives using the Control Panel, the device becomes unmanageable as the status may not display correctly. A device is encrypted with BitLocker from the UEM console, it must be decrypted from the UEM console as well.
- Once the user initiates the encryption or decryption process, do not change the TPM settings as it may cause instability and unwanted behavior.

Configure an Encryption Profile (Windows 7)

Create an Encryption profile to secure your data on Windows Desktop devices using the native BitLocker encryption.

Procedure

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

- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Configure the Encryption settings.

Settings	Descriptions
Encrypted Volume	<p>Use the drop-down menu to select the type of encryption as follows:</p> <ul style="list-style-type: none"> ■ System Partition – Encrypts a partition or drive in the same location where Windows is installed and from which it boots. ■ Complete Hard Disk – Encrypts the entire hard disk on the device, including the System Partition where the OS is installed. This option also encrypts any attached drives such as USB drives. <p>Note If any additional devices are included during encryption, you must decrypt the additional drives and the complete hard disk. If you decrypt the hard disk without including the additional drives, you will be unable to decrypt the additional drives.</p>
Enforce Encryption PIN on Login	Select to require users to enter a PIN upon starting the device.

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

Configure a Passcode Profile (Windows 7)

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

Using this profile requires users to reset their device passcode even if the existing passcode is stronger than the minimum requirements.

Prerequisites

To push the Passcode profile to devices, you must first enable it in the Workspace ONE Intelligent Hub Settings. Navigate to **Devices & Users > Windows > Windows 7 > Hub Settings** and select **Enforce Passcode**.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Passcode** profile.

- 5 Select **Require Passcode on device** and configure the Passcode settings.

Settings	Descriptions
Allow Simple Value	Select to allow simple passcodes instead of complex passcodes requiring multiple characters and numbers.
Enforce Passcode History	Enter a value to force end users to select a passcode they have not used before. The value entered (0-24) is the number of passcodes kept in the history that an end user has used before. You cannot use Previous passcodes again until it is no longer kept in the history.
Maximum Passcode Age (days)	Enter the number of days a passcode can be used before it must be changed.
Minimum Passcode Age (days)	Enter the number of days that must pass before an end user may change their passcode. If the value is 0, then Passcode History is not effective.
Minimum Passcode Length	Enter the minimum number of characters a passcode must have.
Account Lockout Duration (mins.)	Enter the number of minutes a device is locked out after entering the passcode incorrectly too many times.
Account Lockout Threshold	Enter the number of passcode attempts allowed before the device is locked out.
Reset Account Lockout Count After (mins.)	Enter the number of minutes that must pass after a failed login attempt before the failed login attempt-counter is reset. This value must be less than or equal to Account Lockout Duration.
Inactivity Period Before Locking Screen (mins.)	Enter the number of minutes of inactivity that must pass before the screen is automatically locked.
Reset Password and Account Lockout Policies upon Enterprise Wipe	Enabled by default Enable to reset password and account lockout policies to simple values with no enforcement after an Enterprise Wipe command is sent to the device.

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

Configure an Automatic Updates Profile (Windows 7)

Create a Windows Updates profile to manage the Windows Updates settings for Windows Desktop devices. The profile ensures that all your devices are up-to-date, which improves device and network security.

Important The Windows Automatic profile only affects non-domain joined Windows 7 devices.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then select **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Automatic Updates** profile.

5 Configure the Windows Automatic Updates settings.

Settings	Descriptions
Windows Update Source	<p>Select the source for Windows Updates:</p> <ul style="list-style-type: none"> ■ Microsoft Default – Select to use the default Microsoft Update Server. ■ Corporate WSUS – Select to use a corporate server and enter the WSUS Server URL and WSUS Group. <p>Note Choosing Corporate WSUS as a source allows your IT Admin to view updates installed and device status of devices in the WSUS Group.</p>
Important Updates	Select the rules to use for Important Updates.
Install Recommended Updates the Same Way as Important Updates	Enable to install Recommended Updates using the same rules Important Updates use.
Update Other Microsoft Products When Updating Windows	Enable to allow other Microsoft Products to update when Windows is updated.

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

Configure a Firewall Profile (Windows 7)

The Firewall profile for Windows Desktop devices allows you to configure the Windows Firewall settings for devices. With devices all having the Windows Firewall configured and enabled, you greatly increase your network security.

The Firewall profile only affects non-domain joined Windows 7 devices.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
- 2 Select **Windows** and then **Windows 7**.
- 3 Configure the profile **General** settings.
- 4 Select the **Firewall** profile.
- 5 Configure the Firewall settings.

Settings	Description
Use Windows Recommended Settings	Enable this setting to use the Windows Recommended Settings and disable all other options available for this profile.
Enable Firewall	Enable to ensure that the firewall is running on devices.
Block all connections to apps that are not on the list of allowed apps	Enable to restrict all access for non-whitelisted apps.
Block all incoming connections including those in the list of allowed apps	Enable to block all incoming connections while allowing outbound connections.
Notify User when Windows Firewall blocks a new app	Enable to allow notifications to display when the Windows Firewall blocks a new app.

