Windows Desktop Documentation

VMware Workspace ONE UEM 2111

vmware

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

https://docs.vmware.com/

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

Contents

Workspace ONE UEM Device Management, Enrollment Requirements, and Supported Windows Operating Systems

1

Workspace ONE UEM powered by AirWatch provides you with a set of mobility management solutions for enrolling, securing, configuring, and managing your Windows device deployment. To use Workspace ONE UEM's management solutions, meet the requirements to enroll supported Windows devices. Management solution availability depends on the Windows OS version of your devices.

This chapter includes the following topics:

Workspace ONE UEM Supports Windows 11

Workspace ONE UEM supports Windows 11 devices. When configuring the console, use the **Windows Desktop** option because this option works for Windows 10 and Windows 11 devices. Windows 11 is built on the same foundation as Windows 10 so features in Workspace ONE UEM that are available for Windows 10 are also available for Windows 11. If you find a Workspace ONE UEM feature that works on Windows 10 but not on Windows 11, let us know by contacting VMware Global Services.

For details on Windows 11, see Microsoft's documentation on What's new in Windows.

Workspace ONE UEM Device Management for Windows Devices

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

Workspace ONE UEM 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 Workspace ONE UEM allows you to secure and configure devices to meet your needs.

Enrollment Requirements for Windows Devices

Before enrolling your Windows devices with Workspace ONE UEM, your devices and users must meet the listed requirements and configurations or enrollment does not work.

User-Side Requirements

Your Windows users must meet this list of requirements to enroll their devices with Workspace ONE UEM.

- **Admin Permissions** – The logged in user enrolling the device must be an Administrator.
- **Group ID** – If your Workspace ONE UEM environment prompts users for their Group ID, the logged in user needs this value.
- **Device Root Certificate** - All users need the Device Root Certificate configured in the System Settings before enrolling their devices. To configure the certificate, navigate to **Groups & Settings** > **All Settings** > **System** > **Advanced** > **Device Root Certificate**.
- **Enrollment URL** – All users can enter a unique URL that takes them directly to the enrollment screen to enroll in a Workspace ONE UEM environment. For example, **mdm.example.com**.**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.

Device-Side Requirements

Your Windows devices must access the listed sites, have the listed settings enabled, and have the listed services running to enroll with Workspace ONE UEM.

- **Access URLs** - Trust these URLs in your firewall policies so your enrolled devices can access them.
  - **App Center API URLs** - Allows Workspace ONE Intelligent Hub for Windows to provide crash information to the Microsoft Store.
    - `api.appcenter.ms`
    - `api.mobile.azure.com`

    - **Microsoft Store API URL** - Ensures that the Workspace ONE Intelligent Hub for Windows launches on your Windows devices no matter what Microsoft Store market your devices are used in. If you are interested in information on the Microsoft Store and app support by market, see the article Define Market Selection.
        - `http://licensing.mp.microsoft.com/v7.0/licenses/contentHTTPSUsed`
- **PowerShell Execution** - Enable PowerShell Execution on your Windows devices because Workspace ONE UEM uses PowerShell for installation and operational changes through the Workspace ONE Intelligent Hub.
- **Windows Services** - Your Windows devices must have the listed services in a **Service State: Running** to enroll and work in your Workspace ONE UEM deployment.
    - DmEnrollmentSvc (Device Management Enrollment Service)
    - DiagTrack (Connected User Experiences and Telemetry)
    - Schedule (Task Scheduler)
    - BITS (Background Intelligent Transfer Service)
    - dmwappushservice (Device Management Wireless Application Protocol (WAP) Push message Routing Service)

What Windows OS Versions Are Supported?

Workspace ONE UEM supports enrolling and managing Windows devices. The level of support depends on the OS version and device architecture.

Workspace ONE UEM supports devices running the following operating systems:

- Windows Pro
- Windows Enterprise
- Windows Education
- Windows Home
- Windows S

Workspace ONE Intelligent Hub does not support Windows ARM Snapdragon or Hololens devices. These devices must use native MDM functionality.

Important: To see the OS version each update branch supports, see Microsoft's documentation on Windows release information: Windows release health.

Windows Version Matrix

Compare the MDM functionality available in each version of the Windows OS. Workspace ONE UEM supports all versions of Windows OS and the functions they support.

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

Feature	Windows OS Home	Windows OS Professional	Windows OS Enterprise	Windows OS Education
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	✓	✓	✓	✓
SMS				
Email Messages		✓	✓	✓
Password Policy	✓	✓	✓	✓
Enterprise Wipe	✓	✓	✓	✓
Full Device Wipe	✓	✓	✓	✓
Email & Exchange ActiveSync	✓	✓	✓	✓
Wi-Fi	✓	✓	✓	✓
VPN	✓	✓	✓	✓
Certificate Management	✓	✓	✓	✓
Device Restrictions and Settings	✓	✓	✓	✓
Windows Hello	✓	✓	✓	✓
Personalization			✓	✓
Encryption		✓	✓	✓
Application Control (AppLocker)			✓	✓
Health Attestation	✓	✓	✓	✓

Feature	Windows OS Home	Windows OS Professional	Windows OS Enterprise	Windows OS Education
Windows Update for Business		✓	✓	✓
Assigned Access			✓	✓
Application Management		✓	✓	✓
Workspace ONE Content	✓	✓	✓	✓
Asset Tracking		✓	✓	✓
Device Status		✓	✓	✓
IP Address				
Location	✓	✓	✓	✓
Network		✓	✓	✓
Send Support Message (Email and SMS only)		✓	✓	✓

Enrolling Windows Devices into Workspace ONE UEM

2

Workspace ONE UEM supports several different methods to enroll your Windows devices. Learn which enrollment workflow best services your needs based on your Workspace ONE UEM deployment, enterprise integrations, and device operating system.

This chapter includes the following topics:

Enrollment Basics

Simplify your end-user enrollments by setting up the Windows Auto-Discovery Services (WADS) in your Workspace ONE UEM 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, Workspace ONE Intelligent Hub for Windows, or Azure AD integration.

If you want to use Workspace ONE UEM 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 Workspace ONE UEM.

- Workspace ONE Intelligent Hub for Windows Enrollment

  The simplest enrollment workflow uses Workspace ONE Intelligent Hub for Windows to enroll devices. End users simply download Workspace ONE Intelligent Hub from getwsone.com and follow the prompts to enroll.

Consider using Workspace ONE Intelligent Hub for the Windows Enrollment workflow. Workspace ONE UEM supports additional enrollment flows that meet specific use cases.

- Azure AD Integration Enrollment

  Through integration with Microsoft Azure Active Directory, Windows devices automatically enroll into Workspace ONE UEM 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 Workspace ONE UEM.

  Before you can enroll your devices using Azure AD integration, you must configure Workspace ONE UEM and Azure AD.

- Native MDM Enrollment

  Workspace ONE UEM 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.

  Only users with local admin permissions on the device can enroll a device into Workspace ONE UEM and enable MDM.

- Device Staging

  If you want to configure device management on a Windows device before shipping it to your end user, consider using Windows Desktop device staging. This enrollment workflow allows you to enroll a device through Workspace ONE Intelligent Hub, 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 devices.

- Windows Desktop Auto-Enrollment

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

- Bulk Provisioning and Enrollment

  Bulk provisioning creates a pre-configured package that stages Windows devices and enrolls them intoWorkspace ONE UEM. 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 Workspace ONE UEM settings in the provisioning package so that provisioned devices automatically enroll during the initial Out of Box Experience.

- Registered Mode - Enroll Without Device Management

  To allow some Windows devices to enroll into Workspace ONE UEM without device management services, you can enable Registered Mode. Assign this mode to an entire organization group or with smart groups.

Workspace ONE Intelligent Hub for Windows Enrollment

Workspace ONE Intelligent Hub provides a single resource for enrollment and facilitates communication between the device and the Workspace ONE UEM console. Use Workspace ONE Intelligent Hub to enroll your Windows devices. Workspace ONE Intelligent Hub provides a simplified enrollment flow for end users that is quick and easy enrollment.

Consider using Workspace ONE Intelligent Hub for Windows to enroll your Windows Desktop devices as it provides the simplest enrollment flow for users. If you have Workspace ONE configured, downloading Workspace ONE Intelligent Hub from https://getwsone.com/ also downloads the Workspace ONE app. When you finish enrolling with Workspace ONE Intelligent Hub, the Workspace ONE app auto-launches and configures based on your Workspace ONE UEM deployment.

The Workspace ONE Intelligent Hub 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.

AirWatch Cloud Messaging (AWCM) enables real-time policy and command delivery to Workspace ONE Intelligent Hub. Without AWCM, Workspace ONE Intelligent Hub only receives policy and command delivery during its normal check-in intervals set in the Workspace ONE UEM console. Consider using AWCM for real-time policy and command delivery to Windows Desktop devices.

Procedure to Enroll with the VMware Workspace ONE Intelligent Hub

1 On the Windows Desktop device, navigate to https://getwsone.com.

2 Install Workspace ONE Intelligent Hub. When the installation is finished, start Workspace ONE Intelligent Hub.

3 Enter the email address and select **Next**.

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

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

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

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

5 **Accept** the terms of use.

6 Select **Done**.

7 Open Workspace ONE Intelligent Hub and complete the enrollment.

Native MDM Enrollment for Windows Desktop

Windows Desktop enrollment methods all use the Work Access native MDM Client. Use the native MDM enrollment to enroll both corporate owned and BYOD devices through the same enrollment flow. You can enroll with or without Windows Auto Discovery.

Work Access first processes an Azure AD work flow for domains connected to Office 365 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 Workspace ONE Intelligent Hub to enroll Windows 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 enabled **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.

Only users who have local admin permissions on the device can enroll a device into Workspace ONE UEM and enable MDM. Domain Admin permissions do not work for enrolling a device. To enroll a device with a standard user, you must use Bulk Provisioning for Windows devices.

By using the Windows Auto-Discovery Service, you simplify enrollment for your end user by reducing the necessary interaction during enrollment.

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 devices. Enrolling through Work Access and using Windows Auto Discovery provides a quick and easy enrollment flow for end users.

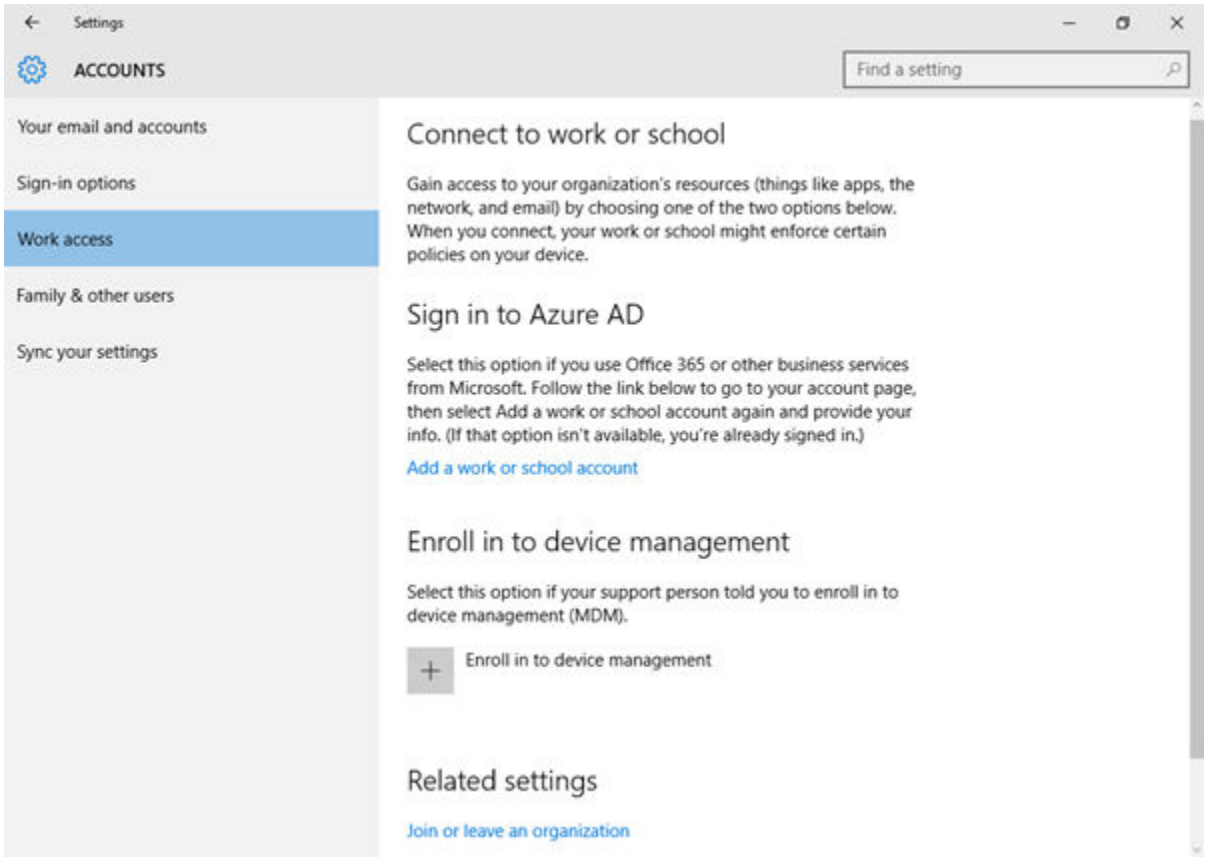
Prerequisites

Registering your domain in Workspace ONE UEM removes the need to enter the Group ID during enrollment.

Note: Consider using the Workspace ONE Intelligent Hub for Windows to enroll your Windows 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.

Procedure

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**.

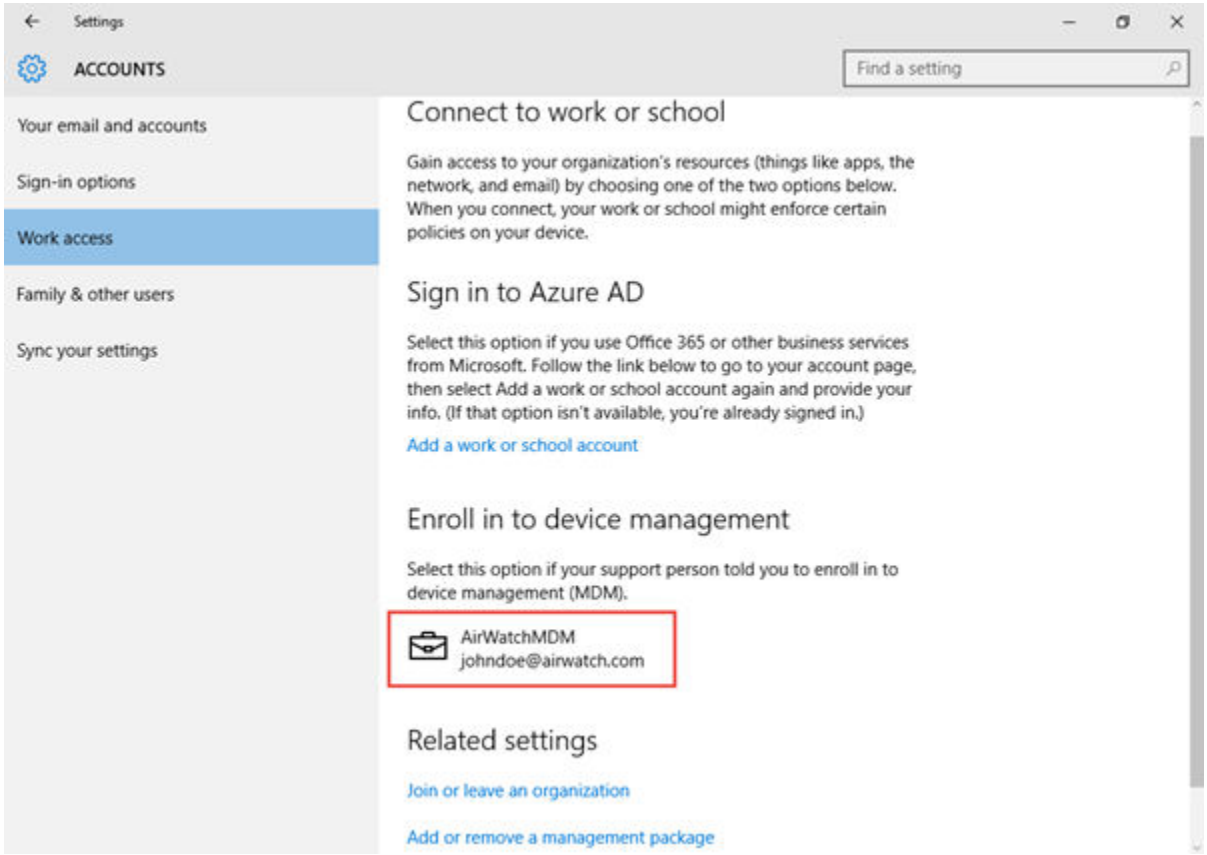
4 Enter your **username** and **password** and select **Next**. These credentials may be your directory services credentials or dedicated credentials specific to your Workspace ONE UEM environment.

5 **Optional**: Review the End User License Agreement and select **Accept** to agree to the terms of use.

6 **Optional**: Select **Yes** to save sign-in info.

