

# SDK and Managing Applications

VMware Workspace ONE UEM 2203

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

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1** App Management with VMware Workspace ONE SDK Settings 4
- 2** Supported SDK Settings and Policies by Platform 8
- 3** Security Policies Profiles for the SDK 11
- 4** Settings Profiles for the SDK 27
- 5** SDK App Compliance Profiles for the SDK 32
- 6** Privacy Policies for Data Collection in Productivity Applications 35

# App Management with VMware Workspace ONE SDK Settings

# 1

The **Settings and Policies** area in VMware Workspace ONE<sup>®</sup> UEM powered by AirWatch has settings that control security, application behaviors, and the retrieval of specified data in apps that use the Workspace ONE SDK framework. To deploy Workspace ONE UEM features to apps, assign the default SDK profile or a custom SDK profile set with your Workspace ONE SDK settings.

Apply these SDK features and settings to the listed applications.

- Applications built with the Workspace ONE SDK
- Workspace ONE productivity apps
- Applications wrapped by the AirWatch App Wrapping engine

## Types of SDK Profiles

Workspace ONE UEM has two types of SDK profiles - default and custom. To select the type of SDK profile, determine the scope of deployment.

- Default profiles work well across organization groups, applying to large numbers of devices.

Find the settings for the default SDK profile in **Groups & Settings > All Settings > Apps > Settings and Policies** and then select **Security Policies**, **Settings**, or **SDK App Compliance**. You can apply these default profile options across all the Workspace ONE UEM applications in an organization group. Options shared across all organization groups are easier to manage and configure because you can manage them from a single profile.

- Custom profiles work for individual devices or for small numbers of devices with applications that require special mobile application management (MAM) features. Although they offer granular control, custom profiles require separate input and maintenance.

You can configure various types of custom profiles.

- **SDK Profile** - This profile offers most options found in the default SDK profiles. They work for applications that have the Workspace ONE SDK embedded in them.
- **Application Profile** - This legacy profile was used to configure certificate authorities or other credential sources for SDK-built apps. However, to apply certificate configurations to your SDK-built apps, consider using the **Credentials** option in an **SDK Profile**.
- **App Wrapping Profile** - This profile configures your apps wrapped with the AirWatch App Wrapping service.

## Requirements to Use SDK Features

You must complete several tasks to successfully use SDK features with your SDK and productivity apps.

- 1 You must configure either the default SDK profile or create a custom SDK profile.
- 2 You must assign the profile to your SDK or productivity app.

Assign the profile when you upload or edit the application to the Workspace ONE UEM console in the **Apps** section. When you change the default or custom profile, Workspace ONE UEM applies these edits when you select **Save**. Changes to end-use devices can take a few minutes to deploy. Users can close and restart Workspace ONE UEM applications to receive updated settings.

---

**Note** There is no process to use push notifications to trigger devices to retrieve SDK policy updates. The console includes a scheduler task to fetch and send SDK settings and policies to devices. To get policy updates immediately, users can stop and start their SDK-built apps.

---

- a Navigate to **Resources > Apps > Native > <App Type>**.
- b Add or edit an application.
- c Select a profile on the **SDK** tab. You can use the default SDK profile or you can use a custom profile.
  - To use the default SDK profile, select the **Android Default Settings @ Global** or the **iOS Default Settings @ Global** from the **SDK Profile** list.
  - To use a custom SDK profile, select it from the **SDK Profile** list.
- d Make other configurations and then save the application and create assignments for its deployment.

- 3 You must assign the default SDK profile to the Workspace ONE Intelligent Hub. You configure the default SDK profile in the console at **Groups & Settings > All Settings > Apps > Settings and Policies** and then select **Security Policies, Settings, or SDK App Compliance**. If you do not assign the default SDK profile to the Workspace ONE Intelligent Hub to apply SDK configurations, your SDK configurations in **Settings and Policies** do not work in applications.

---

**Note** You cannot use custom SDK profiles with the Workspace ONE Intelligent Hub. The Workspace ONE Intelligent Hub only supports the default profile set in either the **Security Policies, Settings, or SDK App Compliance** sections of **Settings and Policies**.

---

**Note** The system assigns the default SDK profile for iOS to the Workspace ONE Intelligent Hub for iOS by default. You do not need to manually apply this mechanism. The steps to assign the default SDK remain in the documentation so you know where the settings reside. This mechanism is not in place for the Android platform.

---

- Workspace ONE Intelligent Hub for iOS
  - 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Intelligent Hub Settings**.
  - 2 Set the **SDK Profile** option to the default profile by selecting **iOS Default Settings @ Global**.
- Workspace ONE Intelligent Hub for Android
  - 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Intelligent Hub Settings**.
  - 2 Set the **SDK Profile** option to the default profile by selecting **Android Default Settings @ Global**.

## What Happens if You Do Not Assign Your SDK or Productivity Apps an SDK Profile?

Workspace ONE UEM assigns profiles at the closest organization group (OG). You can control which profile your apps get (and what SDK functionality the apps use) when you upload and deploy them in the **Apps** section of the console. Assigning the SDK profile to the app in the **Apps** section is best.

If you do not assign an SDK profile (default or custom) to your SDK and productivity apps in the **Apps** section of the console, then Workspace ONE UEM assigns the default SDK profile configured at the OG closest to the device.

Another scenario that influences the SDK features your SDK and productivity apps use occurs if you have the same app at the parent and its child OG. If you do not assign an SDK profile to an app in a child OG that is also in the parent OG, there are various outcomes.

**Table 1-1. Apps Deployed Both at Child and Parent OGs, What SDK Profile Does Your App in the Child OG Receive?**

Is the SDK profile (custom or default) set in the Apps section for the Child version of the app?	Does the parent version have the SDK profile set in Apps?	Result
No	Yes	Devices that enroll in the child OG receive the app with the parent OG version of the SDK profile set in the <b>Apps</b> section.
No	No	Devices that enroll in the child OG receive the app with the default SDK profile set at the child OG.

