omnissa™

Windows Desktop Management

February 10, 2026

Release Version: SaaS

Contents

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

Workspace ONE UEM offers a suite of mobility management solutions for enrolling, securing, configuring, and managing your Windows device deployment. To utilize these management solutions, ensure that your devices meet the enrollment requirements for supported Windows OS versions. The availability of management solutions varies based on the Windows OS version of your devices.

Support for Windows Desktop and Server Devices

Workspace ONE UEM supports:

- Windows 10 and 11 desktop devices
- Windows Server 2016, 2019, 2022, and 2025

The same capabilities are provided for both Windows desktop and server devices, with the exception of Microsoft CSP-based policies and the Intelligent Hub application.

Omnissa is working to achieve parity in Workspace ONE capabilities between supported Windows desktop and server devices. All Windows-specific settings, including Intelligent Hub settings, are accessible under the **Groups & Settings > All Settings > Devices & Users > Microsoft > Windows** menu in the Console. You can find more information about the supported versions of Windows Desktop and Windows Server in the Workspace ONE Intelligent Hub for Windows Release Notes. For details on supported Windows LTSC and IoT versions with Workspace ONE UEM and Intelligent Hub, refer to KB92979.

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

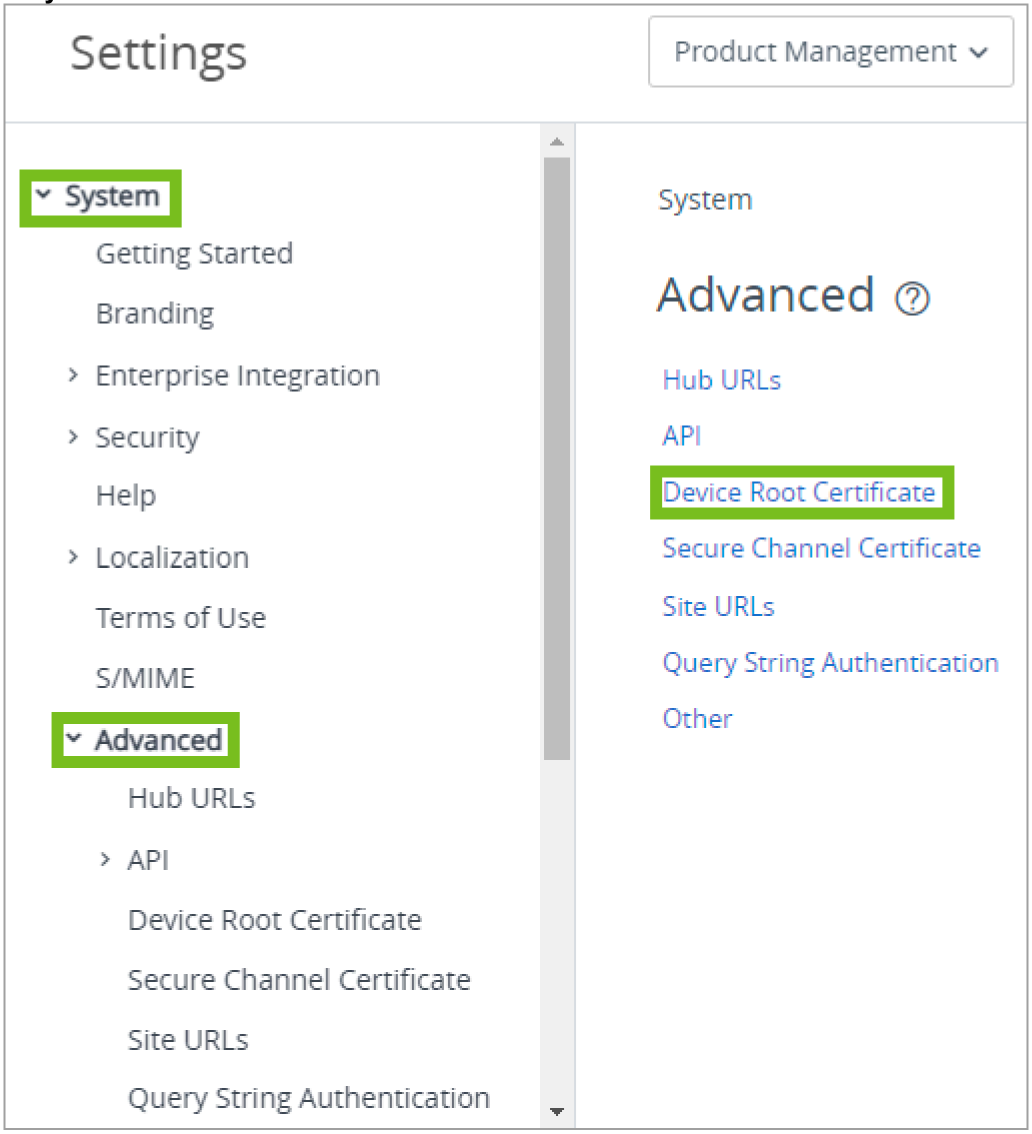
Before enrolling your Windows devices with Workspace ONE UEM, your devices and users must meet the listed requirements and configurations or enrollment does not work.

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 have access to the following sites, have specific settings enabled, and run required services to enroll in Workspace ONE UEM and use the Workspace ONE Intelligent Hub for Windows application. Some URLs and services might not be necessary for Windows Server and registered mode Windows Desktop devices.

- **Omnissa Access URLs** - Trust these URLs in your firewall policies so your enrolled devices can connect to Omnissa Access to utilize Hub Services features and authenticate if Omnissa Access is configured as the Source of Auth
- **App Center API URLs** - Allows Workspace ONE Intelligent Hub for Windows to provide crash information to the Microsoft Store. This is only required for Windows devices running the Workspace

ONE Intelligent Hub application. It is not required on Windows Server devices that were deployed with UI=Headless parameter - `api.appcenter.ms` - `api.mobile.azure.com`

- **Microsoft Store API URL** - Ensures that the Workspace ONE Intelligent Hub for Windows launches on your Windows Desktop 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, refer to 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) - not required for Windows Server and Registered Mode Windows Desktop devices
  - DiagTrack (Connected User Experiences and Telemetry) - not required for Windows Server and Registered Mode Windows Desktop devices
  - Schedule (Task Scheduler)
  - BITS (Background Intelligent Transfer Service)
  - dmwappushservice (Device Management Wireless Application Protocol (WAP) Push message Routing Service) - not required for Windows Server and Registered Mode Windows Desktop devices

Supported Windows Desktop Editions

Workspace ONE UEM supports enrolling and managing Windows Desktop devices with the following operating system editions:

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

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

Windows Desktop Edition and Windows Server Functionality Support Matrix

Workspace ONE UEM supports all versions of Windows 10 and Windows 11 Desktop OS as well as Windows Server 2016, 2019, 2022 and 2025 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 Desktop Home	Windows Desktop Professional	Windows Desktop Enterprise & Windows Desktop Education	Windows Server
Native Client Enrollment		✓	✓	
Agent Based Enrollment	✓	✓	✓	✓
Requires a Windows Account ID				

Feature	Windows Desktop Home	Windows Desktop Professional	Windows Desktop Enterprise & Windows Desktop Education	Windows Server
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		✓	✓	
Windows Update for Business		✓	✓	✓
Assigned Access			✓	

Feature	Windows Desktop Home	Windows Desktop Professional	Windows Desktop Enterprise & Windows Desktop Education	Windows Server
Application Management		✓	✓	✓
Asset Tracking	✓	✓	✓	✓
Device Status	✓	✓	✓	✓
IP Address				
Location	✓	✓	✓	✓
Network	✓	✓	✓	✓
Send Support Message (Email and SMS only)		✓	✓	

NOTE: An upgrade from Windows Home Edition to Windows Professional or Windows Enterprise will require a re-enrollment of the device.

Enrolling Windows Devices into Workspace ONE UEM

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.

Enrollment Basics

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

- Workspace ONE Intelligent Hub for Windows Enrollment

  The simplest enrollment workflow uses Workspace ONE Intelligent Hub for Windows to enroll Windows Desktop and Windows Server devices. Simply download Workspace ONE Intelligent Hub from getwsone.com and follow the prompts to enroll. This enrollment flow is supported on Windows Desktop and Windows Server devices. 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. This enrollment flow is supported on Windows Desktop devices only.

  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. This enrollment flow is supported on Windows Desktop devices only.

  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. This enrollment flow is supported on Windows Desktop devices only.

- Windows Desktop Auto-Enrollment

  Workspace ONE UEM supports the auto-enrollment of specific Windows Desktop devices. Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience. This enrollment flow is supported on Windows Desktop devices only.

- Bulk Provisioning and Enrollment

  Bulk provisioning creates a pre-configured package that stages Windows Desktop devices and enrolls them into Workspace 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. This enrollment flow is supported on Windows Desktop devices only.

  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 Devices - Enroll Without OMA-DM

  To allow Windows Desktop devices to enroll into Workspace ONE UEM without OMA-DM based device management services, you can enable Registered Mode. Windows Server devices always enroll as Registered Mode devices as there is no OMA-DM management agent on Windows Server. Simply assign this mode to an entire organization group and enroll Windows Server devices into that organization group. Alternatively, create smart groups that only include Windows Server devices and enroll Windows Server devices into that organization group. Smart group membership will be triggered for those devices and the enrollment mode applied.

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 Desktop and Server devices with a simplified enrollment flow that is quick and easy.

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 a Windows Desktop device 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.

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 Workspace ONE Intelligent Hub

1. On the Windows Desktop and/or Windows Server device, navigate to https://getwsone.com.
2. Install Workspace ONE Intelligent Hub. When the installation is finished, start Workspace ONE Intelligent Hub.
3. If using Windows Auto-Discovery, 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. If enrolling a Windows Desktop and/or Windows Server devices, open Workspace ONE Intelligent Hub and complete the enrollment.

Intelligent Hub Application Version Control

This feature gives administrators control over which version of the Intelligent Hub is installed on Windows devices, including both Win32 and ARM platforms. Once enabled (available upon request via Omnissa Support or your Account Team), the setting **Intelligent Hub Automatic Updates** in the UEM Console (**System Settings > Devices & Users > Microsoft > Windows > Intelligent Hub Application**) is renamed to **Use Intelligent Hub Version Control**. A new section called **Intelligent Hub Target Seeding** appears, allowing version selection per Organizational Group (OG).

Administrators can assign a specific version to a production OG to ensure consistency, while using the latest available version in a test OG to validate new GA or Beta builds. Once testing is complete, the production OG can be updated to the new version. This setting applies immediately for newly enrolled devices (including OOBE and Autopilot), and existing devices running an older version will update automatically but that process may take up to 48 hours. Devices already running a newer version will not be downgraded, Intelligent Hub downgrades are not supported.

If **Intelligent Hub Automatic Updates** was enabled before the feature was activated, the new setting will also be enabled automatically, and the version will default to **Latest available**, maintaining the current behavior. If the original setting was disabled, the new version control setting will also remain disabled.

This feature enables Intelligent Hub updates to be deployed independently of Workspace ONE UEM updates. Administrators gain direct access to new GA and Beta versions without needing to wait for console upgrades. Additionally, Beta versions no longer require manual download and upload which makes testing significantly easier. The version control system supports both Intel/AMD (Win32) and ARM-based Windows devices, streamlining Hub deployment across all hardware types.

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.

Work Access first processes an Azure AD workflow 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 workflow. 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.

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.

Prerequisites

Registering your domain in Workspace ONE UEM enrollment screen 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

Work Access is the native MDM enrollment method for Windows devices. 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 Devices Staging Enrollment

With device staging, you can configure your Windows Desktop devices for device management by Workspace ONE UEM before you send the devices to your end users.

Device Staging enrolls the device to a staging account and deploys any assigned profiles and applications to the device. The Workspace ONE Intelligent Hub must launch during this process. After the device is fully enrolled and configured, you can ship it to your end users. When an end user logs in for the first time, the Workspace ONE Intelligent Hub updates the device record in the Workspace ONE UEM console. The device is then reassigned to the end user, and any user-level profiles are pushed to the device.

There are two staging methods:

- **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.

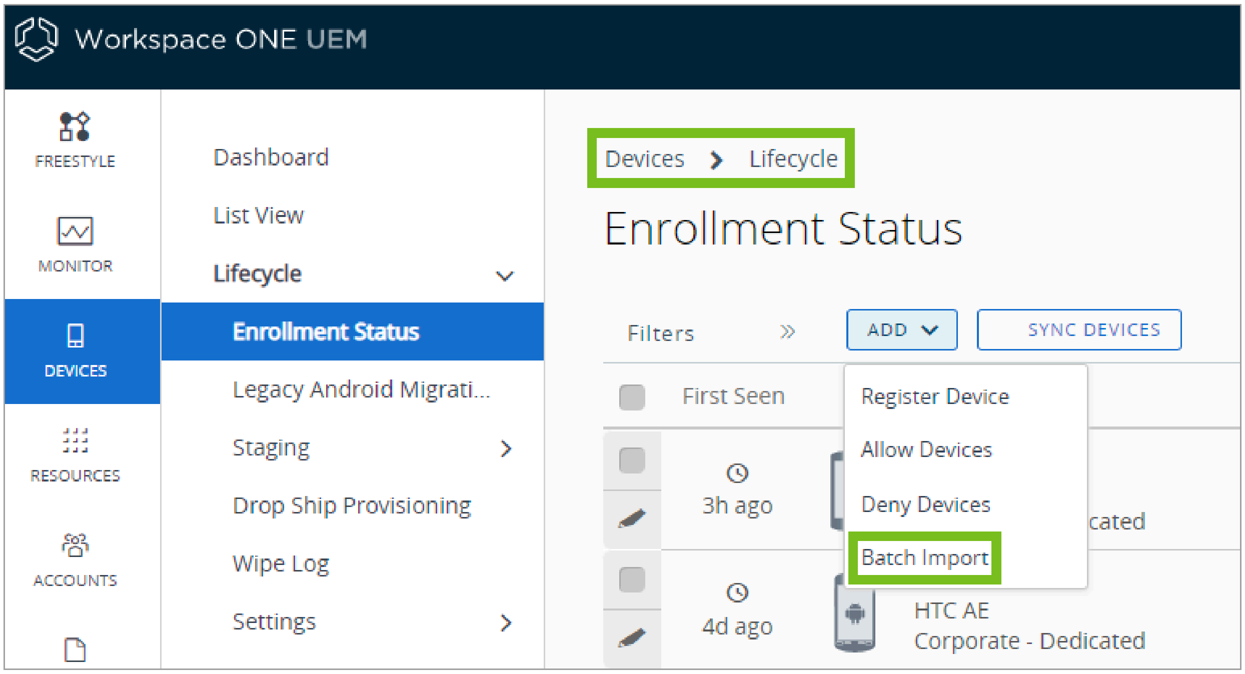
The enrollment completes by either updating the UEM console device registry when an Active Directory user logs onto the device or by comparing the enrolled user name against a list of previously registered serial numbers.

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.

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 process to install Workspace ONE Intelligent Hub for Windows silently on 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.

Note: For more detailed information regarding command line enrollment, refer to Tech Zone.

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 as described in the Silent Enrollment Parameters and Values section below.

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.

Provisioning Mode and Command Line Enrollment for Windows Devices

The Intelligent Hub Provisioning Mode and Command Line Enrollment introduce an additional enrollment flow for both Windows Desktop physical and virtual machines. These improvements allow for the separation of the Intelligent Hub installation and the device enrollment process, providing greater flexibility in deployment scenarios.

Key Features

- Provisioning Mode: Intelligent Hub can now be installed in provisioning mode without requiring immediate device enrollment. You may configure the Windows device, perform reboots, or even Sysprep and clone it. The Intelligent Hub remains installed and ready for device enrollment using the command line.

- Command Line Enrollment: Administrators can trigger device enrollment at a later time using a command line option.

- Support for Virtual Machines: Hub can be installed on a template VM (gold image) and remain installed after Sysprep and cloning, allowing for streamlined provisioning of VM pools.

Procedure

To install Hub in Provisioning Mode, use this code in the **command line:**

```
Msiexec.exe /i airwatchagent.msi PROVISIONHUB=Y
```

Next, use the following code to trigger Automating Enrollment at User Logon:

command line:

```
C:\Program Files (x86)\Airwatch\AgentUI\AWProcessCommands.exe enroll --SERVER htt
ps://ds1234.awmdm.com --OG MyOG --USERNAME staginguser --PASSWORD mypassword --AS
SIGNTOLOGGEDINUSER
```

Results

After the Intelligent Hub is installed in provisioning mode, it will remain installed but unenrolled until a command line enrollment is completed.

Example Usage for Windows Virtual Machines

- Install Hub in provisioning mode on the template VM (gold image)
- Sysprep is run as part of the cloning process
- Create a pool of VMs based on the template
- Enrollment flow can be triggered automatically using cmd line enrollment script at user logon

Deferred Enrollment for Windows Devices

The Intelligent Hub Deferred Enrollment Mode provides the ability to install Hub and defer enrollment until an interactive Windows user session is initiated.

Key Features

- Install Hub using cmd line installation while deferring enrollment process to first Windows user session.

- Suppresses Hub UI prompts for enrollment details.

Procedure

To install Hub in Deferred Enrollment Mode, use this code in the **command line:**

```
Msiexec.exe /i airwatchAgent.msi /q DEFERENROLLMENT=Y ENROLL=Y SERVER=ds###awmdm.com LGName=<groupID> USERNAME=<staginguser> PASSWORD=<stagingpassword> ASSIGNTOLOGGEDINUSER=Y
```

Results

After the Intelligent Hub is installed in Deferred Enrollment mode, enrollment will be deferred until a valid interactive Windows user session occurs.

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. `/q,/qn` - Controls the UI levels for installation `/L` - Log levels and log paths. For more information, refer to: Microsoft's 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.
DEFERENROLLMENT	Used to enable caching of enrollment info. `DEFERENROLLMENT=Y`
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.

Enrollment Parameters	Values to Add to Parameter
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 argument is no longer supported and should be removed from any command line enrollment scripts. Refer to: KB 78733 for more information.
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.
PROVISIONHUB	Used to embed Hub in template or gold image. Also used for Hub installation that will survive Sysprep operation. `PROVISIONHUB=Y` Select Y for provisioning. Select N for enrollment.
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.

Enroll On Behalf Of (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.

Example of Basic Silent 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 /q ENROLL=Y SERVER=ds###awmdm.com LGName=<groupID> USERNAME=<staginguser> PASSWORD=<stagingpassword> ASSIGNTOLOGGEDINUSER=Y
```
~~~

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. -If you have a custom domain name associated with your Saas instance, please refer to the next section (On-Premises Environments or SaaS Environment with a Custom Domain Name) for those specific instructions instead.

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**.

  a. Select **Azure Active Directory** to view the **Overview** page.
  b. 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** app, and choose **Add**.
   c. Select the **AirWatch** 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 or SaaS Environment with a Custom Domain Name: 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**.
      a. Select **Azure Active Directory** to view the **Overview** page.
      b. 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

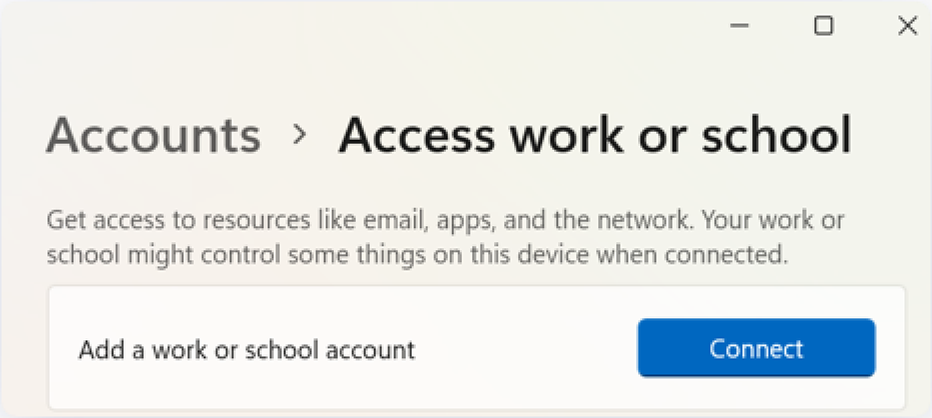
- Windows OS build 14393.82 and above.
- KB update KB3176934 installed.
- No MDM applications installed under your Azure AD management portal.
- Azure AD account configured on the device.

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. If you are not using Windows Auto-Discovery, refer to Enroll Through Work Access.

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.



Accounts › Access work or school

Get access to resources like email, apps, and the network. Your work or school might control some things on this device when connected.

Enroll Through Out of Box Experience

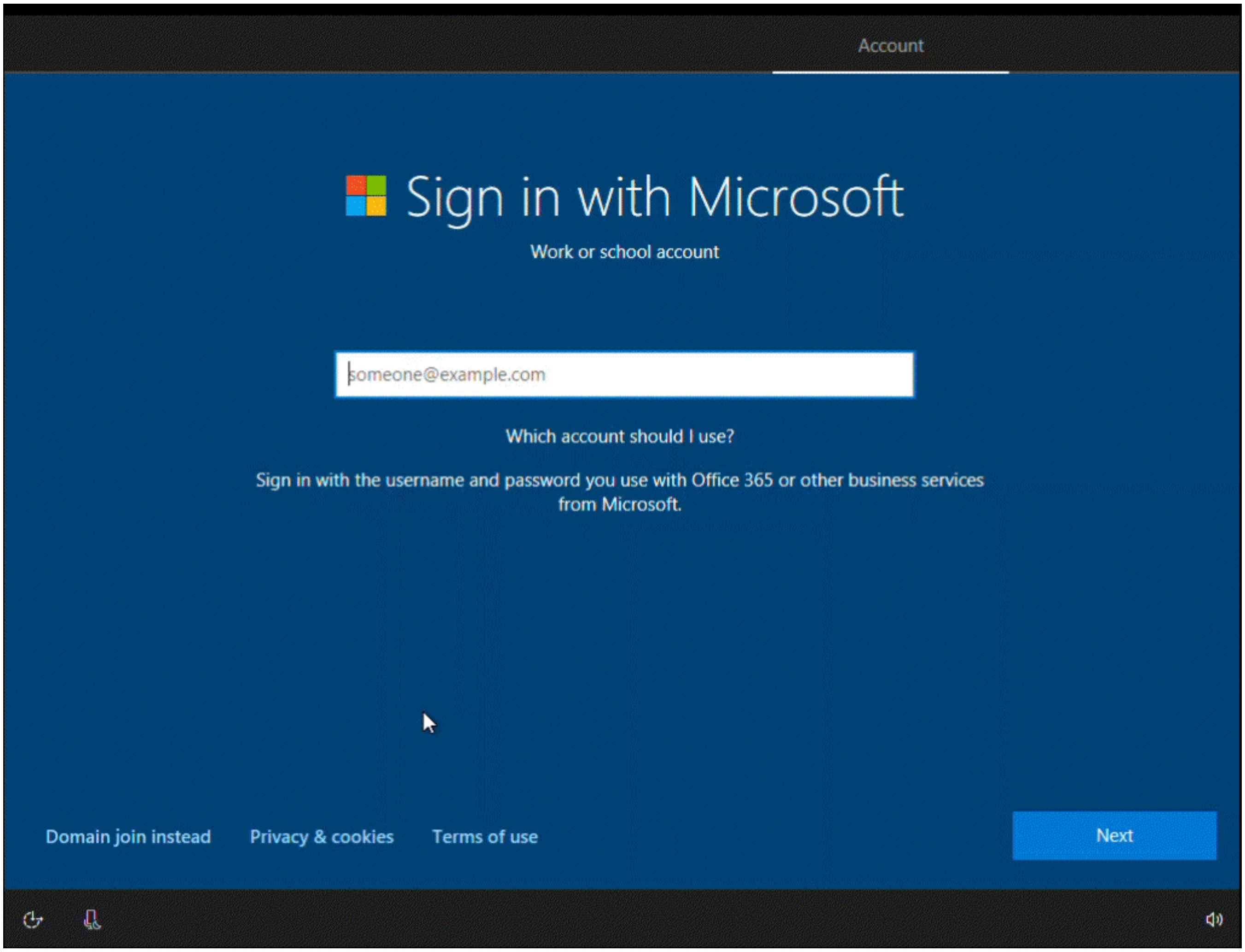
Out of Box Experience (OOBE) enrollment automatically enrolls a device into the correct organization group as part of the initial setup and configuration of a Windows device.

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.

Note: The custom settings profiles cannot be tracked during OOBE and will not apply during provisioning.

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.



Sign in with Microsoft

Work or school account

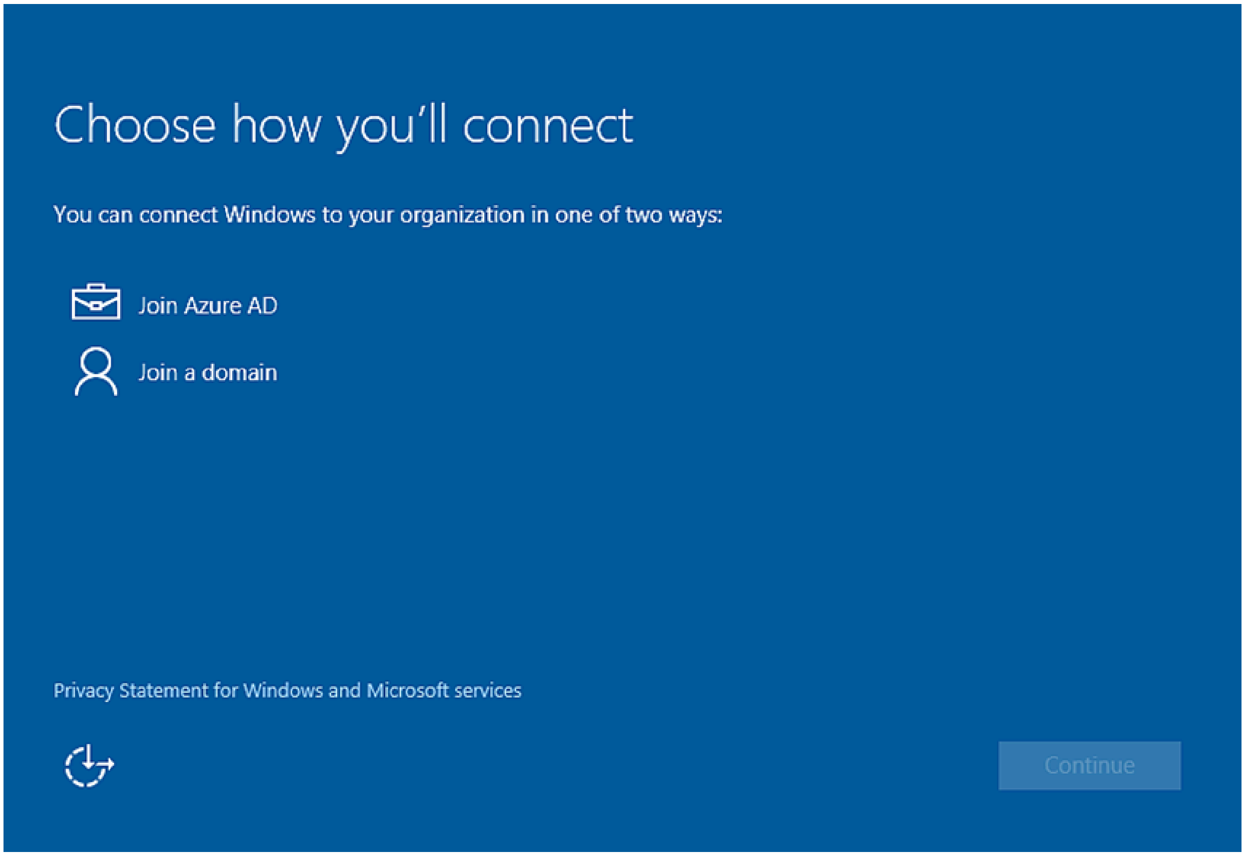
someone@example.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

Procedure

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

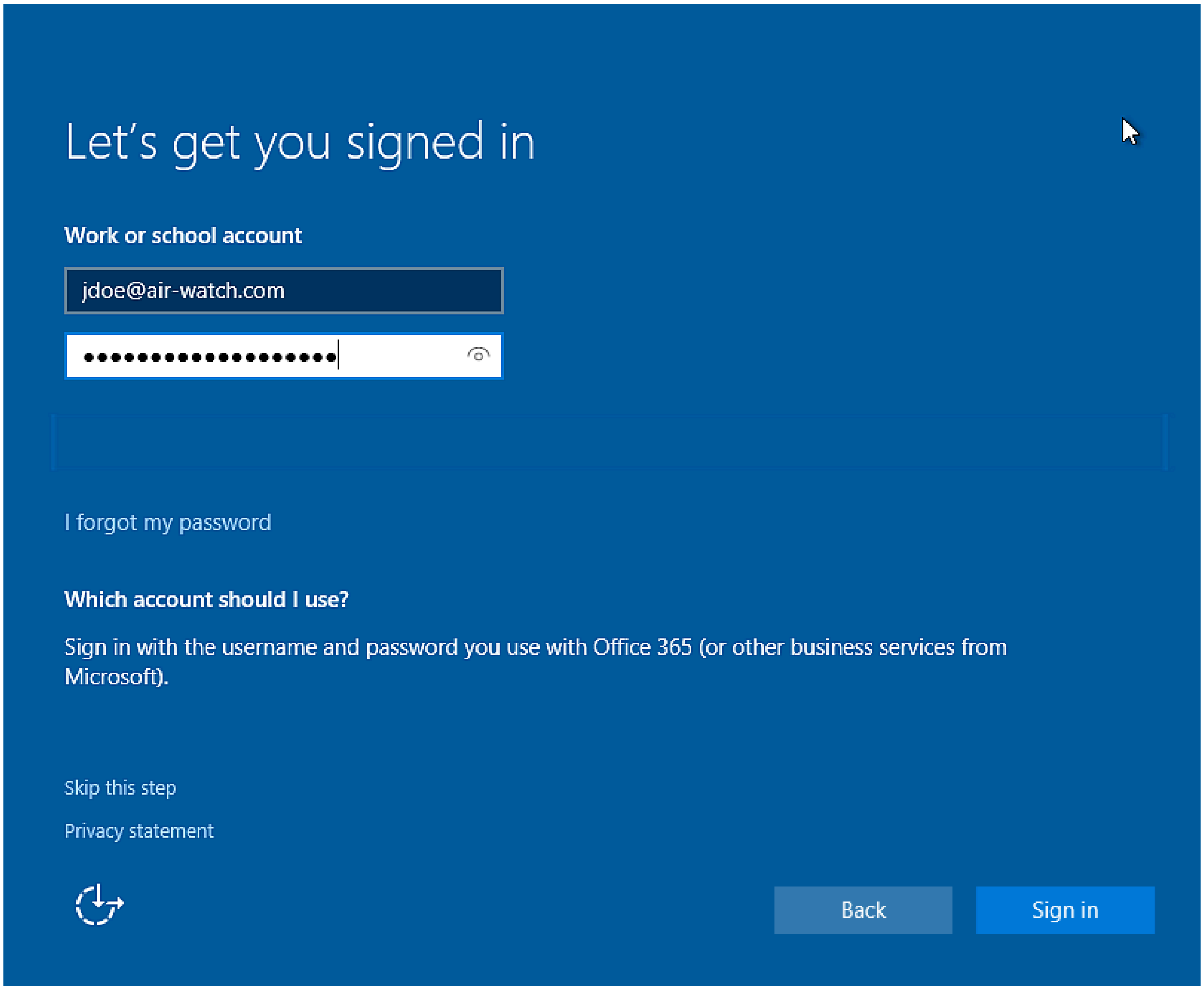


Choose how you'll connect

You can connect Windows to your organization in one of two ways:

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

3. Enter your Azure AD/Workspace ONE UEM email address as the **Work or school account**.



Let's get you signed in

Work or school account

jdoe@air-watch.com

•••••••••••••••••••

I forgot my password

Which account should I use?

Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

Skip this step

Privacy statement

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.

Note: Windows 10 (21H2 and later) and Windows 11 (all versions) are no longer supported for this type of enrollment flow. Please ensure you are using a compatible version of Windows to proceed with this process. We recommend reviewing your operating system version and updating your workflow or system requirements accordingly.

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, 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	Registered	Registration	Enrolled	Registration	Registered	Registration

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
attributes Attributes are Serial Number, IMEI, and UDID.		Active		Active		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
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

Multi User Support and Management

The Multi User feature has made large changes in how an admin will manage their devices going forward. By using the new Modern Stack architecture, Workspace ONE will be able to manage devices with multiple users. Whoever is logged into Windows Desktop will become the device's enrolled user. We will then track the enrolled user for everyone who signs in. It is very important that the device resources are assigned to the device.

Multi User is now the default enrollment method for Workspace ONE managed Windows devices. Starting in UEM 2406 and Intelligent Hub 2404 all devices will be Multi User enabled by default. This change will create new use cases including shift-based work and the ability to reassign devices without an enterprise wipe. There are no additional command line switches or arguments that need to be passed to enable the Multi User feature.

Enrollment

There are five types of enrollment options and some have additional requirements.

1. **Out of Box Enrollment:** Devices enrolled using Autopilot are supported. However, the Intelligent Hub must be installed in order to enable the Multi User feature. In your **System Settings > Devices & Users > Microsoft > Windows**, ensure that the **Publish Intelligent Hub** option is selected.

2. **Command Line Enrollment:** For Multi User Mode, all devices will be Multi User enabled by default with no additional command line switch needed.

3. **Agent Enrollment:** Agent Based enrollment is supported. No additional configuration is required to enable Multi User during Agent enrollment.

4. **Enrollment with Dropship Provisioning (Online and Offline):** Supports Multi User Mode with no additional configuration is required.

5. **Staging Enrollment Flows:** Standard Single User Staging is supported with no additional configuration needed. Advanced Single User or Multi User Staging is not supported. To verify your staging user settings, navagate to: the user **details > Advanced > Staging**.

Note: Any user can now become a Staging User. Administrators are no longer required to pre-configure a user to be a dedicated Staging User. If the common resources are created in the device context and the assignments are configured for all users of the device, resources will not be re-installed.

A feature was added in 2506 that gives the admin the ability to select the type of User Mode to use for a new enrollment. The default for the User Mode is set to Multi User, but you can now select Single User enrollment from here if you need. This can also be configured per organization group (OG). You can find this in the console under: **System > Devices & Users > Microsoft > Windows > Intelligent Hub Settings > Default User Mode for Enrollment**.

For more enrollment information refer to: Workspace ONE UEM Windows Multi User on TechZone.

Shared Device Settings

The default setting is to prompt user for their organization group (OG). If this setting is not changed, the user will be prompted to enter the Organization Group ID. It is recommended to change this setting to **Fixed Organization Group** or **User Group Organization Group** so that user reassignment is silent. For Fixed Organization Group, the device will then remain in the current Organization Group while the User Group Organization will move the device to the configured Organization Group. The **Group Assignment Mode** is under **System Settings > Devices and Users > General > Shared Device**. From there, you can control how to map a device to the right Organization Group.

