

VMware AirWatch Windows Desktop Platform Guide

Deploying and managing Windows Desktop devices

AirWatch v9.3

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

| | |
|---|-----------|
| Chapter 1: Overview | 4 |
| Introduction to Windows Desktop | 5 |
| Windows Desktop Enrollment Requirements | 5 |
| Supported Windows Desktop Devices | 5 |
| Chapter 2: Windows Desktop Device Enrollment | 10 |
| Windows Desktop Enrollment Overview | 11 |
| Windows Desktop and Windows 7 Devices | 12 |
| AirWatch Agent for Windows Enrollment | 13 |
| Native MDM Enrollment for Windows Desktop | 14 |
| Device Staging Enrollment | 21 |
| Windows 10 Provisioning Service by VMware AirWatch | 25 |
| Enrollment Through Azure AD Integration | 26 |
| Bulk Provisioning and Enrollment | 36 |
| AirWatch Protection Agent for Enrollment | 39 |
| Chapter 3: Windows Desktop Device Profiles | 41 |
| Windows Desktop Profiles Overview | 43 |
| Configure a Passcode Profile (Windows Desktop) | 44 |
| Configure a Wi-Fi Profile (Windows Desktop) | 46 |
| VPN Profile (Windows Desktop) | 48 |
| Credentials Profile (Windows Desktop) | 53 |
| Configure a Restrictions Payload (Windows Desktop) | 55 |
| Data Protection Profile (Windows Desktop) | 61 |
| Passport for Work Profile (Windows Desktop) | 64 |
| Configure a Firewall Profile (Windows Desktop) | 66 |
| Configure a Single App Mode Profile (Windows Desktop) | 67 |
| Configure an Antivirus Profile (Windows Desktop) | 68 |
| Encryption Profile (Windows Desktop) | 70 |
| Configure a Windows Updates Profile (Windows Desktop) | 74 |
| Configure a Web Clips Profile (Windows Desktop) | 81 |
| Exchange ActiveSync Profile (Windows Desktop) | 82 |

| | |
|--|------------|
| SCEP Profile (Windows Desktop) | 87 |
| Application Control Profile (Windows Desktop) | 88 |
| Configure an Exchange Web Services Profile (Windows Desktop) | 91 |
| Create a Windows Licensing Profile (Windows Desktop) | 91 |
| Configure a BIOS Profile (Windows Desktop) | 92 |
| Configure the OEM Updates Profile (Windows Desktop) | 95 |
| Use Custom Settings (Windows Desktop) | 98 |
| Chapter 4: Compliance Policies | 101 |
| Compliance Policy Overview | 102 |
| Compromised Device Detection with Health Attestation | 102 |
| Chapter 5: Apps for Windows Desktop Devices | 105 |
| Windows Desktop Application Overview | 106 |
| VMware Workspace ONE for Windows Desktop | 106 |
| Configure the AirWatch Agent for Windows Desktop Devices | 106 |
| VMware Content Locker for Windows Desktop Devices | 108 |
| VMware Browser for Windows Desktop | 108 |
| Chapter 6: Dell Client Command Integration | 109 |
| Dell Command Monitor Integration | 110 |
| Dell Command Update Overview | 111 |
| Chapter 7: Product Provisioning for Windows Desktop Devices | 113 |
| Product Provisioning Overview | 114 |
| Chapter 8: Managing Windows Desktop Devices | 115 |
| Windows Desktop Device Management Overview | 116 |
| Device Dashboard | 116 |
| Device List View | 116 |
| Windows Desktop Device Details Page | 117 |
| Remote Management | 118 |
| Accessing Other Documents | 119 |

Chapter 1:

Overview

- Introduction to Windows Desktop5
- Windows Desktop Enrollment Requirements 5
- Supported Windows Desktop Devices5

Introduction to Windows Desktop

AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Windows 8.1 and Windows 10 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 of our device profiles, you can properly configure and secure your Windows devices. Detect compromised devices and remove their access to corporate resources using the compliance engine.

Enrolling your devices into AirWatch allows you to secure and configure devices to meet your needs.

Windows Desktop Enrollment Requirements

Before enrolling your Windows Desktop devices, ensure you have met the requirements. These requirements include important information to provide end users enrolling their own devices.

Requirements

- **Active Environment** – Your active AirWatch environment and your access to the AirWatch Console.
- **Appropriate Admin Permissions** – A type of permission that allows you to create profiles, determine policies, and manage devices within the AirWatch Console.
- **Enrollment URL** – This URL is unique to your enrollment environment and takes you directly to the enrollment screen. For example, **mdm.example.com**.
- **Group ID** – This Group ID associates your device with your corporate role and is defined in the AirWatch Console.

Important: If your enrollment server is behind a proxy, you must configure the Windows service WINHTTP to be proxy-aware when configuring your network settings.

Supported Windows Desktop Devices

The Windows Desktop platform includes versions of the Windows operating system ranging from Windows 8.0 to Windows 10 and the various versions of each iteration.

Platforms and Devices Supported

Devices running the following operating systems:

| | |
|------------------------|-----------------------|
| Windows 8.1 RT | Windows 10 Home |
| Windows 8.1 Core | Windows 10 Pro |
| Windows 8.1 Pro | Windows 10 Enterprise |
| Windows 8.1 Enterprise | Windows 10 Education |

AirWatch supports the following versions of Windows 10:

- 1507
- 1511
- 1607
- 1703
- 1709

 **Important:** To see the OS version each update branch supports, see Microsoft's documentation on Windows 10 release information: <https://technet.microsoft.com/en-us/windows/release-info.aspx>.

Windows Desktop Features Matrix

Compare which AirWatch features are available to the Windows 8.0/RT, Windows 8.1/RT, and Windows 10 operating systems. AirWatch supports all versions of Windows 8.0 and up, but the functionality differs based on the operating system.

Feature Matrix

| Feature | Windows 8.0/RT | Windows 8.1/RT | Windows 10 |
|--|----------------|----------------|------------|
| Activation & Enrollment | | | |
| Native Client Enrollment | | ✓ | ✓ |
| Agent Based Enrollment | ✓ | ✓ | ✓ |
| Requires a Windows Account ID | ✓ | | |
| Force EULA/Terms of Use Acceptance | ✓ | ✓ | ✓ |
| Support for Option Prompts during Enrollment | ✓ | ✓ | ✓ |
| Active Directory/ LDAP | ✓ | ✓ | ✓ |
| Cloud Domain Join Enrollment | | | ✓ |
| Out of Box Experience Enrollment | | | ✓ |
| Bulk Provisioning Enrollment | | | ✓ |
| Device Staging | | | ✓ |
| Architecture | | | |
| SMS | ✓ | ✓ | ✓ |
| Email Messages | ✓ | ✓ | ✓ |
| Security Policies & Compliance Monitoring | | | |
| Password Policy | ✓ ¹ | ✓ ³ | ✓ |
| Enterprise Wipe | ✓ ¹ | ✓ | ✓ |

| Feature | Windows 8.0/RT | Windows 8.1/RT | Windows 10 |
|---|----------------|----------------|----------------|
| Full Wipe | | | ✓ |
| Over-the-Air Provisioning | | | |
| Email & Exchange ActiveSync | | ✓ ² | ✓ |
| Wi-Fi | | ✓ | ✓ |
| VPN | | ✓ | ✓ |
| Certificate Management | | ✓ | ✓ |
| Device Restrictions and Settings | | ✓ | ✓ |
| Passport for Work | | | ✓ |
| Encryption | | ✓ | ✓ |
| Application Control (AppLocker) | | | ✓ ⁴ |
| Health Attestation | | | ✓ |
| Application Management | | | |
| Application Management | ✓ | ✓ | ✓ |
| AirWatch Applications | | | |
| VMware Browser | | ✓ | ✓ |
| VMware Content Locker | | ✓ | ✓ |
| Asset Tracking | | | |
| Asset Tracking | ✓ | ✓ | ✓ |
| Device Status | ✓ | ✓ | ✓ |
| IP Address | ✓ | | |
| Location | ✓ | ✓ | ✓ |
| Network | ✓ | ✓ | ✓ |
| Remote Management Support | | | |
| Send Support Message (Email and SMS only) | ✓ | ✓ | ✓ |

1 – Denotes the requirement of PowerShell integration.

2 – Denotes the requirement of AirWatch Inbox to use.

3 – Windows 8.1/RT devices cannot enforce the use of a passcode if one is not already created. The passcode can only be enforced to remain in use if it was created before the passcode profile was pushed to the device.

4 – This feature is only available in Enterprise and Education version of Windows 10.

Windows 10 Version Matrix

Compare the MDM functionality available in each version of the Windows 10 OS. AirWatch supports all versions of Windows 10 OS and the functions they support.

The different editions of Windows 10 (Home, Professional, Enterprise, and Education) have different functionality. Windows 10 Home edition does not support the advanced functionality available to the Windows 10 OS. AirWatch recommends using Enterprise or Education editions for the most functionality.

| Feature | Windows 10 OS Version | | | |
|--|-----------------------|--------------|-------------------------|-----------|
| | Home | Professional | Enterprise ¹ | Education |
| Activation & Enrollment | | | | |
| Native Client Enrollment | ✓ | ✓ | ✓ | ✓ |
| Agent Based Enrollment | ✓ | ✓ | ✓ | ✓ |
| Requires a Windows Account ID | | | | |
| Force EULA/Terms of Use Acceptance | ✓ | ✓ | ✓ | ✓ |
| Support for Option Prompts during Enrollment | ✓ | ✓ | ✓ | ✓ |
| Active Directory/ LDAP | ✓ | ✓ | ✓ | ✓ |
| Cloud Domain Join Enrollment | | ✓ | ✓ | ✓ |
| Out of Box Experience Enrollment | | ✓ | ✓ | ✓ |
| Bulk Provisioning Enrollment | | ✓ | ✓ | ✓ |
| Device Staging | ✓ | ✓ | ✓ | ✓ |
| Architecture | | | | |
| SMS | | | | |
| Email Messages | | ✓ | ✓ | ✓ |
| Security Policies & Compliance Monitoring | | | | |
| Password Policy | ✓ | ✓ | ✓ | ✓ |
| Enterprise Wipe | ✓ | ✓ | ✓ | ✓ |
| Full Device Wipe | ✓ | ✓ | ✓ | ✓ |
| Over-the-Air Provisioning | | | | |
| Email & Exchange ActiveSync | ✓ | ✓ | ✓ | ✓ |
| Wi-Fi | ✓ | ✓ | ✓ | ✓ |
| VPN | ✓ | ✓ | ✓ | ✓ |
| Certificate Management | ✓ | ✓ | ✓ | ✓ |
| Device Restrictions and Settings | ✓ | ✓ | ✓ | ✓ |
| Passport for Work | ✓ ³ | ✓ | ✓ | ✓ |
| Encryption | ✓ ⁴ | ✓ | ✓ | ✓ |
| Application Control (AppLocker) | | | ✓ | ✓ |
| Health Attestation | ✓ | ✓ | ✓ | ✓ |
| Windows Update for Business | | ✓ | ✓ | ✓ |

| Feature | Windows 10 OS Version | | | |
|---|-----------------------|----------------|-------------------------|----------------|
| | Home | Professional | Enterprise ¹ | Education |
| Assigned Access | | | ✓ | ✓ |
| Application Management | | | | |
| Application Management | | ✓ | ✓ | ✓ |
| AirWatch Applications | | | | |
| VMware Browser | ✓ ⁴ | ✓ | ✓ | ✓ |
| VMware Content Locker | ✓ ⁴ | ✓ | ✓ | ✓ |
| Asset Tracking | | | | |
| Asset Tracking | | ✓ | ✓ | ✓ |
| Device Status | | ✓ | ✓ | ✓ |
| IP Address | | | | |
| Location | ✓ ⁵ | ✓ ⁵ | ✓ ⁵ | ✓ ⁵ |
| Network | | ✓ | ✓ | ✓ |
| Remote Management Support | | | | |
| Send Support Message (Email and SMS only) | | ✓ | ✓ | ✓ |

1 – Enterprise also includes IoT Enterprise and Long-Term Servicing Branch (LTSB). LTSB is a separate Windows 10 Enterprise image with many native apps, including Microsoft Edge, Cortana, and the Microsoft Store, removed. Some AirWatch functionality which leverage these features will not be supported.

2 – Microsoft Passport requires TPM 1.2 or 2.0 hardware based protection of credentials or keys; if no TPM exists or is configured, credentials and keys protection will be OS-based.

3 – Device encryption for home does not include BitLocker encryption.

4 – Can be downloaded from the Microsoft Store only. Windows 10 Home does not support pushing internal apps.

5 – Requires the AirWatch Agent downloaded from the Microsoft Store.

Chapter 2:

Windows Desktop Device Enrollment

| | |
|--|----|
| Windows Desktop Enrollment Overview | 11 |
| Windows Desktop and Windows 7 Devices | 12 |
| AirWatch Agent for Windows Enrollment | 13 |
| Native MDM Enrollment for Windows Desktop | 14 |
| Device Staging Enrollment | 21 |
| Windows 10 Provisioning Service by VMware AirWatch | 25 |
| Enrollment Through Azure AD Integration | 26 |
| Bulk Provisioning and Enrollment | 36 |
| AirWatch Protection Agent for Enrollment | 39 |

Windows Desktop Enrollment Overview

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

Enrollment Basics

The enrollment methods for Windows Desktop devices vary based on your AirWatch deployment, enterprise integrations, and device operating system. The Windows Desktop platform supports various OS versions and SKUs for Windows devices. For more information, see [Supported Windows Desktop Devices on page 5](#).

Before enrolling devices, ensure that you have the required enrollment information. See [Windows Desktop Enrollment Requirements on page 5](#) 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 AirWatch Agent for Windows, or Azure AD integration.

 If you want to use AirWatch to manage Windows devices managed by SCCM, you must download the VMware AirWatch SCCM Integration Client. Use this client to enroll SCCM-managed devices into AirWatch. For more information, see the Knowledge Base article [VMware AirWatch SCCM Integration Client: https://support.airwatch.com/articles/115001664948](https://support.airwatch.com/articles/115001664948).

AirWatch Agent for Windows Enrollment

The simplest enrollment workflow uses the AirWatch Agent for Windows to enroll devices. End users simply download the AirWatch Agent from the Microsoft Store and follow the prompts to enroll. For more information on Agent-based enrollment, see [AirWatch Agent for Windows Enrollment on page 13](#).

Native MDM Enrollment

AirWatch supports enrolling Windows Desktop 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 Enrollment for Windows Desktop on page 14](#).

Device Staging

If you want to configure device management on a Windows 10 device before shipping a device to your end user, consider using Windows Desktop device staging. This enrollment workflow allows you to enroll a device through the AirWatch Agent, install device-level profiles, and then ship the device to end users. The two methods of device staging are manual installation and command-line installation. Manual installation requires devices to be domain-joined to an Azure AD integration. Command-line installation works for all Windows 10 devices. See [Device Staging Enrollment on page 21](#) for more information.

Windows Desktop Auto-Enrollment

AirWatch supports the auto-enrollment of specific Windows Desktop devices purchased from Dell. Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.

Windows 10 Provisioning Service by VMware AirWatch only applies to select Dell Enterprise devices with the correct Windows 10 image. The auto-enrollment functionality must be purchased as part of the purchase order from Dell.

For more information, see [Windows 10 Provisioning Service by VMware AirWatch on page 25](#).

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 three different enrollment flows: Join Azure AD, Out of Box Experience enrollment, and Office 365 enrollment. 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 for SaaS Deployments on page 27](#).

To enroll through Azure AD integration workflows, see [Enrollment Through Azure AD Integration on page 26](#).

Bulk Provisioning and Enrollment

Bulk provisioning creates a pre-configured package that stages Windows 10 devices and enrolls them into AirWatch. Bulk provisioning requires downloading the Microsoft Assessment and Development Kit and installing the Imaging and Configuration Designer tool. This tool creates the provisioning packages used to image devices.

With the bulk provisioning workflow, you can include AirWatch settings in the provisioning package so that provisioned devices automatically enroll during the initial Out of Box Experience. For more information, see [Bulk Provisioning and Enrollment on page 36](#).

AirWatch Protection Agent

The AirWatch Protection Agent adds endpoint protection to ensure that your Windows Desktop devices remain secure. By enabling the AirWatch Protection Agent, you allow AirWatch to configure and use native Windows features for device security. The Encryption, Firewall, and Windows Updates profiles require the AirWatch Protection Agent to provision devices. For more information, see [AirWatch Protection Agent for Enrollment on page 39](#).

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 AirWatch Agent for Windows.

The table shows the differences in enrollment methods. Consider enrolling Windows 8 and Windows 10 devices using the native MDM enrollment method because of the increased device management functionality.

| Functionality | Windows 7 | Windows Desktop |
|------------------------------|-----------|-----------------|
| Native MDM Enrollment Method | | ✓ |

| Functionality | Windows 7 | Windows Desktop |
|--|-----------|-----------------|
| AirWatch Agent Enrollment | ✓ | ✓ |
| AirWatch Protection Agent Support | ✓ | ✓ |
| Supports Full Windows 10 functionality | | ✓ |
| Supports SCCM Managed Devices | ✓ | ✓ |
| Supports Windows 7 Devices | ✓ | |

AirWatch Agent for Windows Enrollment

The AirWatch Agent provides a single resource for enrollment and facilitates communication between the device and the AirWatch Console. Use the AirWatch Agent to simplify enrollment and enable full MDM functionality.

Consider using the AirWatch Agent for Windows to enroll your Windows 10 devices as the agent provides the simplest enrollment flow for users.

The AirWatch Agent provides extra functionality to your Windows Desktop devices including location services.

You can simplify enrollment for your end users by using Windows Auto-Discovery. Windows Auto-Discovery enables end users to enter their email address to fill in the text boxes automatically with their enrollment credentials.

For more information on Auto-Discovery, see the **VMware AirWatch Windows Auto-Discovery Installation Guide** and the **Mobile Device Management Guide** available on [AirWatch Resources](#).

Enroll With the VMware AirWatch Agent

Use the AirWatch Agent to start enrollment of your Windows Desktop devices. The AirWatch Agent provides a simplified enrollment flow for end users that is quick and easy enrollment.

To enroll Windows 10 devices using the AirWatch Agent:

1. On the Windows 10 device, open the Microsoft Store starts and search for the AirWatch Agent. Download the agent.
2. Install the AirWatch Agent. When the installation is finished, start the agent.
3. Select **Connect a work or school account**. The AirWatch Agent then opens the Workplace native app to complete enrollment.
4. Enter the email address and select **Next**.

If you are not using Windows Auto-Discovery, complete the following settings:

- Enter the **Server URL** and select **Next**.
 - Enter the **Group ID** and select **Next**.
 - Enter the **Username** and **Password**.
5. **Accept** the terms of use.
 6. Select **Done**.
 7. Open the AirWatch Agent and complete the enrollment.

Native MDM Enrollment for Windows Desktop

Windows Desktop enrollment methods all use the Workplace or Work Access native MDM Client. Use the native MDM enrollment to enroll both corporate owned and BYOD devices through the same enrollment flow.

Windows 10 devices use Work Access enrollment and Windows 8.1/RT devices use Workplace enrollment.

Work Access first processes an Azure AD work flow for domains connected to Office 360 or Azure AD when you select **Connect** and does not automatically complete the enrollment workflow. If you use Office 365 or Azure AD without a premium license, consider using the AirWatch Agent to enroll Windows 10 devices instead of native MDM enrollment. To complete the enrollment workflow using native MDM enrollment, select **Connect** twice. If you have an Azure AD premium license, you can enable **Require Management** in your Azure instance to have native MDM enrollment complete the enrollment flow after the Azure work flow. You can use native MDM enrollment without issue if you do not use Office 365 or Azure AD.

 For more technical information on how the enrollment flow works after the Windows 10 Anniversary Update, see the knowledge base article **Enrollment changes for Windows devices after Windows Anniversary update** available here: <https://support.air-watch.com/articles/115001665408>.

Only users who have local admin permissions on the device can enroll a device into AirWatch and enable MDM. Domain Admin permissions do not work for enrolling a device. To enroll a device with a standard user, you must use Enroll on Behalf of Others enrollment for Windows 8.1 devices or Bulk Provisioning for Windows 10 devices.

By using the Windows Auto-Discovery Service, you simplify enrollment for your end user by reducing the necessary interaction during enrollment. Using the Windows Auto-Discovery Service requires you to follow the steps outlined in the **VMware AirWatch Windows Auto-Discovery Service Installation Guide**.

Devices joined to a domain can enroll using the native Workplace enrollment. The email address entered in the settings is auto-populated with the Active Directory UPN attribute. If the end user wants to use a different email address, they must download the optional update.

Enroll Through Work Access With Windows Auto Discovery

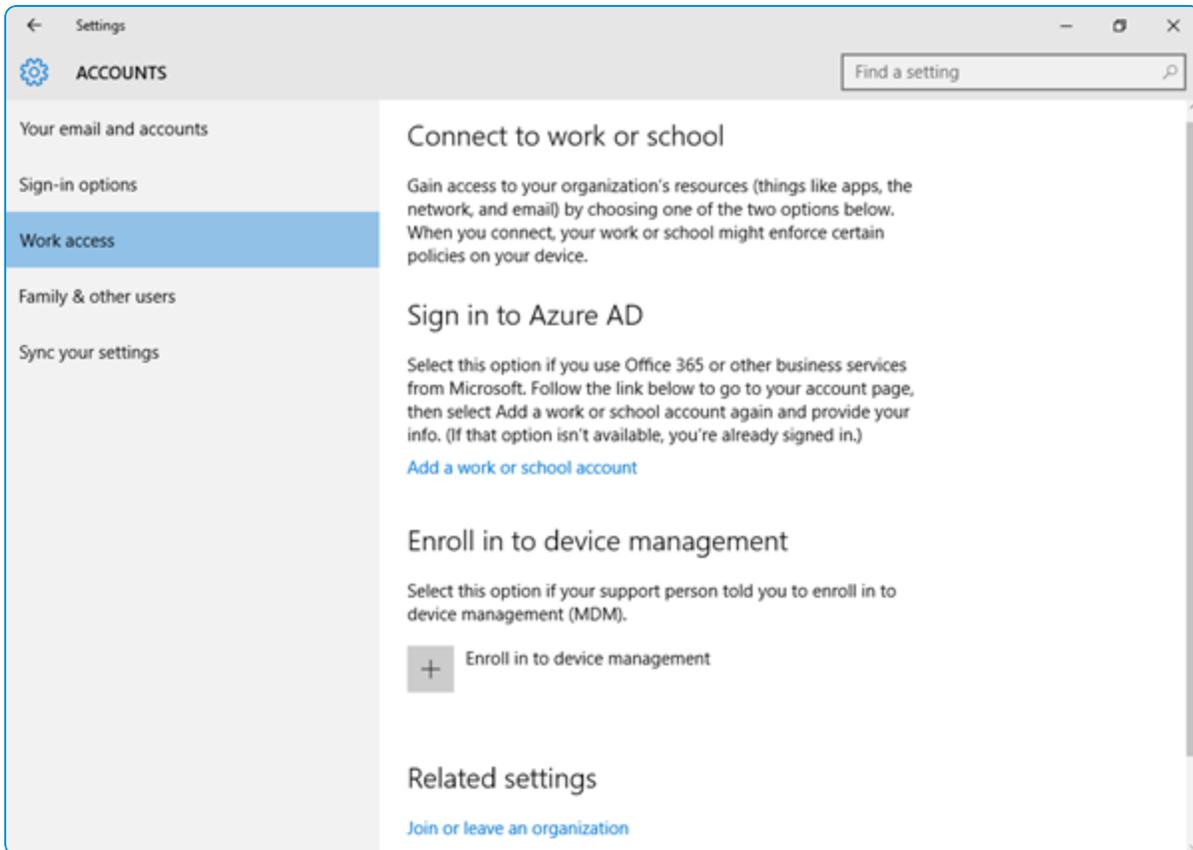
Work Access is the native MDM enrollment method for Windows 10 devices. Enrolling through Work Access and using Windows Auto Discovery provides a quick and easy enrollment flow for end users.