# Supported SDK Settings and Policies by Platform

## 2

Use the default settings in the **Policies and Settings** area to apply Workspace ONE SDK functionality to SDK-built applications, Workspace ONE UEM productivity applications, or wrapped applications. Use the matrix to see if an SDK default setting is supported for Android and iOS.

The table lists the default settings supported by the SDK. For information about supported features for Workspace ONE UEM applications, see the content for that application.

**Table 2-1. Key to Matrix Values**

Value	Description
Supported	The SDK reads and enforces the setting in the SDK-built app.
Not Supported	The SDK does not read the setting, it does not enforce the setting, and it does not pass the setting from the console to an SDK-built app.
<i>Passes</i>	The SDK passes the setting from the Workspace ONE UEM console to the SDK-built app. The app reads and enforces the setting.

**Table 2-2. Supported Settings and Policies Options By Platform**

SDK Default Payload	Workspace ONE SDK for Android	Workspace ONE SDK for iOS (Swift)
Force Token For App Authentication	Supported	Supported
Passcode: Authentication Timeout	Supported	Supported
Passcode: Maximum Number of Failed Attempts	Supported	Supported
Passcode: Passcode Mode Numeric	Supported	Supported
Passcode: Passcode Mode Alphanumeric	Supported	Supported
Passcode: Allow Simple Value	Supported	Supported
Passcode: Minimum Passcode Length	Supported	Supported
Passcode: Minimum Number Complex Characters	Supported	Supported



Table 2-2. Supported Settings and Policies Options By Platform (continued)

SDK Default Payload	Workspace ONE SDK for Android	Workspace ONE SDK for iOS (Swift)
Passcode: Maximum Passcode Age	Supported	Supported
Passcode: Passcode History	Supported	Supported
Passcode: Biometric Mode	Supported	Supported
Username and Password: Authentication Timeout	Supported	Supported
Username and Password: Maximum Number of Failed Attempts	Supported	Supported
Single Sign On	Supported	Supported
Integrated Authentication: Enable Kerberos	<b>Not Supported</b>	<b>Not Supported</b>
Integrated Authentication: Use Enrollment Credentials	Supported	Supported
Integrated Authentication: Use Certificate	Supported	Supported
Offline Access	Supported	Supported
Compromised Detection	Supported	Supported
AirWatch App Tunnel	Supported	Supported
Geofencing: Area	<i>Passes</i>	Not Supported
DLP: Bluetooth	<i>Passes</i>	Not Supported
DLP: Camera	<i>Passes</i>	Supported
DLP: Composing Email	<i>Passes</i>	<i>Passes</i>
DLP: Copy and Paste Out	Supported	Supported
DLP: Copy and Paste Into	Supported	Supported
DLP: Data Backup	<i>Passes</i>	<b>Not Supported</b>
DLP: Location Services	<i>Passes</i>	Not Supported
DLP: Printing	<i>Passes</i>	Supported
DLP: Screenshot	Supported	<b>Not Supported</b>
DLP: Third Party Keyboards	Not Supported	Supported
DLP: Watermark	Supported	Supported
DLP: Limit Documents to Open Only in Approved Applications	Not Supported	<i>Passes</i>
NAC: Cellular Connection	Supported	Not Supported

Table 2-2. Supported Settings and Policies Options By Platform (continued)

SDK Default Payload	Workspace ONE SDK for Android	Workspace ONE SDK for iOS (Swift)
NAC: Wi-Fi Connection	Supported	Not Supported
Branding	Supported	Supported
Logging	Supported	Supported
Analytics	Supported	Supported
SDK App Compliance: Application Version	Not Supported	Supported
SDK App Compliance: Application Inactivity	Supported	Supported
SDK App Compliance: OS Version	Not Supported	Supported
SDK App Compliance: Security Patch Date	Not Supported	Not Supported

# Security Policies Profiles for the SDK

# 3

**Security Policies** profiles offer security controls for SDK-built apps. Control security with authentication methods, tunneling app traffic, and restricting access to features with data loss prevention.

## Navigation

In the Workspace ONE UEM console, you can find these default SDK settings in **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.

## Assign the Default SDK Profile to the Workspace ONE Intelligent Hub

Control and apply SDK functionality with the Workspace ONE Intelligent Hub and the default SDK profile.

---

**Note** You cannot use custom SDK profiles with the Workspace ONE Intelligent Hub. A profile set in **Groups & Settings > All Settings > Apps > Settings and Policies > Profiles** is a custom SDK profile. It is not the default SDK profile. The Workspace ONE Intelligent Hub only supports the default profile set in either the **Security Policies**, **Settings**, or **SDK App Compliance** sections of **Settings and Policies**.

---

The Workspace ONE Intelligent Hub works as a "broker application" for SDK features, such as SSO. You must configure the default SDK profile with the features you want the Workspace ONE Intelligent Hub to apply to apps. If you do not set the Workspace ONE Intelligent Hub to use the default SDK profile, then the system does not apply your settings you configured in the **Settings and Policies** section.

## SDK Profile Configurations Must Match To Work

The configuration in the SDK profile assigned to the productivity app must match the configuration in the default SDK profile you assigned to your Workspace ONE Intelligent Hub. If configurations do not match, then the SDK feature does not work in your Workspace ONE productivity app.

For example, if you want managed apps to use SSO, ensure that the default SDK profile assigned to your Workspace ONE Intelligent Hub has SSO enabled. If you have assigned a custom SDK profile to a productivity app, you must enable SSO in the custom profile. SSO does not work if the profiles assigned to the Hub or the productivity app have SSO deactivated.

## Force Token for App Authentication

This setting controls how the system allows users to access SDK-built applications, either initially or through a forgotten-passcode procedure. When enabled, the system forces the user to generate an application token through the Self-Service Portal (SSP) and does not allow user name and password. This setting does not force the reset of the enrollment token.

## Authentication Type

Select an authentication method that meets the security needs of your network. The passcode gives device users flexibility while user name and password offers compatibility with the Workspace ONE UEM system. If security is not an issue, then you do not have to require an authentication method.

