AirWatch Container

VMware Workspace ONE UEM

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

Introduction to the AirWatch Container 1

AirWatch Container offers a flexible approach to Bring Your Own Device (BYOD) management by pushing a secure work space to a personal device. Businesses can distribute Workspace ONE UEM applications and internal applications to the AirWatch Container for employees to use on their mobile devices.

Applications are visible inside and outside the AirWatch Container, but the enterprise applications are secure through a common SDK framework and a container passcode. These apps can interact seamlessly using single sign on authentication and can connect securely to the Internet through an app tunnel VPN. For instructions on how to use the AirWatch Container on a device, see the **VMware AirWatch Container User Guide for iOS** or the **VMware AirWatch Container User Guide for Android.**

Business Friendly

Create a practical and convenient solution for both businesses and employees.

- **Cost-effective for employers** – There is no need to buy or distribute corporate devices. Corporate data can be managed and monitored from the Workspace ONE UEM console.
- **Separation between work and play** – Personal data is separated from corporate data. AirWatch Container cannot track personal information and does not have the ability to wipe any personal items.
- **Intuitive user experience** – Add custom branding and customize menus. Allow users to seamlessly access apps without entering credentials every time.

Easily Managed

Take advantage of Workspace ONE UEM capabilities while allowing employees to use their devices freely.

- **Works with a hybrid device deployment** – Add AirWatch Container functionality to your current deployment. Add devices to the desired organization group to adopt the settings from that group.
- **Uses application-level management** – Productivity tools are granted to end users through Workspace ONE UEM apps and internal apps that are wrapped. These can be managed at the app-level rather than the device level.
- **No MDM Required** – End users do not have to worry about MDM restrictions. Employees can feel comfortable maintaining a single device for all their needs.

Security and Encryption

Standardize security and data loss prevention strategies across mobile devices.

- **Enforces Passcode/Encryption only within AirWatch Container** – Set complex passcodes that do not intrude on personal use because encryption is only enforced locally within the applications. iOS devices are secured with FIPS 140-2 encryption and allows for the use of Touch ID or EyeVerify.
- **Prevents data leakage outside of the app**– Use Workspace ONE UEM security controls built into Workspace ONE UEM apps, third-party integrated apps, wrapped apps, Web Clips and Bookmarks.
- **Incorporates email** – With AirWatch Inbox or IBM Notes Traveler on Android devices, end users can access email from their secure AirWatch Container instead of having to maintain two devices.

Requirements

Meet the following requirements to facilitate a successful deployment of AirWatch Container.

Supported Devices and Software
Android v4.4+ (KitKat)
iOS v6.0 +
Console Requirements
Workspace ONE UEM console v6.5 +
Other Requirements
AirWatch App Catalog enabled for iOS devices

AirWatch Container Enrollment 2

Each device in your organization's deployment must be enrolled before it can communicate with Workspace ONE UEM and access internal content and features. Enroll devices using one of three methods: Basic, Directory, Authentication Proxy. Also, AirWatch Container supports Autodiscovery and Security Assertion Markup Language (SAML) integration to help simplify enrollment.

Enrolling Devices

1. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment > Authentication**.
2. Select the Authentication Mode. Choose either **Basic**, or **Directory**, or **AuthenticationProxy** methods.
3. If desired, choose to use **Autodiscovery** to associate devices with an email domain.

To learn more, see the Autodiscovery section in the **VMware Workspace ONE UEM Mobile Device Management** guide.

Integrating with SAML

Choose to set up SAML 2.0 integration to enable single sign on architecture or federal authentication. Begin by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.

Note For information on SAML enrollment, see the **VMware AirWatch SAML Integration guide**.

This chapter includes the following topics:

- Terms of Use
- Configure Profile Payloads

Terms of Use

You can enforce terms of use (TOU) on all managed devices.

Ensure that all users with managed devices agree to the policy by defining and enforce terms of use (TOU). If necessary, users must accept the TOU before proceeding with enrollment, installing apps, or accessing the UEM console. The UEM console allows you to customize fully and assign a unique TOU to each organization group and child organization group.