Console View

Devices show their current user mode (Multi User, Single User) in multiple areas within the console.

- **Multi User Mode:** The enrolled user of the device will be updated based on the current logged in Windows user.

- **Single User Mode:** The enrolled user will always be the user who is enrolled on the device. The enrolled user will not be updated if another user signs into Windows.

Device List & Details Page

The **Device List** custom view shows the User Mode column which displays the current mode. The **Device Details** view also displays the current User Mode in the Device Info Panel.

Filters

On the Device List View Page, filters have been added to aid in multiple administrative scenarios:

- **Single User (legacy):** Devices enrolled as a Single User device due to an old Intelligent Hub version that does not support Multi User.

- **Multi User:** Devices enrolled or migrated to Multi User Mode.

- **Multi User Capable:** Devices that are currently enrolled as Single User (legacy) but are available to migrated. These devices meet the requirement to migrate to Multi User including the correct Intelligent Hub version. Use this filter when migrating existing Single User (legacy) devices to Multi User.

- **Single User:** Multi User devices that currently have their user reassignment functionality paused. The enrollment user will not be updated on these devices when a new user signs into Windows. User Reassignment can be paused (or unpaused) on both the device list view or device details page.

Directory Services Support

Multi User has introduced support for the following directory type configurations:

- **LDAP Active Directory** is supported
- **LDAP Lotus Domino** is NOT supported
- **LDAP Novell e-Directory** is NOT supported
- **LDAP Other** is supported
- **Omnissa Identity Services** is supported
- **None** is supported

Attributes for Unique Identifier

To identify who is currently logged in and match them to a user object in the UEM console, it is necessary to set up the attributes used for the matching. In the Windows Intelligent Hub settings, administrators should pick the appropriate pair from the possible UEM User Attributes and the four attributes that the Intelligent Hub can gather from the device. The recommendation is to use UPN / UPN for most use cases. Under the Attributes for Unique Identifier, select the UEM User Attribute that aligns with the desired Client User Attribute as shown below.

UEM User Attributes	Client User Attributes
Object Identifier	Object GUID (requires line of sight to Domain Controler)

Username	Sam Account Name
Recommended: User Principal Name	User Principal Name
EmployeeID	User SID
Email Address	
Custom Attribute 1-5	

By default, the unique identifier is set to Object Identifier / Object GUID. We highly recommend changing this based on your environment needs. Be aware that Object GUID requires an active connection to the Domain Controller to get the GUID on the device. To configure go to: **Settings > Device Settings > Devices & Users > Microsoft > Windows > Intelligent Hub Settings**.

Migration

Starting in 2406, all newly enrolled Windows Desktop devices will be Multi User enabled by default. Existing enrolled Windows Desktop devices will remain as Single User (Legacy) devices. Administrators will be required to migrate their previously enrolled devices to Multi User. The reason for this is to allow administrators to validate their resource assignments prior to Multi User enablement. This will ensure that if the enrollment user is updated after migration, no resources are inadvertently removed.

Example: A device was enrolled by an IT team member using command line staging. During this set up, the team member signed into the device to complete some additional configuration and inadvertently enrolled the device to themselves. The device is then handed off to the actual end user. Upon migration to Multi User, this device's enrollment user will be changed to the actual end user. If the resource assignments are not assigned to actual end user, they would be removed upon migration. See Resource Assignments section for more information on how to properly configure common resources for use in a Multi User scenario.

Migration to Multi User

Migrating devices that were previously enrolled can be done in a few different ways:

- **Device List View:** In the Device List view, select one or more devices via the checkbox and select Change to Multi User Mode. To identify which devices are capable of being migrated, leverage the "Multi User Capable" filter in Filters section of the Device List View page. This filter will list all devices that are capable of being migrated (currently Single User and meet the minimum Intelligent Hub requirements to support Multi User). Administrators will then be presented with the following acceptance screen. Click Proceed.

Note: The Device List View is limited to selecting 100 devices at a time. To migrate more than 100 devices at a time, it is recommended to leverage the API method.

- **Migration via API:** The migration can be triggered with the following POST URL: `https://%APISERVERUL%/api/mdm/devices/action/` with the following body:

```
{
"action_name": "MIGRATE_TO_Multi User",
"filter":
{
"organization_group_uuid": "999362E5-7D35-487B-A74F-7C0A377BB521",
"device_uuids": [
"338234E5-F1DE-46CF-AE1C-DFFD919CFE32",
"40D18DF3-0B04-4648-A26A-E5D24F2CD4D9"
]
} }
```

Important Please make sure to select the version 3 of the API. This data needs to be added to the API header like in this example: `“Accept”, “application/json; version=3”`

The following actions are available:

- MIGRATE_TO_Multi User – For migrating devices from Multi User Capable to Multi User device
- CHANGE_TO_SINGLEUSER – To change a Multi User Device to a Single User Device
- CHANGE_TO_Multi User – To change a Single User Device to a Multi User Device

End User Experience when Switching Users:

Multi User was designed to be as seamless to the end user as possible. To re-assign the device to a new user, simply sign out of Windows and sign in with a different corporate User.

On Domain Joined devices (Active Directory, Hybrid Join, or AAD), the user reassignment will be performed silently. To confirm that re-assignment was successful, the end user will see the following Windows notification after login. This notification will only be shown once after user switch.

On Workgroup Joined devices, Workspace ONE is unable to lookup the required attributes needed to silently re-assign the device. On those devices, the Intelligent Hub will prompt the end user to authenticate using their corporate credentials. After entering their credential successfully, the user will see the notification indicating their user is now connected to Workspace ONE and the device has been properly re-assigned.

- **Failed User Re-Assignment:** When a new User signs in to a Domain Joined machine, Workspace ONE will silently attempt to check out the device. If the first attempt fails, Workspace will wait two minutes before trying again. This will repeat three times. In the event Workspace ONE was unable to silently checkout the device, the Intelligent Hub will then prompt the user to enter their credentials. Upon entering their credentials, the device will then be re-assigned.
- **Sign out vs. Switch User:** To perform the user re-assignment, it is required for the current user to sign out of Windows. Performing a User Switch is not supported. It is recommended to leverage a CSP or GPO to block User Switching on devices that will be frequently switching users. For more information on CSP, refer to Microsoft at: https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-cspwindowslogon

Assignment	User A	User B
System Context application - Assigned to Device	Application will stay on the device	Application will stay on the device
System Context application - Assigned to User A	Application will stay on the device	Application gets removed
System Context application - Assigned to User B	Application gets removed	Application will stay on the device
System Context application - Assigned to User A and B	Application will stay on the device	Application will stay on the device
User Context application - Assigned to User A	Application will stay on the device	Application will stay on the device
User Context application - Assigned to User B	Application will stay on the device	Application will stay on the device
User Context application - Assigned to User A and B	Application will stay on the device	Application will stay on the device

Profile Context

Profile context works similarly in that device level configurations. They are installed using Device Profiles and affect all users on a device. A few examples of this are the encryption of the device, and/or general DLP settings. User profiles are then used to install user specific resources like identity certificates or customizations.

Assignment Groups

Workspace ONE leverages Assignment Groups to assign resources to devices. If a user does not have an assignment to a resource, that resource will be uninstalled. It is crucial that all users be assigned to common resources on a shared workstation. For example: An application that will be used by all users. For all required resources, check the assignment groups used. If you leverage User Groups make sure they include all users or if you use Smart Groups check if the user groups are part of the criteria and if any user exclusions are applied.

Workflows

Workflows, with all included resources, are fully supported on Multi User devices. The behavior of assigned Workflows is different than Profiles or Applications. Workflows will be re-executed and reevaluated with every user switch. This ensures that user context resources are applied to the current enrollment user. Applications and Profiles that are already installed on the device will not be re-installed since the UEM detection will check the installation status before.

Certificates

User and Device certificates can be used on a Multi User device. Assigned Device Certificates are available for all users, while User Certificates are only available for the current enrollment user. If a user logs in the first time to the device, the User Certificate(s) will be requested and installed for the enrollment user. If the user logs in to the device again, the certificate is already installed and there will be no new request on the CA generated.

Prevent User Reassignment

There are two ways in the UEM Consol to prevent or block user reassignments.

Checkout Restrictions: If there is a need to block a specific group from checking out devices to their user account, there is the following configuration available:

- All members of the user group(s) that are added in the “Windows Multi User Checkout Restrictions” section, will not be able to change the enrollment user on a device. This setting can be configured per OG and will be inherited to all child OG’s – if the “Override” option is not selected in a child OG.

  For example: User A is logged in to the device and a help desk employee logs in to the device. The device should stay assigned to User A. In this case the account of the help desk employee can be added to a user group and configured in the checkout restrictions. The help desk employee will not change the enrollment user on any device in this OG anymore.
  User Accounts that are configured for the Checkout Restrictions are still able to enroll devices, but they cannot change the user on an already enrolled device. This does not apply to staging flows - a staging flow device can’t be changed to a user in the checkout restrictions group.

Switch from Multi User Mode to Single User Mode: If there is a need to temporary or permanently pause/stop the user reassignment, one or multiple devices can be selected in the console to switch from Multi User Mode to Single User Mode. If the the device is in Single User Mode, the enrollment user will not change to any new logged in users. This can also be used for Single User devices if they might be enabled to use Multi User capabilities in the future without re-enrollment of the device. After the device switched back to Multi User Mode, every user change will change the enrollment user of the device. Next, Pause and Resume via API.

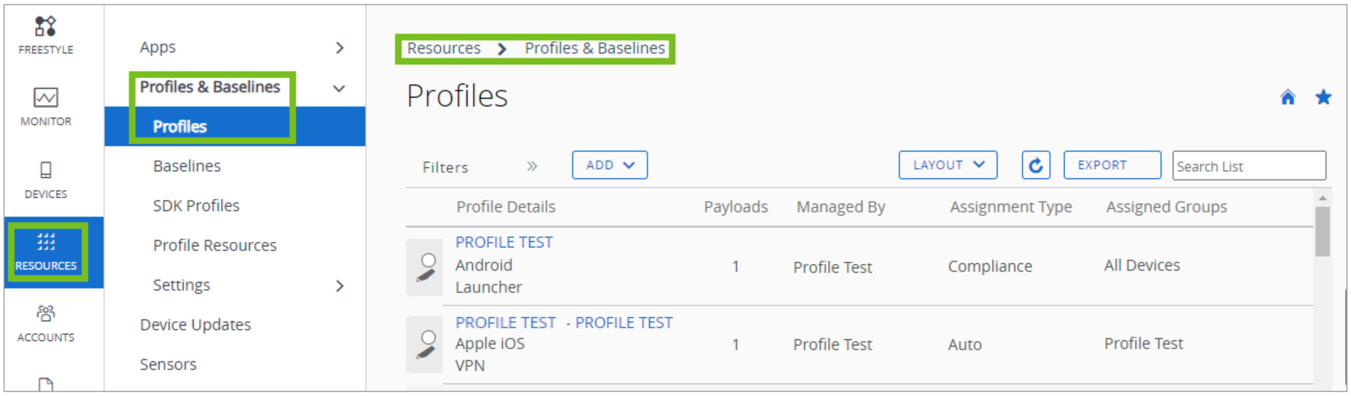
Workspace ONE UEM Profiles for Windows

Profiles in Workspace ONE UEM are the primary means to manage and configure your Windows devices. Find information about various profiles that connect to and protect resources, that restrict and control devices, and that are specific to Dell.

What Are Profiles

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

A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload. In the Workspace ONE UEM console, you can find both user and device profiles by Navigating to: **Resources** > **Profiles & Baselines** > **Profiles**.



Profile Details	Payloads	Managed By	Assignment Type	Assigned Groups
PROFILE TEST Android Launcher	1	Profile Test	Compliance	All Devices
PROFILE TEST - PROFILE TEST Apple iOS VPN	1	Profile Test	Auto	Profile Test

User or Device Level

Windows Desktop profiles apply to a device at either the user level or the device level. When creating Windows Desktop profiles, you select the level the profile applies to. Some profiles are not available for both levels and you can only apply them to either the user level or the device level. The Workspace ONE UEM console identifies which profiles are available at what level. Some caveats for the successful use of device and user profiles include the following list.

- Workspace ONE UEM runs commands that apply to the device context even if the device has no active enrolled user login.
- User-specific profiles require an active enrolled user login.

There are some standard profiles and commands you can use to set up and control the device. The chart below shows commands for both the profile and the console that no longer require an active window user to execute them.

Profile Name	Installs with No Active Windows User
Password	Yes
Wifi	Yes
VPN	Yes
Credentials	Yes

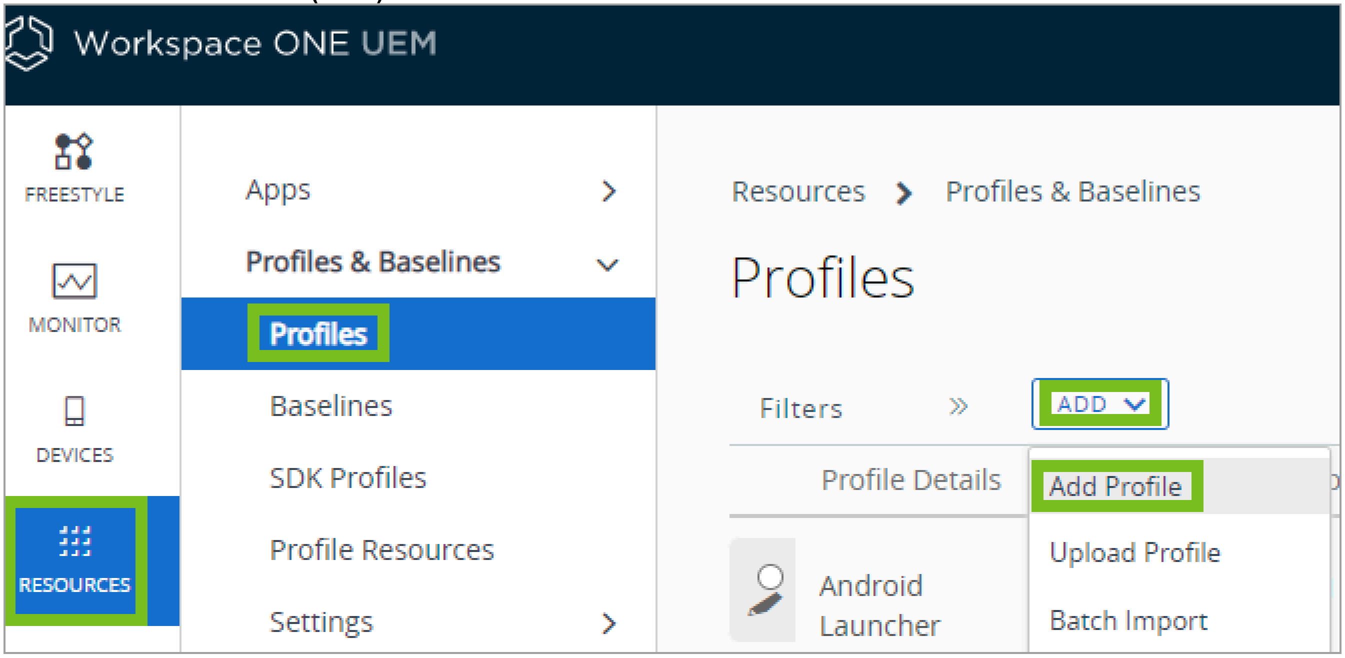
Profile Name	Installs with No Active Windows User
Restriction	Yes
Defender Exploit Guard	Yes
Data Protection	Yes
Windows Hello	Yes
Firewall	Yes
Encryptions	Yes
Anti-Virus	Yes
Windows Updates	Yes
Proxy	Yes
SCEP	Yes
Application Control	Yes
Windows Licensing	Yes
Custom Profile (HUB and OMA-DM)	Yes
Kiosk	Yes
Personalization	Yes
Peer Distribution	Yes
Unified Writer Filter	Yes

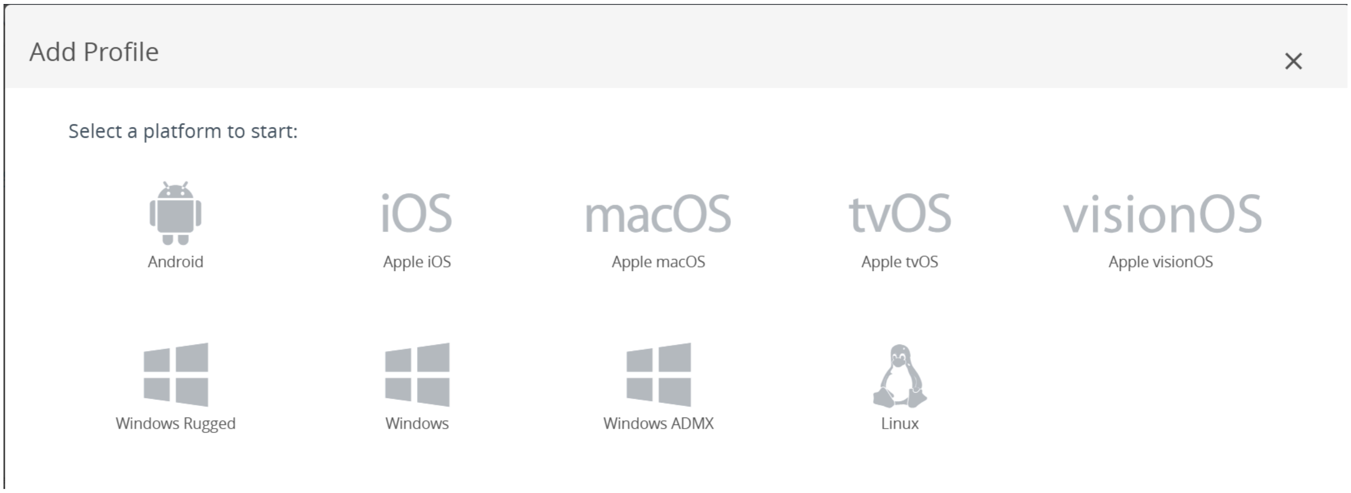
Console Action	Works with No Active Windows User
Device Security	Yes
Windows Information	Yes
Health Attestation	Yes
Available OS Updates	Yes
Hub Check In	Yes
Certificate List Sample	Yes
Security Information	Yes
Information	Yes
App List Sample - HUB	Yes
App List Sample - OMA-DM	Yes
Sensor	Yes
Workflow	Yes
Time Window	Yes
Reboot	Yes
Enterprise Wipe	Yes

Console Action	Works with No Active Windows User
Device Wipe	Yes
Enterprise Reset	Yes
Request Device Log	Yes

New Profile Options for Configuring Windows User and Device Profiles

We have updated your options of how to assign user and device profiles by adding a second Windows(Beta) platform builder. In the console, when adding a user or device profile, you will need to select from either Windows or Windows(Beta) platforms. Navigation: **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Windows -OR- Windows(Beta)**



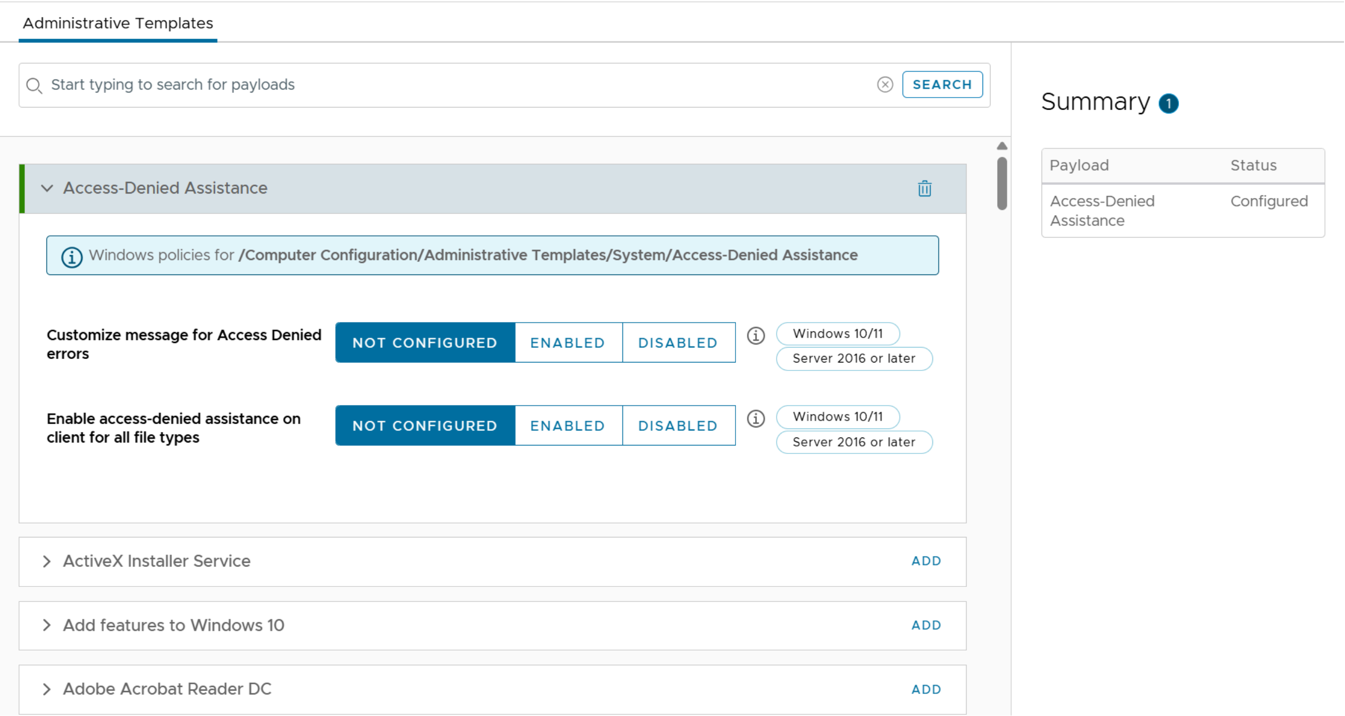


Windows Platform Option

You can continue to add and customize user and device profiles with custom settings and integration with the Workspace ONE Intelligent Hub by using this platform option.

Windows ADMX Profiles

The new **Windows ADMX** Profiles feature provides a modern and structured way to manage administrative template settings across Windows devices. This feature is currently in Limited Availability (LA) behind a feature flag and is designed to replace the existing “Windows (Beta)” profiles, offering a more robust and extensible configuration experience. **Note:** To access this feature and/or any other LA features, you can raising a Service Request (SR) to have the feature flag enabled or contact the Omnissa Account Team.



Summary 1

Payload	Status
Access-Denied Assistance	Configured

Access-Denied Assistance

Windows policies for **/Computer Configuration/Administrative Templates/System/Access-Denied Assistance**

Setting	Value	Supported
Customize message for Access Denied errors	NOT CONFIGURED	Windows 10/11 Server 2016 or later
Enable access-denied assistance on client for all file types	NOT CONFIGURED	Windows 10/11 Server 2016 or later

ActiveX Installer Service

Add features to Windows 10

Adobe Acrobat Reader DC

Once the feature flag is turned on, the **Windows (Beta)** platform will be removed from the UI, and a new option called **Windows ADMX** will become available for profile creation. It’s important to note that while existing Beta profiles will remain editable, customers will no longer be able to create new ones. This marks the beginning of the planned deprecation of the Beta experience in a future release.

With **Windows ADMX** Profiles enabled, customers can create both Device and User profiles. In addition to the standard Windows Administrative Templates, the new ADMX platform also supports third-party ADMX files, including those for Google Chrome, Microsoft Office, Mozilla Firefox, and more, expanding the flexibility and coverage of policy management. Within each profile, administrators can select and configure one or multiple payloads, allowing for precise control over device behavior. However, it is strongly recommended to group payloads by application or configuration type —for example, creating a profile specifically for Google Chrome or Microsoft Edge, rather than mixing them. This approach simplifies troubleshooting and isolates any issues that may arise within a specific configuration set.

Once created, ADMX profiles can be assigned to any Smart Group. After assignment, the Intelligent Hub agent on the device will enforce the settings as defined in the profile. Deployment and configuration status can be monitored directly through the UI or via log files on the endpoint. For diagnostics, administrators can review the log file named: `ADMXProfile-%Timestamp%.log`.

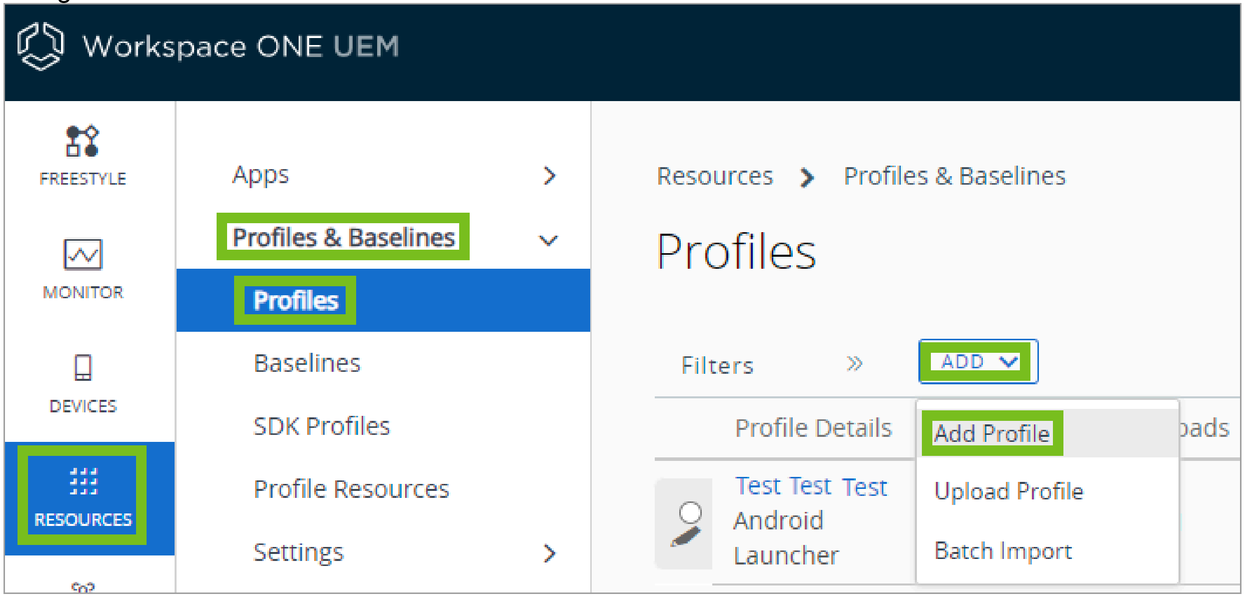
As this is a Limited Availability feature, there are some known limitations. Currently, **Baselines and ADMX Profiles cannot coexist on the same device** — even if the settings do not overlap, applying a Baseline will override the ADMX configuration. A fix for this limitation is expected in an upcoming release of Intelligent Hub. Additionally, supported version indicators within the UI may not always reflect actual compatibility, potentially listing payloads for Windows versions that do not support them. Furthermore, payload metadata is not yet surfaced in the Profiles List View, meaning administrators cannot easily see how many payloads a profile contains or which ones are included. The same applies to Freestyle Workflows, where payload names are currently not visible. Lastly, due to a bug in the payload generation logic, payloads that require comma-separated values are not supported at this time.

Antivirus Profile

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

Important: This profile only configures native Windows Defender Antivirus and not other third-party antivirus appliances.

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



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

3. Select **Device Profile**.

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

5. Select the **Antivirus** Profile.

6. Configure the **Antivirus** settings:

Settings	Descriptions
Real-time Monitoring	Enable to configure Windows Defender Antivirus to monitor the device in real time.
Real-time Scan Direction	Enable to configure Windows Defender Antivirus to monitor inbound files, outbound files, or all files. Use this option to help network performance for those servers or server roles you defined for Windows Server installations that handle traffic in one direction.
Cloud Protection Level	Enable to configure how aggressive Windows Defender Antivirus is in blocking and scanning suspicious files. Consider network performance when setting this menu item.
Cloud Block	Select a time, in seconds, for a file to remain blocked while Windows Defender

Settings	Descriptions
Timeout	Antivirus analyzes it threat potential. The default block time is 10 seconds. The system adds the seconds set in this menu item to the default time.
Signature Updates	Signature update interval in hours Signature update file shares sources Check for Signature Before Running Scan Signature Update Fallback Order
Scan Interval	**Full Scan** - Enable to schedule when a full system scan runs. Select the time interval (in hours) between scans. **Quick Scan** - Enable to schedule when a quick system scan runs. Select the time interval (in hours) between scans.
Exclusions	Select the file paths or processes to exclude from the Windows Defender Antivirus scans. Select **Add New** to add an exception.
Threat Default Action (Low, Moderate, High, Severe threats)	Set the default action for the different threat levels found during scans. **Clean** – Select to clean the issues with the threat. **Quarantine** – Select to separate the threat into a quarantine folder. **Remove** – Select to remove the threat from your system. **Allow** – Select to let the threat stay. **User Defined** – Select to let the user decide what to do with the threat. **No Action** – Select to take no action with the threat. **Block** – Select to block the threat from accessing the device.
Advanced	**Scan Avg CPU Load Factor** - Set the maximum average percentage of CPU Windows Defender Antivirus can use during scans. **UI Lockdown** - Enable to lock down completely the UI so end users cannot change settings. **Catchup Full Scan** - Enable to allow run a full scan that was interrupted or missed previously. A catch-up scan is a scan that is initiated because a regularly scheduled scan was missed. Usually these scheduled scans are missed because the computer was turned off at the scheduled time. **Catchup Quick Scan** - Enable to allow run a quick scan that was interrupted or missed previously. A catch-up scan is a scan that is initiated because a regularly scheduled scan was missed. Usually these scheduled scans are missed because the computer was turned off at the scheduled time. **Behavior Monitoring** - Enable to set the virus scanner to send an activity log to Microsoft. **Intrusion Prevention System** - Enable to configure the network protection against the exploitation of known vulnerabilities. This option enables Windows Defender Antivirus to monitor the connections continuously and identify potentially malicious behavior patterns. In this respect, the software behaves like a classic virus scanner, except that instead of scanning files it now scans network traffic. **PUA Protection** - Enable to set Windows Defender Antivirus to monitor for potentially unwanted applications (PUA) on end clients.

Settings	Descriptions
	IOAV Protection - Enable to have Windows Defender scan downloaded files. **OnAccess Protection** - Enable to set Windows Defender Antivirus to protect files and folders from unauthorized access. Cloud Protection - Enable to set Windows Defender Antivirus to detect and prevent threats quickly using proprietary resources and machine learning. **User Consent** - Enable to set Windows Defender Antivirus to prompt the end client user for consent before it acts on identified threats. **Scan Email** - Enable to allow Windows Defender to scan emails. **Scan Mapped Network Drives** - Enable to allow Windows Defender Antivirus to scan network drives mapped to devices. **Scan Archives** - Enable to allow Windows Defender Antivirus to run a full scan archived folders. **Scan Removable Drives** - Enable to allow Windows Defender Antivirus to scan any removable drives attached to the device. **Remove Quarantined Files After** - Set how long files are quarantined before being removed.

7. Select **Save & Publish**.

Application Control Profile

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

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

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

Configuring an Application Control Profile

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

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

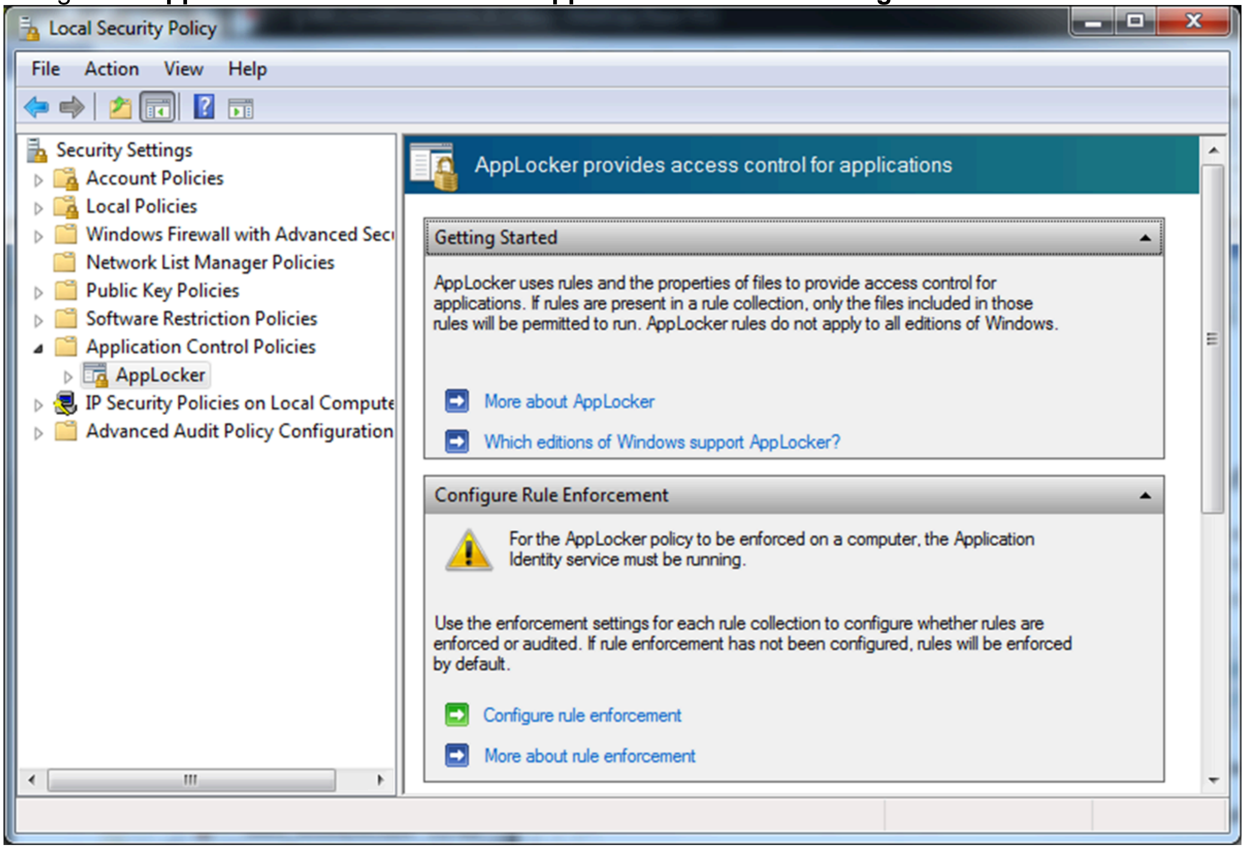
The Application Control profile requires Windows Enterprise or Education.

Important:

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

Procedure

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


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Getting Started
More about AppLocker
Which editions of Windows support AppLocker?
Configure Rule Enforcement
Configure rule enforcement
More about rule enforcement

AppLocker provides access control for applications

AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.