**Table 3-1. Descriptions of Authentication Items**

Setting	Description
Passcode	Designates a local passcode requirement for supported applications. Device users set their passcode on devices at the application level when they first access the application.
User name and Password	Requires users to authenticate to supported applications using their Workspace ONE UEM credentials. Set these credentials when you add users in the <b>Accounts</b> page of the Workspace ONE UEM console.
Disabled	Requires no authentication to access supported applications.

Passcode Setting	Description
Passcode	Enable this option to require a local passcode requirement.
Authentication Timeout	Define the time elapsed, ranging from the last successful authentication to the value set here, that triggers the system to prompt for Workspace ONE UEM credentials. On newer Android applications, authentication timeout prompts for credentials when the session is inactive for the set time.
Maximum Number Of Failed Attempts	Set the maximum times, a user can log in, with an incorrect passcode before the system throws an error. Actions depend on the platform. <ul style="list-style-type: none"> <li>■ Android – The system performs an enterprise wipe on the device.</li> <li>■ iOS – The system performs an enterprise wipe on the device.</li> </ul>

Passcode Setting	Description
Passcode Mode	<p>Select an option depending on your security needs and the platform.</p> <ul style="list-style-type: none"> <li>■ <b>Numeric</b> <ul style="list-style-type: none"> <li>■ Android - You can enter only numbers.</li> <li>■ iOS - You can enter numbers and letters.</li> </ul> </li> <li>■ <b>Alphanumeric</b> <ul style="list-style-type: none"> <li>■ Android - You can enter numbers and letters.</li> <li>■ iOS - You can enter numbers and letters.</li> </ul> </li> </ul>
Allow Simple Value	Set the passcode to allow simple strings. For example, allow strings like 1234 and 1111.
Minimum Passcode Length	Set the minimum number of characters for the passcode.
Minimum Number Of Complex Characters (if Alphanumeric is selected)	Set the minimum number of complex characters for the passcode. For example, allow characters like [], @, and #.
Maximum Passcode Age (days)	Set the number of days the passcode remains valid before you must change it.
Passcode History	Set the number of passcodes the Workspace ONE UEM console stores so that users cannot use recent passcodes.
Biometric Mode	<p>Select the system used to authenticate for access.</p> <ul style="list-style-type: none"> <li>■ <b>Enabled</b> – Allow the use of Fingerprint, Touch ID, or Face ID for authentication to the application.</li> <li>■ <b>Disabled</b> – Does not require biometric authentication systems to access the application.</li> </ul>
Username and Password Setting	Description
Username and Password	Enable this option to set authentication to use the Workspace ONE UEM credentials.
Authentication Timeout	<p>Define the time elapsed, ranging from the last successful authentication to the value set here, that triggers the system to prompt for Workspace ONE UEM credentials.</p> <p>On newer Android applications, authentication timeout prompts for credentials when the session is inactive for the set time.</p>
Maximum Number Of Failed Attempts	<p>Set the maximum times, a user can log in, with an incorrect passcode before the system throws an error.</p> <p>Actions depend on the platform.</p> <ul style="list-style-type: none"> <li>■ Android – The system performs an enterprise wipe on the device.</li> <li>■ iOS – The system performs an enterprise wipe on the device.</li> </ul>
Biometric Mode	<p>Select the system used to authenticate for access.</p> <ul style="list-style-type: none"> <li>■ <b>Enabled</b> – Allow the use of Fingerprint, Touch ID, or Face ID for authentication to the application.</li> <li>■ <b>Disabled</b> – Does not require biometric authentication systems to access the application.</li> </ul>

Disabled Setting	Description
Disabled	Select to require no authentication to access the application.

## Authentication Type and SSO

Authentication Type and SSO can work together or alone.

- **Alone** – If you enable an **Authentication Type** (passcode or user name/password) without SSO, then users must enter a separate passcode or credentials for each individual application. The exception to this configuration is the Workspace ONE Intelligent Hub for Android. This productivity app does not prompt users to create a passcode or PIN. See the section SSO, the Workspace ONE Intelligent Hub for Android, and Forced PINs for details.
- **Together** – If you enable both **Authentication Type** and SSO, then users enter either their passcode or credentials (whichever you configure as the **Authentication Type**) once. They do not have to reenter them until the SSO session ends.

## SSO, the Workspace ONE Intelligent Hub for Android, and Forced PINs

If you deactivate **SSO** and use **Authentication Type > Passcode** and you are deploying the Workspace ONE Intelligent Hub for Android (which uses the Workspace ONE SDK framework), the Workspace ONE Intelligent Hub for Android does not prompt the user to create a PIN for access. If you want to protect the Workspace ONE Intelligent Hub with a passcode, you must either enable **SSO** or assign a **Passcode** profile under **Resources** and apply it to the whole device in the Workspace ONE UEM console.

## Single Sign-On

If you want to require a single sign-on (SSO) passcode on devices, enable **Single Sign-On** and set **Authentication Type** to **Passcode** and set the **Passcode Mode** to either **Numeric** or **Alphanumeric**.

Using either the Workspace ONE Intelligent Hub or Workspace ONE as a "broker application," end users can authenticate once using either their normal credentials or an SSO passcode. They gain access to other applications so long as the SSO session is active.

If you enable SSO but do not enable an **Authentication Type**, the system does not prompt end users with any recurring authentication. An exception to this behavior occurs when end users must authenticate during an initial installation of the application. They use their normal credentials to authenticate in this instance.

## SSO Sessions and SDK App Login Behaviors

An SSO session establishes when a user authenticates with an application participating in SSO. Although SSO sessions help streamline the login experience for the user, the variables that impact the SSO mechanism and the login behavior of the SDK app are varied and complex. The session is active until it reaches the **Authentication Timeout** value or the user manually locks the application (includes forcing it closed). The SDK app prompts for credentials depending on multiple variables including but not limited to the platform, SSO setting, SSO session status, and Authentication Type.

