VMware AirWatch Integration with Apple Configurator 2 Guide

Using Apple Configurator 2 and Workspace ONE UEM to simplify mass deployments

Workspace ONE UEM v9.4

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

Table of Contents

Chapter 1:
Overview

Introduction to Workspace ONE UEM and Apple Configurator 2

Workspace ONE UEM integrates with Apple Configurator to enable you to supervise and manage scaled deployments of Apple iOS devices. Administrators can create configuration profiles, import existing profiles from the iPhone Configuration Utility, install specific operating system versions and enforce iOS device security policies.

Install and run Apple Configurator 2 from a macOS laptop to integrate with the Workspace ONE UEM console to supervise and configure one or many devices at the same time.

- Install the Workspace ONE UEM MDM profile as part of the configuration to enroll devices silently.
- Supervise dedicated line-of-business devices that are shared among different users.
- Create configuration profiles to change device settings for Wi-Fi networks, preconfigure mail and Microsoft Exchange settings, and more.
- Distribute public apps without entering an Apple ID on the device using Configurator.
- Create blueprints to automate device management. Use blueprints as templates to configure profiles and application and push them quickly to devices
- Add Supervision to devices and take advantage of even more management capabilities including showing or hiding applications, modifying the device name, wall paper, passcodes, keyboard short cuts and more.
- Back up user settings and app data, including new user-created data using Configurator.

Apple Configurator 2 also works with Apple's Device Enrollment Program (DEP) to automate Mobile Device Management (MDM) enrollment and the Volume Purchase Program (VPP) by assigning managed licenses apps to devices.

Apple Configurator 2 Integration Requirements

- A Basic or Directory user account with staging settings enabled if you are staging devices for end users.
- A macOS computer, which will be used to connect to iOS devices using Apple Configurator 2 running macOS EL Capitan or later and iTunes 12.3 or later.
- The latest version of Apple Configurator 2 available in the App Store and access to the Workspace ONE UEM console.

  These instructions are based on the use of Apple Configurator 2 version 2.2.1. Any other versions of the software may function differently.

  Important: Integration with any third-party software product is not guaranteed, and is dependent upon the proper functioning of those third-party solutions.

- iOS devices including iPad, iPhone, iPod touch, Apple TV (2nd generation or later)
- USB cable or USB 2.0 or high speed hubs or carts to connect devices

Supervised Devices and MDM

Benefits of Supervised Mode

Once a device is supervised and enrolled in Workspace ONE UEM, the administrator has the following enhanced features available for configuration when compared to normal devices.

- **Elevated Restrictions over MDM**
  - Prevent User from Removing Applications. Removing applications can also be restricted locally on the device using restrictions under System Configuration.
  - Prevent AirDrop.
  - Prevent users from modifying iCloud and Mail account settings which prevents account modification.
  - Disable iMessage.
  - Set iBookstore Content rating restrictions.
  - Disable Game Center and iBookstore.
- **Enhanced Security**
  - Prevent end users from visiting websites with adult content in Safari.
  - Restrict which devices can connect to specified AirPlay destinations, such as Apple TVs.
  - Prevent the installation of certificates or unmanaged configuration profiles.
  - Force all device network traffic through a global HTTP proxy.
- **Kiosk Mode**
  - Lock down devices to one app with single app mode and disable the home button.
- **Customize Wallpaper and Text on Device**
- **Enable or Clear Activation Lock**

For a complete list of features and functionality available to supervised and unsupervised devices, refer to the iOS Functionality Matrix: Supervised vs. Unsupervised on page 18.

Chapter 2:
Integration with AC2 and Device Enrollment Program

Apple Configurator 2 with the Device Enrollment Program

You may optionally use Apple Configurator 2 in the conjunction with Apple's Device Enrollment Program.

Use both of these deployment programs together to automate device enrollment, add Supervision, prevent the removal of an MDM profile, and to add supervised identities to devices.