Results

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



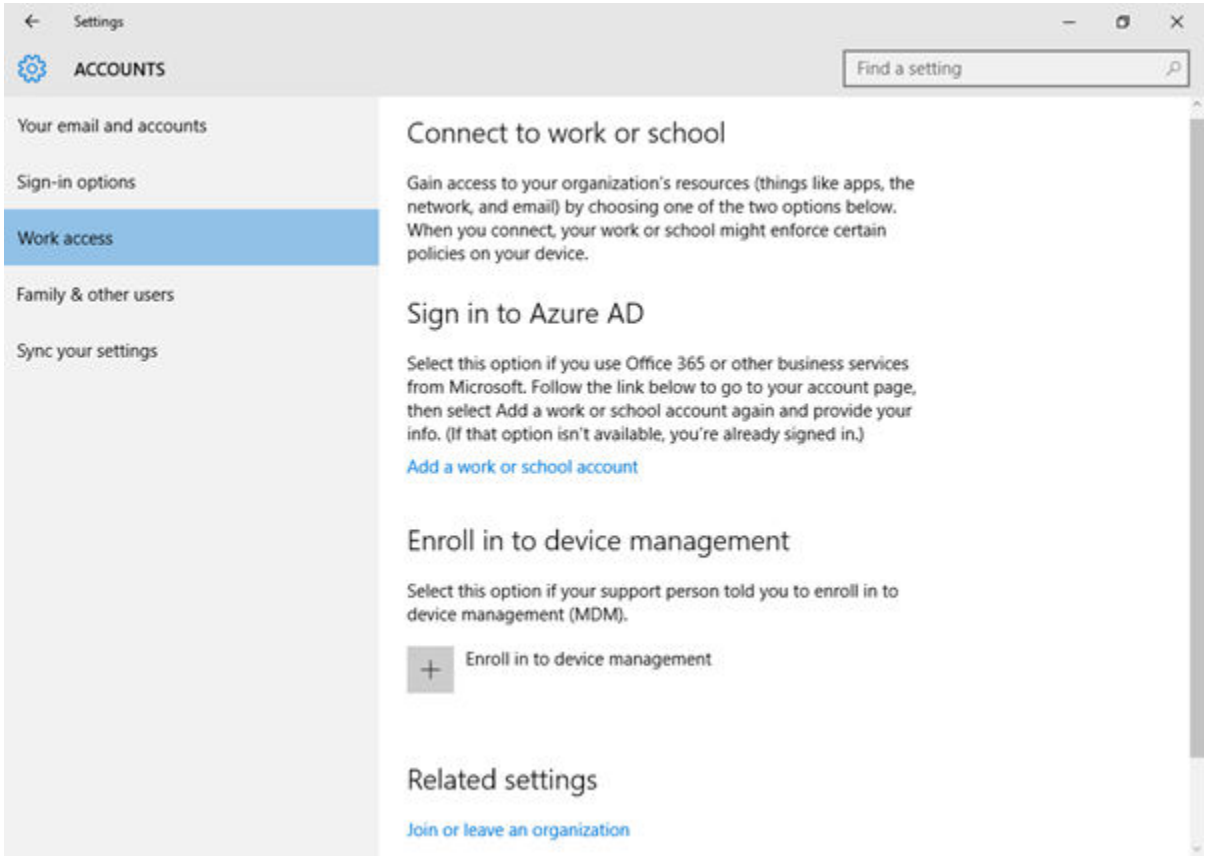
Enroll Through Work Access Without Windows Auto Discovery

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

Consider using the Workspace ONE Intelligent Hub for Windows to enroll your Windows 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.

Procedure

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. **Example**: `ds156.awmdm.com/deviceservices/discovery.aws`.

4 Select **Continue**.

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

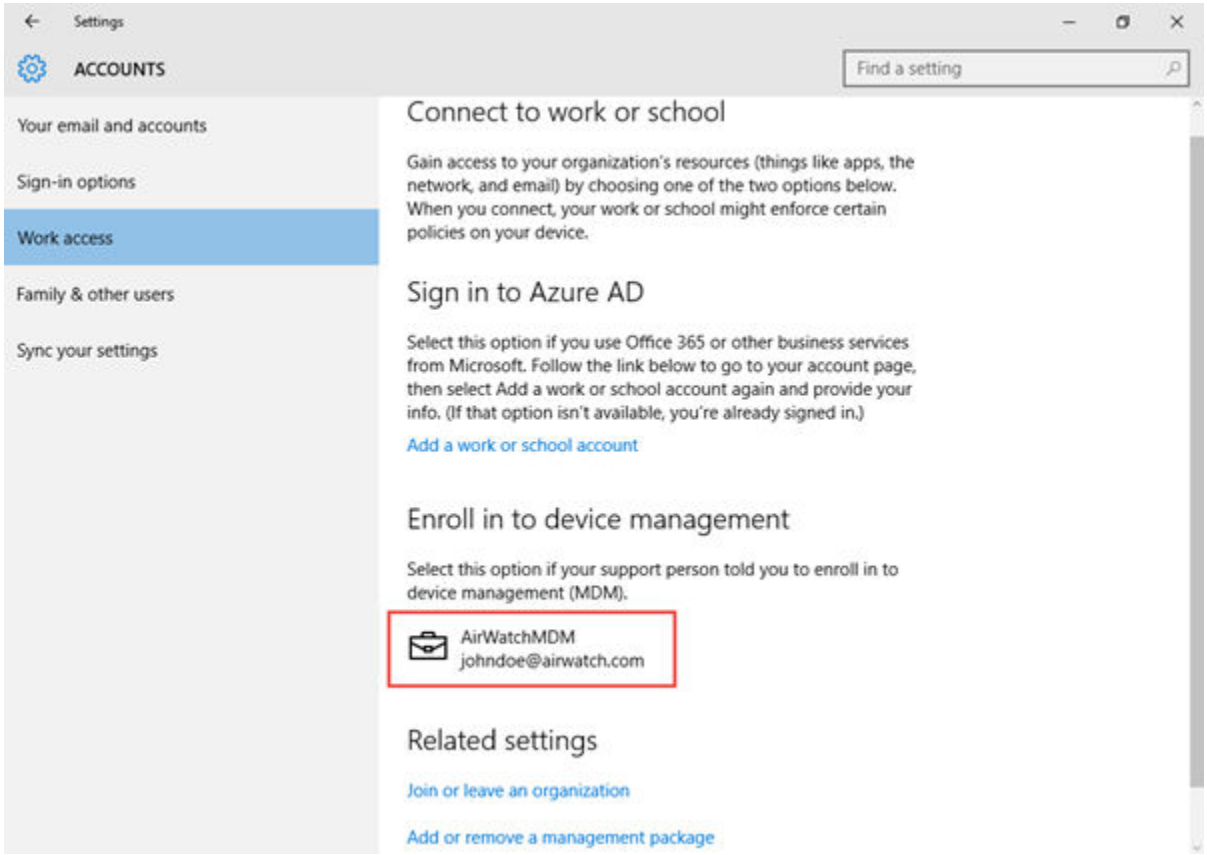
6 Enter your **username** and **password** and select **Next**. These credentials may be your directory services credentials, or dedicated credentials specific to your Workspace ONE UEM environment.

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.

Results

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



Windows Device Staging Enrollment

With device staging, you can configure your Windows devices for device management by Workspace ONE UEM before you send the devices to your end users. Learn how to enroll and configure your devices with Workspace ONE Intelligent Hub on behalf of your end users.

Device staging enrollment enables you to enroll your Windows device into Workspace ONE UEM. This enrollment requires the Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub updates the device record in the Workspace ONE UEM console. Workspace ONE UEM 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 Workspace ONE Intelligent Hub and enter enrollment credentials. This method requires devices to be domain-joined before enrollment.
- **Command Line Installation** – Download the Workspace ONE Intelligent Hub and then install and enroll the device using the command line.

The enrollment completes by either updating the UEM 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 Workspace ONE UEM Console. The bulk import requires a CSV file with all the serial numbers to import.

Procedure

1 Navigate to **Accounts** > **Users** > **List View** or **Devices** > **Lifecycle** > **Enrollment Status**.

2 Select **Add** and then **Batch Import** to display the **Batch Import** screen.

3 Complete each of the required options. **Batch Name**, **Batch Description**, and **Batch Type**.

4 Within the **Batch File (.csv)** option is a list of task-based templates you can use to load users and their devices in bulk.

5 Select the appropriate download template and save the comma-separated values (CSV) file to somewhere accessible.

6 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.

7 Save the completed template as a CSV file. In the UEM 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.

8 Select **Save** to complete registration for all listed users and corresponding devices.

Carbon Black and Workspace ONE Intelligent Hub for Windows

Do you use Carbon Black for endpoint protection on your Windows devices? You can install Carbon Black on your Windows devices when you install the Workspace ONE Intelligent Hub for Windows.

Enroll your Windows devices with this command-line staging process. Enter Carbon Black specific silent enrollment parameters and their respective URL values that you generated in Carbon Black. Entering the generated URLs instructs the Workspace ONE Intelligent Hub to retrieve the URLs for the Carbon Black sensor kit and the Carbon Black sensor configuration file for installation.

After you install Carbon Black and the Workspace ONE Intelligent Hub, upload the Carbon Black public app to the Workspace ONE UEM console and publish the app to your Windows devices.

For details on how to generate the required URLs for the Carbon Black sensor kit and the Carbon Black sensor configuration file, access the content in the *Carbon Black Cloud User Guide*. You can sign in to VMware Carbon Black Cloud and select **Help** > **User Guide**. Type `workspace one` in the search bar and press **Enter**.

Where Are The Carbon Black Parameters?

The Carbon Black parameters are listed in this topic in the **Silent Enrollment Parameters and Values** section. You can also find them in the Carbon Black Cloud console at **Inventory > Endpoints > Sensor Options > Configure Workspace ONE sensor kit**. If you do not see this option in the Carbon Black Cloud console, contact your Carbon Black support to enable the feature.

Enroll Through Command-Line Staging

Simplify enrollment for end users by staging your Windows Desktop devices using the Windows Command Line. This enrollment method for Workspace ONE UEM 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 breaks the staging command. Also, Do not use bulk serial number import if you want to use command-line staging.

Note: Do not use this product to install Workspace ONE Intelligent Hub for Windows silently on BYOD devices. If you silently install onto BYOD devices, you are solely responsible for providing any necessary notices to your device end users regarding your use of silent installation and the data collected from the silently installed apps. You are responsible for obtaining any legally required consents from your device end users, and otherwise complying with all applicable laws.

Procedure

1 Navigate to https://getwsone.com/ to download Workspace ONE Intelligent Hub for Windows.

   Only download Workspace ONE Intelligent Hub. Do not start the executable or select **Run** as that initiates a standard enrollment process and defeats the purpose of silent enrollment. If necessary, move Workspace ONE Intelligent Hub from the download folder to a local or network drive folder.

2 Open a command line or create a BAT file and enter all the necessary paths, parameters, and values.

3 Run the command.

Results

After the command runs, the device enrolls into Workspace ONE UEM. If the device is domain-joined, Workspace ONE Intelligent Hub updates the Workspace ONE UEM console device registry with the correct user.

Enroll Through Manual Device Staging

Simplify enrollment for end users by staging your Windows devices using the Workspace ONE Intelligent Hub. 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.

Prerequisites

These devices must be joined to a domain.

1 Navigate to https://getwsone.com/ to download the Workspace ONE Intelligent Hub Installer.

2 Start the installer once the download completes.

3 Select **Run** to begin the installation.

4 Select **Email** if you have Auto-Discovery enabled, otherwise select **Server Detail**.

5 Complete the settings required based on the authentication type selected.

   a Enter the email address to auto-fill the server details screen. Select **Next** and the details are entered.

   b Enter the Server Name and Group ID if you are not using 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.

Results

Once the Workspace ONE Intelligent Hub detects a staging user, the Workspace ONE Intelligent Hub listener runs and listens for the next Windows login. When the end user logs into the device, the Workspace ONE Intelligent Hublistener reads the user UPN and email from the device registry. This information is sent to the Workspace ONE UEM 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 Workspace ONE Intelligent Hub downloads and installs onto Windows devices.

Note: Do not use this product to install Workspace ONE Intelligent Hub for Windows silently on BYOD devices. If you silently install to BYOD devices, you are solely responsible for providing any necessary notices to your device end users regarding your use of silent installation and the data collected from the silently installed apps. You are responsible for obtaining any legally required consents from your device end users, and otherwise complying with all applicable laws.

The following tables list the enrollment parameters you can enter into a command line or into a BAT file, and the respective values for each parameter. If you are Enrolling on Behalf of Others (EOBO), ensure you use the EOBO parameters.

General Parameters

Enrollment Parameters	Values to Add to Parameter
All MSI parameters	These parameters control the app installation behavior. `/quiet` - Completely silent `/q` - Controls the UI levels for installation `passive` - Minimal controls for the user to guide the application `/L` - Log levels and log paths. For more information, see https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options.
ASSIGNTOLOGGEDINUSER	Select `Y` to assign the device to the domain user that is logged in. Enter this parameter as the last argument in the command line.
DEVICEOWNERSHIPTYPE^	Select `CD` for Corporate Dedicated. Select `CS` for Corporate Shared. Select `EO` for Employee Owned. Select `N` for None.
DOWNLOADSBUNDLE	This parameter controls the download of the Workspace ONE application during enrollment. Select `TRUE`, to download the Workspace ONE app installer during the installation of Workspace ONE Intelligent Hub. If you enroll a device using Workspace ONE Intelligent Hub, installing Workspace ONE is not optional. If you do not set DOWNLOADSBUNDLE to `TRUE`, the Workspace ONE app installer does not download regardless of the UI-level used.
ENROLL	Select `Y` to enroll. Select `N` for image only. The agent tries to enroll in silent mode only if this parameter is set to `Y`.
IMAGE	This flag takes priority over everything, if this flag is set to `Y`, the agent is put into image mode. Select `Y` for image. Select `N` for enrollment.
INSTALLDIR^	Enter the directory path if you want to change the installation path. **Note**: If this parameter is not present, the Workspace ONE Intelligent Hub uses the default path: `C:\Program Files (x86)\AirWatch`.
LGName	Enter the organization group name.
PASSWORD	Enter the password for the user you are enrolling or the staging user password if staging the device on the behalf of a user.
SERVER	Enter the enrollment URL.
USERNAME	Enter the user name for the user you are enrolling or the staging user name if staging the device on the behalf of a user.

Items denoted with a caret (^) are optional.

EOBO Parameters

Enrollment Parameters	Values to Add to Parameter
SECURITYTYPE	EOBO Workflow Only: Use this parameter if a user account is added to the Workspace ONE UEM console during the enrollment process. Select `D` for **Directory**. Select `B` for **Basic User**.
STAGEEMAIL^	EOBO Workflow Only: Enter the email address for the user you are enrolling.
STAGEEMAILUSRNAME^	EOBO Workflow Only: Enter the email user name for the user you are enrolling.
STAGEPASSWORD	EOBO Workflow Only: Enter the password for the user you are enrolling.
STAGEUSERNAME	EOBO Workflow Only: Enter user name for the enrolling user.

Items denoted with a caret (^) are optional.

Carbon Black Parameters

Enrollment Parameters	Values to Add to Parameter
CBSENSORCONFIGURL^	Use this parameter to instruct the Workspace ONE Intelligent Hub for Windows to retrieve the Carbon Black configuration file URL. Enter the URL for the sensor configuration file that you generated in Carbon Black.
CBSENSORURL^	Use this parameter to instruct the Workspace ONE Intelligent Hub for Windows to retrieve the applicable Carbon Black sensor kit URL. Enter the URL for the sensor kit that you generated in Carbon Black.

Items denoted with a caret (^) are optional.

Examples of Silent Enrollment

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

- **Agent Install for Image Only Without Enrollment**

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

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

- **Basic User Enrollment**

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

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

- **Workspace ONE Intelligent Hub Installed Elsewhere**

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

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

- **Installation Directory and Workspace ONE Intelligent Hub on Network Drive**

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

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

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

- **Available Parameters and Values**

  The following snippet is an example of the syntax using most of the available parameters and values.

```
msiexec.exe /I "<Path>AirwatchAgent.msi" /quiet ENROLL=<Y/N>IMAGE=<Y/
N>SERVER=<CompanyURL>LGNAME=<Location Group ID>USERNAME=<Staging
Username>PASSWORD=<Staging Username Password>STAGEUSERNAME=<Enrolling
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>
```

Workspace ONE UEM and Azure AD Integration

Through integration with Microsoft Azure Active Directory, you can automatically enroll your Windows devices into Workspace ONE UEM with minimal end-user interaction. Learn how Azure AD integration simplifies enrolling your Windows devices.

Before you can enroll your devices using Azure AD Integration, you must configure Workspace ONE UEM and Azure AD. The configuration requires entering information into your Azure AD and Workspace ONE UEM deployments to facilitate communication. Setup is different depending on your environment. Follow the appropriate procedure for your SaaS or on-premises deployment.

Azure AD integration enrollment supports three different enrollment flows.

- Join Azure AD
- Out of Box Experience enrollment
- Office 365 enrollment

All methods require configuring Azure AD integration with Workspace ONE UEM.

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

SaaS Environments: Azure AD as an Identity Service

Before you can use Azure AD to enroll your Windows devices, you must configure Workspace ONE UEM to use Azure AD as an identity service. Enabling Azure AD requires entering data in both the Azure Management Portal and in Workspace ONE UEM. Use tabs in your browser to have both instances open to help with entering data in both consoles.

Prerequisites

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

Important: Configure and Save LDAP First If you are setting the **Current Setting** to **Override** on the Directory Services system settings page in Workspace ONE UEM, you must configure and save the LDAP settings before enabling Azure AD for identity services.

Procedure

1 In Workspace ONE UEM, enable the integration with Azure AD, enter the Azure AD Tenant ID, and retrieve MDM enrollment URLs to enter into Azure.

   a Select the applicable organization group.

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

   c On the **Server** tab, enable **Azure AD Integration**.

   d In another tab in your browser, log in to the Azure Management Portal with your Microsoft account or organizational account to get the **Azure AD Tenant ID**.

      1 Select **Azure Active Directory** to view the **Overview** page.

      2 Copy the **Azure AD Tenant ID** from the Azure AD **Overview** page

   e Go back to the Workspace ONE UEM console instance and paste the Azure AD Tenant ID into in the **Directory ID** text box.

   f Continuing in the Workspace ONE UEM instance, enable **Use Azure AD For Identity Services**. Note the **MDM discovery URL** and the **MDM Terms of Use URL** because you must enter them into Azure. You can copy them between tabs if you are using multiple browser tabs or consider copying them somewhere on your PC.