- Platform
  - Android
  - iOS
- **SSO** configuration
  - Enabled
  - Disabled
- **SSO** session status
  - Active
  - Inactive
- **Authentication Type** configuration
  - **Username and Password**
  - **Passcode**
  - **Disabled**
- **Authentication Type** state
  - Credential value exists (**Passcode** or **Username and Password**)
  - Credential value does not exist
  - **Authentication Timeout** is active or expired
- SDK app state
  - App forcibly closed
  - SDK upgraded

On iOS devices, the existence of a valid identity sent from the Workspace ONE UEM console also influences the login behaviors in SDK apps. This identity is a one-time use token and it establishes the user identity in the SDK app. If the identity exists in the SDK app, then the system does not prompt for credentials.

The system displays specific prompts in the SDK app depending on the **Authentication Type** and the request sent from the Workspace ONE UEM console.

Table 3-2. Login Prompts

Authentication Type	Request	Login Prompt
Passcode	Create Credentials	Create Passcode
	Provide Credentials	Enter Passcode
Username and Password	Create Credentials	Enter Username and Password
	Provide Credentials	Enter Username and Password

## Android and SSO - Login Prompts for Authentication Modes, Passcode and Username and Password (Login Values)

SSO Setting	SSO Session Status	State (Login Value or App)	Login Behavior
Enabled	Active	Credential exists	The system does not prompt for the login value.
		Credential does not exist	The system prompts to create the login value.
		App closes	When user accesses the app, and another SDK-app is still involved in the SSO session, the system does not prompt for the login value.  If the app is stopped or forcibly closed without reaching the <b>Authentication Timeout</b> value, the system does not prompt for the login value.
		SDK upgraded	When user accesses app after upgrade, the system does not prompt for the login value.
	Inactive	Credential exists	The system prompts the user for the login value.
		Credential does not exist	The system prompts the user to create the login value.
		App closes	The system prompts the user for the login value.
		SDK upgraded	The system prompts the user for the login value.



SSO Setting	SSO Session Status	State (Login Value or App)	Login Behavior
Disabled  <b>Authentication Timeout</b> status impacts behavior (active or expired).	NA	Credential exists	The system prompts the user for the login value.
		Credential does not exist	The system prompts the user to the create login value.
		App closes	The system prompts the user for the login value if <b>Authentication Timeout</b> has expired.
		SDK upgraded	The system does not prompt for the login value.

## Android and SSO - Login Prompts for Authentication Mode Disabled

SSO Setting	SSO Session Status	Login Behavior
Enabled	Active	The system does not prompt for login values.  The SDK app opens with no challenges.
	Inactive	The system does not prompt for login values.  The SDK app opens with no challenges.
Disabled	NA	The system prompts the user for the Workspace ONE UEM credentials as the login values on first start.  After the initial start, the system opens the SDK app with no challenges.

## iOS and SSO - Login Prompts for Authentication Modes, Passcode and Username and Password (Login Values)

SSO Setting	SSO Session Status	State (Login Value or App)	Login Behavior
Enabled  Keychain-sharing apps share the session.	Active	Credential exists	The system does not prompt since the credential exists and the SSO session is active.
		Credential does not exist	The system prompts the user to create credentials.

SSO Setting	SSO Session Status	State (Login Value or App)	Login Behavior
		App closes	When user accesses app after closing, the system prompts the user for the credential value.
		SDK upgraded	When the user accesses app after upgrade, the system prompts the user for the credential value. iOS quits the app on upgrade.
		Credential exists	The system prompts the user for the credential value. When the SSO session expires, credentials are removed and the system prompts for the credentials again.
		Credential does not exist	The system prompts the user to create credentials.
		App closes	When the user accesses the app after closing, the system prompts the user for the credential value.
		SDK upgraded	When the user accesses app after upgrade, the system prompts the user for the credential value. iOS closes the app on upgrade.
Disabled Keychain-sharing apps are not sharing the session. <b>Authentication Timeout</b> status impacts behavior (active or expired).	NA	Credential exists	The system does not prompt since the credential exists and <b>Authentication Timeout</b> session is active. If the <b>Authentication Timeout</b> is expired, the system prompts the user for the credential value. When the session expires, credentials are removed and prompted for again.
		Credential does not exist	The system prompts the user to create credentials no matter if the <b>Authentication Timeout</b> is active or expired.

SSO Setting	SSO Session Status	State (Login Value or App)	Login Behavior
		App closes	When the user accesses the app after closing, the system prompts the user for the credential value no matter if the <b>Authentication Timeout</b> is active or expired.
		SDK upgraded	<p>If the <b>Authentication Timeout</b> is active, and the user accesses the app after upgrading, the system prompts the user for the credential value.</p> <p>If the <b>Authentication Timeout</b> is expired, and the user accesses app after upgrade, the system prompts the user for the credential value because iOS closes the app after upgrading.</p>

## iOS and SSO - Login Prompts for Authentication Mode Disabled

SSO Setting	SSO Session Status	Login Behavior
Enabled	Active	<p>The system does not prompt for login values.</p> <p>The SDK app opens with no challenges.</p>
	Inactive	<p>The system does not prompt for login values.</p> <p>The SDK app opens with no challenges.</p>
Disabled	NA	<p>If the device is MDM managed, then the system does not prompt for login values. The SDK app opens with no challenges.</p> <p>If the device is in Registered Mode, the system prompts the user for the Workspace ONE UEM credentials as the login values on first start. After the initial start, the system opens the SDK app with no challenges.</p>

## iOS and SSO - One Time Login Prompts When the App Is Missing the Identity (Valid Token)

SSO Setting	Scenario	Login Behavior
Enabled	Valid one time token is available through Workspace ONE UEM.	The system does not prompt for <b>Username and Password</b> authentication because it uses a one time token to establish identity.
	A valid one time token is NOT available. The first Keychain-sharing app is installed within a Keychain sharing cluster.	If the one time token is not available to establish identity, the system prompts for the <b>Username and Password</b> authentication to establish identity.
	A valid one time token is NOT available. The second Keychain-sharing app is installed within a Keychain sharing cluster.	The system does not prompt for the <b>Username and Password</b> authentication and establishes the identity silently.
Disabled	Valid one time token is available through Workspace ONE UEM.	The system does not prompt for the <b>Username and Password</b> authentication because it uses a one time token to establish identity.
	Valid one time token is NOT available.	If the one time token is not available to establish identity, the system prompts for the <b>Username and Password</b> authentication to establish identity.