Registering your domain in AirWatch removes the need to enter the Group ID during enrollment.

See the **VMware AirWatch Windows Auto-Discovery Guide** available on [AirWatch Resources](#) for more details.

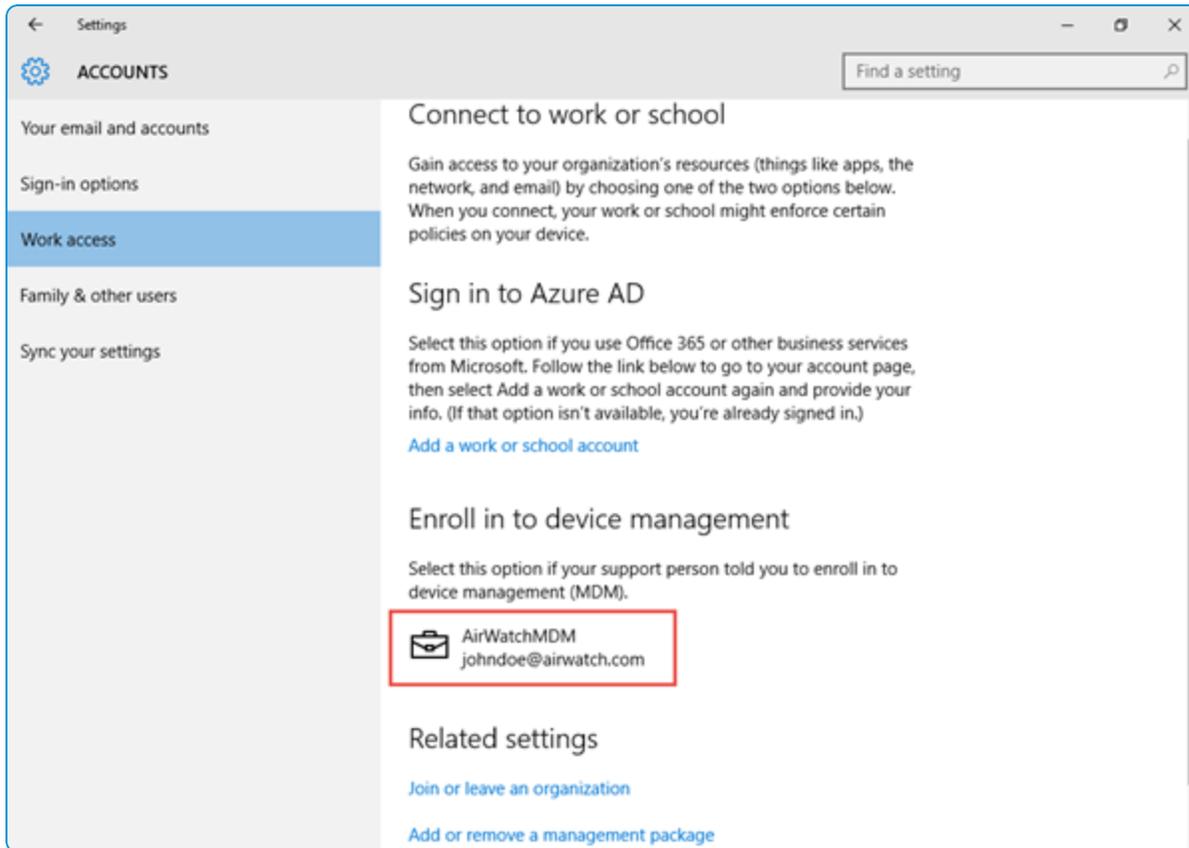
Note: Consider using the AirWatch Agent for Windows to enroll your Windows 10 devices instead of using native MDM enrollment. The native MDM enrollment flow does not enroll devices into MDM if you use Office 365 or Azure AD on the same domain.

1. Navigate on the device to **Settings > Accounts > Work Access** and select **Enroll in to device management**.



2. Enter the user name you provided to your end user into the **Email** text box, followed by the domain for the environment in the format Username@domain.com (such as jdoe1@acme.com). Select **Continue**.
3. Enter the **Group ID** and select **Next**.
4. Enter your **username** and **password** and select **Next**.
These credentials may be your directory services credentials or dedicated credentials specific to your AirWatch environment.
5. Review the End User License Agreement and select **Accept** to agree to the terms of use.
This step is optional and only displays if enabled in the AirWatch Console.
6. (Optional) Select **Yes** to save sign-in info.

The device then attempts to connect to AirWatch. If it connects successfully, a briefcase icon displays with AirWatch written next to it. This icon shows your successful connection to AirWatch.



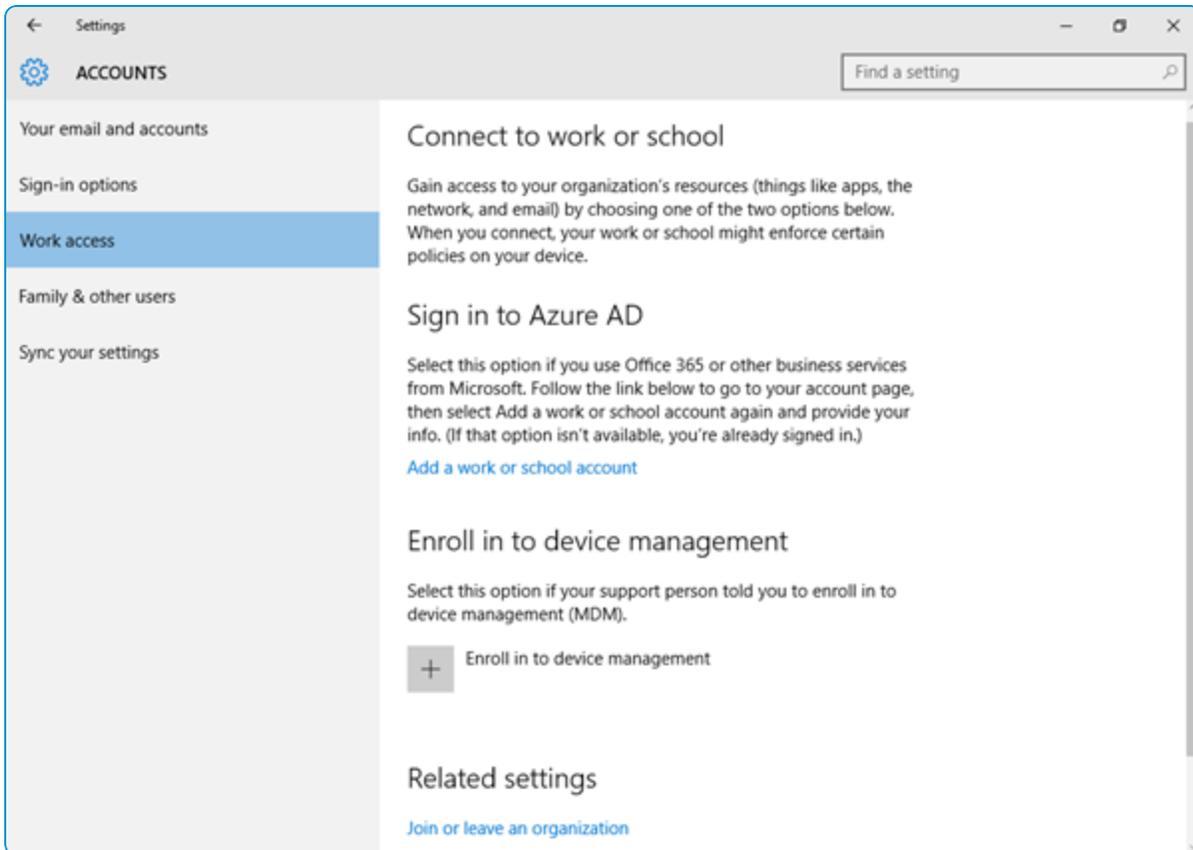
Enroll Through Work Access Without Windows Auto Discovery

Work Access is the native MDM enrollment method for Windows 10 devices. Enrolling through Work Access without WADS requires manually entering end-user credentials.

Note: Consider using the AirWatch Agent for Windows to enroll your Windows 10 devices instead of using native MDM enrollment. The native MDM enrollment flow does not enroll devices into MDM if you use Office 365 or Azure AD on the same domain.

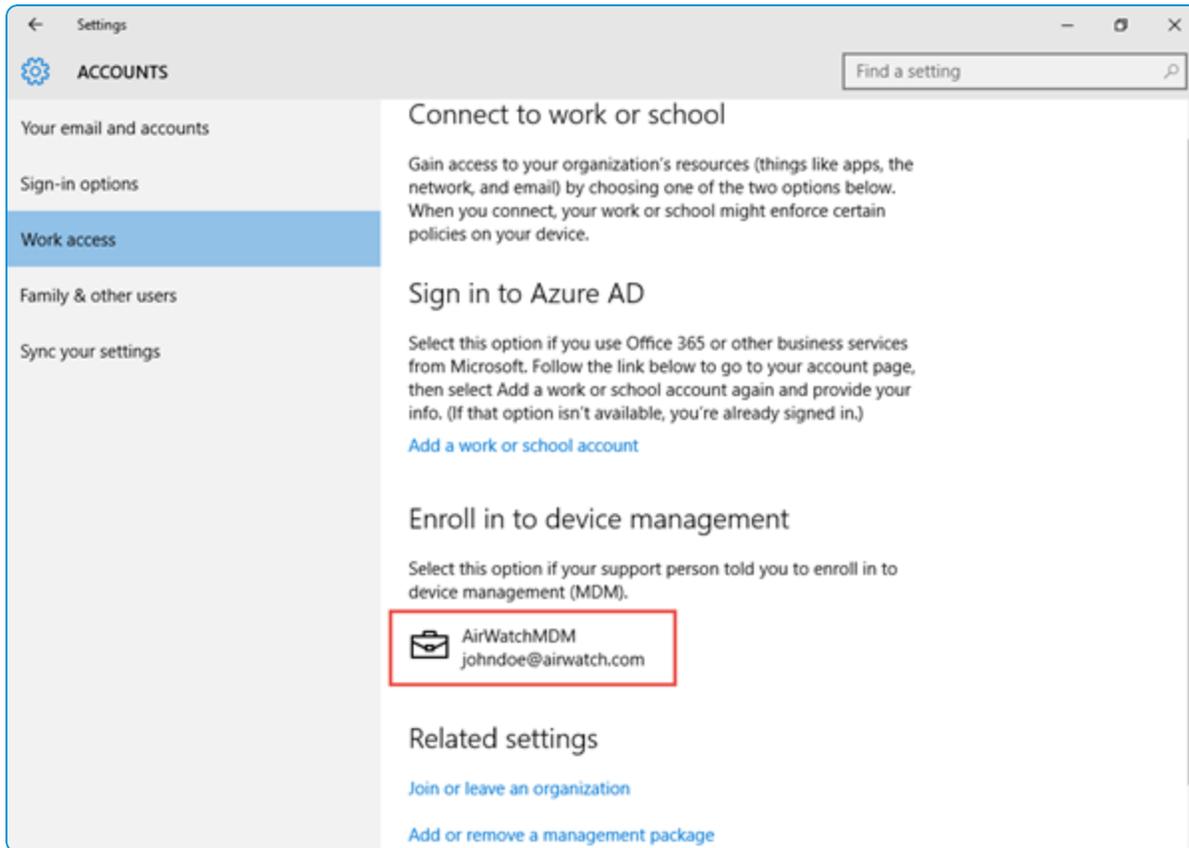
To enroll through Work Access without WADS:

1. Navigate on the device to **Settings > Accounts > Work Access** and select **Enroll in to device management**.



2. Enter the user name you provided to your end user into the **Email** text box, followed by the domain for the environment in the format Username@domain.com (such as jdoe1@acme.com).
3. **Enter server address** as follows: <DeviceServicesURL>/DeviceServices/Discovery.aws. Do not include 'https://' in the URL. For example: ds156.awmdm.com/deviceservices/discovery.aws.
4. Select **Continue**.
5. Enter the **Group ID** and select **Next**.
6. Enter your **username** and **password** and select **Next**.
These credentials may be your directory services credentials, or dedicated credentials specific to your AirWatch environment.
7. (Optional) Review the End-User License Agreement and select **Accept** to agree to the terms of use.
This step is optional and only displays if you choose to enable it.
8. (Optional) Select **Yes** to save sign-in info.

The device then attempts to connect to AirWatch. If it connects successfully, a briefcase icon displays with AirWatch written next to it. This icon shows your successful connection to AirWatch.



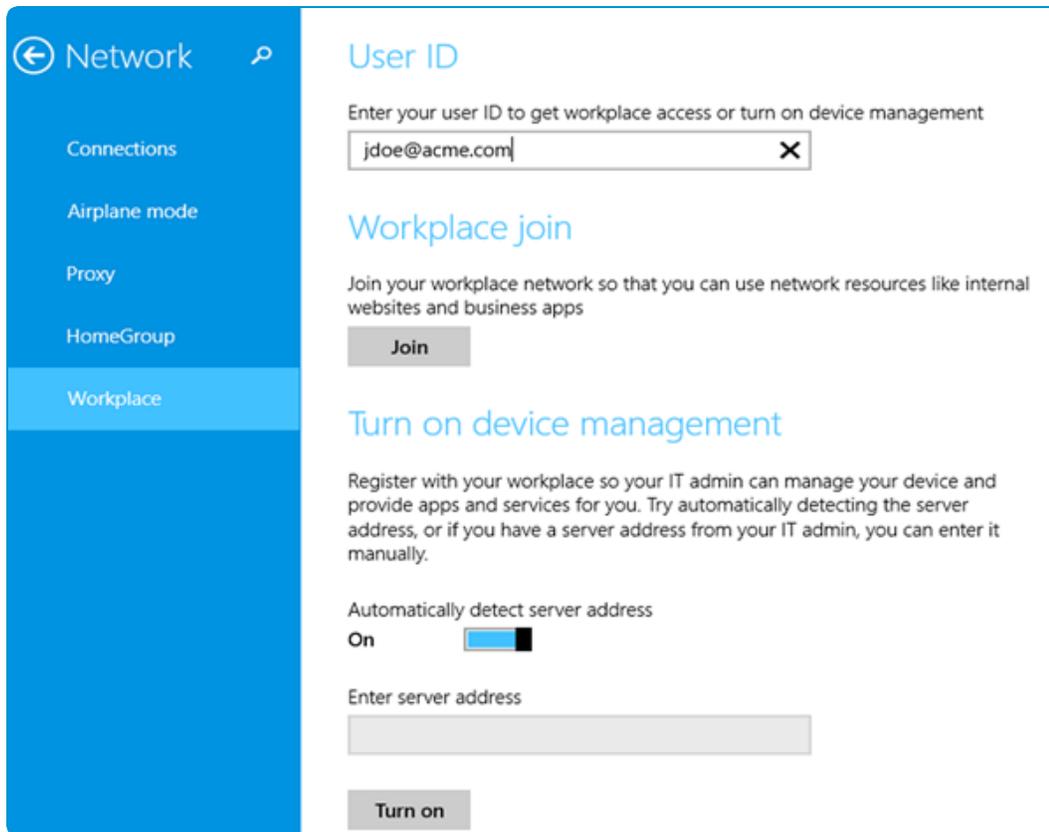
Enroll Through Workplace With Windows Auto Discovery

Workplace is the native MDM enrollment method for Windows 8.1 devices. Enrolling through Workplace and using the Windows Auto Discovery provides a quick and easy enrollment flow for end users.

Service (WADS) provides a quick and easy enrollment flow for end users.

To enroll through Workplace with WADS:

1. Navigate on the device to **Settings > Change PC Settings > Network > Workplace**.



2. Enter the user name you provided to your end user into the **Email** text box, followed by the domain for the environment in the format Username@domain.com (such as jdoe1@acme.com).
The email address text box does not display for devices that are domain joined. Registering the UPN domain during WADS configuration removes the need to enter the email address for all AD users.
3. Under **Turn on device management**, leave the **Automatically detect server address** slider set to **On**.
4. Leave the **Enter server address** text box blank.
5. Select **Turn On**.
6. Enter the **Group ID** and select **Next**.
Registering your domain in AirWatch removes the need to enter the Group ID during enrollment.
7. Enter your **username** and **password** and select **Next**.
These credentials may be your directory services credentials or dedicated credentials specific to your AirWatch environment.
8. Select **Turn On**. If the button changes from **Turn On** to **Turn Off**, you have successfully enrolled the device. Do not select **Turn Off** or the device unenrolls from AirWatch.

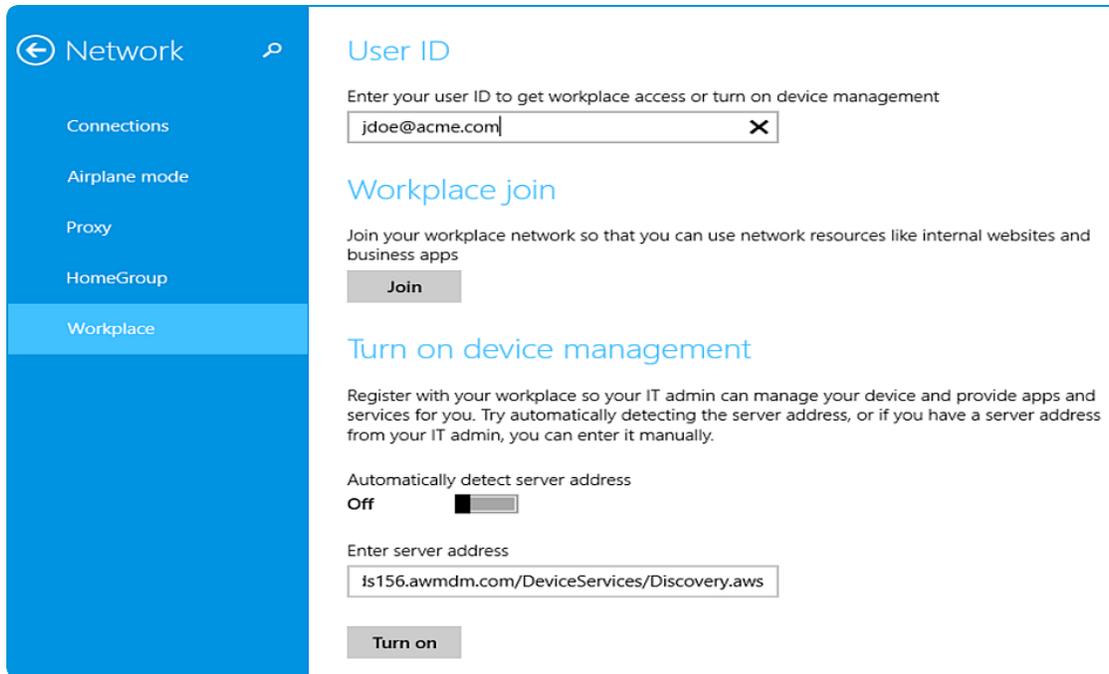
Enroll Through Workplace Without Windows Auto Discovery

Workplace is the native MDM enrollment method for Windows 8.1 devices. Enrolling through Workplace and without WADS requires manually entering end-user credentials.

Important This enrollment method requires an optional update from Microsoft. For more information about this update, refer to <http://support.microsoft.com/kb/2955164>.

To enroll through Workplace without WADS:

1. Navigate on the device to **Settings > Change PC Settings > Network > Workplace**.



2. Enter the user name you provided to your end user into the **Email** text box, followed by the domain for the environment in the format Username@domain.com (such as jdoe1@acme.com).
The email address text box does not display for devices that are domain joined.
3. Under **Turn on device management**, set the **Automatically detect server address** slider to **Off**.
4. **Enter server address** as follows: <DeviceServicesURL>/DeviceServices/Discovery.aws. Do not include 'https://' in the URL.
For example: ds156.awmdm.com/deviceservices/discovery.aws.
5. Select **Turn On**.
6. Enter the **Group ID** and select **Next**.
7. Enter your **username** and **password** and select **Next**.
These credentials may be your directory services credentials or dedicated credentials specific to your AirWatch environment.
8. Complete the optional steps if you choose to allow device users the ability to make these selections.
 - Select the **Device Ownership** type, **Employee Owned**, **Corporate-Dedicated**, or **Corporate-Shared**.
 - Select **Next**.

- Review the End User License Agreement and select **Accept** to agree to the terms of use.
 - Select the **I understand** check box to allow installation of applications and services deployed.
9. Select **Turn On**. If the button changes from **Turn On** to **Turn Off**, you have successfully enrolled the device. Do not select **Turn Off** or the device unenrolls from AirWatch.

Device Staging Enrollment

Admins often prefer to configure device management before shipping a device to an end user. By using device staging enrollment, you can enroll a device with the AirWatch Windows Agent, install device-level profiles, and ship it to an end user.

Device staging enrollment enables you to enroll your Windows 10 device into AirWatch. This enrollment requires the AirWatch Windows Agent to start. After the device enrolls, any assigned device-level profiles download to the device. Once the device is fully enrolled and configured, you can ship the device to your end users. When the end user signs in to the device, the AirWatch Windows Agent updates the device record in the AirWatch Console. AirWatch reassigns the device to the end user and pushes any user-level profiles to the device.