2 In Azure AD, add the Workspace ONE UEM app and add the MDM URLs.

   a In the Azure Management Portal instance, select your directory and navigate to the **Mobility (MDM and MAM)** tab.

   b Select **Add Application**, select the **AirWatch by VMware** app, and choose **Add**.

   c Select the **AirWatch by VMware** app that you just added to change the MDM user scope to **All**.

   d Copy your **MDM Terms of Use URL** from your PC or from the browser tab with the Workspace ONE UEM instance, and paste it into the **MDM terms of use URL** text box in Azure.

   e Copy your **MDM discovery URL** from your PC or from the browser tab with the Workspace ONE UEM console instance and paste it into the **MDM discovery URL** text box in Azure.

f Save your settings.

3 In Workspace ONE UEM, enter the Azure AD **Primary** domain and save the settings.

a In the Azure Management Portal instance, go to the Azure AD **Overview** page and copy the **Primary** domain from the Azure AD **Overview** page.

b On the browser tab with the Workspace ONE UEM console instance, paste the **Primary** domain string in the **Tenant Name** text box.

c Save the settings on the Workspace ONE UEM **Directory Services** page.

4 In Azure, assign premium licenses.

a In the Microsoft Azure console, select **Azure Active Directory > Licenses**.

b Select **All Products** and select the proper license in the list.

c Select **Assign**, select the users or groups for the license, and select **Assign** to complete the process.

On-Premises Environments: Azure AD as an Identity Service

Before you can use Azure AD to enroll your Windows devices, you must configure Workspace ONE UEM to use Azure AD as an identity service. Enabling Azure AD requires entering data in both the Azure Management Portal and in Workspace ONE UEM. Use tabs in your browser to have both instances open to help with entering data in both consoles.

Prerequisites

- You must have a Premium Azure AD P1 or P2 subscription to integrate Azure AD with Workspace ONE UEM.
- Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory (such as LDAP) is configured.
- In the Azure Active Directory portal, add a custom domain for your domain name with Microsoft Azure. Follow Microsoft's documentation at Add your custom domain name using the Azure Active Directory portal.

Important: Configure and Save LDAP First If you are setting the **Current Setting** to **Override** on the **Directory Services** system settings page in Workspace ONE UEM, you must configure and save the LDAP settings before enabling Azure AD for identity services.

Procedure

1 In Workspace ONE UEM, enable the integration with Azure AD, enter the Azure AD Tenant ID, and retrieve MDM enrollment URLs to enter into Azure.

a Select the applicable organization group.

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

c On the **Server** tab, enable **Azure AD Integration**.

d In another tab in your browser, log in to the Azure Management Portal with your Microsoft account or organizational account and get the **Azure AD Tenant ID**.

1 Select **Azure Active Directory** to view the **Overview** page.

2 Copy the **Azure AD Tenant ID** from the Azure AD **Overview** page.

e Go to the Workspace ONE UEM console instance and paste the Azure AD Tenant ID into in the **Directory ID** text box.

f Continuing in the Workspace ONE UEM instance, enable **Use Azure AD For Identity Services**. Note the **MDM discovery URL** and the **MDM Terms of Use URL** because you must enter them into Azure. You can copy them between tabs if you are using multiple browser tabs or consider copying them somewhere on your PC.

2 In Azure AD, add the on-premises version of the Workspace ONE UEM app and add the MDM URLs.

a In the Azure Management Portal instance, select your directory and navigate to the **Mobility (MDM and MAM)** tab.

b Select **Add Application** and select the **On Premises MDM** app. Then, choose **Add**.

c Select the **On Premises MDM** app that you just added to set the **MDM user scope** to **All** or **Some**.

d Select a group of users.

e Copy your **MDM Terms of Use URL** from your PC or from the browser tab with the Workspace ONE UEM instance, and paste it into the **MDM terms of use URL** text box in Azure.

f Copy your **MDM discovery URL** from your PC or from the browser tab with the Workspace ONE UEM console instance and paste it into the **MDM discovery URL** text box in Azure.

g Save your settings.

3 In the Azure Management Portal, add your Workspace ONE UEM device services URL.

a In the Workspace ONE UEM instance, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** and copy your **Device Services URL**.

b In the Azure Management Portal instance, select **On-Premises MDM application settings > Expose an API**.

c Select **Edit** for **Application ID URI** and enter your device services URL in the **Application ID URI** text box.

d Save the settings. **Note**: Saving the settings works if you performed the prerequisite task of adding a custom domain name. If you see an error, check that you added your custom domain to Azure.

4 In Workspace ONE UEM, enter the Azure AD **Primary** domain and save the settings.
   a In the Azure Management Portal instance, go to the Azure AD **Overview** page and copy the **Primary** domain from the Azure AD **Overview** page.
   b In the Workspace ONE UEM console instance, paste the **Primary** domain string in the **Tenant Name** text box.
   c Save the settings on the Workspace ONE UEM **Directory Services** page.
5 In Azure, assign premium licenses.
   a In the Microsoft Azure console, select **Azure Active Directory > Licenses**.
   b Select **All Products** and select the proper license in the list.
   c Select **Assign**, select the users or groups for the license, and select **Assign** 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 Workspace ONE UEM 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.

Procedure

1 Navigate on the Windows device to **Settings > Accounts > Access Work or School**. Select **Continue**.
2 Enter your **Email Address**. Select **Next**.
3 Ensure that the Workspace ONE UEM 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 Workspace ONE UEM.
6 Select **Finish** to complete joining your device to Workspace ONE UEM. Your device now downloads the applicable policies and profiles.

Enroll an Azure AD Managed Device into Workspace ONE UEM

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 Workspace ONE UEM.

Prerequisites

- Windows 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

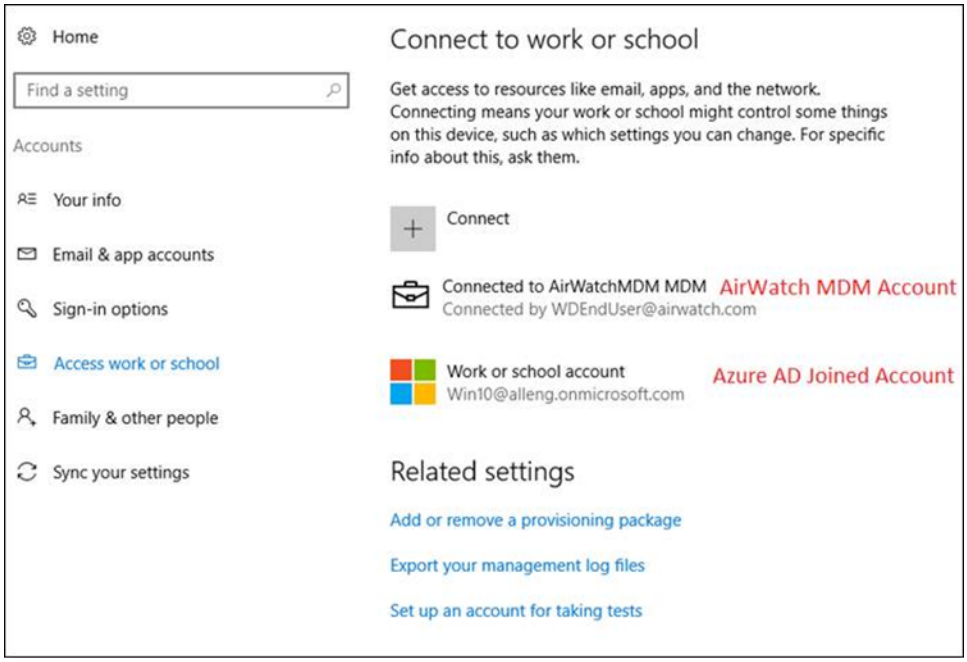
1 On the device, navigate to **Settings > Accounts > Access work or school** and select **Enroll only in device management**. You may also enroll through the Workspace ONE Intelligent Hub for Windows.

2 Complete the enrollment process. You must enter an email address with a different domain than your Azure AD account.

   a If you are using Windows Auto-Discovery, see Enroll Through Work Access With Windows Auto-Discovery.

   b If you are not using Windows Auto-Discovery, see Enroll Through Work Access Without Windows Auto-Discovery.

3 Navigate to **Settings > Accounts > Access** work or school and ensure that there is an Azure AD account and a Workspace ONE UEM MDM account added.



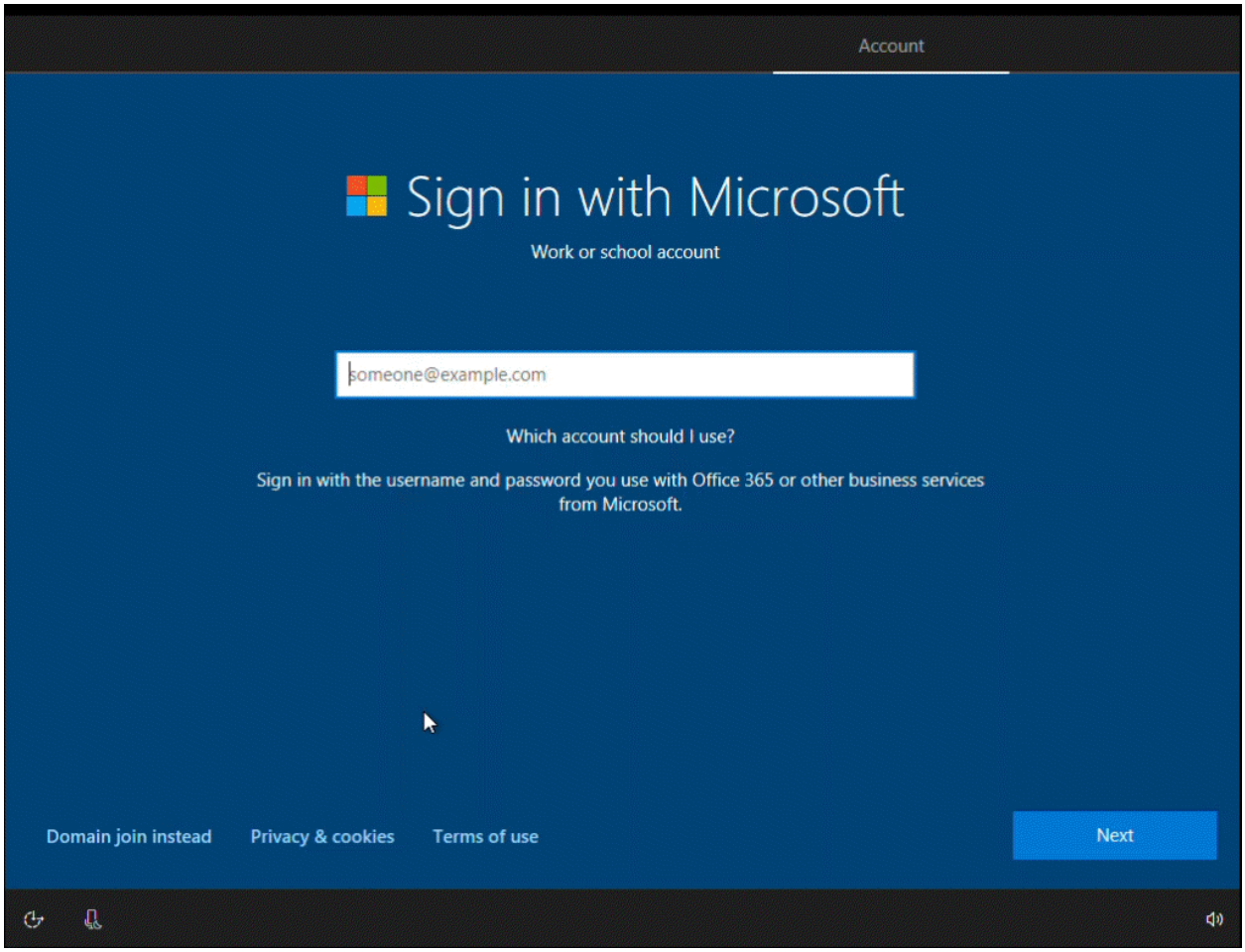
Enroll Through Out of Box Experience

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 device.

Important: The OOBE enrollment flow does not support Enterprise Wipe. If you perform an enterprise wipe, users cannot log into the device as connection to Azure AD has been broken. You must create a local admin account before sending an Enterprise Wipe or you get locked out of the device and forced to reset the device.

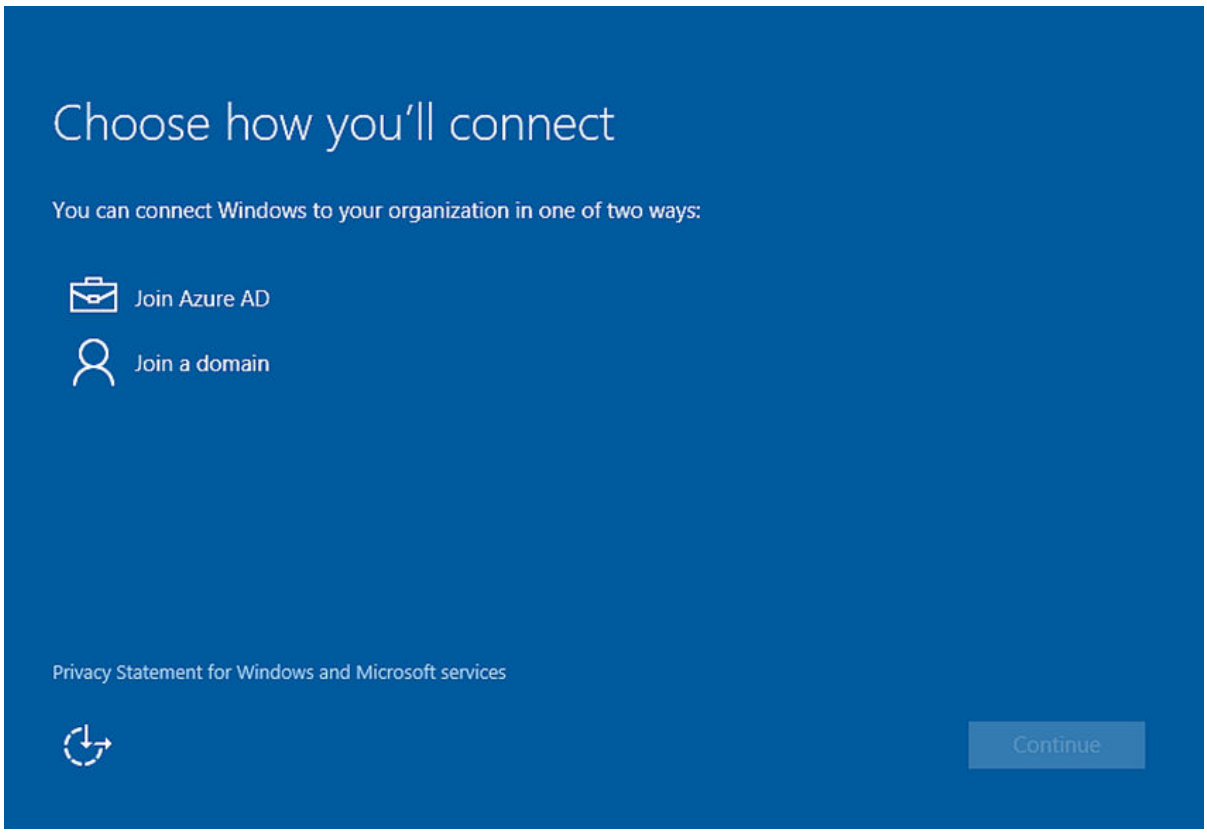
Prerequisites

The OOBE process can take some time to complete on end-user devices. Consider enabling the progress display for the install status. This display allows end users to know where they are in the process. To enable the display, navigate to **Groups & Settings** > **All Settings** > **General** > **Enrollment** > **Optional Prompt**. To display the status of profiles during enrollment, you must enabled the **Track Profile Status during OOBE Provisioning** option in the **General** profile settings.