## Integrated Authentication

Allow access to corporate resources, such as content repositories, through the Workspace ONE Intelligent Hub using Workspace ONE UEM SSO credentials.

Setting	Description
Enable Kerberos	Use your Kerberos system for authenticating to corporate resources and sites.
Use Enrollment Credentials	<p>Access corporate resources listed in the <b>Allowed Sites</b> field with the SSO credentials.</p> <p>Enter systems in the <b>Allowed Sites</b> text box to control access to a specific set of sites and domains. You must complete this setting for <b>Integrated Authentication</b> to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.</p>
Use Certificate	<p>Upload the <b>Credential Source</b> or set a <b>Defined Certificate Authority</b> to access corporate resources listed in the <b>Allowed Sites</b> text box with the SSO credentials.</p> <p>Enter systems in the <b>Allowed Sites</b> text box to control access to a specific set of sites and domains. You must complete this setting for <b>Integrated Authentication</b> to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.</p>

## Offline Access

The SDK restricts or allows offline access depending on the configurations.

Offline Access	Behavior
Enabled Maximum Period Allowed = time	The SDK allows offline access and then restricts access when time offline meets the maximum period allowed value.
Enabled Maximum Period Allowed = 0	The SDK allows offline access indefinitely.
Disabled	The SDK prevents offline access.

## Compromised Protection

Protect your mobile network from compromised resources with an enterprise wipe. It clears privileged corporate data off devices. The system does not perform wipe actions on data unrelated to the enterprise.

## AirWatch App Tunnel

Allow an application to communicate through a VPN or reverse proxy to access internal resources, such as a SharePoint or intranet sites. To use **Allow all non-FQDN URLs through App tunnel**, applications must use Workspace ONE SDK v19.3+ (both Android and iOS Swift).

The Per-App Tunnel provides Device Traffic Rules. Device Traffic Rules allow you to set individual traffic policies for tunneling, blocking, and bypassing traffic for each of your apps.

Before you can use **VMware Tunnel - Proxy** or **VMware Tunnel** menu items, you must install these tunnels. See [VMware Tunnel](#).

If you are switching from **VMware Tunnel - Proxy** to **VMware Tunnel**, migrate the **App Tunnel URLs** entries.

If users access an internal resource through a non-standard port (a port that is not port 80 or 443), explicitly list the port number in the URL you enter in **App Tunnel URLs**. For example, if the resource URL is data.company.com and it is accessed through port 7777, you must add **data.company.com:7777** in the **App Tunnel URLs** field.

Setting	Description
VMware Tunnel	<p>Sets devices to access corporate resources using the Per-App Tunnel component of VMware Tunnel.</p> <p>For this option to work, install VMware Tunnel.</p> <p>Also, the Per-App Tunnel component of VMware Tunnel uses rules to set policies for tunneling, blocking, or bypassing specific domains. Ensure that you have setup web and other SDK-enabled apps on the <b>Device Traffic Rules</b> page before enabling it here.</p> <p>If you have some SDK applications that still use <b>VMware Tunnel - Proxy</b>, enable <b>Tunnel Proxy for Backward Compatibility</b>. This menu item allows those SDK applications that have not migrated to Per-App Tunnel to continue to work using Proxy.</p> <p>This setting does not act as a backup. If your Tunnel gateway is not available, applications do not fall back to Proxy.</p>
VMware Tunnel - Proxy	<p>Sets devices to access corporate resources using the proxy component of the VMware Tunnel, also called Proxy.</p> <p>Consider migrating to the Per-App Tunnel component for better performance and new features.</p> <p>For this option to work, install VMware Tunnel. If this feature is not installed and configured, use the UI links to go to the configuration pages.</p> <ul style="list-style-type: none"> <li>■ Select <b>Configure VMware Tunnel - Proxy Settings</b> to enable Proxy if you have not already set this feature.</li> <li>■ Use <b>Allow all non-FQDN URLs through App tunnel</b> to control traffic to non-FQDN (fully qualified domain name) URLs through the tunnel. <ul style="list-style-type: none"> <li>■ <b>YES</b> - All non-FQDN URLs use the tunnel.</li> <li>■ <b>NO</b> - Only non-FQDN that are explicitly listed in the <b>App Tunnel URLs</b> use the tunnel.</li> </ul> </li> <li>■ To restrict the communication to a set of tunnel domains, enter domains in the <b>App Tunnel URLs</b> text box. All other traffic not listed in this text box, goes directly to the Internet.</li> </ul> <p>Use wildcards to allow access to any site with a domain subset. For example, <b>*.&lt;example &gt; .com</b> allows traffic to any site that contains <b>.&lt;example &gt; .com</b> in its domain. Similarly, it allows access to any port on that site with an implementation similar to <b>*.&lt;example &gt; .com</b>.</p> <p>If nothing is listed in this text box, all traffic directs through the app tunnel.</p>
Standard Proxy	<p>Sets devices to request resources using a proxy server that allows or denies connections to enterprise systems.</p> <ul style="list-style-type: none"> <li>■ To access your internal network, select an <b>App Tunnel Proxy</b> from the menu . Add standard proxies by selecting <b>Configure Standard Proxy Settings</b>.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>■ Use <b>Allow all non-FQDN URLs through App tunnel</b> to control traffic to non-FQDN (fully qualified domain name) URLs through the tunnel. <ul style="list-style-type: none"> <li>■ <b>YES</b> - All non-FQDN URLs use the tunnel.</li> <li>■ <b>NO</b> - Only non-FQDN that are explicitly listed in the <b>App Tunnel URLs</b> use the tunnel.</li> </ul> </li> <li>■ To restrict the communication to a set of tunnel domains, enter domains in the <b>App Tunnel URLs</b> text box. All other traffic not listed in this text box, goes directly to the Internet.</li> </ul> <p>Use wildcards to allow access to any site with a domain subset. For example, *.&lt;example&gt;.com allows traffic to any site that contains .&lt;example&gt;.com in its domain. Similarly, it allows access to any port on that site with an implementation similar to *.&lt;example&gt;.com.</p> <p>If nothing is listed in this text box, all traffic directs through the app tunnel.</p>

## Migrate Proxy App Tunnel URLs to Per-App Tunnel

If you migrate from **VMware Tunnel - Proxy** to **VMware Tunnel** (Per-App Tunnel) and want to keep the domains that use the tunnel, enter the **App Tunnel URLs** from the Proxy to the **Device Traffic Rules** settings for Per-App Tunnel.