The TOU displays during each device enrollment. Get access to the following functions.

- Set version numbers.
- Set platforms to receive the TOU.
- Notify users by email with the TOU updates.
- Create language-specific copies of the TOU.
- Create multiple TOU agreements and assign them to organization groups based on platform or the type of ownership.
- Meet the liability requirements of specific groups by customizing TOU.

Create Enrollment Terms of Use

You can create an agreement about terms of use (TOU) specific to enrollment purposes. You can also limit devices allowed for enrollment by device platform, ownership type, and enrollment type.

1 Ensure that your current active organization group is correct for the TOU you are creating.

2 Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and select the **Terms of Use** tab.

3 Select the **Add New Enrollment Terms of Use** button and complete the following options.

Setting	Description
Name	Enter a unique name for the new TOU.
Type	This option is pre-populated as **Enrollment**.
Version	This option is automatically tracked and populated accordingly.
Platforms, **Device Ownership**, and **Enrollment Type**	If you do not want to make your TOU for any specific category of device, then keep the default selection of **Any** for these options. If you prefer to specify a platform, ownership, and enrollment, you can select one or more of these categories and define the limitations specific to your TOU. ■ If you select **Selected Platform** option, then choose your desired platforms from the list that appears. Your TOU applies to the device platforms you select, excluding all others. ■ If you select **Selected Ownership Types** option, then you must choose your desired ownership from the list that appears. Your TOU applies to the ownership types you select, excluding all others. ■ If you select **Selected Enrollment Types** option, then you must choose your desired enrollment from the list that appears. Your TOU applies to the types of enrollment you select, excluding all others.

Setting	Description
Notification	Send an email to users whenever the TOU is updated by selecting this check box. The notification email is sent when you select **Save** in step 5.
Select Language	Optionally, for localization purposes, you may enter a TOU agreement for each language applicable to your needs by making a choice in the **Select Language** drop-down.

4 In the text box provided, enter your customized TOU.

The editor provides a basic text entry tool to create a TOU or paste in an existing TOU. To paste text from an external source, right-click the text box and choose **Paste as plain text** to prevent any HTML or formatting errors.

5 Select **Save**.

You can enforce MDM terms of use acceptance by creating a compliance policy for **MDM Terms of Use Acceptance**.

Configure Profile Payloads

Profile payload configurations helps to apply a specific restriction or setting to devices.

Use Mobile Device Management (MDM) functionality to enhance app performance by configuring a profile payloads in a two-step process. First, configure general settings. Then, specify the type of restriction or setting to apply to the device by selecting a payload from the list.

The available payloads and their configurable settings differ between platforms. This section provides a description of applicable payloads and brief instructions to help you get started.

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

2 Select the appropriate platform for the profile that you want to deploy.

3 Configure **General** settings to determine how the profile deploys, who receives it, and other overall settings.

4 Select and configure a **Payload**.

Payload	Description	iOS	Android
General	Create a customized profile for a device deployment.	✓	✓
Wi-Fi	Connect to corporate networks such as hidden, encrypted, or password protected networks using wifi profile.	✓	✓
EAS via AirWatch Inbox	Create an email profile for AirWatch Inbox.	✓	✓
EAS via IBM Notes	Create an email profile for IBM Notes.		✓
Webclips	Publish a profile of web clips to your devices.	✓	
Bookmarks	Create a web link your users can quickly access from your devices.		✓

1 For step-by-step instructions on configuring a specific **Payload** for a particular platform, refer to the applicable **Platform Guide**. Select **Save & Publish**.

Default SDK Configurations 3

Default SDK settings apply across Workspace ONE UEM and wrapped apps, providing a unified user experience on devices. Since the configured SDK settings apply to all Workspace ONE UEM and wrapped apps by default, configure the default SDK profile with the entire Workspace ONE UEM and wrapped app suite.

Not all Workspace ONE UEM apps support all available default SDK profile settings. Please keep this in mind while reading this example. Review the SDK features matrix In the case that

The recommendations provided apply to an app suite that includes:

- Workspace ONE Web
- Workspace ONE Content
- Enrolled devices
- Workspace ONE UEM or wrapped apps
- SDK settings

1 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.