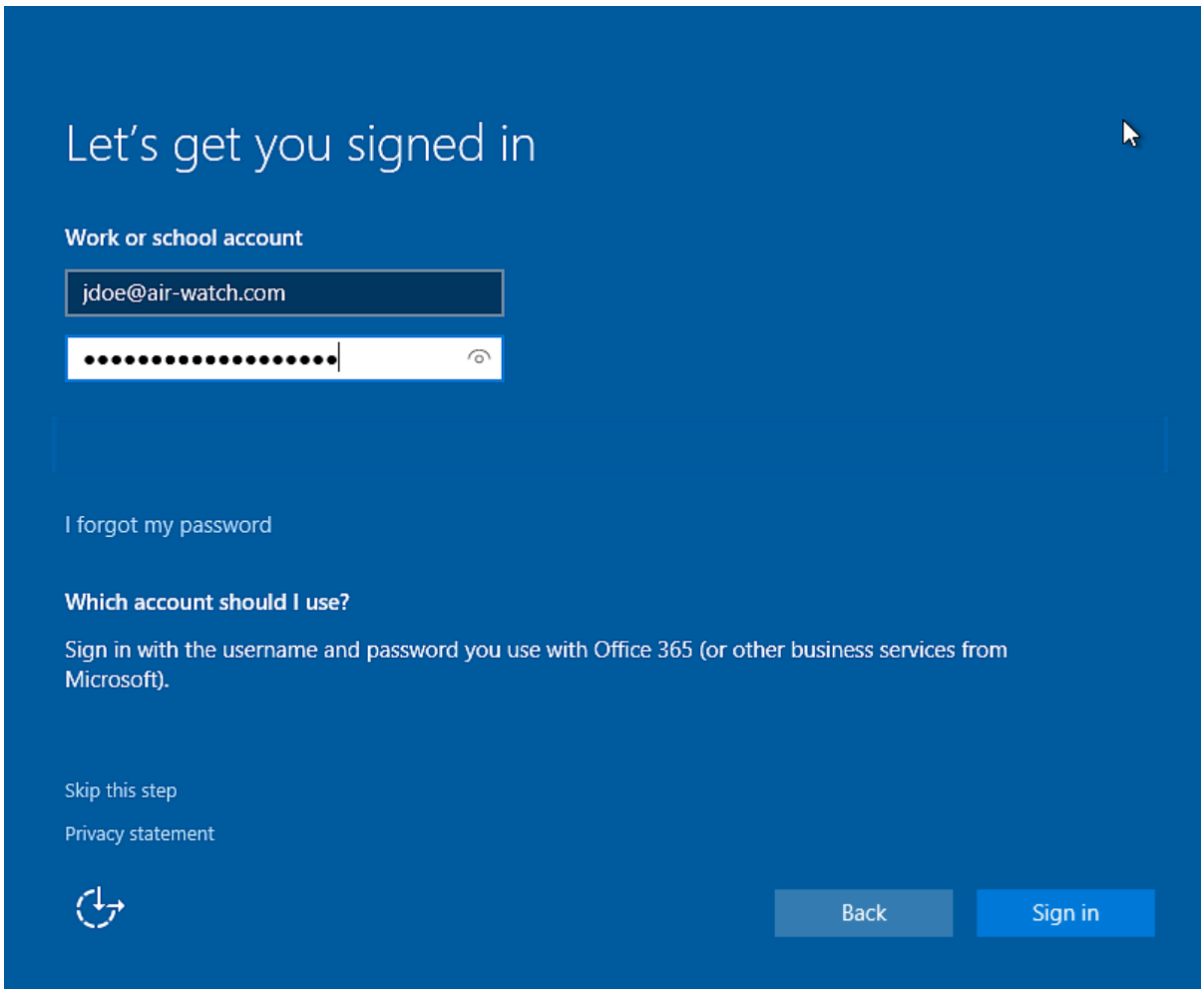
Procedure

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



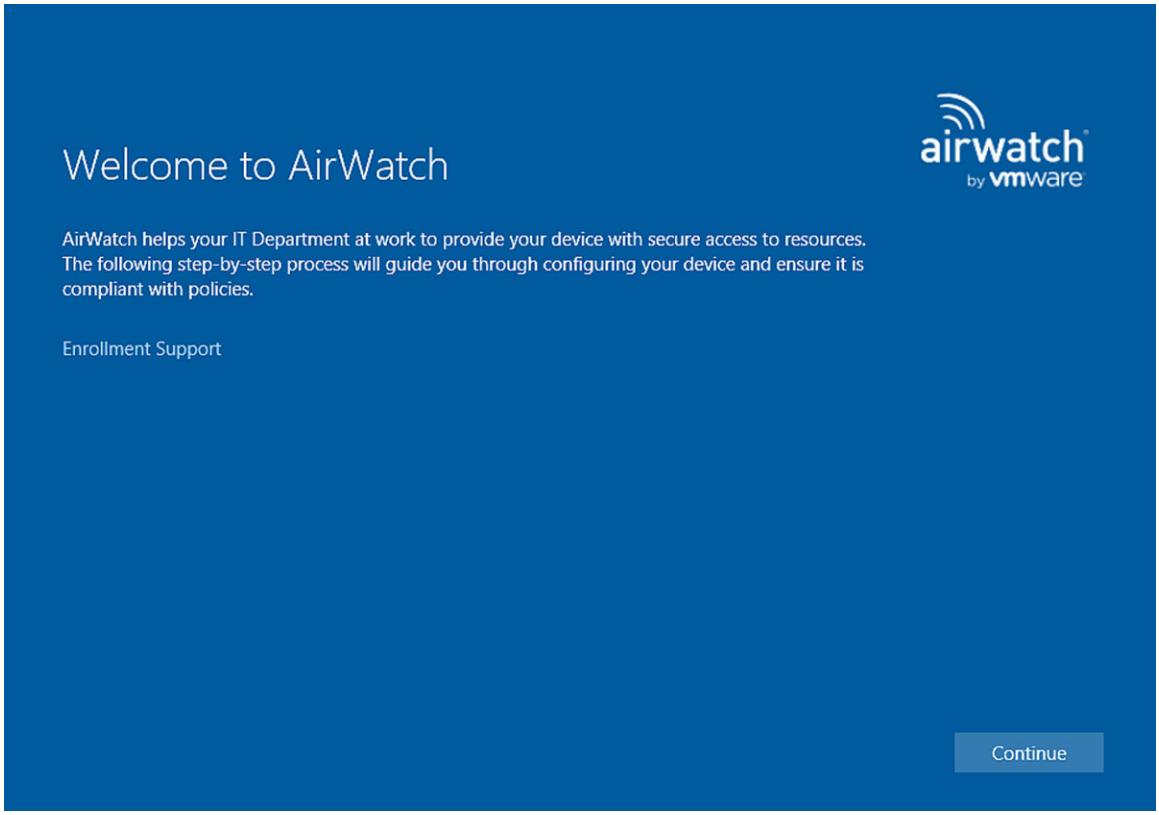
2 Select **Join Azure AD**. Select **Continue**.

3 Enter your Azure AD/Workspace ONE UEM 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 the **Device Ownership** type and enter the **Asset Number** if applicable. Select **Next**.

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

8 Select **Join** to confirm that you want to enroll in Workspace ONE UEM.

9 Select **Finish** to complete joining your device to Workspace ONE UEM. 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.

Procedure

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 Workspace ONE UEM 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 Workspace ONE UEM.

6 Select **Finish** to complete joining your device to Workspace ONE UEM. Your device now downloads the applicable policies and profiles.

Bulk Provisioning and Enrollment for Windows Devices

Bulk provisioning lets you create a pre-configured package that stages Windows devices and enrolls them into Workspace ONE UEM. Learn how to use bulk provisioning to enroll and configure multiple devices with a standard user account.

This enrollment flow is the only way to enroll a device with a standard user account. Admin permissions are still required 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 Workspace ONE UEM configuration settings so that provisioned devices are automatically enrolled into Workspace ONE UEM 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 devices into Workspace ONE UEM quickly and easily. Once the package is installed, the device automatically enrolls into Workspace ONE UEM.

Procedure

1 Download the Microsoft Assessment and Deployment Kit for Windows 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.

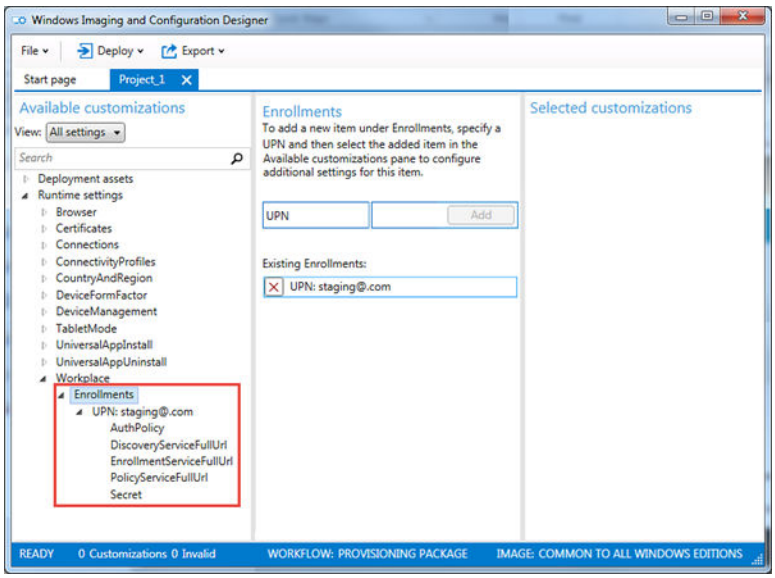
4 (Optional) Import a provisioning package if you want to create a provisioning package based on the settings of a previous package.

5 Navigate to **Runtime Settings > Workplace > Enrollments**.

6 In the Workspace ONE UEM 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.

   a Select **AuthPolicy** and select the value displayed in the Workspace ONE UEM console.

   b Select **DiscoveryServiceFullURL** and copy the URL displayed in the Workspace ONE UEM console.

   c Select **EnrollmentServiceFullURL** and copy the URL displayed in the Workspace ONE UEM console.

   d Select **PolicyServiceFullURL** and copy the URL displayed in the Workspace ONE UEM console.

   e Select **Secret** and copy the value displayed in the Workspace ONE UEM 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.

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.

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 Workspace ONE UEM console before provisioning, the device is assigned upon enrollment.

Enroll with Registered Mode

Windows devices enrolled through the Workspace ONE Intelligent Hub or OOBE are MDM managed by default. To allow Windows devices to enroll without MDM management, you can enable registered mode (unmanaged) for an entire organization group or with smart groups and specific criteria.

Registered mode supports the listed enrollment methods.

- Staging Users
  - Command line staging
  - Manual device staging
  - Silent enrollment parameters and values
- Workspace ONE Intelligent Hub for Windows with SAML authentication

Enable registered mode by organization groups or by smart groups. When you use smart groups, group devices for registered mode by OS version, platform, ownership type, or users.

With registered mode enrollment, users can use a subset of Workspace ONE services without MDM management including Workspace ONE Assist, VMware Workspace ONE Tunnel, Digital Experience Employee Management (DEEM), and Workspace ONE Hub Services.

Procedure

1 In the Workspace ONE UEM console, select the organization group to be enabled with registered mode enrollment and navigate to **Devices** > **Devices Settings** > **Device & Users** > **General** > **Enrollment** > **Management Mode**.

2 For **Current Setting**, select **Override**.

3 For **Windows**, select **Enabled**.

4 Select **Enabled** for **All Windows devices in this Organization Group**.

5 Optionally, you can add smart groups that are enabled for registered mode enrollments in **Windows Smart Groups**.

6 Save your settings.

Results

Users with Windows devices from the configured smart group or the specified organization group can use product capabilities without MDM management. Device information and management capabilities from with the console are limited. Only the relevant profiles are installed on these devices.

Post-Enrollment Onboarding Settings

Admins have been shifting from imaging-based workflows to just-in-time provisioning over-the-air. In these provisioning scenarios, it is important to inform users about what is happening while their devices enroll. Workspace ONE Intelligent Hub for Windows displays and notifies the statuses of applications that are actively downloading and installing during the Windows enrollment process. This feature also provides a way to customize the user messaging during setup.

Considerations

- Post-enrollment onboarding settings are enabled by default on Windows devices managed in Workspace ONE UEM.
- The feature works in Workspace ONE UEM 2105 or later.
- The feature works with the Workspace ONE Intelligent Hub for Windows 21.05 and later.
- Enrolling through the Workspace ONE Intelligent Hub for Windows is not required as this feature works for any enrollment method, including Web Enrollment. However, you must install the app on devices to apply configurations and to display the experience.

Behaviors of the Workspace ONE Intelligent Hub

- When installed, the Workspace ONE Intelligent Hub for Windows detects the enrollment and launches the experience. **Note**: The experience does not apply to upgrade scenarios. It only impacts new enrollments.
- Directly after enrollment, the Workspace ONE Intelligent Hub launches and displays your customizations and tracks all apps which are set to **Automatic** deployment.

Deactivate the Post-Enrollment Onboarding Experience

1 Select the applicable organization group.

2 In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > Devices & Users > General > Enrollment > Optional Prompt > Windows > Enable Post-Enrollment Onboarding Experience**.

3 Deactivate the setting.

Customize the Post-Enrollment Onboarding Experience Message

1 Select the applicable organization group.

2 In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > Devices & Users > General > Enrollment > Optional Prompt > Windows > Enable Post-Enrollment Onboarding Experience**.

3 If this feature was deactivated previously, select **Enabled**. The feature is enabled by default.

4 When post-enrollment onboarding is enabled, you can customize the **Welcome Header**, **Welcome Subheader**, and **Body Text** fields of the post-enrollment onboarding experience message using text and lookup values.

Windows Enrollment Statuses

If you look at enrollment settings on the **Devices** > **Devices Settings** > **Devices & Users** > **General** > **Enrollment** page, you see three general enrollment scenarios for Windows devices.

- **Open Enrollment**

  Allows anyone meeting other enrollment criteria (authentication mode, restrictions, and so on) to enroll.

- **Registered Devices Only**

  Allows users to enroll using devices you or they have registered. Device registration is the process of adding corporate devices to the Workspace ONE UEM console before they are enrolled. This matrix applies to devices that register without a token.

- **Require Registration Token**

  If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment. This increases security by confirming that a particular user is authorized to enroll.

Device Type

The type of device guides how the Workspace ONE UEM system tracks and displays the device's enrollment status.

- Allowlisted devices - The Workspace ONE UEM admin adds a list of devices that are pre-approved to enroll.
- Denylisted devices - The Workspace ONE UEM admin adds a list of devices that are not allowed to enroll.
- Registered devices (without attributes) - The Workspace ONE UEM admin registers devices by adding device information to the console. If the admin does not enter device attributes, the system uses device information, which includes user, platform, model, and ownership type.
- Registered devices (with attributes) - The Workspace ONE UEM admin registers devices by adding device attributes to the console. Device attributes include UDID, IMEI, and serial number.

Enrollment Lifecycle for Devices

Device enrollment with Workspace ONE UEM has three general stages.

1 (Optional) Admins register devices or users self-register their devices in Workspace ONE UEM.

  Registration helps restrict enrollment.

2 Device users or admins enroll devices with Workspace ONE UEM.

3 Device users or admins unenroll devices with Workspace ONE UEM.

Console Displays Set Statuses

The enrollment type, device type, and stage of enrollment dictate the **Enrollment Status** and **Token Status** displayed for Windows devices on the **Devices** > **Lifecycle** > **Enrollment Status** page.

Open Enrollment

Type	Registered devices - Enrollment Status	Registered devices - Token Status	Enrolled devices - Enrollment Status	Enrolled devices - Token Status	Unenrolled devices - Enrollment Status	Unenrolled devices - Token Status
Allowlisted device	Registered	Compliant	Enrolled	Compliant	Unenrolled	Compliant
Denylisted device	Denylisted	Non-Compliant	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Registered device without attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Registration Active	Registered	Registration Active
Registered device with attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Registration Active	Registered	Registration Active

Registered Devices Only (No Token)

Type	Registered devices - Enrollment Status	Registered devices - Token Status	Enrolled devices - Enrollment Status	Enrolled devices - Token Status	Unenrolled devices - Enrollment Status	Unenrolled devices - Token Status
Allowlisted device	Registered	Compliant	Enrolled	Compliant	Unenrolled	Compliant
Denylisted device	Denylisted	Non-Compliant	Not Applicable	Not Applicable	Not Applicable	Not Applicable

Type	Registered devices - Enrollment Status	Registered devices - Token Status	Enrolled devices - Enrollment Status	Enrolled devices - Token Status	Unenrolled devices - Enrollment Status	Unenrolled devices - Token Status
Registered device without attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Registration Active	Registered	Registration Active
Registered device with attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Expired	Registered	Registration Active

Require Registration Token

Type	Registered devices - Enrollment Status	Registered devices - Token Status	Enrolled devices - Enrollment Status	Enrolled devices - Token Status	Unenrolled devices - Enrollment Status	Unenrolled devices - Token Status
Registered device without attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Not Applicable	Unenrolled	Registration Expired
Registered device with attributes Attributes are Serial Number, IMEI, and UDID.	Registered	Registration Active	Enrolled	Not Applicable	Unenrolled	Registration Expired

Using Baselines

3

Keep your Windows Desktop devices configured to best practices with Baselines. Workspace ONE UEM curates industry-recommended settings into one Baseline configuration to simplify securing your devices. Baselines reduce the time it takes to set up and configure Windows devices.

This chapter includes the following topics:

Cloud-Based Micro-Service

Baselines use a cloud-based micro service to handle the policy catalog. If you are an on-premises customer, ensure that your environment can communicate with the micro-service.

Baselines Require Constant Connectivity to Device Services

All enrolled Windows devices that use Baselines require uninterrupted connectivity to the Workspace ONE UEM Device Services (DS) server. Devices need this constant connectivity for Baseline statuses to remain current.

If you use a proxy setup or have certain firewall settings, these configurations can interrupt the connection between your Windows devices and the DS server. For example, if devices use a VPN or a restricted network to access resources, this set up interrupts the connection to the DS server. Baselines on these devices are at risk of being out of date.

Types of Baselines

- Custom
  - If you have an existing Group Policy Object (GPO) backup file, you can create a custom Baseline with those policies. Use the template process to create this custom Baseline.
  - You can also create a custom Baseline without a template. Workspace ONE UEM offers policies in the **Create your own** process for Baselines.
- CIS Windows Benchmarks - This Baseline applies the configuration settings proposed by CIS Benchmarks. To ensure that Baselines use only the best settings and configurations, CIS (Center for Internet Security) certifies VMware to provide industry favorites such as CIS Benchmarks for Windows.
- Windows Security Baseline - This Baseline applies the configuration settings proposed by Microsoft.

Baselines are based on the Windows OS version of your devices. You can change the OS version of any Baseline later when editing. During configuration, you can choose which Baseline to use and customize any of the Baseline policies. You can also add additional Microsoft ADMX-backed policies as part of the configuration process.

CIS Benchmark Considerations

CIS reports the listed benchmarks to establish a more secure connection between your server and your devices. However, these benchmarks are not currently supported by the CIS Windows Benchmarks Baseline template. Admins must configure these benchmarks. See the applicable Windows Server CIS Benchmark report for details.

- Configure an Interactive logon title and text for users attempting to login.
- Install the LAPS (Local Administrator Password Solution) AdmPwd GPO Extension / CSE.

What Happens After You Assign Baselines?

After enrolling a device into Workspace ONE UEM, you can add the device to a smart group and assign a Baseline to the group. The device receives and applies all the settings and configurations in the Baseline after a device restart. The device checks for the Baseline configurations upon publishing the Baseline and at the defined check-in intervals. When you push a Baseline to a device, Workspace ONE UEM stores a snapshot of the device settings.