Supervised Identities for Configurator 2 Devices

Apple Configurator 2 allows you to supervise devices and pair them with other Apple Configurator 2 workstations. Each workstation must also have a matching supervision identity for authentication. The identity is applied to devices when enrolled using a DEP profile or paired with an Apple Configurator 2 workstation. If the wrong identity is applied to a device, the device must be device wiped to change the identity.

Create a Supervision Identity for Apple Configurator 2

Create a supervision identity to add your organization's information to devices so that it will appear for users. Then, add supervision identities to other Apple Configurator 2 workstations to securely configure devices.

1. Navigate to **Apple Configurator 2 > Preferences**.
2. Select **Organizations**.
3. Select the **+** action button
4. Follow the prompts to create a new supervision identity. Select **Done**.
5. Enter credentials and select **Update Settings**.
6. Select the **gear** button in the **Organizations** window.
7. Select **Export Supervision Identity** and choose where to save it. Select Save.
8. Add a **Password** to the identity. This .p12 file will be uploaded to the UEM console when creating a Device Enrollment Program profile.

Chapter 3:
Automated Enrollment

Automated Enrollment for Apple Configurator

Configure devices to allow for automatic enrollment using Apple's Device Enrollment Program (DEP).

Before beginning, ensure that you uploaded a supervised identity when setting up DEP. Then, navigate to Apple Configurator 2 on your desktop and create a Wi-Fi configuration profile for your organization's network and a blueprint with MDM information and a supervised identity attached. For more information on Wi-Fi profiles and blueprints, see the Apple Configurator 2 help documentation.

Configure Automated Enrollment with Apple Configurator 2

Use functionality in Apple Configurator 2 to create a Wi-Fi profile and apply a blueprint that allows devices to automatically enroll with the UEM console.

1. Navigate to **File > New Profile** in Apple Configurator 2.
2. Select **Wi-Fi > Configure** and enter the profile information. Optionally, choose to sign the profile. Then save the profile configuration.
3. Navigate to **Blueprints > Edit Blueprints > New** to prepare a blueprint to apply to the profile.
4. Select the blueprint and select **Prepare**.
5. Choose **Automated Enrollment** from the Configuration drop-down menu. Select **Next**.
6. **Choose** the configuration profile that you just created. Select **Next**
   - If required, enter the credentials for the MDM server if Authentication was turned on when configuring a Device Enrollment Program profile.
7. Select **Prepare**.
8. Navigate to the device browser and select a device or device group.
9. Select **Actions > Apply** and choose the blueprint needed for enrollment. All blueprint actions and profiles are pushed to devices.

Chapter 4:
Manual Enrollment Options

Apple Configurator Manual Enrollment

Manual Enrollment refers to the process of manually creating user accounts and user groups for each of your organization's users. If your organization is not integrating Workspace ONE UEM with a directory service, this is how you create user accounts.

Set up manual enrollment through an MDM Enrollment Profile or an MDM Enrollment URL.

You can save time and effort of uploading individual user account details filling out and uploading CSV (comma-separated values) template files that contain all user information through the batch import feature.

Generate the MDM Enrollment Profile or Enrollment URL for Apple Configurator Enrollments

Create an enrollment profile for the desired organization group in the UEM console. The enrollment profile contains MDM enrollment settings along with a certificate that uniquely identifies the MDM server URL, group ID, and username to assign to the device.

1. Navigate to **Devices > Device Settings > Devices & Users > Apple > Apple Configurator**.
2. Select **Enable Automated Enrollment.** You may need to **Override** the current organization group to do this.
3. Select the **Platform** for staging.
4. Select the appropriate **Staging Mode** depending on how the device is going to be used. Pre-register devices by selecting **None** or **Single User** mode to pre-assign an end user to each device.

   If you do not register any devices, the enrollment user is dependent on the Staging Mode selected below:

   - **None** – Does not stage device for other users. For non-registered devices, all devices will be enrolled under the Default Enrollment User. In this case, only non-staging users are available as default staging user options.

