SDK and Managing Applications

VMware Workspace ONE UEM 2001

vmware®

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

MAM Functionality with VMware Workspace ONE SDK 1

The Settings and Policies in VMware Workspace ONE® UEM powered by AirWatch has settings that control security, application behaviors, and the data retrieval of specific applications. The settings are also called SDK settings because they run on the Workspace ONE SDK framework.

You can apply these SDK features to applications built with the Workspace ONE SDK, to supported Workspace ONE UEM applications, and to applications wrapped by the VMware AirWatch App Wrapping engine. Same features can be applied in both the places as the Workspace ONE SDK framework processes the functionality.

Types of Options for SDK Settings

Workspace ONE UEM has two types of the SDK settings, default and custom. To choose the type of SDK setting, determine the scope of deployment.

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

  Find the default settings in **Groups & Settings > All Settings > Apps > Settings and Policies** and then select **Security Policies**, **Settings**, or **SDK App Compliance**. You can apply these options across all the Workspace ONE UEM applications in an organization group. Shared options are easier to manage and configure because they are in a single location. View the matrices for information on which default settings apply to specific Workspace ONE UEM applications or the Workspace ONE SDK and app wrapping.

- Custom settings work with individual devices or for small numbers of devices with applications that require special mobile application management (MAM) features.

  Find the custom settings in **Groups & Settings > All Settings > Apps > Settings and Policies > Profiles**. Custom settings for profiles offer granular control for specific applications and the ability to override default settings. However, they also require separate input and maintenance.

Assign the Default or Custom Profile

2

To apply Workspace ONE UEM features built with the VMware Workspace ONE SDK, you must apply the applicable default or custom profile to an application.

Apply the profile when you upload or edit the application to the Workspace ONE UEM console.

When you make changes to the default or custom profile, Workspace ONE UEM applies these edits when you select **Save**.

Changes can take a few minutes to push to end-user devices. Users can close and restart Workspace ONE UEM applications to receive updated settings. Make other configurations and then save the application and create assignments for its deployment.

Procedure

1 Navigate to **Apps & Books > Applications > Native > <App Type>**.

2 Add or edit an application.

3 Select a profile on the **SDK** tab.

Setting	Description
Default Settings Profile	■ For Android applications, select the **Android Default Settings @ Global >** . ■ For Apple iOS applications, select the **iOS Default Settings @ Global >** .
Custom Settings Profiles	For Android and Apple iOS applications, select the applicable legacy or custom profile.

4 Make other configurations and then save the application and create assignments for its deployment.

Assign the SDK Profile to the Workspace ONE Intelligent Hub for Apple iOS

To apply SDK functionality to SDK-built resources, configure the Workspace ONE Intelligent Hub for Apple iOS to use the correct SDK profile.

If you do not assign the SDK profile to the Workspace ONE Intelligent Hub to apply SDK configurations, your default SDK configurations in **Settings and Policies** do not work in applications.

Procedure

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**.
3. **Save** your settings.

Assign the SDK Profile to the Workspace ONE Intelligent Hub for Android

To apply SDK functionality to SDK-built resources, configure the Workspace ONE Intelligent Hub for Android to use the correct SDK default profile.

If you do not assign the SDK profile to the Workspace ONE Intelligent Hub to apply SDK configurations, your default SDK configurations in **Settings and Policies** do not work in applications.

Procedure

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**.
3. **Save** your settings.

Supported SDK Settings and Policies by Platform

3

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 3-1. 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.
Passes	The SDK passes the setting from the Workspace ONE UEM console to the SDK-built app. The app reads and enforces the setting.

Table 3-2. 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
Passcode: Maximum Passcode Age	Supported	Supported
Passcode: Passcode History	Supported	Supported

Table 3-2. Supported Settings and Policies Options By Platform (continued)

SDK Default Payload	Workspace ONE SDK for Android	Workspace ONE SDK for iOS (Swift)
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	**Not Supported**	**Not Supported**
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	*Passes*	`Not Supported`
DLP: Bluetooth	*Passes*	`Not Supported`
DLP: Camera	*Passes*	Supported
DLP: Composing Email	*Passes*	*Passes*
DLP: Copy and Paste Out	Supported	Supported
DLP: Copy and Paste Into	Supported	Supported
DLP: Data Backup	*Passes*	**Not Supported**
DLP: Location Services	*Passes*	`Not Supported`
DLP: Printing	*Passes*	Supported
DLP: Screenshot	Supported	**Not Supported**
DLP: Third Party Keyboards	`Not Supported`	Supported
DLP: Watermark	Supported	Supported
DLP: Limit Documents to Open Only in Approved Applications	`Not Supported`	*Passes*
NAC: Cellular Connection	Supported	`Not Supported`
NAC: Wi-Fi Connection	Supported	`Not Supported`
Branding	Supported	Supported
Logging	Supported	Supported
Analytics	Supported	Supported