How Do I Control the Assignment of Baselines?

You can limit the assignment of the Baseline using the **Exclusions** tab of the **Assignment** dialog box. You can designate smart groups to exclude from the assignment.

Baselines Management

You can manage your Baselines from the **Baselines** list view, found in the console at **Resources > Profiles & Baselines > Baselines**. From here, you can edit, copy, and delete existing Baselines.

- **Copy**: You can copy Baselines and edit a few policies on the **Customize** and **Add Policies** tabs to fit the Baseline to another deployment scenario. Select the desired Baseline to display the **Copy** menu item.
  - You cannot edit the Baseline template. If you need a different template, create a new Baseline.
  - Workspace ONE UEM saves the copied Baseline as `Copy of <Baseline Name>`, but you can change the name.
  - Save the copied Baseline but do not assign devices to it until you have edited the **Managed By** field (organization group). You cannot move copied Baselines that already have devices assigned.
  - Organization groups (**Managed By**) and copied Baselines have caveats.
    - To change the organization group, you edit the copied Baseline after you save it.
    - You can move the copied Baseline to child organization groups or leave it in the original organization group.
    - You cannot move the copied Baseline up the organization group hierarchy. This behavior mirrors the behavior for profiles.
- **Delete**: If you delete a Baseline that was pushed to devices, the device settings revert to their previous configurations based on the snapshot stored by Workspace ONE UEM.

You can see which Baselines are applied to a device in the **Device Details** page.

Example of How To Copy a Baseline

Here is a general example of how you can copy an existing Baseline and update the **Managed By** field to move the Baseline to a child organization group.

1 In the Workspace ONE UEM console, go to the applicable organization group.

2 Go to **Resources > Profiles & Baselines > Baselines**.

3 Select a Baseline from the list and select **Copy**.

4 Update the name of the Baseline in the **Baseline Name** field. You cannot update the organization group at this time.

5 Move through the Baselines wizard making updates as needed. You do not have to make changes, you can select **Next** for any tab.

6 On the **Summary** tab, select **Save & Assign**.

7 On the **Assign Baseline** page, select **Cancel**. This action cancels assigning devices to the copied Baseline. **Important**: Do not assign devices to your copied Baseline until you have edited the organization group.

8 Select the copied Baseline in the list and select **Edit**.

9 Update the organization group by selecting a child organization group in **General > Managed By**.

10 Move through the wizard and select **Save and Publish**.

11 Select the copied Baseline and select **Assign** when you are ready to add devices.

Baselines Compliance Status

Ensure that your device follows the Baselines with the Baseline compliance status. Find the **Compliance Status** in the console at **Resources > Profiles & Baselines > Baselines**, select the Baseline, and see the **Compliance Status** card. The **Baseline Compliance Status** card shows when devices are compliant, intermediate, non-compliant, or not available.

Note: Baseline compliance status only applies to Baselines created using the UI. You cannot see the compliance status for custom Baselines created using GPO backup files.

- The **Intermediate** status identifies devices that are 85% to 99% compliant. This status is an indicator that your devices have decreased their compliance with assigned Baselines.
- The **Not Available** status means that the Workspace ONE UEM console does not have a compliance sample for the device. You can force a sample by opening the Baseline and publishing it again.

Verifying Compliance Status

In the event a setting on the device does not match the Baseline, use the troubleshooting tab in **Device Details** to verify that Workspace ONE UEM received the device sample.

1 In the Workspace ONE UEM console, go to **Devices** and select the specific Windows Desktop device.

2 Select the **Troubleshooting** tab in the **Device Details** view to see the **Event Log** and the **Commands** tab.

3 On the **Commands** tab, see a list of Baseline query commands. You can see the listed statuses.

   - **Queued**: The system has entered the command into the server database.
   - **Pending**: The device has received the request, but has not responded.
   - **Processed**: The device has sent a sample or the device has the sample queued for the next user session.

4 On the **Event Log** tab, see an **Event** that confirms that **Baseline Sample Response Received**.

Creating Baselines

Create a Baseline with templates or without them to configure your devices to industry-recommended settings and configurations. Workspace ONE UEM curates Baselines based on industry favorites including CIS Benchmarks and Microsoft's Windows security Baselines.

Prerequisites

Your devices must be enrolled in Workspace ONE UEM and they must have the Workspace ONE Intelligent Hub installed.

If you are publishing a custom Baseline using a GPO backup file, you must add the LGPO.exe to all devices that you want to assign a Baseline to. You must install the EXE at `C:\ProgramData\Airwatch\LGPO\LGPO.exe`. If you are using the CIS Benchmark template, Windows Security template, or Create-your-own wizard, you do not need to add this file.

Creating with Templates

If you want to use a GPO backup file to create your Baselines, use the template process.

1 Navigate to **Resources** > **Profiles & Baselines** > **Baselines** and select **New**.

2 Select **Use template**.

3 Enter a **Baseline Name**, **Description**, and select the smart group the Baseline is **Managed By**. Then select **Next**.

4 Select a Baseline.

Setting	Description
CIS Windows Benchmarks	This Baseline applies the configuration settings proposed by CIS Benchmarks. Select the OS version and benchmark level to apply.
Windows Security Baseline	This Baseline applies the configuration settings proposed by Microsoft. Select the OS version and benchmark level to apply.
Custom Baseline	Upload a ZIP file with a GPO backup. You must create this Baseline outside of Workspace ONE UEM. The backup must be less than 5 MB with at least one GPO folder.

5 Select **Next**.

6 Customize the Baseline as needed. You can change any of the existing ADMX policies configured in the Baseline. When creating a custom Baseline from a GPO Baseline, you cannot customize the existing ADMX-backed policies. Ensure you use SIDs when creating User Rights ADMX policies. For more information, see Well-known security identifiers in Windows operating systems.

7 Select **Next**.

8 Add additional policies to the Baseline. These policies come from Microsoft ADMX files. Search for any policy to add and configure it.

9 Select **Next**.

10 Review the summary and select **Save & Assign**. The summary includes any customized or added policies.

11 During assignment, enter the smart group containing the Windows devices you want to assign the Baseline to. You can redefine which devices get the Baseline using the **Exclusions** tab. Enter the smart groups you want to exclude from assignment. Exclusions override assignments. If a device is in an excluded smart group, that device does not receive the Baseline. If that device already had the Baseline from a previous assignment, the Baseline is removed from the device.

12 Restart devices to deploy Baselines.

Creating Your Own

If you do not want to use a template, create your own Baselines without a template.

1 Navigate to **Resources** > **Profiles & Baselines** > **Baselines** and select **New**.

2 Select **Create your own**.

3 Enter a **Baseline Name**, **Description**, and select the smart group the Baseline is **Managed By**. Then select **Next**.

4 In the **Add Policy** window, select the Windows OS version, then start to enter a policy name. For example, enter `User` or `Computer Configuration` and then select the desired policy from the list.

5 Add additional policies to the Baseline. These policies come from Microsoft ADMX files. Search for a policy to add and configure it. These policies are the same ones available with templates, but they display as **Not Configured**. You must enable and configure the policy or you must disable the policy.

6 Select the status of this policy on devices as **Enabled**, **Disabled**, or **Not Configured**.

7 Review the summary and select **Save & Assign**. The summary includes all policies.

8 During assignment, enter the smart group containing the Windows devices you want to assign the Baseline to. You can redefine which devices get the Baseline using the **Exclusions** tab. Enter the smart groups you want to exclude from assignment. Exclusions override assignments. If a device is in an excluded smart group, that device does not receive the Baseline. If that device already had the Baseline from a previous assignment, the Baseline is removed from the device.

9 Restart devices to deploy Baselines.

Compliance Policies

4

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

This chapter includes the following topics:

Compliance Policies in Workspace ONE UEM

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

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

Dell BIOS Verification for Workspace ONE UEM

Ensure that your Dell Windows Desktop devices remain secure with Dell Trusted Device (formerly, Dell BIOS Verification). This service analyses the BIOS of your Dell devices and reports the status to Workspace ONE UEM so you can act against any compromised devices.

Benefits of Dell Trusted Device

The BIOS is a part in maintaining the overall device health and security. Modern computer systems rely on BIOS firmware to initialize hardware during the boot process and for runtime services that support the operating system and applications. This privileged position within the device architecture makes unauthorized modification of the BIOS firmware a significant threat. The Dell Trusted Device service provides secure BIOS validation using a secure signed response model. The status of the secure validation helps you act on compromised devices with the compliance policy engine.

Prepare Your Devices for Dell Trusted Device

To use Dell Trusted Device on your Windows Desktop devices, you must install the Dell Trusted Device service on the device. You must download the latest client from Dell (https://www.dell.com/support/home/product-support/product/trusted-device/drivers. Consider using Software Distribution to install the client on your Dell Windows Desktop devices.

Dell BIOS Verification Statuses

After you install the client onto your devices, you can see the reported status in the Device Details page. The statuses are as follows:

- Pass - The Dell Trusted Device client is installed on the device and the device is secure.
- Fail - The Dell Trusted Device client is installed and one of the following issues is present:
  - The Pre-Check event returns a fail result. This result happens when the client detects an invalid binary signature.
  - The BIOS Utility event returns a fail result for the validation test.
  - The BIOS Server Processing event returns a fail result for an invalid signature, invalid exit code, or the payload status is out of sync.
- Warning - The Dell Trusted Device is installed and the client detects an issue. The device might not be secured, so investigate the issue. Causes for a Warning status might include the following list.
  - No network connection
  - Invalid command-line argument
  - Application is running with insufficient privileges.
  - Internal errors in the client
  - Server responds with an error.
  - Driver issues with the client
  - Unknown results in the BIOS verification

- If you see a gray warning icon, the Dell Trusted Device client is not installed on the device.

Compromised Device Detection with Health Attestation

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.

Workspace ONE UEM enables you to configure the Windows Health Attestation service to ensure device compliance. If any of the enabled checks fail, the Workspace ONE UEM 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 Workspace ONE UEM 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 Workspace ONE UEM to check the device integrity during startup and take corrective actions.

Procedure

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
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 Deactivated	Enable to flag compromised device status when Secure Boot is deactivated 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.

Settings	Descriptions
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 Deactivated	Enable to flag compromised device status when the DEP is deactivated 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 deactivated	Enable to flag compromised device status when BitLocker encryption is deactivated on the device.
Code Integrity Check Deactivated	Enable to flag compromised device status when the code integrity check is deactivated 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 Deactivated	Enable to flag compromised device status when the early launch anti-malware is deactivated on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.

4 Select **Save**.

Windows Desktop Applications 5

You can use Workspace ONE UEM applications in addition to Workspace ONE UEM MDM features to further secure devices and configure them with added functionality. Use the Workspace ONE Intelligent Hub for Windows to catalog and manage your applications and to facilitate communication between the device and the Workspace ONE UEM console.

This chapter includes the following topics:

Workspace ONE Productivity Apps

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

Deploying Win32 apps to Windows Desktop devices requires the Workspace ONE Intelligent Hub to be present on the device.

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 App for Windows Desktop

When the Workspace ONE application is installed on devices, users can sign in to Workspace ONE to 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 start 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.

Configure the Workspace ONE Intelligent Hub for Windows Desktop

You can update the Workspace ONE Intelligent Hub settings to meet certain business needs.

1 Navigate to **Groups & Settings** > **All Settings** > **Devices & Users** > **Windows** > **Windows Desktop** > **Intelligent Hub Settings**.

2 Configure the **Data Sample Interval (min)** menu item to define the intervals at which the Workspace ONE Intelligent Hub takes samples of data.

3 Configure the **MDM Channel Security** menu item to set the app-layer security between the device and the Workspace ONE UEM console.

4 Configure the **Privacy** settings if you use analytics tools for data collection.

- **Show Privacy Screen** - Display a screen to tell your users that you collect data.
- **Collect Analytics** - Collect various data points, like app creshes and endpoint numbers and send that data to your app analytics vendor.

What to do next

You can prevent end users from disabling the Workspace ONE UEM Service on their device using a Custom Settings profile.

Collect Data with Sensors for Windows Desktop Devices

6

Windows Desktop devices contain multiple attributes such as hardware, OS, certificates, patches, apps, and more. With Sensors, you can collect data for these attributes using the Workspace ONE UEM console. Display the data in Workspace ONE Intelligence and in Workspace ONE UEM.

This chapter includes the following topics:

Freestyle Feature

Sensors is a Freestyle feature that is available for SaaS environments. For details on Freestyle, access Freestyle Orchestrator.

Sensors Description

Devices have a huge number of attributes associated with them. This number increases when you track the different apps, OS versions, patches, and other continually changing variables. It can be difficult to track all these attributes.

Workspace ONE UEM tracks a limited number of device attributes by default. However with Sensors, you can track the specific device attributes you want. For example, you can create a sensor that tracks the driver details for a mouse driver, the warranty information for the OS, and the registry value for your internal apps. Sensors allow you to track various attributes across your devices. Find **Sensors** in the main Workspace ONE UEM console navigation under **Resources**.

To work with Sensors data from Workspace ONE UEM, you can use Workspace ONE Intelligence. Workspace ONE Intelligence has dashboards and reports where you can view and analyze your Sensors data. Data transfer between the two system occurs over secure HTTP using SSL on port 443.

Important: Sensors are not permitted to be assigned to Employee-Owned devices for privacy reasons.

Workspace ONE UEM Options

Sensors Triggers

When configuring Sensors, you can control when the device reports the sensor data back to the Workspace ONE UEM console with triggers. You can schedule these triggers based on the Windows Sample Schedule or specific device events such as login and logout.

Added PowerShell Scripts

The PowerShell script you create determines the value of each sensor.

Device Details > Sensors

You can see data for single devices on the **Sensors** tab in a device's **Device Details** page.

The configuration **Device State** must be enabled in your data center so that Workspace ONE UEM can display Sensors data for devices on the **Sensors** tab. Workspace ONE UEM enables this configuration for SaaS customers.

Note: Workspace ONE UEM is working on a solution for on-premises environments, but until this solution is created, the **Sensors** tab is not available in **Device Details** for on-premises deployments.

Workspace ONE Intelligence Options

Reports and Dashboards To Analyze Data

If you use the Workspace ONE Intelligence service, you can run a report or create a dashboard to view and interact with the data from your Sensors. When you run reports, use the **Workspace ONE UEM** category, **Device Sensors**. You can find your sensors and select them for queries in reports and dashboards.

RBAC to Control Access To Data

To control who has access to Sensors, use the Roles Based Access Control (RBAC) feature in Workspace ONE Intelligence. RBAC assigns permissions to admins, so use them to prevent or allow specific Workspace ONE Intelligence users from accessing Sensors data.

Encryption

All data at rest is encrypted in Workspace ONE Intelligence. For details, refer to the content on the VMware Cloud Trust Center. This site has reports with details on compliance certs, CAIQ, SOC2, SOC3, and other security best practices.

Use Write-Ouput and Not Write-Host in Scripts

The `Write-Host` string in a script directly writes to the screen, and it does not report the sensor output to Workspace ONE Intelligence. However, the string `Write-Output` does write to the pipeline, so use it instead of `Write-Host`. Update applicable scripts to `Write-Output` or `echo` (`echo` is an alias for `Write-Output`.)

For details, access topics in Microsoft | Docs for Write-Host and for Write-Output.

Example of a Non-Working Script

- Returns Time Zone
- Return Type: String

```
$os=Get-TimeZone
write-host $os
```

- Write-Host is not the output of the script, so there is no output from the script.
- Write-Host directly writes to the 'screen' and not to the pipeline.

Example of a Working Script

- Returns Time Zone
- Return Type: String

```
$os=Get-TimeZone
write-output $os
```

Workspace ONE Intelligence Documentation

For details on how to work in Workspace ONE Intelligence, access VMware Workspace ONE Intelligence Products.

Windows Desktop Devices and Sensors Data

Sensors data is not stored locally on Windows devices. A sensor runs PowerShell code that evaluates an attribute on a system and reports that data to Workspace ONE Intelligence. After it evaluates and reports, the PowerShell process terminates.

PowerShell Script Examples for Sensors

When you create Sensors for Windows devices, you must upload a PowerShell script or enter the PowerShell commands in the text box provided during configuration in the Workspace ONE UEM console. These commands return the values for the sensor attributes.

The following examples contain the settings and code needed. You can also visit https://code.vmware.com/samples?id=4930 for more Sensors samples.

Note: Any sensor that returns a date-time data type value uses the ISO format.