Settings	Description
Enable Firewall	Enable to ensure that the firewall is running on devices.
Block all connections to apps that are not on the list of allowed apps	Enable to restrict all access for non-whitelisted apps.
Block all incoming connections including those in the list of allowed apps	Enable to block all incoming connections while allowing outbound connections.
Notify User when Windows Firewall blocks a new app	Enable to allow notifications to display when the Windows Firewall blocks a new app.

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

Compliance Policies

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.

Windows 7 Application Overview

5

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

Use the VMware Content Locker to safeguard corporate content on mobile devices. Download the Workspace ONE Intelligent Hub for Windows to monitor your devices on a more granular level.

This chapter includes the following topics:

- [Configure the Workspace ONE Intelligent Hub for Windows 7](#)
- [VMware Content Locker for Windows 7](#)

Configure the Workspace ONE Intelligent Hub for Windows 7

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

The Workspace ONE Intelligent Hub for Windows adds features and functionality for managing and configuring Windows 7 devices. Besides enrollment, the Workspace ONE Intelligent Hub reports the device status to the Workspace ONE UEM Console and allows for advanced profiles such as Firewall and Windows Updates.

The Workspace ONE Intelligent Hub for Windows can be found on the Resource Portal and at awagent.com.

Configuring the Workspace ONE Intelligent Hub

Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows 7 > Hub Settings** to change the following settings:

Setting	Description
Beacon Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will check in with the Workspace ONE UEM console.
Data Sample Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will collect a data sample from the device.

Setting	Description
Data Transmit Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will transmit the collected data sample to the console. This settings also controls how often the Workspace ONE Intelligent Hub checks for a new automatic upgrade if enabled.
Block Enrollment if Windows Genuine validation fails	Enable to block devices with non-genuine copies of Windows Operating Systems from enrolling into Workspace ONE UEM. <ul style="list-style-type: none"> ■ If a device is enrolled and the Workspace ONE Intelligent Hub detects the Windows copy is not genuine, the Workspace ONE Intelligent Hub will send an Enterprise Wipe command to the device. ■ If a device attempts to enroll and the copy of Windows is not genuine, a Non-Compliance message will display and immediately unenroll a device.
Enforce Passcode Profile	Enable to force the Workspace ONE Intelligent Hub to prompt end users for password changes when a passcode profile is installed or updated. This option does not apply to domain-joined devices.
Windows Agent Automatic Updates	Enable to automatically update the Workspace ONE Intelligent Hub when an update becomes available.

Remote Management

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user sees when a remote request is sent. ■ Enter the Yes Caption message for the accept button the end user sees on the Seek Permission request. ■ Enter the No Caption message for the decline button the end user sees on the Seek Permission request.

Workspace ONE Intelligent Hub for Windows Upgrades

When you update the Workspace ONE Intelligent Hub for Windows on a Windows 7 device, you must ensure that you use specific file names. Ensure that the file name is correct when downloading the Workspace ONE Intelligent Hub.

The Workspace ONE Intelligent Hub download file is **AirwatchAgent.msi**. The file name must be exactly **AirwatchAgent.msi** or the automatic upgrade fails. For example, if you download a second copy of the file, it is labeled as **AirwatchAgent.msi(1)**. Attempts to use this numbered copy fail to upgrade.

If you enable the Windows Agent Automatic Updates option, the Workspace ONE Intelligent Hub for Windows automatically updates without end-user interaction. If you are using any version before Workspace ONE Intelligent Hub for Windows v7.0.0, you must upgrade the Workspace ONE Intelligent Hub manually to v7.0.0+.

Important During the upgrade process for end users, an alert displays if the upgrade fails three times. If an end user contacts you about this message, perform an enterprise wipe and instruct your end users to reinstall the Workspace ONE Intelligent Hub.

VMware Content Locker for Windows 7

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.

Product Provisioning Overview

Product provisioning enables you to create, through Workspace ONE™ UEM, products containing profiles, applications, files/actions, and event actions (depending on the platform you use). These products follow a set of rules, schedules, and dependencies as guidelines for ensuring your devices remain up-to-date with the content they need.

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

Windows 7 Device Management

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](#)
- [Device Details Page, Win7](#)
- [Advanced Remote Management](#)

Device Dashboard

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

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

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

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

- **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 Device List View to see a full listing of devices in the currently selected organization group.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on 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 friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate it from other devices, particularly other devices of the same make and model.

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.

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.

Device Details Page, Win7

Use the Device Details page to track detailed device information for Windows 7 devices 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 Workspace ONE UEM deployment.

Remote Actions

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

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

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **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.
- **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.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **Query All** – Send a query command to the device to return a list of installed apps (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles and security measures.
- **Remote Management** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshoot on the device. Android devices require Remote Control Service to be installed on the device.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.

Advanced Remote Management

Advanced Remote Management (ARM) allows you to connect remotely to end-user devices so you can help with troubleshooting and maintenance. ARM requires your computer and the end-user device to connect to the Advanced Remote Management Server to facilitate communication between the Workspace ONE UEM console and the end-user device.

For more information, see **VMware Workspace ONE Advanced Remote Management Documentation** on docs.vmware.com.