For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

3. Enable **Executable Rules**, **Windows Installer Rules**, and **Script Rules** enforcement by selecting **Enforce Rules**.
4. Create **Executable Rules**, **Windows Installer Rules**, and **Script Rules** by selecting the folder on the right then right-clicking the folder and selecting **Create New Rule**. Remember to create Default Rules to reduce chances of locking the default configuration or breaking the device.
5. After creating all the rules you want, right-click **AppLocker** and select **Export Policy** and save the XML configuration file.
6. Navigate in the Workspace ONE UEM console to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
7. Select **Windows** and then select **Windows Desktop**.
8. Select **Device Profile**.
9. Configure the profile **General** settings.
10. Select the **Application Control** payload.
11. Select **Import Sample Device Configuration** and select **Upload** to add your **Policy Configuration File**.
12. Select **Save & Publish**.

BIOS Profile

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

Support for the BIOS profile settings varies by Dell Enterprise device. The Dell Command | Monitor must be uploaded and/or assigned to each device.

Prerequisites

- If you want to use the configuration package feature, you must push the Dell Command | Configure app to devices.
- This profile also requires integration with Dell Command | Monitor. Add Dell Command | Products.

Procedure

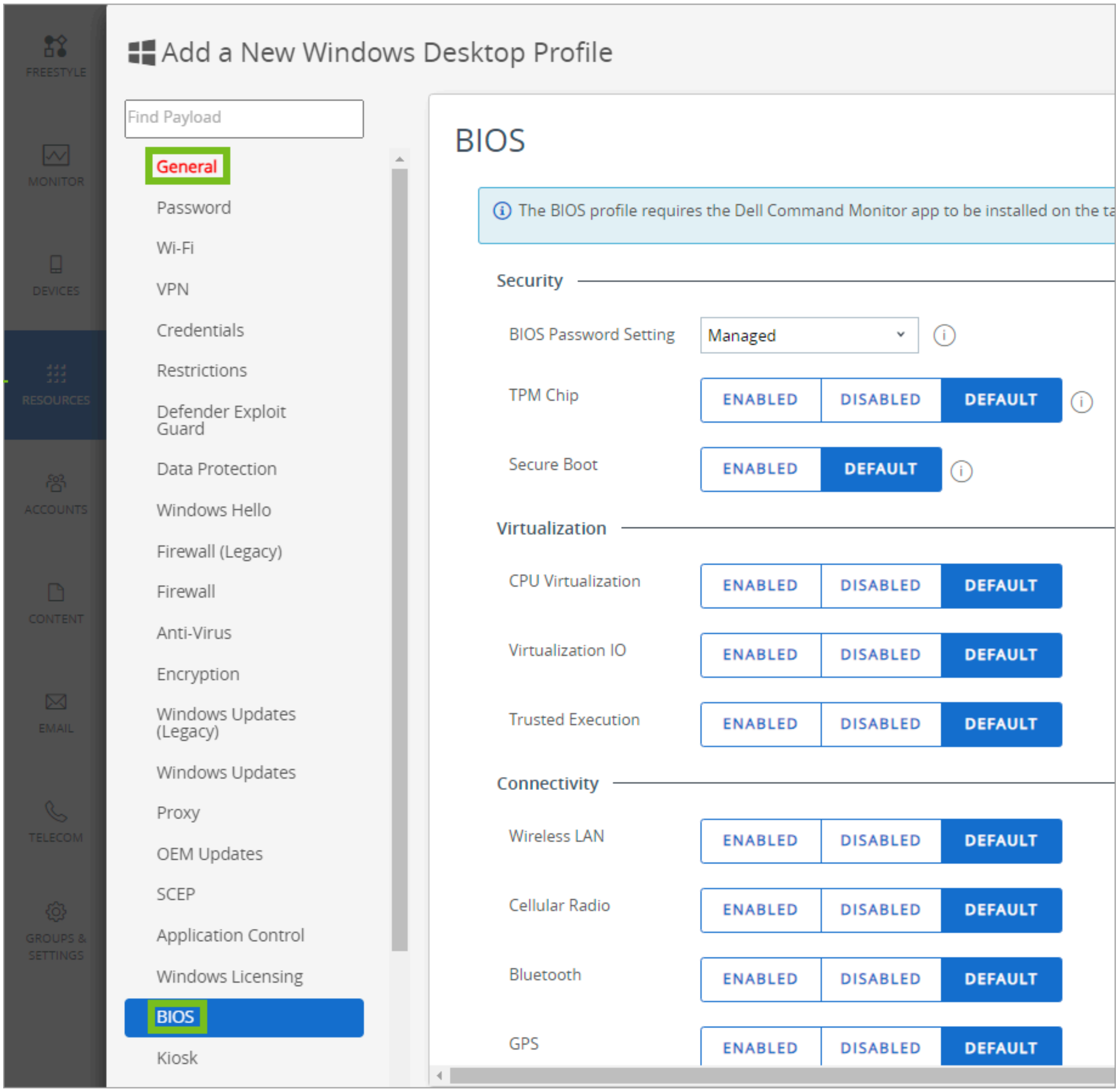
1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.

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

3. Select **Device Profile**.

Note: There is now a default option for the profiles. The default option will make no changes to the setting on the device. In the new profile defaults, the password settings will be set to **Manage** and all the other settings will be set to **Default**.

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



Add a New Windows Desktop Profile

BIOS

The BIOS profile requires the Dell Command Monitor app to be installed on the ta

Security

BIOS Password Setting: Managed

TPM Chip: ENABLED | DISABLED | DEFAULT

Secure Boot: ENABLED | DEFAULT

Virtualization

CPU Virtualization: ENABLED | DISABLED | DEFAULT

Virtualization IO: ENABLED | DISABLED | DEFAULT

Trusted Execution: ENABLED | DISABLED | DEFAULT

Connectivity

Wireless LAN: ENABLED | DISABLED | DEFAULT

Cellular Radio: ENABLED | DISABLED | DEFAULT

Bluetooth: ENABLED | DISABLED | DEFAULT

GPS: ENABLED | DISABLED | DEFAULT

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

   - **BIOS Password Setting** - Select **Managed** to have Workspace ONE UEM auto-generate a strong, unique BIOS password for devices. You can access the generated password from the Device Details page. Select **Manual** to enter your own BIOS password.
   - **BIOS Password** - Enter the password used to unlock the BIOS of the device. This setting displays when the **BIOS Password Setting** is set to Manual.
   - **TPM Chip** - Select **Enable** to enable the device Trusted Platform Module chip. If you disable the TPM Chip, you also disable the one-time BIOS password capability. The BIOS password set from the Managed BIOS Profile does not rotate after use.
   - **Secure Boot** - Select **Enable** to use Secure Boot settings on the device. You cannot disable Secure Boot with DCM.
   - **CPU Virtualization** - Select **Enable** to allow hardware virtualization support.
   - **Virtualization IO** - Select **Enable** to allow input/output virtualization.
   - **Trusted Execution** - Select **Enable** to allow the device to use the TPM chip, CPU Virtualization, and Virtualization IO for trust decisions. Trust Execution requires the **TPM Chip**, **CPU Virtualization**, and **Virtualization IO** settings to be set to **Enabled**.
   - **Wireless LAN** - Select **Enable** to allow use of the device wireless LAN functionality.

- **Cellular Radio** - Select **Enable** to allow use of the device cellular radio functionality.
- **Bluetooth** - Select **Enable** to allow use of the device Bluetooth functionality.
- **GPS** - Select **Enable** to allow use of the device GPS functionality.
- **SMART Reporting** - Select **Enable** to use SMART monitoring of the device storage solutions.
- **Primary Battery Charge** - Select the charging rules for the device. These rules control when the battery starts and stops charging. If you select **Custom Charge**, you can manually set the charge percentage to start and stop charging the battery.
    - Standard Charge - Consider using this option for users who switch between battery power and an external power source. This option fully charges the battery at a standard rate. Charge time varies by device model.
    - Express Charge - Consider using this option for users who need the battery charged over a short time period. Dell's fast charging technology allows a completely discharged battery to typically charge to 80% in about 1 hour when the computer is turned off and to 100% in approximately 2 hours. Charge time may be longer with the computer turned on.
    - AC Charge - Consider using this option for users who primarily operate their system while plugged in to an external power source. This setting may extend your battery's lifespan by lowering the charge threshold.
    - Auto Charge - Consider using this option for users who want to set the option and not change it. This option lets the system optimize your battery settings based on your typical battery usage pattern.
    - Custom Charge - Consider using this option for advanced users that desire greater control over when their battery starts and stops charging.
- **Primary Battery Custom Charge Start Limit** - Set the battery charge percentage that must be reached before the device starts charging the battery.
- **Primary Battery Custom Charge Stop Limit** - Set the battery charge percentage that must be reached before the device stops charging the battery.
- **Peak Shift** - Select **Enable** to use peak shift to control when a device uses battery charge or AC current. Peak shift allows you to use battery power instead of AC current during specified times. To set the schedule for **Peak Shift**, select the calendar icon.
- **Peak Shift Scheduling** - The three parameters for peak shift scheduling control when a device uses battery or AC current and when the device charges the battery.
    - **Peak Shift Start** – Set the start time for Peak Shift when devices switch to battery power.
    - **Peak Shift End** – Set the end time for Peak Shift when devices switch to AC current.
    - **Peak Shift Charge Start** – Set the start time for Peak Shift Charge when the devices charge the batteries while using AC current.
- **Peak Shift Battery Threshold** - Set the battery charge percentage that must be reached before devices switch back to AC current from battery power. The **Peak Shift Charge Start** setting controls the time when devices charge the batteries after switching to AC current.
- **System Properties** - Select **Add System Properties** to add a custom system property. Select the button again to add additional properties. These properties are advanced options. Consider reviewing Dell documentation before using these settings. System Properties override any pre-defined settings configured in the profile.
- **Class** - Enter a class and select it from the drop-down menu. Displays after selecting **Add System Properties**.
- **System Property** - Enter a system property and select it from the drop-down menu. Displays after selecting **Add System Properties**.
- **BIOS Attributes** - Select **Add BIOS Attribute** to add a custom BIOS attribute. Select the button again to add additional attributes. These attributes are advanced options. Consider reviewing Dell documentation before using these settings. BIOS Attributes override any pre-defined settings configured in the profile.
- **BIOS Attribute** - Enter a BIOS attribute and select it from the drop-down menu. Displays after selecting **Add BIOS Attribute**.
- **Value** - Select a value for the BIOS attribute. If a value is not supplied, the BIOS Attribute is read only. Displays after selecting **Add BIOS Attribute**.
- **Configuration Package** - Select **Upload** to add a Dell Command | Configure configuration package. Uploading a package allows you to configure multiple Dell devices with a single configuration. Configuration packages override any custom system properties or attributes. If

you trust the file extensions allowed, you must add the CCTK file extension to the allow list. Navigate to **Groups & Settings** > **All Settings** > **Content** > **Advanced** > **File Extensions** to add the file extension.

6. Select **Save & Publish**.

Credentials Profile

A Credentials profile allows you to push Root, Intermediate, and Client certificates to your Windows devices to support any Public Key Infrastructure (PKI) and certificate authentication use case. The profile pushes configured credentials to the proper credentials store on the Windows Desktop device. Learn how to configure a credentials profile to enable authentication for your Windows devices.

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

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

Configuring a Credentials Profile

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

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

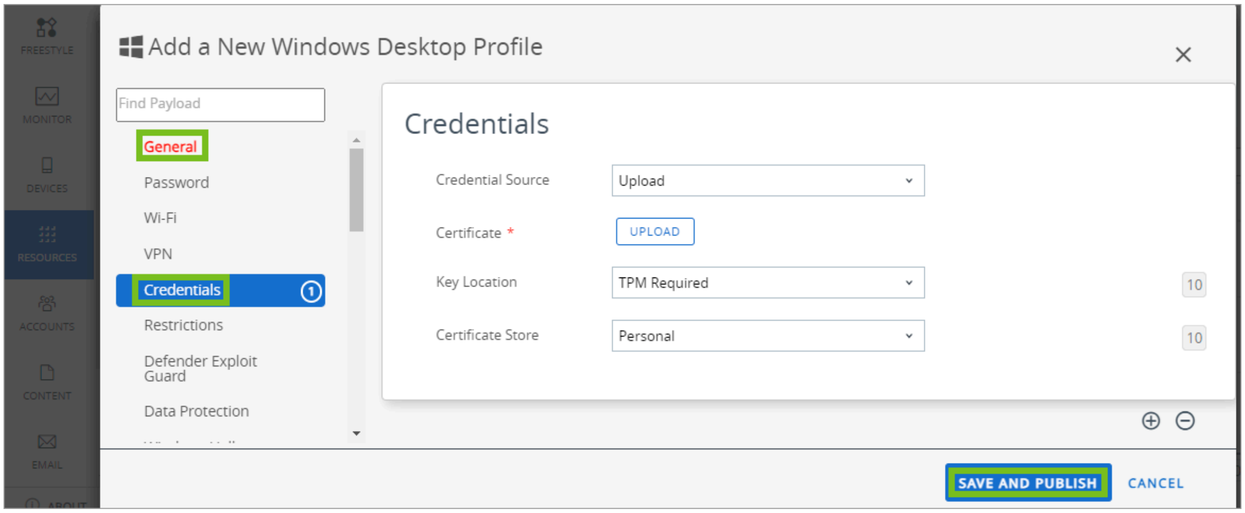
The credentials profile also allows you to push S/MIME certificates to devices. These certificates are uploaded under each user account and controlled by the credentials profile.

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

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

3. Select **User Profile** or **Device Profile**.

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



Credentials

Credential Source: Upload

Certificate *

Key Location: TPM Required

Certificate Store: Personal

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

Settings	Descriptions
Credential Source	Select the credential source as either an **Upload**, a **Defined Certificate Authority**, or **User Certificate**. The remaining payload options are source-dependent. If you select Upload, you must upload a new certificate. If you select Defined Certificate Authority, you must choose a predefined certificate authority and Template. If you select User Certificate, you must select how the S/MIME certificate is used.
Upload	Select to navigate to the desired credential certificate file and upload it to the Workspace ONE UEM console. This setting displays when **Upload** is selected as the **Credential Source**.
Certificate Authority	Use the drop-down menu to select a predefined certificate authority. This setting displays when **Defined Certificate Authority** is selected as the **Credential Source**.
Certificate Template	Use the drop-down menu to select a predefined certificate template specific to the selected certificate authority. This setting displays when **Defined Certificate Authority** is selected as the **Credential Source**.
Key Location	Select the location for the certificate private key: **TPM If Present** – Select to store the private key on a Trusted Platform Module if one is present on the device, otherwise store it in the OS. **TPM Required** – Select to store the private key on a Trusted Platform Module. If a TPM is not present, the certificate does not install and an error displays on the device. **Software** – Select to store the private key in the device OS. **Passport** – Select to save the private key within the Microsoft Passport. This option requires the Azure AD integration.
Certificate Store	Select the appropriate certificate store for the credential to reside in on the device: **Personal** – Select to store personal certificates. Personal certificates require the Workspace ONE Intelligent Hub on the device or using the SCEP payload. **Intermediate** – Select to store certificates from Intermediate Certificate Authorities.

Settings	Descriptions
	Trusted Root – Select to store certificates from Trusted Certificate Authorities and root certificates from your organization and Microsoft. **Trusted Publisher** – Select to store certificates from Trusted Certificates Authorities trusted by software restriction policies. **Trusted People** – Select to store certificates from trusted people or end entities that are explicitly trusted. Often these certificates are self-signed certificates or certificates explicitly trusted in an application such as Microsoft Outlook.
Store Location	Select **User** or **Machine** to define where the certificate is located.
S/MIME	Select whether the S/MIME certificate is for encryption or signing. This option only displays if **Credential Source** is set to **User Certificate**.

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

Custom Settings Profile

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

Prerequisites

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

Example Code

```
  <Replace>
    <CmdID>2</CmdID>
      <Item>
        <Target>
          <LocURI>./Device/Vendor/MSFT/AssignedAccess/KioskModeApp</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>{"Account":"standard","AUMID":"AirWatchLLC.AirWatchBrowser_htcwkw4r
x2gx4!App"}</Data>
      </Item>
  </Replace>
```

Procedure

1. Navigate to the Flings program

2. Select the Configuration Service Providers policy you want to use to create your custom profile.

3. Select **Configure**.

4. On the Configure page, configure the policy settings to meet your business needs.

5. Select the command verb to use with the policy: **Add**, **Delete**, **Remove**, or **Replace**.

6. Select the **Copy** button.

7. In the Workspace ONE UEM console, navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.

8. Select **Windows** and then select **Windows Desktop**.

9. Select **User Profile** or **Device Profile**.

10. Configure the profile **General** settings.

11. Select the **Custom Settings** payload and select **Configure**.

12. Select a **Target** for the custom profile.

    Most use cases use **OMA-DM** as the **Target**. Use **Workspace ONE Intelligent Hub** when you are customizing a BitLocker profile or looking to prevent users from disabling the airwatch service.

13. Select **Make Commands Atomic** as long as your SyncML uses the `Add`, `Delete`, or `Replace` commands. If your code uses `Exec`, do not select **Make Commands Atomic**.

14. Paste the XML you copied in the **Install Settings** text box. The XML code you paste must contain the complete block of code, from `<Add>` to `</Add>` or whatever command your SyncML code uses Do not include anything before or after these tags..

15. Add the removal code to the Delete Settings text box. The removal code must contain `<replace> </replace>` or `<delete> </delete>`.

    This code enables Workspace ONE UEM functionality such as Remove Profile and Deactivate Profile. Without the removal code, you cannot remove the profile from the devices besides pushing a second Custom Settings profile. For more information, see https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference.

16. Select **Save and Publish**.

Preventing Users from Disabling the Workspace ONE UEM Service

Use a Custom Settings profile to prevent end users from disabling the Workspace ONE UEM (AirWatch) Service on their Windows devices. Preventing end users from disabling the Workspace ONE UEM Service ensures that the Workspace ONE Intelligent Hub runs regular check-ins with the Workspace ONE UEM console and receives the latest policy updates.

1. Create a **Custom Settings** profile.

2. Set the **Target** to **Protection Agent**.

3. Copy the following code and paste it into the **Custom Settings** text box.

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

4. Select **Save & Publish**. If you want to remove the restriction from end user devices, you must push a separate profile using the following code.

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

Dynamic Environment Manager (DEM) Profile

Dynamic Environment Manager (DEM) provides a persistent user experience across user sessions on Windows devices. Capabilities include personalizing Windows and app settings and performing user and computer actions at certain triggers or at app launch. You can integrate Dynamic Environment Manager and Workspace ONE UEM to use these capabilities with the DEM profile.

The DEM profile in Workspace ONE UEM deploys a DEM config profile created in the Dynamic Environment Manager Management Console (DEM Management Console). The DEM config profile works on Workspace ONE UEM managed, Windows devices, whether the devices are virtual, physical, or cloud-based. On the device, the Workspace ONE Intelligent Hub for Windows and the DEM FlexEngine extract and apply your profiles.

DEM Documentation

See the Docs site for details on Dynamic Environment Manager.

CDN Required

The CDN is required for this feature.

- If you have a SaaS environment and you have disabled CDN, you must enable CDN or the DEM integration is not available.
- If you have an on-premises environment and you do not use or have not configured CDN, the DEM integration is not available.

Considerations

- In DEM, use **UEM Integrated** mode to create the DEM config profile. If you do not use this mode, you cannot create DEM config profiles. Workspace ONE UEM does not support DEM configuration SMB at this time.
- Ensure that your configurations in Dynamic Environment Manager and Workspace ONE UEM do not conflict. For example, do not restrict certain configurations in one console and permit them in another.
- In Workspace ONE UEM, do not assign multiple DEM profiles to a single device. Assigning multiple DEM profiles to a single device might deploy incorrect configurations.
- Extract and install the DEM Management Console and the DEM FlexEngine using the **custom** installation process and not the default installation process. The default installation process installs only the DEM Management Console.
- Use DEM v2106 or later because this integration is not supported in earlier versions.

Do These Tasks Before Integrating

Before you can integrate Dynamic Environment Manager (DEM) and Workspace ONE UEM, you must install the DEM Management Console and you must deploy the DEM FlexEngine to managed devices.

- Download and extract the DEM Management Console and the DEM FlexEngine.
  - Go to the Customer Connect site for Dynamic Environment Manager.
  - Download the applicable versions of the console and the engine.
- Install the DEM Management Console on a device where you want to create config profiles.
  - Switch the DEM Management Console to **UEM Integrated** mode by choosing `Configure | Integration | Workspace ONE UEM Integration`.
- When you create your DEM config profile, complete the following tasks.
  - Include a NoAD.xml file as part of your configuration.
  - Include a license file by importing one from the main menu icon in the DEM Management Console.
  - Save the DEM config profile so you can upload it to Workspace ONE UEM using the DEM profile.

- Deploy the DEM FlexEngine as an app (MSI) to managed Windows devices with Workspace ONE UEM. Managed devices need both the DEM FlexEngine and the Workspace ONE Intelligent Hub for Windows to apply the DEM config profiles on the device.

  1. In the Workspace ONE UEM console, select the applicable organization group.
  2. Navigate to **Resources > Apps > Native > Internal**.
  3. Upload the DEM FlexEngine MSI file.

  4. On the **Deployment Options** tab, enable **UEM Integrated** mode on the command line during installation.

     a. Go to the **How To Install** section.
     b. Enter the command in the **Install Command** text box.

  5. **Save & Assign** the app to deploy it to the appropriate smart groups that include your managed Windows devices.

Configuring a DEM Profile

Use Workspace ONE UEM device profiles to deploy your DEM (Dynamic Environment Manager) configurations across your managed Windows devices.

1. In Workspace ONE UEM, navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **Add Profile**.
2. Select **Windows** and choose **Windows Desktop** as the platform.
3. Select **Device Profile**.
4. Configure the profile **General** settings. The **General** payload includes the smart groups assignment, so assign the smart groups that include your managed Windows devices to receive the DEM config profile.
5. Select the **Dynamic Environment Manager** (DEM) payload.
6. Use the **DEM** page to upload the DEM config file and select **Save and Publish** to complete the configurations.

Workspace ONE UEM deploys the DEM config profile to the managed devices in the assigned smart groups. The DEM FlexEngine and the Workspace ONE Intelligent Hub for Windows on the device apply your DEM config profiles. The profile changes are only visible after logging off and logging on to the device after the system delivers the profile.

Applying DEM Config Profile Changes

The device user must log off and then log back in to the managed Windows device in order to see the profile changes deployed by the DEM config profiles.

Data Protection Profile

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

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

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

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

- Enlightened Apps – These apps fully support WIP functionality. Enlightened apps can access both personal and corporate data without issues. If data is created with an enlightened app, you can save the data as unencrypted personal data or encrypted corporate data. You can restrict users from saving personal data with enlightened apps using the Data Protection profile.
- Allowed – These apps support WIP-encrypted data. Allowed apps can access both corporate and personal data but the apps save any accessed data as encrypted corporate data. Allowed apps save personal data as encrypted corporate data that cannot be accessed outside of WIP-approved apps. Consider slowly trusting apps on a case-by-case basis to prevent issues accessing data. Reach out to software providers for information on WIP approval.
- Exempt – You determine which apps are exempt from WIP policy enforcement when you create the Data Protection profile. Exempt any apps that do not support WIP-encrypted data. If an app does not support WIP-encryption, the apps break when attempting to access encrypted corporate data. No WIP policies apply to exempt apps. Exempt apps can access unencrypted personal data and encrypted corporate data. Because exempt apps access corporate data without WIP policy enforcement, use caution when trusting exempt apps. Exempt apps create gaps in data protection and leak corporate data.
- Not Allowed – These apps are not trusted or exempted from WIP policies and cannot access encrypted corporate data. Not allowed apps can still access personal data on a WIP-protected device.

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

Configuring a Data Protection Profile

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

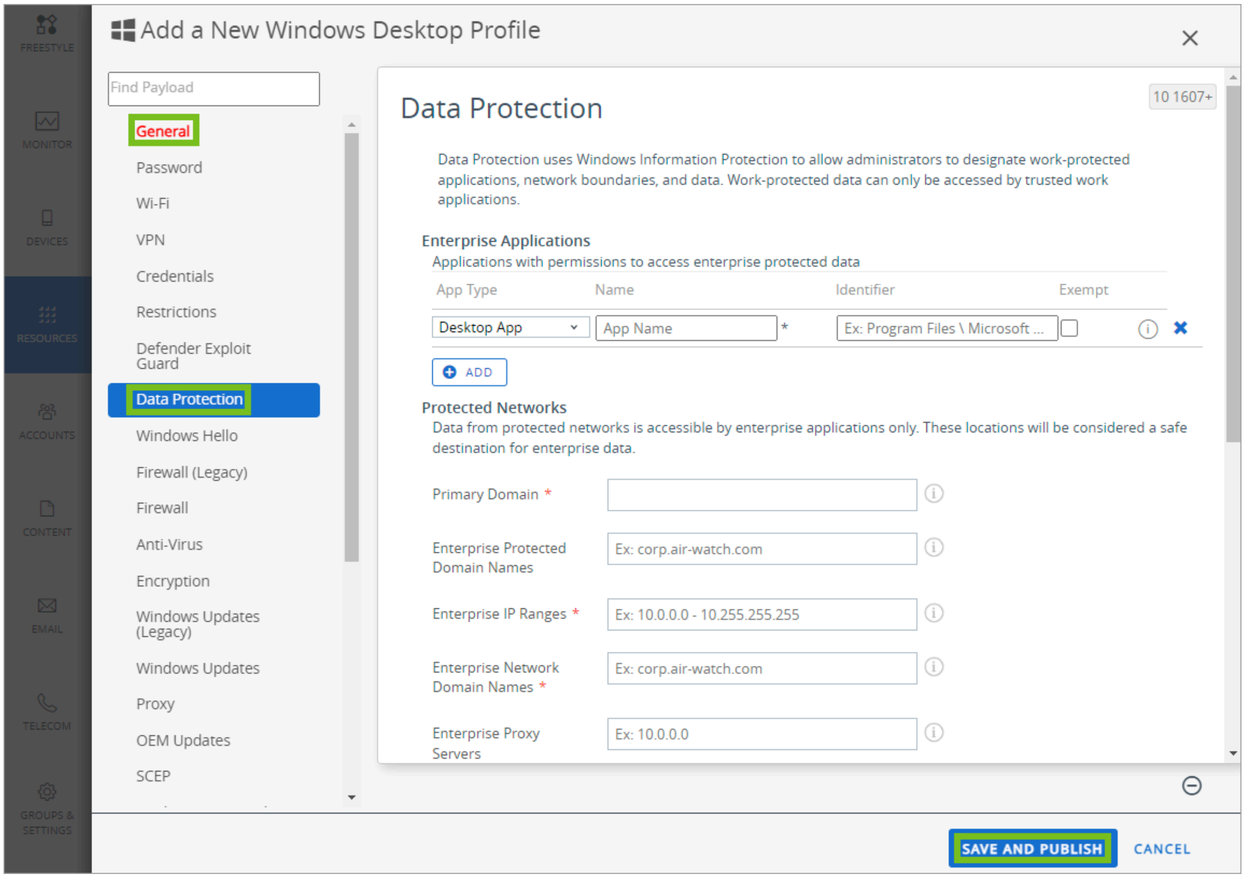
1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.

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

3. Select **Device Profile**.

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

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



Add a New Windows Desktop Profile

Data Protection

10 1607+

Data Protection uses Windows Information Protection to allow administrators to designate work-protected applications, network boundaries, and data. Work-protected data can only be accessed by trusted work applications.

Enterprise Applications

Applications with permissions to access enterprise protected data

App Type	Name	Identifier	Exempt
Desktop App	App Name *	Ex: Program Files \ Microsoft ...	□

ADD

Protected Networks

Data from protected networks is accessible by enterprise applications only. These locations will be considered a safe destination for enterprise data.

Primary Domain *

Enterprise Protected Domain Names: Ex: corp.air-watch.com

Enterprise IP Ranges *: Ex: 10.0.0.0 - 10.255.255.255

Enterprise Network Domain Names *: Ex: corp.air-watch.com

Enterprise Proxy Servers: Ex: 10.0.0.0

6. Configure the Enterprise Data Protection settings:

Settings	Descriptions
Add	Select to add enterprise applications to the enterprise allowed list. Applications added here are trusted to use enterprise data.
App Type	Select whether the application is a traditional desktop application or a Microsoft Store app. You can also select an application publisher for desktop applications or store apps. Selecting a publisher trusts all apps from the publisher.
Name	Enter the app name. If the app is a Microsoft Store app, select the **Search** icon to search for the app Package Family Name (PFN).
Identifier	Enter the file path for a desktop application or the package family name for a store app.
Exempt	Select the check box if the app does not support full data protection but still needs access to enterprise data. Enabling this option exempts the app from data protection restrictions. These apps are often legacy apps not yet updated for data protection support. Creating exemptions creates gaps in data protection. Only create exemptions when necessary.
Primary Domain	Enter the primary domain that your enterprise data uses. Data from protected networks is accessible by enterprise applications only. Attempting to access a protected network from an application not on the enterprise allowed list results in enforcement policy action.

Settings	Descriptions
	Enter domains in lowercase characters only.
Enterprise Protected Domain Names	Enter a list of domains (other than your primary domain) used by the enterprise for its user identities. Separate the domains with the vertical bar character `|`. Enter domains in lowercase characters only.
Enterprise IP Ranges	Enter the enterprise IP ranges that define the Windows devices in the enterprise network. Data that comes from the devices in range are considered part of the enterprise and are protected. These locations are considered a safe destination for enterprise data sharing.
Enterprise Network Domain Names	Enter the list of domains that are the boundaries of the enterprise network. Data from a listed domain that is sent to a device is considered enterprise data and is protected. These locations are considered a safe destination for enterprise data sharing.
Enterprise Proxy Servers	Enter the list of proxy server that the enterprise can use for corporate resources.
Enterprise Cloud Resources	Enter the list of enterprise resource domains hosted in the cloud that need to be protected by routing through the enterprise network through a proxy server (on port 80). If Windows cannot determine whether to allow an app to connect to a network resource, it will automatically block the connection. If you want Windows to default to allow the connections, add the `/*AppCompat*/` string to the setting. For example: `www.air-watch.com	/*AppCompat*/` Only add the `/*AppCompat*/` string once to change the default setting.
Application Data Protection Level	Set the level of protection and the actions taken to protect enterprise data.
Show EDP Icons	Enable to display an EDP icon in the Web browser, file explorer, and app icons when accessing protected data. The icon also displays in enterprise-only app tiles on the Start menu.
Revoke on Unenroll	Enable to revoke Data Protection keys from a device when the device unenrolls from Workspace ONE UEM.
User Decryption	Enable to allow users to select how data is saved using an enlightened app. They can select Save as Corporate or Save as Personal. If this option is not enabled, all data saved using an enlightened app will save as corporate data and encrypt using the corporate encryption.
Direct Memory Access	Enable to allow users direct access to device memory.
Data Recovery Certificate	Upload the special Encrypting File System certificate to use for file recovery if your encryption key is lost or damaged.

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

Creating an Encrypting File System Certificate

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

1. On a computer without an EFS certificate, open a command prompt (with admin rights) and navigate to the certificate store you where you want to store the certificate.
2. Run the command: `cipher /r:<EFSRA>`

   The value of is the name of the .cer and .pfx files that you want to create.
3. When prompted, enter the password to help protect your new .pfx file.
4. The .cer and .pfx files are created in the certificate store you selected.
5. Upload your .cer certificate to devices as part of a Data Protection profile.

Defender Exploit Guard Profile

Protect your Windows devices from exploits and malware with the Windows Defender Exploit Guard profile. Workspace ONE UEM uses these settings to protect your devices from exploits, reduce attack surfaces, control folder access, and protect your network connections.

Windows Defender Exploit Guard

Various malware and exploits use vulnerabilities in your Windows devices to gain access to your network and devices. Workspace ONE UEM uses the Windows Defender Exploit Guard profile to protect your devices from these bad actors. The profile uses the Windows Defender Exploit Guard settings native to Windows. The profile contains four different methods of protection. These methods cover different vulnerabilities and attack vectors.

Exploit Protection

Exploit protection automatically applies exploit mitigations to both the operating system and apps. These mitigations also work with third-party antivirus and Windows Defender antivirus. In the Windows Defender Exploit Guard profile, you configure these settings by uploading a configuration XML file. This file must be created using the Windows Security App or PowerShell.

Attack Surface Reduction

Attack surface reduction rules help prevent the typical actions malware use to infect devices. These rules target actions such as:

- Executable files and scripts used in Office apps or web mail that try to download or run files
- Obfuscated or otherwise suspicious scripts
- Actions that apps do not usually use

Attack surface reduction rules require Windows Defender Real Time Protection enabled.

Controlled Folder Access

Controlled folder access helps protect your valuable data from malicious apps and threats including ransomware. When enabled, Windows Defender Antivirus reviews all apps (.EXE, .SCR, .DLL, and so on). Windows Defender then determines if the app is malicious or safe. If the app is marked as malicious or suspicious, then Windows prevents the app from changing files in protected folders.

Protected folders include common system folders. You can add you own folders to Controlled Folder Access. Most known and trusted apps can access protected folders. If you want an internal or unknown app to access protected folders, you must add the app file path when creating the profile.

Controlled folder access requires Windows Defender Real Time Protection enabled.

Network Protection

Network protection helps protect users and data from phishing scams and malicious websites. These settings prevent users from using any app to access dangerous domains that might host phishing attacks, exploits, or malware.

Network protection requires Windows Defender Real Time Protection enabled.

Additional Information

For more information on the specific exploit protections and settings configured, see https://docs.microsoft.com/en-us/sccm/protect/deploy-use/create-deploy-exploit-guard-policy.

Creating a Defender Exploit Guard Profile

Create a Defender Exploit Guard profile through Workspace ONE UEM to protect your Windows devices against exploits and malware. Learn how to use the profile to configure the Windows Defender Exploit Guard settings on your Windows devices.

When you create rules and settings for **Attack Surface Reduction**, **Controlled Folder Access**, and **Network Protection**, you must select Enabled, Disabled, or Audit. These options change how the rule or setting functions.