Check Remaining Battery

- **Value Type**: integer
- **Execution Context**: User

```
$battery_remain=(Get-WmiObject win32_battery).estimatedChargeRemaining |
Measure-Object -Average | Select-Object -ExpandProperty Averageecho $battery_remain
```

Get Serial Number

- **Value Type**: String
- **Execution Context**: User

```
$os=Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
echo $os.SerialNumber
```

Get System Date

- **Value Type**: DateTime
- **Execution Context**: User

```
$date_current = get-Date -format s -DisplayHint Date
echo $date_current
```

Check If TPM Is Enabled

- **Value Type**: Boolean
- **Execution Context**: Administrator

```
$obj = get-tpm
echo $obj.TpmReady
```

Check If TPM Is Locked

- **Value Type**: Boolean

- **Execution Context**: Administrator

```
$obj = get-tpm
echo $obj.LockedOut
```

Get TPM Locked Out Heal Time

- **Value Type**: String
- **Execution Context**: Administrator

```
$tpm=get-tpm
echo $tpm.LockoutHealTime
```

Check If SMBIOS Is Present

- **Value Type**: Boolean
- **Execution Context**: User

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
echo $os.SMBIOSPresent
```

Check SMBIOS BIOSVersion

- **Value Type**: Boolean
- **Execution Context**: User

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
echo $os.SMBIOSBIOSVersion
```

Get BIOS Version

- **Value Type**: String
- **Execution Context**: User

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
echo $os.Version
```

Get BIOS Status

- **Value Type**: String
- **Execution Context**: User

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
echo $os.Status
```

Get Average CPU Usage (%)

- **Value Type**: Integer
- **Execution Context**: User

```
cpu_usage= Get-WmiObject win32_processor | Select-Object -ExpandProperty LoadPercentage
echo $cpu_usage
```

Get Average Memory Usage

- **Value Type**: Integer
- **Execution Context**: User

```
$os = Get-WmiObject win32_OperatingSystem
$used_memory = $os.totalvisiblememorysize - $os.freephysicalmemory
echo $used_memory
```

Get Average Virtual Memory Usage

- **Value Type**: Integer
- **Execution Context**: User

```
$os = Get-WmiObject win32_OperatingSystem
$used_memory = $os.totalvirtualmemorysize - $os.freevirtualmemory
echo $used_memory
```

Get Average Network Usage

- **Value Type**: Integer
- **Execution Context**: User

```
$Total_bytes=Get-WmiObject -class Win32_PerfFormattedData_Tcpip_NetworkInterface
|Measure-Object -property BytesTotalPersec -Average |Select-Object -ExpandProperty Average
echo ([System.Math]::Round($Total_bytes))
```

Get Average Memory Usage For A Process

- **Value Type**: String
- **Execution Context**: User

```
$PM = get-process chrome |Measure-object -property PM -Average|Select-Object
-ExpandProperty Average
$NPM = get-process chrome |Measure-object -property NPM -Average|Select-Object
-ExpandProperty Average
echo [System.Math]::Round(($PM+$NPM)/1KB)
```

Check If A Process Is Running Or Not

- **Value Type**: Boolean
- **Execution Context**: User

```
$chrome = Get-Process chrome -ea SilentlyContinue
          if($chrome){
              echo $true
              }
          else{
              echo $false
              }
```

Check If Secure Boot Is Enabled

- **Value Type**: Boolean
- **Execution Context**: Administrator

```
try { $bios=Confirm-SecureBootUEFI }
catch { $false }
echo $bios
```

Active Network Interface

- **Value Type**: String
- **Execution Context**: User

```
$properties = @('Name','InterfaceDescription')
$physical_adapter = get-netadapter -physical | where status -eq "up"
|select-object -Property $properties
echo $physical_adapter
```

Check The PowerShell Version

- **Value Type**: String
- **Execution Context**: User

```
$x = $PSVersionTable.PSVersion
echo "$($x.Major).$($x.Minor).$($x.Build).$($x.Revision)"
```

Check Battery Max Capacity

- **Value Type**: Integer

- **Execution Context**: User

```
$max_capacity = (Get-WmiObject -Class "BatteryFullChargedCapacity" -Namespace
"ROOT\WMI").FullChargedCapacity | Measure-Object -Sum |
Select-Object -ExpandProperty Sum
echo $max_capacity
```

Check Battery Charging Status

- **Value Type**: String
- **Execution Context**: User

```
$charge_status = (Get-CimInstance win32_battery).batterystatus
$charging = @(2,6,7,8,9)
if($charging -contains $charge_status[0] -or $charging -contains $charge_status[1] )
{
                echo "Charging"
                }else{
                echo "Not Charging"
}
```

Active Power Management Profile

- **Value Type**: String
- **Execution Context**: Administrator

```
$plan = Get-WmiObject -Class win32_powerplan -Namespace root\cimv2\power
-Filter "isActive='true'"
echo $plan
```

Check If Wireless Is Present

- **Value Type**: Boolean
- **Execution Context**: User

```
$wireless = Get-WmiObject -class Win32_NetworkAdapter -filter "netconnectionid like 'Wi-
Fi%'"
    if($wireless){echo $true}
    else {echo $false}
```

Get Java Version

- **Value Type**: String
- **Execution Context**: User

```
$java_ver = cmd.exe /c "java -version" '2>&1'
echo $java_ver
```

Create a Sensor for Windows Desktop Devices

Create Sensors in the Workspace ONE UEM console to track specific device attributes such as remaining battery, OS version, or average CPU usage. Each sensor includes a script of code to collect the desired data. You can upload these scripts or enter them directly into the console.

Sensors use PowerShell scripts to gather attribute values. You must create these scripts yourself either before creating a sensor or during configuration in the scripting window.

Each script contains only one sensor. If a script returns multiple values, Workspace ONE Intelligence and Workspace ONE UEM read only the first value as the response from the script. If a script returns a null value, Workspace ONE Intelligence and Workspace ONE UEM do not report the sensor.

Prerequisites

If you want to view Sensors for multiple devices and interact with the data in reports and dashboards, you must opt into Workspace ONE Intelligence. If you want to view Sensors data for a single device, you do not need Workspace ONE Intelligence. Go to the device's **Device Details** page and select the **Sensors** tab to view the data.

Procedure

1 Navigate to **Resources** > **Sensors** > **Add**.

2 Select **Windows**.

3 Configure the sensor settings for the **General** tab.

- **Name** - Enter a name for the sensor. The name must start with a lowercase letter followed by alpha-numeric characters and underscores. The name must be between 2-64 characters. Do not use spaces in this menu item.
- **Description** - Enter a description for the sensor.

4 Select **Next**.

5 Configure the sensor settings for the **Details** tab.

- **Language** - Workspace ONE UEM supports PowerShell.
- **Execution Context** - This setting controls whether the script for the sensor runs on a user or system context.
- **Execution Architecture** - This setting controls whether the script for the sensor runs on a device based on the architecture. You can limit the script to run on 32-bit devices or 64-bit devices only or to run the script based on the device architecture. You can also force the script to run as 32-bit regardless of the device.
- **Response Data Type** - Select the type of response to the script for the sensor. You can choose between:
  - **String**
  - **Integer**

- **Boolean**
- **Date Time**

- **Script Command** - Upload a script for the sensor or write your own in the text box provided.

6 Select **Save** to assign your Sensors later or select **Save & Assign** to assign Sensors to devices with groups.

7 To continue with assignment, select **Add Assignment**.

8 On the **Definition** tab, enter the **Assignment Name** and use the **Select Smart Group** menu item to select the group of devices you want to collect Sensors data from.

9 On the **Deployment** tab, select the trigger for the sensor to report the device attribute. You can select multiple values.

What to do next

After creating a sensor, use the **Device Details** page in Workspace ONE UEM to see data for single devices or go to Workspace ONE Intelligence to use reports and dashboards to interact with data for multiple devices.

Automate Endpoint Configurations with Scripts for Windows Desktop Devices

7

Use Scripts to run PowerShell code for endpoint configurations on Windows Desktop devices using Workspace ONE UEM.

This chapter includes the following topics:

Freestyle Feature

Scripts is a Freestyle feature that is available for SaaS environments. For details on Freestyle, access Freestyle Orchestrator.

Scripts Description

With Scripts, located in the main navigation under **Resources**, you can push code to Windows devices to do various processes. For example, push a PowerShell script that notifies users to restart their devices.

Use **Variables** in your scripts to protect sensitive static data like passwords and API keys, or use lookup values for dynamic data such as device ID and user name. You can also make this code available to your Windows users so they can run it on their devices when needed. Make code available by integrating the Workspace ONE Intelligent Hub with Scripts so that users can access the code in the Apps area of the catalog.

Important: Scripts are not permitted to be assigned to Employee-Owned devices for privacy reasons.

How Do You Know Your Scripts Are Successful?

You can find out if Scripts ran successfully using the **Scripts** tab in a device's Device Details page. In the Workspace ONE UEM console, go to the applicable organization group, select **Devices** > **List View**, and choose an applicable device. On the **Scripts** tab, look in the Status column for a **Executed** or **Failed** status. Statuses depend on the exit code (also known as error code or return code).

- Executed - Workspace ONE UEM displays this status after the exit code returns a 0.
- Failed - Workspace ONE UEM displays this status after the exit code returns any value that is not a 0.

Create a Script for Windows Desktop Devices

Scripts for Windows Desktop managed by Workspace ONE UEM supports using PowerShell to execute codes on end user devices. Integrate Scripts with the Workspace ONE Intelligent Hub for Windows and enable self-service to Scripts for your users.

Procedure

1 Navigate to **Resources > Scripts > Add**.

2 Select **Windows**.

3 Configure the script settings for the **General** tab.

Setting	Description
Name	Enter a name for the script.
Description	Enter a description for the script.
App Catalog Customization	Enable offering self-service access to Scripts in the Workspace ONE Intelligent Hub catalog. **Display Name** - Enter the name that users see in the catalog. **Display Description** - Enter a brief description of what the script does. **Icon** - Upload an icon for the script. **Category** - Select a category for the script. Categories help users filter apps in the catalog. Although you have completed the settings for the script in the catalog, there is another configuration to set to display your script in the Workspace ONE Intelligent Hub. When you assign the script to devices, enable the **Show in Hub** menu item or these customizations do not display in the catalog.

4 Configure the script settings for the Details tab.

Setting	Description
Language	Workspace ONE UEM supports PowerShell.
Execution Context	This setting controls whether the script runs in the user or system context.
Execution Architecture	This settings controls whether the script runs on a device based on the architecture. You can limit the script to run on 32-bit devices or 64-bit devices only or to run the script based on the device architecture. You can also force the script to run as 32-bit regardless of the architecture of the device.

Setting	Description
Timeout	In case the script gets looped or is unresponsive for some reason, enter a length of time in seconds for the system to run the script and then stop.
Code	Upload a script or write your own in the text box provided.

5 Select **Next** to configure the **Variables** tab. Add static values, such as API keys, service account names or password by providing the key and the value of the variable. Or, add dynamic values such as **enrollmentuser** by providing a key and then selecting the lookup value icon. To use variables in a script, reference the variable by using `$env:key`. For instance, if the variable definition has a key named **SystemAccount** and a value of admin01, the script can assign the variable to a script-variable, named account by referencing `$account = $env:SystemAccount`.

6 To assign Scripts to devices, select the script, choose **Assign**, and select **New Assignment**.

7 On the **Definition** tab, enter the **Assignment Name** and use the **Select Smart Group** menu item to select the group of devices you want to push Scripts to.

8 On the **Deployment** tab, for **Triggers**, select the trigger that starts the script. You can select multiple triggers.

9 Enable **Show In Hub** to show your **App Catalog Customization** settings for the script in the Workspace ONE Intelligent Hub. You can disable this option to hide a script from users in the catalog.

What to do next

Go to the **Scripts** tab in a device's **Device Details** to view the status of your Scripts.

Dell Command | Product Integrations

8

Integrate Workspace ONE UEM with the Dell Command | products (Dell Command | Configure, Dell Command | Monitor, and Dell Command | Update) to configure device BIOS settings, to configure the information Workspace ONE UEM collects from Dell enterprise devices, and to enable updating firmware, drivers, and applications.

This chapter includes the following topics:

Dell Command | Configure Integration

Integrate Workspace ONE UEM with Dell Command | Configure to configure device BIOS settings. This integration enables the full functionality of the BIOS profile for Windows Desktop devices.

Basics

Integrating with Dell Command | Configure to enhance the device management of Dell enterprise devices. If you want to use the configuration packages feature of the BIOS profile, you must add this integration to your environment.

Supported Devices

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

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.

Add Dell Command | Configure to Workspace ONE UEM

Add Dell Command | Configure to the Workspace ONE UEM console to enhance management of your Dell enterprise devices. If you want to use the configuration packages feature of the BIOS profile, you must add this integration to your environment.

Prerequisites

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

Procedure

1 Navigate to Dell Command | Configure and download the latest version of Dell Command | Configure.

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 UEM 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.

5 In the **Deployment Options** tab, set the **Admin Privileges** to **Yes**.

6 Add an assignment of the application to your Dell enterprise devices.

Results

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

Dell Command | Monitor Integration

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

Basics

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

Supported Devices

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

BIOS Profile

Configure certain BIOS settings on Dell enterprise devices using a BIOS profile. The settings allow you to control hardware virtulization and BIOS security.

Battery Health Status

The overall health of a battery affects the lifespan of a device. With Dell Command | Monitor and WinAPI, 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.

Dell Command | Update Integration

Dell Command | Update is a client-side management software and part of the Dell Client 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, Workspace ONE UEM 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

Configure the OEM Updates Profile

Configure the OEM Updates profile to enabled Dell Command | Update on end-user devices.

Add Dell Command | Update to Workspace ONE UEM

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

For details on how to create an MSI file, access the Dell documentation topic How to Create Dell Command Update MSI Installer Package.

Prerequisites

You must enable Software Distribution to push Dell Command | Update to your devices. Access the topic Upload and Configure Win32 Files for Software Distribution for details on how to package files for Software Distribution.

Procedure

1 Navigate to Dell Command | Update and download the latest version of Dell Command | Update.

2 In the Workspace ONE UEM console, add the EXE file or the 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.

3 In the **Deployment Options** tab, set the **Admin Privileges** to **Yes**.

4 Add an assignment of the application to your Dell enterprise devices.

Results

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

Windows Desktop Device Management

9

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

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

This chapter includes the following topics:

Device Dashboard

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

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

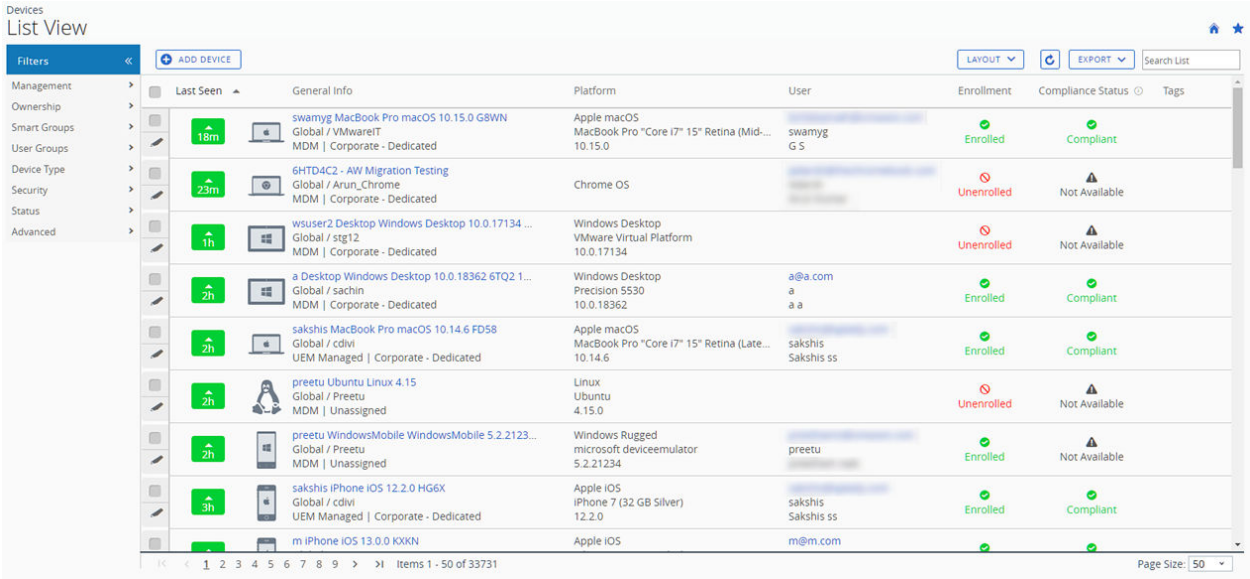
You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

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

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.
  - **Not Encrypted** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph. **Ownership** – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.
- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send out a query command so that the devices can check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for each supported OS. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Device List View

Use the Device List View in Workspace ONE UEM powered by AirWatch to see a full listing of devices in the currently selected organization group.



The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on how long the device is inactive. The default value is 480 minutes (8 hours) but you can customize this value by navigating to **Groups & Settings** > **All Settings** > **Devices & Users** > **General** > **Advanced** and change the **Device Inactivity Timeout (min)** value.

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

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

Customize Device List View Layout

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

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

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

Some notable device list view custom layout columns include the following.

- Android Management

- SSID (Service Set Identifier or Wi-Fi network name)
- Wi-Fi MAC Address
- Wi-Fi IP Address
- Public IP Address

Exporting List View

Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

Search in Device List View

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

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

Device List View Action Button Cluster

With one or more devices selected in the Device List View, you can perform common actions with the action button cluster including Query, Send , Lock, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer, model, enrollment status, and the specific configuration of your Workspace ONE UEM console.

Remote Assist

You can start a **Remote Assist** session on a single qualifying device allowing you to view the screen and control the device. This feature is ideal for troubleshooting and performing advanced configurations on devices in your fleet.

To use this feature, you must satisfy the following requirements.

- You must own a valid license for Workspace ONE Assist.
- You must be an administrator with a role assigned that includes the appropriate Assist permissions.
- The Assist app must be installed on the device.
- Supported device platforms:
  - Android

- iOS
- macOS
- Windows Desktop
- Windows Mobile

Select the check box to the left of a qualifying device in the **Device List View** and the **Remote Assist** button displays. Select this button to initiate a Remote Assist session.

Windows Desktop Device Details Page

Use the Device Details page in Workspace ONE UEM powered by AirWatch to track detailed device information for Windows Desktop devices and quickly access user and device management actions.

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

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

Windows Notification Service Details

You can see the status of device communications with the Windows Notification Service(WNS) from the Network tab of the Device Details page. The WNS supports sending your devices notifications and it is not used for sensitive information. If a device is not currently online, the service caches the notifications until the device connects again. For more information on WNS, refer to Push notification support for device management.

The WNS statuses include the following:

- **WNS Server Status** - displays the state of your WNS server.
- **Last WNS Renewal Request** - The date and time of last attempt made to renew the Windows Notification Services (WNS) connection with the device. This connection allows Workspace ONE UEM to query and push policies to the device (Networking, Battery Sense, and Data Sense conditions permitting).
- **Next WNS Get Request**: - The date and time of the next scheduled attempt to renew the connection between WNS and the device.
- **WNS Channel URI**- The WNS communication endpoint that devices and Workspace ONE UEM use. This endpoint uses the following format: `https://*.notify.windows.com/?token=_{TOKEN}`.