The two staging methods are:

- **Manual Installation** – Download and install the AirWatch Agent and enter enrollment credentials. This method requires devices to be domain-joined before enrollment.
- **Command Line Installation** – Download the AirWatch Agent and then install and enroll the device using the command line.

The enrollment completes by either updating the AirWatch Console device registry when a user enrolls into a domain-joined device or by comparing the enrolled user name against a list of previously registers serial numbers.

Bulk Import Device Serial Numbers

Import device serial numbers for use with device staging to quickly add devices to the AirWatch Console. The bulk import requires a CSV file with all the serial numbers to import.

To register multiple devices:

1. Navigate to **Accounts > Users > List View** or **Devices > Lifecycle > Enrollment Status**.
 - a. Select **Add** and then **Batch Import** to display the **Batch Import** screen.
2. Complete each of the required fields. **Batch Name**, **Batch Description**, and **Batch Type**.
3. Under the **Batch File (.csv)** field is a list of task-based templates you can use to load users and their devices in bulk.
4. Select the appropriate download template and save the comma-separated values (CSV) file to somewhere accessible.
5. Locate the saved CSV file, open it with Excel, and enter all the relevant information for each of the devices that you want to import.

Each template is pre-populated with sample entries demonstrating the type of information (and its format) intended to be placed in each column.

Fields in the CSV file denoted with an asterisk (*) are required.

6. Save the completed template as a CSV file. In the AirWatch Console, select the **Choose File** button from the **Batch Import** screen, navigate to the path where you saved the completed CSV file and select it.
7. Select **Save** to complete registration for all listed users and corresponding devices.

Enroll through Command-Line Staging

Simplify enrollment for end users by staging your Windows Desktop devices using the Windows Command Line. This enrollment method enrolls the device and downloads device-level profiles base on the user credentials entered.

Important: Do not change the name of the `AirWatchAgent.msi` file as this change breaks the staging command.

To enroll through command-line staging:

1. On the end-user device, log into a local admin account.
2. Download the VMware AirWatch Windows 10 Agent UWP from [AirWatch Resources](#).
Only download the AirWatch Agent. 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 AirWatch Agent from the download folder to a local or network drive folder.
3. 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 on page 23](#).
If the end user account is a domain-joined account, ensure that you use the `ASSIGNTOLOGGEDINUSER` parameter.
4. Run the command. For examples of syntax, see [Examples of Silent Enrollment on page 24](#).
5. Verify that enrollment completes with the staging credentials

After the command runs, the device enrolls into AirWatch. If the device is domain-joined, the AirWatch Agent updates the AirWatch Console device registry with the correct user. If you are using the bulk serial number import, the AirWatch Agent updates the AirWatch Console device registry and connects the user credentials to the serial number of the device.

Enroll through Manual Device Staging

Simplify enrollment for end users by staging your Windows 10 devices using the AirWatch Windows Agent. This enrollment method enrolls the device and downloads device-level profiles so the end user must only log in to the device to begin using it.

These devices must be joined to a domain.

To stage your Windows 10 devices:

1. Navigate to www.awagent.com to download the AirWatch Agent Installer.
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:
 - Enter the email address to auto-fill the server details screen. Select **Next** and the details are entered.
 - Enter the Server Name and Group ID if you are not using AirWatch Auto-Discovery to complete the settings. Select **Next**.
6. Enter the staging **Username** and **Password** and select **Next**.
7. Complete any optional screens.
8. Select **Finish** to complete the enrollment.

Once the AirWatch Agent detects a staging user, the agent listener runs and listens for the next Windows login. When the end user logs into the device, the agent listener reads the user UPN and email from the device registry. This information is sent to the AirWatch Console and the device registry is updated to register the device to the user.

Silent Enrollment Parameters and Values

Silent enrollment requires command-line entries or a BAT file to control how the AirWatch Agent 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. Parameters highlighted in **blue** and **green** are the minimum parameters required for enrollment. Blue designates image only. Blue plus green designates user enrollment.

| 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 AirWatch 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. |

| Enrollment Parameters | Values to Add to Parameter |
|--|---|
| 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 AirWatch Agent uses the default path: C:\Program Files (x86)\AirWatch. |
| Items denoted with an asterisk (*) are optional. | |