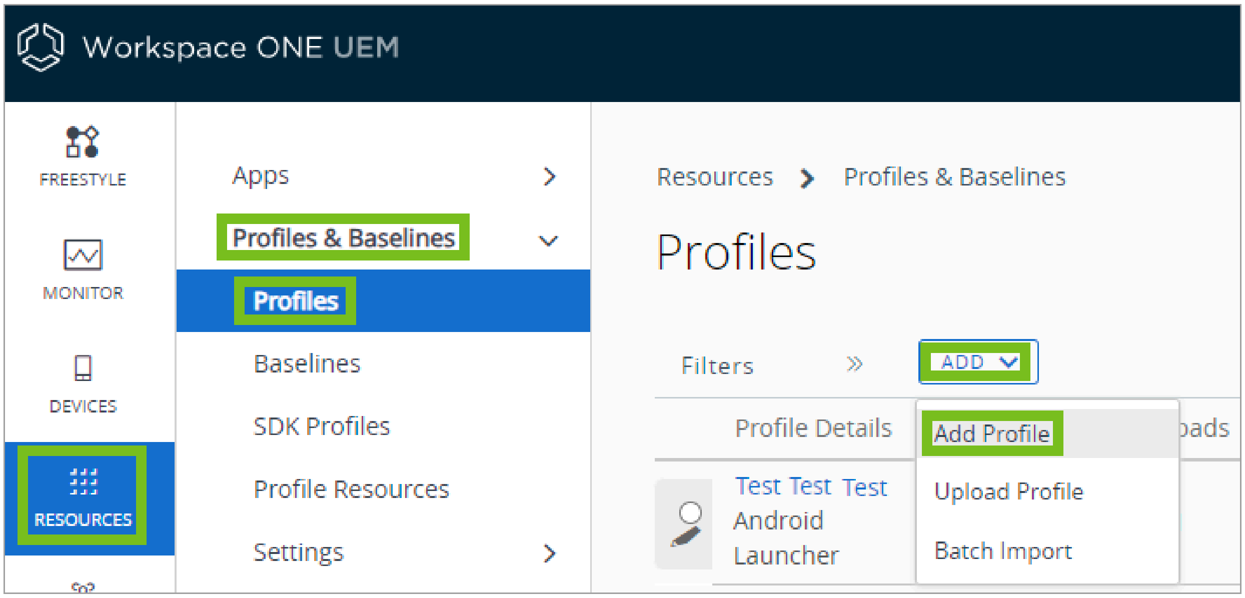
- Enabled - Configures Windows Defender to block exploits for that method. For example, if you set Controlled Folder Access to Enabled, Windows Defender will block exploits from accessing the protected folders.
- Disabled - Doe not configured the policy for Windows Defender.
- Audit - Configured Windows Defender to block the exploits the same as Enabled, but also logs the event in the event viewer.

Prerequisites

To use the Exploit Protection settings in this profile, you must create a configuration XML file using Windows Security App or PowerShell on an individual device before creating the profile.

Procedure

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



2. Select **Windows** and then select **Windows Desktop**.
3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Defender Exploit Guard** payload.
6. Upload **Exploit Protection Settings** configuration XML file.

   These settings automatically apply exploit mitigation techniques to both the operating system and individual apps. You must create the XML file using the Windows Security App or PowerShell on an individual device.
7. Configure the **Attack Surface Reduction** settings. These rules help prevent the typical actions malware uses to infect devices with malicious code. Select **Add** to add additional rules.

   The description of each rule describes what apps or file types the rule applies to. Attack surface reduction rules require Windows Defender Real-Time Protection enabled.
8. Configure the **Controlled Folder Access** settings. Set **Controlled Folder Access** to **Enabled** to use these settings. When enabled, the setting protects several folders by default. To see the list, point to over the **?** icon. These settings automatically protect your data from malware and exploits. Controlled folder access requires Windows Defender Real-Time Protection enabled.
   - Add additional folders to protect by selecting **Add New** and enter the folder file path.
   - Add applications that can access protected folders by selecting **Add New** and entering the application file path. Most known and trusted apps can access the folders by default. Use this setting to add internal or unknown apps to access protected folders.
9. Configure the Network Protection settings. Set **Network Protection** to **Enabled** to use these settings. These settings protect users and data from phishing scams and malicious websites. Network protection requires Windows Defender Real-Time Protection enabled.
10. Select **Save and Publish** when you are finished to push the profile to devices.

Encryption Profile

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

BitLocker encryption is only available on Windows Enterprise, Education, and Pro devices.

Because laptops and tablets are mobile devices by design, they risk your organization’s data being lost or stolen. By enforcing an encryption policy through Workspace ONE UEM, you can protect data on the hard drive. BitLocker is the native Windows encryption and Dell Data Protection | Encryption is a third-party encryption solution from Dell. With the Encryption profile enabled, Workspace ONE Intelligent Hub continually checks the encryption status of the device. If Workspace ONE Intelligent Hub finds that the device is not encrypted, it automatically encrypts the device.

If you decide to encrypt with BitLocker, a recovery key created during encryption is stored for each drive (if configured) in the Workspace ONE UEM console. The admin has the option to make the recovery keys a single use key. If selected, a new recovery key will be generated after it is used once. Then the user would need to contact the administrator for the new updated recovery key. See Recovery Keys for more information.

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

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

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

BitLocker Functionality

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

BitLocker uses the Trusted Platform Module (TPM) on devices to store the encryption key for the device. If the drive is removed from the motherboard, the drive remains encrypted. For enhanced authentication, you can enable an encryption PIN to boot the system. You can also require a password for devices when a TPM is not available.

Deployment Behavior

The Windows-native BitLocker encryption secures data on Windows Desktop devices. Deploying the Encryption profile may require additional actions from the end user, such as creating a PIN or password.

If the Encryption profile is pushed to an encrypted device and the current encryption settings match the profile settings, Workspace ONE Intelligent Hub adds a BitLocker protector and sends a recovery key to the Workspace ONE UEM console.

With this feature, if a user or an admin attempts to disable BitLocker on the device, the Encryption profile can re-encrypt it. The encryption is enforced even if the device is offline.

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

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

Note: BIOS profile changes apply after Encryption profiles. Changes to the BIOS profile such as disabling or clearing the TPM can cause a recovery event to occur that requires the recovery key to restart the system. Suspend BitLocker before making any changes to the BIOS.

Encryption Statuses

If BitLocker is enabled and in use, you can see information about the state of encryption in the listed areas.

- Workspace ONE UEM **Device Details**
    - Device Details displays recovery key information. Use the **View Recovery Key** link to view and

copy recovery keys for all your encrypted drives.

    - Find several BitLocker statuses on the **Summary** tab that include **Encrypted**, **Encryption in Progress**, **Decryption in Progress**, **Suspended**, and **Partially Protected**.
        - The **Suspended (X reboots remaining)** status reflects the suspension of the disk's protection, although the disk is still encrypted. You might see this status if an operating system is getting updated or if system level changes are being made to the system. Once the number of reboots is exhausted, BitLocker protection is automatically re-enabled.
        - The **Partially Protected** status reflects the situation where the OS drive is encrypted but other drives are not.
    - On the **Security** tab in **Device Details**, view the encryption status and the encryption method of your drives. You can find out at a glance if a machine is not using the level of encryption you have set in the Encryption profile. Workspace ONE UEM only displays the encryption method. It does not decrypt disks, even if they do not match the **Encryption Method** setting in the **Encryption** profile.
- Workspace ONE UEM Self-Service Portal
    - The Security page of the Self-Service Portal displays the BitLocker recovery key.
    - BitLocker protection displays as enabled.

Recovery Keys

Workspace ONE UEM escrows recovery keys for **OS Drive and All Fixed Hard Drives** when you have this setting enabled for **Encrypted Volume** in the **Encryption** profile. If a drive needs to be recovered, the recovery key is available for each individual drive.

The admin has the option to make the recovery keys single use by selecting **Enable Single Use Recovery Key** from the **Encryption Profile** settings. See Configuring an Encryption Profile for more information. If enabled once a recovery key is used to recover a drive, a new recovery key is generated by the Intelligent Hub and is escrowed back to the UEM console.

For a brief period of time, until the new recovery key is successfully escrowed to the UEM console, both Previous Personal Recovery Key (old) and Personal Recovery Key (new) will be available for use. On successful escrow of the new recovery key, the previous recovery key will be deleted and can no longer be used for recovering the drive.

For troubleshooting purposes, you can see who recovered a removable drive with a specific key, when recovery occurred, and which admin helped with the process. In the Workspace ONE UEM console, go to **Devices > Details View > More - Troubleshooting > Event Log** to find the details.

Removal Behavior

If the profile is removed from the Workspace ONE UEM console, Workspace ONE UEM no longer enforces the encryption and the device automatically decrypts. Enterprise wiping or manually uninstalling Workspace ONE Intelligent Hub from the Control Panel disables BitLocker encryption.

When you create the Encryption profile, you can enable the **Keep System Encrypted at All Times** option. This setting ensures that the device remains encrypted even if the profile is removed, the device is wiped, or communication with Workspace ONE UEM ends.

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

BitLocker and Compliance Policies

You can configure compliance policies to support the BitLocker encryption status you want to enforce. In the Rules section of a compliance policy, select **Encryption** > **Is** and select from the choices of **Not applied to system drive**, **Not applied to some drives** (partially protected), or **Suspended**.

BitLocker To Go Support

With the Encryption profile, you can require the encryption of removable drives for your Windows devices using BitLocker To Go. Select the **Enable BitLocker To Go Support** check box to enable this feature. Removable drives are read-only until encrypted. By selecting an option in the Encryption Method drop down, you may choose which method to use to encrypt the device.

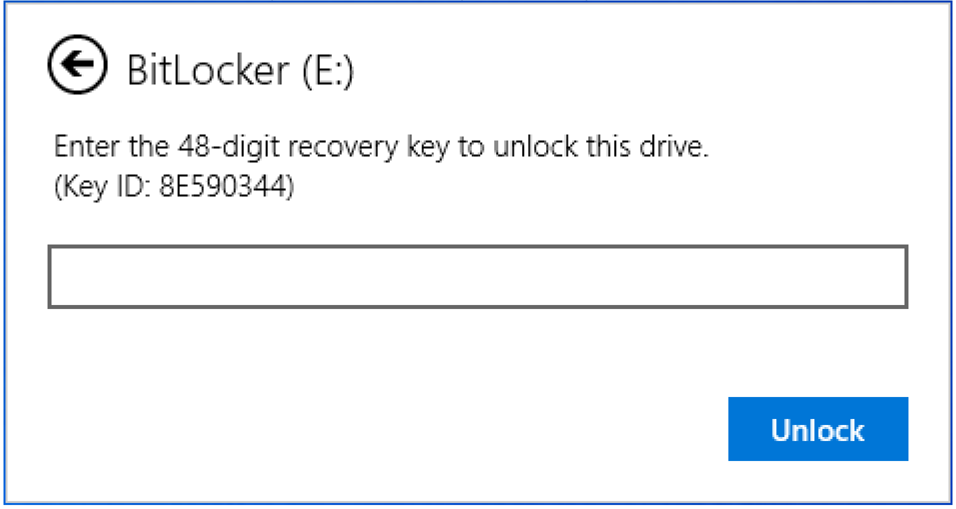
The Workspace ONE Intelligent Hub for Windows prompts your users to create password to access and use the drives. The minimum length of that password can be set by the admin in the console under the **BitLocker To Go Settings**. When users plug the encrypted drive into the Windows device, they use their password to access the drive, copy content to the drive, edit files, delete content, or any other task performed with removable drives. The admin can also select if they would like to encrypt only used space on the drive or the total drive.

Where Do You Find Recovery Key Information?

If users lose their passwords, you can recover the drives from the console in **Devices > Peripherals > List View > Removable Storage**. Use the **View** link for the drive to copy the recovery key and email it to the applicable user. You can also access this page from the user's account at **Accounts > Users > List View**, select the user, and choose the **Removable Storage** tab.

For deployments with thousands of recovery IDs, you can filter content on the **Removable Storage** page. There are several ways to filter content.

- Have the user give you the **Key ID** and then select the filter caret on the **Recovery ID** column and type the value. The recovery ID with that key ID displays in the results.



BitLocker (E:)

Enter the 48-digit recovery key to unlock this drive.
(Key ID: 8E590344)

- Select the filter caret on the **Username** column and type the applicable user name to find the drive and its recovery key.

For auditing purposes, you can see who recovered a removable drive with a specific key, when recovery occurred, and which admin helped with the process. In the Workspace ONE UEM console, go to **Devices > Peripherals > List View > Events** to find the details.

You can look up key information by user. In the Workspace ONE UEM console, go to **Accounts > Users > List View** and select the user. The user's record has a **Removable Storage** tab if they encrypted at least one drive.

Suspend BitLocker From the Console

You can now suspend and resume BitLocker encryption from the console. This menu item is added as an action in device records. Find it in **Devices > List View**, select the device, and select the **More Actions** menu item. This option is helpful for users who do not have permissions to manage BitLocker but need help with their device.

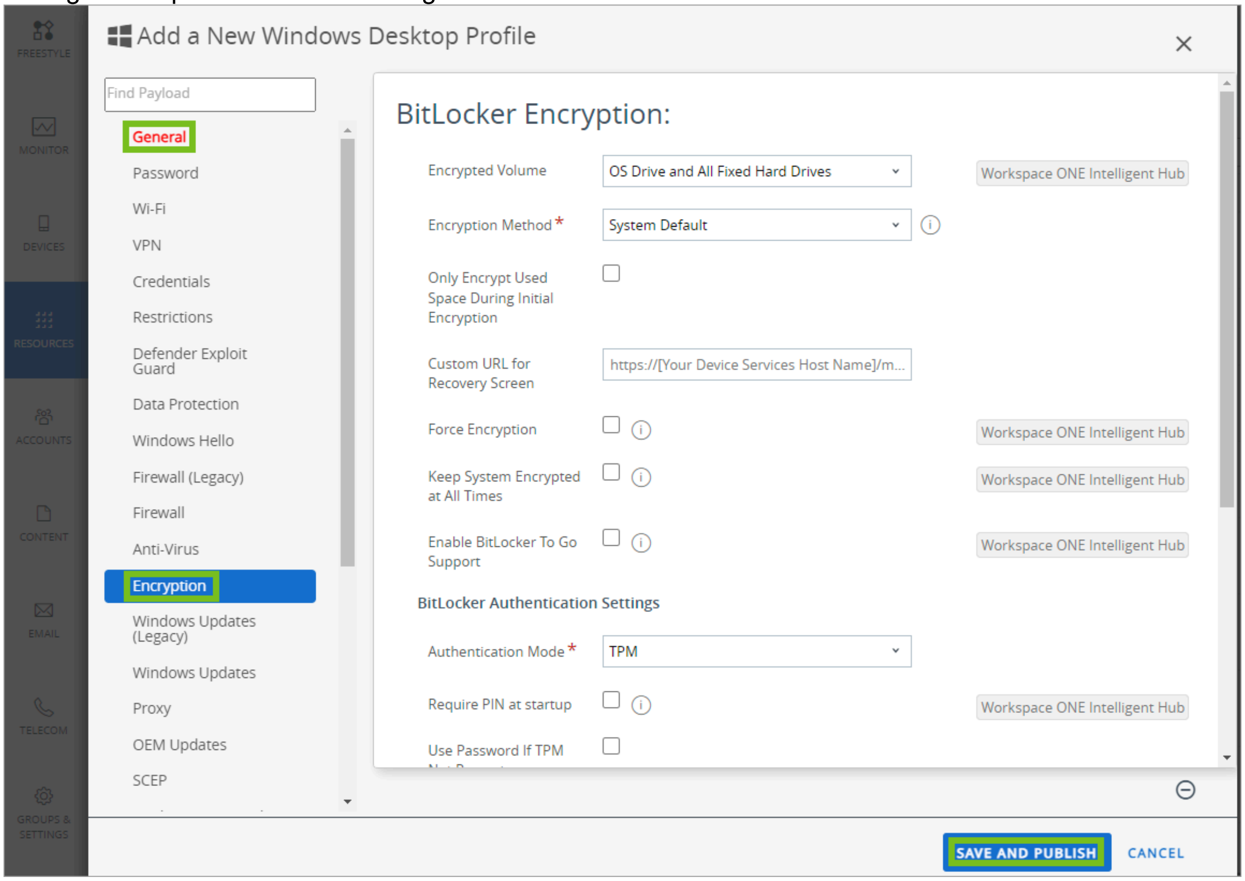
When you select to **Suspend BitLocker** for a device, the console displays several options and one of them is for **Number of Reboots**. For example, helping a user update their BIOS can require the system to reboot twice, so select **3**. This value gives the system one extra reboot with encryption 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.

Configuring an Encryption Profile

Create an **Encryption** profile to secure your data on Windows Desktop devices using the native BitLocker and BitLocker To Go encryptions.

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



Add a New Windows Desktop Profile

BitLocker Encryption:

Encrypted Volume: OS Drive and All Fixed Hard Drives — Workspace ONE Intelligent Hub

Encryption Method*: System Default

Only Encrypt Used Space During Initial Encryption: □

Custom URL for Recovery Screen: https://[Your Device Services Host Name]/m...

Force Encryption: □ — Workspace ONE Intelligent Hub

Keep System Encrypted at All Times: □ — Workspace ONE Intelligent Hub

Enable BitLocker To Go Support: □ — Workspace ONE Intelligent Hub

BitLocker Authentication Settings

Authentication Mode*: TPM

Require PIN at startup: □ — Workspace ONE Intelligent Hub

Use Password If TPM: □

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

Settings	Descriptions
Encrypted Volume	Use the drop-down menu to select the type of encryption as follows: **OS Drive and All Fixed Hard Drives** – Encrypts all hard drives on the device, including the System Partition where the OS is installed. **OS Drive** – Encrypts the drive that Windows is installed on and from which it boots.
Encryption Method	Select the encryption method for the device.

Settings	Descriptions
Default to System Encryption Method	Select this check box if your OEM specifies a default encryption method for a given type of device. This setting applies the default encryption algorithm.
Only Encrypt Used Space During Initial Encryption	Enable to limit the BitLocker encryption to only the used space on the drive at the time of encryption.
Custom URL for Recovery Key	Enter the URL to display on the lock screen directing end users to get the recovery key. Consider entering the Self Service Portal URL as Workspace ONE UEM hosts the recovery key there.
Force Encryption	Enable to force encryption on the device. This enforcement means that the device immediately re-encrypts if BitLocker is manually disabled. Consider disabling this setting to prevent issues during upgrades or Enterprise Wipes.
Keep System Encrypted at All Times	Enable this option to keep the device encrypted at all times. Use this option to ensure that device wipes, profile removals, or break in communication with Workspace ONE UEM does not decrypt the device. If you enable this setting and wipe a device, you can only access the recovery from the Workspace ONE UEM console for 30 days. After 30 days, the system may be unrecoverable.
Enable BitLocker To Go Support	Enable this option to require BitLocker to encrypt removable drives on Windows devices. When selected, removable drives are read-only until encrypted. The admin can configure the Encryption Method, minimum password length, and whether they want to only encrypt used space or everything during the initial encryption. Users must create a password to access the drives. If your users forget their passwords, find recovery IDs and keys for these encrypted drives in the console at **Devices > Peripherals > List View > Removable Storage**.
BitLocker Authentication Settings: Authentication Mode	Select the method for authenticating access to a BitLocker encrypted device. **TPM** — Uses the devices Trusted Platform Module. Requires a TPM on the device. **Password** — Uses a password to authenticate.
BitLocker Authentication Settings: Require PIN at startup	Select the check box to require users to enter a PIN to boot the device. This option prevents OS start up and auto-resume from suspend or hibernate until the user enters the correct PIN.
BitLocker Authentication Settings: PIN Length	Select this setting to configure a specific length for the PIN at startup. This PIN is numeric unless otherwise configured with **Allow Enhanced PIN** at Startup.
BitLocker Authentication Settings: Allow	Select this check box to allow users to set PINs with more than numbers. Users can set uppercase and lowercase letters, use symbols, numbers, and spaces. If the machine does not support enhanced PINs in a pre-boot environment, this

Settings	Descriptions
Enhanced PIN at Startup	settings does not work.
BitLocker Authentication Settings: Use Password if TPM Not Present	Select the check box to use a password as a fallback to encrypt the device if the TPM is unavailable. If this setting is not enabled, any devices without a TPM do not encrypt.
BitLocker Authentication Settings: Suspend BitLocker until TPM is initialized	Select this option to postpone encryption on the device until TPM is initialized on the machine. Use this option for enrollments that require encryption before TPM initializes such as OOBE.
BitLocker Authentication Settings: Minimum Password Length	Select the minimum number of characters a password must be. Displays if the **Authentication Mode** is set to **Password** or if **Use Password if TPM Not Available** is enabled.
BitLocker Recovery Key Settings: Enable Single Use Recovery Key	Select the check box to make the recovery keys single use. Once used a new recovery key will be generated. The user must contact the administrator for the updated recovery key.
BitLocker Static Recovery Key Settings: Create Static BitLocker Key	Select the check box if a static recovery key is enabled.
BitLocker Static Recovery Key Settings: BitLocker Recovery Password	Select the **Generate** icon to generate a new recovery key.
BitLocker Static Recovery Key Settings: Rotation Period	Enter the number of days until the recovery key rotates.
BitLocker Static Recovery Key Settings: Grace Period	Enter the number of days after rotation that the previous recovery key still works.
BitLocker Suspend: Enable BitLocker	Select the check box to enable BitLocker Suspension. This functionality suspends BitLocker encryption during a specified time period. Use this feature to suspend BitLocker when updates are scheduled so devices can

Settings	Descriptions
Suspend	reboot without requiring end users to enter the Encryption PIN or password.
BitLocker Suspend: Suspend BitLocker Type	Select the type of suspension. **Schedule** — Select to enter the specific time period that BitLocker suspends. Then set the schedule repeat to daily or weekly. **Custom** — Select to enter the day and time to begin and end BitLocker suspension.
BitLocker Suspend: BitLocker Suspend Start Time	Enter the time to start BitLocker suspension.
BitLocker Suspend: BitLocker Suspend End Time	Enter the time to end BitLocker suspension.
BitLocker Suspend: Scheduled Repeat Type	Set whether the scheduled suspension repeats daily or weekly. If you select weekly, select the days of the week to repeat the schedule.

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

Exchange ActiveSync Profile

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

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

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

Removing Profiles or Enterprise Wiping

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

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

Username and Password

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

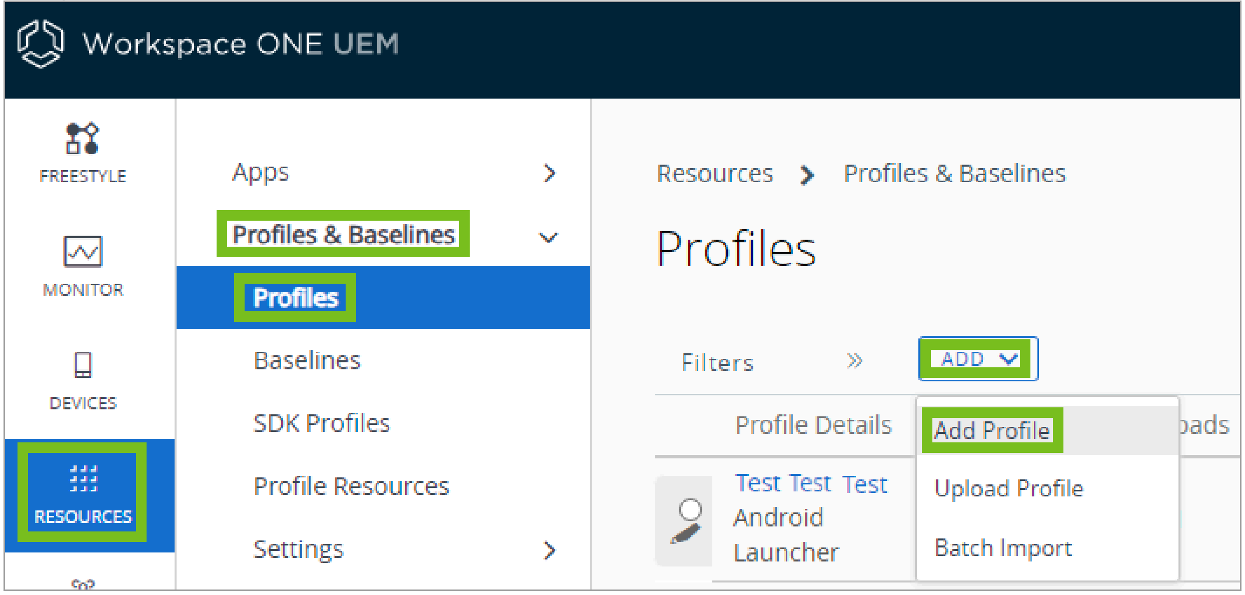
Create an Exchange ActiveSync profile to give Windows Desktop devices access to your Exchange ActiveSync server for email and calendar use.

Configuring an Exchange ActiveSync Profile

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

Note: Workspace ONE UEM does not support Outlook 2016 for Exchange ActiveSync profiles. Exchange Web Services (EWS) profile configuration for Outlook Application on a Windows Desktop device through Workspace ONE UEM is no longer supported with Microsoft Exchange 2016 version.

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



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

3. Select **User Profile**.

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

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

6. Configure the Exchange ActiveSync settings:

Settings	Descriptions
Mail Client	Select the Mail Client that the EAS profile configures. Workspace ONE UEM supports the Native Mail Client.
Account Name	Enter the name for the Exchange ActiveSync account.
Exchange ActiveSync Host	Enter the URL or IP Address for the server hosting the EAS server.
Use SSL	Enable to send all communications through the Secure Socket Layer.
Domain	Enter the email domain. The profile supports lookup values for inserting enrollment user login information.

Settings	Descriptions
Username	Enter the email user name.
Email Address	Enter the email address. This text box is a required setting.
Password	Enter the email password.
Identity Certificate	Select the certificate for the EAS payload.
Next Sync Interval (Min)	Select the frequency, in minutes, that the device syncs with the EAS server.
Past Days of Mail to Sync	Select how many days of past emails sync to the device.
Diagnostic Logging	Enable to log information for troubleshooting purposes.
Require Data Protection Under Lock	Enable to require data to be protected when the device is locked.
Allow Email Sync	Enable to allow the syncing of email messages.
Allow Contacts Sync	Enable to allow the syncing of contacts.
Allow Calendar Sync	Enable to allow the syncing of calendar events.

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

Exchange Web Services Profile

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

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

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile**.
4. Configure the profile **General** settings.
5. Select the **Exchange Web Services** profile and configure the settings:

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

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

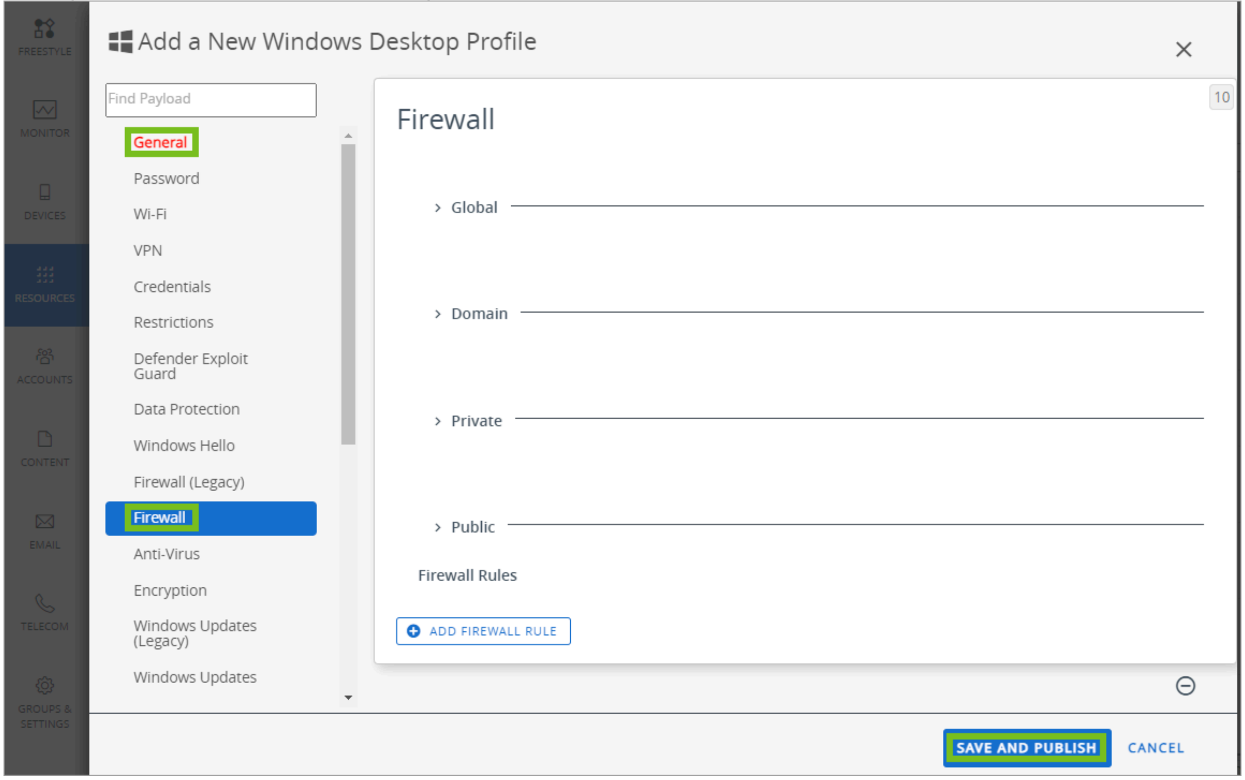
   Removing an Exchange Web Services profile removes all Outlook accounts from the device.

Firewall Profile

Create a Firewall profile to configure the native Windows Desktop firewall settings. This profile uses more advanced functionality than the Firewall (Legacy) profile.

Workspace ONE UEM trusts the OMA-DM agent automatically to ensure the Workspace ONE UEM console can always communicate with devices.

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



5. Select the **Firewall** payload.
6. Configure the **Global** settings.

Setting	Description
Stateful FTP	Set how the firewall handles FTP traffic. If you select Enable, the firewall tracks all FTP traffic. If you select **Disable**, the firewall does not inspect FTP traffic.
Security Association Idle Time	Select **Configured** and set the maximum amount of time (in seconds) the device waits before deleting idle security associations. Security associations are an agreement between two peers or endpoints. These agreements contain all the information required to securely exchange data.
Preshared Key Encoding	Select the type of encoding used for the preshared key.

Setting	Description
IPSec Exemptions	Select the IPSec exemptions to use.
Certification Revocation List Verification	Select how to enforce the certificate revocation list verification.
Opportunity Match Auth Set Per KM	Select how key modules ignore authentication suites. Enabling this option forces key modules to ignore only the authentication suites they do not support. Disabling this option forces key modules to ignore the entire authentication set if they do not support all the authentication suites in the set.
Enable Packet Queue	Select how packet queuing works on the device. This setting allows you to ensure proper scaling.

7. Configure how the firewall behaves when connected to **Domain**, **Private**, and **Public** networks.

Setting	Description
Firewall	Set to **Enable** to enforce policy settings on the network traffic. If disabled, the device allows all network traffic, regardless of other policy settings.
Outbound Action	Select the default action the firewall takes on outbound connections. If you set this setting to **Block**, the firewall blocks all outbound traffic unless explicitly specified otherwise.
Inbound Action.	Select the default action the firewall takes on inbound connections. If you set this setting to **Block**, the firewall blocks all inbound traffic unless explicitly specified otherwise.
Unicast Responses to Multicast or Broadcast Network Traffic	Set the behavior for the responses to multicast or broadcast network traffic. If you disable this option, the firewall blocks all responses to multicast or broadcast network traffic.
Notify User When Windows Firewall Blocks a New App	Set the notification behavior for the firewall. If you select **Enable**, the firewall may send notifications to the user when it blocks a new app. If you select **Disable**, the firewall does not send any notifications.
Stealth Mode	To set the device in stealth mode, select **Enable**. Stealth mode helps prevent bad actors from gaining information about network devices and services. When enabled, stealth mode blocks outgoing ICMP unreachable and TCP reset messages from ports without an app actively listening on that port.
Allow IPSec Network Traffic in Stealth Mode	Set how the firewall handles unsolicited traffic secured by IPSec. If you select **Enable**, the firewall allows unsolicited network traffic secure by IPSec. This setting only applies when you enable Stealth Mode.
Local Firewall Rules	Set how the firewall interacts with local firewall rules. If you select **Enable**, the firewall follows local rules. If you select Disable, the firewall ignores local rules and does not enforce them.
Local Connection Rules	Set how the firewall interacts with local security connection rules. If you select **Enable**, the firewall follows local rules. If you select Disable, the firewall ignores local rules and does not enforce them, regardless of the schema and connection security versions.

Setting	Description
Global Port Firewall Rules	Set how the firewall interacts with global port firewall rules. If you select **Enable**, the firewall follows the global port firewall rules. If you select **Disable**, the firewall ignores the rules and does not enforce them.
Authorized Application Rules	Set how the firewall interacts with local authorized application rules. If you select **Enable**, the firewall follows local rules. If you select Disable, the firewall ignores local rules and does not enforce them.

8. To configure you own firewall rules, select **Add Firewall Rule**. After adding a rule, configure the settings as needed. You can add as many rules as you need.

9. When finished, select **Save And Publish** to push the profile to devices.

Firewall (Legacy) Profile

The Firewall (Legacy) profile for Windows Desktop devices allows you to configure the Windows Firewall settings for devices. Consider using the new Firewall profile for Windows Desktop as the new profile uses new Windows features.

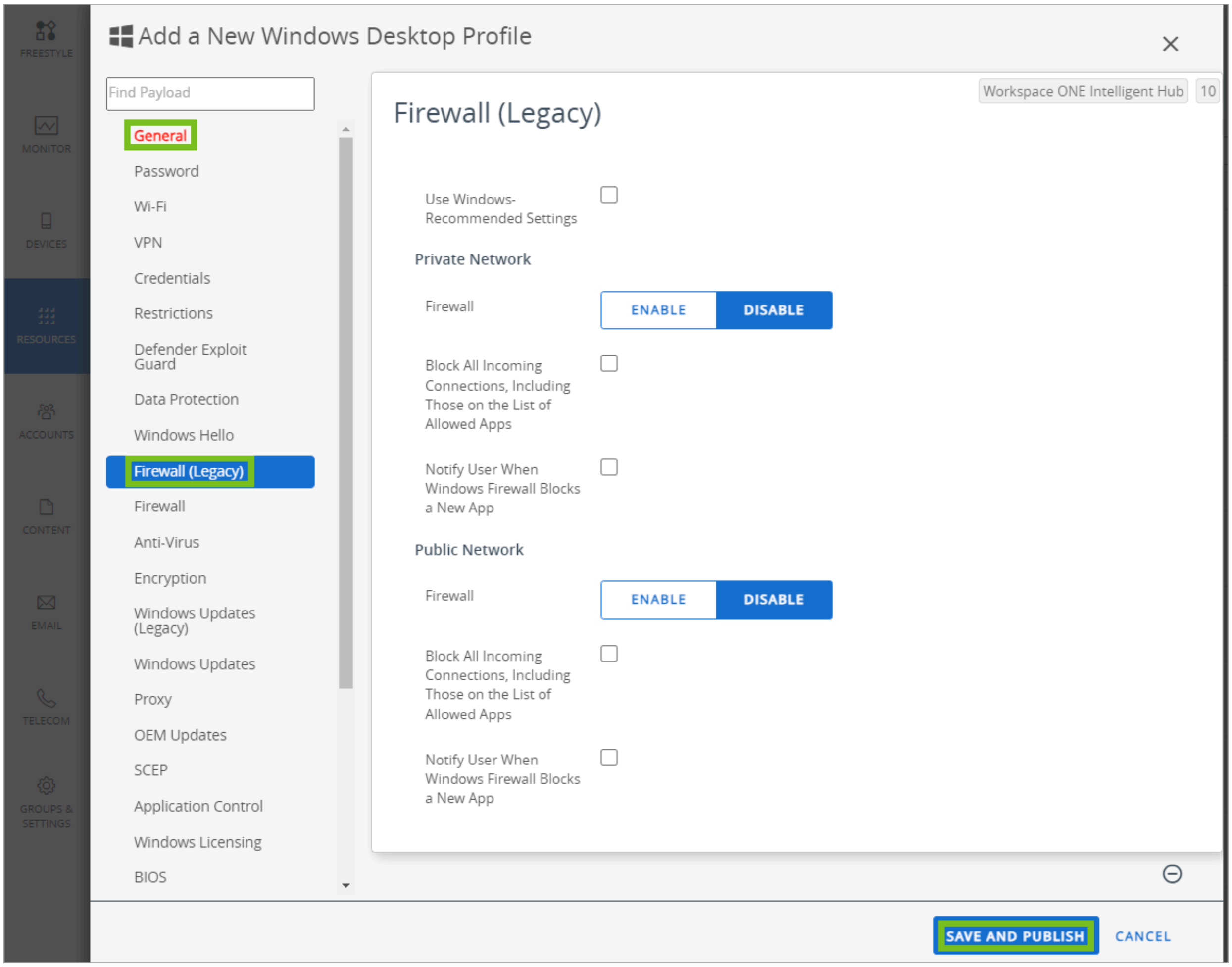
Important: The Firewall profile requires the Workspace ONE Intelligent Hub to be installed on the device.