More 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 Workspace ONE UEM console settings or enrollment status.

- **Apps (Query)** – Send an MDM query command to the device to return a list of installed applications.

  The Apps (Query) action requires an active enrolled user login.

- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.

  The Certificates (Query) requires an active enrolled user login.

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

  If you want to change the organization group for multiple devices at a time, you must select devices for the bulk action. Use the Block selection method (using the shift-key) instead of the Global check box (next to the Last Seen column heading in the device list view).

- **Change Passcode** - Change the device password on a Windows Desktop device enrolled with a basic user. This menu item does not support directory services. When you select to use this option, Workspace ONE UEM generates a new password and displays it in the Workspace ONE UEM console. Use the new password to unlock the device.

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

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

- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This action cannot be undone.

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

- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.

Enterprise Reset restores a device to a Ready to Work state when a device is corrupted or has malfunctioning applications. It reinstalls the Windows OS while preserving user data, user accounts, and managed applications. The device will resync auto-deployed enterprise settings, policies, and applications after resync while remaining managed by Workspace ONE.

- **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 is required before Workspace ONE UEM can manage this device again.
  - This device action includes options to prevent future re-enrollment and a **Note Description** text box for you to add information about the action.
  - Use the **Keep Apps On Device** menu item in the **Enterprise Wipe** wizard when you want to keep managed apps on your Windows devices. This feature is helpful when you want to quickly enroll a device to a new user and you do not want to wait for large apps to install on the reassigned Windows device. You cannot access this feature unless your Windows devices and apps meet these requirements.
    - The Windows machine must have the App Deployment agent installed on it.
      - Workspace ONE UEM enables **Software Distribution** by default for SaaS and on-premises deployments. The **Software Distribution** feature automatically deploys the App Deployment agent to Windows devices managed in your Workspace ONE UEM environment. If you disabled this feature, you must re-enable it to ensure the latest App Deployment agent is deployed to devices.
      - The console sends the latest App Deployment agent with every console update and devices receive the update automatically.
      - The **Keep Apps on Device** column in the Enterprise Wipe wizard indicates whether your devices have met the requirements to use the feature.
    - The apps you want to keep on devices after an enterprise wipe must be managed in Workspace ONE UEM. This feature does not work for unmanaged apps.

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

- **Force BIOS Password Reset** – Force the device to reset the BIOS password to a new auto-generated password.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.

  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 applications (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles, and security measures.
- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again.
- **Remote Management** – Take control of a supported device remotely using this action, which starts a console application that enables you to perform support and troubleshoot on the device.
- **Repair Hub** - Repair the Workspace ONE Intelligent Hub on Windows devices to re-establish communication between the console and the device.

  Certain events might impact the communication between the device and the console. Some examples are stopping key Workspace ONE UEM services, removing or the corruption of Workspace ONE Intelligent Hub related files, and the failing of upgrades of Workspace ONE Intelligent Hub components due to network interruptions.

  The Repair Hub command takes steps to remediate these issues. After the Hub is successfully repaired, it checks for commands to recover HMAC. If there were HMAC errors, it automatically recovers HMAC. The Repair Hub also checks for a version upgrade. If an update is detected and is automatic, the updates to the Hub are enabled, and the Hub is upgraded.
- **Request Device Log** – Request the debug log for the selected device, after which you can view the log by selecting the **More** tab and selecting **Attachments** > **Documents**. You cannot view the log within the Workspace ONE UEM console. The log is delivered as a ZIP file that can be used to troubleshoot and provide support.

  When you request a log, you can select to receive the logs from the **System** or the **Hub**. **System** provides system-level logs. **Hub** provides logs from the multiple agents running on the device.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, and so on).
- **Send Message** – Send a message to the user of the selected device. Select between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.
- **View BIOS Password** – View the BIOS password for the device that the Workspace ONE UEM console auto-generated. You see the **Last Password Applied**and the **Last Password Submitted**.
- **Suspend BitLocker** - You can now suspend and resume BitLocker encryption from the console. This feature is helpful for users who do not have permissions to manage BitLocker but need help with their device. When you select to **Suspend BitLocker** for a device, the console displays several options and one of them is for **Number of Reboots**. Select the number of times you think the device restarts for the applicable scenario. For example, helping a user update their BIOS can require the system to reboot twice, so select **3**. This value gives the

system one extra reboot with encryption suspended to ensure that the BIOS updates properly before resuming BitLocker. However, if you do not know how many reboots a task requires, select a larger value. You can use the **More Actions > Resume BitLocker** after you have completed the task.

Manage Your Microsoft HoloLens Devices

Workspace ONE UEM supports enrolling and managing Microsoft HoloLens devices. You must use the native enrollment and management functionality to manage your Windows HoloLens devices.

Before you can manage your HoloLens devices using Workspace ONE UEM, you must apply the Licensing XML file to the devices. If you are using HoloLens 1 devices, you must apply the file before enrolling. For more information on applying licensing, see Unlock Windows Holographic for Business features. This step is not required for HoloLens 2 devices.

Enroll Your HoloLens Devices

You can enroll your Microsoft HoloLens devices into Workspace ONE UEM using native management functionality. You must use native Windows enrollment methods as HoloLens devices do not support Workspace ONE Intelligent Hub functionality. Enroll with one of the native MDM enrollment procedures, with or without Windows Auto Discovery.

Manage Your HoloLens Devices

After enrolling, you can apply supported profiles to your HoloLens devices using Workspace ONE UEM. For a list of the supported CSP, see CSPs suported in HoloLens devices.

Product Provisioning

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

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

How Do You Deploy Domain Join Configurations for Windows?

10

Windows domain join enables your users to remotely connect to a work domain using active directory credentials or local device credentials. Use Workspace ONE UEM to deploy your domain join configurations for on-premises, workgroups, and hybrid domain joins for your Windows (Windows Desktop) devices.

This chapter includes the following topics:

Integration with Microsoft Autopilot (Hybrid Domain Join)

If you manage users in the cloud and on-premises, you can use Workspace ONE UEM to assign your hybrid domain join configurations to Windows devices leveraging Windows Autopilot + OOBE (Out of Box Experience).

Use a Windows Autopilot Profile for OOBE Enrollments

Windows Autopilot allows you to configure a profile that specifies the Domain Join type for devices going through OOBE. You must configure and assign an Autopilot profile with the hybrid domain join setting in Azure. The devices assigned this profile will go through the OOBE process and be **Hybrid Azure AD joined**.

Important: If you do not assign an Autopilot profile with the Hybrid Join specification in Azure, your Windows devices will go through OOBE and be Azure AD joined. Once devices are Azure AD joined, you cannot initiate a Hybrid domain join without completely resetting the devices.

For details on Autopilot, access the topics on Microsoft | Docs, Configure Autopilot profiles.

- If your users use a third-party VPN client to access resources (for example, users work from home), configure the Autopilot profile menu item **Skip AD connectivity check (preview)** as **Yes**.
- If your users do not use a third-party VPN client to access resources (for example, users are on the corporate network), configure the Autopilot profile menu item **Skip AD connectivity check (preview)** as **No**.

Requirements

- Windows Automatic Enrollment: Configure automatic enrollment in Azure with Workspace ONE UEM as the mobile device management (MDM) system. Access Configure Workspace ONE UEM to Use Azure AD as an Identity Service for details.
- Workspace ONE UEM: Disable the Status Tracking Page for OOBE.
  a In Workspace ONE UEM, go to **Groups & Settings > All Settings > Device & Users > General > Enrollment**.
  b Select the **Optional Prompt** tab.
  c Go to the **Windows** section and disable **Enable the Status Tracking Page for OOBE**.
- Microsoft Subscription: Use one of the Microsoft subscriptions that support Windows Autopilot licensing. Access the article in Microsoft | Docs titled Windows Autopilot licensing requirements.
- Windows Autopilot Profile: Configure this profile in Azure so that your Windows devices are assigned the hybrid domain join setting. For details, access the topics on Microsoft | Docs, Configure Autopilot profiles.
- Register Devices with the Autopilot Profile: For details on how to setup Autopilot devices, access the article in Microsoft | Docs titled Manually register devices with Windows Autopilot.
- AirWatch Cloud Connector (ACC): Use ACC to enable domain join for On-premises Active Directory in Workspace ONE UEM.
- Active Directory Users and Computers (ADUC): You need the MMC snap-in called ADUC to configure on-premises domain join through Workspace ONE UEM.

Assumptions

- You have configured Windows automatic enrollment with Azure in Workspace ONE UEM.
- You have configured and assigned an Autopilot profile in Azure so that devices join to Azure AD as **Hybrid Azure AD joined**.
- You have registered your Windows devices in Azure and assigned the relevant Hybrid Join Autopilot profile.
- You have domains and Organization Units in Active Directory.
- You have configured Directory Services in the Workspace ONE UEM console if you are using Active Directory.
- You have configured and assigned a Domain Join configuration in Workspace ONE UEM console.

Order of Tasks

1 In Azure, set up your Autopilot devices according to Microsoft | Docs. Currently, this process includes the following steps.

   a Register your Autopilot devices.

   b Create a device group.

   c Create and assign an Autopilot deployment profile.

2 Configure on-premises domain join in ADUC, ACC, and Workspace ONE UEM.

   a In ADUC, configure a user account with Windows Server delegate permissions, create a custom delegate task, and configure permissions.

   b In ACC, update the Airwatch Cloud Connector service to login with the user account created in ADUC and add write permissions to the ACC folder.

   c In Workspace ONE UEM, create a domain join configuration for on-premises Active Directory.

   d In Workspace ONE UEM, specify the Organization Unit information by creating and deploying single or multiple assignments for the domain join configuration.

Step One: Configure Autopilot Devices

In Azure, set up your Autopilot devices according to Microsoft documentation. Currently, this process includes the following steps.

1 Create a device group.

2 Register your Autopilot devices.

3 Create and assign an Autopilot deployment profile.

Step Two: Configure On-Premises Domain Join

The steps below outline how to configure and assign a domain join configuration in Workspace ONE UEM. These steps allow a device to join an on-premises domain on enrollment into Workspace ONE. When configured along with a Hybrid Join Autopilot profile, devices go through OOBE to join Azure AD as **Hybrid Azure AD joined**. If you met all the requirements and assumptions for hybrid domain join, you have met them all for on-premises domain join so you can move on to setting this up, starting with **Step One: Configure ADUC** in the **On-Premises Domain Join** section.

On-Premises Domain Join

If you use Active Directory to manage users, you can use Workspace ONE UEM to assign your on-premises domain join configurations.

Requirements

- AirWatch Cloud Connector (ACC): Use ACC to configure domain join for on-premises Active Directory.
- Active Directory Users and Computers (ADUC): You need the MMC snap-in called ADUC to configure on-premises domain join. This snap-in is part of Remote Server Administration Tools (RSAT). See Microsoft | Docs for the latest documentation on Windows Server.

Assumptions

- You have domains and Organization Units set in your domain in Azure.
- You have configured Directory Services in the Workspace ONE UEM console if you are using Active Directory. For details on how to configure Directory Services, access Integrating Workspace ONE UEM with your Directory Services

Order of Tasks

1 In ADUC, configure a user account with Windows Server delegate permissions, create a custom delegate task, and configure permissions.

2 In ACC, update the login with the user account created in ADUC and add write permissions. Ensure that the user also has local admin privileges on the ACC server so that they can successfully start the service.

3 In Workspace ONE UEM, create a domain join configuration for on-premises Active Directory.

4 In Workspace ONE UEM, specify the Organization Unit information by creating and deploying single or multiple assignments for the domain join configuration.

Step One: Configure ADUC

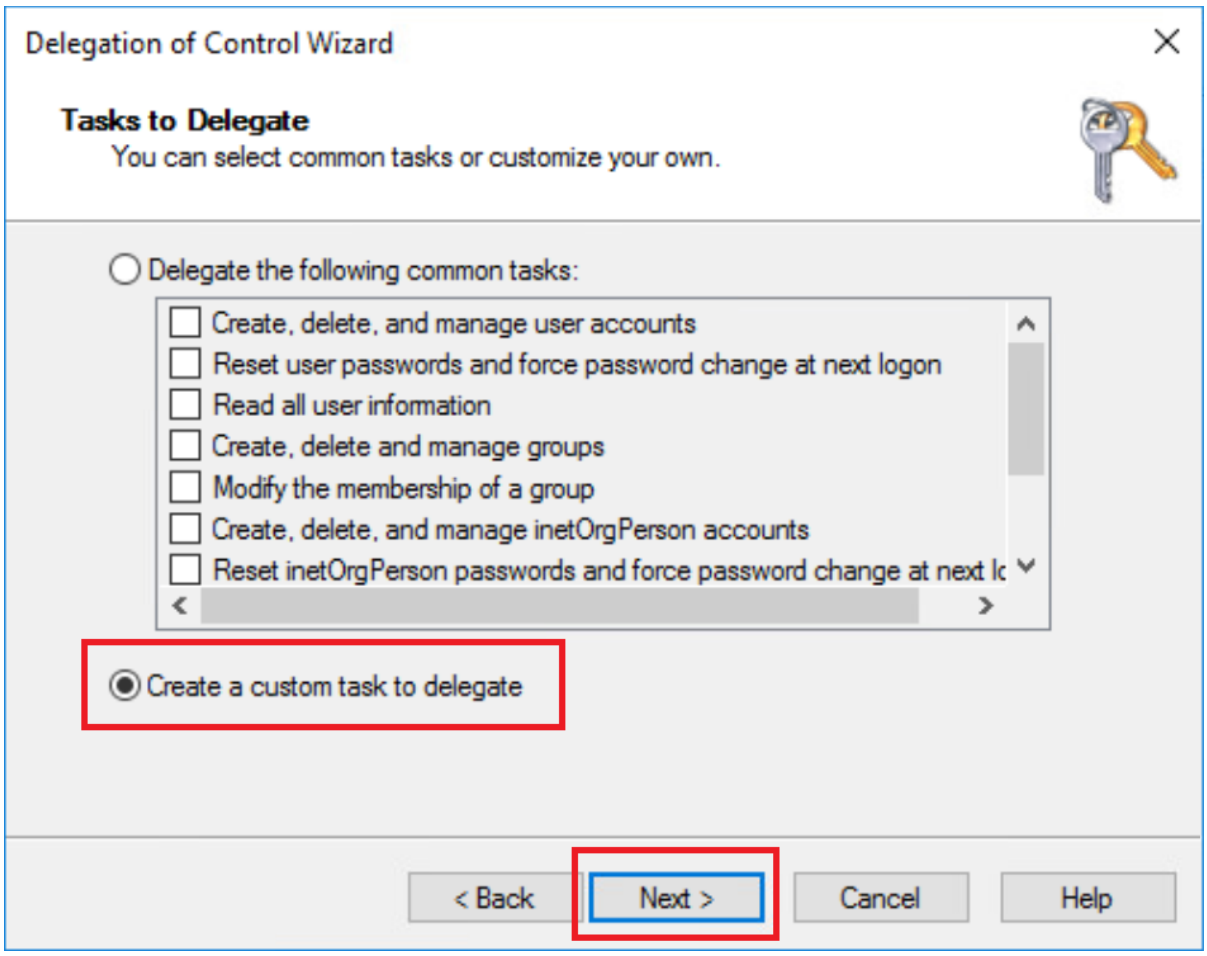
In ADUC, select the user with Windows Server delegate permissions, create a custom delegate task, and configure permissions.

1 Right-click the container or folder where you want to add devices and select **Delegate Control**. This selection displays the **Delegation of Control Wizard**.

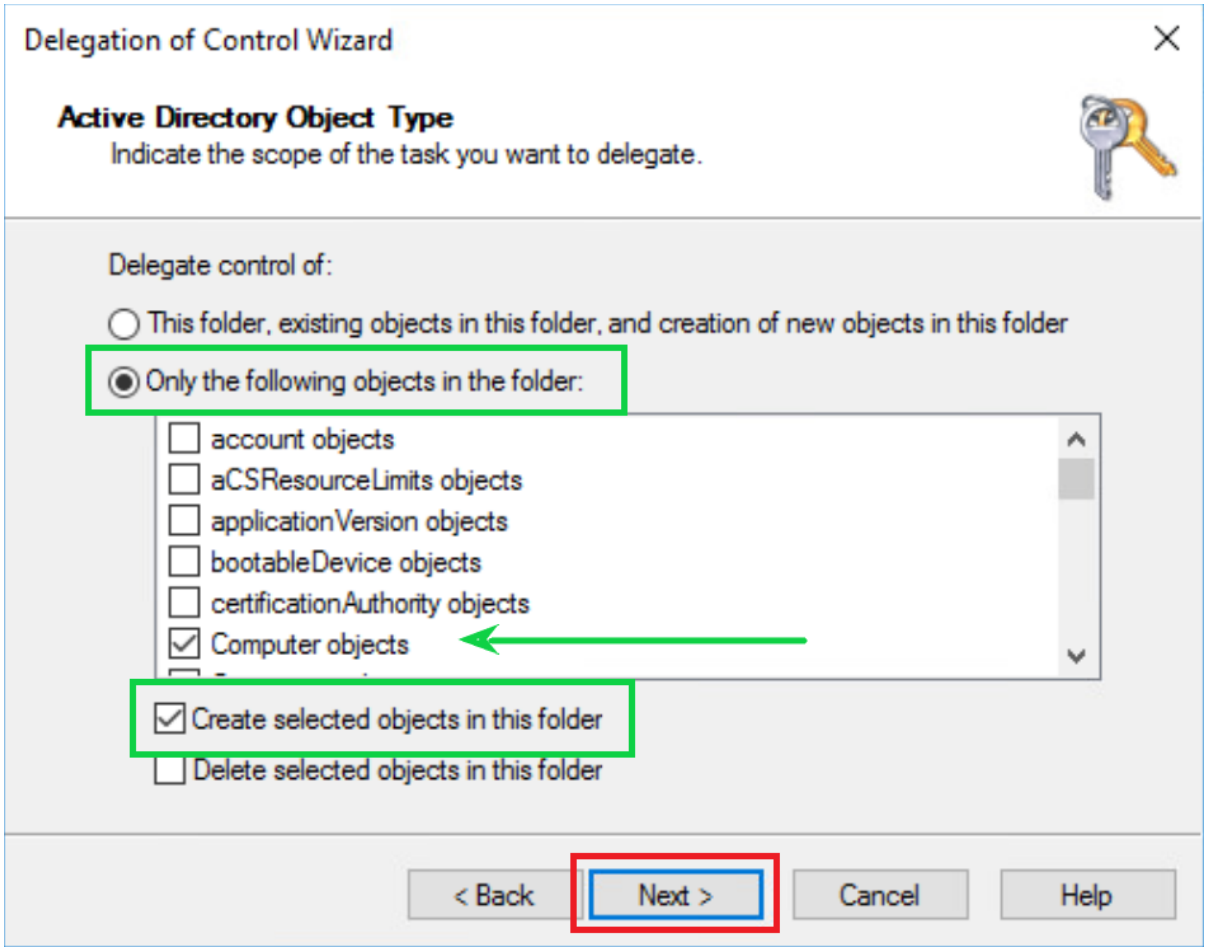
2 Select **Next** in the **Delegation of Control Wizard**.