Examples of Silent Enrollment

The following 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 agent 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
```

AirWatch Agent 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 AirWatch Agent on Network Drive

The following is an example of the installation directory parameter with the AirWatch Agent 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 10 Provisioning Service by VMware AirWatch

AirWatch supports the auto-enrollment of specific Windows Desktop devices purchased from Dell. Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.

Windows 10 Provisioning Service by VMware AirWatch only applies to select Dell devices with the correct Windows 10 image. The auto-enrollment functionality must be purchased as part of the purchase order from Dell. AirWatch only supports Windows 10 Pro, Enterprise, and Education SKUs for Cloud Provisioning.

Windows 10 Provisioning Service by VMware AirWatch matches registered devices with users and automatically enrolls the device following the Out-of-Box-Experience. When the end user signs in to the device, the provisioning agent on the device receives the profiles and apps assigned to the device and user. This functionality works similar to the Apple Device Enrollment Program.

When you purchase your Dell devices, Dell supplies AirWatch with the device details of the purchased devices. To use auto-enrollment, you must register the serial numbers for all the devices purchased from Dell. When registering the devices, you must select Windows Desktop as the Platform. AirWatch matches the serial number to the ones provides by dell for use with AirWatch Auto-Discovery.

You must register the devices with a user account before sending the devices to end users.

For a seamless enrollment experience, consider configuring the External Access Token authentication method for VMware Identity Manager. The External Access Token authentication enables Workspace ONE to open automatically and deliver apps to the device. When the feature is enabled, Workspace ONE automatically authenticates and provides the user with the first-launch experience that shows the application and policy installation progress.

Important: Devices enrolled through Windows 10 Provisioning Service by VMware AirWatch cannot be enrolled again after unenrollment until the device undergoes a factory reset.

Configure Windows 10 Provisioning

Configure Windows 10 Provisioning Service by VMware AirWatch to enroll Dell Windows Desktop devices automatically. Auto-enrollment compares registered device serial numbers against a list provided by Dell to enroll devices as part of the Out-of-Box-Experience.

Prerequisites

Before configuring Windows 10 Provisioning Service by VMware AirWatch, you must meet the prerequisites:

- Purchased Windows 10 Provisioning Service by VMware AirWatch as part of your purchase order from Dell
- AirWatch Auto-Discovery enabled for your environment

Procedure

To configure Windows 10 Provisioning Service by VMware AirWatch:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Auto Enrollment**.
2. Configure the Auto Enrollment settings:

| Settings | Description |
|---------------------------------------|--|
| Auto Enrollment | Select Enable to use Windows 10 Provisioning Service by VMware AirWatch |
| Sync Interval | Select the amount of time between sync attempts between the AirWatch Provisioning Agent and the AirWatch Console. |
| Enforce Policies Before Log In | Select Enable to enforce the device policies before the user logs in to the device. |
| Maximum Time Before Log In | Select the maximum number of minutes that may pass before a user logs in after completing the Out-of-Box-Experience. |

3. Select **Save**.
4. Register the device serial numbers with AirWatch. There are three workflows for registering devices:
 - a. Navigate to **Accounts > Users > Add > Add User** and add the user account. When you are done adding the user, select **Save and Add Device**. Then complete the Add Device settings. You must set the **Platform** to **Windows Desktop**.
 - b. Navigate to **Accounts > Users > Add > Batch Import**. Download and complete the CSV template for User and/or Device. Upload the CSV and select **Import**. You must enter **Windows Desktop** as the **Device Platform** when completing the template. You must set the **Platform** to **Windows Desktop**.
 - c. Navigate to **Devices Lifecycle > Enrollment Status > Add > Register Device**. You must set the **Platform** to **Windows Desktop**.

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 three different enrollment flows: Join Azure AD, Out of Box Experience enrollment, and Office 365 enrollment. All methods require configuring Azure AD integration with AirWatch.

For more information on configuring Active Directory in general, see the **Directory Services Guide** available on [AirWatch Resources](#).

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

Configure Azure AD Identity Services for SaaS Deployments

Before you can use Azure AD to enroll your Windows devices, you must configure AirWatch 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. Adding these details provides the Tenant ID and Name details for AirWatch and Azure to sync.

Prerequisites

If you are enrolling with a custom domain URL, the domain must be registered with the AirWatch Azure application. This registration requires the creation of a DNS record with your domain services provider. To register your domain, contact AirWatch Professional Services.

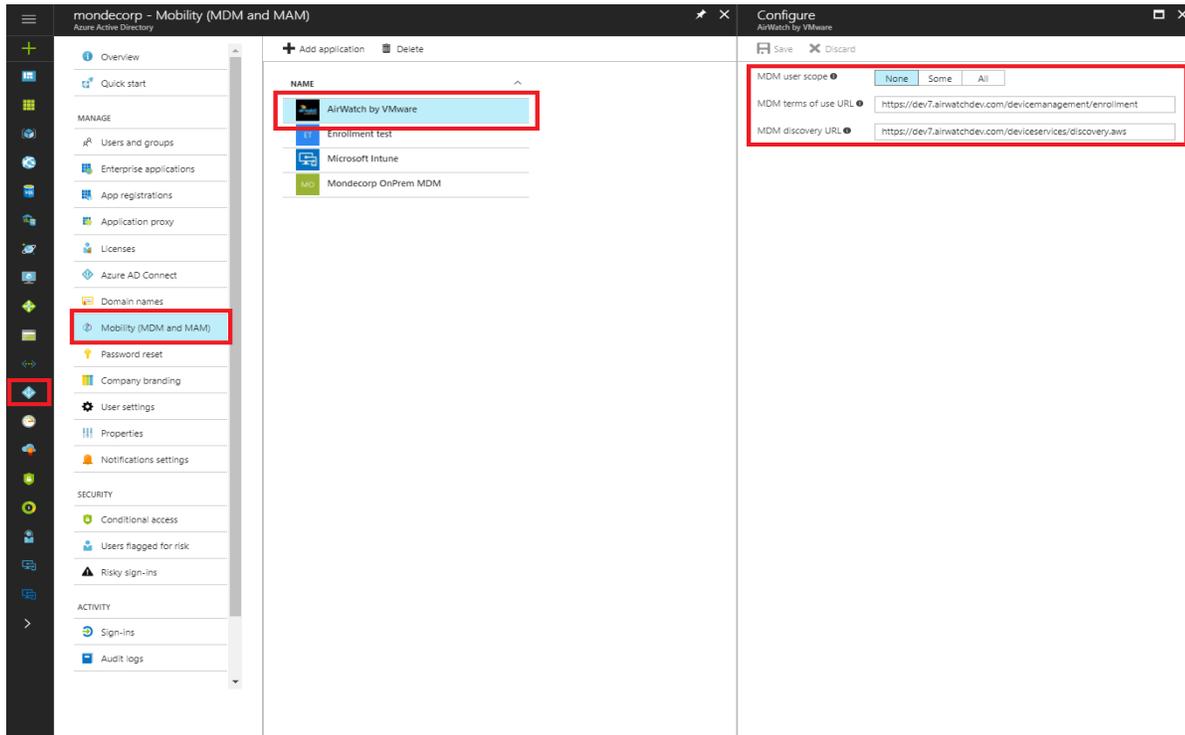
You must have a Premium Azure AD subscription to integrate Azure AD with AirWatch. Azure AD integration with AirWatch must be configured at the tenant where Active Directory (such as LDAP) is configured.

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.

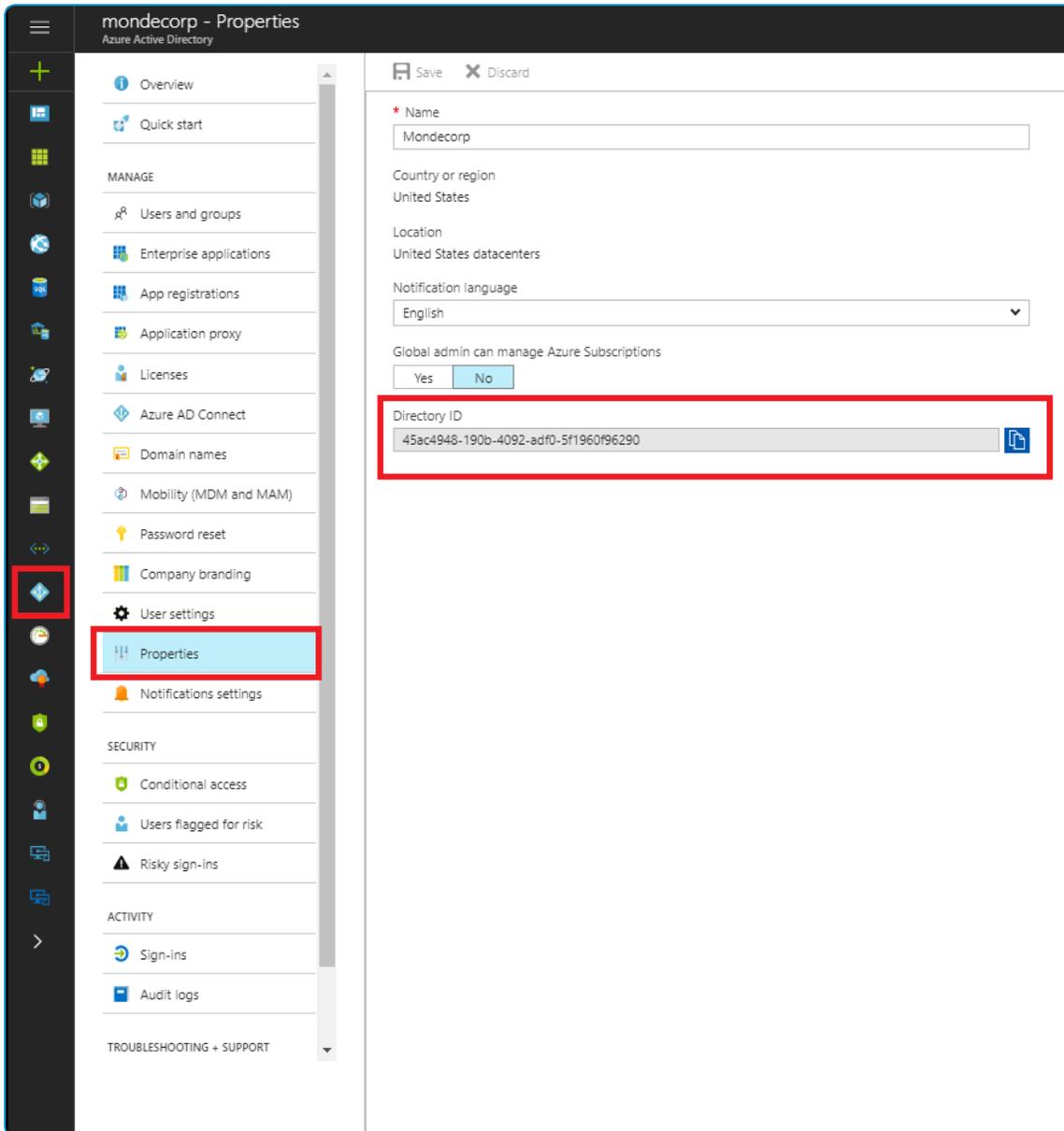
Procedure

To Configure Azure AD for Identity Services:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
2. Enable **Use Azure AD for Identity Services** under **Advanced** options.
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 (<https://portal.azure.com>) with your Microsoft account or organizational account.
4. Select your directory and navigate to the **Mobility (MDM and MAM)** tab. This was formerly the Applications tab.
5. Select **Add Application** and select the AirWatch by VMware application..



6. Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **All**.
7. Configure the AirWatch by VMware application by entering the **MDM Enrollment URL** and **MDM Terms of Use URLs** from the AirWatch Console. Then configure the **Manage devices for these users settings** based on your organization rules. Select **Save** to continue.
8. Navigate to the **Properties** tab to find the **Azure Directory ID**. This was formerly called the **Tenant ID**.



9. Select the User Account Details option 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.
10. Return to the AirWatch Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.
11. Enter the **Azure Directory ID** as the **Tenant Identifier**. Enter the name of your Azure Directory as the **Tenant Name**.
12. Select **Save** to complete the process.

Configure Azure AD Identity Services for On-premises Deployments

Before you can use Azure AD to enroll your Windows devices, you must configure AirWatch 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.

If you are using an on-premises deployment, you must follow these steps.

Prerequisites

If you are enrolling with a custom domain enrollment URL (SaaS-dedicated or On-Premises), the domain must be registered with the AirWatch Azure application. This registration requires the creation of a DNS record with your domain services provider. To register your domain, contact AirWatch Professional Services.

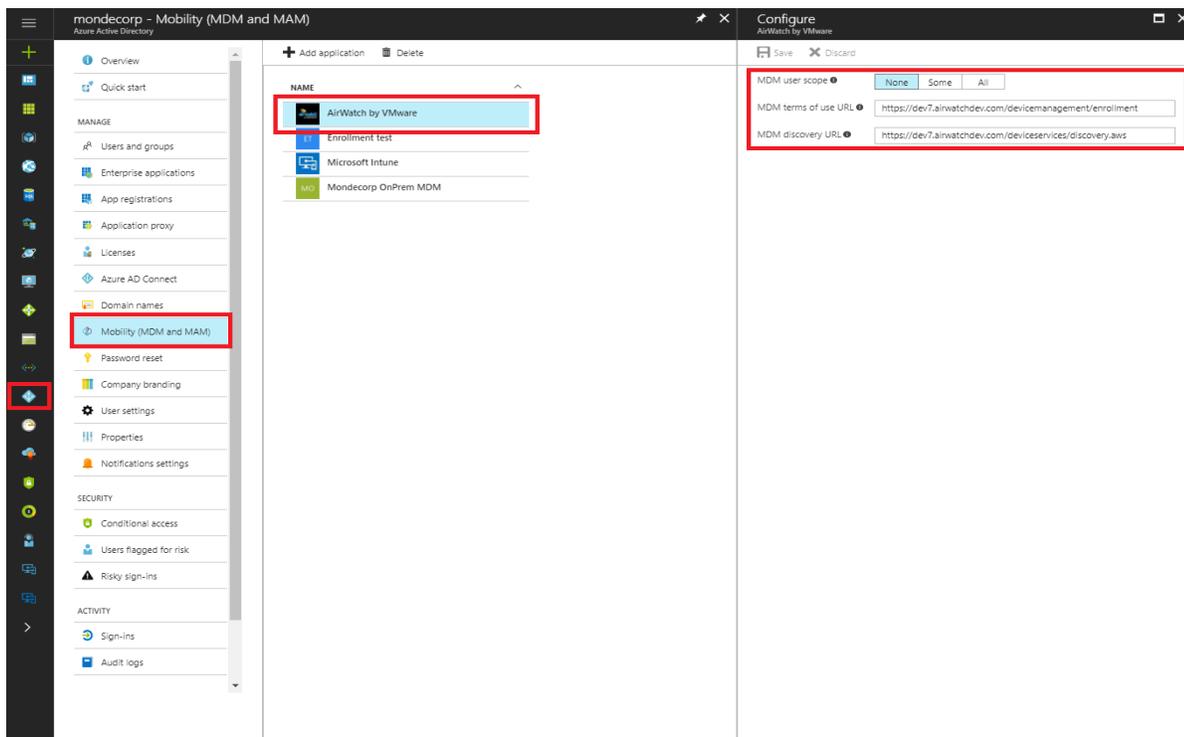
You must have a Premium Azure AD subscription to integrate Azure AD with AirWatch. Azure AD integration with AirWatch must be configured at the tenant where Active Directory (such as LDAP) is configured.

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.

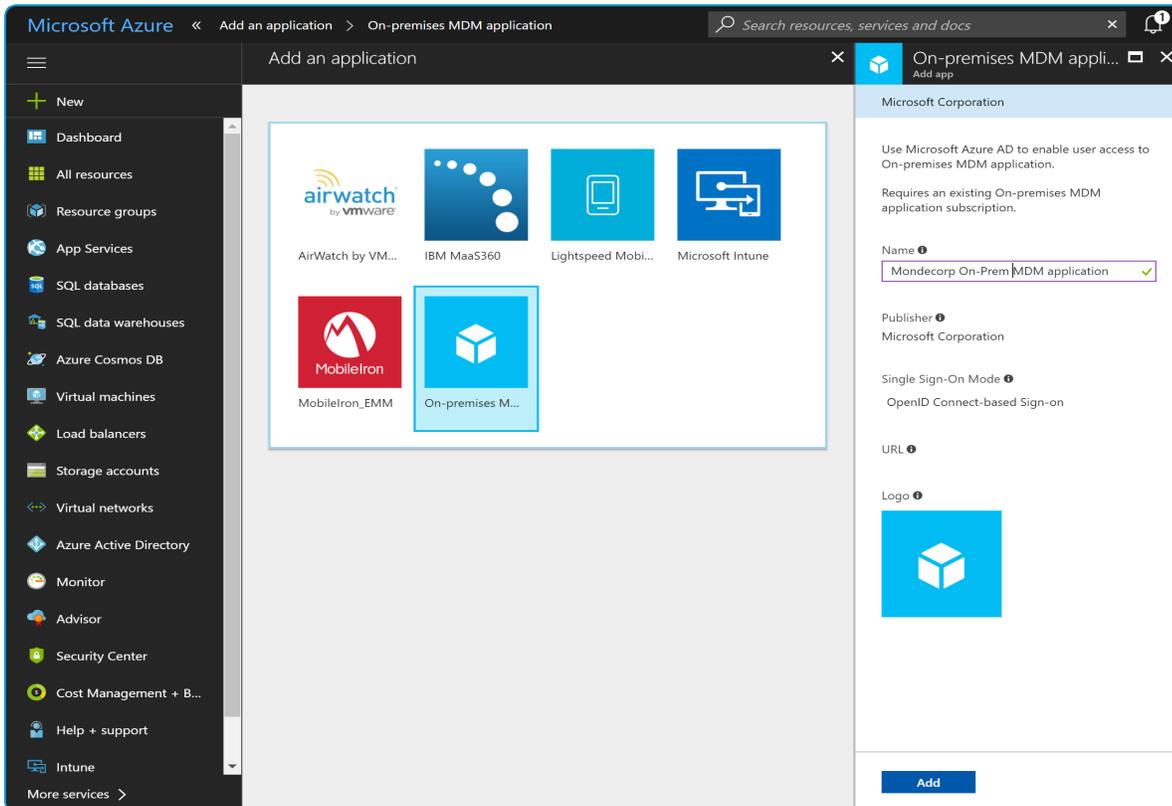
Procedure

To Configure Azure AD for Identity Services:

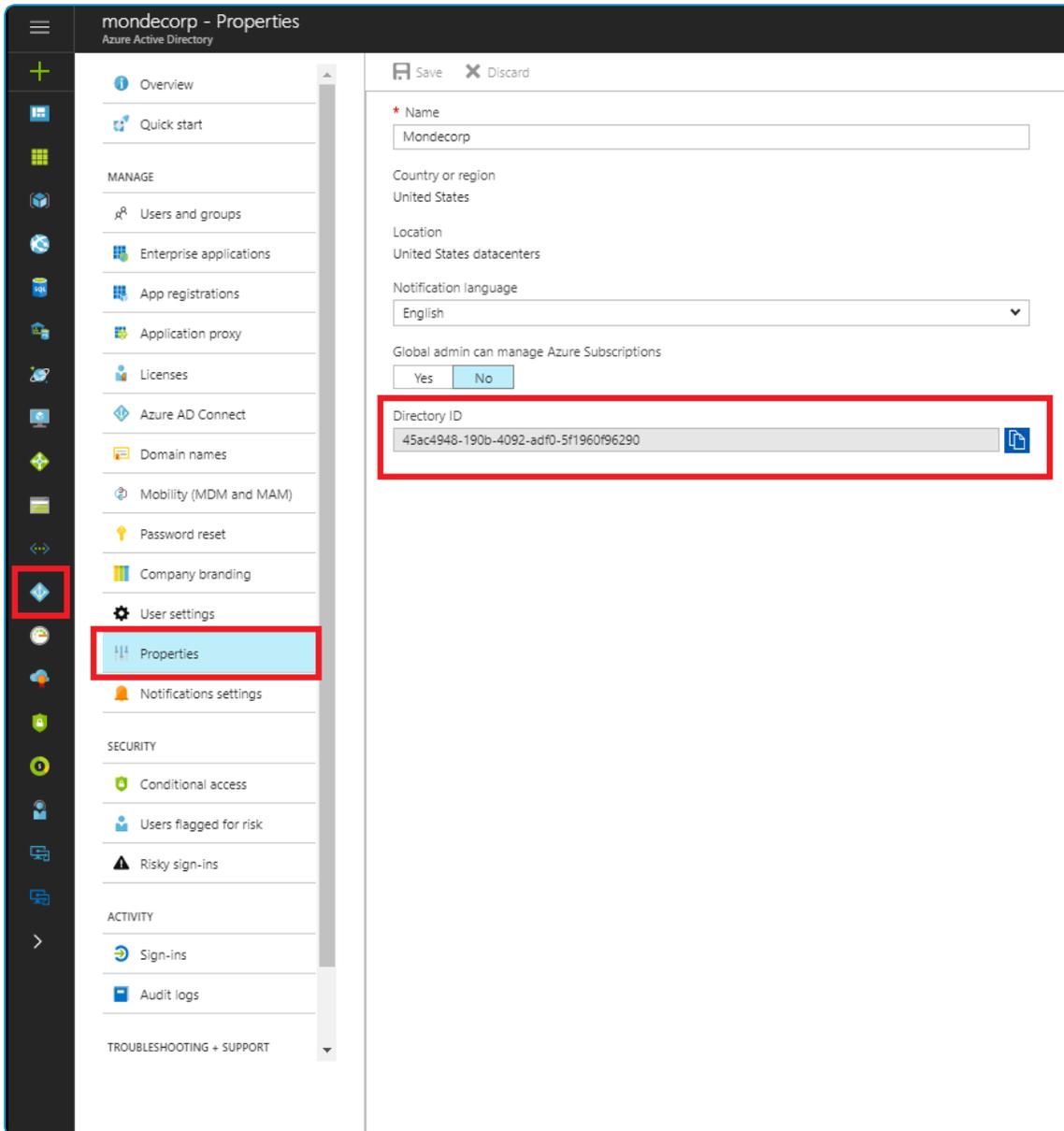
1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
2. Enable **Use Azure AD for Identity Services** under **Advanced** options.
Once enabled, take note of the MDM Enrollment and MDM Terms of Use URLs as they are needed when configuring the Azure 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 was formerly the Applications tab.
5. Select **Add Application** and select the AirWatch by VMware application..



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



7. Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **None**.
8. Configure the On Premises MDM application by entering the **MDM Enrollment URL** and **MDM Terms of Use URLs** from the AirWatch Console.
9. Change the Permissions as follows:
 - Application Permissions
 - Select **Read and write directory data**.
 - Select **Read and write devices**.
 - Delegated Permissions
 - Select **Access the directory as the signed-in user**.
 - Select **Read directory data**.
 - Select **Sign in and read user profile**.
10. Set the **Single-sign on** settings and enter your device services url in the **APP ID URL** textbox.
Example format: https:// <MDM DS SERVER>
11. Set **MDM user scope** to **All**. Select **Save** to continue.
12. Navigate to the Properties tab to find the Azure Directory ID. This was formerly called the **Tenant ID**.



13. Select the User Account Details option 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.
14. Return to the AirWatch Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.
15. Return to the AirWatch Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.
16. Enter the **Azure Directory ID** as the **Tenant Identifier**. Enter the name of your Azure Directory as the **Tenant Name**.
17. Select **Save** to complete the process.

Enroll a Device With Azure AD

Enroll devices with Azure AD integration to enroll a device into the correct organization group in AirWatch automatically. Devices enrolled through Azure AD join completely, meaning all users on the device join the domain.

This enrollment flow is for devices not already joined to Azure AD. For more information on enrolling an Azure AD managed device, see [Enroll an Azure AD Managed Device into AirWatch on page 33](#).

To enroll a device through cloud domain-join:

1. Navigate on the Windows 10 device to **Settings > Accounts > Work Access > Join or Leave Azure AD > Join Azure AD**. Select **Continue**.
2. Enter your **Email Address** and **Password**. Select **Sign In**.
3. Ensure that the AirWatch welcome page displays. Select **Continue**.
4. Select **Accept** if terms of use are enabled.
5. Select **Join** to confirm that you want to enroll in AirWatch.
6. Select **Finish** to complete joining your device to AirWatch. Your device now downloads the applicable policies and profiles.

Enroll an Azure AD Managed Device into AirWatch

Devices that are joined to Azure AD use a different enrollment flow than devices enrolling through Azure AD integration. Use this enrollment flow to enroll a device that is already joined to Azure AD into AirWatch.

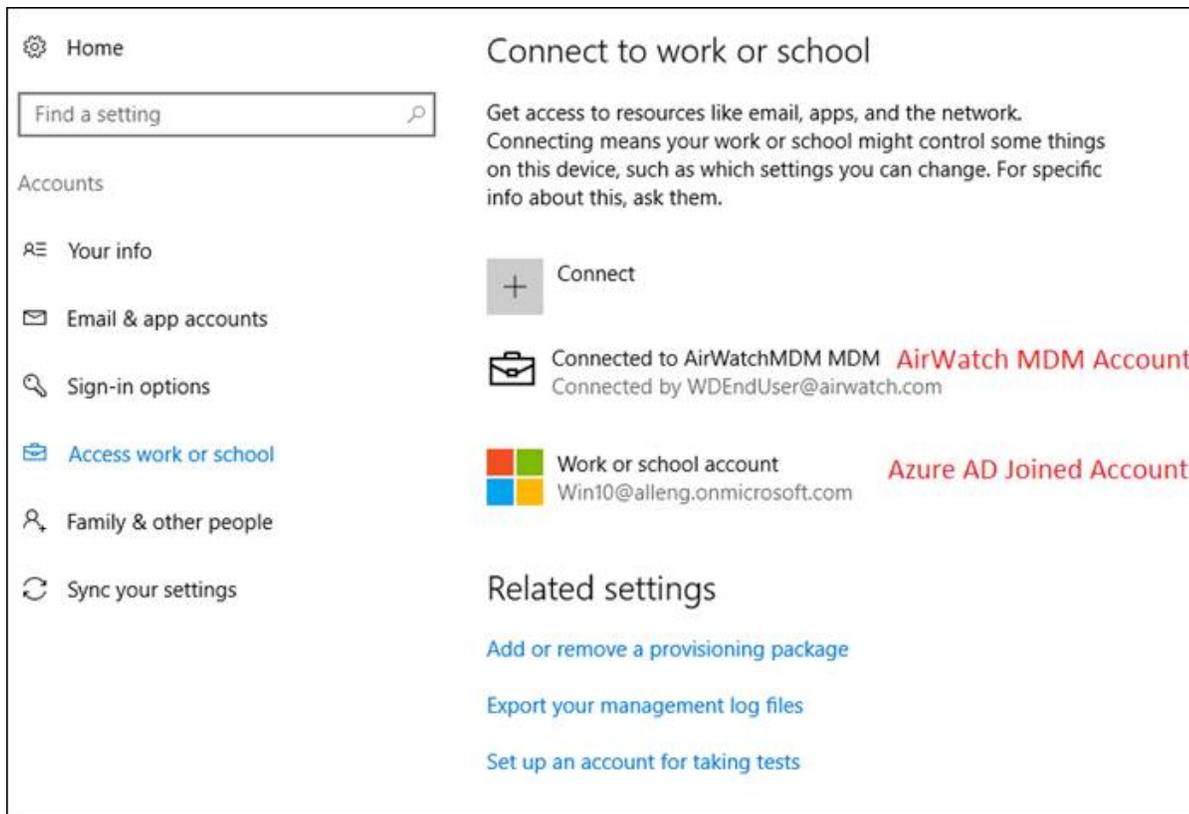
Requirements

- Windows 10 OS build 14393.82 and above.
- KB update KB3176934 installed
- No MDM applications installed under your Azure AD management portal
- Azure AD account configured on the device.

Procedure

1. On the device, navigate to **Settings > Accounts > Access work or school** and select **Enroll only in device management**.
You may also enroll through the VMware AirWatch Agent for Windows.
2. Complete the enrollment process. You must enter an email address with a different domain than your Azure AD account.
If you are using Windows Auto-Discovery, see [Enroll Through Work Access With Windows Auto Discovery on page 14](#).
If you are not using Windows Auto-Discovery, see [Enroll Through Work Access With Windows Auto Discovery on page 14](#).
3. Navigate to **Settings > Accounts > Access work or school** and ensure there is an Azure AD account and an AirWatch

MDM account added.

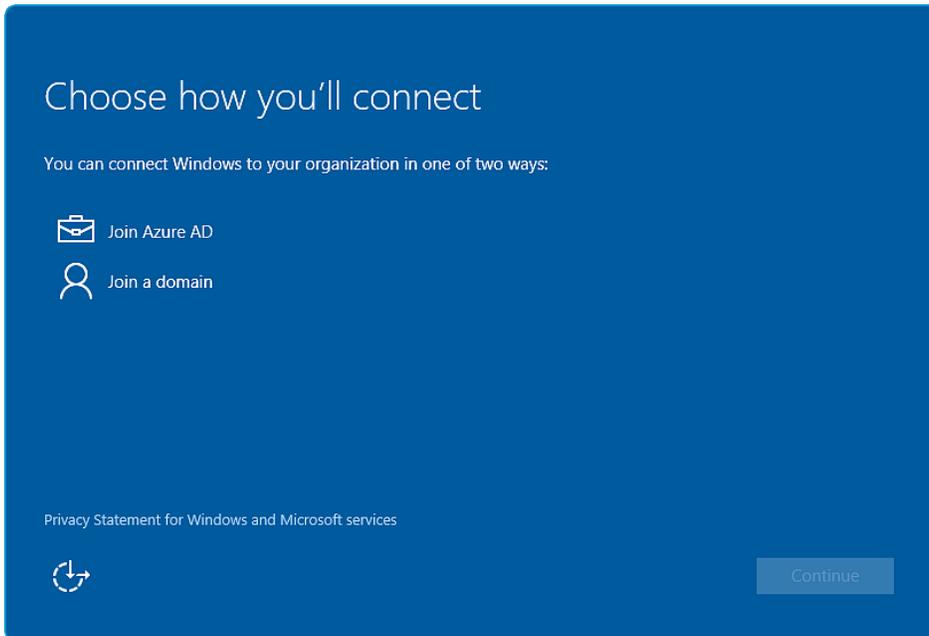


Enroll Through Out of Box Experience

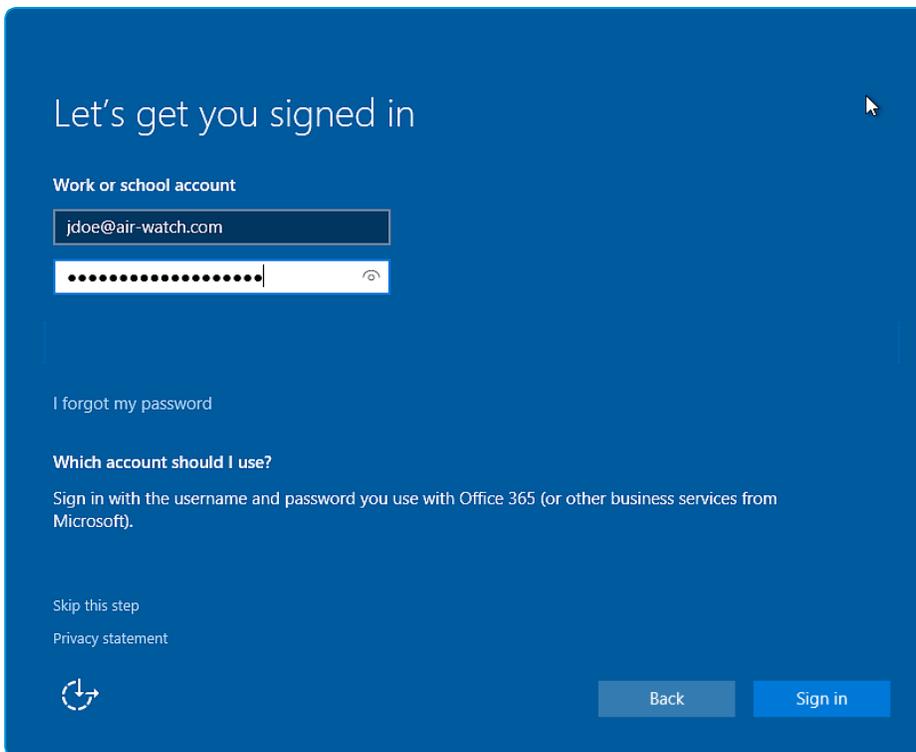
Out of Box Experience (OOBE) enrollment automatically enrolls a device into the correct organization group as part of the initial setup and configuration of a Windows 10 device.

To enroll a device with OOBE:

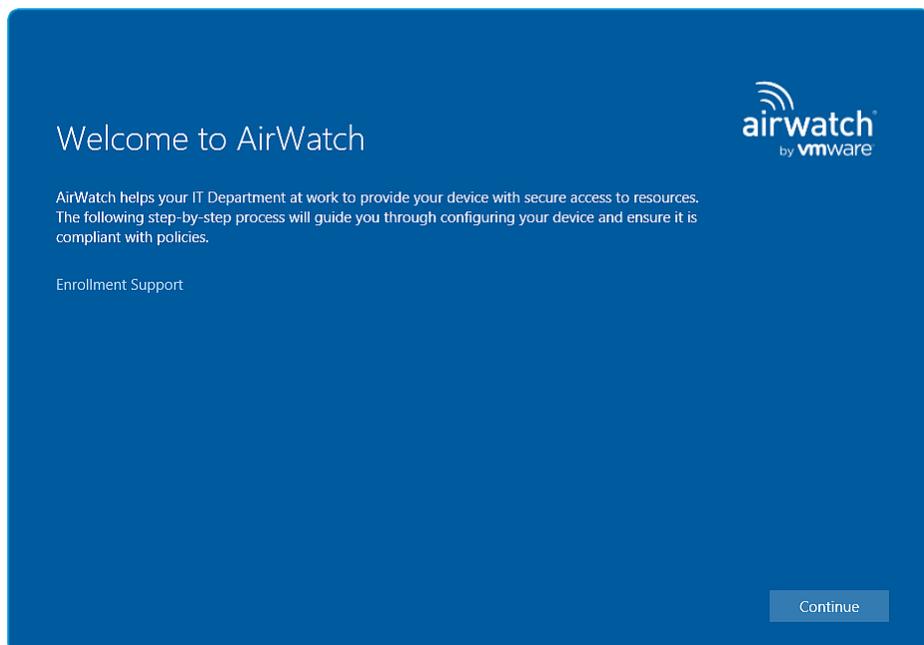
1. Power on the device and follow the steps to configure Windows until you reach the **Choose how you'll connect** screen.



2. Select **Join Azure AD**. Select **Continue**.
3. Enter your Azure AD/AirWatch email address as the **Work or school account**.



4. Enter your **Password**. Select **Sign In**.
5. Ensure that the **Welcome to AirWatch** screen displays. Select **Continue**.



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 Through Office 365 Apps

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

To enroll through Office 365 apps:

1. Select **Add a Work Account** the first time you open an Office 365 application.
2. Enter your **Email Address** and **Password**. Select **Sign In**.
3. Ensure that the AirWatch welcome page displays. Select **Continue**.
4. Select **Accept** if terms of use are enabled.
5. Select **Join** to confirm that you want to enroll in AirWatch.
6. Select **Finish** to complete joining your device to AirWatch. Your device now downloads the applicable policies and profiles.

Bulk Provisioning and Enrollment

Bulk provisioning creates a pre-configured package that stages Windows 10 devices and enrolls them into AirWatch. Use bulk provisioning to enroll and configure multiple devices with a standard user account quickly.

This enrollment flow is the only way to enroll a device with a standard user account. Admin permissions are still required to run the pre-configured package. Bulk provisioning only supports single user standard staging.

To use bulk provisioning, download the Microsoft Assessment and Development Kit and installing the Imaging and Configuration Designer (ICD) tool. The ICD creates provisioning packages used to image devices. As part of these provisioning packages, you can include AirWatch configuration settings so that provisioned devices are automatically enrolled into AirWatch during the initial Out of Box Experience (OOBE).

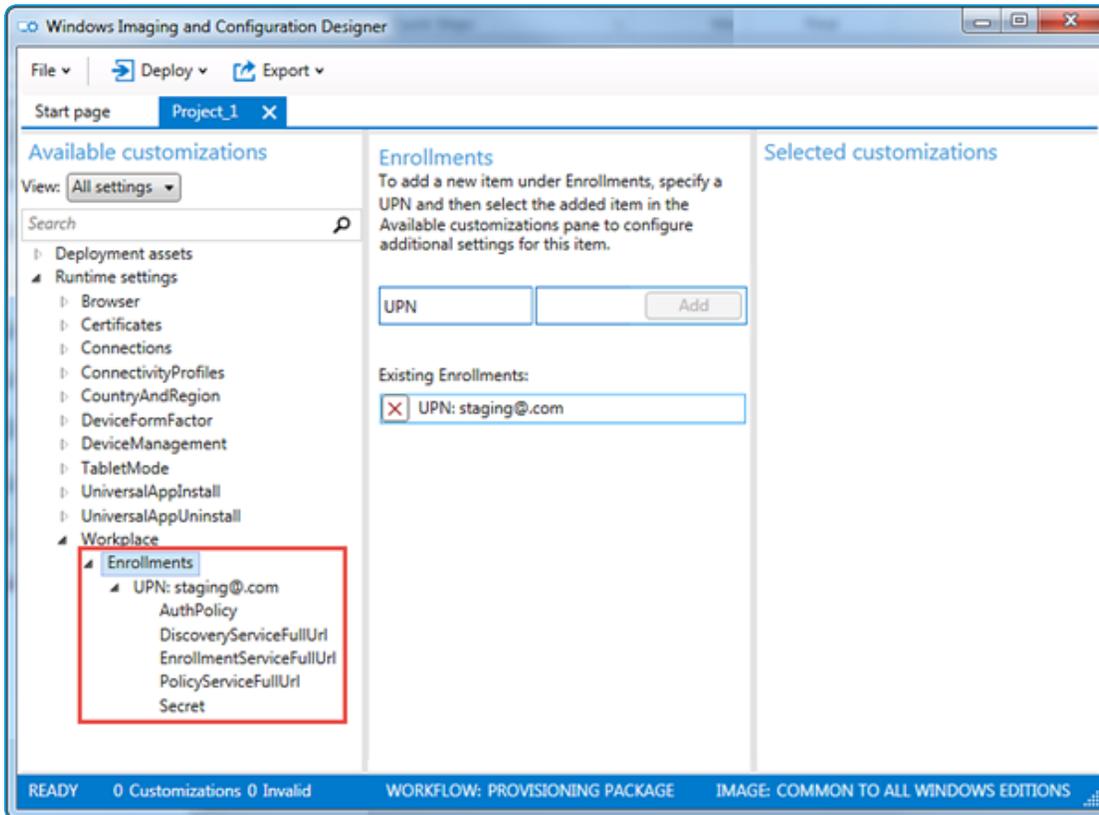
To map the devices to the correct end user automatically, register the devices per user or using a bulk import before creating the provisioning package. .

Enroll With Bulk Provisioning

The Microsoft Imaging and Configuration Designer tool allows you to create a provisioning package to enroll multiple Windows 10 devices into AirWatch quickly and easily. Once the package is installed, the device automatically enrolls into AirWatch.

To create a provisioning package:

1. Download the Microsoft Assessment and Deployment Kit for Windows 10 and install the Windows Imaging and Configuration Designer tool (ICD).
2. Start the Windows ICD and select **New Provisioning Package**.
3. Enter a **Project Name** and select the settings to view and configure.
The typical choice is the **Common to all Windows desktop editions** option.
4. (Optional) Import a provisioning package if you want to create a provisioning package based on the settings of a previous package.
5. Navigate to **Runtime Settings > Workplace > Enrollments**.
6. In the AirWatch Console, navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Staging and Provisioning**.
When you navigate to this settings page, a staging user is created and URLs pertaining to the created staging user display. You can create your own staging user for use with bulk provisioning but the settings displayed on this settings page do not apply to any created users.
7. Copy the **UPN** and paste it into the **UPN** text box of the ICD.
8. Select the down arrow next to **Enrollments** in the **Available Customizations** window.



9. Configure the following settings:
 - Select **AuthPolicy** and select the value displayed in the AirWatch Console.
 - Select **DiscoveryServiceFullURL** and copy the URL displayed in the AirWatch Console.
 - Select **EnrollmentServiceFullURL** and copy the URL displayed in the AirWatch Console.
 - Select **PolicyServiceFullURL** and copy the URL displayed in the AirWatch Console.
 - Select **Secret** and copy the value displayed in the AirWatch Console.
10. Select **File > Save** to save the project.
11. Select **Export > Provisioning Package** to create a package for use with bulk provisioning then select **Next**.
12. Save the **Encryption password** for later use if you choose to encrypt the package and then select **Next**.
13. Save the package to a USB drive for transfer to each device you want to provision. You can also email the package to the device.
14. Select **Build** to create the package.

Next Steps

Next you must install the bulk provisioning package. For more information, see [Install Bulk Provisioning Packages on page 39](#).

Install Bulk Provisioning Packages

After you create the provisioning packages using the Microsoft Imaging and Configuration Designer, you must install the provisioning package onto the end-user devices.

To install a provisioning package:

1. On the device you want to provision, navigate to **Settings > Accounts > Work Access** and select **Add or remove a package for work or school**. If the package was emailed, start the package from your mail client.
2. Select **Add a package** and select the **Removable Media** choice as the method to add the package.
3. Select the correct package from the list provided.

If you added the device to the user account in the AirWatch Console before provisioning, the device is assigned upon enrollment.

AirWatch Protection Agent for Enrollment

The AirWatch Protection Agent adds endpoint protection to ensure that your Windows Desktop devices remain secure. The agent allows AirWatch to use native Windows features to ensure device security.

By using the AirWatch Protection Agent, you can create profiles for devices to configure native BitLocker, Windows Firewall, and Windows Automatic Updates to your specific settings and preferences.

Important: The AirWatch Protection Agent does not support RT devices, as they have ARM processors and do not support legacy applications. Only Windows 8.1 or Windows 10 devices can use the functionality related to the AirWatch Protection Agent.

AirWatch Protection Agent Installation

After a device enrolls into AirWatch, the AirWatch Protection Agent silently installs on the device if enabled. This installation is automatic and does not require end-user interaction.

For users with a Windows 8.1 and Windows 10 Home device, the AirWatch Protection Agent must be manually installed following installation. End users start the installation by clicking the Web clip that appears on the device desktop. This Web clip only displays if AirWatch Protection Agent is enabled.

Pending Agent Status

While your device is in the Pending Agent status, no profiles, applications, or content push to the device. Profiles already deployed to the device are not removed either. The device is in a quarantine-like state. Once the AirWatch Protection Agent is downloaded and the status changes to enrolled, profiles and other content resume working.

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) enables real-time policy and command delivery to the AirWatch Protection Agent. Without AWCM, the AirWatch Protection Agent only receives policy and command delivery during its normal check-in intervals set in the AirWatch console. AirWatch recommends using AWCM for real-time policy and command delivery to Windows 8.1 and Windows 10 devices.

AirWatch Protection Agent Settings

The AirWatch Protection Agent offers only one configurable setting. You can set the Data Sample Interval Rate, which controls how often the agent checks in and queries the AirWatch Console for policy violations. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Agent Settings** to change the setting.

Enable the AirWatch Protection Agent

The AirWatch Protection Agent provides extra functionality for Windows Desktop devices. Enable the AirWatch Protection Agent before enrolling your Windows Desktop devices to ensure the full protection and security by AirWatch.

To enable the AirWatch Protection Agent:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Agent Application**.

2. Enable **Publish AirWatch Protection Agent**.

To ensure the AirWatch Protection Agent remains up to date, enable **Protection Agent Automatic Updates**. If a new version of the AirWatch Protection Agent is seeded into the AirWatch Console, end-user devices automatically update to the latest version.

3. Choose the **Device Ownership Type(s)** that require the AirWatch Protection Agent based on your choice.
4. Select **Save**.

Chapter 3:

Windows Desktop Device Profiles

| | |
|---|----|
| Windows Desktop Profiles Overview | 43 |
| Configure a Passcode Profile (Windows Desktop) | 44 |
| Configure a Wi-Fi Profile (Windows Desktop) | 46 |
| VPN Profile (Windows Desktop) | 48 |
| Credentials Profile (Windows Desktop) | 53 |
| Configure a Restrictions Payload (Windows Desktop) | 55 |
| Data Protection Profile (Windows Desktop) | 61 |
| Passport for Work Profile (Windows Desktop) | 64 |
| Configure a Firewall Profile (Windows Desktop) | 66 |
| Configure a Single App Mode Profile (Windows Desktop) | 67 |
| Configure an Antivirus Profile (Windows Desktop) | 68 |
| Encryption Profile (Windows Desktop) | 70 |
| Configure a Windows Updates Profile (Windows Desktop) .. | 74 |
| Configure a Web Clips Profile (Windows Desktop) | 81 |
| Exchange ActiveSync Profile (Windows Desktop) | 82 |
| SCEP Profile (Windows Desktop) | 87 |
| Application Control Profile (Windows Desktop) | 88 |
| Configure an Exchange Web Services Profile (Windows Desktop) | 91 |
| Create a Windows Licensing Profile (Windows Desktop) | 91 |
| Configure a BIOS Profile (Windows Desktop) | 92 |
| Configure the OEM Updates Profile (Windows Desktop) | 95 |

Use Custom Settings (Windows Desktop) 98

Windows Desktop Profiles Overview

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

A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload.

Windows Desktop profiles apply to a device at either the user level or the device level. When creating Windows Desktop profiles, you select the level the profile applies to. Some profiles can only be applied to the user level or device level.

Device Access

Some device profiles configure the settings for accessing a Windows Desktop 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 \(Windows Desktop\) on page 44](#)
- Configure the native Passport functionality. For more information, see [Passport for Work Profile \(Windows Desktop\) on page 64](#)
- Limit the device to a single application with a Single App Mode profile. For more information, see [Configure a Single App Mode Profile \(Windows Desktop\) on page 67](#).

Device Security

Ensure that your Windows Desktop 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 a Wi-Fi Profile \(Windows Desktop\) on page 46](#).
- Keep corporate data secure with the Data Protection profile. For more information, see [Data Protection Profile \(Windows Desktop\) on page 61](#).
- Ensure access to internal resources for your devices with the VPN profile. For more information, see [VPN Profile \(Windows Desktop\) on page 48](#).

Device Configuration

Configure the various settings of your Windows Desktop 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 Profile \(Windows Desktop\) on page 82](#).
- Restrict what applications can install on a device with the Application Control profile. For more information, see [Application Control Profile \(Windows Desktop\) on page 88](#).
- Ensure that the devices remain up to date with the Windows Updates profile. For more information, see [Configure a Windows Updates Profile \(Windows Desktop\) on page 74](#).

Configure a Passcode Profile (Windows Desktop)

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.

Passcodes set using this payload only take effect if the passcode is stricter than existing passcodes. For example, if the existing Microsoft Account passcode requires stricter settings than the Passcode payload requirements, the device continues to use the Microsoft Account passcode.

Important: The Passcode payload does not apply to domain-joined devices.

To configure a Passcode profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Passcode** profile.
6. Configure the Passcode settings:

| Settings | Descriptions |
|------------------------------------|--|
| Password Complexity | Set to Simple or Complex to your preferred level of password difficulty. |
| Require Alphanumeric | Enable to require the passcode to be an alphanumeric passcode. |
| Minimum Password Length | Enter the minimum number of characters a Password must contain. |
| Maximum Password Age (days) | Enter the maximum number of days that may elapse before the end user is required to change the Password. |

| Settings | Descriptions |
|--|---|
| Minimum Password Age (days) | Enter the minimum number of days that must elapse before the end user is required to change the Password. |
| Device Lock Timeout (in Minutes) | Enter the number of minutes before the device automatically locks and requires a passcode re-entry. |
| Maximum Number of Failed Attempts | Enter the maximum number of attempts the end user may enter before the device is restarted. |
| Password History (occurrences) | Enter the number of occurrences a password is remembered. If the end user reuses a password within the number of recorded occurrences, they cannot reuse that password. For example, if you set the history to 12, an end user cannot reuse the past 12 passwords. |
| Reversible Encryption for Password Storage | Enable to set the operating system to store passwords using reversible encryption. Storing passwords using reversible encryption is essentially the same as storing plain text versions of the passwords. For this reason, do not enable this policy unless application requirements outweigh the need to protect password information. |
| Use Protection Agent for Windows 10 Devices | Enable to use the AirWatch Protection Agent to enforce Password profile settings instead of the native DM functionality. Enable this settings if you have issues using the native DM functionality. |
| Windows 8.0 Password Policy | Enable to use the legacy Windows 8.0 Password Policy. See Windows 8.0 Password Policy on page 45 . |
| Expire Password | Enable to expire the existing password on the device and require a new password to be created. Requires AirWatch Protection Agent to be installed on the device. |

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

Windows 8.0 Password Policy

If you enable the Windows 8.0 Password Policy, configure the following settings.

Note: Consider upgrading your Windows Desktop devices to Windows 8.1. It is a free upgrade that allows for more MDM capabilities.

| Settings | Descriptions |
|------------------------------------|--|
| Allow Simple Value | Enable to allow end users to use simple passcodes. Disable to force passcodes to meet complexity settings. |
| Require Alpha Numeric Value | Enable to require the end user to create a passcode using minimum length and minimum number of complex characters. |

| Settings | Descriptions |
|---|---|
| Minimum Number of Complex Characters | Enter the minimum number of complex characters (lowercase, uppercase, symbols, and numbers) required for a passcode. |
| Minimum Password Length | Enter the number of characters a passcode must contain as a minimum. |
| Maximum Passcode Age (days) | Enter the number of days that may elapse before the end user is required to change the passcode. |
| Maximum Number of Failed Attempts | Enter the maximum number of attempts the end user may enter before the device is restarted. |
| Device Lock Timeout (in Minutes) | Enter the number of minutes before the device automatically locks and requires a passcode re-entry. |
| Passcode History | Enter the number of occurrences a password is remembered. If the end user reuses a password within the number of recorded occurrences, the user cannot reuse that password. For example, if you set the history to 12, an end user cannot reuse the past 12 passwords. |

Configure a Wi-Fi Profile (Windows Desktop)

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 need access to multiple networks or for configuring devices to connect automatically to the appropriate wireless network.

 Looking to use certificate-based EAP authentication for VPN and Wi-Fi profiles? See the Knowledge Base article: <https://support.air-watch.com/articles/115001664448>.

To configure a Wi-Fi payload:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Wi-Fi** profile.
6. Configure the **General** settings:

| Settings | Descriptions |
|---------------------------------------|--|
| Service Set Identifier | Enter an identifier that is associated with the name (SSID) of the desired Wi-Fi network. The SSID cannot contain spaces. |
| Hidden Network | Enable if the network is not open to broadcast. |
| Auto-Join | Enable to set the device to join the network automatically. |
| Security Type | Use the drop-down menu to select the security type (for example, WPA2 Personal) for the Wi-Fi network. |
| Encryption | Use the drop-down menu to select the encryption type used. Displays based on the Security Type . |
| Password | Enter the password required to join the Wi-Fi network for networks with static passwords. Select the Show Characters check box to disable hidden characters within the text box. Displays based on the Security Type . |
| Proxy | |
| 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 | |
| Protocols | Select the type of protocols to use: <ul style="list-style-type: none"> • Certificate • EAP-TTLS • PEAP-MsChapv2 • Custom This section displays when the Security Type is set to WPA Enterprise or WPA2 Enterprise. |
| Authentication | |
| Inner Identity | Select the method of authentication through EAP-TTLS: <ul style="list-style-type: none"> • Username/Password • Certificate This section displays when the Protocols option is set to EAP-TTLS or PEAP-MsChapv2. |
| Require Crypto Binding | Enable to require cryptographic binding on both authentications. This limits man-in-the-middle attacks. |
| Use Windows Log On Credentials | Enable to use the Windows login credentials are the user name/password to authenticate. Displays when Username/Password is set as the Inner Identity . |
| Identity Certificate | Select an Identity Certificate, which you can configure using the Credentials payload. See Credentials Profile (Windows Desktop) on page 53 for more information. Displays when Certificate is set as the Inner Identity . |

| Settings | Descriptions |
|-------------------------------|---|
| Trust | |
| Trusted Certificates | Select Add to add Trusted Certificates to the Wi-Fi profile. 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 box. |

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

VPN Profile (Windows Desktop)

AirWatch supports configuring device VPN settings so end users can remotely and securely access your organizations internal network. The VPN profile provides detailed 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
- L2TP
- PPTP
- Check Point Mobile
- F5 Edge Client
- Juniper Pulse
- Sonic Wall Mobile Connect
- Automatic
- VMware Tunnel
- GlobalProtect

Per-app VPN

Per-app VPN lets you to configure VPN traffic rules based on specific applications. When configured, the VPN connects automatically when a specified app starts and sends the application traffic through the VPN connection but not traffic from other applications. With this flexibility, you can ensure that your data remains secure while not limiting device 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.

VPN TRAFFIC RULES

Per-app VPN Rules ⓘ

Policies follow OR logic operator

| | | |
|-------------------|---------------------------------------|----|
| Application ID | AirWatchLLC.AirWatchMDMagen ⓘ | 10 |
| VPN On Demand | <input checked="" type="checkbox"/> ⓘ | |
| Routing Policy | Force All Traffic Through VPN ▾ | |
| DNS Routing Rules | <input type="checkbox"/> ⓘ | ✕ |
| Application ID | %ProgramFiles%/Internet Explor ⓘ | 10 |
| VPN On Demand | <input checked="" type="checkbox"/> ⓘ | |
| Routing Policy | Allow Direct Access to Extern ▾ | |
| DNS Routing Rules | <input checked="" type="checkbox"/> ⓘ | ✕ |

| Filter Type | Filter Value | |
|--------------|--------------|---|
| IPAddress ▾ | 10.64.0.123 | ✕ |
| Ports ▾ | 80,100-500 | ✕ |
| IPProtocol ▾ | 6 | ✕ |

Filter Types follow AND logic operator

✕ Add New Per App VPN Rule

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 must 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 Desktop)

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

Looking to use certificate-based EAP authentication for VPN and Wi-Fi profiles? See the Knowledge Base article : <https://support.air-watch.com/articles/115001664448>

To enforce a VPN profile:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile** or **Device Profile**.
4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **VPN** profile.
6. Configure the **Connection Info** settings:

| Settings | Descriptions |
|-------------------------------------|---|
| Connection Name | Enter the name of the VPN connection. |
| Connection Type | Select the type of VPN connection: |
| Server | Enter the VPN server hostname or IP Address. |
| Port | Enter the port the VPN server uses. |
| Advanced Connection Settings | Enable to configure advanced routing rules for device VPN connection. |
| Routing Addresses | Select Add to enter the IP Addresses and Subnet Prefix Size of the VPN server. You may add more routing addresses as needed. |
| DNS Routing Rules | Select Add to enter the Domain Name that governs when to use the VPN. Enter the DNS Servers and Web Proxy Servers to use for each specific domain. |
| Routing Policy | Choose either to Force All Traffic Through VPN or Allow Direct Access to External Resources . <ul style="list-style-type: none"> • Force All Traffic Through VPN (Force Tunnel): For this traffic rule, all IP traffic must go through the VPN Interface only. • Allow Direct Access to External Resources (Split Tunnel): For this traffic filter rule, only the traffic meant for the VPN interface (as determined by the networking stack) goes over the interface. Internet traffic can continue to go over the other interfaces. |
| Proxy | Select Auto Detect to detect automatically 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 . |

| Settings | Descriptions |
|---------------------------------------|---|
| Bypass proxy for local | Enable to bypass the proxy server when the device detects it is on the local network. |
| Authentication | |
| Protocol | Select the authentication protocol for the VPN: <ul style="list-style-type: none"> • EAP – Allows for various authentication methods • Machine Certificate – Detects a client certificate in the device certificate store to use for authentication. |
| EAP Type | Select the type of EAP authentication: <ul style="list-style-type: none"> • EAP-TLS – Smart Card or client certificate authentication • EAP-MSCHAPv2 – User name and Password • EAP-TTLS • PEAP • Custom Configuration – Allows all EAP configurations <p>Displays only if Protocol is set to EAP.</p> |
| 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 display by the most recent certificated issued for each entity. 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 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. |

| Settings | Descriptions |
|--------------------------|---|
| VPN Traffic Rules | |
| Per-app VPN Rules | Select Add to add traffic rules for specific Legacy and Modern applications. For more information on Per-app VPN, see Per-app VPN on page 48 |
| Application ID | <p>First select whether the app is a Store App or a Desktop App. Then enter the application file path for Desktop apps or package family name for Store Apps to specify the app the traffic rules apply to.</p> <ul style="list-style-type: none"> • File Path example: %ProgramFiles%/ Internet Explorer/iexplore.exe • Package Family Name example: AirWatchLLC.AirWatchMDMAgent_htcwk4rx2gx4 <p>The PFN Lookup allows you to search for the application PFN by selecting the Search icon. A display window opens allowing you to select the app you want to configure Per-app VPN rules to govern. The PFN is then autopopulated.</p> |