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

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

3. Select **Device Profile**.

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



Firewall (Legacy)

Use Windows-Recommended Settings □

Private Network

Firewall ENABLE **DISABLE**

Block All Incoming Connections, Including Those on the List of Allowed Apps □

Notify User When Windows Firewall Blocks a New App □

Public Network

Firewall ENABLE **DISABLE**

Block All Incoming Connections, Including Those on the List of Allowed Apps □

Notify User When Windows Firewall Blocks a New App □

5. Select the **Firewall (Legacy)** payload.

6. Enable **Use Windows Recommended Settings** to use the Windows Recommended Settings and disable all other options available in this profile. The settings will automatically change to the recommended settings and you cannot change them.

7. Configure the **Private Network** settings:

Settings	Description
Firewall	Enable to use the firewall when the device is connected to private network connections.
Block All Incoming Connections, Including Those on the List of Allowed Apps	Enable to block all incoming connections. This setting allows outbound connections.
Notify User when Windows Firewall Blocks a New App	Enable to allow notifications to display when the Windows Firewall blocks a new app.

8. Configure the **Public Network** settings:

Settings	Description
Firewall	Enable to use the firewall when the device is connected to private network connections.

Settings	Description
Block All Incoming Connections, Including Those on the List of Allowed Apps	Enable to block all incoming connections. This setting allows outbound connections.
Notify User when Windows Firewall Blocks a New App	Enable to allow notifications to display when the Windows Firewall blocks a new app.

9. Select **Save and Publish** when you are finished to push the profile to devices.

Kiosk Profile

Configure a Kiosk profile to turn your Windows Desktop device into multi-app kiosk device. This profile allows you to configure the apps that display in the device start menu.

You can upload your own custom XML to configure the Kiosk profile or create your kiosk as part of the profile. This profile does not support domain accounts or domain groups. The user is a built-in user account created by Windows.

- Supported Apps
  - .EXE apps
    - MSI and ZIP files require you to add the file path.
  - Built-In apps
    - Select built-in apps are automatically added to the designer. These apps include:
    - News
    - Microsoft Edge
    - Weather
    - Alarms & Clock
    - Sticky Notes
    - Maps
    - Calculator and Photos.

Procedure

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

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

3. Select **Device Profile**.

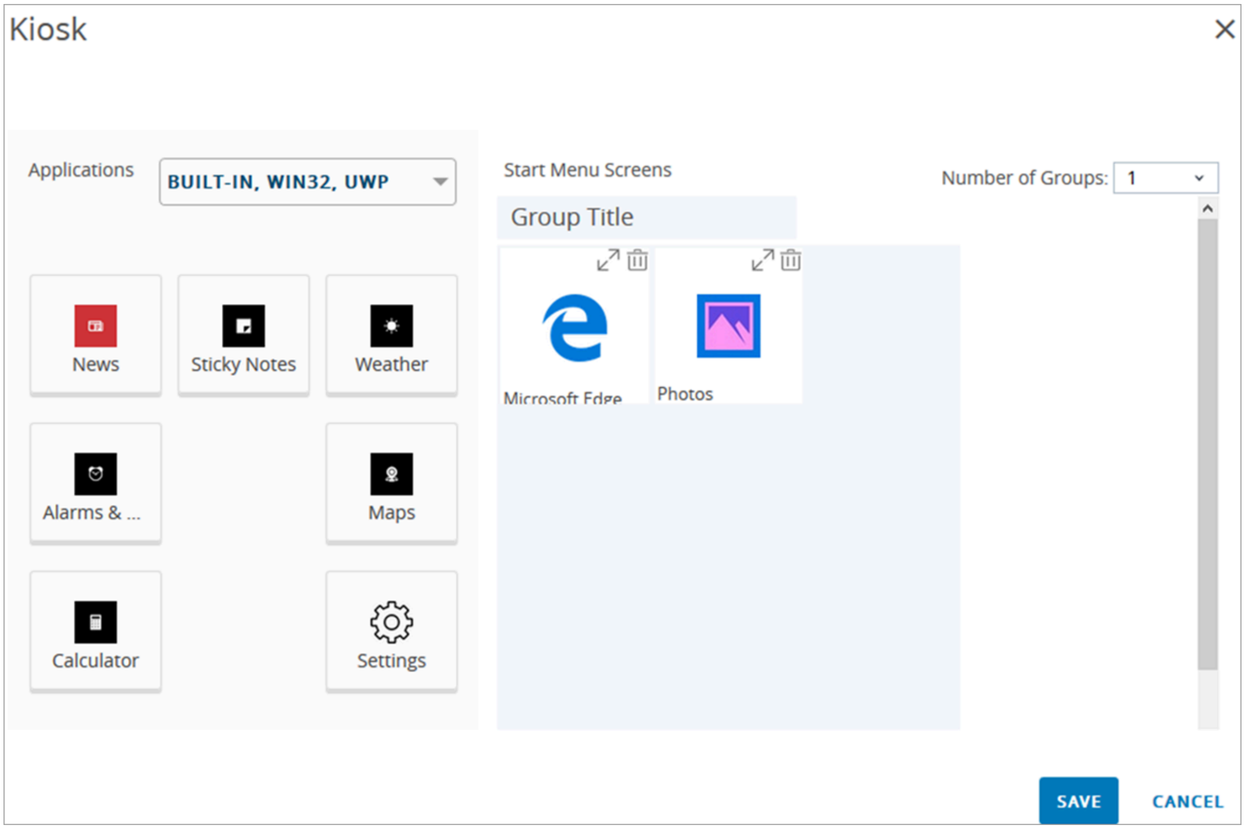
4. Configure the profile **General** settings. You must add an assignment before configuring the Kiosk profile.

5. Select the **Kiosk** profile.

6. If you have your custom XML already, select Upload Kiosk XML and complete the **Assign Access Configuration XML** settings. Select **Upload** and add your Assigned Access Configuration XML. You can also paste your XML into the text box. For more information, see https://docs.microsoft.com/en-us/windows/client-management/mdm/assignedaccess-csp.

7. If you do not have any custom XML, select **Create Your Kiosk** and configure the app layout.

   This layout is the device Start Menu in a grid. The apps that display on the left are the apps assigned to the assignment group you selected. Some apps have a gear icon with a red dot in the top-right corner. This icon displays for apps that require additional settings when added to the kiosk layout. After you configure the settings, the red dot disappears but the icon remains. You can select the arrow icon to change the size of the apps. For classic desktop apps, you can only select Small or Medium.



For applications that require additional support applications, the Kiosk profile supports adding these support applications using the Additional Settings option. For example, the Horizon client requires up to four support applications to run in Kiosk mode. Add these additional support applications when you configure the primary kiosk application by adding the additional **Application Executable Paths**.

8. Drag all the apps you want to add to the start menu to the center. You can create up to four groups for your apps. These groups combine your apps into sections on the start menu.
9. Once you have added all the apps and groups you want, select **Save**.
10. On the Kiosk profile screen, select **Save & Publish**.

Results

The profile does not install onto the device until all apps included in the profile are installed. After the device receives the profile, the device restarts and runs in Kiosk mode. If you remove the profile from the device, the device disables Kiosk mode, restarts, and removes the Kiosk user.

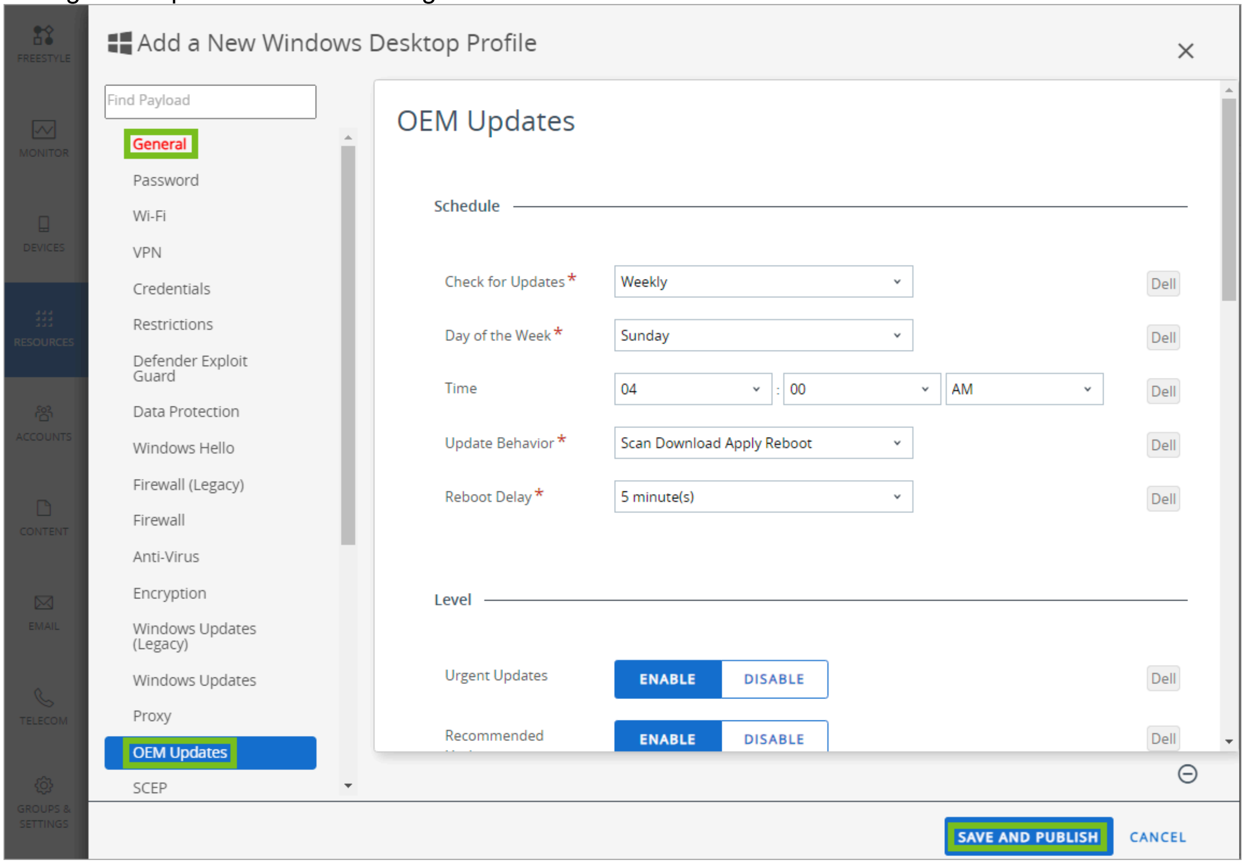
OEM Updates Profile

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

Support for the OEM Update profile settings varies by Dell Enterprise device. Workspace ONE UEM only pushes the settings a device supports. You can see all OEM updates deployed to your Windows Desktop devices on the **Device Updates** page, found at **Resources** > **Device Updates** > **OEM Updates tab**.

Note: The OEM Updates profile supports Dell Command | Update versions 3.x onward. The current version of Dell Command | Update is tested with each console release.

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



Add a New Windows Desktop Profile

OEM Updates

Schedule

Check for Updates * Weekly

Day of the Week * Sunday

Time 04 : 00 AM

Update Behavior * Scan Download Apply Reboot

Reboot Delay * 5 minute(s)

Level

Urgent Updates ENABLE DISABLE

Recommended ENABLE DISABLE

5. Select the **OEM Updates** payload and configure the following settings.
   - **Check for Updates** - Select the interval used to check for updates.
   - **Day of the Week** - Select the day of the week to check for updates. Only displays when **Check for Updates** is set to **Weekly**.
   - **Day of the Month** - Select the day of the month to check for updates. Only displays when **Check for Updates** is set to **Monthly**.
   - **Time** - Select the time of day to check for updates.
   - **Update Behavior** - Select the actions to take when checking for updates.
     - Select **Scan Notify** to scan for updates and notify the user that updates are available.
     - Select **Scan Download Notify** to scan for updates, download any available, and notify the user that updates are available for installation.
     - Select **Scan Notify Apply Reboot** to scan for updates, download any available, install the updates, and reboot the device.
   - **Reboot Delay** - Select the amount of time the device delays rebooting after downloading updates.
   - **Urgent Updates** - Select **Enable** to apply Urgent Updates to the device.
   - **Recommended Updates** - Select **Enable** to apply Recommended Updates to the device.
   - **Optional Updates** - Select **Enable** to apply Optional Updates to the device.
   - **Hardware Drivers** - Select **Enable** to apply hardware driver updates provided by the OEM to the device.
   - **Application Software** - Select **Enable** to apply application software updates provided by the OEM to the device.

- **BIOS Updates** - Select **Enable** to apply BIOS updates provided by the OEM to the device. If the BIOS passwords is managed by the BIOS profile, you will not need to disable the password.
- **Firmware Updates** - Select **Enable** to apply firmware updates provided by the OEM to the device.
- **Utility Software** - Select **Enable** to apply utility software updates provided by the OEM to the device.
- **Other** - Select **Enable** to apply other updates provided by the OEM to the device.
- **Audio** - Select **Enable** to apply audio device updates provided by the OEM to the device.
- **Chipset** - Select **Enable** to apply chipset device updates provided by the OEM to the device.
- **Input** - Select **Enable** to apply input device updates provided by the OEM to the device.
- **Network**- Select **Enable** to apply network device updates provided by the OEM to the device.
- **Storage** - Select **Enable** to apply storage device updates provided by the OEM to the device.
- **Video** - Select **Enable** to apply video device updates provided by the OEM to the device.
- **Others** - Select **Enable** to apply other device updates provided by the OEM to the device.

6. Select **Save & Publish**.

Password Profile

Use a Password profile to protect your Windows devices by requiring a password each time they return from an idle state. Learn how a Password profile with Workspace ONE UEM ensures that all your sensitive corporate information on managed devices remains protected.

Passwords set using this profile only take effect if the password is stricter than existing passwords. For example, if the existing Microsoft Account password requires stricter settings than the Password payload requirements, the device continues to use the Microsoft Account password.

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

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Password** profile.
6. Configure the Password settings:

Settings	Descriptions
Password Complexity	Set to Simple or Complex to your preferred level of password difficulty. Simple complexity is only supported if “Use Protection Agent for Windows Devices” is enabled.
Require Alphanumeric	Enable to require the password to be an alphanumeric password.
Minimum Password Length	Enter the minimum number of characters a Password must contain.
Maximum Password Age (days)	Enter the maximum number of days that may elapse before the end user is required to change the Password.
Minimum Password	Enter the minimum number of days that must elapse before the end user is required to change the Password.

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

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

Peer Distribution Profile

Workspace ONE Peer Distribution uses the native Windows BranchCache feature that is built into the Windows operating system. This feature provides a peer-to-peer technology alternative.

Configure peer distribution on your Windows devices with the **Peer Distribution Windows Desktop** Profile. Peer distribution supports **Distributed**, **Hosted** and **Local** BranchCache modes along with their configuration settings; disk space percentage and max cache age. You can also view the BranchCache Statistics of an application from the Peer Distribution Details panel under **Apps&Books** > **Native** > **List View** > **Application Details**.

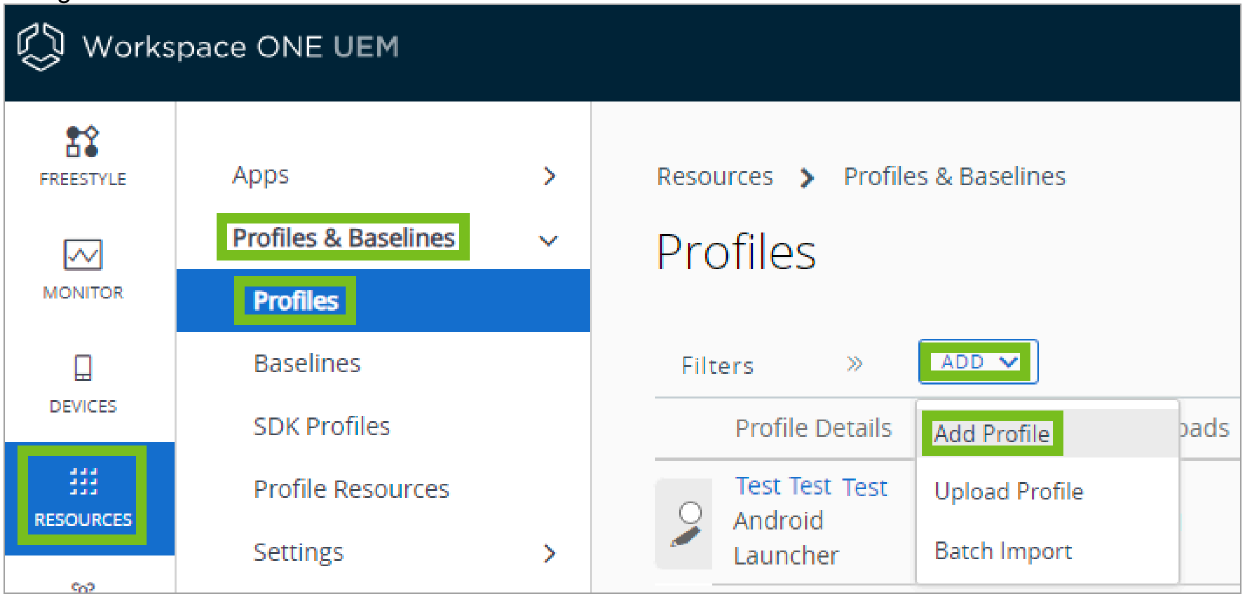
Peer distribution with Workspace ONE allows you to deploy your Windows apps to enterprise networks. This profile uses the native Windows BranchCache functionality built into the the Windows operating system.

Configuring a Peer Distribution Profile

Peer distribution with Workspace ONE allows you to deploy your Windows apps to enterprise networks. This profile uses the native Windows BranchCache functionality built into the Windows operating system.

Before you can use the Peer Distribution profile for peer-to-peer distribution, you must meet the peer distribution with Workspace ONE requirements.

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



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

3. Select **Device Profile**.

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

5. Select the **Peer Distribution** profile and select **Configure**.

   You must have File Storage configured before you can create a Peer Distribution profile.

6. Select the **Workspace ONE Peer Distribution Mode** you want to use.

Setting	Description
Distributed	Select this option to have your devices download apps from peers in a local subnet.
Hosted	Select this option to have your devices to download apps from a hosted cache server.
Local	Select this option to have your devices to download apps from local device caching only.
Disabled	Select this option to disable peer distribution.

7. Configure the **Cache** settings:

Setting	Description
Maximum Cache Age (days)	Enter the maximum number of days that peer distribution items should remain in the cache before the device purges the items.
Percentage of Disk Space Used for BranchCache	Enter the amount of local disk space the device should allow peer distribution to use.

8. If you set the distribution mode to Hosted, configure the **Hosted Cache Servers** settings. You must add at least one hosted cache server for devices to download and upload content to and from.

9. Select **Save & Publish**.

Personalization Profile

Configure a Personalization profile for Windows Desktop devices to configure the Windows Personalization settings. These settings include the desktop background and the start menu settings.

The options in this profile are all optional. Consider only configuring the settings you need to meet your Personalization requirements.

This profile does not create a multi-app kiosk device like the Kiosk profile.

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Personalization** profile.
6. Configure the **Images** settings:

Settings	Descriptions
Desktop Image	Select **Upload** to add an image to use as the desktop background.
Lock Screen Image	Select **Upload** to add an image to use as the lock screen background.

7. **Upload** a start layout XML. This XML file overrides the default start menu layout and prevents users from changing the layout. You can configure the layout of tiles, the number of groups, and the apps in each group. You must create this XML yourself. For more information on creating a start layout XML, see https://docs.microsoft.com/en-us/windows/configuration/customize-and-export-start-layout.
8. Configure the **Start Menu Policies** settings. These settings allow you to control which shortcuts are allowed in the start menu. You can also choose to **Hide** or **Show** certain options such as the **Shut Down** option or the **App List**.
9. Select **Save & Publish**.

Proxy Profile

Create a Proxy profile to configure a proxy server for your Windows Desktop devices. These settings do not apply to VPN connections.

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Proxy** profile and configure the settings:

Settings	Description
Automatically	Enable to have the system automatically try to find the path to a proxy auto-

Settings	Description
Detect Settings	config (PAC) script.
Use Setup Script	Enable to enter the file path to the PAC script.
Script Address	Enter the file path to the PAC script. This option displays when **Use Setup Script** is enabled.
Use Proxy Server	Enable to use a static proxy server for Ethernet and Wi-Fi connections. This proxy server is used for all protocols. These settings do not apply to VPN connections.
Address to Proxy Server	Enter the proxy server address. The address must follow the format: `<server>[“:”<port>].`
Exceptions	Enter any addresses that should not use the proxy server. The system will not user the proxy server for these addresses. Separate entries with a semicolon (;).
User Proxy for Local (Intranet) Addresses	Enable to use the proxy server for local (intranet) addresses.

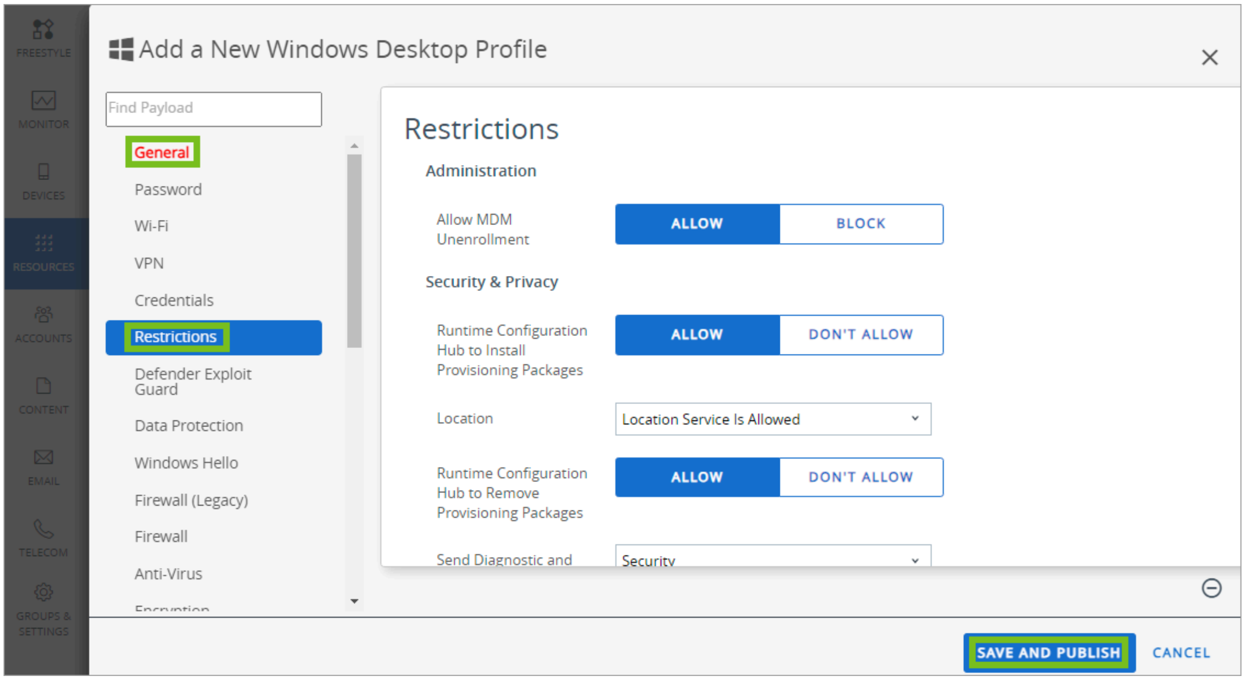
6. Select **Save And Publish**.

Restrictions Profile

Use the Restrictions profile to disable end-user access to device features to ensure that your Windows devices are not tampered with. Learn how to control what settings and options end users can use or change with the Workspace ONE UEM restrictions profile.

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

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



Add a New Windows Desktop Profile

Restrictions

Administration

Allow MDM Unenrollment: ALLOW | BLOCK

Security & Privacy

Runtime Configuration Hub to Install Provisioning Packages: ALLOW | DON'T ALLOW

Location: Location Service Is Allowed

Runtime Configuration Hub to Remove Provisioning Packages: ALLOW | DON'T ALLOW

Send Diagnostic and: Security

5. Select the **Restrictions** profile.

6. Configure the **Administration** settings:

Settings	Description
Allow Manual MDM Unenrollment	Allow the end user to unenroll from Workspace ONE UEM manually through the Workplace/Work Access enrollment. This restriction is not supported for Windows Home edition devices.
Runtime Configuration Hub to Install Provisioning Packages	Enable to allow the use of provisioning packages to enroll devices into Workspace ONE UEM (bulk provisioning). This restriction is not supported for Windows Home edition devices.
Location	Select how location services run on the device. This restriction is not supported for Windows Home edition devices.
Runtime Configuration Agent to Remove Provisioning Packages	Enable to allow the removal of provisioning packages. This restriction is not supported for Windows Home edition devices.
Send Diagnostic and Usage Telemetry Data	Select the level of telemetry data to send to Microsoft . This restriction is not supported for Windows Home edition devices.
Require Microsoft Account for MDM	Enable to require a Microsoft Account for devices to receive policies or applications.
Require of Microsoft Account for Modern Applications	Enable to require a Microsoft Account for devices to download and install Windows Apps.
Provisioning Packages Must Have a Certificate Signed by a Device Trusted Authority	Enable to require a trusted certificate for all provisioning packages (bulk provisioning). This restriction is not supported for Windows Home edition devices.
Allow User to Change Auto Play Settings	Allow the user to change what program is used for Auto Play of file types. This restriction is not supported for Windows Home edition devices.

Settings	Description
Allow User to Change Data Sense Settings	Allow the user to change the Data Sense settings to restrict data use on the device. This restriction is not supported for Windows Home edition devices.
Date/Time	Allow the user to change the Date/Time settings. This restriction is not supported for Windows Home edition devices.
Language	Allow the user to change the language settings. This restriction is not supported for Windows Home edition devices.
Allow User to Change Power and Sleep Settings	Allow the user to change the Power and Sleep settings. This restriction is not supported for Windows Home edition devices.
Region	Allow the user to change the region. This restriction is not supported for Windows Home edition devices.
Allow User to Change Sign-In Options	Allow the user to change the Sign-In Options. This restriction is not supported for Windows Home edition devices.
VPN	Allow the user to change the VPN settings. This restriction is not supported for Windows Home edition devices.
Allow User to Change Workplace Settings	Allow the user to change Workplace settings and change how MDM functions on the device. This restriction is not supported for Windows Home edition devices.
Allow the User to Change Account Settings	Allow the user to change Account settings. This restriction is not supported for Windows Home edition devices.
Bluetooth	Allow the use of Bluetooth on the device. This restriction is not supported for Windows Home edition devices.
Device Bluetooth Advertising	Allow the device to broadcast Bluetooth Advertisements. This restriction is not supported for Windows Home edition devices.
Bluetooth-enabled devices can discovery the device	Allow Bluetooth discovery of the device by other Bluetooth devices. This restriction is not supported for Windows Home edition devices.
Camera	Allow access the camera function of the device. This restriction is not supported for Windows Home edition devices.
Cortana	Allow access to the Cortana application. This restriction is not supported for Windows Home edition devices.
Device Discovery UX on the Lock Screen	Allow the device discovery UX on the lock screen to discover projectors and other displays. When enabled, the Win+P and Win+K shortcuts do not work. This restriction is not supported for Windows Home edition devices.
IME Logging	Enable to allow the user to turn on and off the logging for incorrect conversions and saving of auto-tuning result to a file and history-based predictive input. This restriction is not supported for Windows Home edition devices.
IME Network Access	Enable to allow the user to turn on the Open Extended Dictionary to integrate Internet searches to provide input suggestions that do not exist in a devices local dictionary. This restriction is not supported for Windows Home edition devices.
Smart Screen	Enable to allow the end user to use the Microsoft SmartScreen feature,

Settings	Description
	which is a form of security requesting the end user to draw shapes on an image to unlock the device. This option also allows end users to use PINs as their password. **Note**: After you disable the function, you cannot reenable it through Workspace ONE UEM MDM. To reenable it, you must factory reset the device. This restriction is not supported for Windows Home edition devices.
Search to Leverage Location Information	Allow the search to use the device location information. This restriction is not supported for Windows Home edition devices.
Storage Card	Enable to allow the use of an SD card and the device USB ports. This restriction is not supported for Windows Home edition devices.
Windows Sync Settings	Allow user to sync Windows settings across devices. This restriction is not supported for Windows Home edition devices.
Windows Tips	Allow Windows Tips on the device to help the user. This restriction is not supported for Windows Home edition devices.
User Account Control Setting	Select the level of notification sent to end users when a change to the operating system requires device admin permission.
Allow Non-Microsoft Store Trusted Applications	Allows the downloading and installation of applications not trusted by the Microsoft Store.
App Store Auto Updates	Enable to allow apps downloaded from the Microsoft Store to update automatically when new versions are available. This restriction is not supported for Windows Home edition devices.
Allow Developer Unlock	Allows the use of the Developer Unlock setting for sideloading applications onto devices. This restriction is not supported for Windows Home edition devices.
Allow DVR & Game Broadcasting	Enable to allow the recording and broadcasting of games on the device. This restriction is not supported for Windows Home edition devices.
Allow Share Data Among Multiple Users of the Same App	Allows sharing of data between multiple users of an app. This restriction is not supported for Windows Home edition devices.
Restrict App Data to System Volume	Restricts app data to the same volume as the OS instead of secondary volumes or removable media. This restriction is not supported for Windows Home edition devices.
Restrict Installation of Applications to System Drive	Restricts the installation of apps to the system drive instead of secondary drives or removable media. This restriction is not supported for Windows Home edition devices.
Auto Connect to Wi-Fi Hotspots	Enable to allow the device to connect to Wi-Fi hotspots automatically using the Wi-Fi Sense functionality. This restriction is not supported for Windows Home edition devices.
Cellular Data On Roaming	Enable to allow cellular data use while roaming. This restriction is not supported for Windows Home edition devices.
Internet Sharing	Enable to allow Internet sharing between devices. This restriction is not supported for Windows Home edition devices.

Settings	Description
Data Usage on Roaming	Enable to allow end users to transmit and receive data while roaming. This restriction applies to all Windows devices.
VPN Over Cellular	Allow the use of a VPN over cellular data connections. This restriction is not supported for Windows Home edition devices.
VPN Roaming Over Cellular	Allow the use of a VPN while on roaming cellular data connections. This restriction is not supported for Windows Home edition devices.
Auto fill	Allow the use of Auto fill to complete user information. This restriction is not supported for Windows Home edition devices.
Cookies	Allow the use of cookies. This restriction is not supported for Windows Home edition devices.
Do Not Track	Allow the use of Do Not Track requests. This restriction is not supported for Windows Home edition devices.
Password Manager	Allow the use of a password manager. This restriction is not supported for Windows Home edition devices.
Pop-ups	Allow pop-up browser windows. This restriction is not supported for Windows Home edition devices.
Search Suggestions in Address Bar	Allow search suggestions to appear in address bar. This restriction is not supported for Windows Home edition devices.
Smart Screen	Allow the use of the SmartScreen malicious site and content filter. This restriction is not supported for Windows Home edition devices.
Send Intranet Traffic to Internet Explorer	Allow intranet traffic to use Internet Explorer. This restriction applies to all Windows devices.
Enterprise Site List URL	Enter the URL for an enterprise site list. This restriction applies to all Windows devices.

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

SCEP Profile

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

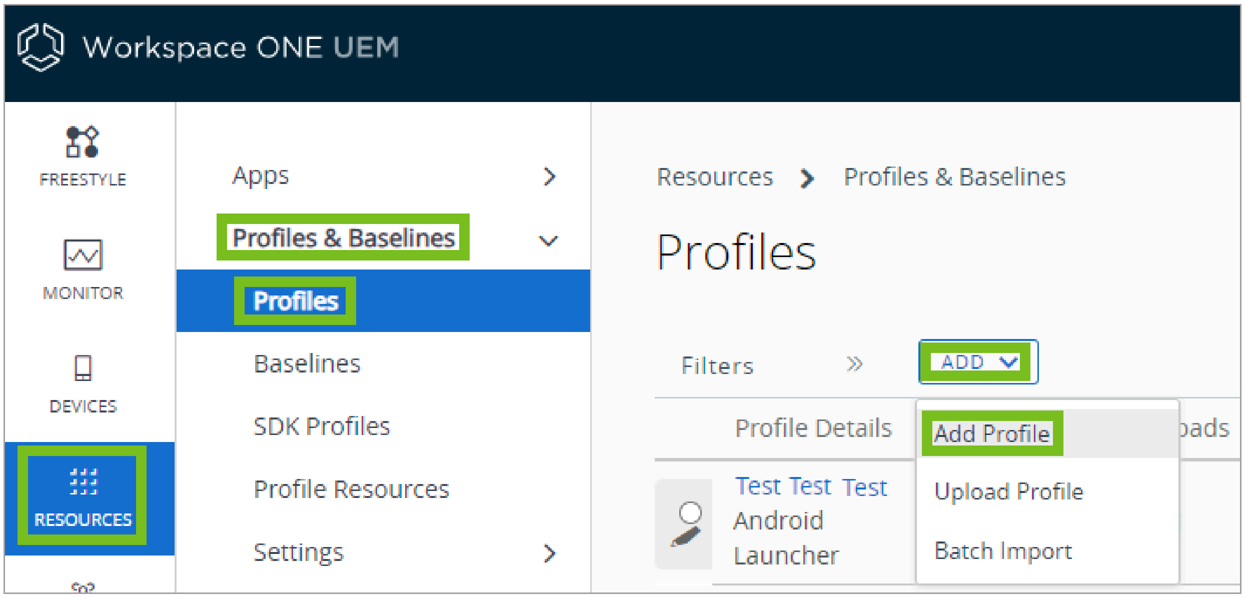
Even with strong passwords and other restrictions, your infrastructure remains vulnerable to brute force, dictionary attacks, and employee error. For greater security, you can implement digital certificates to protect corporate assets. To use SCEP to install these certificates to devices silently, you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

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

Configuring a SCEP Profile

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

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



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

3. Select **User Profile** or **Device Profile**.

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

5. Select the **SCEP** profile.

6. Configure the SCEP settings, including:

Settings	**Descriptions**
Credential Source	This drop-down menu is always set to defined certificate authority.
Certificate Authority	Select the certificate authority you want to use.
Certificate Template	Select the template available for the certificate.
Key Location	Select the location for the certificate private key: **TPM If Present** – Select to store the private key on a Trusted Platform Module if one is present on the device, otherwise store it in the OS. **TPM Required** – Select to store the private key on a Trusted Platform Module. If a TPM is not present, the certificate does not install and an error displays on the device. **Software** – Select to store the private key in the device OS. **Passport** – Select to save the private key within the Microsoft Passport. This option requires the Azure AD integration.
Container Name	Specify the Passport for Work (now called 'Windows Hello for Business') container name. This setting displays when you set **Key Location** to **Passport**.