2 Set **Authentication Type** to **Disabled** and **SSO** to **Enabled** to open apps without prompting the end user to enter credentials.

3 Set **Offline Access** to **Enabled** so that end users can open and use Workspace ONE UEM and wrapped apps when disconnected from Wi-Fi. Offline Workspace ONE UEM apps cannot perform downloads, and end users must return online for a successful download. Once enabled, configure the following:

Setting	Description
Maximum Period Allowed Offline	Choose an acceptable time frame for offline access before requiring the device to return online for a compliance and security check with Workspace ONE UEM.

4 Set **Compromised Protection** to **Enabled** to override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.

5 **Save** your settings.

6 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

7 Set **Branding** to **Disabled** to maintain the Workspace ONE UEM brand throughout your app suite.

1 **Save** your settings.

Configuring AirWatch Container Settings

1. Navigate to **Groups and Settings > All Settings > Apps > Container**.
2. Select whether to **Inherit** or **Override**
   - **Inherit** – Use the settings of the current organization group's parent OG.
   - **Override** – Edit and modify the current organization group's settings directly.
3. Configure the relevant settings:

Setting	Description
Notification	
Apple	Select to set iOS device system preferences.
Android	Select to set Android device system preferences.
Application Type	Leave the application type as **System** or select **Internal** to set system preferences. ■ **System** – Download this app type from an app store. ■ **Internal**– Upload this app type to the UEM console.
Application Name	Provide an app name for **Internal** applications. Navigate to **Apps & Books > Internal List View**and scan the list for an app name that matches the app name you entered. This list view only displays internal applications were uploaded with a matching APNs certificate.
Bundle ID	Review the auto-populated field. This Bundle ID matches the application bundle ID that was uploaded internally or selected from the drop-down menu.

4. **Save**.

Configuring and Deploying Applications

4

You can distribute applications to end users automatically once an app is activated in the UEM console or on-demand through an App Catalog.

For more on managing apps with the App Catalog, please see the **VMware Workspace ONE UEM Mobile Application ManagementGuide**.

Refer to the Chapter 5 SDK Profiles, Policies and Settings Compatibility for an extensive list of capabilities by platform, SDK and App Wrapping.

The following information applies to different types of apps you can publish:

- **Workspace ONE UEM applications** – These apps include Workspace ONE Content and Workspace ONE web.
- **Internal applications** – Internal apps can be wrapped apps or apps that you have integrated with the AirWatch SDK. Apps that are not wrapped must have a **Default Scheme** built into the app, which is extracted and saved when the app is uploaded to the UEM console.
  - Android end users are prompted to install all assigned internal apps automatically after enrollment.
  - For iOS devices, you must enable the App Catalog for applicable organization groups so internal apps can be launched directly from the AirWatch Container.

  Note Irrespective of the default scheme applied or not, the internal applications and public applications (other that Workspace ONE UEM applications) do not reside inside Container but will be seen on the device screen and App Catalog.

- **Public/Purchased applications** – Public apps are only available as on-demand, recommended apps. They are not considered containerized and do not support SSO, branding, console commands, or updated badges.
  - These apps can be installed from the AirWatch Container springboard if a **Default Scheme** is included in the application information in the UEM console. If the **Default Scheme** is not included in the application information, the app will be available in the App Catalog.
    - To review an application's **Default Scheme**, navigate to **Apps & Books > List View.** From the Actions menu, select **Edit** ✎ to see the application information.

  - If no default scheme populates in the application information, then contact the appropriate vendor for that information.

    Note Irrespective of the default scheme applied or not, the internal applications and public applications (other that Workspace ONE UEM applications) do not reside inside Container but will be seen on the device screen and App Catalog.

  To improve app functionality on Android devices, push Workspace ONE UEM applications to enrolled devices as managed apps from the UEM console, even if the apps have already been downloaded.

  For AirWatch Inbox on iOS devices, make sure the correct Default Scheme (**awemailclient**) has been entered in the UEM console.