| VPN On Demand | Enable to have the VPN connection automatically connect when the application is launched. |
| Routing Policy | <p>Select the routing policy for the app.</p> <ul style="list-style-type: none"> • Allow Direct Access to External Resources allows for both VPN traffic and traffic through the local network connection. • Force All Traffic Through VPN forces all traffic through the VPN. |
| DNS Routing Rules | <p>Enable to add DNS routing rules for the app traffic.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 Protocol: Numeric value from 0-255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17. <p>For more information on how these filters and policies function and the logic used, see Per-app VPN on page 48.</p> |

| Settings | Descriptions |
|--|--|
| Device Wide VPN Rules | <p>Select Add to add traffic rules for the entire device.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 Protocol: Numeric value from 0–255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17. |
| Policies | |
| Remember Credentials | Enable to remember the end user login credentials. |
| Always On | Enable to force the VPN connection to be always on. |
| VPN Lockdown | <p>Enable to force the VPN to always be on, never disconnect, disable any network access if the VPN is not connected, and prevent other VPN profiles from connecting on the device.</p> <p>A VPN profile with VPN Lockdown enabled must be deleted before you push a new VPN profile to the device.</p> |
| Bypass for Local | Enable to bypass the VPN connection for local intranet traffic. |
| Trusted Network Detection | Enter, separated by commas, trusted network addresses. The VPN does not connect when a trusted network connection is detected |
| Domain Name Resolution via VMware Tunnel Server | |
| Domain | <p>Select Add New Domain to add domains to resolve through the VMware Tunnel server.</p> <p>Any domains added resolve through the VMware Tunnel server regardless of the app originating the traffic. For example, if you add www.air-watch.com, any traffic to that domain routes through the VMware Tunnel server if it comes from the configured Chrome app and the not-configured Edge app.</p> <p>This option only displays when you create the VPN profile as a user profile.</p> |

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

Credentials Profile (Windows Desktop)

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 Desktop 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.

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.

For Windows 8.1 devices, Personal certificates require the SCEP payload and the AirWatch Protection Agent on the device.

 Looking to use certificate-based EAP authentication for VPN and Wi-Fi profiles? See the Knowledge Base article : <https://support.air-watch.com/articles/115001664448>

Configure a Credentials Profile (Windows Desktop)

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

To configure a Credentials payload:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile** or **Device Profile**.
4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Credentials** payload and configure the following settings:

| Settings | Descriptions |
|------------------------------|---|
| Credential Source | Select the credential source as either an Upload , a Defined Certificate Authority , or User Certificate . The remaining payload options are source-dependent. <ul style="list-style-type: none"> • 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. • 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. This setting displays when Upload is selected as the Credential Source . |
| Certificate Authority | Use the drop-down menu to select a predefined certificate authority. 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. This setting displays when Defined Certificate Authority is selected as the Credential Source . |

| Settings | Descriptions |
|---------------------------|---|
| Export Private Key | Select Allow to let end users export certificates using Windows Certificate Manager. Select Don't Allow to prohibit end users from exporting certificates. |
| Key Location | Select the location for the certificate private key: <ul style="list-style-type: none"> • 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 OS. • 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. • Software – Select to store the private key in the device OS. • Passport – Select to save the private key within the Microsoft Passport. This option requires the Azure AD integration. |
| Certificate Store | Select the appropriate certificate store for the credential to reside in on the device: <ul style="list-style-type: none"> • Personal – Select to store personal certificates. Personal certificates require the AirWatch Protection Agent on the device or using the SCEP payload. • Intermediate – Select to store certificates from Intermediate Certificate Authorities. • Trusted Root – Select to store certificates from Trusted Certificate Authorities and root certificates from your organization and Microsoft. • Trusted Publisher – Select to store certificates from Trusted Certificates Authorities trusted by software restriction policies. • Trusted People – Select to store certificates from trusted people or end entities that are explicitly trusted. Often these certificates are self-signed certificates or certificates explicitly trusted in an application such as Microsoft Outlook. |
| Store Location | Select User or Machine to define where the certificate is located. |
| S/MIME | Select whether the S/MIME certificate is for encryption or signing. |

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

Configure a Restrictions Payload (Windows Desktop)

Deploy a restrictions payload for added security on Windows Desktop devices. Use the Restrictions payload to disable end-user access to device features to ensure that devices are not tampered with.

The Windows version and edition you use change what restrictions apply to a device.

To enforce a Restrictions profile:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select **Windows** and then select **Windows Desktop**.

3. Select **Device Profile**.4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Restrictions** profile.6. Configure the **Administration** settings:

| Settings | Descriptions |
|---|---|
| Allow Manual MDM Unenrollment | <p>Allow the end user to unenroll from AirWatch manually through the Workplace/Work Access enrollment.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Security and Privacy | |
| Runtime Configuration Agent to Install Provisioning Packages | <p>Enable to allow the use of provisioning packages to enroll devices into AirWatch (bulk provisioning).</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Location | <p>Select how location services run on the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Runtime Configuration Agent to Remove Provisioning Packages | <p>Enable to allow the removal of provisioning packages.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow the Device to Send Diagnostic and Usage Telemetry Data | <p>Enable to allow the device to send diagnostic and usage telemetry data to the AirWatch Console.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Require Microsoft Account for MDM | <p>Enable to require a Microsoft Account for devices to receive policies or applications.</p> |
| Require of Microsoft Account for Modern Applications | <p>Enable to require a Microsoft Account for devices to download and install Windows Apps.</p> |
| Provisioning Packages Must Have a Certificate Signed by a Device Trusted Authority | <p>Enable to require a trusted certificate for all provisioning packages (bulk provisioning).</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |

| Settings | Descriptions |
|--|---|
| Settings | |
| Allow User to Change Auto Play Settings | <p>Allow the user to change what program is used for Auto Play of file types.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow User to Change Data Sense Settings | <p>Allow the user to change the Data Sense settings to restrict data use on the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Date/Time | <p>Allow the user to change the Date/Time settings.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Language | <p>Allow the user to change the language settings.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow User to Change Power and Sleep Settings | <p>Allow the user to change the Power and Sleep settings.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Region | <p>Allow the user to change the region.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow User to Change Sign-In Options | <p>Allow the user to change the Sign-In Options.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| VPN | <p>Allow the user to change the VPN settings.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow User to Change Workplace Settings | <p>Allow the user to change Workplace settings and change how MDM functions on the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow the User to Change Account Settings | <p>Allow the user to change Account settings.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Bluetooth | |
| Bluetooth | <p>Allow the use of Bluetooth on the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |

| Settings | Descriptions |
|--|---|
| Device Bluetooth Advertising | <p>Allow the device to broadcast Bluetooth Advertisements.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Bluetooth-enabled devices can discover the device | <p>Allow Bluetooth discovery of the device by other Bluetooth devices.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Device Functionality | |
| Camera | <p>Allow access the camera function of the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Cortana | <p>Allow access to the Cortana application.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Device Discovery UX on the Lock Screen | <p>Allow the device discovery UX on the lock screen to discover projectors and other displays.</p> <p>When enabled, the Win+P and Win+K shortcuts do not work.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| IME Logging | <p>Enable to allow the user to turn on and off the logging for incorrect conversions and saving of auto-tuning result to a file and history-based predictive input.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| IME Network Access | <p>Enable to allow the user to turn on the Open Extended Dictionary to integrate Internet searches to provide input suggestions that do not exist in a devices local dictionary.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Smart Screen | <p>Enable to allow the end user to use the Microsoft SmartScreen feature, which is a form of security requesting the end user to draw shapes on an image to unlock the device. This option also allows end users to use PINs as their passcode.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: After you disable function, you cannot reenale it through AirWatch MDM. To reenale it, you must factory reset the device.</p> </div> <p>This restriction applies to both Windows 8.1 and Windows 10 devices. The restriction does not apply to Windows 10 Home edition devices.</p> |

| Settings | Descriptions |
|--|---|
| Search to Leverage Location Information | <p>Allow the search to use the device location information.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Storage Card | <p>Enable to allow the use of an SD card.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Windows Sync Settings | <p>Allow user to sync Windows settings across devices.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Windows Tips | <p>Allow Windows Tips on the device to help the user.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| User Account Control Setting | <p>Select the level of notification sent to end users when a change to the operating system requires device admin permission.</p> |
| Applications | |
| Allow Non-Microsoft Store Trusted Applications | <p>Allows the downloading and installation of applications not trusted by the Microsoft Store.</p> <p>This restriction applies to all Windows 10 devices.</p> |
| App Store Auto Updates | <p>Enable to allow apps downloaded from the Microsoft Store to update automatically when new versions are available.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow Developer Unlock | <p>Allows the use of the Developer Unlock setting for sideloading applications onto devices.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow DVR & Game Broadcasting | <p>Enable to allow the recording and broadcasting of games on the device.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Allow Share Data Among Multiple Users of the Same App | <p>Allows sharing of data between multiple users of an app.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Restrict App Data to System Volume | <p>Restricts app data to the same volume as the OS instead of secondary volumes or removable media.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |

| Settings | Descriptions |
|--|--|
| Restrict Installation of Applications to System Drive | <p>Restricts the installation of apps to the system drive instead of secondary drives or removable media.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Network | |
| Auto Connect to Wi-Fi Hotspots | <p>Enable to allow the device to connect to Wi-Fi hotspots automatically using the Wi-Fi Sense functionality.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Cellular Data On Roaming | <p>Enable to allow cellular data use while roaming.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Internet Sharing | <p>Enable to allow Internet sharing between devices.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Data Usage on Roaming | <p>Enable to allow end users to transmit and receive data while roaming.</p> <p>This restriction applies to all Windows devices.</p> |
| VPN Over Cellular | <p>Allow the use of a VPN over cellular data connections.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| VPN Roaming Over Cellular | <p>Allow the use of a VPN while on roaming cellular data connections.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Edge Browser | |
| Auto fill | <p>Allow the use of Auto fill to complete user information.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Cookies | <p>Allow the use of cookies.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Do Not Track | <p>Allow the use of Do Not Track requests.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |
| Password Manager | <p>Allow the use of a password manager.</p> <p>This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.</p> |

| Settings | Descriptions |
|---|--|
| Pop-ups | Allow pop-up browser windows. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices. |
| Search Suggestions in Address Bar | Allow search suggestions to appear in address bar. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices. |
| Smart Screen | Allow the use of the SmartScreen malicious site and content filter. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices. |
| Send Intranet Traffic to Internet Explorer | Allow intranet traffic to use Internet Explorer. This restriction applies to all Windows 10 devices. |
| Enterprise Site List URL | Enter the URL for an enterprise site list. This restriction applies to all Windows 10 devices. |

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

Data Protection Profile (Windows Desktop)

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.

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 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 Desktop)

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.

To configure the Enterprise Data Protection profile:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and choose **Windows Desktop** as the platform.'
3. Select **Device Profile**.
4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

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 whether the application is a traditional desktop application or a Microsoft Store app. You can also select an application publisher for desktop applications or store apps. 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 file path for a desktop application or the package family name for a store app. |

| Settings | Descriptions |
|--|---|
| 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. |
| Protected Networks | |
| 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. |
| 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 <code>/*AppCompat*/</code> string to the setting. For example: <pre>www.air-watch.com /*AppCompat*/</pre> Only add the <code>/*AppCompat*/</code> string once to change the default setting. |
| Enforcement Policies | |
| Application Data Protection Level | Set the level of protection and the actions taken to protect enterprise data. |

| Settings | Descriptions |
|----------------------------------|---|
| 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. |
| 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 Desktop) on page 64. |

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

Create an Encrypting File System Certificate (Windows Desktop)

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.

To create an EFS certificate:

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 \(Windows Desktop\)](#) on page 62.

Passport for Work Profile (Windows Desktop)

Microsoft Passport provides a secure alternative to using passwords for security. The Passport for Work profile configures Microsoft Passport for your Windows Desktop 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 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. After authentication through Passport, the device gains instant access to Web sites, applications, and networks.

Important: Passport for Work requires Azure AD integration to work.

Create a Windows Hello Profile (Windows Desktop)

Create a Windows Hello profile to configure Windows Hello for Business for your Windows Desktop devices so end users can access your applications, Web sites, and networks without entering a password.

Important: Windows Hello profiles only apply to devices enrolled through Azure AD integration.

To configure a **Passport** profile, follow the steps detailed below:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Windows Hello** profile and configure the settings:

| Settings | Descriptions |
|---------------------------|---|
| Biometric Gesture | Enable to allow end users to use the device biometric readers. |
| PIN requirements | |
| 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.

Configure a Firewall Profile (Windows Desktop)

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.

Important: The Firewall profile requires the AirWatch Protection Agent to be installed on the device.

To configure a Firewall profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Firewall** profile and configure the 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. |
| Private Network | |
| Enable Firewall | Enable to ensure that the firewall runs on devices. |
| 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. |
| Public Network | |
| Enable Firewall | Enable to ensure that the firewall is running on devices. |
| 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.

Configure a Single App Mode Profile (Windows Desktop)

The Single App Mode profile allows you to limit access on the device to a single application. With Single App Mode, the device is locked into a single application until the payload is removed. The policy enables after a device reboot.

Requirements

Single App Mode has some restrictions and limitations.

- Windows Universal or Modern apps only. Single App Mode does not support legacy .msi or .exe applications.
- Users must be local standard users only. They cannot be a domain user, admin user, Microsoft account, or guest. The Standard User must be a Local User. Domain Accounts are not supported.

Procedure

To configure the Single App Mode profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Single App Mode** Profile.
6. Configure the **Single App Mode** settings:

| Settings | Descriptions |
|-------------------------|--|
| Application Name | Enter the application friendly name. For Windows apps, the friendly name is the Package Name or Package ID. Run a PowerShell command to get the friendly name of the app installed on the device. The command "Get-AppxPackage" returns the application friendly name as "name." |

7. Select **Save & Publish**.

Activate Single App Mode

After configuring a Single App Mode profile, you must set up Single App Mode on the device.

To begin using Single App Mode:

1. After receiving the Single App Mode profile on the device, reboot the device to begin.
2. Once the device restarts, you are prompted to sign into the device with the Standard User account.

Once signed in, the policy launches and Single App Mode is ready for use. If you must sign out of Single App Mode, press the Windows key 5X fast to launch the login screen to log in to a different user.

Configure an Antivirus Profile (Windows Desktop)

Create an Antivirus profile to configure the native Windows Defender antivirus on Windows Desktop devices. Windows Defender configured for all your devices ensures that your end users are protected as they use the device.

Important: The Antivirus profile requires the AirWatch Protection Agent to be installed on the device. This profile only configures native Windows Defender and not other third-party antivirus appliances.

To configure the Antivirus Profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Antivirus** Profile.
6. Configure the **Antivirus** settings:

| Settings | Descriptions |
|---|---|
| Real Time Monitoring | Enable to configure Windows Defender to monitor the device in real time. |
| Set Signature Update Interval | Enable to set the day and time that the device checks for updates for Defender. |
| Set Scan Interval | Enable to configure the interval between the different system scan. You can select various times and various scan types. Enabling this setting displays Full Scan , Quick Scan , and Remediation Scan settings. |
| Full Scan | Enable to schedule when a full system scan runs. Select the specific time and day. |
| Quick Scan | Enable to schedule when a quick system scan runs. Select the specific time and day. |
| Remediation scan | Enable to schedule when a remediation scan to fix errors runs. Select the specific time and day. |
| Exclusions | |
| Exclusions | Select the file paths or processes to exclude from the Windows Defender scans. Select Add New to add an exception. |
| Threat Default Action | |
| Threat Default Action (Unknown, Low, Moderate, High, Severe threats) | Set the default action for the different threat levels found during scans. <ul style="list-style-type: none"> • Clean – Select to clean the issues with the threat. • Quarantine – Select to separate the threat into a quarantine folder. • Remove – Select to remove the threat from your system. • Allow – Select to let the threat stay. • User Defined – Select to let the user decide what to do with the threat. • No Action – Select to take no action with the threat. • Block – Select to block the threat from accessing the device. |
| Advanced | |
| Scan Avg CPU Load Factor | Set the maximum average percentage of CPU Windows Defender can use during scans. |
| Scan Only If Idle Enabled | Enable to restrict Windows Defender to scan only when the CPU is idle. |
| UI Lockdown | Enable to lock down completely the UI so end users cannot change settings. |

| Settings | Descriptions |
|---------------------------------------|---|
| Catchup Full Scan | Enable to allow run a full scan that was interrupted or missed previously. A catch-up scan is a scan that is initiated because a regularly scheduled scan was missed. Usually these scheduled scans are missed because the computer was turned off at the scheduled time. |
| Catchup Quick Scan | Enable to allow run a quick scan that was interrupted or missed previously. A catch-up scan is a scan that is initiated because a regularly scheduled scan was missed. Usually these scheduled scans are missed because the computer was turned off at the scheduled time. |
| Behavior Monitoring | Enable to set the virus scanner to send an activity log to Microsoft. |
| Privacy Mode | Enable to prevent users, other than administrators, from displaying threat history. |
| Intrusion Prevention System | Enable to configure the network protection against exploitation of known vulnerabilities. This option enables Windows Defender to monitor the connections continuously and identify potentially malicious behavior patterns. In this respect, the software behaves like a classic virus scanner, except that instead of scanning files it now scans network traffic. |
| Scan Email | Enable to allow Windows Defender to scan emails. |
| Scan Mapped Network Drives | Enable to allow Windows Defender to scan network drives mapped to devices. |
| Scan Archives | Enable to allow Windows Defender to run a full scan archived folders. |
| Scan Removable Drives | Enable to allow Windows Defender to scan any removable drives attached to the device. |
| Remove Quarantined Files After | Set how long files are quarantined before being removed. |

7. Select **Save & Publish**.

Encryption Profile (Windows Desktop)

Secure your organization data on Windows Desktop devices with the Encryption profile. The Encryption profile sets the native BitLocker encryption policy on your Windows Desktop devices to ensure data remains secure.

BitLocker encryption is only available on 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 an encryption policy through AirWatch, you can protect data on the hard drive. BitLocker is the native Windows encryption and Dell Data Protection | Encryption is a third-party encryption solution from Dell. With the Encryption profile enabled, the AirWatch Protection Agent continually checks the encryption status of the device. If the agent finds that the device is not encrypted, it automatically encrypts the device.

If you decide to encrypt with BitLocker, a recovery key created during encryption is stored in the AirWatch Console and in the Self-Service Portal.

The Encryption profile requires the AirWatch Protection Agent to be installed on the device.

Note: The Encryption profile does not configure or enable Dell Data Protection | Encryption. The status of the encryption is reported to the AirWatch Console and Self-Service Portal, but the encryption must be configured manually on the device.

Caution: Windows 10 does not support devices without a pre-boot onscreen keyboard. Without a keyboard, you cannot enter the start up pin necessary to unlock the hard drive and start Windows on the device. Pushing this profile to devices without a pre-boot onscreen keyboard breaks your device.

BitLocker Functionality

The Encryption profile uses advanced BitLocker functionality to control authentication and deployment of BitLocker encryption.

BitLocker uses the Trusted Platform Module (TPM) on devices to store the recovery password on the device to decrypt hard drives connected to the motherboard. If the drive is removed from the motherboard, the drive does not decrypt. For enhanced authentication, you can enable an encryption PIN to confirm user authentication. You can also require a password for devices as a fallback for when the TPM is not available.

Deployment Behavior

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

Note: For BitLocker encryption to take place on a Windows 8.1 device, the device must have TPM enabled and activated. The exact process to enable and activate TPM might vary from one system to another but is typically done by restarting the device and accessing the BIOS security settings.

Already-Encrypted Devices

If the Encryption profile is pushed to an encrypted device and the current encryption settings match the profile settings, the AirWatch Protection Agent adds a new recovery key and sends it to the AirWatch Console. This new recovery key is also stored in an encrypted database on the device. With this feature, if a user or an admin attempts to decrypt the device, the Encryption profile re-encrypts the device with the new recovery key. The encryption is enforced even if the device is offline.

If the existing encryption does not meet the authentication settings of the Encryption profile, the existing protectors are removed and new protectors are applied that meet the Encryption profile settings.

If the existing encryption method does not match the Encryption profile, AirWatch leaves the existing method in place and does not override it. This functionality also applies if you add a new version of the Encryption profile to a device managed by an existing Encryption profile. The existing encryption method is not changed.

Encryption Status

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

- AirWatch Dashboard
 - Device Details displays recovery key information.
 - BitLocker protection displays as enabled.
- AirWatch Self-Service Portal
 - Self-Service Portal displays that the recovery key is stored, but not the recovery key details.
 - BitLocker protection displays as enabled.

Removal Behavior

If the profile is removed from the AirWatch Console, AirWatch no longer enforces the encryption and the device automatically decrypts. Enterprise wiping or manually uninstalling the AirWatch Protection Agent from the Control Panel disables BitLocker encryption.

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.

Configure an Encryption Profile (Windows Desktop)

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

To create an Encryption profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the [VMware AirWatch Mobile Device Management Guide](#), available on [AirWatch Resources](#).

5. Select the **Encryption** profile and configure the settings:

| Settings | Descriptions |
|--------------------------|--|
| Encrypted Volume | Use the drop-down menu to select the type of encryption as follows: <ul style="list-style-type: none"> • Complete Hard Disk – Encrypts the entire hard disk on the device, including the System Partition where the OS is installed. • System Partition – Encrypts a partition or drive in the same location Windows is installed and from which it boots. |
| Encryption Method | Set the encryption method. |

| Settings | Descriptions |
|--|---|
| Only encrypt used space during initial encryption | Enable to limit the BitLocker encryption to only the used space on the drive at the time of encryption. |
| Custom URL for Recovery Screen | Enter the URL to display on the lock screen directing end users to get the recovery key. Consider entering the Self Service Portal URL as AirWatch hosts the recovery key there. |
| BitLocker Authentication Settings | |
| Authentication Mode | Select the method for authenticating access to a BitLocker encrypted device. <ul style="list-style-type: none"> • TPM — Uses the devices Trusted Platform Module. Requires a TPM on the device. • Password — Uses a password to authenticate |
| Enforce Encryption PIN on Login | Select the check box to require users to enter a PIN to unlock the device. This option locks out the OS start up and auto-resume from suspend or hibernate until the user enters the correct PIN. |
| Use Password if TPM Not present | Select the check box to use a password as a fallback to decrypt the device if the TPM is unavailable. If this settings is not enabled, any devices without a TPM do not encrypt. |
| Minimum Password Length | Select the minimum number of characters a password must be. Displays if the Authentication Mode is set to Password or if Use Password if TPM Not Available is enabled. |
| BitLocker Static Recovery Key Settings | |
| Create Static BitLocker Password | Select the check box if a static recovery key is enabled. |
| BitLocker Recovery Password | Select the Generate icon (🔄) to generate a new recovery key. |
| Rotation Period | Enter the number of days until the recovery key rotates. |
| Grace Period | Enter the number of days after rotation that the previous recovery key still works. |
| BitLocker Suspend | |
| Enable BitLocker Suspend | Select the check box to enable BitLocker Suspension. This functionality suspends BitLocker encryption during a specified time period. Use this feature to suspend BitLocker when updates are scheduled so devices can reboot without requiring end users to enter the Encryption PIN or password. |

| Settings | Descriptions |
|-------------------------------------|--|
| Suspend BitLocker Type | Select the type of suspension. <ul style="list-style-type: none"> • Schedule — Select to enter the specific time period that BitLocker suspends. Then set the schedule repeat to daily or weekly. • Custom — Select to enter the day and time to begin and end BitLocker suspension. |
| BitLocker Suspend Start Time | Enter the time to start BitLocker suspension. |
| BitLocker Suspend End Time | Enter the time to end BitLocker suspension. |
| Scheduled Repeat Type | Set whether the scheduled suspension repeats daily or weekly. If you select weekly, select the days of the week to repeat the schedule. |

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

Configure a Windows Updates Profile (Windows Desktop)

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

To use advanced settings, the Windows Update profile requires the AirWatch Protection Agent to be installed on the device.

 **Important:** To see the OS version each update branch supports, see Microsoft's documentation on Windows 10 release information: <https://technet.microsoft.com/en-us/windows/release-info.aspx>.

To enforce a Windows Update profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
5. Select the **Windows Updates** profile.
6. Configure the Windows Updates settings. The profile supports Windows 8.1 and Windows 10 devices. The settings differ based on the OS. For Windows 10 devices, configure the settings:

| Settings | Descriptions |
|--|--|
| Branching and Deferral | |
| Windows Update Source | <p>Select the source for Windows Updates:</p> <ul style="list-style-type: none"> • Microsoft Update Service– 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>The device must contact the WSUS at least once for this setting to take effect.</p> <p>Choosing Corporate WSUS as a source allows your IT Admin to view updates installed and device status of devices in the WSUS Group.</p> |
| Update Branch | <p>Select the update branch to follow for updates.</p> <p>For more information on the update branches, refer to the Microsoft documentation available here: https://technet.microsoft.com/en-us/windows/release-info.aspx.</p> |
| Defer Feature Updates Period in Days | <p>Select the number of days to delay feature updates before installing the updates on the device.</p> |
| Pause Feature Updates | <p>Enable to pause all feature updates for 60 days or until disabled. This setting overrides the Defer Feature Updates Period in Days setting.</p> <p>Use this option to delay an update that causes issues that normally installs following your deferral settings.</p> |
| Defer Quality Updates Period In Days | <p>Select the number of days to delay quality updates before installing the updates on the device.</p> |
| Pause Quality Updates | <p>Enable to pause all quality updates for 60 days or until disabled. This setting overrides the Defer Quality Updates Period in Days setting.</p> <p>Use this option to delay an update that causes issues that normally installs following your deferral settings.</p> |
| Enable Settings for Previous Windows versions | <p>Select to enable deferral settings for previous versions of Windows. The settings include:</p> <ul style="list-style-type: none"> • Defer New Features (months) • Defer New Updates (weeks) • Pause Deferrals |

| Settings | Descriptions |
|---|---|
| Update Installation Behavior | |
| Automatic Updates | <p>Set how updates from the selected Update Branch are handled:</p> <ul style="list-style-type: none"> • Install updates automatically • Install Updates but let the user schedule the computer restart. • Install updates automatically and restart at specified time. • Install updates automatically and prevent users from modifying the control panel settings. • Check for updates but let users choose whether to download and install them. • Never check for updates (not recommended). |
| Active Hours Start Time | <p>Enter the start time for active hours.</p> <p>Set the active hours to prevent the system from rebooting during these hours.</p> |
| Active Hours End Time | <p>Enter the end time for active hours.</p> <p>Set the active hours to prevent the system from rebooting during these hours.</p> |