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

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

Single App Mode Profile

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

Single App Mode has some restrictions and limitations.

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

Procedure

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**
3. Select **User Profile**.
4. Configure the profile **General** settings.
5. Select the **Single App Mode** Profile.
6. Configure the **Single App Mode** settings for **Application Name** and enter the application friendly name. For Windows apps, the friendly name is the Package Name or Package ID.bRun a PowerShell command to get the friendly name of the app installed on the device. The command “Get-AppxPackage” returns the application friendly name as “name.”
7. After configuring a Single App Mode profile, you must set up Single App Mode on the device.
    - After receiving the Single App Mode profile on the device, reboot the device to begin.
    - Once the device restarts, you are prompted to sign into the device with the Standard User account.

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

VPN Profile

Workspace ONE UEM supports configuring device VPN settings so your end users can remotely and securely access your organizations internal network. Learn how the VPN profile provides detailed VPN settings control including specific VPN provider settings and Per-App VPN access.

Important: Before enabling **VPN Lockdown**, verify that the VPN configuration for the VPN profile works. If the VPN configuration is incorrect, there is a chance you cannot delete the VPN profile off the device because there is no Internet connection.

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

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

3. Select **User Profile** or **Device Profile**.

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

5. Select the **VPN** profile.

6. Configure the **Connection Info** settings.

    - **Connection Name** - Enter the name of the VPN connection.
    - **Connection Type** - Select the type of VPN connection:
    - **Server** - Enter the VPN server hostname or IP Address.
    - **Port** - Enter the port the VPN server uses.

- **Advanced Connection Settings** - Enable to configure advanced routing rules for device VPN connection.
- **Routing Addresses** - Select **Add** to enter the IP Addresses and Subnet Prefix Size of the VPN server. You can add more routing addresses as needed.
- **DNS Routing Rules** - Select Add to enter the **Domain Name** that governs when to use the VPN. Enter the **DNS Servers** and **Web Proxy Servers** to use for each specific domain.
- **Routing Policy** - Choose either to **Force All Traffic Through VPN** or **Allow Direct Access to External Resources**.
    - **Force All Traffic Through VPN** (Force Tunnel): For this traffic rule, all IP traffic must go through the VPN Interface only.
    - **Allow Direct Access to External Resources** (Split Tunnel): For this traffic filter rule, only the traffic meant for the VPN interface (as determined by the networking stack) goes over the interface. Internet traffic can continue to go over the other interfaces.
- **Proxy** - Select **Auto Detect** to detect any proxy servers used by the VPN. Select **Manual** to configure the proxy server.
- **Server** - Enter the IP Address for the proxy server. Displays when **Proxy** is set to **Manual**.
- **Proxy Server Config URL** - Enter the URL for the proxy server configuration settings. Displays when **Proxy** is set to **Manual**.
- **Bypass proxy for local** - Enable to bypass the proxy server when the device detects it is on the local network.
- **Protocol** - Select the authentication protocol for the VPN:
    - EAP – Allows for various authentication methods.
    - Machine Certificate – Detects a client certificate in the device certificate store to use for authentication.
- **EAP Type**|Select the type of EAP authentication:
    - EAP-TLS – Smart Card or client certificate authentication
    - EAP-MSCHAPv2 – User name and Password
    - EAP-TTLS
    - PEAP
    - Custom Configuration – Allows all EAP configurations. Displays only if **Protocol** is set to **EAP**.
- **Credential Type** - Select **Use Certificate** to use a client certificate. Select **Use Smart Card** to use a Smart Card to authenticate. Displays when **EAP Type** is set to **EAP-TLS**.
- **Simple Certificate Selection** - Enable to simplify the list of certificates from which the user selects. The certificates display by the most recent certificated issued for each entity. Displays when **EAP Type** is set to **EAP-TLS**.
- **Use Windows Log On Credentials** - Enable to use the same credentials as the Windows device. Displays when **EAP Type** is set to **EAP-MSCHAPv2**.
- **Identity Privacy** - Enter the value to send servers before the client authenticates the server identity. Displays when **EAP Type** is set to **EAP-TTLS**.
- **Inner Authentication Method** - Select the authentication method for inner identity authentication. Displays when **EAP Type** is set to **EAP-TTLS**.
- **Enable Fast Reconnect** - Enable to reduce the delay in time between an authentication request by a client and the response from the server. Displays when **EAP Type** is set to **PEAP**.
- **Enable Identity Privacy** - Enable to protect the user identity until the client authenticates with the server.
- **Per-app VPN Rules** - Select **Add** to add traffic rules for specific Legacy and Modern applications.
- **Application ID** - First select whether the app is a Store App or a Desktop App. Then, enter the application file path for Desktop apps. You can also enter the package family name for Store Apps to specify the app the traffic rules apply to.
    - File Path example: %ProgramFiles%/ Internet Explorer/iexplore.exe
    - Package Family Name example: AirWatchLLC.AirWatchMDMAgent_htcwkw4rx2gx4 The PFN Lookup allows you to search for the application PFN by selecting the **Search** icon. A display window opens allowing you to select the app you want to configure Per-app VPN rules to govern. The PFN is then auto populated.
- **VPN On Demand** - Enable to have the VPN connection automatically connect when the application is launched.
- **Routing Policy** - Select the routing policy for the app.

  - **Allow Direct Access to External Resources** allows for both VPN traffic and traffic through the local network connection.
  - **Force All Traffic Through VPN** forces all traffic through the VPN.
- **DNS Routing Rules** - Enable to add DNS routing rules for the app traffic. Select **Add** to add **Filter Types** and **Filter Values** for the routing rules. Only traffic from the specified app that matches these rules can be sent through the VPN.
  - **IP Address**: A list of comma-separated values specifying remote IP address ranges to allow.
  - **Ports**: A list of comma-separated values specifying remote port ranges to allow. For example, 100–120, 200, 300–320. Ports are only valid when the protocol is set to TCP or UDP.
  - **IP Protocol**: Numeric value 0–255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17.
- **Device Wide VPN Rules** - Select **Add** to add traffic rules for the entire device. Select **Add** to add **Filter Types**and **Filter Values** for the routing rules. Only traffic that matches these rules can be sent through the VPN.
  - **IP Address**: A list of comma-separated values specifying remote IP address ranges to allow.
  - **Ports**: A list of comma-separated values specifying remote port ranges to allow. For example, 100–120, 200, 300–320. Ports are only valid when the protocol is set to TCP or UDP.
  - **IP Protocol**: Numeric value from 0–255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17. For a list of the numeric value of all protocols, see https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.
- **Remember Credentials** - Enable to remember the end user login credentials.
- **Always On** - Enable to force the VPN connection to be always on.
- **VPN Lockdown** - Enable to force the VPN to be on always, never disconnect, disable any network access if the VPN is not connected, and prevent other VPN profiles from connecting on the device. A VPN profile with VPN Lockdown enabled must be deleted before you push a new VPN profile to the device. This feature only displays if the profile is set to Device context.
- **Bypass for Local** - Enable to bypass the VPN connection for local intranet traffic.
- **Trusted Network Detection** - Enter, separated by commas, trusted network addresses. The VPN does not connect when a trusted network connection is detected.
- **Domain** - Select **Add New Domain** to add domains to resolve through the Tunnel server. Any domains added resolve though the Tunnel server regardless of the app originating the traffic. For example, omnissa.com resolves through the Tunnel server if you use the trusted Chrome app or the untrusted Edge apps. This option only displays when you create the VPN profile as a user profile.

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

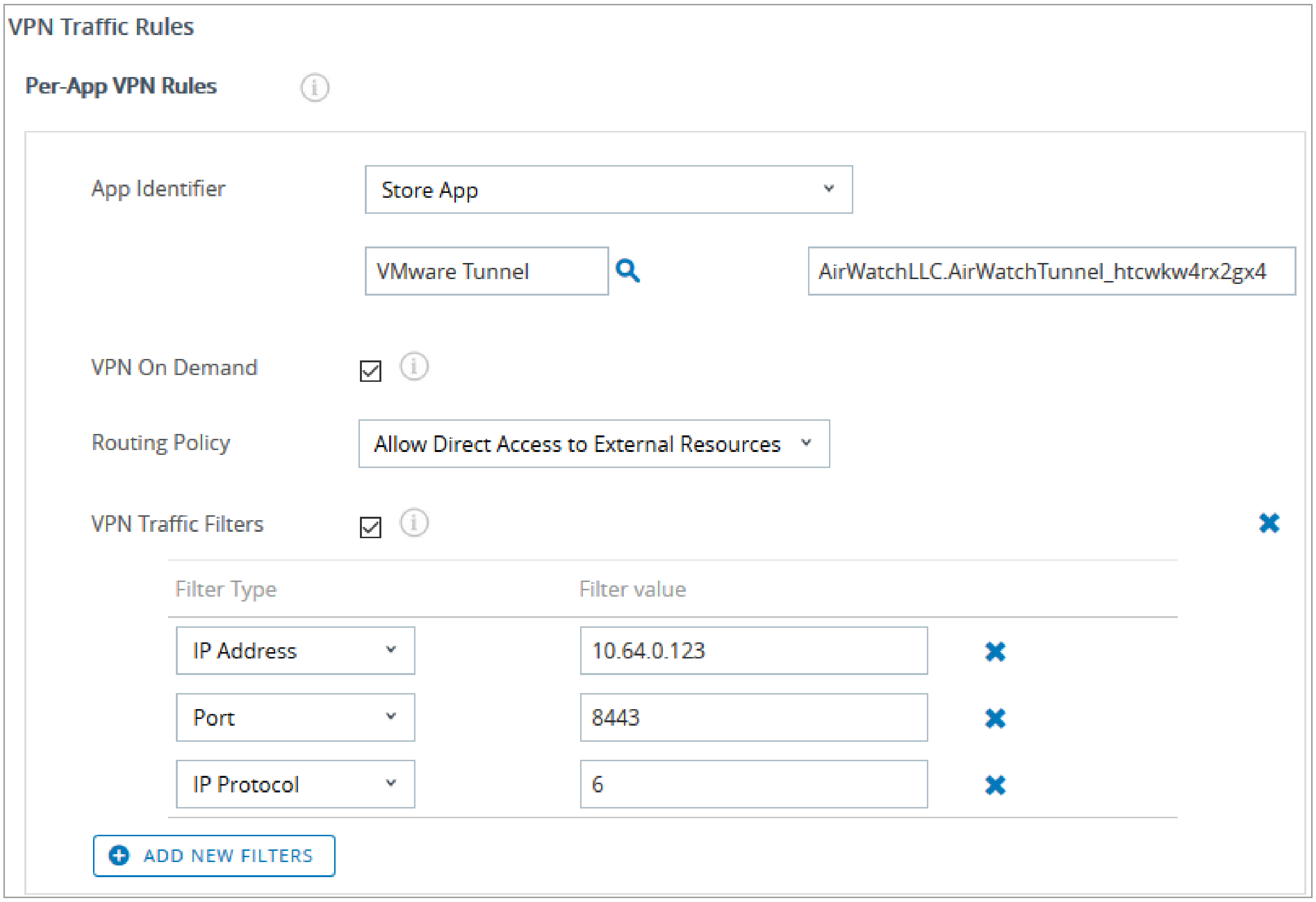
Workspace ONE UEM VPN profiles support configuring Per-App VPN settings for Windows devices. Learn how to configure your VPN profile to use the specific traffic rules and logic to enable Per-App VPN access.

Per-App VPN for Windows Using the VPN Profile

Workspace ONE UEM VPN profiles support configuring Per-App VPN settings for Windows devices. Learn how to configure your VPN profile to use the specific traffic rules and logic to enable Per-App VPN access.

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

Each rule group under the Per-App VPN Rules section uses the logical OR operator. So if the traffic matches any of the configured policies, it is allowed through the VPN.



VPN Traffic Rules

Per-App VPN Rules

App Identifier: Store App

VMware Tunnel — AirWatchLLC.AirWatchTunnel_htcwkw4rx2gx4

VPN On Demand ☑

Routing Policy: Allow Direct Access to External Resources

VPN Traffic Filters ☑

Filter Type	Filter value
IP Address	10.64.0.123
Port	8443
IP Protocol	6

The applications for which Per-app VPN traffic rules apply can be legacy Windows applications such as EXE files or modern apps downloaded from the Microsoft Store. By setting specific applications to start and use the VPN connection, only the traffic from those apps uses the VPN and not all device traffic. This logic allows you to keep corporate data secure while reducing the bandwidth sent through your VPN.

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

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

Web Clips Profile

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

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **User Profile**.
4. Configure the profile **General** settings.
5. Select the **Web Clips** profile.
6. Configure the **Web Clips** settings, including:

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

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

Wi-Fi Profile

Create a Wi-Fi profile through Workspace ONE UEM to connect your devices to hidden, encrypted, or password-protected corporate networks. Learn how Wi-Fi profiles are useful for end users who need access to multiple networks or for configuring devices to connect automatically to the appropriate wireless network.

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

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

3. Select **Device Profile**.

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

5. Select the **Wi-Fi** profile and configure the settings.

Settings	Descriptions
Service Set Identifier	Enter an identifier for the name (SSID) of the desired Wi-Fi network. The network SSID cannot contain spaces.
Hidden Network	Enable this option if the network uses a hidden SSID.
Auto-Join	Enable this option to set the device to join the network automatically.
Security Type	Use the drop-down menu to select the security type (for example, WPA2 Personal) for the Wi-Fi network.
Encryption	Use the drop-down menu to select the encryption type used. Displays based on the **Security Type**.
Password	Enter the password required to join the Wi-Fi network for networks with static passwords. Select the Show Characters check box to disable hidden characters within the text box. Displays based on the **Security Type**.
Proxy	Enable this option to configure proxy settings for the Wi-Fi connection.
URL	Enter the URL for the proxy.
Port	Enter the port for the proxy.
Protocols	Select the type of protocols to use: **Certificate**: PEAP-MsChapv2 **EAP-TTLS**: Custom

Settings	Descriptions
	This section displays when the **Security Type** is set to WPA Enterprise or WPA2 Enterprise.
Inner Identity	Select the method of authentication through EAP-TTLS: Username/Password Certificate This section displays when the **Protocols** option is set to EAP-TTLS or PEAP-MsChapv2.
Require Crypto Binding	Enable this option to require cryptographic binding on both authentications. This menu item limits man-in-the-middle attacks.
Use Windows Log On Credentials	Enable this option to use the Windows login credentials are the user name/ password to authenticate. Displays when **Username/Password** is set as the **Inner Identity**.
Identity Certificate	Select an Identity Certificate, which you can configure using the Credentials payload. Displays when **Certificate** is set as the **Inner Identity**.
Trusted Certificates	Select **Add** to add Trusted Certificates to the Wi-Fi profile. This section displays when the **Security Type** is set to WPA Enterprise or WPA2 Enterprise.
Allow Trust Exceptions	Enable to allow trust decisions to be made by the user through a dialog box.

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

Windows Hello Profile

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

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

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

Important: Windows Hello for Business requires Azure AD integration to work.

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

Creating a Windows Hello Profile

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

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

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.
3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Windows Hello** profile and configure the settings:

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

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

Windows Licensing Profile

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

Important:

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

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

Procedure

1. Navigate to **Resources** > **Profiles & Baselines** > **Profiles** > **Add** and select **Add Profile**.
2. Select **Windows** and then select **Windows Desktop**.

3. Select **Device Profile**.
4. Configure the profile **General** settings.
5. Select the **Windows Licensing** profile and configure the following settings:

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

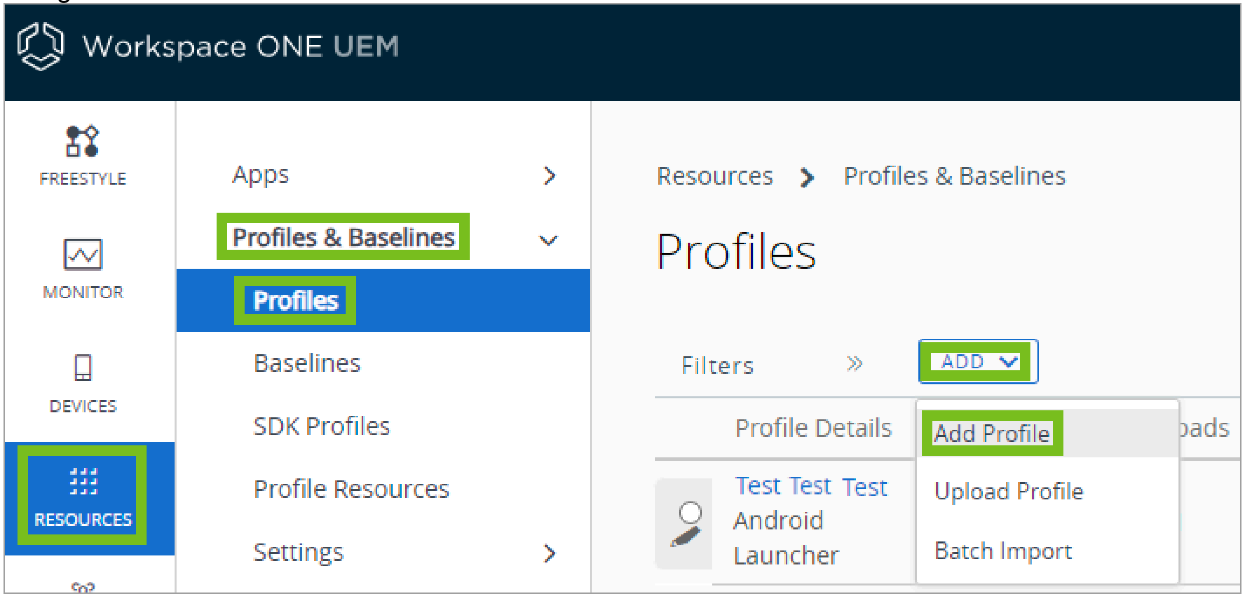
6. Select **Save & Publish** to push the profile to devices.

Windows Updates Profile

Create a Windows Updates profile to manage the Windows Updates settings for Windows Desktop devices using Windows 10, 2004 and above. This profile has more enhancements and additional functionality than the Windows Update (Legacy) profile. Using the updated version will ensure that all your devices are up-to-date and will be able to take advantage of the new features added to the console as well as improving device and network security.

To create or configure a Windows Updates profile, use the Windows Device Manager.

1. Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **Add** > and select **Add Profile**.



2. Choose **Windows** > **Windows Desktop** > **Device Profile**.
3. From the **Device Profile**, select **Windows Updates** and then click the button to **Configure** it.
4. Once configured, you can customize the settings as needed. This table provides more information regarding what each setting is meant to do.

Setting	**Description**
Definition	
Windows	Select the source for Windows Updates.

Setting	Description
Update Source	**Microsoft Update Service** – Select to use the default Microsoft Update Server. **Corporate WSUS** – Select to use a corporate server and enter the WSUS Server URL and WSUS Group. The device must contact the WSUS at least once for this setting to take effect. Selecting Corporate WSUS as a source allows your IT Admin to view updates installed and device status of devices in the WSUS Group. NOTE: The source cannot be changed after it is set.
Update Branch	Select the update branch to follow for updates. **Windows Insider - Dev Channel** – Insider Preview builds in this channel are released approximately once a week and contain the very latest features. This makes them the ideal for feature exploration.) **Windows Insider- Beta Channel** – Insider Preview builds in this channel are released approximately once a month and are more stable than Fast Ring releases, making them better suited for validation purposes. **Windows Insider - Release Preview Channel** – Insider Preview builds in this channel are the nearly finished GA releases to validate the upcoming GA version. **General Availability Channel (Targeted)** – There is no insider preview, and the feature updates are released annually.
Manage Preview Builds	Select the access to preview builds. If you want to run a device in Insider Preview, make sure this option is set to “Enable Preview Builds”: **Disable Preview Builds** **Disable Preview Builds Once the Next Release is Public** **Enable Preview builds**
Device Scheduling	
Enable Device Scheduling	When enabled you can define how the devices handle the scheduling of update installation and automatic (forced) reboot. When enabled you will see more options to configure the Automatic updated behavior, set the Active Hours, and configure the number of days the users will have before the updates are automatically pushed to their devices.
Update Behavior	
Enable Update Behavior	When enabled you can define the types of updates offered and when eligible devices will receive them. When enabled you will see more options to Disable Dual Scan, Allow Microsoft Application Updates, set how long to defer a feature update, and to exclude Windows Drivers and/or disable Safe Guard.
Device Behavior	
Enable Device Behavior	When enabled you can define how Update Behavior configurations are handled by the device. When enabled you will see more options to allow auto Windows update to download over metered networks, ignore cellular data download limits for ap updates, and ignore cellular data download limits for system updates.
Delivery Optimization	

Setting	Description
Enable Delivery Optimization	When enabled you can define how to reduce bandwidth consumption. When enabled you will see more options to select the Download Mode, Cache Host Source, the Group ID Source, the HTTP Source, the Cache Server Source, the Network, Device Requirements, and the Network Bandwidth limitation.
OS Version	
OS Version	When enabled you can specify which Target Release and Target Product version should move or say until the end of service.

5. When you have finished customizing the profile, remember to select **Save & Publish** to push the profile to your devices.

Troubleshooting Feature & Quality Updates

Because Windows Updates can cause issues in combination with specific drivers or applications, three buttons were added to help troubleshoot these situations. The **Pause** button will allow you to pause both feature and quality updates before they go out (but only for 35 days). The **Rollback** button will allow updates that were made but caused unforeseen issues to be temporarily returned to the previous version while you resolve the issue. The **Resume** button will enable Windows Update search and installation again.

Windows Updates (Legacy) Profile

The Windows Updates (Legacy) profile is for Windows Desktop devices using Windows 10, 1909 or previous. Consider migrating or using the new Windows Update profile to be able to take advantage of new features and enhancements made after 2004. The profile ensures that all your devices are up-to-date, which improves device and network security.

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

To create or configure a Windows Updates Legacy profile, use the Windows Device Manager.

1. Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **Add** > and select **Add Profile**.

2. Choose **Windows** > **Windows Desktop** > **Device Profile**.

3. Inside **Device Profile**, you will see a menu of items you can customize. Select **Windows Updates (Legacy)** and then click the button to **Configure** the settings.

Note: You may notice an alert that informs you of the ability to migrate existing profiles to the new version. You can use the **Migrate** button to migrate your settings to the new Windows Updates profile if you so choose. Be aware that if you do migrate the profiles, some of the settings have been enhanced and updated causing some of the older options to no longer be valid. Those changes won't be migrated from the previous versions.

4. Once configured, you can customize the settings for a Legacy profile (again this is for Windows 10, 2004 or before). This table provides more information regarding what each setting is meant to do.

Settings	Descriptions
Branching and Deferrals	
Windows Update Source	Select the source for Windows Updates.

Settings	Descriptions
	Microsoft Update Service – Select to use the default Microsoft Update Server. **Corporate WSUS** – Select to use a corporate server and enter the WSUS Server URL and WSUS Group. The device must contact the WSUS at least once for this setting to take effect. Selecting Corporate WSUS as a source allows your IT Admin to view updates installed and device status of devices in the WSUS Group.
Update Branch	Select the update branch to follow for updates. Semi-Annual Channel Windows Insider Branch - Fast (Less Stable, Dev build) Windows Insider Branch - Slow (More Stable, Dev build) Insider - Release (More Stable, Public build)
Insider Builds	Allow the download of Windows Insider builds of Windows. NOT Allowed - This was added to Windows 10 Version 1709 and specifies whether to allow access to Windows 10 Insider Preview builds.
Defer Feature Updates Period in Days	Select the number of days to delay feature updates before installing the updates on the device. The maximum number of days you can defer an update changed in Windows version 1703. Devices running a version before 1703 can only defer for 180 days. Devices running a version later than 1703 can defer up to 365 days. If you defer an update for longer than 180 days and push the profile to a device running Windows before the 1703 update, the profile fails to install on the device.
Pause Feature Updates	Enable to pause all feature updates for 60 days or until disabled. This setting overrides the **Defer Feature Updates Period in Days** setting. Use this option to delay an update that causes issues that can normally install following your deferral settings.
Defer Quality Updates Period in Days	Select the number of days to delay quality updates before installing the updates on the device.
Pause Quality Updates	Enable to pause all quality updates for 60 days or until disabled. This setting overrides the **Defer Quality Updates Period in Days** setting. Use this option to delay an update that causes issues that can normally install following your deferral settings.
Enable Settings for Previous Windows versions	Select to enable deferral settings for previous versions of Windows. This setting enables the deferral features for older versions of Windows 10 like 1511 and below. They were modified in the 1607 anniversary update to the current settings.
Update Installation Behavior	
Automatic Updates	Set how updates from the selected **Update Branch** are handled: Install updates automatically (recommended). Install Updates automatically but let the user schedule the computer restart.

Settings	Descriptions
	Install updates automatically and restart at specified time. Install updates automatically and prevent user from modifying the control panel settings. Check for updates but let the user choose whether to download and install them. Never check for updates (Not recommended).
Active Hours Maximum (Hours)	Enter the maximum number of active hours that prevent the system from rebooting due to updates.
Active Hours Start Time	Enter the start time for active hours. Set the active hours to prevent the system from rebooting during these hours.
Active Hours End Time	Displays the end time for active hours This time is determined by the **Active Hours Start Time** and the **Active Hours Maximum**.
Quality Updates Auto Restart Deadlines	Set the maximum number of days that can pass after installing a Quality or Feature Update before a system reboot is mandatory.
Feature Updates Auto Restart Deadlines	Set the maximum number of days that can pass after installing a Feature Update before a system reboot is mandatory.
Auto-Restart Notification (Minutes)	Select the number of minutes to display a warning before an auto-restart.
Auto-Restart Required Notification	Set how an auto-restart notification must be dismissed. **Auto Dismissal** - Automatically dismissed **User Dismissal** - Requires the user to close the notification.
Quality Updates Engaged Restart Deadline	Engaged Restarts allow to manage when the device reboots after installing a Quality or Feature update during Active Hours. Use this option to set the number of days a user can engage a reboot before a reboot is automatically scheduled outside of active hours.
Feature Updates Engaged Restart Deadline	Engaged Restarts allow to manage when the device reboots after installing a Feature update during Active Hours. Use this option to set the number of days a user can engage a reboot before a reboot is automatically scheduled outside of active hours.
Quality Updates Engaged Restart Snooze Schedule	Enter the number of days a user can snooze an Engaged Restart. After the snooze period passes, a reboot time is scheduled outside active hours.
Feature Updates Engaged Restart Snooze Schedule	Enter the number of days a user can snooze an Engaged Restart. After the snooze period passes, a reboot time is scheduled outside active hours.
Scheduled Auto-Restart Warning (Hours)	Select the number of hours before a scheduled auto-restart to warn users.
Scheduled Auto-Restart Warning (Minutes)	Select the number of minutes before a scheduled auto-restart to warn users.

Settings	Descriptions
Scheduled Imminent Auto-Restart Warning (Minutes)	Select the number of minutes before a scheduled imminent auto-restart to warn users.
Update Policies	
Allow Public Updates	Allow updates from the public Windows Update service. Not allowing this service can cause issues with the Microsoft Store.
Allow Microsoft Updates	Allow updates from Microsoft Update.
Update Scan Frequency (Hours)	Set the number of hours between scans for updates.
Dual Scan	Enable to use Windows Update as your primary update source while using Windows Server update Services to provide all other content.
Exclude Windows Update Drivers from Quality Updates	Enable to prevent driver updates from automatically installing on devices during Quality Updates.
Install Signed Updates from 3rd Party Entities	Allow the installation of updates from approved third parties.
Mobile Operator App Download Limit	Select whether to ignore any Mobile Operator download limits for downloading apps and their updates over a cellular network.
Mobile Operator Update Download Limit	Select whether to ignore any Mobile Operator download limits for downloading OS updates over a cellular network.
Administrator-Approved Updates	
Require Update Approval	Enable to require updates to have approval before downloading to the device. Enable to require admins explicitly approve updates before downloading to the device. This approval is either through Update Groups or individual update approval. This option requires you to accept any required EULA on behalf of your end users before the update pushes to devices. If a EULA must be accepted, a dialog box opens displaying the EULA. To approve updates, navigate to **Lifecycle > Windows Updates**.
Delivery Optimization	
Peer-to-Peer Updates	Allow the use of peer-to-peer downloading of updates.

5. When you have finished customizing the profile, remember to select **Save & Publish** to push the profile to your devices.

Device Updates for Windows Desktop

Workspace ONE UEM supports reviewing and approving OS and OEM updates for Windows devices. The **Device Updates** page lists all updates available for Windows devices enrolled in the selected organization group.

Managed Application on Windows Desktop Profile

An admin can manage the removal of managed applications on devices. Under **Add a New Windows Desktop Profile > Managed Applications**, the admin can either enable or disable the ability to keep managed applications on the device if it is unenrolled.

Navigation

Find the available **Device Updates** in **Resources** > **Device Updates**. This page lists updates for **Windows** and **OEM Updates**.

Windows Tab

From the **Windows** tab, you can approve updates and assign the updates to the specific smart groups as meets your business needs. This tab displays all updates with their published date, platform, classification, and assigned group. Only the updates available for the Windows devices enrolled in the selected organization group (OG) display. If you do not have any Windows devices enrolled in the OG, no updates display.

Selecting the update name displays a window with detailed information, a link to the Microsoft KB page for the update, and the status of the update installation.

This process requires that you publish a Windows Update profile to devices with **Require Update Approval** enabled.

The update installation status shows the deployment of the update across your devices. See the status of the update deployment by selecting the update in the list or selecting **View** in the Installed Status column.

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

OEM Updates Tab

From this tab, you can see all OEM updates deployed to your Windows Desktop devices. You can order the list view by name, level, type, and device category. You can also filter the displayed updates with filters including audio drivers, chipset drivers, BIOS updates, and more.

See the installation status of the update deployment by selecting the update name.

Using Baselines

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

Cloud-Based Micro-Service

Baselines use a cloud-based micro service to manage 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 setup 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 Omnissa to supply 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 trying to login.
- Install the LAPS (Local Administrator Password Solution) AdmPwd GPO Extension / CSE.

Note: CIS is only available for Windows Desktop.

Assigning Baselines

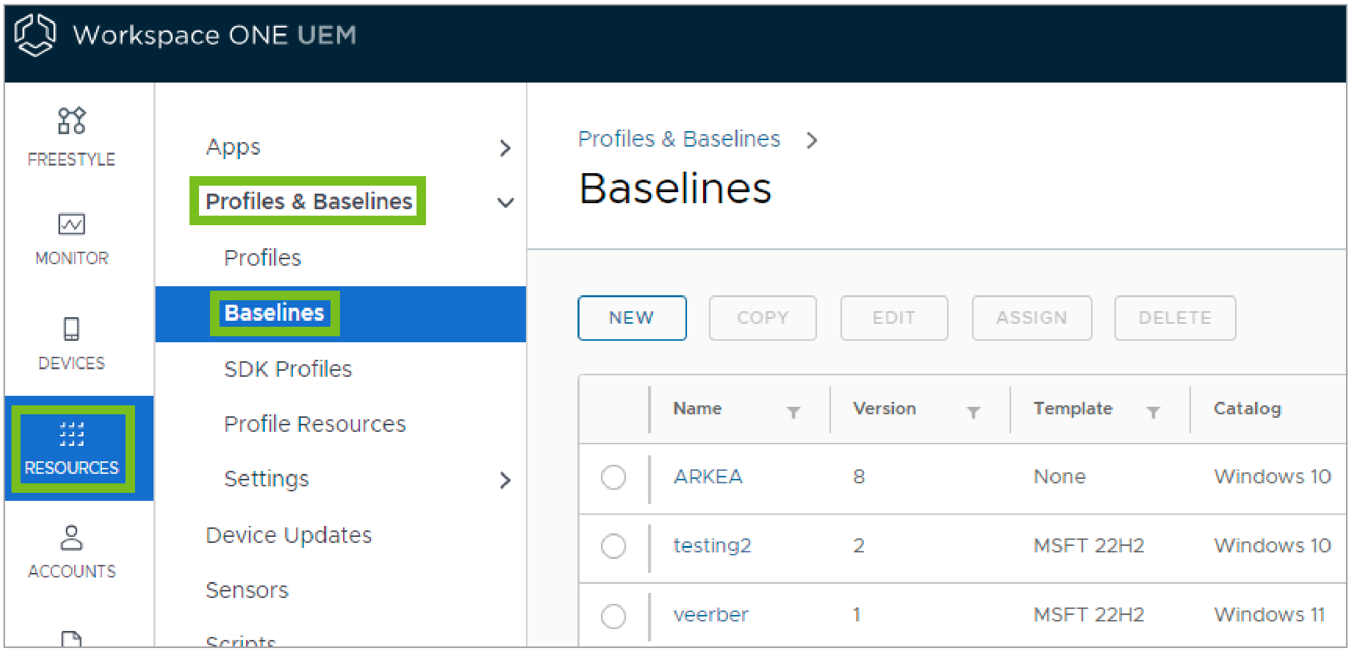
After enrolling a device into Workspace ONE UEM, you can add the device to a smart group and assign a

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.

You can limit the assignment of the Baseline using the **Exclusions** tab of the **Assignment** dialog box. You can also choose 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**.



	Name	Version	Template	Catalog
○	ARKEA	8	None	Windows 10
○	testing2	2	MSFT 22H2	Windows 10
○	veerber	1	MSFT 22H2	Windows 11

From here, you can edit, copy, and delete existing Baselines.