Go to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies > App Tunnel Mode > VMware Tunnel - Proxy** and record the entries in the **App Tunnel URLs** field.

The Per-App Tunnel provides Device Traffic Rules. Device Traffic Rules allow you to set individual traffic policies for tunneling, blocking, and bypassing traffic for each of your apps.

- 1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Network Traffic Rules > Device Traffic Rules**.
- 2 Select the applicable SDK application (like Workspace ONE Web). This configuration differs from the default SDK setting because you must enter the domains to tunnel by the app rather than as a blanket entry for all SDK-built apps. Use Add to enter multiple applications.
- 3 Select **Tunnel** for the **Action**.
- 4 Enter the app tunnel URLs from the VMware Tunnel - Proxy option in Destination Hostname. Define a default policy for domains that do not match patterns with your destination host names.
- 5 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**, select **App Tunnel Mode**, and change from **VMware Tunnel - Proxy** to **VMware Tunnel**.



## Content Filtering

Integrates your Forcepoint (Websense) content filtering service and the Workspace ONE Web. This integration requires settings on multiple pages in the console.

This integration requires configurations on different pages in the Workspace ONE UEM console.

- **Third-Party Proxies** – Add information on the Third-Party Proxies page for your content filtering system so Workspace ONE UEM can communicate with it. Configure your Forcepoint information in **Groups & Settings > All Settings > System > Enterprise Integration > Third Party Proxies**.
- **Settings and Policies** – Used for content filtering on the Settings and Policies page. Using the Settings and Policies, you can filter traffic in the Workspace ONE Web with the policies and rules set in your Forcepoint service.

Integration results in the system filtering the Workspace ONE Web traffic with the settings in the content filtering system. If you use another application tunnel, Workspace ONE UEM sends data that is not going through your content filtering service to the configured app tunnel.

## Geofencing

Restrict access to applications depending on the distances set in Geofencing settings in the Workspace ONE UEM console.

## Data Loss Prevention (DLP)

Protect sensitive data in applications. DLP options control how and what data transmits back and forth.

Setting	Description
Enable Bluetooth	Allows applications to access Bluetooth functionality on devices when set to <b>Yes</b> .
Enable Camera	Allows applications to access the device camera when set to <b>Yes</b> .
Enable Composing Email	Allows an application to use the native email client to send emails when set to <b>Yes</b> .
Enable Copy and Paste Out	<p>Allows users to copy and paste content from SDK-built applications to external destinations when set to <b>Yes</b>.</p> <p>When you set it to <b>No</b>, the system allows copy and paste only between Workspace ONE UEM applications.</p> <p>Encryption of the pasted content depends upon the configurations for authentication and SSO. If you enable authentication and SSO, the system encrypts the content with a user pin-based key. Otherwise, the system encrypts content with a randomly generated key.</p> <p>The system migrates the setting configured previously in the option to <b>Enable Copy and Paste</b> to this feature.</p>

Setting	Description
Enable Copy and Paste Into	Allows users to copy and paste content from external destinations into SDK-built applications when set to <b>Yes</b> . When you set it to <b>No</b> , the system allows copy and paste only between Workspace ONE UEM applications.
Enable Data Backup	Allows wrapped iOS applications to sync data with a storage service like iCloud when set to <b>Yes</b> .
Enable Location Services	Allows wrapped applications to receive the latitude and longitude of the device when set to <b>Yes</b> .
Enable Printing	Allows an application to print from devices when set to <b>Yes</b> .
Enable Screenshot	Allows applications to access screenshot functionality on devices when set to <b>Yes</b> .
Enable Third-Party Keyboards	On iOS devices when set to <b>No</b> , SDK-built applications always open in the native keyboard and prevent the use of third-party keyboards. On Android devices when set to <b>No</b> and the user did not set the system keyboard as the primary keyboard, SDK-built applications prevent user access.
Enable Watermark	Displays text in a watermark in documents in the VMware Content Locker when set to <b>Yes</b> . Enter the content to display in the <b>Overlay Text</b> text box or use lookup values. You cannot change the design of a watermark from the Workspace ONE UEM console.
Limit Documents to Open Only in Approved Apps	Enter options to control the applications used to open resources on devices.
Allowed Applications List	Enter the applications that you allow to open documents.

## Network Access Control

Allow applications to access the mobile network.

Setting	Description
Allow Cellular Connection	Controls cellular connections by allowing them all the time, allowing connections when the device is not roaming, or never allowing cellular connections.
Allow Wi-Fi Connection	Allows connections using Wi-Fi networks, or limits connections by Service Set Identifier (SSID).
Allowed SSIDs	Enter the Service Set Identifiers (SSIDs) that devices can use to access the Wi-Fi network during limiting connections.

# Settings Profiles for the SDK

# 4

**Settings** profiles offer ways to customize how SDK-built apps look. These profiles also manage app logs and analytics for troubleshooting and analysis.

## Navigation

Find settings in **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

## Branding

Change the look and feel of applications to reflect the unique brand of your company with **Branding** settings when you configure the app to use the default SDK settings.