     Important: If you do not pre-register your devices and select **None** and specify a default enrollment user, then all devices that receive the .mobileconfig file will be enrolled to that user. To ensure devices are enrolled to distinct users, pre-register them to specific users or create a staging user account and select **Single User** as your **Staging Mode**.

   - **Single User** – Stages device for a single, known or unknown user. Only staging users are available as Default Enrollment User options. When end users open the AirWatch Agent, they must enter credentials to fully enroll the staged device. At that time, the device details will update in the UEM console and the device is associated with that end user.
   - **Multi User** – Places device into Shared Device Mode. This stages the device for multiple, known or unknown users. Only staging users are available as Default Enrollment User options. When end users open the AirWatch Agent, they must enter credentials to check out the device for use.

5. Select **Copy** and follow the prompt to copy the **MDM Server URL**. Save this information so you can paste into an Apple Configurator 2 blueprint later.

   OR

   Select **Export** to save a **.mobileconfig** file that includes the name of the organization group.

- If you performed this step on a macOS computer, note that your macOS device may display a System Preferences window asking you to install the profile. Select **Cancel**.
- If you performed this step on a Windows PC, then transfer the file to the macOS computer that is running Apple Configurator 2.

6. Select **Save and Copy URL** to save the staging settings.

Prepare a Blueprint to Enroll with an MDM Profile

Use Apple Configurator 2 on the staging macOS computer to manually prepare devices. This workflow allows you to enroll devices, add supervision and choose what screens are seen during device's Setup Assistant.

1. Navigate to **File > New Profile** in Apple Configurator 2.
2. Select **Wi-Fi > Configure** and enter the profile information. Optionally, choose to sign the profile. Then save the profile configuration.
3. Navigate to **Blueprints > Edit Blueprints > New** to prepare a blueprint to apply to the profile.
4. **Name** this blueprint *Prepare*.
5. Select the blueprint and select **Prepare**.
6. Choose **Manual** as the enrollment type. Select **Next**.
7. Select **Do not enroll in MDM**. Select **Next**.
8. Choose the **Server** for device management.
9. Select **supervision** to the management capabilities.
10. Select whether to **Allow devices to connect to other computers**. Select **Next**.
11. Choose the **Organization** to assign devices. Select **Next**.
12. Configure the **iOS Setup Assistant** steps by selecting which screens are available to the end user.
13. Select **Prepare**.
14. Select **Add > Profiles** in the Apple Configurator 2 window.
15. Choose the Wi-Fi profile that you created earlier and add it to the blueprint.

Next, deploy this blueprint using the steps found in Deploy Enrollment Profiles for Apple Configurator 2 Enrollments on page 13.

Then Add an Enroll Blueprint with Add an Enroll Blueprint to Enroll with an MDM Profile on page 12.

Add an Enroll Blueprint to Enroll with an MDM Profile

This is the second step to enrolling with an MDM profile through Apple Configurator 2. Create an *Enroll* blueprint in addition to the *Prepare* blueprint you created earlier and push these two blueprints to devices together.

1. Navigate to **Blueprints > Edit Blueprints > New** to prepare a blueprint to apply to the profile.
2. **Name** this blueprint *Enroll*.
3. Select the blueprint and select **Add > Profiles**.
4. Choose the .mobileconfig profile that you created in the UEM console and add it to the blueprint. Do not prepare the blueprint.

Deploy the enrollment profiles using Deploy Enrollment Profiles for Apple Configurator 2 Enrollments on page 13.

Prepare the blueprint to enroll with an MDM profile, using Prepare a Blueprint to Enroll with an MDM Profile on page 12.

Prepare a Blueprint to Enroll with an Enrollment URL

Configure devices so that users can enroll directly in to an organization group instead of adding an MDM profile to the device.