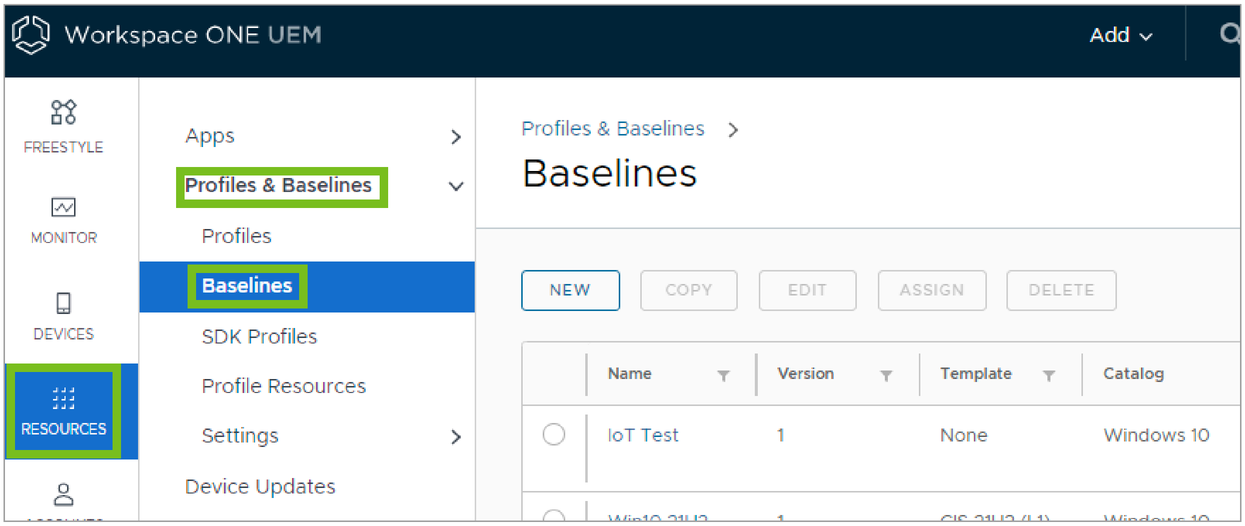
- **Copy**: You can copy Baselines and edit a few policies on the **Customize** and **Add Policies** tabs to fit the Baseline to another deployment scenario. Select the desired Baseline to display the **Copy** menu item.
  - You cannot edit the Baseline template. If you need a different template, create 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**.



Name	Version	Template	Catalog
IoT Test	1	None	Windows 10
Win10 21H2	1	CIS 21H2 (L1)	Windows 10

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.

Reapplying Baselines

There are multiple ways to enable local enforcement of Baselines. To execute a script that adds the reapply registry key on a device, you can use sensors, product provisioning, scripts in apps and books, or create a custom settings profile.

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.

Querying Baselines for Compliance Statuses

You can query devices for Baseline samples to refresh the compliance status. To query a Baseline, begin in the **Device Details** view.

Note: You can query the compliance status of a specific device but not multiple devices at once.

1. In the Workspace ONE UEM console, go to **Devices** and select the specific Windows Desktop device from the **Device List View**.
2. Select **More Actions > Query > Baselines**. This process initiates the query command.
3. To see the updated Baseline compliance status, go to **Resources > Profiles & Baselines > Baselines**, select the Baseline, and see the **Compliance Status** card.

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

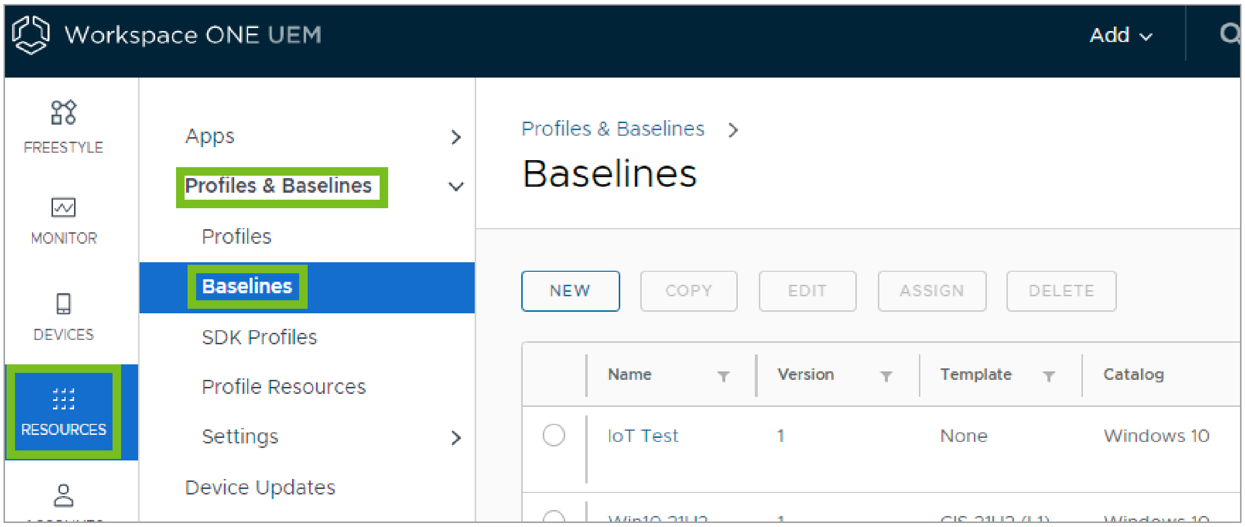
Your devices must be enrolled in Workspace ONE UEM and they must have the Workspace ONE Intelligent Hub installed.

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 Baselines with a Template

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

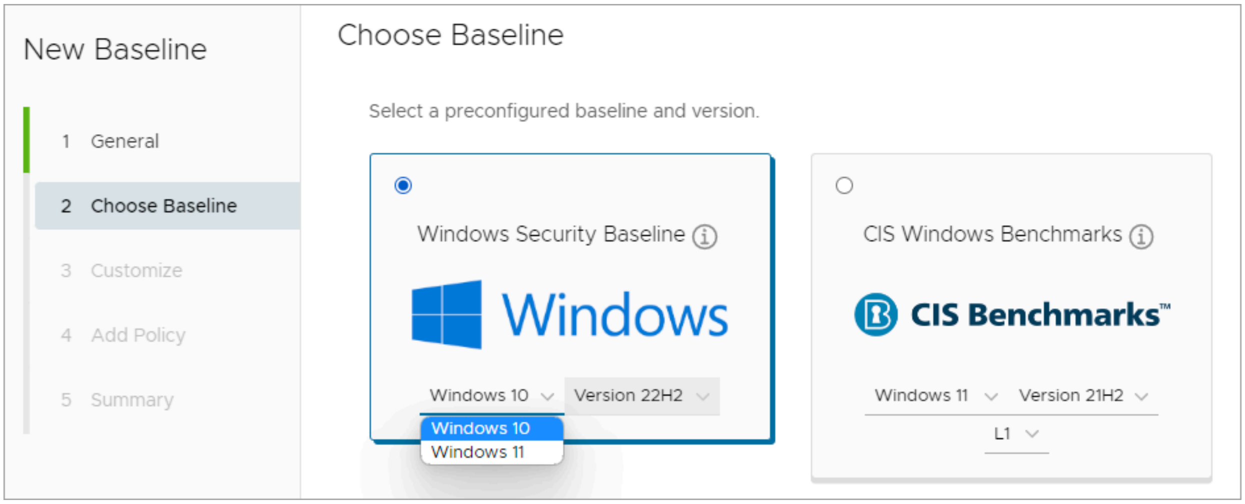
1. Navigate to **Resources** > **Profiles & Baselines** > **Baselines** and select **New**.



Name	Version	Template	Catalog
IoT Test	1	None	Windows 10
Win10 21H2	1	CIS 21H2 (L1)	Windows 10

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.



Select a preconfigured baseline and version.

Setting	Description
Windows Security Baseline	This Baseline applies the configuration settings proposed by Microsoft. Select the OS platform and version to apply.
CIS Windows Benchmarks	This Baseline applies the configuration settings proposed by CIS Benchmarks. Select the OS platform, 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 Custom Baselines

If you do not want to use a template to create your Baselines, follow these steps to create your own.

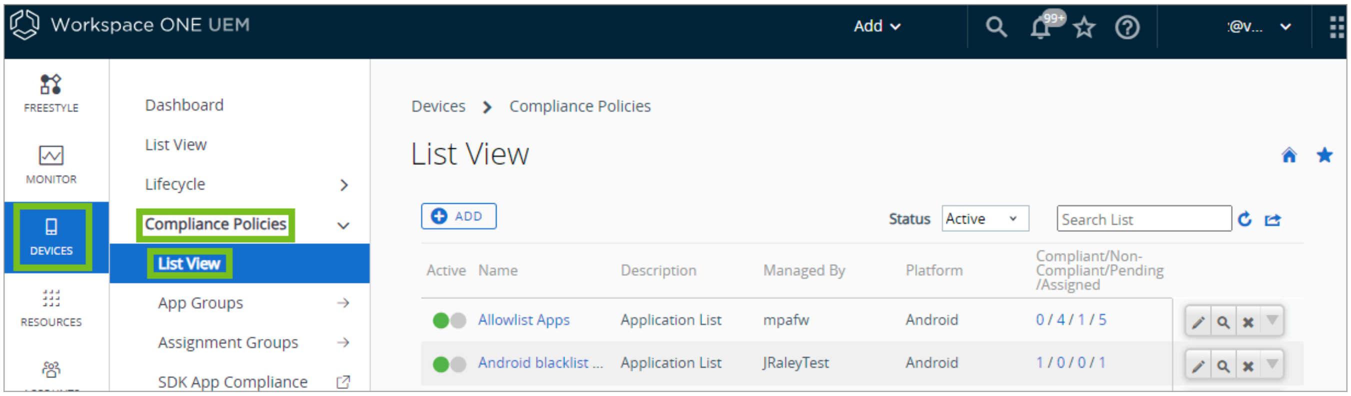
1. Navigate to **Resources** > **Profiles & Baselines** > **Baselines** and select **New**.
2. Select **Create your own**.
3. Enter a **Baseline Name**, **Description**, and select the smart group the Baseline is **Managed By**. Then select **Next**.
4. In the **Add Policy** window, select the Windows 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

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

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.



Status: Active

Active	Name	Description	Managed By	Platform	Compliant/Non-Compliant/Pending /Assigned
●	Allowlist Apps	Application List	mpafw	Android	0 / 4 / 1 / 5
●	Android blacklist ...	Application List	JRaleyTest	Android	1 / 0 / 0 / 1

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.

Note: This is only supported for Windows Desktop devices at this time.

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.

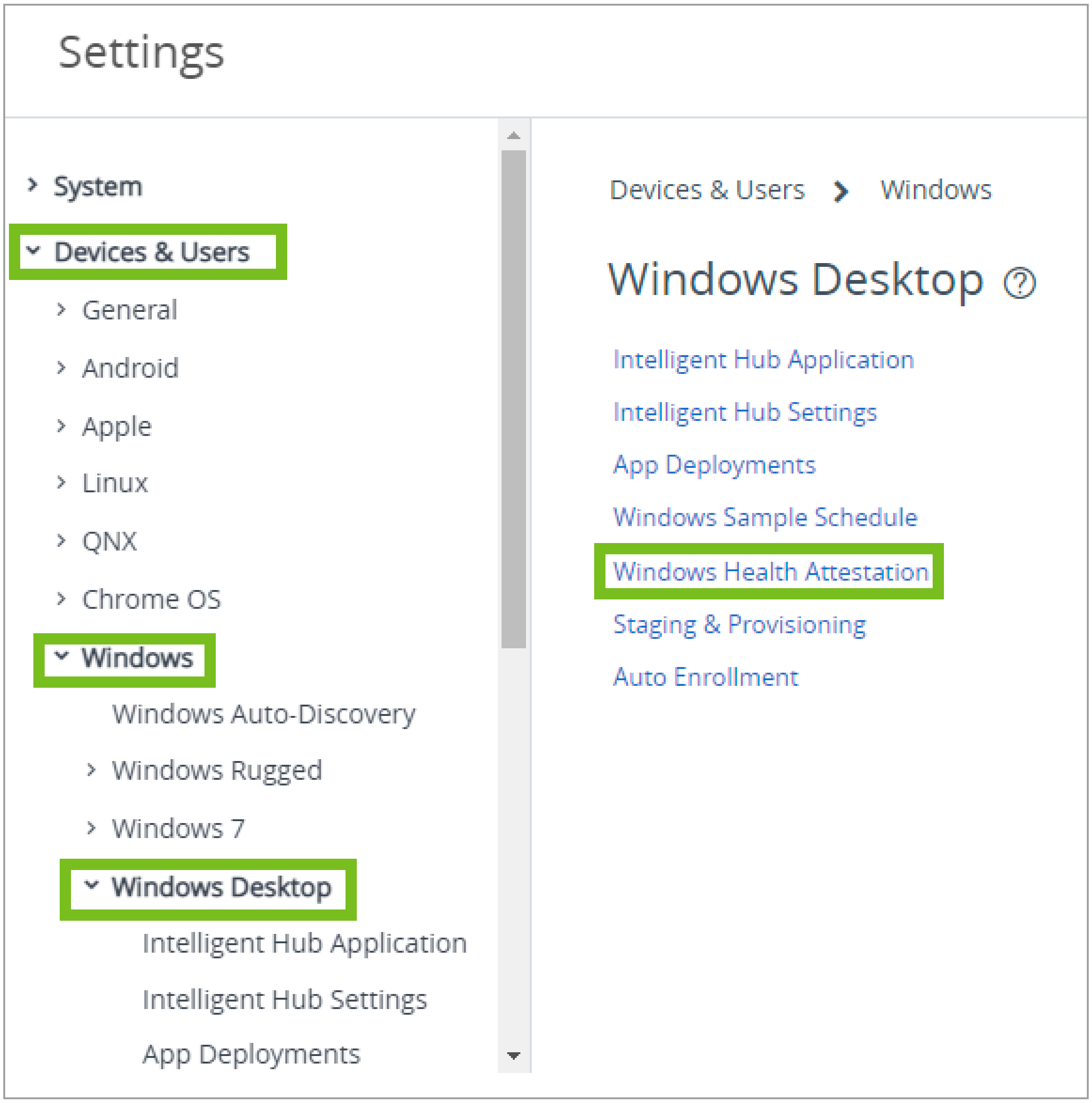
Workspace ONE UEM enables you to configure the Windows Health Attestation service to ensure device compliance. If any of the enabled checks fail, the Workspace ONE UEM compliance policy engine applies security measures based on the configured compliance policy. This functionality allows you to keep your 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

Settings	Descriptions
	tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.
Data Execution Prevention (DEP) Policy 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

You can use Omnissa Workspace ONE UEM to distribute, track, and manage your internal applications for Windows Desktop and Windows Server managed devices. Additionally, use the Workspace ONE Intelligent Hub for Windows to provide an application catalog for Windows Desktop devices.

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.

Workspace ONE Intelligent Hub for Windows

When the Workspace ONE Intelligent Hub is installed on Windows Desktop 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 Intelligent Hub allows a user to click to Install, Reinstall, or Remove (Uninstall) native applications assigned to that device or user. Native applications as well as websites can be Favorited by clicking the star and categorized to enable easier user browsing of available applications.

Installing Native Apps

Currently apps can only be installed from the catalog, not launched from the hub. For detailed instructions on installing apps, refer to TechZone: Deploying Workspace ONE UEM applications to Windows devices.

A new feature for the 2506 release (feature flag: WindowsNativeAppLaunchFeatureFlag) allows admins to define the launch path for applications and launch native Windows apps directly from Intelligent Hub.

Once the feature flag is enabled, go to the Console and navigate to: **Resources > Native Apps > Internal > Add > Application File**. In the **Details** box, select the **Deployment Options** tab. Under **How To Install**, you'll find two new fields: **Launch Type and Launch Command**.

Launch Type can be set to either LaunchPath or LaunchUri. **Launch Command** should be the path or URI for the application, for example: C:\Program Files\Adobe\Acrobat\acrobat.exe (when using LaunchPath). This command is executed locally by Intelligent Hub allowing end users to launch native applications from the Intelligent Hub App catalog as well.

For existing applications, once the feature flag is turned on, admins will see an empty Launch Command field and a default value selected for Launch Type.

Troubleshooting:

When the feature flag is **ON**: Two new fields become visible. For existing applications, once the feature flag is enabled, the admin will see an empty LaunchCommand textbox and the default option selected for LaunchType. To enable the launch option for an existing application, enter the LaunchCommand and republish the application.

When the feature flag is **OFF**: These two new fields are hidden.

API's can also be uploaded using the following API endpoints

1. mam/apps/internal/begininstall
2. mam/apps/internal/application

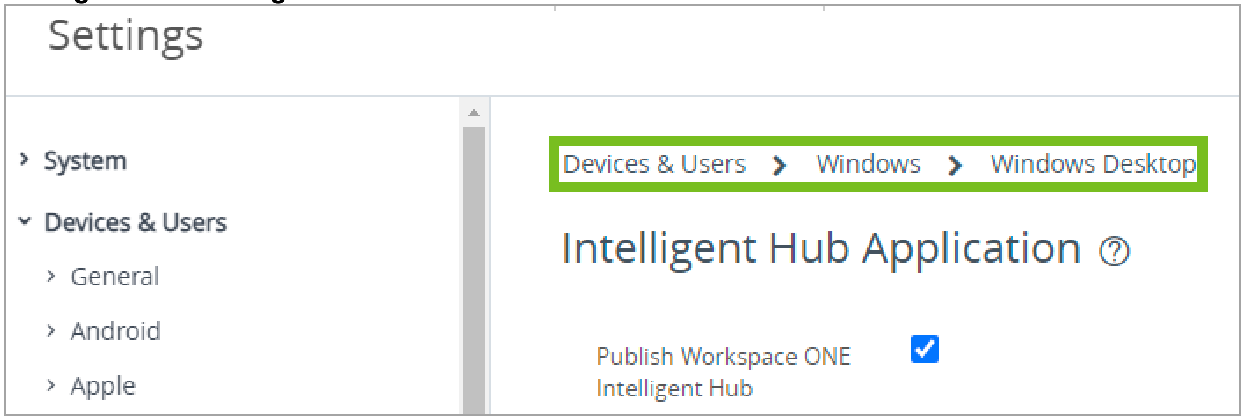
Software Delivery (SFD) Package Deployment

In the current workflow, when devices are enrolled, SFD needs to be downloaded before it can be pushed down to the device and installed. Starting in 2506 and later, SFD will be installed from the local resource instead of a separate download, which will reduce the time needed from enrollment to the first installation.

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**.



Settings
System
Devices & Users
General
Android
Apple
Devices & Users > Windows > Windows Desktop
Intelligent Hub Application
Publish Workspace ONE Intelligent Hub ☑

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 crashes 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.

Note: UI Lockdown - Enable to lock down completely the UI so end users cannot change settings.

Adding Win32 Applications and Management

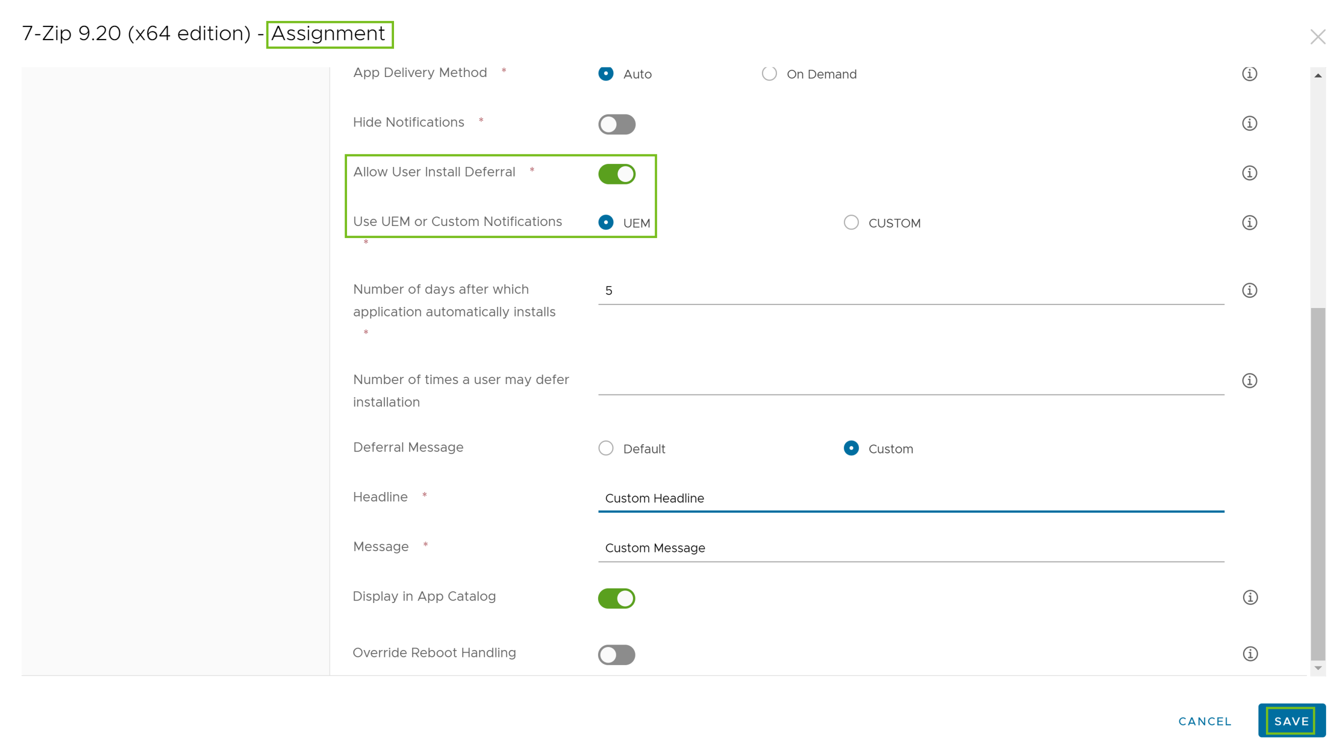
When installing any new Win32 application, you will start in the Workspace ONE UEM console, under **Resources > Apps > Native > Add > Application File**. You can choose the file from either a local file or link and then click

Save. Once the app is chosen, you will see an **Add Application** window open that will allow you to set and customize the settings. After successful installation, the extracted content from the .zip files will be removed.

Note: Beginning with 2410 and later, an optimized SFD Download behavior no longer requires a full application download when the cache is cleared where an application is using scripts for detection or uninstallation. This optimization significantly reduces bandwidth consumption and speeds up application deployment.

Defer the Application Installation in the UEM

As an admin you can enable the option to allow users to manage and defer the app installs. In the Application **Assignment** menu, under **Distribution**, toggle on the **Allow User Install Deferral** option. Then, under **Use UEM or Custom Notifications** choose **UEM**. Now you can define how long the end user can defer the app installs.
Note: Application Installation Deferral is supported on Windows Desktop devices with an active logged in user and Workspace ONE Intelligent Hub for Windows installed.



7-Zip 9.20 (x64 edition) - Assignment

App Delivery Method * ● Auto ○ On Demand

Hide Notifications * ☐

Allow User Install Deferral * ☑

Use UEM or Custom Notifications * ● UEM ○ CUSTOM

Number of days after which application automatically installs * 5

Number of times a user may defer installation

Deferral Message ○ Default ● Custom

Headline * Custom Headline

Message * Custom Message

Display in App Catalog ☑

Override Reboot Handling ☐

You can choose to set:

1. The Deferral Deadline- The number of **days** after which the application automatically installs.
2. The Deferral Count- The number of **times** a user may defer installation.
3. Both the Deferral Deadline and the Deferral Count.

If you choose to set both options, the first deferral option timeline that is reached will be when this would take effect. At that point, the user will be given the ability to defer one last time, but only for 30 minutes. After that the app will start the install process. *Example: The admin sets both the Deferral Deadline to 10 Days and sets the Deferral Count to 3. The event that happens first will be the one that applies. So if the user reaches that 3rd deferral count option in 4 days, that is when the user will see the option to defer for only 30 minutes and then the app will start the installation.*

The UEM does offer a default deferral toast notification message. However, if you would like to create your own, under **Deferral Message** choose **Custom** and provide your own deferral **Headline** and **Message**.

Managing Extracted Content Removal

The Extracted Content Removal feature determines whether temporary files generated during application installation are automatically deleted once the process is complete. Although this helps optimize disk space, some applications may need these extracted files to remain available for troubleshooting or future updates.

To avoid problems from deleting these files early, Workspace ONE UEM allows administrators to deactivate the Extracted Content Removal feature, either globally for all applications or individually for specific apps.

Note: The Extracted Content Removal feature requires a minimum SFD version 24.10.7 or later.

Disabling Extracted Content Removal Globally

The Extracted Content Removal feature can be deactivated without any console or UI configuration. Administrators can instead use a Windows registry setting to turn off this feature globally.

The Registry location is: `HKLM\SOFTWARE\AirWatchMDM\AppDeploymentAgent\Common\{00000000-0000-0000-0000-000000000000}`

Note: By default, if no registry value is configured, the extracted files are automatically removed after the installation completes.

Flag Name	Type	Value (Data)	Description
Feature.DisableExtractedContentsCleanup	REG_SZ	True	Retains extracted contents after installation (deactivates cleanup).
NA	NA	False	Deletes extracted contents after installation (activates cleanup).
NA	NA	Empty or any other non-true value	Deletes extracted contents after installation (default behavior).

The configuration behavior of the Extracted Content Removal feature is as follows:

- When the global registry flag is set to True, cleanup of extracted installation files is deactivated for all applications.
- When the flag is absent or set to False, the cleanup process functions normally.
- The registry settings are read and applied during App Deployment Agent startup or the next relevant initialization phase. These changes take effect automatically, without requiring any console updates.

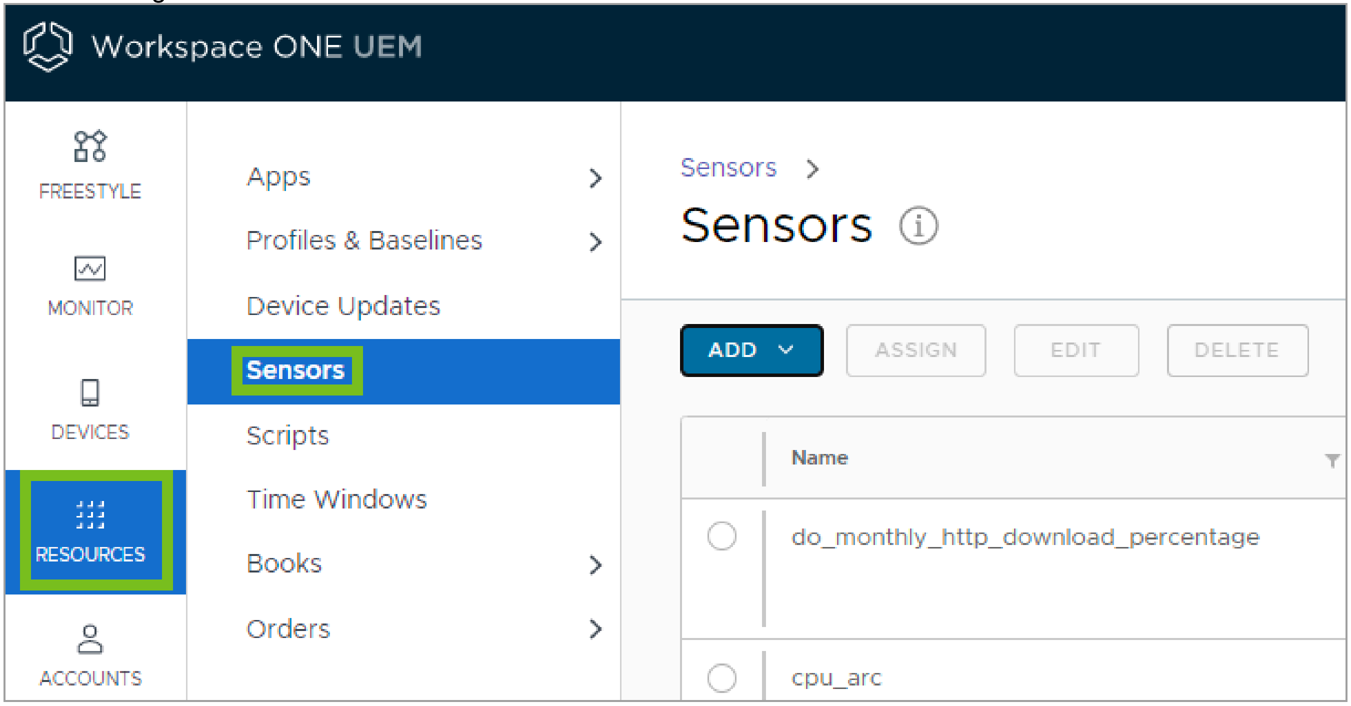
Collect Data with Sensors

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 Omnissa Intelligence and in Workspace ONE UEM.

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**.



Sensor return values are displayed within the Sensors tab of each Windows Desktop and Windows Server device. To work with Sensors data from Workspace ONE UEM, you can use Omnissa Intelligence Dashboards and Reports for reporting, or Freestyle within Omnissa Intelligence and Workspace ONE UEM consoles to create Orchestration Workflows.

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.

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 Omnissa 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.

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.

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 Omnissa Intelligence. After it evaluates and reports, the PowerShell process terminates.

Omnissa Intelligence Options

Reports and Dashboards To Analyze Data

If you use the Omnissa 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 Omnissa Intelligence. RBAC assigns permissions to admins, so use them to prevent or allow specific Omnissa Intelligence users from accessing Sensors data.

Encryption

All data at rest is encrypted in Omnissa Intelligence.

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
```

Omnissa Intelligence Documentation

For details on how to work in Omnissa Intelligence, access Omnissa Intelligence Products.

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. More examples are available within the Omnissa euc-samples github repository.

The following examples contain the settings and code needed.

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 $batte
ry_remain
```

Get Serial Number

- **Value Type**: String

- **Execution Context**: User

```
$os=Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlyc
ontinue
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 silentl
ycontinue
echo $os.SMBIOSPresent
```