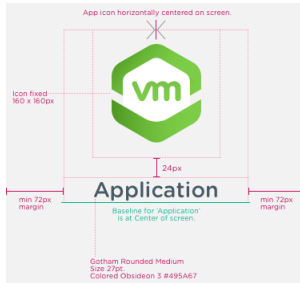
Setting	Description
Colors	<p>Reflect your company colors by choosing colors for the Workspace ONE UEM console from the color palette beside the color options.</p> <p>Choose primary and secondary colors listed options including tool bars and text.</p>
Organization Name	Enter the name that represents your organization to display in the Workspace ONE UEM system.
Device Backgrounds	<p>Upload images that the system displays as the background and as the logo for the organization on the listed device types.</p> <ul style="list-style-type: none"> <li>■ Apple iOS options <ul style="list-style-type: none"> <li>■ Background Image iPhone</li> <li>■ Background Image iPhone (Retina)</li> <li>■ Background Image iPhone 5 (Retina)</li> <li>■ Background Image iPad</li> <li>■ Background Image iPad (Retina)</li> </ul> </li> <li>■ Android options <ul style="list-style-type: none"> <li>■ Background Image Small</li> <li>■ Background Image Medium</li> <li>■ Background Image Large</li> <li>■ Background Image Extra Large</li> </ul> </li> <li>■ Platform neutral options <ul style="list-style-type: none"> <li>■ Company Logo Phone</li> <li>■ Company Logo Phone High Res</li> <li>■ Company Logo Tablet</li> <li>■ Company Logo Tablet High Resolution</li> </ul> </li> </ul>

## Branding - Splash Screens

It is difficult to find a single image that displays perfectly on every mobile device. However, certain dimensions for images displayed on iOS and Android devices can work for most displays. Use these specifications for application splash screens.

- Mobile - iOS
  - Icon, centered - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 72 pixels

**Figure 4-1. Example Splash Screen Specifications**



- Tablet, Portrait - iOS
  - Icon - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 264 pixels
- Tablet, Landscape - iOS
  - Icon - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 56 pixels
- Mobile - Android
  - Icon - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 56 pixels
- Tablet, Portrait - Android
  - Icon - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 260 pixels
- Tablet, Landscape - Android
  - Icon - 160 x 160 pixels
  - Branded text distance from icon – centered at a distance of 24 pixels
  - Branded text – 27 point
  - Margins - 388 pixels

## Logging

The Workspace ONE UEM system collects logs until the log file size reaches 200 MB for SaaS environments. If the log size exceeds 200 MB, the system stops collecting logs. The Workspace ONE UEM console notifies you when your application log size reaches 75% of 200 MB. To act on the application log size, contact your Workspace ONE UEM Representative.

- Ask for an increase in your application log size.
- Ask for a purge of your application log. The system can purge logs older than two weeks.

The Workspace ONE UEM console reports the messages that match the configured logging level plus any logs with a higher critical status. For example, if you set the logging level to Warning, messages with a Warning and Error level display in the Workspace ONE UEM console.

The SDK-built application collects logs over time and stores them locally on the device until another API or command is invoked to transmit the logs.

**Note** When an enterprise wipe occurs, the console does not purge the log files. You can retrieve logs after a device re-enrolls to determine what issues occurred in the last enrollment session to cause the enterprise wipe.

**Table 4-1. SDK Logging Level APIs and Level Descriptions**

Level	Logging API	Description
Error	AWLogError("{log message}")	Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL.
Warning	AWLogWarning("{log message}")	Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications.
Information	AWLogInfo("{log message}")	Records a significant amount of data for informational purposes. An information logging level displays general processes, warning, and error messages.
Debug or Verbose	AWLogVerbose("{log message}")	Records all data to help with troubleshooting. This option is not available for all functions.

## Analytics

Use SDK analytics to view how many times a file or an application has been opened and how long the file or application remained open. These statistics offer a quick view of which end users have downloaded and viewed high-priority content.

Display events for applications that use SDK functionality. Workspace ONE UEM reports event analytics by the application ID and event name. These events are custom created and developers can code any process or behavior they want to track. Find them in **Apps & Books > Applications > Logging > SDK Analytics**.

## Custom Settings

Use **Custom Settings** to enter XML code. This XML code allows you to activate or deactivate certain settings, manually. You can add custom features to your environment to support the unique needs of your mobile network. For the most current list of the supported lookup values for custom settings, select the **Insert Lookup** icon, the plus sign (+), next to the text box.

# SDK App Compliance Profiles for the SDK

# 5

**SDK App Compliance** profiles help monitor and enforce compliance on devices that have Workspace ONE SDK-built apps. Devices with these profiles do not require an MDM profile and can be offline and still comply with app security policies.

---

**Note** The **SDK App Compliance** feature is not available with custom profiles.

---

## Navigation

Find settings in **Groups & Settings > All Settings > Apps > Settings and Policies > SDK App Compliance**.

## Block and Wipe Functions for SDK App Compliance Settings

SDK App Compliance identifies non-compliant devices with SDK-built applications installed and act with the block or wipe function. It identifies non-compliance when a device's status satisfies the configured rules.

---

**Note** Note: The **App Version** setting only applies the block action.

---

- **Wipe** - The Wipe action, also called an enterprise wipe, clears privileged corporate data off devices that are not compliant with the applicable parameter. The system does not perform wipe actions on data unrelated to the enterprise. SDK App Compliance settings that use this action include the following list.
  - OS Version
  - Security Patch Date

---

**Note** The wipe function for Application Inactivity is not an enterprise wipe. The system wipes only the data on the device that pertains to the SDK-built app.

---

- **Block** - The Block action prevents user access to SDK-built applications that meet a configured parameter. SDK App Compliance settings that use this action include the following list.
  - App Version
  - OS Version



- Security Patch Date

## Application Version

Restricts devices from accessing SDK-built applications unless the version is approved.

You cannot add more than one version of an SDK-built application.

Here is an example of how to configure this setting. You can enter and select Workspace ONE Boxer, select Less Than, and enter 4.9. This group of parameters sets the SDK to block access to any version of Workspace ONE BoxerVMware Boxer that is earlier than v4.9. This text box evaluates version identifiers as numeric values separated by a period. For example, 2.3.5 or 7.5.4.1. If your version contains non-numeric values, like 2.a.5, the SDK uses only the leading numeric values and it evaluates this value as 2. For a version number of 2.3.4.a, the SDK evaluates this value as 2.3.4.

## Application Inactivity

Restricts devices from accessing SDK-built applications in case the applications stay inactive for a specified number of days. When enabled, application data is wiped when an iOS or Android application (specified by an app ID) reaches the allowed days of inactivity (1-90 days).

This policy does not impact older versions of apps.