  Note The Workspace ONE UEM Container for iOS does not support the deployment of iOS applications purchased through Apple's Volume Purchase Program (VPP).

- **Web Clips and Bookmarks** – Web Clips for iOS and Bookmarks for Android are hyperlinks to web addresses and appear as icons on the device springboard. Workspace ONE Web is required to open these links. If Workspace ONE Web has not been downloaded to the device, then the user will be prompted to download it to open these links.
  - Ensure that Web Clips or Bookmarks have the **Show in the App Catalog** checkbox selected in the appropriate payload in UEM console.

Managing AirWatch Container Devices from the Device Dashboard

Once AirWatch Container is enabled and users begin to enroll their personal devices, the UEM console detects those devices and displays the information on the Device Dashboard. Search for specific devices in your fleet that are AirWatch Container-only and perform AirWatch Container-specific actions on those devices.

Important When users unenroll from AirWatch Container, they must unenroll the app before deleting it. If AirWatch Container is simply deleted, the users' devices are still tracked in the UEM console.

Locate a single device from either the Device Dashboard or by searching for the device using the Global Search feature. Use the Filters to find all AirWatch Container-only devices if desired. The **List View** screen provides device information. From here, select multiple devices or select a specific device to perform applicable remote actions.

Lock SSO

End any current app sessions and prompt user to enter their passcode again.

If a user is no longer with the organization or if their device is lost or stolen, take immediate action and lock the SSO session. This forces the user to enter their credentials again.

Clear SSO Passcode

Clear the current passcode used to sign into apps and prompt the user to enter a new one.

Forgetting a passcode is the most common issue users face, but it is also the easiest to rectify. Use this action to reset a user's passcode and create a new one.

Enterprise Wipe

Unenroll the user from AirWatch Container and remove any application data from internal apps using the AirWatch SDK.

Similar to the Device Lock feature, Enterprise Wipe can be used if a device is lost or stolen. More than simply ending an SSO session, an enterprise wipe removes all organization-related content and features.

When a device is unenrolled from AirWatch Container, all internal apps and public apps remain on the device, but the data from the internal applications is deleted if theapps use the AirWatch SDK.

Push Email Profile

Send a newly configured or updated email profile to the device for access within AirWatch Container.

Email access is often a user's primary need when it comes to access on-the-go. Use the **Push Email Profile** action to send down new email credentials or updated credentials to ensure access is never lost.

Push Notifications

Send messages directly from the UEM console to AirWatch Container.

Send important notifications to end users' devices.

SDK Profiles, Policies and Settings Compatibility

5

AirWatch Container leverages several existing Workspace ONE UEM applications and features, each of which hosts a variety of available settings and policies **(Groups & Settings > All Settings > Apps > Settings and Policies)**. These settings also extend to wrapped applications and applications built with the AirWatch SDK

Settings and Policies Supported Options for Workspace ONE UEM Applications

The following matrix shows support for Workspace ONE UEM applications built with the Workspace ONE UEM SDK. Inbox refers to Workspace ONE UEM Inbox, and not VMware Boxer, which is not built with the Workspace ONE UEM SDK. You can configure similar settings for Boxer when deploying the application.

Table 5-1.

UI Label	Container		Workspace ONE Web		Workspace ONE Content	
	Android	**iOS**	**Android**	**iOS**	**Android**	**iOS**
Force Token For App Authentication: Enable	x	x	✓	✓	x	x
Passcode: Authentication Timeout	✓	✓	✓	✓	✓	✓
Passcode: Maximum Number Of Failed Attempts	✓	✓	✓	✓	✓	✓
Passcode: Passcode Mode Numeric	✓	✓	✓	✓	✓	✓
Passcode: Passcode Mode Alphanumeric	✓	✓	✓	✓	✓	✓
Passcode: Allow Simple Value	✓	✓	✓	✓	✓	✓
Passcode: Minimum Passcode Length	✓	✓	✓	✓	✓	✓
Passcode: Minimum Number Complex Characters	✓	✓	✓	✓	✓	✓

Table 5-1. (Continued)