| Auto Restart Deadline Period in Days | Select the number of days before a restart becomes mandatory. |
| Auto Restart Notification Schedule in Minutes | Select the period (in minutes) for auto-restart reminder notifications. |
| Auto Restart Required for Notification Dismissal | Select whether the notification is auto dismissed or if a user must dismiss the notification. |
| Engaged Restart Deadline in Days | <p>Select the number of days before an automatic restart transitions to an engaged restart.</p> <p>An engaged restart is a user-scheduled restart.</p> |
| Engaged Restart Snooze Schedule in Days | Select the number of days a user can snooze an engaged restart before a restart is automatically scheduled and ran outside of active hours. |
| Schedule Restart Warning in Hours | Select the number of hours before an auto-restart to warn users. |
| Update Policies | |
| Allow Update Service | <p>Allow updates from the public Windows Update service.</p> <p>Not allowing this service can cause issues with the Microsoft Store.</p> |
| Allow MU Updates | Allow updates from Microsoft Update |
| Update Scan Frequency in Hours | Select the number of hours between scans for new updates. |

| Settings | Descriptions |
|---|---|
| Dual Scan for Deferral Policies | Enable to prevent unexpected update scans due to deferral policies. If the setting is enabled, users can configure deferral policies as required. |
| Exclude WU Drivers in Quality Update | Prevents the update of Windows Update drivers during system updates. |
| Install Signed Updates from 3rd Party Entities | Allow the installation of updates from approved third parties. |
| Mobile Operator App Download Limit | Set to Ignore to allow unlimited downloading over a cellular network for apps and their updates. |
| Mobile Operator Update Download Limit | Set to Ignore to allow unlimited downloading over a cellular network for OS updates. |
| Insider Builds | Allow the download of Windows Insider builds of Windows 10. |
| Administrator Approved Updates | |
| Require Update Approval | <p>Enable to require updates to have approval before downloading to the device.</p> <p>Enable to require admins to explicitly approve updates before downloading to the device. This approval is either through Update Groups or individual update approval.</p> <p>This option requires you to accept any required EULA on behalf of your end users before the update pushes to devices. If a EULA must be accepted, a dialog box opens displaying the EULA.</p> <p>To approve updates, navigate to Lifecycle > Windows Updates. For more information, see Approve Windows Updates on page 81.</p> |
| Auto-Approved Updates | <p>Enable this option to set update groups that are automatically approved to download onto end-user devices.</p> <p>This option requires you to accept any required EULA on behalf of your end users before the update pushes to devices. If a EULA must be accepted, a dialog box opens displaying the EULA.</p> |
| Application | <p>Set to Allowed to automatically approve all app updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Connectors | <p>Set to Allowed to automatically approve all Office 365 connectors updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Critical | <p>Set to Allowed to automatically approve all critical updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |

| Settings | Descriptions |
|--|---|
| Definition | <p>Set to Allowed to automatically approve all Windows Defender definition updates for download to assigned devices.</p> <p>Consider setting this option to Allowed to ensure your devices remain protected by Windows Defender. This option is enabled by default.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Developer Kit | <p>Set to Allowed to automatically approve all developer kit updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Feature Pack | <p>Set to Allowed to automatically approve all feature pack updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Guidance | <p>Set to Allowed to automatically approve all guidance updates for download to assigned devices.</p> |
| Security | <p>Set to Allowed to automatically approve all security updates for download to assigned devices.</p> <p>Consider setting this option to Allowed to ensure that your devices remain secure. This option is enabled by default.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Service Pack | <p>Set to Allowed to automatically approve all service pack updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Tool Updates | <p>Set to Allowed to automatically approve all tool updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Update Rollups | <p>Set to Allowed to automatically approve all update rollups for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| General | <p>Set to Allowed to automatically approve all general updates for download to assigned devices.</p> <p>Displays if the Auto-Approved Updates setting is enabled.</p> |
| Delivery Optimization | |
| Peer-to-Peer Updates | Allow the use of peer-to-peer downloading of updates. |
| Allowed Peer-to-Peer Method | Select the method of peer-to-peer connection you want to allow. |
| Limit Peer Usage to Member with the Same Group ID | Limit peer-to-peer downloading to devices within the same organization group. |

| Settings | Descriptions |
|--|--|
| Maximum time each file is held in the delivery optimization cache (seconds) | Set the number of seconds a file is held in the delivery optimization cache before being pushed to devices. The optimization cache keeps updates available on other peers that the device can reach for quicker downloading of updates. |
| Maximum cache size that delivery optimization can utilize (%) | Enter the percentage of the cache that delivery optimization can use. |
| Maximum upload bandwidth that a device will use across all concurrent upload activity (KB/second) | Enter maximum upload bandwidth in KB/second that a device uses when sending updates to peers. |
| VPN Peer Caching | Allow peer caching while connected to a VPN. |
| Minimum Battery Required for Peer Uploads (%) | Set the minimum battery percentage required for peer uploads. |
| Memory | |
| Maximum Allowed Cache Size | Set the maximum size in GB of delivery optimization cache. This setting overrides Maximum cache size that delivery optimization can use (%) . |
| Maximum cache size that delivery optimization can use (%) | Set the maximum percentage of disk space that delivery optimization can use as a cache. |
| Maximum time each file is held in the delivery optimization cache (seconds) | Set the maximum number of seconds that each file is held in the delivery optimization cache after downloading. |
| Minimum disk size for device to use peer caching. | Set the minimum disk size required for a device to use peer caching. |
| Minimum RAM for device to use peer caching | Set the minimum RAM required for a device to use peer caching. |
| Minimum Content File Size That Can Use Peer Caching | Set the minimum content file size required for a file to use peer caching. |
| Drive location used for peer cache | Enter the file path for the peer cache. |
| Network | |
| Maximum upload bandwidth that a device will use across all concurrent upload activity (KB/second) | Set the maximum upload bandwidth that a device will use across all concurrent upload activity using delivery optimization. |
| Maximum download bandwidth that a device will use (KB/second) | Set the maximum download bandwidth that a device uses across all concurrent upload activity using delivery optimization. |
| Maximum download bandwidth as a percentage of total available (%) | Set the maximum percentage of bandwidth a device uses to download through delivery optimization. |
| Minimum QoS for background downloads (KB/second) | Set the minimum download Quality of Service (speed) for background downloads. |

| Settings | Descriptions |
|-------------------------------------|---|
| Monthly upload data cap (GB) | Set the maximum amount (in GB) that delivery optimization is allowed to upload per month. |

For Windows 8.1 devices, configure the settings:

| Settings | Descriptions |
|--|--|
| Windows 8.1 | |
| Updates Managed By | Set to Administrator to configure how Windows Updates. Setting to User does not override the device settings. |
| Install Important Updates Automatically | Require all Important Automatic Updates to install automatically. |
| Install Recommended Updates Automatically | Require all Recommended Automatic Updates to install automatically. |
| Protection Agent Advanced Configuration | Configure the advanced settings for the Windows Automatic Update profile. |
| 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>The device must contact the WSUS at least once for this setting to take effect.</p> <p>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. |

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

Windows Updates

AirWatch supports reviewing and approving updates for Windows 10 devices. The Windows Updates console page lists all updates available for Windows 10 devices.

From this screen, you can approve updates and assign the updates to the specific smart groups as meets your business needs. The console page displays all updates with their published date, platform, classification, and assigned group. Selecting the update name displays a window with detailed information, a link to the Microsoft KB page for the update, and the status of update installation.

View Update Status

The update installation status shows the deployment of the update across your devices.

See the status of the update deployment by selecting **View**.

| Status | Descriptions |
|----------------------|---|
| Assigned | The update is approved and assigned to the device |
| Approved | The approved update is successfully assigned to the device. |
| Available | The update is available on the device for installation |
| Pending Installation | The installation is approved and available but not yet installed. |
| Pending Reboot | Installation is paused until the device reboots. |
| Installed | The update successfully installed |
| Failed | The updated failed to install. |

Approve Windows Updates

Review and approve Windows Updates for installation on your Windows 10 devices. This feature allows you to ensure your devices remain up-to-date while controlling the distribution of updates to meet your business needs.

Prerequisites

You must publish a Windows Update profile with **Require Update Approval** enabled.

Procedure

To approve and assign an update:

1. Navigate to **Lifecycle > Updates > Windows**.
2. Select the check box on the left of the update. Select the **Assign** button.
3. Enter the smart groups to which the update applies.
4. Select **Add**.

For more information on the Windows Updates console page, see [Windows Updates on page 80](#).

Configure a Web Clips Profile (Windows Desktop)

A Web Clips Profile allows you to push URLs on to end-user devices for easy access to important Web sites.

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the [VMware AirWatch Mobile Device Management Guide](#), available on [AirWatch Resources](#).

5. Select the **Web Clips** profile.
6. Configure the **Web Clips** settings, including:

| Settings | Description |
|----------------------------|---|
| Label | Enter a description for the Web clip. |
| URL | Enter the target URL for the Web clip. |
| Show in App Catalog | Enable to show the Web clip in the app catalog. |

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

Exchange ActiveSync Profile (Windows Desktop)

The Exchange ActiveSync profiles enable you to configure your Windows Desktop 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. See [Configure a Credentials Profile \(Windows Desktop\) on page 54](#) for more information.

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

Important: Native Mail Client support is only available for Windows 10 devices.

Removing Profile or Enterprise Wiping

If the profile is removed using the remove profile command, compliance policies, or through an enterprise wipe, all email data is deleted, including:

- User account/login information.
- Email message data.
- Contacts and calendar information.
- Attachments that were saved to the internal application storage.

Username and Password

You can define the user name that is assigned for users to log in to the AirWatch Inbox. The user name can be their actual email address or an email user name that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the AirWatch **Inbox** profile settings, there is a **User** text box under **Login Information** that you can set to a predefined lookup value.

If you have email user names that are different than user email addresses, you can use the `{EmailUserName}` text box, which corresponds to the email user names imported during directory service integration. Even if your user user names are the same as their email addresses, use the `{EmailUserName}` text box, because it uses email addresses imported through the directory service integration.

Configure an Exchange ActiveSync Profile (Windows Desktop)

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

Use the following steps to create a configuration profile for the native mail client:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and choose **Windows Desktop** as the platform.
3. Select **User Profile**.
4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

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

6. Configure the Exchange ActiveSync settings:

| Settings | Descriptions |
|---|--|
| Mail Client | Select the Mail Client that the EAS profile configures. AirWatch supports the Native Mail Client and AirWatch Inbox. |
| Account Name | Enter the name for the Exchange ActiveSync account. |
| Exchange ActiveSync Host | Enter the URL or IP Address for the server hosting the EAS. |
| Use SSL | Enable to send all communications through the Secure Socket Layer. |
| Login Information | |
| Domain | Enter the email domain. The profile supports lookup values for inserting enrollment user login information. For more information, see Exchange ActiveSync Profile (Windows Desktop) on page 82 . |
| Username | Enter the email user name. |
| Email Address | Enter the email address. This text box is a required setting. |
| Password | Enter the email password. |
| Identity Certificate | Select the certificate for the EAS payload. See Configure a Credentials Profile (Windows Desktop) on page 54 for more information. |
| Settings | |
| Next Sync Interval (Min) | Select the frequency, in minutes, that the device syncs with the EAS server. |
| Past Days of Mail to Sync | Select how many days of past emails sync to the device. |
| Diagnostic Logging | Enable to log information for troubleshooting purposes. |
| Content Type | |
| Require Data Protection Under Lock | Enable to require data to be protected when the device is locked. |

| Settings | Descriptions |
|----------------------------|---|
| Allow Email Sync | Enable to allow the syncing of email messages. |
| Allow Contacts Sync | Enable to allow the syncing of contacts. |
| Allow Calendar Sync | Enable to allow the syncing of calendar events. |

7. Select **Save** to keep the profile in the AirWatch Console or **Save & Publish** to push the profile to the devices.

Configure an EAS Profile for AirWatch Inbox (Windows Desktop)

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.

Use the following steps to create a configuration profile for the AirWatch Inbox:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and choose **Windows Desktop** as the platform.
3. Select **User Profile**.
4. Configure the profile **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
5. Select the **Exchange ActiveSync** payload. By default, **AirWatch Inbox** is selected in the **Mail Client** drop-down menu.
6. Enter the **Exchange ActiveSync Host**, which is the information of your EAS server. For example: `webmail.airwatchmdm.com`.

| Settings | Descriptions |
|----------------------------|--|
| Use SSL | Enable to send all communications through the Secure Socket Layer. |
| Use S/MIME | Enable to store end-user S/MIME certificates. This option is necessary for S/MIME-enabled profiles. |
| Login Information | |
| Domain | Enter the email domain. |
| User | Enter the email user name. |
| Email Address | Enter the email address. This text box is a required setting. |
| Password | Enter the email password. |
| Payload Certificate | Select the certificate for the EAS payload. See Configure a Credentials Profile (Windows Desktop) on page 54 for more information. |

| Settings | Descriptions |
|---|--|
| Settings | |
| Require Passcode | Enable to require a passcode when the AirWatch Inbox app is opens. |
| Type | Select the type of login credentials required: <ul style="list-style-type: none"> • Passcode • Username and Password |
| Complexity | Select the level of complexity for the passcode: <ul style="list-style-type: none"> • Simple • Alphanumeric |
| Minimum Length | Select the minimum number of characters the passcode must have. |
| Allow Simple Value | Enable to allow passcodes that do not meet complexity requirements. |
| Minimum Number of Complex Characters | Select the smallest number of non-alphanumeric characters allowed. Displayed when Complexity is set to Alphanumeric . |
| Maximum Age | Select the maximum number of days a passcode may be used. |
| History | Select the number of previous passcodes remembered. If a user changes a passcode and it matches a stored previous passcode, the passcode is not accepted. |
| Auto Lock When Device Locks | Enable to lock AirWatch Inbox automatically when the device locks. |
| Grace Period | Select the number of minutes the app remains open and unlocked before automatically locking. |
| Maximum Number of Failed Attempts | Select the number of incorrect passcode entry attempts allowed before the data in AirWatch Inbox is erased. |
| Passcode | |
| Require Passcode | Enable to require a passcode when the AirWatch Inbox app is opens. |
| Type | Select the type of login credentials required: <ul style="list-style-type: none"> • Passcode • Username and Password |
| Complexity | Select the level of complexity for the passcode: <ul style="list-style-type: none"> • Simple • Alphanumeric |
| Minimum Length | Select the minimum number of characters the passcode must have. |
| Allow Simple Value | Enable to allow passcodes that do not meet complexity requirements. |

| Settings | Descriptions |
|---|--|
| Minimum Number of Complex Characters | Select the smallest number of non-alphanumeric characters allowed. Displayed when Complexity is set to Alphanumeric . |
| Maximum Age | Select the maximum number of days a passcode may be used. |
| History | Select the number of previous passcodes remembered. If the end user reuses a password within the number of recorded occurrences, they cannot reuse that password. |
| Auto Lock When Device Locks | Enable to lock AirWatch Inbox when the device locks. |
| Grace Period | Select the number of minutes the app remains open and unlocked before automatically locking |
| Maximum Number of Failed Attempts | Select the number of incorrect passcode entry attempts allowed before the data in AirWatch Inbox is erased. |
| Restrictions | |
| Disable Copy-Paste | Enable to restrict the copy/paste actions in AirWatch Inbox: <ul style="list-style-type: none"> • Disable ability to long press email text and copy it to the clipboard. • Disable ability to copy text from outside of the email client and paste it into a mail message. |
| Disable Attachments | Enable to restrict end user from opening attachments inside the AirWatch Inbox app. |
| Maximum Attachment Size (MB) | Enter the maximum size (in MB) that a received attachment may be. |
| Restrict Domains | Enable to restrict the mail flow to specific domains. |
| Restriction Type | Select the type of restriction for email domains. |
| Domain Name | Select Add to add a domain to the whitelist or blacklist. |

7. Select **Save** to keep the profile in the console or **Save & Publish** to push the profile to the devices.

SCEP Profile (Windows Desktop)

Simple Certificate Enrollment Protocol (SCEP) profiles enable you to install certificates onto devices silently without interaction from the end user.

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

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

Configure a SCEP Profile (Windows Desktop)

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

To configure a SCEP profile:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile** or **Device Profile**.
4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **SCEP** profile.
6. 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: <ul style="list-style-type: none"> • Context User – Stores the SCEP with the specific user. • Context Machine – Stores the SCEP for all users on the machine. |

7. Configure the Wi-Fi, VPN, or EAS profile.
8. Select **Save & Publish** when you are finished to push the profile to devices.

Application Control Profile (Windows Desktop)

Limit which applications can be installed onto Windows Desktop devices with the Application Control profile. Limiting application installs protects your data from malicious apps and prevents end users from accessing unwanted apps on corporate devices.

To allow or prevent installation of applications on devices, you can enable Application Control to whitelist and blacklist specific applications. While the compliance engine monitors devices for whitelisted and blacklisted apps, Application Control prevents users from even attempting to add or remove applications. For example, prevent a certain game application from ever installing on a device, or allow only specific apps whitelisted to be installed on a device. Blacklisted apps installed on the device before the Application Control payload is pushed to the device are disabled after the profile is pushed.

The Application Control profile helps reduce the cost of device management by preventing user from running prohibited apps that cause issues. Preventing apps from causing issues reduces the number of calls your support staff must answer.

Configure an Application Control Profile (Windows Desktop)

Enable Application Control to whitelist and blacklist specific applications to allow or prevent use of applications on devices. Application Control uses Microsoft AppLocker configurations to enforce app control on Windows 10 devices.

Prerequisites

To configure an XML configuration file, you must configure the AppLocker settings on a device and export the file for use with the profile.

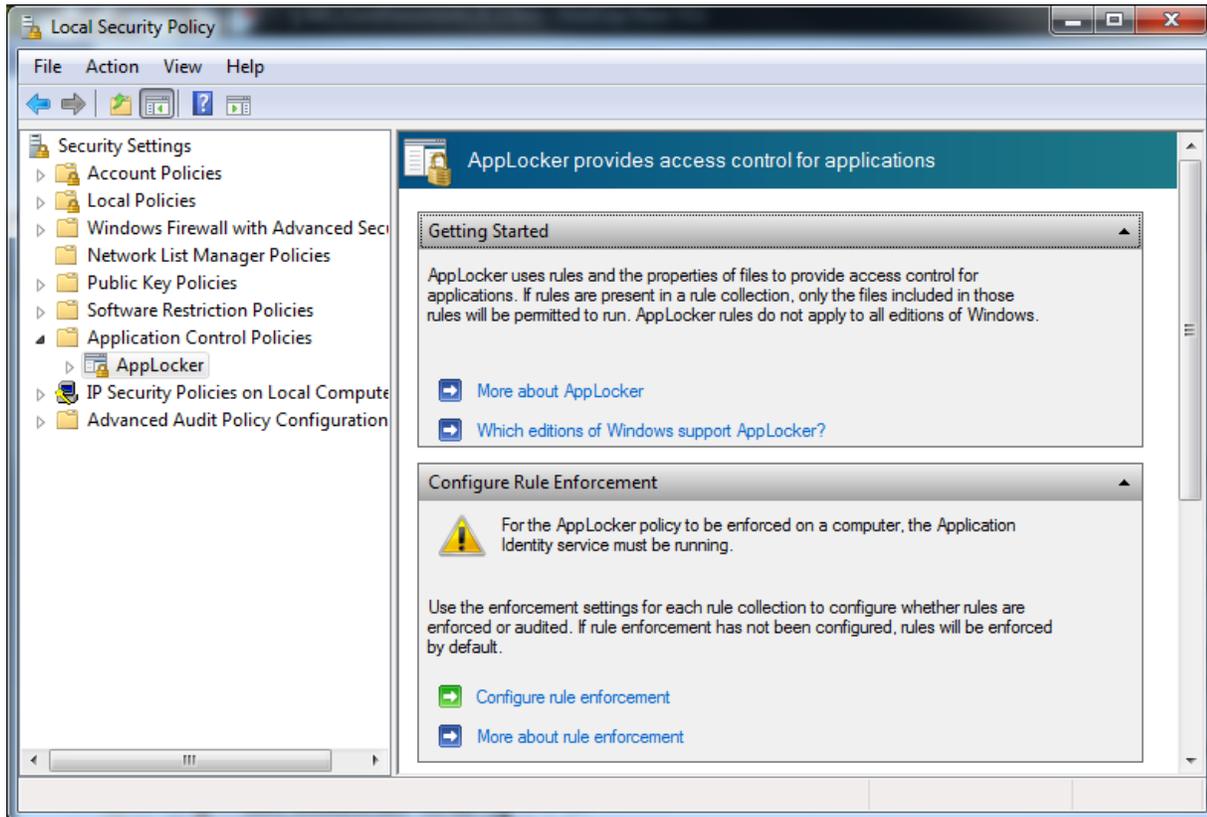
The Application Control profile requires Windows 10 Enterprise or Education.

Important Recommendations

- Create policies using Audit Only mode first. After verifying with the Audit Only version on a test device, create an Enforce mode version for use with your devices. Failing to test policies before general use may result in your devices becoming unusable.
- Create default rules and any other desired rules for your organization to reduce chances of locking the default configurations or breaking devices after reboot. For more information on creating rules, see the Microsoft TechNet article on AppLocker.

To configure an Application Control profile:

1. On the configuration device, start the **Local Security Policy** editor.
2. Navigate to **Application Control Policies > AppLocker** and select **Configure Rule Enforcement**.



3. Enable **Executable Rules**, **Windows Installer Rules**, and **Script Rules** enforcement by selecting **Enforce Rules**.
4. Create **Executable Rules**, **Windows Installer Rules**, and **Script Rules** by selecting the folder on the right then right-clicking the folder and selecting **Create New Rule**.
Remember to create Default Rules to reduce chances of locking the default configuration or breaking the device.
5. After creating all the rules you want, right-click **AppLocker** and select **Export Policy** and save the XML configuration file.
6. Navigate in the AirWatch Console to **Devices > Profiles > List View > Add** and select **Add Profile**.
7. Select **Windows** and then select **Windows Desktop**.
8. Select **Device Profile**.
9. Configure the profile **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
10. Select the **Application Control** payload.
11. Select **Import Sample Device Configuration** and select **Upload** to add your **Policy Configuration File**.
12. Select **Save & Publish**.

Configure an Exchange Web Services Profile (Windows Desktop)

Create an Exchange Web Services profile to allow end users to access corporate email infrastructures and Microsoft Outlook accounts from their devices.

Important: During first-time configuration, the device must have access to the Internal Exchange Server.

To create an Exchange Web Services profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Exchange Web Services** profile and configure the 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.

Create a Windows Licensing Profile (Windows Desktop)

Configure a Windows Licensing profile to provide your Windows 10 devices with a Windows 10 Enterprise or Windows 10 Education license key. Use this profile to upgrade devices that do not come with Windows 10 Enterprise.

This upgrade cannot be reversed. If you publish this profile to BYOD devices, you cannot remove the licensing through MDM. Windows 10 can only upgrade following a specific upgrade path:

- Windows 10 Enterprise to Windows 10 Education
- Windows 10 Home to Windows 10 Education
- Windows 10 Pro to Windows 10 Education
- Windows 10 Pro to Windows 10 Enterprise

To create a Windows Licensing profile:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.

3. Select **Device Profile**.4. Configure the profile **General** settings.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **Windows Licensing** profile and configure the following settings:

| Settings | Descriptions |
|---------------------------------------|--|
| Windows Edition | Select either Enterprise or Education edition. |
| Please Enter valid License Key | Enter the license key for the edition of Windows that you are using. |

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

Configure a BIOS Profile (Windows Desktop)

Configure BIOS settings for select Dell enterprise devices with the BIOS profile. This profile requires integration with Dell Command | Monitor.

Support for the BIOS profile settings varies by Dell Enterprise device. AirWatch only pushes the settings a device supports.

For more information on configuring Dell Command | Monitor integration, see [Dell Command | Monitor Integration on page 110](#).

Prerequisites

Only specific Dell enterprise devices are supported. For more information, see [Dell Command | Monitor Integration on page 110](#).

Procedure

To configure a BIOS profile:

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **BIOS** payload and configure the following settings:

| Settings | Descriptions |
|-----------------------------|---|
| Security | |
| BIOS Password | Enter the password used to unlock the BIOS of the device. This field is required. |
| TPM Chip | Select Enable to enable the device Trusted Platform Module chip. |
| Boot | |
| Boot Mode | Select whether the device boots in BIOS or UEFI mode. |
| Boot Mode Protection | Select Enable to prevent issues with the OS installed on the device from booting. This protection prevents a change in Boot Mode on a device with an installed OS. |
| Secure Boot | Select Enable to use Secure Boot settings on the device. You cannot disable Secure Boot with DCM. If your devices already use Secure Boot, you must manually disable the settings on the device. Secure Boot requires Boot Mode to be set to UEFI and Legacy Option ROMS to be set to Disable . |
| Legacy Option ROMS | Select Enable to allow the use of legacy option ROMS during the boot process. |
| Virtualization | |
| CPU Virtualization | Select Enable to allow hardware virtualization support. |
| Virtualization IO | Select Enable to allow input/output virtualization. |
| Trusted Execution | Select Enable to allow the device to use the TPM chip, CPU Virtualization, and Virtualization IO for trust decisions. Trust Execution requires the TPM Chip , CPU Virtualization , and Virtualization IO settings to be set to Enabled . |
| Connectivity | |
| Wireless LAN | Select Enable to allow use of the device wireless LAN functionality. |
| Cellular Radio | Select Enable to allow use of the device cellular radio functionality. |
| Bluetooth | Select Enable to allow use of the device Bluetooth functionality. |
| GPS | Select Enable to allow use of the device GPS functionality. |
| Storage | |
| SMART Reporting | Select Enable to use SMART monitoring of the device storage solutions. |

| Settings | Descriptions |
|--|--|
| Power Management | |
| Primary Battery Charge | <p>Select the charging rules for the device:</p> <ul style="list-style-type: none"> • Standard Charge • Express Charge • AC Charge • Auto Charge • Custom Charge <p>These rules control when the battery starts and stops charging. If you select Custom Charge, you can manually set the charge percentage to start and stop charging the battery.</p> |
| Primary Battery Custom Charge Start Limit | Set the battery charge percentage that must be reached before the device starts charging the battery. |
| Primary Battery Custom Charge Stop Limit | Set the battery charge percentage that must be reached before the device stops charging the battery. |
| Peak Shift | <p>Select Enable to use peak shift to control when a device uses battery charge or AC current. Peak shift allows you to use battery power instead of AC current during specified times.</p> <p>To set the schedule for Peak Shift, select the calendar icon.</p> |
| Peak Shift Scheduling | <p>The three parameters for peak shift scheduling control when a device uses battery or AC current and when the device charges the battery.</p> <ul style="list-style-type: none"> • Peak Shift Start – Set the start time for Peak Shift when devices switch to battery power. • Peak Shift End – Set the end time for Peak Shift when devices switch to AC current. • Peak Shift Charge Start – Set the start time for Peak Shift Charge when the devices charge the batteries while using AC current. |
| Peak Shift Battery Threshold | <p>Set the battery charge percentage that must be reached before devices switch back to AC current from battery power.</p> <p>The Peak Shift Charge Start setting controls the time when devices charge the batteries after switching to AC current.</p> |
| Custom | |
| System Properties | <p>Select Add System Properties to add a custom system property. Select the button again to add additional properties.</p> <p>These properties are advanced options. Consider reviewing Dell documentation before using these settings.</p> <p>System Properties override any pre-defined settings configured in the profile.</p> |

| Settings | Descriptions |
|------------------------------|---|
| Class | Enter a class and select it from the drop-down menu. Displays after selecting Add System Properties . |
| System Property | Enter a system property and select it from the drop-down menu. Displays after selecting Add System Properties . |
| BIOS Attributes | Select Add BIOS Attribute to add a custom BIOS attribute. Select the button again to add additional attributes. These attributes are advanced options. Consider reviewing Dell documentation before using these settings. BIOS Attributes override any pre-defined settings configured in the profile. |
| BIOS Attribute | Enter a BIOS attribute and select it from the drop-down menu. Displays after selecting Add BIOS Attribute . |
| Value | Select a value for the BIOS attribute. If a value is not supplied, the BIOS Attribute is read only. Displays after selecting Add BIOS Attribute . |
| Configuration Package | |
| Configuration Package | Select Upload to add a Dell Command Configure configuration package. Uploading a package allows you to configure multiple Dell devices with a single configuration. Configuration packages override any custom system properties or attributes. If you whitelist the file extensions allowed, you must add the CCTK file extension to the whitelist. Navigate to Groups & Settings > All Settings > Content > Advanced > File Extensions to add the file extension. |

6. Select **Save & Publish**.

Configure the OEM Updates Profile (Windows Desktop)

Configure OEM Update settings for select Dell enterprise devices with the OEM Updates profile. This profile requires integration with Dell Command | Update.

Support for the OEM Update profile settings varies by Dell Enterprise device. AirWatch only pushes the settings a device supports.

For more information on configuring Dell Command | Monitor integration, see [Dell Command | Update Overview on page 111](#).

Prerequisites

Only specific Dell enterprise devices are supported. For more information, see [Dell Command | Update Overview on page 111](#).

Procedures

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

5. Select the **OEM Updates** payload and configure the following settings:

| Settings | Description |
|----------------------|--|
| Schedule | |
| Check for Updates | Select the interval used to check for updates. |
| Day of the Week | Select the day of the week to check for updates. Only displays when Check for Updates is set to Weekly . |
| Day of the Month | Select the day of the month to check for updates. Only displays when Check for Updates is set to Monthly . |
| Time | Select the time of day to check for updates. |
| Update Behavior | Select the actions to take when checking for updates. <ul style="list-style-type: none"> • Select Scan Notify to scan for updates and notify the user that updates are available. • Select Scan Download Notify to scan for updates, download any available, and notify the user that updates are available for installation. • Select Scan Notify Apply Reboot to scan for updates, download any available, install the updates, and reboot the device. |
| Reboot Delay | Select the amount of time the device delays rebooting after downloading updates. |
| Level | |
| Urgent Updates | Select Enable to apply Urgent Updates to the device. |
| Recommended Updates | Select Enable to apply Recommended Updates to the device. |
| Optional Updates | Select Enable to apply Optional Updates to the device. |
| Update Type | |
| Hardware Drivers | Select Enable to apply hardware driver updates provided by the OEM to the device. |
| Application Software | Select Enable to apply application software updates provided by the OEM to the device. |
| BIOS Updates | Select Enable to apply BIOS updates provided by the OEM to the device. Consider disabling any BIOS passwords if you want to use the OEM Update profile to manage BIOS updates. Some BIOS updates prompt users to enter the BIOS password. |
| Firmware Updates | Select Enable to apply firmware updates provided by the OEM to the device. |
| Utility Software | Select Enable to apply utility software updates provided by the OEM to the device. |

| Settings | Description |
|-------------------|---|
| Other | Select Enable to apply other updates provided by the OEM to the device. |
| Device Categories | |
| Audio | Select Enable to apply audio device updates provided by the OEM to the device. |
| Chipset | Select Enable to apply chipset device updates provided by the OEM to the device. |
| Input | Select Enable to apply input device updates provided by the OEM to the device. |
| Network | Select Enable to apply network device updates provided by the OEM to the device. |
| Storage | Select Enable to apply storage device updates provided by the OEM to the device. |
| Video | Select Enable to apply video device updates provided by the OEM to the device. |
| Others | Select Enable to apply other device updates provided by the OEM to the device. |

6. Select **Save & Publish**.

Use Custom Settings (Windows Desktop)

The Custom Settings payload provides a way to use Windows Desktop 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 enable or disable certain settings manually.

Requirements

You must write your own SyncML code for Windows Desktop profiles. Microsoft publishes a Configuration Service Provider reference site available on their web site.

The Custom Settings profiles appends the appropriate code to the beginning and the end of the code. You must write the appropriate code between any <Add>, <Replace>, <Delete>, or <Get> tags. Before adding the code to the profile, remove all whitespace from the XML code.

Example code:

```
<Replace><CmdID>2</CmdID><Item><Target><LocURI>./Device/Vendor/MSFT/AssignedAccess/KioskModeApp</LocURI></Target><Meta><Format xmlns="syncml:metinf">chr</Format></Meta><Data>{"Account":"standard","AUMID":"AirWatchLLC.AirWatchBrowser_htcwkw4rx2gx4!App"}</Data></Item></Replace>
```

Procedure

To configure a Custom payload:

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile** or **Device Profile**.

4. Configure the profile **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
5. 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.
6. **Save**, but do not publish, your profile.
7. Select the radio button from the **Profiles List View** for the row of the profile you want to customize.
8. Select the **XML** button at the top to view the profile X
9. 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.
10. Copy this section of text and close the XML View. Open your profile.
11. Select the **Custom Settings** payload and select **Configure**. Paste the XML you copied in the text box. The XML code you paste must contain the complete block of code, from <[characteristic]> to </[characteristic]>.
12. 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.

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

13. Select **Save & Publish**.

Prevent Users from Disabling the AirWatch Service

Use a Custom Settings profile to prevent end users from disabling the AirWatch Service on their Windows 10 devices. Preventing end users from disabling the AirWatch Service ensures that the AirWatch Agent runs regularly checks in with the AirWatch Console and receives the latest policy updates.

To prevent users from disabling the AirWatch Service:

1. Create a **Custom Settings** profile. For more information, see [Use Custom Settings \(Windows Desktop\) on page 98](#).
2. Set the **Target** to **Protection Agent**.
3. Copy the following code and paste it into the **Custom Settings** text box:

```
<wap-provisioningdoc id="c14e8e45-792c-4ec3-88e1-be121d8c33dc" name="customprofile">
  <characteristic type="com.airwatch.winrt.awservicelockdown" uuid="7957d046-7765-4422-9e39-6fd5eef38174">
    <parm name="LockDownAwService" value="True"/>
  </characteristic>
</wap-provisioningdoc>
```

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

4. Select **Save & Publish**.

If you want to remove the restriction from end user devices, you must push a separate profile using the following code:

```
<wap-provisioningdoc id="c14e8e45-792c-4ec3-88e1-be121d8c33dc" name="customprofile">  
    <characteristic type="com.airwatch.winrt.awservicelockdown" uuid="7957d046-7765-4422-9e39-  
6fd5eef38174">  
        <parm name="LockDownAwService" value="False"/>  
    </characteristic>  
</wap-provisioningdoc>
```

Chapter 4:

Compliance Policies

Compliance Policy Overview 102

Compromised Device Detection with Health Attestation 102

Compliance Policy Overview

The compliance engine is an automated tool by AirWatch that ensures all devices abide by your policies. These policies may include basic security settings such as requiring a passcode and having a minimum device lock period. For certain platforms, you may 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 AirWatch.

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, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).

Compromised Device Detection with Health Attestation

Health Attestation scans devices during startup to for failures in device integrity. Use Health Attestation to detect compromised Windows Desktop devices.

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

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

Configure the Health Attestation for Windows Desktop Compliance Policies

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

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

To use compromised device detection:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Windows Health Attestation**.
2. (Optional) Select **Use Custom Server** if you are using a custom on-premises server running Health Attestation. Enter the **Server URL**.
3. Configure the Health Attestation settings:

| Settings | Descriptions |
|--|--|
| 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. |

| Settings | Descriptions |
|---|---|
| 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. |
| 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 PCR0 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. |

4. Select **Save**.

Chapter 5:

Apps for Windows Desktop Devices

| | |
|---|-----|
| Windows Desktop Application Overview | 106 |
| VMware Workspace ONE for Windows Desktop | 106 |
| Configure the AirWatch Agent for Windows Desktop Devices | 106 |
| VMware Content Locker for Windows Desktop Devices | 108 |
| VMware Browser for Windows Desktop | 108 |

Windows Desktop Application Overview

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 AirWatch Agent for Windows to monitor your devices on a more granular level.

Deploying Win32 apps to Windows Desktop devices requires the AirWatch Protection Agent to be present on the device. For more information about deploying public, internal, and purchased applications, including an App Catalog, see the comprehensive **AirWatch Mobile Application Management Guide**.

Important: All public applications deployed to Windows Desktop devices are unmanaged applications. Unmanaged apps cannot be pushed to devices (end users must download the app themselves) nor can unmanaged apps be removed from devices through Enterprise Wipe.

VMware Workspace ONE for Windows Desktop

When the Workspace ONE application is installed on devices, users can sign in to Workspace ONE to securely access a catalog of applications that your organization enabled for them. When the application is configured with single sign-on, users do not need to reenter their sign-in credentials when they launch the app.

The Workspace ONE user interface works similarly on phones, tablets, and desktops. Workspace ONE opens to a Launcher page that displays resources that have been pushed to Workspace ONE. Users can tap or click to search, add, and update apps; right-click on an app to remove it from the page, and go to the Catalog page to add entitled resources.

If an app requires device enrollment, Workspace ONE uses adaptive management to start the enrollment process for the end user. For more information on Workspace ONE, see [Setting up the VMware Workspace ONE Application on Devices](https://www.vmware.com/support/pubs/identitymanager-pubs.html) available on the VMware Identity Manager Documentation Center (<https://www.vmware.com/support/pubs/identitymanager-pubs.html>).

Configure the AirWatch Agent for Windows Desktop Devices

The AirWatch Agent for Windows Desktop devices is pre-configured with AirWatch. Change these settings when you need the AirWatch Agent to meet certain business needs.]

You can prevent end users from disabling the AirWatch Service on their device using a custom XML profile. For more information, see [Prevent Users from Disabling the AirWatch Service on page 99](#).

Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Agent Settings** to edit the AirWatch Agent Settings:

- Configure the **Modern Agent** settings so that the AirWatch Agent transmits the desired data to the AirWatch Console:

| Settings | Descriptions |
|-----------------------------------|--|
| Heartbeat Interval (min) | Defines the intervals at which the AirWatch Agent and the AirWatch Console confirm a continued connection and synchronize. |
| Data Sample Interval (min) | Defines the intervals at which the AirWatch Agent takes samples of data. |
| Administrative Passcode | Sets the passcode to access administrative settings on the device. |

- Configure the **AirWatch Protection Agent** settings to ensure prompt communication between the device and the AirWatch Console.

| Settings | Descriptions |
|----------------------------|---|
| Data Sample Interval (min) | Defines the intervals at which the AirWatch Protection Agent takes samples of data. |

- Configure the **Remote Management** settings to enable communication between the AirWatch Agent and the Remote Management Server.

For more information, see the **VMware AirWatch Remote Management Guide** available on [AirWatch Resources](#).

| Setting | Description |
|------------------------------------|--|
| Download Remote Control Cab | Select this link to download the cabinet (CAB) installer file for AirWatch Remote Management. |
| Seek Permission | <p>Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin.</p> <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. |
| Advanced | |
| Remote Management Port | <p>Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device.</p> <p>This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.</p> |
| Device Log Level | Set the Device Log Level to control the verbosity of the remote management application on the device. |
| Log Folder Path | Define the Log Folder Path where the application saves the remote management log file on the device. |

| Setting | Description |
|--|---|
| Display Tray Icon | Enable Display Tray Icon to show the remote management applet on the device. |
| Max Sessions | Enter the maximum number of concurrent sessions allowed on a device. |
| Number of Retries | Enter the number of retries allowed before communication attempts stop. |
| Retry Frequency (Seconds) | Enter the amount of time between attempts to communicate. |
| Heartbeat Interval (Seconds) | Enter the amount of time (in seconds) that passes between status updates that are sent from the device. |
| Connection Loss Retry Frequency (Seconds) | Enter the amount of time (in seconds) that passes between attempts to reestablish the connection. |

VMware Content Locker for Windows Desktop Devices

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 Admin Console, content from synced corporate repositories, or their own personal content.

Use the AirWatch 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. For more information about configuring and deploying the VMware Content Locker, see the **Mobile Content Management (MCM) Guide** available in the [Resources Portal](#).

VMware Browser for Windows Desktop

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** available in the [Resources Portal](#).

Chapter 6:

Dell Client Command Integration

Dell Command | Monitor Integration110

Dell Command | Update Overview111

Dell Command | Monitor Integration

Integrate AirWatch with Dell Command | Monitor to enhance the information AirWatch collects from enrolled Dell enterprise devices. This integration also allows you to configure device BIOS settings.

Basics

Integrate with Dell Command | Monitor to enhance the device management of Dell enterprise devices. With this integration, AirWatch reports the device battery health status and certain BIOS settings.



Watch an overview video that explains Dell Command | Monitor Integration and shows the setup process: <https://support.air-watch.com/articles/115006430568>.

Supported Devices

- Dell OptiPlex™ desktop devices
- Dell Precision Workstation™ desktop and laptop devices
- Dell Latitude™ laptop devices

Add Dell Command | Monitor to AirWatch

To integrate Dell Command | Monitor with AirWatch, add the program as an internal Win32 application in the AirWatch Console. For more information, see [Add Dell Command | Monitor to AirWatch on page 110](#).

BIOS Profile

Configure certain BIOS settings on Dell enterprise devices using a BIOS profile. The settings allow you to control hardware virtualization and BIOS security. For more information, see [Configure a BIOS Profile \(Windows Desktop\) on page 92](#).

Battery Health Status

The overall health of a battery affects the lifespan of a device. With Dell Command | Monitor, monitor the health of your Dell enterprise device batteries. This health does not show the current charge of the battery but reports status of the ability to hold a charge, time to charge to full, and other factors as a percentage. According to Dell, any battery with a status under 25% should be replaced.

Add Dell Command | Monitor to AirWatch

To enhance management of your Dell enterprise devices, add the Dell Command | Monitor to the AirWatch Console. The BIOS profile requires this application before pushing to devices.

Prerequisites

You must enable Software Distribution to push Dell Command | Monitor to your devices.

Procedures

To add the Dell Command | Monitor:

1. Navigate to <http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor> and download the latest version of Dell Command | Monitor.
2. Open the EXE and select **Extract**. Save the extracted files into a folder.
3. Navigate to the folder and find the MSI file.
4. In the AirWatch Console, add the extracted MSI file as an internal application. Make sure to set the Supported Processor Architecture to 32-bit or 64-bit based on the device OS.
In the Deployment Options tab, set the **Admin Privileges** to **Yes**.
5. Add an assignment of the application to your Dell enterprise devices.

The application downloads and installs on assigned devices and you can now push BIOS profiles to the device.

Dell Command | Update Overview

Dell Command | Update is a client-side management software and part of the Dell Command Suite. The software enables updating firmware, drivers, and applications for supported Dell devices.

Basics

Integrate with Dell Command | Update to enhance the update management of Dell enterprise devices. With this integration, AirWatch supports remotely updating firmware, drivers, and other applications. You can control when and what types of updates deploy to devices.

Supported Devices

- Dell OptiPlex™ desktop devices
- Dell Precision Workstation™ desktop and laptop devices
- Dell Latitude™ laptop devices

Add Dell Command | Update to AirWatch

To integrate Dell Command | Update with AirWatch, add the application as an internal Win32 application in the AirWatch Console. For more information, see [Add Dell Command | Update to AirWatch on page 111](#).

Configure the OEM Updates Profile

Configure the OEM Updates profile to enabled Dell Command | Update on end-user devices. For more information, see [Configure the OEM Updates Profile \(Windows Desktop\) on page 95](#).

Add Dell Command | Update to AirWatch

To enhance management of your Dell enterprise devices, add the Dell Command | Update to the AirWatch Console. The OEM Update profile requires this application before pushing to devices.

Prerequisites

You must enable Software Distribution to push Dell Command | Update to your devices.

Procedures

To add the Dell Command | Update:

1. Navigate to <http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor> and download the latest version of Dell Command | Update.
2. Open the EXE and select **Extract**. Save the extracted files into a folder.
3. Navigate to the folder and find the MSI file.
4. In the AirWatch Console, add the extracted MSI file as an internal application. Make sure to set the Supported Processor Architecture to 32-bit or 64-bit based on the device OS.
In the Deployment Options tab, set the **Admin Privileges** to **Yes**.
5. Add an assignment of the application to your Dell enterprise devices.

The application downloads and installs on assigned devices and you can now push OEM Update profiles to the device.

Chapter 7:

Product Provisioning for Windows Desktop Devices

Product Provisioning Overview 114

Product Provisioning Overview

Product provisioning allows you to create, through AirWatch, products containing profiles, applications, and files/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 AirWatch Console. Create these servers for each store or warehouse to store product content for distribution to your devices.

For more information on product provisioning for Windows Desktop devices, see the **Product Provisioning for Windows Desktop Guide** available on [AirWatch Resources](#).

Chapter 8:

Managing Windows Desktop Devices

| | |
|--|-----|
| Windows Desktop Device Management Overview | 116 |
| Device Dashboard | 116 |
| Device List View | 116 |
| Windows Desktop Device Details Page | 117 |
| Remote Management | 118 |

Windows Desktop Device Management Overview

After your devices are enrolled and configured, manage the devices using the AirWatch 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 VMware AirWatch Dashboard. 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 AirWatch environment and their status. The Device Details page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

Device Dashboard

As devices are enrolled, you can manage them from the 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.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

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 choose 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**.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You may 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.

Windows Desktop Device Details Page

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 Actions** 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.
- **Apps (Query)** – Send a query command to the device to return a list of installed apps.
- **Certificates (Query)** – Send a query command to the device to return a list of installed certificates.
- **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 Admin Console. This action does not remove any data from the device itself, only its representation in the console.
- **Device Information (Query)** – Send a 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** – Wipe a device clear of all data, including email, profiles and MDM capabilities and the device returns to a factory default state. This includes all personal user information if applicable. 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 VMware AirWatch 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** – Lock the screen of a selected device, rendering it unusable until it is unlocked. Includes optional fields for a custom **Message**, **Phone Number**, and **Note Description**.

Important: When locking a device, an enrolled user must be signed into the device for the command to process. The lock command locks the device and any user signed in must reauthenticate with Windows. If an enrolled user is signed-in to the device, a lock device command locks the device. If an enrolled user is not signed in, the lock device command is not processed.

- **Query All** – Send a query command to the device to return a list of installed apps (including VMware AirWatch Agent, 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.
- **Security (Query)** – Send a query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** and **SMS**.

Remote Management

The Remote Management Service allows you to remotely connect to end-user devices so you can assist in troubleshooting and maintenance. The Remote Management Service requires your computer and the end user device to connect to the Remote Management Server to facilitate communication between the AirWatch Console and the end user device.

For more information on installing, configuring, and using the Remote Management Service, please see the **VMware AirWatch Remote Management Guide**, available on [AirWatch Resources](#).

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.