This feature works for apps built with the Workspace ONE SDK v20.2 or later.

## OS Version

Restricts devices from accessing your enterprise resources that are not on compliant OS versions.

Here is an example of how to configure this setting. Select **Greater Than or Equal To**, and enter **Android 4.4.2**. This group of parameters sets the SDK to block access to an Android device or wipe an Android device that either runs 4.4.2 or an OS version later than 4.4.2. This configuration approves of Android OS version 4.4.1 and earlier.

## Security Patch Date

Restricts Android devices that are on a security patch older than a specified date. Enter a date that identifies the minimum approved security patch that you require Android devices to run in the **Before** text box. If an Android device runs a patch published before this date, the SDK acts with the configured action.

## Where to Get Data

You can find device events for SDK App Compliance using two methods: from the **Device Details** view or from the **Events** page. You can access the following reports.

- **App Compliance Reported Non Compliant** has a severity of **Warning**.

- **App Compliance Reported Compliant** has a severity of **Information**.

If the SDK-built application reported as non-compliant with the SDK App Compliance settings, the applicable device events display in the event log or device events list.

# Privacy Policies for Data Collection in Productivity Applications

## 6

Control data collection in supported VMware productivity applications with custom settings. Display your organization's privacy policy in the app and let users decide whether to share their productivity app data.

### Configurable Privacy Policies

Privacy configurations consist of key-value pairs entered in the Workspace ONE UEM console. The default SDK settings power these configurations, and they provide the listed controls.

- Display your company's privacy policy within the productivity application so that users can review it and know the company's exact policy.
- To allow users to decide if they want to share their feature usage analytics, display a **Data Sharing** page in the productivity application. Sharing feature usage analytics helps VMware improve existing features and develop new ones.
- If you use VMware Workspace ONE Intelligence, you can share the diagnostic data for productivity applications that is collected from these systems. Sharing diagnostic data helps to analyze and troubleshoot problems with applications and your enterprise mobility management environment.

### Redirect Links for Android

Links that redirect users to a privacy policy work for iOS but they do not work on Android devices. If you deploy to Android devices, use direct links to your company's privacy policy.

### Supported VMware Productivity Applications

The privacy policies impact the listed VMware productivity applications.

- Workspace ONE Web
- Workspace ONE Content
- Workspace ONE Boxer
- Workspace ONE

## Access to Privacy Policy Information

Users can access the privacy information in productivity applications and they can change their selections at any time. Users also see the privacy dialog box when they first access the application and when they upgrade the application.

## Configure Privacy Settings to Control Data Collection

Control the collection of data in VMware productivity applications with the default SDK profile in the Workspace ONE UEM console. Enter code in the custom settings text box to display and apply the privacy settings.

Links that redirect users to a privacy policy work for iOS but they do not work on Android devices. If you deploy to Android devices, use direct links to your company's privacy policy.

- 1 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings > Custom Settings**.
- 2 Select **Enabled**.
- 3 Enter the key-value pairs in the text box.

Name	Key	Value	Description
Company Privacy Policy URL	"PrivacyPolicyLink"	"https://www.company.com/privacypolicy"	<p>The value for this key is the company's specific privacy policy URL.</p> <p>Navigate users to a specific privacy disclosure site from the productivity application.</p> <p>Users can review the policy so that they know the company's stance on privacy.</p>
VMware Feature Usage Analytics	"PolicyAllowFeatureAnalytics"	<ul style="list-style-type: none"> <li>0 - Disabled <ul style="list-style-type: none"> <li>Prevents data sharing for all users of productivity applications.</li> <li>This value prevents the display of the Data Sharing page in the productivity application.</li> </ul> </li> <li>1 - Enabled <ul style="list-style-type: none"> <li>Users can decide if they want to share their usage data for productivity applications.</li> <li>This value does display the Data Sharing page in the productivity application.</li> </ul> </li> </ul>	<p>This key controls the display of the <b>Data Sharing</b> page within the productivity application.</p> <p>Users can opt in or out of sharing their feature usage analytics.</p> <p>Feature usage analytics collection helps VMware to improve existing products and to develop new ones.</p>
Diagnostics Data Through VMware Workspace ONE Intelligence and Aptelligent by VMware	<p>"PolicyAllowCrashReporting"</p> <p>For this key to work, you must use Aptelligent by VMware or VMware Workspace ONE Intelligence.</p>	<ul style="list-style-type: none"> <li>false - Disabled <ul style="list-style-type: none"> <li>Prevents the reporting of diagnostic data for productivity applications as reported by Aptelligent by VMware and Workspace ONE Intelligence.</li> <li>When deactivated, your ability to investigate and resolve problems is reduced because your system receives no diagnostic data for productivity applications from Aptelligent by VMware or Workspace ONE Intelligence.</li> </ul> </li> </ul>	<p>This key controls reporting diagnostic data from Aptelligent by VMware and Workspace ONE Intelligence.</p> <p>Aptelligent by VMware and Workspace ONE Intelligence are tools that help analyze, troubleshoot, and maintain applications and enterprise mobility management deployments.</p>

Name	Key	Value	Description
		<ul style="list-style-type: none"> <li>■ <code>true</code> - Enabled                             <ul style="list-style-type: none"> <li>■ Sends diagnostic data for productivity applications as reported by Aptelligent by VMware and Workspace ONE Intelligence.</li> <li>■ When set to <code>true</code>, your system receives diagnostic data for productivity applications from Aptelligent by VMware and Workspace ONE Intelligence to help with investigating and resolving problems.</li> </ul> </li> </ul>	

### Example

```
{
  "PolicyAllowFeatureAnalytics": 1,
  "PrivacyPolicyLink": "https://www.company.com/privacypolicy",
  "PolicyAllowCrashReporting": true
}
```

The example entry configures the listed actions.

- Displays the **Data Sharing** page within the productivity applications so that users can decide to share or not share their feature usage analytics.
- Navigates users to a URL within the productivity application so that users can review the company's privacy policy.
- Shares diagnostic data for productivity applications from Aptelligent by VMware and Workspace ONE Intelligence.

- 4 Save your settings.