Check SMBIOS BIOSVersion

- **Value Type**: Boolean

- **Execution Context**: User

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

Get BIOS Version

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

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

Get BIOS Status

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

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentl
ycontinue
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

```
$Total_bytes=Get-WmiObject -class Win32_PerfFormattedData_Tcpip_NetworkInt
erface
|Measure-Object -property BytesTotalPersec -Average |Select-Object -Expand
Property Average
echo ([System.Math]::Round($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-Obje
ct -ExpandProperty Average
$NPM = get-process chrome |Measure-object -property NPM -Average|Select-Ob
ject -ExpandProperty Average
echo [System.Math]::Round(($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" -Namesp
ace "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_s
tatus[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 and Windows Server 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.

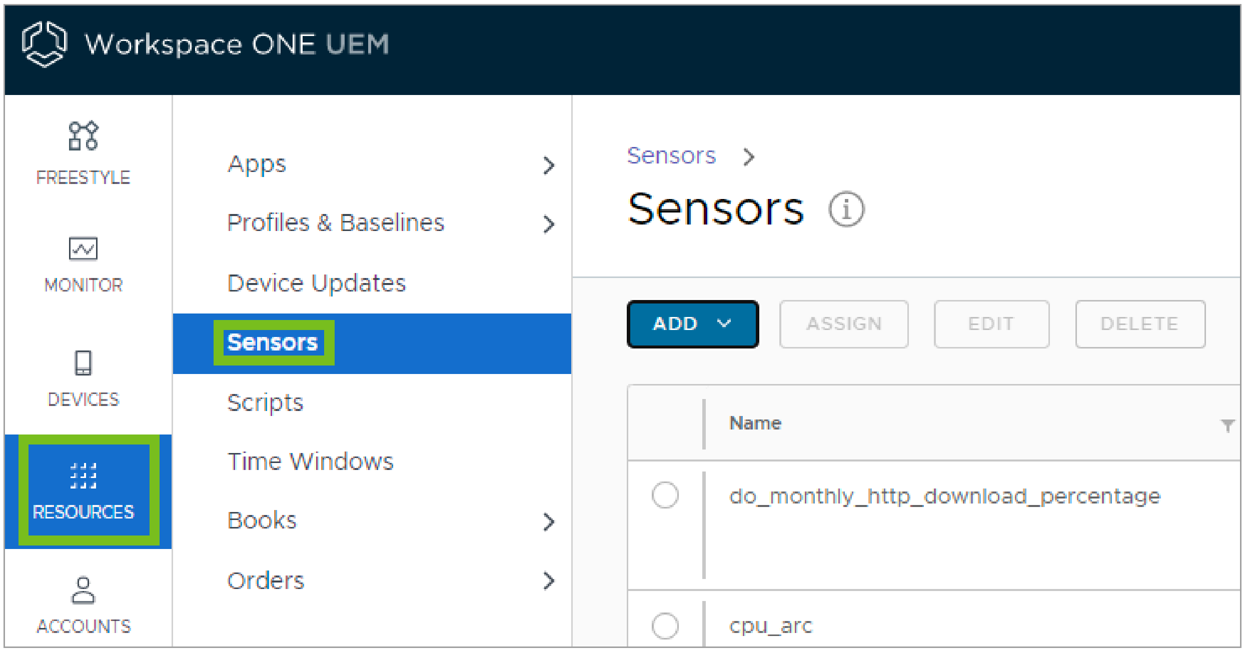
Each script contains only one sensor. If a script returns multiple values, Omnissa Intelligence and Workspace ONE UEM read only the first value as the response from the script. If a script returns a null value, Omnissa Intelligence and Workspace ONE UEM do not report the sensor.

Prerequisites

If you want to view Sensors for multiple devices and interact with the data in reports and dashboards, you must opt into Omnissa Intelligence. If you want to view Sensors data for a single device, you do not need Omnissa 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

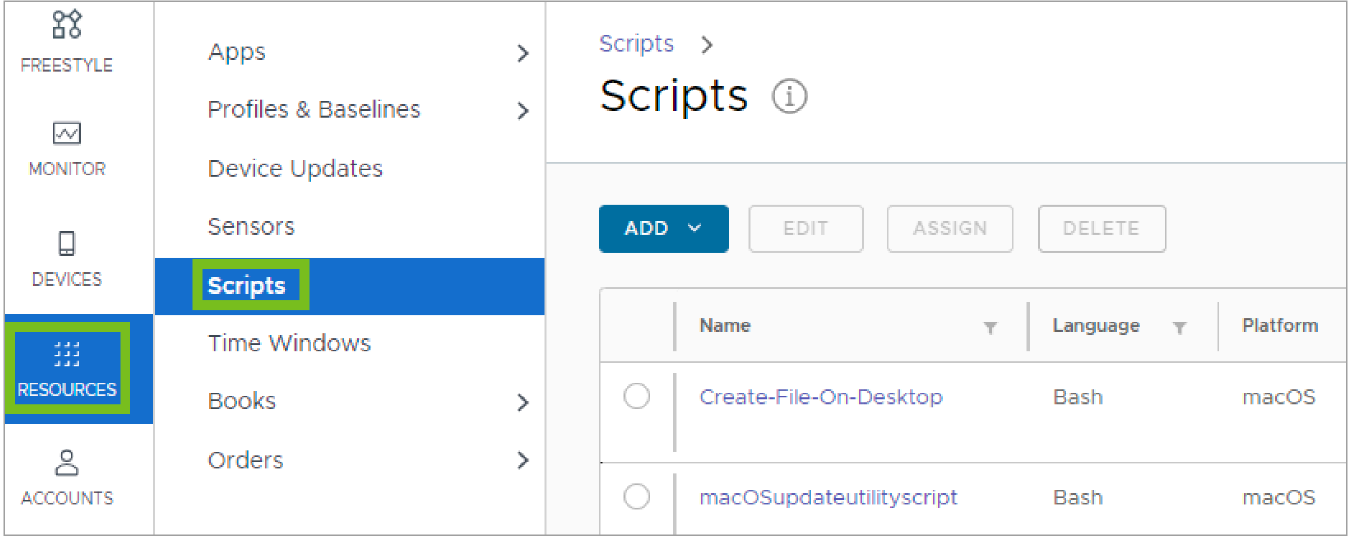
After creating a sensor, use the **Device Details** page in Workspace ONE UEM to see data for single devices or go to Omnissa Intelligence to use reports and dashboards to interact with data for multiple devices.

Automate Endpoint Configurations with Scripts

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

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.



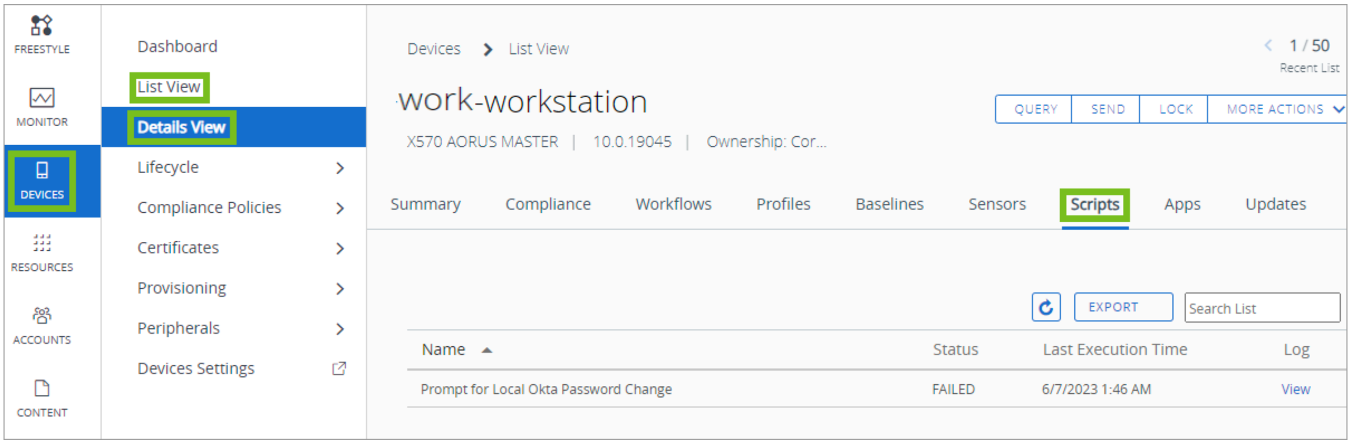
	Name	Language	Platform
○	Create-File-On-Desktop	Bash	macOS
○	macOSupdateutilityscript	Bash	macOS

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).



Name	Status	Last Execution Time	Log
Prompt for Local Okta Password Change	FAILED	6/7/2023 1:46 AM	View

- 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 Devices

Scripts support using PowerShell to execute code on end user devices. Integrate Scripts with the Workspace ONE Intelligent Hub for Windows and enable self-service to Scripts for your users.

Note: If you are publishing scripts to less than 2000 (default value) devices, the devices are notified immediately to fetch the resource. However, if the smart groups assigned have more than 2000 devices, then the devices will receive the resource the next time the devices checks-in with Workspace ONE UEM console.

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.
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. This option is only valid with Windows Desktop devices.

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

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. Dell Command integration is supported on Windows Desktop devices only.

Dell Command | Configure

By intergrating Workspace ONE UEM with Dell Command | Configure you can enhance the device management and enable the full functionality of the BIOS profile for Windows Desktop devices on your Dell enterprise devices. The BIOS profile can control hardware virtualization and BIOS security.

Dell Command | Monitor

Integrate Workspace ONE UEM with Dell Command | Monitor to enhance the information Workspace ONE UEM collects from enrolled Dell enterprise devices. To use the BIOS profile you must add this integration to your environment. This integration allows you to configure device BIOS settings to control hardware virtualization and BIOS security. You must also enable Software Distribution to push Dell Command | Monitor to your devices. Configure the BIOS profile to enabled Dell Command | Monitor.

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

By intergrating Workspace ONE UEM with Dell Command | Update you can control when and what types of updates to deploy to your devices. This client-side management software enables updating firmware, drivers, and applications for supported Dell devices. Configure the OEM Updates profile to enabled Dell Command | Update on end-user devices.

Configure Dell Command | Products to Workspace ONE UEM

To enhance management of your Dell enterprise devices, add the Dell Command | Products to the Workspace ONE UEM console.

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

You can choose to use the installer to automate this process, or you can install from the command line. When using the installer, click the **Extract** button and then click **Install**. To install from the command line:

Prerequisites

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

Download the latest version of the Dell Command | Product to proceed: - Dell Command | Configure - Dell Command | Update - Dell Command | Monitor

Procedure

1. Open the EXE and select **Extract**. Save the extracted files into a folder.
2. Navigate to the folder and find the **MSI** file.
3. 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.
4. In the **Deployment Options** tab, set the **Admin Privileges** to **Yes**.
5. 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.

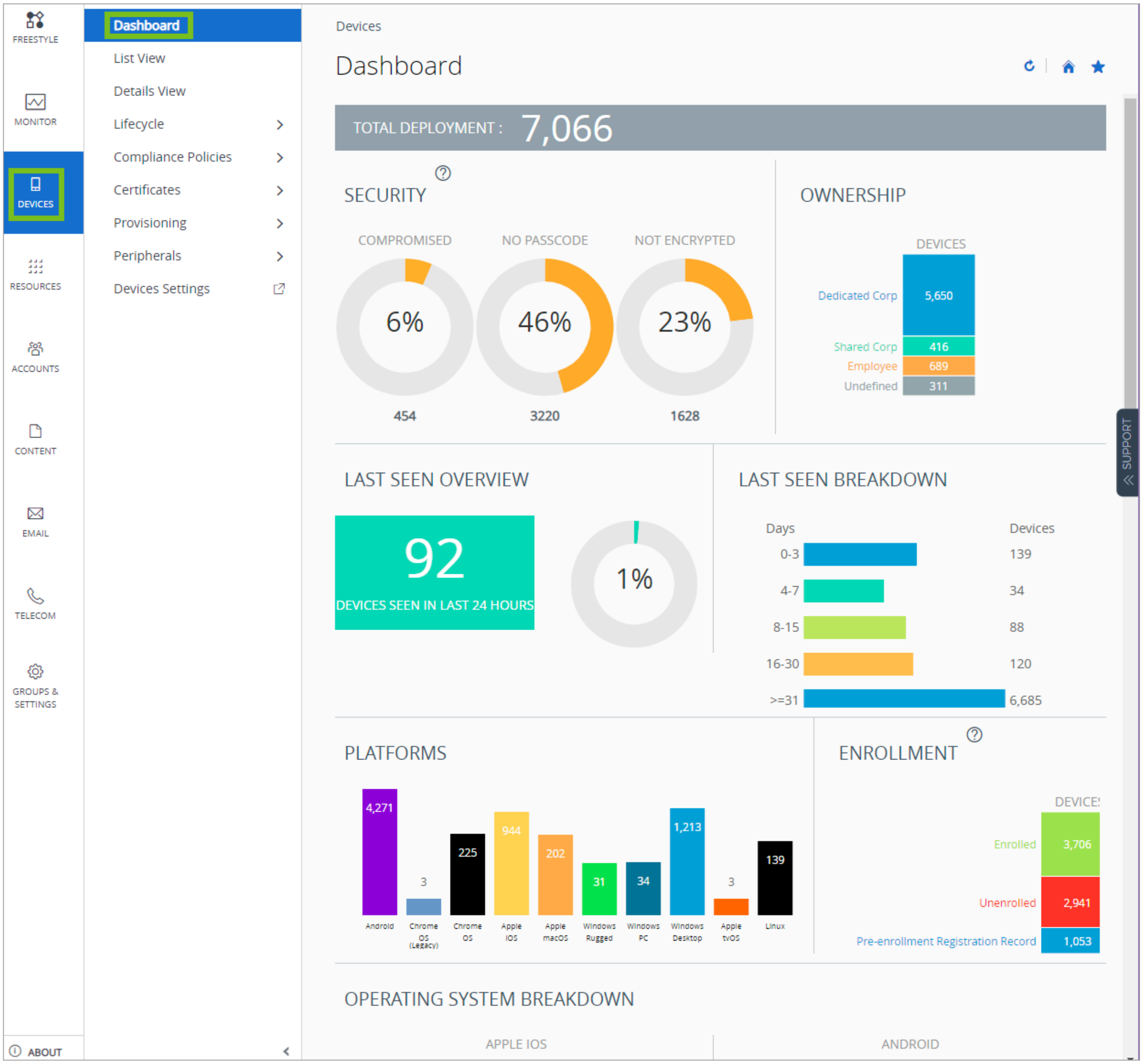
Windows Device Management

After your Windows Desktop and Windows Server devices are enrolled and configured, manage the devices using the Workspace ONE UEM console. The management tools and functions enable you to monitor your devices and remotely perform administrative functions. Monitoring and administrative management functions on Windows Desktop and Windows Server devices are largely the same. Differences are called out in the respective capability sections. The term Windows devices is used to describe both Windows Desktop and Windows Server devices.

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.

Device Dashboard

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



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 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

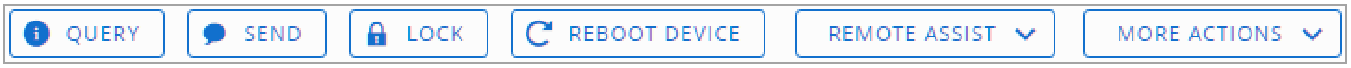
Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

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 [Message], 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 Server
  - 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.

Device Details Page

Use the Device Details page in Workspace ONE UEM to track detailed device information for Windows devices and quickly access user and device management actions. You can access Device Details by selecting the Friendly Name from the Device List View, using one of the Dashboards, or with any of the search tools.

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.

Note: **Enhanced Push Notification Reliability**: Beginning 2410, the Workspace ONE Intelligent Hub silently auto-launches in the background following a fresh install or upgrade. This ensures the reliable delivery of push notifications—even on devices where the app hasn't been manually opened—keeping your employees informed and connected without additional effort. The minimum UEM version necessary to support this is 2410 and is supported on Windows Desktop devices only. 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, enrollment status and platform. For example, Windows Server devices do not support or have the Device Wipe command as this is an OMA-DM and therefore Windows Desktop only command.

- **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:

- **Device Information (Query)** – Send a 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.

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

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

- **Baselines (Query)** – Send a query command to the device to return a list of samples.

- **Security (Query)** – Send a query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, and so on).

- **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.

Management:

- **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 Managed Resources profile to control which resources are kept after a device is unenrolled as part of an Enterprise Wipe or Delete Device action. Keep Managed Apps On Device, Keep Hub-managed Profiles on Device and Keep Baselines on Device enable each respective resource type to be kept on the device, depending upon the Windows OS of the device. Windows Desktop devices only support Keep Managed Apps On Device, whilst Windows Server devices support all three resource types.
      The Managed Resources profile must be deployed and installed to the device prior to executing the Enterprise Wipe or Delete Device action. This feature is helpful on Windows Desktop devices 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 below.
    - Workspace ONE UEM enables **Software Distribution** (SFD) 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 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.

- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again.

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

- **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.

Admin:

- **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. Use the Managed Resources profile to control which resources are kept after a device is unenrolled as part of an Enterprise Wipe or Delete Device action. Keep Managed Apps On Device, Keep Hub-managed Profiles on Device and Keep Baselines on Device enable each respective resource type to be kept on the device, depending upon the Windows OS of the device. Windows Desktop devices only support Keep Managed Apps On Device, whilst Windows Server devices support all three resource types. The Managed Resources profile must be deployed and installed to the device prior to executing the Enterprise Wipe or Delete Device action. This feature is helpful on Windows Desktop devices 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 those requirements.

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

- **Force BIOS Password Reset** – Force the device to reset the BIOS password to a new auto-generated password.

- **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.

- **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.

  Starting with Hub clients 25.05+ a feature flag (WindowsLogFilterFeatureFlag) has been added that when enabled, allows admins to request a log from three components instead of two and filter for targeted log retrieval.

  - **Hub:** provides logs from multiple agents running on the device (Intelligent Hub, App Deployment Agent, Provisioning Agent, Factory Provisioning, MDM).
  - **System:** provides system-level logs (Windows, PCRefresh).
  - **Other:** will now provide logs from Assist, DEEM Telemetry Agent, Workspace ONE Tunnel.

  For targeted log filtering, you can now search by **Duration** and Hub **Components**. The duration timeframe for filtering can be set to either all the logs, or your choice from the last 1,3,7,or 14 days.

  Note: **Automatic merging of large Device logs for enhanced troubleshooting**: Beginning 2410, admins can now collect and access large device logs more efficiently. Previously, the process involved uploading multiple small files from Workspace ONE Hub to UEM, requiring admins to download and merge numerous separate files, which was time consuming for troubleshooting large log files. With the latest update, logs are uploaded and automatically merged into a single file (up to 200MB), reducing the effort and time needed to troubleshoot devices. Minimum UEM version necessary to support this is v2410

- **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.

- **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 supported in HoloLens devices.

Manage and Enroll Your Arm64 Devices

Workspace ONE UEM supports enrolling and managing ARM64 devices that are running Windows 11. Workspace ONE Intelligent Hub is supported on ARM64, allowing your ARM64 devices to be enrolled using the Hub or native MDM enrollment. After enrolling your devices, you can deploy and manage apps, apply sensors, scripts, and some profiles using Workspace ONE UEM. All OMADM profiles and Hub based Encryption profiles are currently supported on ARM64 devices.

Note: WMI based sensor queries are not supported on ARM64 devices. CIM based queries should be used instead. In general, CIM based sensor queries are recommended for all Windows devices.

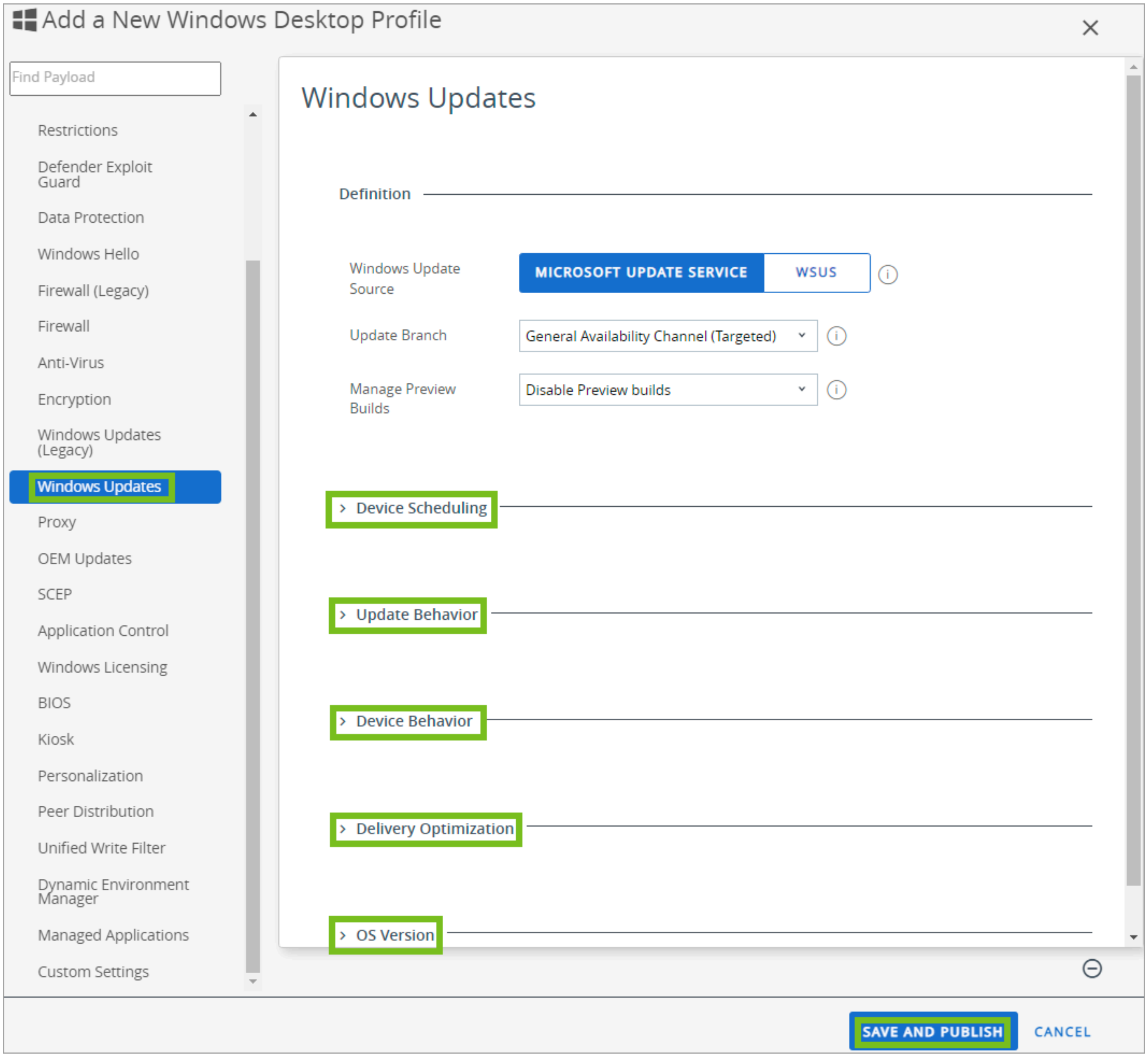
Product Provisioning

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.

Managing Windows Device Updates

Windows device updates are now under the device profile. In the Workspace ONE UEM console navigate to: **Resources > Profiles & Baselines > Profiles > Add > Select Add Profile > Windows > Windows Desktop > Device Profile > Windows Updates**.



Windows Update Source: MICROSOFT UPDATE SERVICE | WSUS

Update Branch: General Availability Channel (Targeted)

Manage Preview Builds: Disable Preview builds

There are five categories that can be configured independently.

- Device Scheduling
- Update Behavior
- Device Behavior
- Delivery Optimization
- OS Version

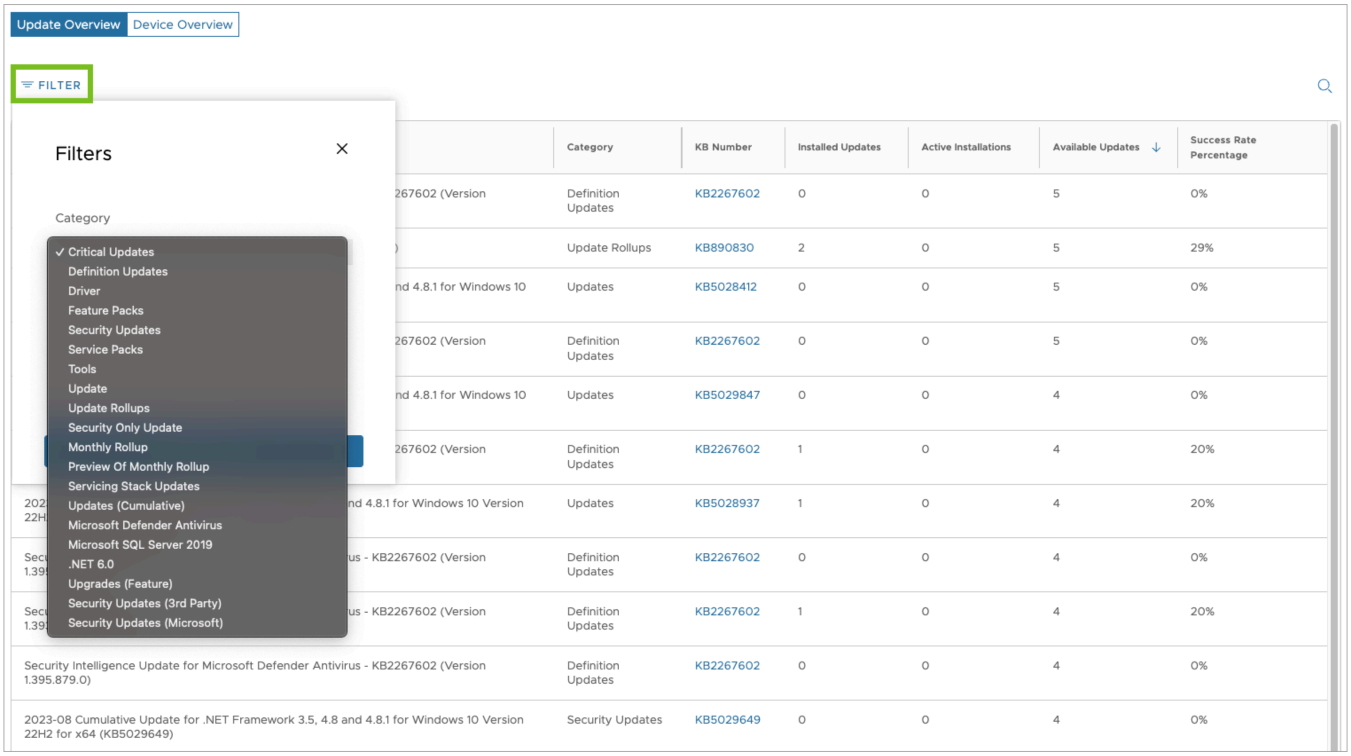
Admins can customize these settings depending on their specific needs. The most frequently used settings are defaulted for each category. By selecting Enable or Disable you can configure these categories as needed. Remember when you are done configuring to select **Save and Publish**.

Resources - Device Updates

For Windows users, a feature has been added with 2406 that will allow for better update reporting. Because Windows has both Windows 10 and Windows 11 devices with different versions, this feature will provide an easy-to-understand overview showing every Windows Version in the organization group as well as the child organization. **NOTE: This does require Modern Stack to be enabled for the environment.**

To find devices that don't run on the latest Quality Update, check the revision overview to see the Version revision that identifies the installed Quality Update.

As the Admin, you can visually see what updates have and have not been delivered to each device, and can click on the sections to change their selections. You can filter or search by either an Update or Device Overview. Then, each of those categories also allow further filtering abilities through both the Filter as well as clicking on the table's column heading.

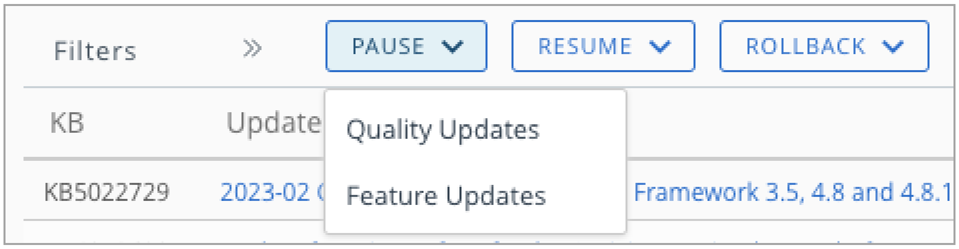


	Category	KB Number	Installed Updates	Active Installations	Available Updates ↓	Success Rate Percentage
267602 (Version	Definition Updates	KB2267602	0	0	5	0%
)	Update Rollups	KB890830	2	0	5	29%
nd 4.8.1 for Windows 10	Updates	KB5028412	0	0	5	0%
267602 (Version	Definition Updates	KB2267602	0	0	5	0%
nd 4.8.1 for Windows 10	Updates	KB5029847	0	0	4	0%
267602 (Version	Definition Updates	KB2267602	1	0	4	20%
202 nd 4.8.1 for Windows 10 Version 22H	Updates	KB5028937	1	0	4	20%
Sec us - KB2267602 (Version 1.39	Definition Updates	KB2267602	0	0	4	0%
Sec us - KB2267602 (Version 1.39	Definition Updates	KB2267602	1	0	4	20%
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.395.879.0)	Definition Updates	KB2267602	0	0	4	0%
2023-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5029649)	Security Updates	KB5029649	0	0	4	0%

In your console under the **Device Details > Device Updates**, a feature has been added to view the devices associated with your updates. If you select the KB number and/or update title, you will then see the update overview. At the bottom it will now show the list the devices included in that update as well as their status overivew. You can filter on that list as needed. We have also moved the KB column over to the left for easier access in the console.

Troubleshooting Feature & Quality Updates

Because Windows Updates can cause issues in combination with specific drivers or applications, three buttons were added to help admins troubleshoot these situations.



1. Pause- this button allows a pause to both feature and quality updates before they go out (but only for 35 days).
2. Resume- this button enables Windows Update search and installation again. Once you resume the updates, you will see that the registry for the start time will be cleared.
3. Rollback- this button allows updates that were made but caused unforeseen issues to be temporarily returned to the previous version while you resolve the issue.

After any of these button commands are activated, the command will be queued on the device and the event log will stay empty. The command status will also not change but continue to show as pending. Success and or Failures will be shown in the troubleshooting tab in the console. For all button commands, 35 days is the maximum time allowed by Microsoft for any delay.

Deploying Domain Join Configurations for Windows Desktop

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.

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 for Deploying Domain Join Configuration

Before deploying the Domain Join Configuration, check to make sure you have completed the following requirements:

- Windows Automatic Enrollment: Configure automatic enrollment in Azure with Workspace ONE UEM as the mobile device management (MDM) system.
- Workspace ONE UEM: Disable the Status Tracking Page for OOBE.
    1. In Workspace ONE UEM, go to **Groups & Settings > All Settings > Device & Users > General > Enrollment**.
    2. Select the **Optional Prompt** tab.
    3. 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.

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

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.

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 Additional Requirements

If you use Active Directory to manage users, you can use Workspace ONE UEM to assign your on-premises domain join configurations. Confirm the following requirements have been completed before you begin:

- 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.
- 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.

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.

Configure the Active Directory Users and Computers (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**, **Write**, and **Create All Child Objects**, and then select **Next**.

Configure the Airwatch Cloud Connector (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>:\Omnissa\AirWatch\CloudConnector`.

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.

Assign a Domain Join Configuration

Below are the steps to assign your domain join configuration:

Important: Assigning more than one Domain Join configuration to a single device is not supported. This includes configurations deployed through direct assignment (as outlined in this section) as well as those delivered via Freestyle Workflows. Applying multiple Domain Join configurations may lead to conflicts and unpredictable behavior on the device. To ensure proper functionality, each device should have only one active Domain Join configuration at any time.

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.

Note: In versions of Workspace ONE UEM prior to 2506, the Offline Domain Join configuration was applied only during device enrollment. Starting with Workspace ONE UEM 2506 and modern architecture enabled, this limitation has been removed — the Offline Domain Join configuration can now be applied at any point in the device lifecycle, providing greater flexibility in deployment scenarios. This in not applicable for Workgroup scenarios.

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

Domain Join configuration assignment is determined by Smart Group membership. The Parent-Child Organizational Group (OG) hierarchy does not influence configuration assignment unless the device qualifies for

Smart Groups in both the parent and child OGs.

If a device qualifies for Offline Domain Join configurations assigned at both the parent and child OG levels, the configuration from the child OG (more specific or “closed” OG) will take precedence and be applied to the device.

When a device receives **multiple Offline Domain Join configurations**, conflict resolution is determined based on the **Domain Name** and **Type**.

- If **all configurations have the same Domain Name and Type**, the **Organization Unit (OU)** is treated as **optional**. The system proceeds with the domain join, treating the OU as empty if necessary.
- If the **Domain Name or Type differs**, the domain join **cannot proceed**.

◆ Scenario 1: Same Domain, Different OU

The device qualifies for **SG1** and **SG2**.

Device SG	Domain Name	Type	Organization Unit
SG1	amst.ad	OfflineDomainJoin	OU=domainJoinOU,DC=amst,DC=ad
SG2	amst.ad	OfflineDomainJoin	DC=amst,DC=ad

Outcome:
Domain Name and Type match; Organization Unit differs. The OU is treated as empty, and domain join proceeds.

Effective Configuration:

Domain Name	Type	Organization Unit
amst.ad	OfflineDomainJoin	*(empty)*

Scenario 2: Identical Configurations

The device qualifies for **SG1** and **SG2**.

Device SG	Domain Name	Type	Organization Unit
SG1	amst.ad	OfflineDomainJoin	OU=domainJoinOU,DC=amst,DC=ad
SG2	amst.ad	OfflineDomainJoin	OU=domainJoinOU,DC=amst,DC=ad

Outcome:
All fields match exactly. Domain join proceeds using the specified Organization Unit.

Effective Configuration:

Domain Name	Type	Organization Unit
amst.ad	OfflineDomainJoin	OU=domainJoinOU,DC=amst,DC=ad

Scenario 3: Different Domains

The device qualifies for **SG1** and **SG2**.

Device SG	Domain Name	Type	Organization Unit
SG1	amst.ad	OfflineDomainJoin	OU=domainJoinOU,DC=amst,DC=ad
SG2	dell.ad	OfflineDomainJoin	OU=domainJoinOU,DC=dell,DC=ad

Outcome:
Domain Names differ. A device cannot be joined to multiple domains. Domain join will **not** be processed.

Effective Configuration:
No Domain Join possible

Device Receives Both Domain Join and Workgroup Configurations

When both a Domain Join and a Workgroup configuration are assigned to the same device, the system will prioritize and apply the Domain Join configuration. The Workgroup configuration will be ignored in this case.

Applying Domain Join Configuration

Before applying the Offline Domain Join configuration, Workspace ONE Intelligent Hub performs a check to determine whether the device is already joined to an Active Directory (AD) or Entra ID domain. - If the device is not domain joined, the configuration will be applied. - If the device is already domain joined, the configuration will be skipped.

To include domain join as part of a broader workflow, avoid assigning the configuration directly to a corporate (work) device outside that workflow.

Note: For devices not configured with Windows Autopilot, a manual reboot is required after applying the Offline Domain Join configuration.

Troubleshooting

To investigate issues with the Offline Domain Join process, you can gather and review logs directly from the device and analyze relevant system components.

Steps to Troubleshoot Collect Workspace ONE Intelligent Hub logs from the following paths: - C:\ProgramData\AirWatch\UnifiedAgent\Logs\DomainJoin-%TIMESTAMP%.log - C:\ProgramData\AirWatch\UnifiedAgent\Logs\DSM-%TIMESTAMP%.log - C:\ProgramData\AirWatch\UnifiedAgent\Logs\TaskScheduler-%TIMESTAMP%.log

Inspect Workflow Log Entries if the Domain Join Config was assigned via Freestyle Workflow In the workflow logs, search for the following key phrase to confirm event processing: “Received domain join hub cache event”

Capture a Fiddler Trace A Fiddler trace may help identify communication issues or failures in the API calls between Workspace ONE components and the device.

Check Registry Settings Review the following registry path for Workspace ONE domain join-related configurations: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AIRWATCH

These artifacts provide a detailed view of what occurred during the domain join attempt and help isolate root causes in case of failure.

Intel Chip To Cloud Integration for Windows on SaaS

Use the new **Integrations** area of Workspace ONE UEM to integrate your Intel vPro Chip To Cloud (C2C) deployment with Workspace ONE UEM. Intel Chip to Cloud manages those Windows devices that are equipped with Intel vPro chipset. Intel C2C 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 C2C, view your Intel C2C and your Workspace ONE UEM managed devices and manage those devices from a single console.

Prerequisites

- This feature is only a SaaS offering and is not supported for on-premise at this time
- Supports Windows Desktop devices only
- Enable the Intel Chip to Cloud integration card in Workspace ONE UEM
- Configure the Intel vPro Profile and deploy to devices with Intel vPro
- On the Intel vPro devices Install all necessary drivers and configure Bios settings properly to utilize Intel Chip to Cloud capabilities thru Workspace ONE UEM

Configure the Intel vPro Integration Card

Enabling the Chip to Cloud capabilities begins with configuring your Workspace ONE UEM environment to interact with Intel Endpoints Cloud Services. Workspace ONE UEM will interact with the Intel ECS APIs to create a container and manage device activation and capabilities. Enabling the integration card only requires click-thru actions to read the terms and conditions and review of capabilities. Once completed the only remaining configuration is included in the Intel vPro profile and can be deployed to new valid vPro endpoints using the profile deployment flow.

Procedure

1. In Workspace ONE UEM, select the applicable organization group.
2. Go to: **Groups & Settings > Integrations**.
3. Select Setup on the IntelvPro card to configure the integration.
4. Click **Next** and read the information regarding the connection to the Intel cloud then **Save**.
5. Workspace ONE UEM communicates with Intel Endpoint Cloud Services to complete the pre-requisite and enable the Intel Chip to Cloud functionality.
    - Workspace ONE UEM provides the details of the tenant and necessary authentication mechanisms.
    - You can view the time/date of successful configuration on the tab of the Intel vPro Integration card.

Configure the Intel vPro Profile

Configure the Intel vPro profile for Windows platform to allow Intel Chip to Cloud functionality on Intel vPro devices. Using this functionality requires you to configure and enable the Intel vPro profile.

Procedure

1. On the Resources tab, select **Profiles**.
2. Go to: **Devices > Profiles & Resources > Profiles > ADD > ADD Profile > Windows > Windows Desktop > Device Profile**.
3. Configure the profile's General settings.

4. Select the Intel vPro payload from the list.
5. Click Enable.
6. Select the appropriate assignment groups to ensure that the profile is deployed ONLY to devices with Intel vPro.
7. Select **Save & Publish**.

Execute Intel C2C Operations on the Managed Devices From the Console

Workspace ONE UEM lists the Intel Chip to Cloud capabilities in the Device Details View.

Prerequisites

All the devices to be managed by Intel Chip to Cloud must meet the listed conditions.

- The devices must have the Intel vPro chipset.
- The devices must have the Intel AMT firmware, version 11 or later.
- For devices already enrolled, they must have properly configured Intel AMT firmware and OEM Bios.

Procedure

From the Device List View, select one or more Intel vPro enrolled devices to view and use the operations listed in theMore Actionsmenu. The device selection drives the availability of the Intel vPro operations. The console lists available operations depending on the device's capabilities. Also, device capabilities may be affected by BIOS/ Firmware settings.

1. In the Workspace ONE UEM console, go to: **Devices > Details** to see the Intel vPro capabilities.
2. From the More Actions menu, find the listed operations.
    - Power On
    - Power Off
    - Power Cycle
    - Reset
    - Remote keyboard, video, mouse (KVM) control

Intel C2C Operation Behaviours

- The Intel C2C operations are sent from Workspace ONE UEM to the Intel Endpoint Cloud Service to the device to perform the actions.
- When you select the Remote KVMoperation, this action takes you to a separate tab within Workspace ONE UEM to interact with the device. The appropriate client control mode 6 digit code is required for KVM functionality.