3 On the **Users or Groups** window, select the user with Windows Server delegate permissions from the list, select **Add**, and then select **Next**. If this user account is not a member of the **Domain Administrators** group, increase the computer account creation limit **(ms-ds-machine-account-quota)** from the default value of 10 to prevent failures after joining 10 devices to the domain.

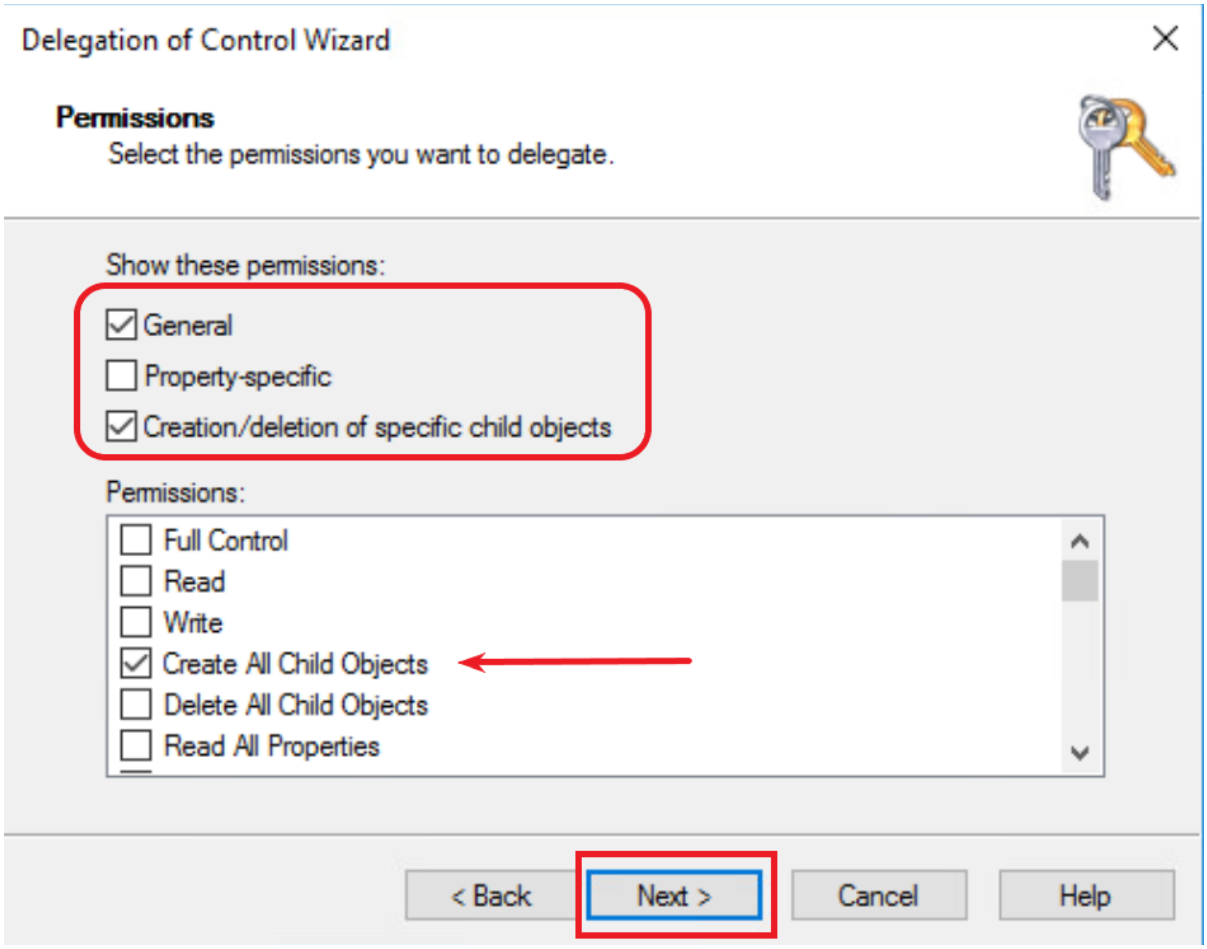
4 On the **Tasks to Delegate** window, select **Create a custom task to delegate** and then select **Next**.



5 On the **Active Directory Object Type** window, select **Only the following objects in the folder:**, **Computer Objects**, and **Create selected objects in this folder** menu items, and then select **Next**.



6 On the **Permissions** window, select **General**, **Creation/deletion of specific child objects**, and **Create All Child Objects**, and then select **Next**.



Step Two: Configure ACC

Update the login and add write permissions for ACC to the user edited in ADUC to delegate a custom task.

1 Change the **Log On As** for the ACC to the user configured with Windows Server delegate permissions. **Note**: Ensure that the user also has local admin privileges on the ACC server so that they can successfully start the service.

2 In the ACC **Advanced Security Settings** area, give the user **WRITE** permissions for the ACC folder at `<Drive>:\VMware\AirWatch\CloudConnector`.

Step Three: Create an On-Premises Domain Join

Deploy a domain join configuration in Workspace ONE UEM to enrolled Windows devices that use Active Directory credentials to access resources.

1 In the Workspace ONE UEM console, go to **Groups & Setting > Configurations** and select **Domain Join** from the list.

2 Select **Add**.

3 Enter a meaningful entry in the **Name** field so you can recognize the domain join. For example, if your users and computers in Active Directory follow a geographic pattern, you can enter `Acme - South America`. This entry does not have to match any settings in Active Directory but using similar patterns in both systems can help organize your devices in your domain joins.

4 Select **On-Premises Active Directory** for the **Domain Join Type**.

5 View the **Domain Name**. The domain join configuration page enters the name of the **Server** configured on the **Directory Services** page. The Workspace ONE UEM directory services configuration allows one server for directory services, so this field is autocompleted. Find Directory Services settings in **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**. **Note**: If you want to change the **Server** entry on the **Directory Services** page, you have to **Disable** the **DNS SRV** menu item.

6 Select the **Domain Friendly Name**. The domain join configuration page offers you a list of available friendly names added to the domain list for your directory services server on the **Directory Services** page. Find Directory Services in **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.

7 Enter your preferred machine name format in the **Machine Name Format** field. Use a supported format for your machine name. The tool tip specifies the accepted formats. Workspace ONE UEM uses a maximum of 15 characters from the `%SERIAL%` or `%RAND:[#]%` formats.

8 Save the domain join configuration to assign it later or select to **Save & Assign** now.

Step Four: Assign a Domain Join Configuration

1 In the Workspace ONE UEM console, navigate to an assignment page by selecting **Assign** from the domain join list view at **Groups & Setting > Configurations** and select **Domain Join**. This configuration window displays if you select to **Save & Assign** your domain join configuration.

2 Select the name of the domain join configuration unless the entry is prepopulated.

3 Add an **Assignment Name** that has meaning for you and that helps you identify the assignment. The entry does not need to match any setting in Active Directory.

4 Search for Organization Units configured in your ADUC settings, and select only one Organization Unit.

5 Search and select smart groups that are configured in Workspace ONE UEM. You can assign a smart group to one Organization Unit and no more. If you try to select a smart group that is already assigned an Organization Unit, the console displays an error message with information so you can troubleshoot and decide which smart groups to use to fit your current deployment scenario.

6 Create and save your assignment.

Computers Container in Active Directory (AD) and OU/Smart Groups Conflicts

You can add multiple assignments to domain join configurations but consider the flexibility of smart groups. Since smart groups are flexible, it is possible you might have a device in multiple assignments for a domain join configuration. This scenario means that the device is also assigned to multiple Organization Units, which is not allowed. When the console identifies that a device is in multiple assignments for a domain join configuration, it puts that device in the **Computers** container in Active Directory. You can go to ADUC and put the device in the desired Organization Unit. The device receives the domain join configuration that matches the assignment for the Organization Unit.

Domain Join Re-assignment

The domain join configuration for a device is evaluated and applied during the enrollment process. Once a device has received a domain join configuration, you cannot update it by changing the assigned smart groups in Workspace ONE UEM. Workspace ONE UEM only delivers a domain join configuration to the device one time upon enrollment.

Workgroup Join

If you have users that use a local account to access their Windows devices and resources, configure a workgroup join in Workspace ONE UEM.

Order of Tasks

1 In Workspace ONE UEM, create a domain join configuration for Workgroup Join.

2 In Workspace ONE UEM, specify the Workgroup Name, Machine Name format, and Local user settings, and then assign the configuration to a Smart Group.

Step One: Create a Domain Join for Workgroups

Deploy a domain join configuration in Workspace ONE UEM for enrolled Windows Desktop devices that use local accounts to access resources.

1 In the Workspace ONE UEM console, go to **Groups & Setting > Configurations** and select **Domain Join** from the list.

2 Select **Add**.

3 Enter a meaningful entry in the **Name** field so you can recognize the domain join. For example, if your users and computers in Active Directory follow a geographic pattern, you can enter `Acme – South America`. This entry does not have to match any settings in Active Directory but using similar patterns in both systems can help organize your devices in your domain joins.

4 Select **Workgroup** for the **Domain Join Type**.

5 Enter a name for the **Workgroup**. The entry is to help you organize and identify the workgroup in the Workspace ONE UEM console.

6 Enter the machine name format in the **Machine Name Format** field. Use a supported format for your machine name. The tool tip specifies supported formats in the UI. Use exactly 15 characters in a `%SERIAL%` or `%RAND:[#]%` format.

7 If you want to create the local user for domain join now, enable **Create Local User**.

8 If you want to give the local user admin permissions, enable **Make Administrator**. Admins have permissions that include the ability to unenroll devices or they can uninstall system apps.

9 Enter a **Local Username** and a **Local User Password** that the device user enters to access the device with this domain join configuration. Give the user name and password entry to your users.

10 Save the domain join configuration to assign it later or select to **Save & Assign** now.

Step Two: Assign a Domain Join Configuration

1 In the Workspace ONE UEM console, navigate to an assignment page by selecting **Assign** from the domain join list view at **Groups & Setting > Configurations** and select **Domain Join**. This configuration window displays if you select to **Save & Assign** your domain join configuration.

2 Select the name of the domain join configuration unless the entry is prepopulated.

3 Add an **Assignment Name** that has meaning for you and that helps you identify the assignment. The entry does not need to match any setting in Active Directory.

4 Search and select smart groups that are configured in Workspace ONE UEM. You can assign a smart group to only one Workgroup configuration. If you try to select a smart group that is already assigned a Workgroup configuration, the console displays an error message with information so you can troubleshoot and decide which smart groups to use to fit your current deployment scenario.

5 Create and save your assignment.

Technical Preview: Intel EMA Integration for Windows

11

Use the **Integrations** area of Workspace ONE UEM to integrate your Intel Endpoint Management Assistant (EMA) deployment with Workspace ONE UEM. Intel EMA manages those Windows devices that are equipped with Intel VPRO chipset. Intel EMA utilizes the Intel Active Management Technology (AMT) to access and act even on those Windows devices that are unresponsive or have a corrupt OS. Integrate the systems so that you can enroll new devices with Intel EMA, view your Intel EMA and your Workspace ONE UEM managed devices and manage those devices from a single console.

This chapter includes the following topics:

Technical previews

Workspace ONE UEM offers the Intel EMA integration for Windows as a technical preview. Technical preview features are not fully tested and some functionality might not work as expected. However, these previews help Workspace ONE UEM improve current functionality and develop future enhancements.

Contact your VMware Representative for information about this technical preview.

UEM app assignments deploy Endpoint Groups

This topic includes general information on how to use an app assignment to deploy your Intel EMA, Endpoint Groups packages in Workspace ONE UEM. For details about app assignments, access Add Assignments and Exclusions to your Applications.

How do you configure the Intel EMA integration?

Enter your Intel EMA server and credential information in Workspace ONE UEM so that the systems can communicate. Workspace ONE UEM discovers your Intel EMA enrolled devices and lists them in the Workspace ONE UEM Device List View. The co managed devices get system generated tags - Intel EMA and End point group name for easy grouping and action.

Prerequisites

- Deploy an Intel EMA server with client credential configured for the tenant.
- Get the listed values from your Intel EMA environment. Workspace ONE UEM uses these values to connect and communicate with Intel EMA.
  - Server URL
  - Client ID
  - Client Secret
- Configure your Endpoint Groups in Intel EMA before starting this integration.

Procedure

1 In Workspace ONE UEM, select the applicable organization group.

2 Go to **Groups & Settings > Integrations**.

3 Select **Setup** on the **Intel** card to configure the integration.

4 Select the **Network Partner Credentials** tab and view or edit the **Current Setting**.

- **Inherit** sets the system to use the settings of the current organization group's (OG's) parent OG.
- **Override** enables the settings for editing so you can modify the current OG's settings directly.

5 Add your Intel EMA values into the **Server**, **Client ID**, and **Client Secret** menu items.

6 Select the **Test Connection** button to check that the systems are communicating.

7 Select to **Save Credentials and Connect**. This action starts several processes.

a Workspace ONE UEM launches a device discovery process.

- The device discovery process finds those devices that were already managed in both Workspace ONE UEM and in Intel EMA before the integration.
- You can relaunch this process on the **Device Discovery** tab of the **Intel** Integrations card.

b Workspace ONE UEM communicates with the Intel EMA server.

- Workspace ONE UEM retrieves the details on all the Endpoint Groups configured on the server.

- You can resync Endpoint Groups on the **Configuration** tab of the **Intel** Integrations card.

8 On the **Configuration** tab, you can see a list view of the discovered Intel EMA Endpoint Groups.

- View the EMA and AMT details for the Endpoint Group package.
- View when the Endpoint Group was last successfully created.
- Download Endpoint Groups if you need them.

9 On the **Configuration** tab, select to **Assign Packages to Devices**. This action takes you to the app assignment flow in Workspace ONE UEM.

10 The system navigates to the apps list view page, where you see your Endpoint Group packages. The apps list view is in the console at **Resources > Apps > Native > Internal**.

11 Select the radio button by one of the **EMA** Endpoint Group packages, and then select **Assign**. You can use the **Search List** text box to find a specific group.

12 Select **Add Assignment**. You can also edit an existing app assignment.

13 On the **Distribution** tab, configure the required fields and select smart groups of devices in the **Assignment Groups** menu item to deploy these Endpoint Group packages to devices.

14 Select **Create** or **Save** to save the app assignment for the Endpoint Group package.

How do you find your Endpoint Group package details in the console?

Workspace ONE UEM lists Endpoint Group package details in the **Device List View**.

1 In the Workspace ONE UEM console, go to **Devices > List View** to see your Intel EMA enrolled devices.

2 Look at the **Tags** column for the listed tags. These tags identify your Intel EMA enrolled devices discovered by Workspace ONE UEM.

- Intel EMA
- Intel EMA endpoint Group

How do you execute Intel EMA powered operations on the managed devices from the console?

Prerequisites

All the devices that need to be co-managed by Workspace ONE UEM and Intel EMA/AMT must meet the listed conditions.

- The devices must have the Intel VPro chip set.

- The devices must have the Intel AMT agent, version 11 or later.
- For devices already enrolled, they must have properly configured Intel AMT and Intel EMA agents.
- All the devices need the Intel Endpoint Configuration Tool deployed. You can deploy it using the Worksapce ONE UEM application deployment flow. This flow enables device sample collection and execution of the Intel EMA/AMT powered operations on devices.

Procedure

From the **Device List View**, select one or more Intel EMA enrolled devices to view and use the operations listed in the **More Actions** menu. The device selection drives the availability of the Intel EMA operations. The console lists available operations depending on the device's endpoint group definition and its capabilities.

From the **More Actions** menu, find the listed operations.

- OOB Power On
- OOB Power Off
- OOB Hard Power Cycle
- OOB Sleep - Light
- OOB Sleep - Deep
- OOB Remote SSO Wipe
- Remote KVM

Intel EMA operation behaviors

- The Intel EMA operations behave the same way as other Workspace ONE UEM device actions.
- You can deploy most of these operations on multiple devices except for the **OOB Remote SSO Wipe** and the **Remove KVM** operations. You can only deploy these operations on single devices.
- When you select the **Remote KVM** operation, this action takes you to the Intel EMA portal. From this portal you can remote into the device.

Official Intel download links

As stated above, the Intel software is a prerequisite for the Intel VPro Integration. If you still need to download the software, please see the following sites:

- To download the official Intel EMA: https://intel.com/content/www/us/en/download/19449/intel-endpoint-management-assistant-intel-ema.html
- To download the official Intel ECT: https://intel.com/content/www/us/en/download/19805/intel-endpoint-management-assistant-configuration-tool-intel-ema-configuration-tool.html