Table 3-2. Supported Settings and Policies Options By Platform (continued)

SDK Default Payload	Workspace ONE SDK for Android	Workspace ONE SDK for iOS (Swift)
SDK App Compliance: Application Version	Not Supported	Supported
SDK App Compliance: Application Inactivity	Not Supported	Not Supported
SDK App Compliance: OS Version	Not Supported	Supported
SDK App Compliance: Security Patch Date	Not Supported	Not Supported

This chapter includes the following topics:

Security Policies Profiles for the SDK

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

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

- Force Token For App Authentication
- Authentication Type

  Authentication Type and SSO
- Single Sign-On

  SSO Session

  SSO and System Login Behavior for iOS Applications
- Integrated Authentication
- Offline Access
- Compromised Protection
- AirWatch App Tunnel

  Migrate Proxy App Tunnel URLs to Per-App Tunnel
- Content Filtering
- Geofencing
- Data Loss Prevention (DLP)

- Network Access Control

Force Token For App Authentication

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

Authentication Type

Select an authentication type 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 type.

Table 3-3. 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 **Accounts** 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. ■ Android – The system performs an enterprise wipe on the device. ■ iOS – The system performs an enterprise wipe on the device.

Passcode Mode	Select an option depending on your security needs and the platform.
	■ **Numeric**
	  ■ Android - You can enter only numbers.
	  ■ iOS - You can enter numbers and letters.
	■ **Alphanumeric**
	  ■ Android - You can enter numbers and letters.
	  ■ iOS - You can enter numbers and letters.

Passcode Setting	Description
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	Select the system used to authenticate for access. ■ **Enabled** – Allow the use of Fingerprint, Touch ID, or Face ID for authentication to the application. ■ **Disabled** – Does not require biometric authentication systems to access the application.

Username and Password Setting	Description
Username and Password	Enable this option to set authentication to use the Workspace ONE UEM credentials.
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. ■ Android – The system performs an enterprise wipe on the device. ■ iOS – The system performs an enterprise wipe on the device.
Biometric Mode	Select the system used to authenticate for access. ■ **Enabled** – Allow the use of Fingerprint, Touch ID, or Face ID for authentication to the application. ■ **Disabled** – Does not require biometric authentication systems to access the application.

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.
- 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.

Single Sign-On

If you want to require an SSO passcode on devices, 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 Session

A single sign-on (SSO) session establishes when a user authenticates with an application participating in an SSO. The session is active until the it reaches the **Authentication Timeout** value or until the user manually locks the application. Control this behavior with the Workspace ONE Intelligent Hub and the SDK profile.

When using the Workspace ONE Intelligent Hub as a "broker application" for features such as SSO, configure the Workspace ONE Intelligent Hub with the applicable SDK profile. If you are using the default SDK profile, ensure that the Workspace ONE Intelligent Hub is configured to use this profile. If you do not set the Workspace ONE Intelligent Hub to use the default SDK profile, then the system does not apply your configurations you configure in the Settings and Policies section.

SSO and System Login Behavior for iOS Applications

SSO Enabled - The authentication process to an application with Workspace ONE UEM SSO enabled includes two phases: accessing the app and securing persistent access.

1 Identify user for app access - The first phase ensures that the user's credentials are valid. The system identifies the user first by silent login. If the silent login process fails, then the system uses a configured, authentication system. Workspace ONE UEM supports username and password, token, and SAML.

2 Secure persistent app access - The second phase grants the user access to the application and keeps the session live with a recurring authentication process. Workspace ONE UEM supports passcode, username and password, and no authentication (disabled).

Authentication Behavior - The SSO configuration controls the login behavior users experience when they access applications. The authentication setting and the SSO setting affect the experience of accessing the application.

Table 3-4. Login Behavior for Users when Passcode is Set for SSO

Authentication Phase	SSO Enabled	SSO Disabled
Identify	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system identifies credentials against a common authentication system (username and password, token, and SAML).	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system identifies credentials against a common authentication system (username and password, token, and SAML).
Secure	■ Prompt if passcode exists: The system does not prompt for the passcode if the session instance is live. ■ Prompt if passcode does not exist: The system prompts users to create a passcode. ■ Session shared: The system shares the session instance across applications configured with Workspace ONE UEM SSO enabled.	■ Prompt if passcode exists: The system prompts users the application passcodes. ■ Prompt if passcode does not exist: The system prompts users to create a passcode. ■ Session not shared: The system does not share the session or the passcode with other applications.