UI Label	Container		Workspace ONE Web		Workspace ONE Content	
	Android	iOS	Android	iOS	Android	iOS
Passcode: Maximum Passcode Age	✓	✓	✓	✓	✓	✓
Passcode: Passcode History	✓	✓	✓	✓	✓	✓
Biometric Mode: Fingerprint	✓	x	✓	✓	✓	✓
Username and Password: Authentication Timeout	✓	✓	✓	✓	✓	✓
Username and Password: Maximum Number of Failed Attempts	✓	✓	✓	✓	✓	✓
Single Sign On: Enable	✓	✓	✓	✓	✓	✓
Integrated Authentication: Enable Kerberos	x	x	x	✓	x	x
Integrated Authentication: Use Enrollment Credentials	✓	✓	✓	✓	x	x
Integrated Authentication: Use Certificate	✓	✓	✓	**✓	x	x
Offline Access: Enable	✓	✓	x	✓	✓	✓
Compromised Protection: Enable	✓	✓	✓	✓	✓	✓
App Tunnel: Mode	✓	x	✓	✓	*✓	*✓
App Tunnel: URLs (Domains)	✓	x	✓	✓	*✓	*✓
Content Filtering: Enable	x	x	✓	x	x	x
Geofencing: Area	x	x	✓	✓	✓	x
DLP: Bluetooth	x	x	x	x	✓	x
DLP: Camera	x	x	x	x	✓	x
DLP: Composing Email	x	x	✓	✓	✓	x
DLP: Copy and Paste Out	x	x	✓	✓	✓	x
DLP: Copy and Paste Into	x	x	✓	✓	✓	x

Table 5-1. (Continued)

UI Label	Container		Workspace ONE Web		Workspace ONE Content	
	Android	iOS	Android	iOS	Android	iOS
DLP: Data Backup	x	x	x	x	✓	x
DLP: Location Services	x	x	x	x	✓	x
DLP:Printing	x	x	✓	x	✓	x
DLP: Screenshot	x	x	x	✓	✓	x
DLP: Third Party Keyboards	x	x	x	x	x	x
DLP: Watermark	x	x	x	x	✓	x
DLP: Limit Documents to Open Only in Approved Apps	x	x	✓	✓	✓	✓
NAC: Enable	x	x	✓	✓	x	x
NAC: Cellular Connection	x	x	✓	✓	x	x
NAC: Wi-Fi Connection	x	x	✓	✓	x	x
Branding: Enable	✓	✓	✓	x	✓	✓
Branding: Toolbar Color	✓	✓	x	x	✓	✓
Branding: Toolbar Text Color	✓	✓	x	x	✓	✓
Branding: Primary Color	x	x	✓	x	✓	✓
Branding: Primary Text Color	✓	✓	✓	x	✓	✓
Branding: Secondary Color	✓	x	x	x	✓	✓
Branding: Secondary Text Color	x	x	✓	x	✓	✓
Branding: Organization Name	x	x	✓	x	✓	✓
Branding: Background Image iPhone and iPhone Retina	✓	x	x	x	✓	x
Branding: Background Image iPhone 5 (Retina)	✓	x	x	x	✓	x
Branding: Background Image iPad and iPad (Retina)	✓	x	x	x	✓	x

Table 5-1. (Continued)

UI Label	Container		Workspace ONE Web		Workspace ONE Content	
	Android	**iOS**	**Android**	**iOS**	**Android**	**iOS**
Branding: Background Small, Medium, Large, and XLarge	x	✓	x	x	x	✓
Logging: Enable	x	x	x	x	✓	x
Logging: Logging Level	x	x	x	x	✓	x
Logging: Send Logs Over Wi-Fi	x	x	x	x	✓	x
Custom Settings: Enable	x	x	x	x	x	x
SDK App Compliance: Enable	x	x	x	x	x	x
Compromised Protection: Enable	✓	✓	✓	✓	✓	✓
Offline Access: Enable	✓	✓	x	✓	✓	✓

*✓ This option is supported but is not configured using Settings and Policies.

**✓ This option requires Android Ice Cream Sandwich and KitKat.