1. Navigate to **Blueprints > Edit Blueprints > New** to prepare a blueprint to apply to the profile.
2. Select the blueprint and select **Prepare**.
3. Name the blueprint *Enroll*.
4. Choose **Manual** as the enrollment type. Select **Next**.
5. Choose **New Server** from the drop-down menu. Select **Next**.
6. Enter the **Name** of the new server
7. Paste the enrollment **URL** that was generated in the UEM console into the text box.
8. Add the anchor certificates as required.
9. Select **supervision** to the management capabilities.
10. Select whether to **Allow devices to connect to other computers**. Select **Next**.
11. Choose the **Organization** to assign devices. Select **Next**.
12. Configure the **iOS Setup Assistant** steps by selecting which screens are available to the end user.
13. Select **Prepare**.
14. Select **Add > Profiles** in the Apple Configurator 2 window.
15. Choose the Wi-Fi profile that you created earlier and add it to the blueprint.

Next, add an Enroll blueprint using Add an Enroll Blueprint to Enroll with an MDM Profile on page 12.

Deploy Enrollment Profiles for Apple Configurator 2 Enrollments

Configure device for enrollment by deploying profiles to devices. Configure devices with an enrollment profile by pushing both the *Prepare* and *Enroll* blueprint, or, configure devices to enroll through a URL by pushing the *Enroll* blueprint that was set up with an enrollment URL.

1. Connect iOS devices to the macOS staging computer using USB. The number of devices attached to staging computer appears in a badge.
2. Navigate to the device browser and select a device or device group.
3. Select **Actions > Apply** and choose the **Prepare** blueprint.
4. If you are configuring devices with an enrollment profile, repeat the previous step and choose the **Enroll** blueprint. The devices are configured with settings from the **Prepare** blueprint and enrolled using the profile added to the **Enroll** blueprint.

Chapter 5:
Enrolling Devices

Apple Configurator Device Enrollment

Once you have selected and set up your device enrollment method, you can begin enrolling devices.

Enrolling devices involves the following tasks:

- Push the AirWatch Agent to devices using AirWatch Agent Enrollment on page 16
- Enroll devices into Workspace ONE UEM using Apple Configurator End User Device Enrollment on page 16
- Verify Configurator 2 Device Enrollment into Workspace ONE UEM on page 16
- Remove Supervision from a Configurator 2 Device on page 16
- Uploading a signed profile to the Workspace ONE UEM console.

AirWatch Agent Enrollment

After you configure devices for enrollment either with an MDM profile or URL, any profiles, apps, or other settings you configured in the UEM console need to be pushed using the UEM console so they are assigned to the staging user.

At a minimum, push the AirWatch Agent as a public, managed application from the UEM console, so that end users can enroll their devices when ready.

Apple Configurator End User Device Enrollment

After installing the AirWatch Agent, end users can enroll into Workspace ONE UEM depending on the staging method you selected earlier.

- If you preregistered the device, then it should be automatically assigned to the user it is associated with in the UEM console.
- If you selected **None** as the staging mode, the device is already enrolled to the Default Enrollment User you selected.
- If you did not preregister devices and opted for **Single User Staging**, then users are prompted to enter their credentials when they enroll using the AirWatch Agent.
- If you selected **Multi User Staging**, then the device will launch into Shared Device mode, where end users can enter their credentials to check the device out.

Verify Configurator 2 Device Enrollment into Workspace ONE UEM

Once the devices are either prepared or supervised using Apple Configurator 2, you can view all enrolled devices in the UEM console. Once the devices populate, administrators can manage and deploy updates and apps to all the devices using Workspace ONE UEM.

Remove Supervision from a Configurator 2 Device

According to Apple's Configurator 2 documentation, you can remove the Supervised status of a device, but doing so erases all content and settings, including apps and media. Therefore, if you want to preserve the data on the device, you

should make a backup of it first. Note that a backup of a supervised device can be restored only to another supervised device.

To remove supervision from a device, open Configurator 2, select the device, and then select **Actions > Advanced > Erase all content and settings**. This will remove the supervision and reset the device to the default factory settings.