Table 3-5. Login Behavior for Users when Username and Password is Set for SSO

Authentication Phase	SSO Enabled	SSO Disabled
Identify	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system identifies credentials against a common authentication system (username and password, token, and SAML).	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system prompts for application login credentials.
Secure	■ Prompt: The system does not prompt for the login credentials if the session instance is live. ■ Session shared: The system shares the session instance across applications configured with Workspace ONE UEM SSO enabled.	■ Prompt: The system prompts for the login credentials for the application on every access attempt. ■ Session not shared: The system does not share the session with other applications.

Table 3-6. Login Behavior for Users when Disabled is Set for SSO

Authentication phase	SSO enabled	SSO disabled
Identify	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system identifies credentials against a common authentication system (username and password, token, and SAML).	■ Silent login: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. ■ Authenticate: The system prompts for application login credentials.
Secure	Prompt: The system does not prompt users for authentication.	Prompt: The system does not prompt users for authentication.

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	Access corporate resources listed in the **Allowed Sites** field with the SSO credentials. Enter systems in the **Allowed Sites** text box to control access to a specific set of sites and domains. You must complete this setting for **Integrated Authentication** to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.
Use Certificate	Upload the **Credential Source** or set a **Defined Certificate Authority** to access corporate resources listed in the **Allowed Sites** text box with the SSO credentials. Enter systems in the **Allowed Sites** text box to control access to a specific set of sites and domains. You must complete this setting for **Integrated Authentication** to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.

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	Sets devices to access corporate resources using the Per-App Tunnel component of VMware Tunnel. 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. 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 **Device Traffic Rules** page before enabling it here. ■ Select **Configure Tunnel Settings** to enable the VMware Tunnel if you have not already set this feature. ■ If you have some SDK applications that still use **VMware Tunnel - Proxy**, enable **Tunnel Proxy for Backward Compatibility**. This menu item allows those SDK applications that have not migrated to Per-App Tunnel to continue to work using Proxy. This setting does not act as a backup. If your Tunnel gateway is not available, applications do not fall back to Proxy.
VMware Tunnel - Proxy	Sets devices to access corporate resources using the proxy component of the VMware Tunnel, also called Proxy. Consider migrating to the Per-App Tunnel component for better performance and new features. 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. ■ Select **Configure VMware Tunnel - Proxy Settings** to enable Proxy if you have not already set this feature. ■ Use **Allow all non-FQDN URLs through App tunnel** to control traffic to non-FQDN (fully qualified domain name) URLs through the tunnel. ■ **YES** - All non-FQDN URLs use the tunnel. ■ **NO** - Only non-FQDN that are explicitly listed in the **App Tunnel URLs** use the tunnel. ■ To restrict the communication to a set of tunnel domains, enter domains in the **App Tunnel URLs** text box. All other traffic not listed in this text box, goes directly to the Internet. Use wildcards to allow access to any site with a domain subset. For example, ***.<example > .com** allows traffic to any site that contains **.<example > .com** in its domain. Similarly, it allows access to any port on that site with an implementation similar to ***.<example > .com**. If nothing is listed in this text box, all traffic directs through the app tunnel.
Standard Proxy	Sets devices to request resources using a proxy server that allows or denies connections to enterprise systems.

Setting	Description

	■ To access your internal network, select an **App Tunnel Proxy** from the menu . Add standard proxies by selecting **Configure Standard Proxy Settings**.
	■ Use **Allow all non-FQDN URLs through App tunnel** to control traffic to non-FQDN (fully qualified domain name) URLs through the tunnel.
	  ■ **YES** - All non-FQDN URLs use the tunnel.
	  ■ **NO** - Only non-FQDN that are explicitly listed in the **App Tunnel URLs** use the tunnel.
	■ To restrict the communication to a set of tunnel domains, enter domains in the **App Tunnel URLs** text box. All other traffic not listed in this text box, goes directly to the Internet.
	  Use wildcards to allow access to any site with a domain subset. For example, ***.<example > .com** allows traffic to any site that contains **.<example > .com** in its domain. Similarly, it allows access to any port on that site with an implementation similar to ***.<example > .com**.
	  If nothing is listed in this text box, all traffic directs through the app tunnel.

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.

For information on Device Traffic Rules, access Create Device Traffic Rules.

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 need to 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 mulitple 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 **Yes**.
Enable Camera	Allows applications to access the device camera when set to **Yes**.
Enable Composing Email	Allows an application to use the native email client to send emails when set to **Yes**.
Enable Copy and Paste Out	Allows users to copy and paste content from SDK-built applications to external destinations when set to **Yes**. When you set it to **No**, the system allows copy and paste only between Workspace ONE UEM applications. 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. The system migrates the setting configured previously in the option to **Enable Copy and Paste** to this feature.

Setting	Description
Enable Copy and Paste Into	Allows users to copy and paste content from external destinations into SDK-built applications when set to **Yes**. When you set it to **No**, 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 **Yes**.
Enable Location Services	Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.
Enable Printing	Allows an application to print from devices when set to **Yes**.
Enable Screenshot	Allows applications to access screenshot functionality on devices when set to **Yes**.
Enable Third-Party Keyboards	On iOS devices when set to **No**, SDK-built applications always open in the native keyboard and prevent the use of third-party keyboards. On Android devices when set to **No** 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 **Yes**. Enter the content to display in the **Overlay Text** 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

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

  Branding - Splash Screens
- Logging
- Analytics
- Custom 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	Reflect your company colors by choosing colors for the Workspace ONE UEM console from the color palette beside the color options. Choose primary and secondary colors listed options including tool bars and text.
Organization Name	Enter the name that represents your organization to display in the Workspace ONE UEM system.

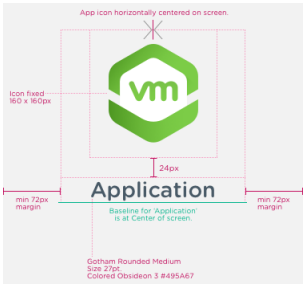
Device Backgrounds	Upload images that the system displays as the background and as the logo for the organization on the listed device types.
	■ Apple iOS options
	  ■ Background Image iPhone
	  ■ Background Image iPhone (Retina)
	  ■ Background Image iPhone 5 (Retina)
	  ■ Background Image iPad
	  ■ Background Image iPad (Retina)
	■ Android options
	  ■ Background Image Small
	  ■ Background Image Medium
	  ■ Background Image Large
	  ■ Background Image Extra Large
	■ Platform neutral options
	  ■ Company Logo Phone
	  ■ Company Logo Phone High Res
	  ■ Company Logo Tablet
	  ■ Company Logo Tablet High Resolution

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 3-1. 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 3-7. 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.

Table 3-7. SDK Logging Level APIs and Level Descriptions (continued)

Level	Logging API	Description
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 enable or disable 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

SDK App Compliance profiles help monitor and enforce compliance on devices that have 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
- Application Version
- OS Version
- Security Patch Date
- Where to Get Data

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
- 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's 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 field 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 evaluate this as 2. For a version number of 2.3.4.a, the SDK evaluates this as 2.3.4

OS Version

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

Here's 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

4

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.

This chapter includes the following topics:

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.

Procedure

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"`	The value for this key is the company's specific privacy policy URL. Navigate users to a specific privacy disclosure site from the productivity application. Users can review the policy so that they know the company's stance on privacy.
VMware Feature Usage Analytics	`"PolicyAllowFeatureAnalytics"`	■ `0` - Disabled ■ Prevents data sharing for all users of productivity applications. ■ This value prevents the display of the Data Sharing page in the productivity application. ■ `1` - Enabled ■ Users can decide if they want to share their usage data for productivity applications. ■ This value does display the Data Sharing page in the productivity application.	This key controls the display of the **Data Sharing** page within the productivity application. Users can opt in or out of sharing their feature usage analytics. Feature usage analytics collection helps VMware to improve existing products and to develop new ones.
Diagnostics Data Through VMware Workspace ONE Intelligence and Apteligent by VMware	`"PolicyAllowCrashReporting"` For this key to work, you must use Apteligent by VMware or VMware Workspace ONE Intelligence.	■ `false` - Disabled ■ Prevents the reporting of diagnostic data for productivity applications as reported by Apteligent by VMware and Workspace ONE Intelligence. ■ When disabled, your ability to investigate and resolve problems is reduced because your system receives no diagnostic data for productivity applications from Apteligent by VMware or Workspace ONE Intelligence. ■ `true` - Enabled ■ Sends diagnostic data for productivity applications as reported by Apteligent by VMware and Workspace ONE Intelligence. ■ When set to `true`, your system receives diagnostic data for productivity applications from	This key controls reporting diagnostic data from Apteligent by VMware and Workspace ONE Intelligence. Apteligent by VMware and Workspace ONE Intelligence are tools that help analyze, troubleshoot, and maintain applications and enterprise mobility management deployments.

Name	Key	Value	Description
		Apteligent by VMware and Workspace ONE Intelligence to help with investigating and resolving problems.	

```
{
    "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 Apteligent by VMware and Workspace ONE Intelligence.

4 Save your settings.