Appendix:
iOS Functionality Matrix: Supervised vs. Unsupervised

The following table shows all the available iOS profile functionality that you can control using the UEM console and the minimum iOS version that applies.

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Passcode			
Passcode settings	✓		-
Wi-Fi			
Wi-Fi settings	✓		-
Auto-Join	✓		iOS 7
Wi-Fi Hotspot 2.0 settings	✓		iOS 7
Proxy settings	✓		iOS 7
QOS Marking Policy	✓		iOS 10
VPN			
VPN settings	✓		-
Per-App VPN	✓		iOS 7
Connect automatically	✓		iOS 7
Email			
Email settings	✓		-
Prevent Moving Messages	✓		iOS 7

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Disable recent contact sync	✓		iOS 7
Prevent Use In 3rd Party Apps	✓		iOS 7
Use S/MIME	✓		iOS 7
Exchange ActiveSync			
EAS settings	✓		-
Use S/MIME	✓		iOS 7
Per-Message S/MIME	✓		iOS 8
Prevent Moving Messages	✓		iOS 7
Prevent Use In 3rd Party Apps	✓		iOS 7
Disable recent contact sync	✓		iOS 7
Prevent Mail Drop	✓		iOS 9
Default Calling App	✓		iOS 10
LDAP			
LDAP settings	✓		-
CalDAV			
CalDAV settings	✓		-
Subscribed Calendars			
Subscribed Calendar settings	✓		-
CardDAV			

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
CardDAV settings	✓		-
Web Clips			
Web Clip settings	✓		-
Credentials			
Credentials certificate settings	✓		-
SCEP			
SCEP settings for certificate authority	✓		-
Global HTTP Proxy			
Global HTTP Proxy settings		✓	iOS 7
Single App Mode			
Single App Mode – Lock device into a single app		✓	iOS 7
Optional settings for "Lock device into a single app"		✓	iOS 7
Autonomous single app mode		✓	iOS 7
Web Content Filter			
Web Content Filter settings (Whitelist, Blacklist, Permitted URLs)		✓	iOS 7
Web Content Filtering with 3rd Party Provider		✓	iOS 8
Managed Domains			
Managed Email Domains	✓		iOS 8
Managed Web Domains	✓		iOS 8

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Managed Safari Password Domains	✓		iOS 9.3
Network Usage Rules			
Network Usage Rules	✓		iOS 9
macOS Server Accounts			
macOS Server Accounts	✓		iOS 9
Single Sign On			
Single Sign On settings with Kerberos authentication	✓		iOS 7
Single Sign On settings with Renewal certificates	✓		iOS 8
AirPrint			
AirPrint destination settings	✓		iOS 7
AirPlay Mirroring			
AirPlay Destination settings (Whitelist)		✓	iOS 7
AirPlay Passwords	✓		
Access Point			
Advanced Access Point settings	✓		
App Installation Settings			
Silent App Installation		✓ +VPP	
Control Cellular Settings			
Voice Roaming	✓		iOS 7

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Data Roaming	✓		iOS 7
Personal Hotspot	✓		iOS 7
Wallpaper Settings			
Set Lock Screen Image		✓	iOS 7
Set Lock Screen Message		✓	iOS 9.3+
Set Home Screen Image		✓	iOS 7
Set Home Screen Layout		✓	iOS 9.3+
Notifications			
Notification settings		✓	iOS 9.3+
Queries and Commands			
Supervised status	✓		iOS 7
Personal Hotspot status	✓		iOS 7
Clear Activation Lock		✓	iOS 7
Clear Restrictions Passcode		✓	iOS 8
Detect OS Server Updates	✓		iOS 9
Force OS updates		✓	iOS 9 + DEP
Custom Fonts and Messaging			
Custom Font Installation	✓		iOS 7
Custom Enrollment Messages	✓		iOS 7

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Custom MDM Prompts	✓		iOS 7
Activation Lock Warning	✓		iOS 7